Faculteit Wetenschappen
Vakgroep Wiskunde
Oktober 2012

Contributions to Pure and Applicable Galois Geometry

Cornelia Rößing

Promotor: Prof. Dr. L. Storme

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

Preface

The term *Galois geometry* originates from an article by Segre [86], wherein he refers to a finite projective plane as Galois plane. Later, Hirschfeld and Thas in their book *"General Galois geometries"* [44] denominate finite projective spaces as Galois geometries. Indeed, both Segre, and Hirschfeld and Thas are united in their desire of emphasizing that an analytical approach to finite projective geometry is predicated on finite or Galois fields and their (Galois) extensions, thus recognising the important contributions made by the famous French mathematician É. Galois (1811-1832) in algebra.

All geometries discussed in this thesis are finite and can be constructed in a finite projective space, such as *generalised quadrangles* (Chapter 1, Section 1.2) or as *egglike inversive planes* (Chapter 1, Section 1.4). In the case of inversive planes, the more common algebraic constructions are based on finite fields and their cubic extensions. Indeed, one can view Galois geometry as the concept that encompasses all analytical geometries over a finite field and its extensions [33]. In Chapter 1 the relevant definitions and theorems for these geometries are gathered for reference later on.

Generalised quadrangles were introduced by J. Tits in his famous paper of 1959 wherein he defines the more general class of generalised polygons [22]. Research also conducted at this time on finite polar spaces established that certain classes of generalised quadrangles can be viewed as a certain class of polar spaces and vice versa. Here we will refer mostly to the definitions and results of S. E. Payne and J. A. Thas [72]. Together with generalised quadrangles, their substructures, such as ovoids and spreads, have been studied. Furthermore, the existence and non-existence of maximal partial ovoids and spreads became a source of research interest; with this later developing into a search for non-interrupted intervals (with respect to the size) of maximal partial ovoids and spreads. In Chapters 2, 3 and 4 we introduce spectra of this kind.

Chapter 2 deals with the case in which the order of the generalised quadrangle is even. Here our results for maximal partial ovoids of the generalised quadrangle $Q(4,q)$ give equivalent results for the generalised quadrangle $W(q)$ as well as for maximal partial spreads of both. Furthermore the same result can be transferred into a result for minimal blocking sets with respect to the planes in $PG(3,q)$ and for maximal partial 1-systems of the Klein quadric. To obtain similar results for the case when the order is odd, we need to differentiate. In Chapter 3, we present a spectrum result for maximal partial ovoids of $Q(4,q)$ which is then equivalent to a spectrum of maximal partial spread of $W(q)$. In Chapter 4, we introduce a spectrum for minimal blocking sets with respect to the planes of $PG(3,q)$ which is known to be equivalent to a spectrum of maximal partial 1-systems of the Klein quadric.

Chapters 5 and 6 focus on inversive planes (originally *Möbiusebenen*) which were introduced by A. F. Möbius (1790-1868) in his work of 1827 entitled *"Der barycentrische Calcul"* [69]. Möbius was primarily known for his work in topology, and besides this the Möbius-strip, Möbius-transforms, and

Möbius-planes were named after him. In his work of 1827, Möbius focuses on geometric transforms; in particular, on a group isomorphic to $PGL(2, L)$, which is today known as the group of Möbius-transforms. These automorphisms of the affine plane map conics onto conics, which he describes as a constant double ratio (doppelverhältnistreu); we will see in Chapter 1, Section 1.4 that they also describe inversive planes. The phrase *inversive planes* goes back to F. Klein (1849-1925) who characterised these planes by using a different group of automorphisms, the inversions, which fix a circle point-wise (see [27, page 219]). As Laguerre planes and Minkowski planes, inversive planes belong to the class of circle geometries.

In Chapter 5, we characterise subplanes of Miquelian inversive planes taking a synthetic and an analytical approach. This characterisation then leads to the characterisation of a certain class of automorphisms of the inversive plane called planar automorphisms. Chapter 6 deals with different aspects of blocking sets; in particular, the issue of cardinality and which substructures may possess promising properties.

Our final chapter deals with an up to date application of generalised quadrangles and inversive planes in coding theory. *Low-density parity-check (LDPC) codes* rank among the most popular codes used today as their outstanding performance has made them the code of choice. They perform close to the *Shannon limit*, the theoretical bound for possible coding. LDPC codes are used for data transfer in and between computers as well as in satellite transmission. They where invented by R. G. Gallager in 1963, however, their practical application has only been made possible with more recent hardware developments. In Chapter 7, we present, among others, our patent-pending LDPC code which we developed from an inversive space (Chapter 7, Section 7.8).

Acknowledgements

First of all I would like to express my gratitude to Leo Storme, not only for sharing his mathematical knowledge, but also for his patience and understanding. Over the years I got a lot of help for this project in many ways. I would like to thank the people who introduced to me to this topic; the questions and challenges arising around these geometries will keep me occupied far beyond this thesis. I would also like to thank my family, for the compromises they had to deal with, from quick meals to lateness, and for challenging my stubbornness. Many friends and extended family I would like to thank for helping me either with mathematical questions along the way or taking other duties of my shoulders, or even both. I would like to thank the person who always believed I could do this. Last but not least, I would like to thank everybody helping me to get these pages together.

Cornelia Rößing Dublin, September 10, 2012

Contents

List of Figures

1 Introduction

The first chapter is a collection of definitions and known facts, starting with incidence geometry and later developing into Galois geometry. This is to provide the reader with axioms, definitions and theorems for future reference.

1.1 Basic Concepts

Besides the definition of projective and affine geometries, we will recall the structure records like the Theorems of Desargues and Pappus. At the end of this section you will find the definition of ovals and ovoids which play a crucial role for generalised quadrangles (Section 1.2) and for inversive planes (Section 1.4). One can find this information and read further in e.g. [10], [12], [31] or [89].

Projective Spaces

Definition 1.1 An incidence structure consisting of points and lines is called a *projective space* $\mathbb{P}$ if the following three axioms hold:

1. Any two distinct points P, Q are incident with a unique line; we denote this line here by $\overline{PQ}$.

2. Every line is incident with at least three points.

3. The *Veblen-Young-Axiom* (see Figure 1.1) holds:

   Let G_1, G_2, H_1, H_2 be four points, such that the line $\overline{G_1G_2}$ is intersecting with $\overline{H_1H_2}$, then also the lines $\overline{G_1H_1}$ and $\overline{G_2H_2}$ intersect.

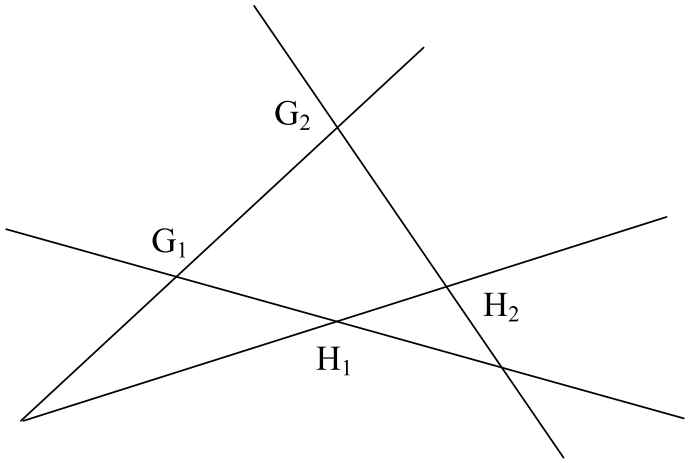

Figure 1.1: Veblen-Young-axiom

A *subspace* $\mathbb{U}$ of a projective space is an incidence structure comprising a subset of the lines and points of the projective space such that for any two distinct points of $\mathbb{U}$ the connecting line is contained in $\mathbb{U}$:

$$\forall\, P, Q \in \mathbb{U} \;\Rightarrow\; \overline{PQ} \in \mathbb{U}.$$

It follows that $\mathbb{U}$ is a projective space itself. Immediate examples for subspaces of a projective space are a point, a line, a hyperplane and the space itself. A point set S is said to *span* or *generate* a subspace $\langle S \rangle$ when $\langle S \rangle$ is the intersection of all subspaces containing S. A point set S is called *independent*, if for all points $P \in S$, $P \notin \langle S - \{P\} \rangle$.

Finally the *dimension* d of a projective space $\mathbb{P}$ is the cardinality of a minimal, independent spanning set minus one. A spanning set S is minimal, if no proper subset of S spans $\mathbb{P}$.

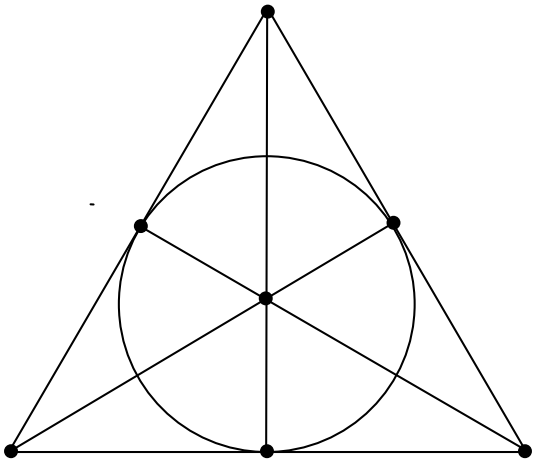

Figure 1.2: PG(2,2) or Fano plane

In a finite projective space of dimension d, every line contains $q+1$ points, where q is the *order* of the projective space, and we will write $PG(d,q)$ instead of $\mathbb{P}$ for the finite projective space over the field of order q. We will come back to this notation when we approach projective spaces via vector spaces in Theorem 1.4 (for $d \geq 3$ all projective spaces can be defined this way, but not all projective planes) and in Theorem 1.5 where we defined them by a finite field of order q. Furthermore $PG(d,q)$ contains $q^d+q^{d-1}+\ldots+q+1$ points. A subspace of dimension 2 is called a *projective plane*. For the smallest example see Figure 1.2. A subspace of $PG(d,q)$ with dimension $d-1$ is called a *hyperplane*.

Affine Spaces

One can view an *affine geometry* as a kind of restriction of the projective geometry, or as its native variant, the raw model for the geometry surrounding us. The main difference, the existence of parallelism, seems natural to us; we are used to consider e.g. lines as parallel. It is not surprising that one geometry can be obtained from the other.

First we construct an affine space from a projective space by cutting out a hyperplane.

Definition 1.2 For a projective space $\mathbb{P}$ of dimension at least 2 and a hyperplane H_∞ we define the geometry $\mathbb{A} = \mathbb{P} \setminus H_\infty$ in the following way:

- The points of $\mathbb{A}$ are those points of $\mathbb{P}$ which are not contained in the hyperplane H_∞.
- The lines of $\mathbb{A}$ are the lines of $\mathbb{P}$ which are not lines of H_∞.
- The t-dimensional subspaces of $\mathbb{A}$ are the t-dimensional subspaces of $\mathbb{P}$ which are not contained in H_∞.
- The incidence of $\mathbb{A}$ is induced by the incidence of $\mathbb{P}$.

The set of all subspaces of $\mathbb{A}$ is called an affine geometry.

This way an affine plane can be derived from a projective plane by removing a line; this line H_∞ is often referred to as the *line at infinity*. If we want to define an affine plane from scratch we need to introduce parallelism. We will do this now using Playfair's parallel axiom.

Definition 1.3 An incidence structure comprising points and lines is called an *affine plane* if the following axioms are satisfied:

1. Every two distinct points are incident with a line.
2. There is an equivalence relation on the lines called *parallelism* which respects the *parallel-axiom*:

   Let g be a line and P a point not incident with g. Then there is a unique line incident with P but not intersecting g.
3. There are three points which are not collinear.

A finite affine plane, denoted as $AG(q)$, contains q^2 points, where q is the order of the affine plane; an affine space $AG(d,q)$ has dimension d and order q. Like in the projective case we will see in Theorem 1.5 that the order q is the order of the finite field; thus the affine space of dimension d and order q consists of q^d points. The smallest examples, of order 2 and 3, are shown in Figure 1.3.

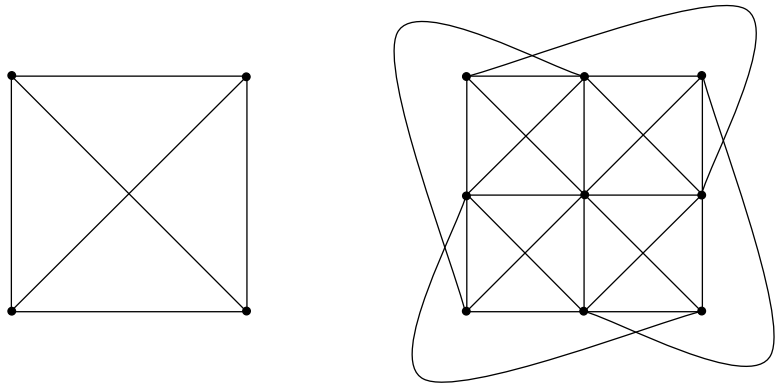

Figure 1.3: $AG(2)$ and $AG(3)$

A *subplane* of an affine plane is a substructure which is an affine plane itself and its parallelism is the restricted parallelism of the affine plane.

We will now enhance the purely incidence geometric approach and embark on the study of algebraic representations of different geometries and their objects, commencing with the two geometries we have introduced so far, $\mathbb{P}$ and $\mathbb{A}$.

The following Theorems of Desargues and Pappus are used to characterise projective and affine geometries: a Desarguesian geometry of dimension d can be derived from a vector space $V(d+1,K)$ where K is an arbitrary field or even a skewfield; for a Pappian geometry K needs to be commutative. Therefore they are also called *Representation Theorems*.

The Theorem of Desargues

For the formulation of the Theorem of Desargues the following property of triangles is useful: Two triangles are said to be *central* to each other if the connecting lines of corresponding vertices intersect in one point. They are *axial* to each other if the intercepts of corresponding sides, or accordingly their extensions, are collinear.

Theorem 1.4 *(Theorem of Desargues) Every pair of axial triangles is also central and vice versa.*

Figure 1.4 shows the Desargues Configuration.

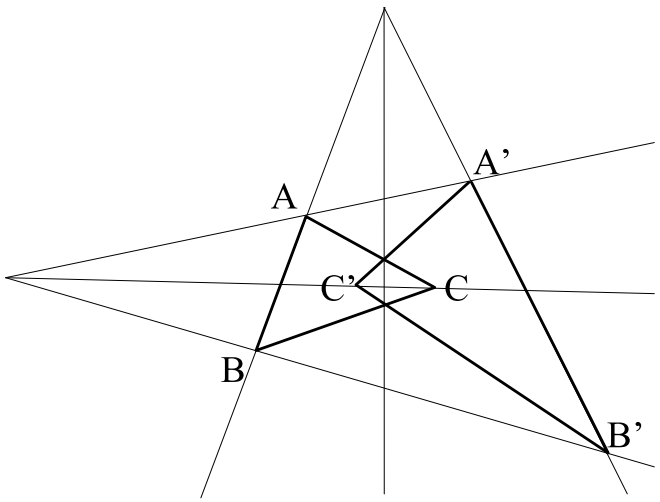

Figure 1.4: Theorem of Desargues

A geometry is called Desarguesian, if the Theorem of Desargues holds.

There are non-Desarguesian projective and affine planes, but it is well known that all projective spaces of dimension 3 or higher are Desarguesian. There is a fundamental coherence between Desarguesian projective spaces and vector spaces:

A vector space V of dimension $d+1$ induces a Desarguesian projective space $P(V)$ of dimension d. Whereas the one-dimensional subspaces are identified with the points of the geometry, the two dimensional subspaces correspond to the lines and the incidence is given by the set-theoretic inclusion. All Desarguesian projective spaces can be represented by a suitable vector space V and will be therefore referred to as $P(V)$.

This way we can introduce (homogeneous) coordinates for projective points. For a fixed basis $v_0, \ldots, v_d$ of V we can express any vector

$$v = a_0 v_0 + a_1 v_1 + \cdots + a_d v_d \in V$$

uniquely by its coordinates $(a_0, \ldots, a_d)$. We take the usually normalised vector $(a_0, \ldots, a_d)$ as a representative of the equivalence class of all multiples (except $(0, \ldots, 0)$) and write $P = (a_0 : \ldots : a_d)$ for the homogeneous coordinates of a point P. In particular the two-dimensional vector space gives an example for the projective line (see Remark 1.6). We will use a projective line later on for a popular construction of inversive planes (see Theorem 1.25).

The Theorem of Pappus

Theorem 1.5 *(Pappus' Theorem) If the points P_1, P_2 and P_3 of a projective or affine plane are collinear and if also the points P_4, P_5 and P_6 are collinear, but none is incident with both lines, then the intersection points $Q_1 := \overline{P_1P_5} \cap \overline{P_2P_4}$, $Q_2 := \overline{P_1P_6} \cap \overline{P_3P_4}$ and $Q_3 := \overline{P_2P_6} \cap \overline{P_3P_5}$ are collinear as well (see Figure 1.5). A projective or affine space $\mathbb{A}$ is called* Pappian *if it satisfies this theorem.*

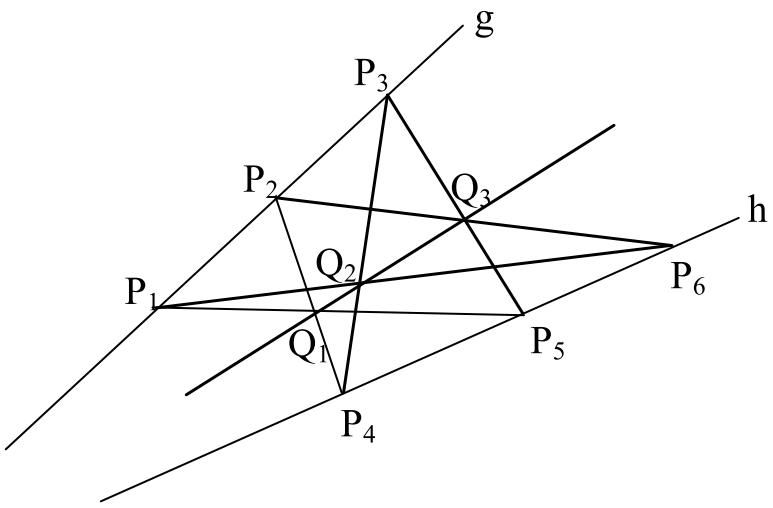

Figure 1.5: Pappus' Theorem

Pappus' Theorem implies Desargues' Theorem (see e.g. [31]). Furthermore, the Pappian affine geometries are induced by a commutative vector space. Thus for a Pappian affine plane $\mathbb{A}$ there is a commutative field K such that $\mathbb{A} \cong AG(K^2)$ where $AG(K^2) = (P, G)$ and

$$\begin{aligned} P &:= K^2 \\ G &:= \{x + Ky \mid x, y \in K^2 \text{ with } y \neq 0\}. \end{aligned}$$

If $\mathbb{A}'$ is a subplane of a Pappian affine plane $\mathbb{A}$ then also $\mathbb{A}'$ is Pappian.

Hence we have an algebraic description of affine and projective planes. In the finite case we can write $AG(q)$ where q is the order of the field. For a finite projective space $PG(d, q)$ or $PG(d, K)$ the field K of order q is the underlying field of the vector space, and d is the dimension of the projective space, thus one less than the dimension of the vector space.

Remark 1.6 For a field K the *projective line* is the set of all one-dimensional subspaces of the two-dimensional space K^2. So $PG(1, K) = PG(K^2) = \{K(x, y) \mid (x, y) \in K^2 \setminus \{0, 0\}\} = \{(0, 1)\} \cup \{(1, x) \mid x \in K\}$.

In a projective plane $\mathbb{P}$ the role of points and lines can be exchanged and the result is again a projective plane, which is not necessarily isomorphic to $\mathbb{P}$. The hereby obtained projective plane is called the *dual* projective plane. If the points and lines of the projective plane $PG(2, K)$ are interchanged, one obtains indeed the same projective plane, thus $PG(2, K)$ is called *self-dual*. The same can be done with an arbitrary projective space, for a projective space we obtain its dual by interchanging the i-dimensional subspaces with $(n - i - 1)$-dimensional subspaces, i.e. points are exchanged with hyperplanes. As a projective space of dimension 3 or higher is induced by a vector space, it is self-dual.

Polarities

A bijection between two projective spaces is called a *collineation* if it preserves the incidence. In particular, if φ is a collineation between two projective spaces with subspaces α and β resp., then $\alpha \subset \beta \Leftrightarrow \alpha^\varphi \subset \beta^\varphi$. This implies that the projective spaces must have the same dimension.

Definition 1.7 A collineation between the projective lines $PG(1,K)$ and $PG(1,K')$ is defined by a bijective semi-linear transformation between $PG(1,K)$ and $PG(1,K')$. If the collineation maps a projective space onto itself, it is called an *automorphism*.

Now consider the Desarguesian projective space $PG(d,q)$ with the underlying vector space V of dimension $d+1$, then every bijective semi-linear map of V induces a collineation in $PG(d,q)$. The *Fundamental Theorem of Projective Geometry* states that the opposite holds as well, every collineation in the Desarguesian projective space induces a semi-linear map of the vector space. Therefore we can describe collineations by semi-linear maps and make use of the coordinate description.

Thus a collineation between two points X and X' in the projective space $PG(d,q)$ can be described by the relation between the two coordinate vectors of these points in V which can be expressed by a non-singular $(d+1)\times(d+1)$ matrix A and field automorphism ϕ of the underlying field of the vector space: $tX' = X^\phi A$, where $X^\phi = (x_0^\phi, \ldots, x_d^\phi)$ and $t \in \mathbb{F}_q \backslash \{0\}$.

A collineation φ between a projective space and its dual space is called a *polarity* when φ is involutory, i.e. $\varphi^2 = id$. It follows that a polarity is a bijection which inverses containment, thus for subspaces α and β with $\alpha \subset \beta \Rightarrow \alpha^\varphi \supset \beta^\varphi$.

Thus a polarity φ maps the point P onto a hyperplane P^φ, called the *polar* of the point and conversely φ maps a hyperplane π onto a point π^φ, called the *pole* of π. If a point Q is incident with the hyperplane P^φ, then P is incident with Q^φ and P and Q are *conjugate* points, conversely P^φ and Q^φ are *conjugate* hyperplanes. Now a *self-conjugate* point P is therefore incident with its polar, we call P *absolute*. A hyperplane is self-conjugate if it contains its pole. A subspace π is *self-conjugate* if either $\pi \subseteq \pi^\varphi$ or $\pi^\varphi \subseteq \pi$; self-conjugate subspaces are called *isotropic*. The *projective index* of a polarity is the dimension of its maximal isotropic subspaces.

We defined a polarity as a collineation, thus in $PG(d,q)$ we can define it by a $(d+1)\times(d+1)$-matrix A and an involutory field automorphism $\phi \in Aut(\mathbb{F}_q)$. This way we know that a point X is self-conjugate iff $XA(X^\phi)^T = 0$. If the field automorphism ϕ is the identity, the polarity is characterised by the matrix A:

If $A = A^T$ then φ is an *orthogonal polarity* for odd order, and a *pseudo polarity* for even order. In the first case the self-conjugate points form a quadric, in the second case the self-conjugate points form a hyperplane.

The case that $-A = A^T$ only occurs for odd dimension and the polarity is called *symplectic* and all points of the projective space are self-conjugate.

If ϕ is not the identity, q is a square, and $(A^T)^\phi = A$ then φ is called a *unitary or Hermitian polarity* and the self-conjugate points are the points of a *Hermitian variety*.

For more details about polarities, see [98].

Quadrics and Conics

A *quadric* is the zero space of a quadratic equation in $PG(d,q)$. The coordinates of the points of a quadric satisfy an equation of the form

$$\sum_{i,j=0}^{d} a_{ij}X_iX_j = 0$$

where $i \leq j$ and not all $a_{i,j} = 0$. If the dimension is two we call such a quadric a *conic*. In a projective space of even dimension there is, up to collineations, only one non-singular quadric; it is called the *parabolic quadric* $Q(2n,q)$ with standard form:

$$x_0^2 + x_1x_2 + \ldots + x_{2n-1}x_{2n} = 0.$$

In odd dimensions the *hyperbolic quadric* $Q^+(2n+1,q)$ exists. The standard form for a hyperbolic quadric is:

$$x_0x_1 + \ldots + x_{2n}x_{2n+1} = 0.$$

The best known hyperbolic quadric is probably $Q^+(5,q)$, also known as the *Klein Quadric*. The remaining class is $Q^-(2n+1,q)$, the *elliptic quadric*, given by a polynomial:

$$f(x_0,x_1) + x_2x_3 + \ldots + x_{2n}x_{2n+1} = 0,$$

where f is an irreducible homogeneous quadratic polynomial over $\mathbb{F}_q$.

Polar Spaces

Taking a more abstract point of view we can get a geometry arising from quadrics, the *polar spaces*. These geometries were first studied by F. D. Veldkamp [103]. His work was taken further by J. Tits [102] which led to the following axiomatic description:
A *polar space* of rank $n \geq 2$ is a set $\mathbb{P}$ of points together with a family of subsets of $\mathbb{P}$ called *subspaces* which satisfy the following axioms.

- A subspace together with all its subspaces is a projective space $PG(d,q)$ with $-1 \leq d \leq n-1$ of dimension d.
- The intersection of two subspaces is again a subspace.
- Given a subspace V of dimension $n-1$ and a point P not contained in V, then there is a unique subspace W consisting of P and all lines joining P to points in V. Then W has dimension $n-1$ and $V \cap W$ has dimension $n-2$.
- There are two disjoint subspaces of dimension $n-1$.

F. D. Veldkamp [103] and J. Tits [102] also classified the finite polar spaces. There are five structures of rank at least three, the finite classical polar spaces:

- In even dimensions the non-singular parabolic quadric $Q(2n,q)$ together with the subspaces of $PG(2n,q)$ completely contained in the quadric gives a polar space of rank n.

- For odd dimension there is the non-singular elliptic quadric $Q^-(2n+1,q)$ with those subspaces of $PG(2n+1,q)$ which are contained in the quadric. The polar space has then rank n.

- The non-singular hyperbolic quadric $Q^+(2n+1,q)$ gives another polar space derived from an odd dimensional projective space. It consists again of the quadric and those subspaces of the projective space, which are completely contained in the quadric. This polar space has rank $n+1$.

- The polar space arising from the non-singular symplectic polarity $W(2n+1,q)$ has rank $n+1$. It consists of the isotropic subspaces of the projective space with respect to the symplectic polarity.

- There is another class of polar spaces derived from *Hermitian varieties* $H(n,q^2)$. For further information see [8].

There exist certain dualities among these polar spaces:

For even order, $W(3,q)$ and $Q(4,q)$ are isomorphic and self dual, while for odd order they are isomorphic to each others dual. The elliptic quadric $Q^-(5,q)$ is isomorphic to the dual of $H(3,q^2)$.

Furthermore $W(2n-1,q)$ and $Q(2n,q)$ are isomorphic for q even. The non-singular parabolic quadric $Q(2n,q)$, q even, has a nucleus, projecting all subspaces incident with this nucleus onto a hyperplane of $PG(2n,q)$ not containing the nucleus together with all subspaces. This way we can derive a symplectic polarity for $W(2n-1,q)$.

The polar spaces of rank 2 are the *generalised quadrangles* which we will study in Section 1.2.

Ovals

We start with the definition of a tangent line and an arc:

Definition 1.8 A set of k points in a projective or affine plane is referred to as a *k-arc*, if no three points are collinear. A line is called a *tangent line* to a set of points if it intersects in one point only. An *oval* is a k-arc, which has exactly one tangent line in each point.

A point P not incident with an oval O is called an *internal point* of O, if no line incident with P is tangent to O. If there is a tangent line through P, we call P an *external point*. If all tangent lines of an oval intersect in one point we call this point the *nucleus* of the oval.

So we can say that an oval in the affine plane is a maximal set of points such that no three are collinear and there is one tangent line for each point.

Theorem 1.9 *A k-arc of a projective or affine plane of order q is an oval, iff $k = q+1$ [26].*

If the order of the plane is even, it follows from the Theorem of Qvist [10, 78], that there exists a nucleus. In the affine plane this means that every parallel class has one line tangent to the oval. For odd order we know that either two or no tangent lines are incident with every point not on the oval. Thus in the affine plane out of every parallel class there are either two tangent lines or none.

Ovoids

Definition 1.10 An *ovoid* in the projective space is a set $\mathbb{O}$ of points such that:

1. Every line intersects $\mathbb{O}$ in at most two points, in other words, no three points of $\mathbb{O}$ are collinear.
2. For every point $P \in \mathbb{O}$, the union of all lines tangent to $\mathbb{O}$ in P is a hyperplane, or vice versa, all lines of this hyperplane incident with P are tangent to $\mathbb{O}$.

For a finite projective space $PG(d,q)$ the second condition is equivalent to the fact that an ovoid has $q^{d-1}+1$ points. Furthermore it is easy to see that there are no ovoids in $PG(d,q)$ for $d>3$.
In a 3-dimensional projective space of odd order every ovoid is a non-singular elliptic quadric, the points of the ovoid are the absolute points of an orthogonal polarity $(A^T = A)$.
An ovoid in $PG(3,q)$, q even, can be derived from a non-singular elliptic quadric. This quadric defines a symplectic polarity $(A^T = -A)$. There is also a second example of an ovoid in $PG(3,q)$, $q = 2^{2h+1}$, $h \geq 1$, known as the *Segre-Tits ovoid* [31].

Linear Spaces and Partial Linear Spaces

A more general concept than the projective geometries are the *linear spaces*. If we want to reconcile the geometry in the following sections with the previous we even need to loosen the restrictions further and use the description of a *partial linear space*. The *generalised quadrangles* in Section 1.2 are examples for partial linear spaces as well as a geometry defined in Chapter 7, Theorem 7.18.

Definition 1.11 A *linear space* is an incidence structure consisting of points and lines such that:

1. Any two distinct points are incident with a unique line.
2. Any line contains at least two points.
3. There are at least two lines.

In Figure 1.6, we present all linear spaces with five points. For simplification, lines connecting only two points are left out.

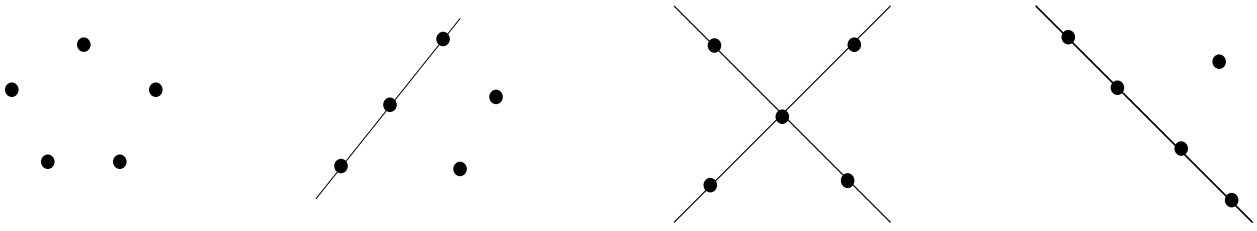

Figure 1.6: Linear spaces with 5 points

Now *partial linear spaces* carry slightly less structure, as the first axiom is replaced by

1. Any two points are incident with at most one line.

Compared to four different linear spaces with 5 points, there are 64 partial linear spaces with 5 points.

1.2 Generalised Quadrangles

Generalised quadrangles were first introduced by J. Tits [101] and can be linked to polar spaces and generalised polygons (see page -7). An incidence structure consisting of points and lines is called a *finite generalised quadrangle* $GQ(s,t)$ if the following axioms hold:

- every line is incident with $s+1$ points, and every point is incident with $t+1$ lines,
- two different lines can intersect in at most one point, and two different points can share at most one line, and
- for any non-incident point-line pair (P,l), there exists a unique line m and unique point Q such that P is incident with m, m is incident with Q, and Q is incident with l.

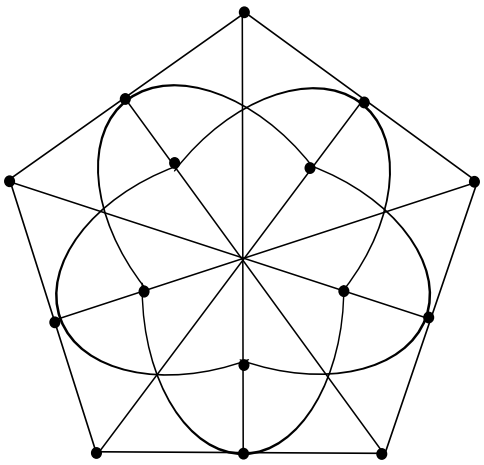

Figure 1.7: GQ(2,2) or W(2)

The parameters s and t are called the *order* of the generalised quadrangle. The points and lines of a non-singular 4-dimensional parabolic quadric $Q(4,q)$ form a classical example of a finite generalised quadrangle of order $(s,t)=(q,q)$ (see Figure 1.7 where q is 2). The parabolic quadric $Q(4,q)$ of $PG(4,q)$ is the quadric having $X_0^2+X_1X_2+X_3X_4=0$ as canonical equation.

Examples 1.12 The other examples of finite classical generalised quadrangles are:

1. the non-singular 5-dimensional elliptic quadrics $Q^-(5,q)$,
2. the non-singular 3-dimensional hyperbolic quadrics $Q^+(3,q)$,

3. the Hermitian varieties $H(3,q^2)$ and $H(4,q^2)$ in three and four dimensions, and

4. the points of $PG(3,q)$ and the totally isotropic lines under the symplectic polarity φ form $W(q)$.

Definition 1.13 Let x,y be points of a generalised quadrangle $GQ(s,t)$, then we say that x and y are *collinear* and write $x \sim y$ if there is a line incident with both points. Every point is said to be collinear with itself. We denote by P the set of points of a generalised quadrangle and for $x \in P$ let $x^\perp = \{y \in P \mid y \sim x\}$. The *trace* $\{x,y\}^\perp$ of two distinct points x,y is defined as $x^\perp \cap y^\perp$. If $x \sim y$ it is clear that $|\{x,y\}^\perp| = s+1$ and for $x \nsim y$ we know $|\{x,y\}^\perp| = t+1$. Now the *span* of a pair (x,y) of distinct points is defined as $\{x,y\}^{\perp\perp} = \{u \in P \mid u \in z^\perp; \forall z \in \{x,y\}^\perp\}$. For $x \nsim y$ the span $\{x,y\}^{\perp\perp}$ is called the *hyperbolic line* of x and y.

We refer to the standard reference [72] for more information on generalised quadrangles.

Ovoids and Spreads of Generalised Quadrangles

An *ovoid* $\mathbb{O}$ of a generalised quadrangle is a set of points such that every line of the generalised quadrangle is incident with exactly one point of $\mathbb{O}$. A *partial ovoid* is a set of points that shares at most one point with every line of the generalised quadrangle, and the partial ovoid is called *maximal* when it is not contained in a larger partial ovoid. Examples for the generalised quadrangle $GQ(2,2)$ are shown in Figure 1.8.

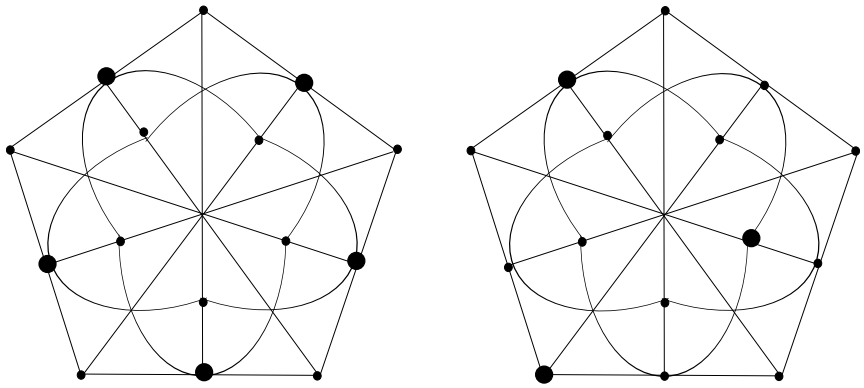

Figure 1.8: Ovoid and partial ovoid of $GQ(2,2)$

A set of lines of a generalised quadrangle is called a *spread* R, if every point of the generalised quadrangle is incident with a unique line of R. A *partial spread* is a set of lines, such that every point of the generalised quadrangle is incident with at most one line of R. A partial spread is *maximal*, whenever it is not contained in a larger partial spread. Figure 1.9 shows an example for a spread and a partial spread of $GQ(2,2)$.

Particular interest has been paid to the existence and non-existence of ovoids in generalised quadrangles [99, 100]. The results of Ebert and Hirschfeld [32] translate into results on the smallest maximal partial ovoids of $Q^-(5,q)$. The result of Aguglia, Ebert, and Luyckx [1] presents the minimal size of a maximal partial ovoid of $H(3,q^2)$. Recently, research has been done to find

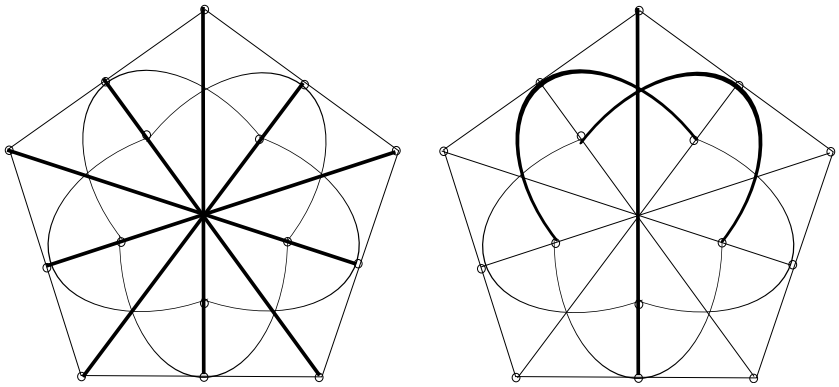

Figure 1.9: Spread and partial spread of $GQ(2,2)$

spectra of sizes of maximal partial ovoids [23, 24], by using computer resources. We contribute in Chapter 2 to this study with a spectrum result on maximal partial ovoids of $Q(4,q)$, for q even and in Chapter 3 for q odd.

The last point is motivated by the observation that the defining property of a generalised quadrangle as well as of an incidence structure derived from an inversive space, see Section 1.4, Definition 1.33, can be weakened in order to obtain larger classes of partial linear spaces. These geometries will also be used in Chapter 7.

Definition 1.14 A partial linear space $\mathbb{S} = (P, L)$ is called an (α, β)*-geometry* if whenever (p, ℓ) is a non-incident point-line pair there are either α or β points on ℓ which are collinear with p.

For further information, see [22, Chapters 3 and 10].

1.3 Designs and Blocking Sets

Many finite geometries have certain regularities which enable them to be viewed combinatorially only. The whole geometric structure is determined by a few parameters. For further information see [31].

Definition 1.15 A *design* consists of a set of elements, we call these elements *points*, and subsets of this set, we call these subsets *blocks*. Now if the number of points is v, every block is incident with exactly k points, and every t points are incident with precisely λ blocks, we call it a $t-(v,k,\lambda)$ *design*.

A whole theory deals with these finite structures: combinatorics. We will make use of many techniques and results which were developed combinatorially. A well known substructure for geometries and designs is the following:

Definition 1.16 In an incidence structure comprising points and blocks a subset of the point set is called a *blocking set* if every block is incident with at least one point of the set. A blocking set is called *irreducible* or *minimal*, if this property gets lost for every proper subset. If an irreducible

blocking set does not include an entire block it is called *non-trivial*. In this case also the complement is a blocking set.

Some publications use the term *intersection set* instead of blocking set, in this case a minimal, non-trivial intersection set is referred to as a blocking set.

An example for a blocking set of a projective plane is the set of points of a line, in an affine plane we can use the points of two intersecting lines. In every incidence structure the entire point set is also a blocking set. All these examples are trivial blocking sets.

For a projective or affine plane of order q^2, meaning that the order is a square number, a subplane of order q is a minimal, non-trivial blocking set. This subplane is called a *Baer subplane*.

In Chapter 2 and 4 we will also discuss blocking sets with respect to the planes of $PG(3,q)$. This is a set of points intersecting every plane in at least one point. It was proven by Bruen and Thas [21] that a minimal intersection set of this type has at most size q^2+1, and that every minimal blocking set of $PG(3,q)$ of size q^2+1 is equal to an ovoid of $PG(3,q)$, i.e., a set of q^2+1 points intersecting a plane in either one or $q+1$ points. For q odd, this implies the complete classification of the minimal intersection sets of size q^2+1 since Barlotti proved that every ovoid of $PG(3,q)$, q odd, is equal to an elliptic quadric [3]. For q even, next to elliptic quadrics, there exist the Segre-Tits ovoids in $PG(3,q)$, $q=2^{2h+1}$, $h\geq 1$ (further details are in [101]).

Regarding large minimal blocking sets with respect to the planes in $PG(3,q)$, Metsch and Storme proved the non-existence of minimal blocking sets of size q^2-1, $q\geq 19$, and of size q^2 [65]. Attention has also been paid to the smallest minimal blocking sets with respect to the planes of $PG(3,q)$. By Bose and Burton [16], the lines are the smallest minimal blocking sets with respect to the planes of $PG(3,q)$. Bruen proved that the smallest non-trivial blocking sets with respect to the planes of $PG(3,q)$ coincide with the smallest non-trivial blocking sets with respect to the lines of a plane $PG(2,q)$ [19]. These results will be extended in corresponding chapters.

1.4 Inversive Planes

This geometry was discovered by A. F. Möbius in 1827, and named after him *Möbius plane*. The English name *inversive plane* goes back to F. Klein (see page -7). Möbius planes belong together with Minkowski and Laguerre planes to the class of circle geometries, these are incidence structures whose blocks are not lines but circles. The inversive planes allow multiple geometric and algebraic representations. In this section we will provide some of these representations as they enable us to pose problems in inversive planes in different settings. There is for example a coherency between inversive planes and affine planes (see Theorem 1.19) which enables us to transfer known facts of the affine plane to inversive planes. The purpose of the introduction to inversive planes is also to provide the fundamental theorems for inversive planes like the bundle theorem and Miquel's theorem.

Definition 1.17 An *inversive plane* or *Möbius plane* is an incidence structure $\mathbb{M}=(P,C)$ where P is a set of *points* and $C\subset 2^P$ a set of *circles* satisfying the following three axioms:

(i) Any three points are contained in exactly one circle.

(ii) If P and Q are points such that P is incident with a circle c and Q is not incident with c then there exists a unique circle d which is incident with Q and intersects c in P only.

(iii) There exist at least four points that are not incident with one circle.

We call the points incident with one circle *concircular*. Two circles sharing exactly one point are called *tangent*, we denote a circle to be tangent to itself.

Definition 1.18 The *internal structure* of an inversive plane $\mathbb{M} = (P, C)$ with respect to one of its points R is the following incidence structure consisting of points and lines:

$$\mathbb{M}_R := (P \setminus \{R\}, C_R) \text{ where } C_R := \{c \setminus \{R\} \mid c \in C \text{ with } R \in c\}.$$

Theorem 1.19 *An incidence structure (where each block is incident with at least one point) is an inversive plane, iff the internal structure taken in any point is an affine plane.*

As mentioned above, this theorem enables us to transfer problems between Möbius planes and affine planes.

Definition 1.20 The set of all circles which are pairwise tangent in one point is called a *pencil*, the point of intersection is called the *carrier*. Such a pencil is uniquely defined by its carrier and a circle or by two of its circles. The pencils with carrier P are the parallel classes in $\mathbb{M}_P$; those circles not incident with P are ovals in $\mathbb{M}_P$ [10]. The set of circles incident with two points P and Q is called a *bundle* with *carrier* P and Q. A bundle is also defined by two of its circles or its carrier. A set of pairwise disjoint circles is called a *flock*, if it covers all points of an inversive plane but two which are called the *carrier* of the flock. Figure 1.10 illustrates these configurations.

The existence or uniqueness of a flock for a chosen carrier is not clear at all. Every point of an inversive plane is either incident with exactly one circle of a bundle, pencil or flock, or is a carrier of the set.

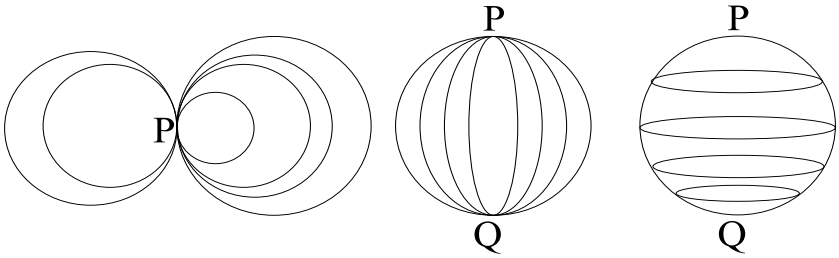

Figure 1.10: Pencil, bundle and flock

We are particularly interested in finite inversive planes. Every internal affine plane has the same order, so we can define the order of the inversive plane by the order of this derived structure.

Theorem 1.21 *Let $\mathbb{M}$ be an inversive plane of order m, then:*

1. *$\mathbb{M}$ consists of $m^2 + 1$ points and $m(m^2 + 1)$ circles.*
2. *Every circle is incident with $m + 1$ points.*
3. *Each point is incident with $m(m + 1)$ circles.*

4. *A pencil consists of* m *circles and there are* $m+1$ *different pencils with the same carrier.*

5. *A bundle consists of* $m+1$ *circles.*

6. *A flock has* $m-1$ *circles.*

7. *Each circle has* m^2 *tangent circles, including itself.*

8. *Each circle intersects with* $\frac{1}{2}m^2(m+1)$ *other circles.*

9. *There are* $\frac{1}{2}m(m-1)(m-2)$ *circles disjoint to a given circle.*

With these combinatorial facts, we can say that the inversive planes of order m are precisely the $3-(m^2+1, m+1, 1)$ designs (see Definition 1.15).

In Figure 1.11 you can see the smallest inversive plane which has order 2, thus 5 points, 10 circles and three points per circle.

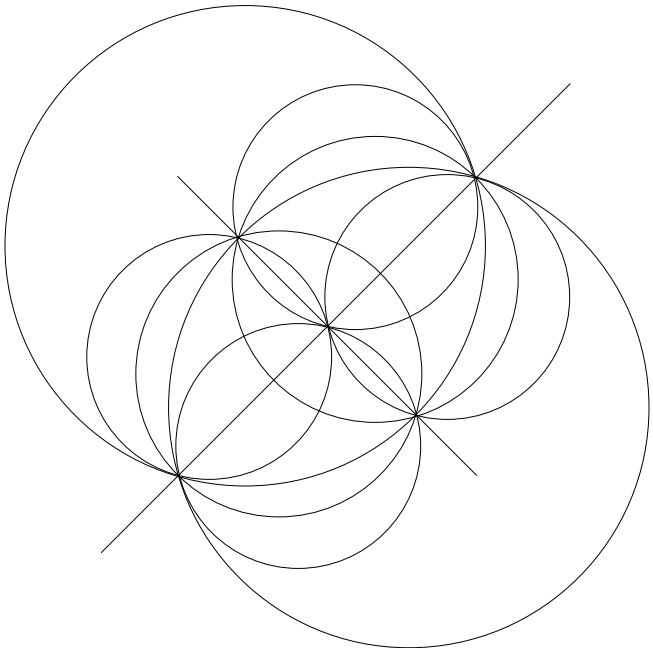

Figure 1.11: Inversive plane or Möbius plane of order 2

Theorem 1.22 *In an inversive plane of even order every three pairwise tangent circles belong to the same pencil.*

This means that Figure 1.12 can only exist in inversive planes of odd order. Also the Bundle Theorem consisting of pencils only is not possible in planes of even order. This fact is named after Qvist [78], it is also mentioned in [10]. We will use this fact in Chapter 7 to improve the LDPC-codes obtained from inversive planes of even order.

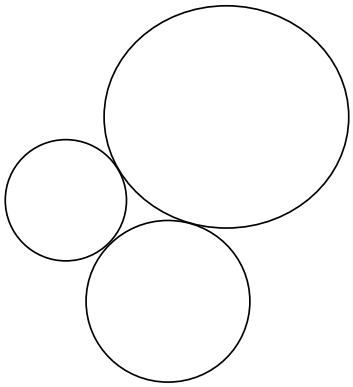

Figure 1.12: Circles in a plane of odd order

All known examples of finite inversive planes can be constructed from an ovoid $\mathbb{O}$ in $PG(3)$ (see Figure 1.13):
$\mathbb{M} = (P, C)$ where

- the points are the points of the ovoid: $P := \{P \in \mathbb{O}\}$,
- and the circles are the plane intersections: $C := \{E \cap \mathbb{O} \mid |E \cap \mathbb{O}| > 1, E \text{ is a plane of } PG(3)\}$.

An inversive plane that is isomorphic to such an incidence structure is called *egglike*. The internal structure of such an egglike inversive plane is Desarguesian (see [29]).

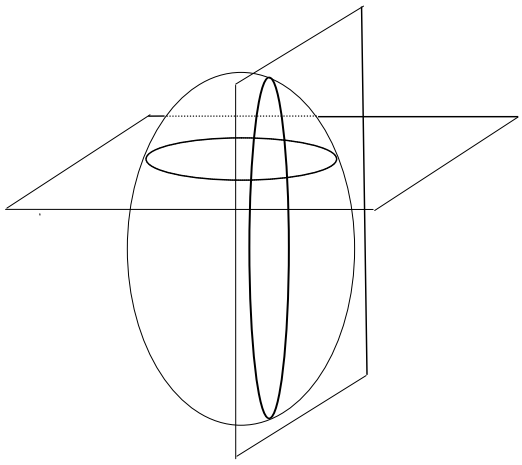

Figure 1.13: Egglike inversive plane

In the eighties of the 20th century, J. Kahn [47, 48] proved that the egglike inversive planes are precisely those following the Bundle Theorem. This way the two representation theorems for inversive planes, the Bundle Theorem and the Theorem of Miquel, are even closely related to the representation theorems of the projective and affine spaces. The internal structure taken in any

point of an inversive plane which complies with the Bundle Theorem is a Desarguesian affine plane; if the Theorem of Miquel holds the affine internal structure will be a Pappian affine plane.

The Bundle Theorem

Theorem 1.23 *Let the circles $c_0, \ldots, c_3$ of an inversive plane $\mathbb{M}$ intersect such that c_0, c_1 belong to a bundle or pencil $\mathbb{B}_1$ and likewise $\{c_1, c_2\} \subset \mathbb{B}_2$, $\{c_2, c_3\} \subset \mathbb{B}_3$, and $\{c_0, c_3\} \subset \mathbb{B}_4$. Then $\mathbb{B}_1$ and $\mathbb{B}_3$ share a circle iff $\mathbb{B}_2$ and $\mathbb{B}_4$ have a circle in common.*

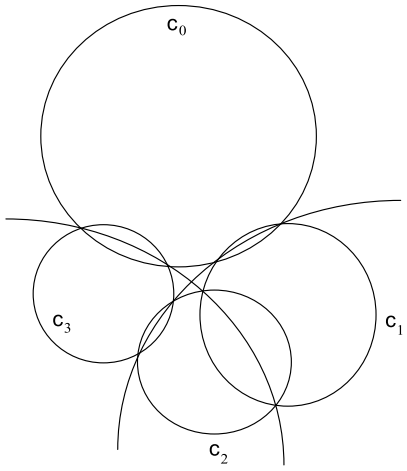

Figure 1.14: Bundle Theorem

The Theorem of Miquel

An inversive plane is called *Miquelian* if the Theorem of Miquel holds:

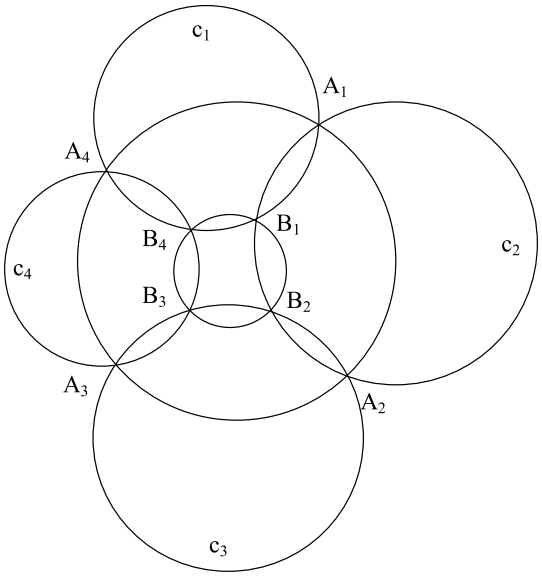

Figure 1.15: Theorem of Miquel

Theorem 1.24 *Let the circles $c_0, \ldots, c_3$ be given such that $c_i \cap c_{i+1} = \{A_i, B_i\}$ with subscripts taken modulo 4 (see Figure 1.15). Then the points A_0, A_1, A_2, A_3 are concircular iff the points B_0, B_1, B_2, B_3 are concircular.*

Note that A_i and B_i are not necessarily different, meaning that they can be the carrier of a bundle or a pencil.

There is only one class of egglike inversive planes known where the Theorem of Miquel does not hold. Those are derived from the Segre-Tits ovoids which were developed in [87, 101].

Here we concentrate on the Miquelian inversive planes and start with some of their possible constructions. We need several, algebraic as well as synthetic, approaches in the following chapters where we will then refer to the following representations.

Representations of Inversive Planes

Theorem 1.25 *Let $L : K$ be a quadratic field extension. Then the embedding of K into L naturally induces an embedding of the projective line $PG(K^2)$ into $PG(L^2)$. We define the incidence structure $\Sigma(K, L) = (P, C)$ by*

$$\begin{aligned} P &:= \mathbb{P}(L^2) \\ C &:= \{c_0 A \mid A \in PGL(2, L)\} \end{aligned}$$

where $c_0 = \{L(x, y) \mid (x, y) \in K^2 \setminus \{(0, 0)\}\}$, and $PGL(2, L)$ is the projective general linear group of rank 2 over L. Then $\Sigma(K, L)$ is a Miquelian inversive plane [31, page 257].

This is a very popular algebraic representation. The circles of the inversive plane can also be constructed via the *cross-ratio*:

Definition 1.26 For elements $A = L(a_1, a_2)$, $B = L(b_1, b_2)$, $C = L(c_1, c_2)$, and $D = L(d_1, d_2)$ on the projective line $\mathbb{P}(L^2)$ we recall the definition of the *cross-ratio* as:

$$\left[\begin{array}{cc} A & B \\ D & C \end{array}\right] := \frac{\left|\begin{array}{cc} a_1 & a_2 \\ c_1 & c_2 \end{array}\right| \cdot \left|\begin{array}{cc} b_1 & b_2 \\ d_1 & d_2 \end{array}\right|}{\left|\begin{array}{cc} a_1 & a_2 \\ d_1 & d_2 \end{array}\right| \cdot \left|\begin{array}{cc} b_1 & b_2 \\ c_1 & c_2 \end{array}\right|}.$$

This ratio takes values in $L \cup \{\infty\}$.

Corollary 1.27 *Let $L : K$ be a quadratic field extension. We define an incidence structure $\Sigma(K, L) = (P, C)$ such that P is the set of points of $\mathbb{P}(L^2)$, and such that the 4 points $A, B, C, D \in P$ are incident with one circle of C if*

$$\left[\begin{array}{cc} A & B \\ D & C \end{array}\right] \in K \cup \{\infty\}.$$

Then $\Sigma(K, L) = (P, C)$ is a Miquelian inversive plane of order $|K|$.

Corollary 1.28 *Let $\mathbb{A}(K^2) = (P, G)$ be the affine plane over a field K that allows a quadratic extension, and let $f(x, y) \in K[x, y]$ be an irreducible homogeneous quadratic form. If we define*

$$\begin{aligned} C &:= \{g \cup \{\infty\} \mid g \in G\} \cup \{c_{a,b,c} \mid a, b, c \in K\} \quad \textit{where} \\ c_{a,b,c} &:= \{(x, y) \in P \mid f(x, y) + ax + by + c = 0\}, \end{aligned}$$

then the incidence structure $\Sigma(K, f) := (P \cup \{\infty\}, C)$ is a Miquelian inversive plane.

The choice of the irreducible homogeneous quadratic form $f(x, y)$ determines the inversive plane, thus which choices for a, b, c will define non-singular circles. We will look into this in Chapter 5, Section 5.1.

Remark 1.29 The group $PGL(2, L)$ is acting sharply 3-transitive on P. For proofs in $\Sigma(K, L) = (P, C)$ or $\Sigma(K, f) = (P, C)$ we can therefore always assume that w.l.o.g. one circle is defined by the points $A = L(1, 0)$, $B = L(1, 1)$, and $C = L(0, 1)$.

Compendium

Figure 1.16 shows the different classes of finite inversive planes and how they relate. Please note, there are no examples known for non-egglike inversive planes of odd order.

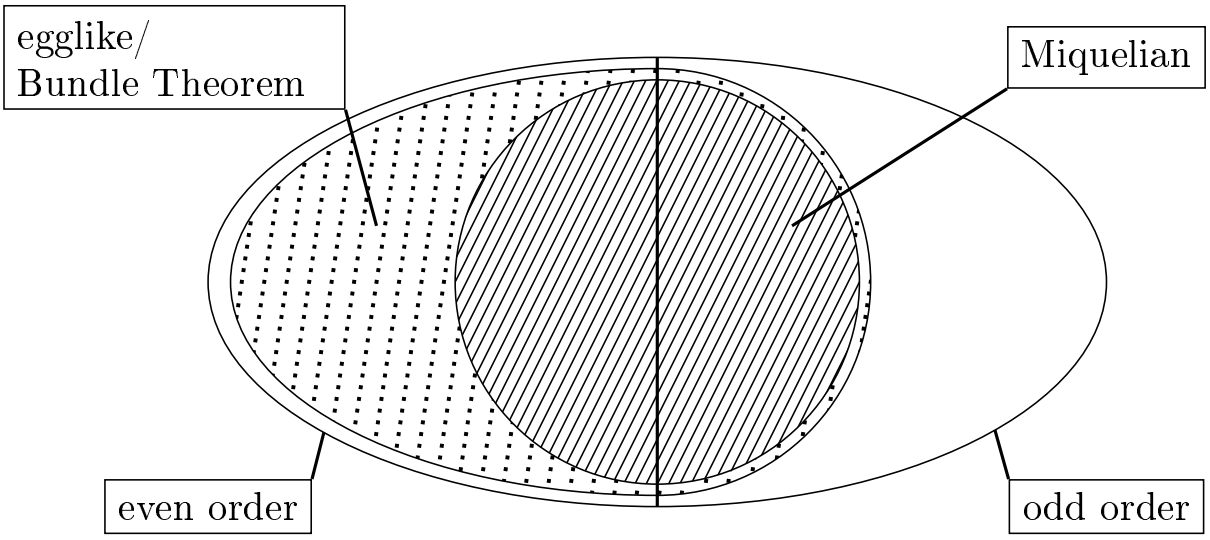

Figure 1.16: Overview of finite inversive planes

We will end this introduction of inversive planes with a small collection of results regarding their automorphism group. These results can be found in [31].

Remarks 1.30 A bijective mapping φ of an inversive plane $\mathbb{M}$ onto another inversive plane $\mathbb{M}'$ is called an *isomorphism* if φ and φ^{-1} preserve the incidence. For $\mathbb{M} = \mathbb{M}'$ these are the automorphisms. The automorphisms of $\mathbb{M}$ can be classified via the set of points they fix.

For an automorphism $\alpha \in Aut(\mathbb{M})$ let $F(\alpha)$ be the substructure consisting of the points that α maps onto themselves and those circles of $\mathbb{M}$, which contain at least three points fixed by α.

- If the automorphism α fixes at least one point P it generates a *collineation* α_P in the affine plane $\mathbb{M}_P$.
  - The map α_P is called a *dilatation* in $\mathbb{M}_P$, if it maps lines onto parallel lines. The automorphism α of $\mathbb{M}$ is called a dilatation as well.
  - A *translation* of the inversive plane is a dilatation that fixes no other point.
- An automorphism α with $F(\alpha)$ incident with a circle of $\mathbb{M}$ is called *circular*. If α is not trivial it is called an *inversion*. For every circle of $\mathbb{M}$ there exists at most one inversion, if $\mathbb{M}$ is Miquelian there exists exactly one and every inversion is involutory.
- If $F(\alpha)$ contains four points not on one circle, $F(\alpha)$ is a subplane (see Definition 5.1 in Chapter 5) of $\mathbb{M}$ and α is called a *planar automorphism* (see [31, page 258]).

Theorem 1.31 *Every automorphism of the inversive plane $\Sigma(K, L)$ is of the form*

$$\alpha A : \mathbb{P}(L^2) \longrightarrow \mathbb{P}(L^2), \quad L(x, y) \mapsto L(x^\alpha, y^\alpha)A,$$

where $A \in \mathrm{PGL}(2, L)$ and α is a field automorphism of L such that $K^\alpha = K$.

Remark 1.32 For $\alpha = \mathrm{id}_L$ these automorphisms are called *Möbius transforms*. It is known that the group of all Möbius transforms acts sharply 3-transitive on the point set of $\Sigma(K, L)$, and hence the group of all generalised Möbius transforms is 3-transitive. Furthermore the group of all Möbius transforms is a normal subgroup of the automorphism group of $\Sigma(K, L)$. In the finite case we can say about a Miquelian inversive plane of order m with $m = p^e$ for some prime p that the automorphism induced by $\alpha \in Aut(L)$ fixes $1 + p^{\frac{2e}{o(\alpha)}}$ points and it is therefore planar for odd $o(\alpha)$ and circular if $o(\alpha)$ is even. (For the proof see [31, page 274].)

Inversive Spaces

Definition 1.33 An *inversive space* is an incidence structure $\mathbb{M} := (P, C)$, where the blocks are called *circles* such that the following axioms are satisfied:

(i) Any three distinct points are contained in exactly one circle.

(ii) For every point P the internal structure $\mathbb{M}_P$ is an affine space.

Hence if two circles c and c' are tangent in P, the lines $c \setminus \{P\}$ and $c' \setminus \{P\}$ are parallel in $\mathbb{M}_P$. The order m and dimension u of the affine space $\mathbb{M}_P$ defines the *order* and *dimension* of the inversive space.

The lines resulting from a pencil with carrier P form a full parallel class in $\mathbb{M}_P$. The number of circles in a pencil is therefore given by m^{u-1}.

Our simple algebraic construction in Theorem 1.25 for Miquelian inversive planes can be generalised for higher dimensions.

Example 1.34 Let $L : K$ be a field extension of degree $u \geq 2$, and let $\alpha \in L \setminus K$. The embedding of K into L induces a natural embedding of the projective line $PG(K^2)$ into $PG(L^2)$. We now define an incidence structure $\Sigma(L : K) := (P, C)$ by

$$\begin{aligned} P &:= \{L(x, y) \mid (x, y) \in L^2 \setminus \{(0, 0)\}\} \\ C &:= \{c_0^\gamma \mid \gamma \in PGL(L, 2)\} \end{aligned}$$

where $c_0 = \{L(x, y) \mid (x, y) \in K^2 \setminus \{(0, 0)\}\}$ and $PGL(L, 2)$ is the projective general linear group of rank 2 over L. Then $\Sigma(L : K)$ is an inversive space of dimension u.

Remark 1.35 Let $\mathbb{M}$ be an inversive space of order m and dimension u.

(a) Every point of $\mathbb{M}$ is a carrier of $\frac{m^u-1}{m-1}$ different pencils.

(b) There are $\frac{m^u-1}{m-1}(m^u + 1)$ distinct pencils in $\mathbb{M}$.

(c) Every circle of $\mathbb{M}$ is a member of $m + 1$ pencils.

(d) Two distinct pencils of $\mathbb{M}$ have at most one circle in common.

Remark 1.36 Let $\mathbb{M} = (P, C)$ be an inversive space. There exist non-negative integers m and u such that the following properties hold.

(a) All circles of $\mathbb{M}$ contain $m + 1$ points.

(b) $\mathbb{M}$ contains exactly $m^u + 1$ points. Each point is incident with exactly $m^{u-1}\,\frac{m^u-1}{m-1}$ circles, and for this reason $\mathbb{M}$ contains $m^{u-1}\,\frac{m^{2u}-1}{m^2-1}$ circles.

(c) $\mathbb{M}$ forms a 3-design with parameters $(m^u + 1, m + 1, 1)$.

2 Partial Ovoids and Blocking Sets in Even Order

We are looking for maximal partial ovoids of $Q(4,q)$ in the projective space of even order. The aim is to find these ovoids in consecutive sizes, then we can say that there exist maximal partial ovoids within a whole interval of cardinalities.

In Chapter 1, Section 1.2, we read that if $Q(4,q)$ is a non-singular parabolic quadric in the projective space $PG(4,q)$, then the set of points and the set of lines of $Q(4,q)$ form a generalised quadrangle of order q. This generalised quadrangle is isomorphic to the generalised quadrangle $W(q)$ of even order q, where the points of $W(q)$ are the points of $PG(3,q)$ and the lines of $W(q)$ are the self-polar lines of a symplectic polarity σ of $PG(3,q)$. The size of an ovoid of a generalised quadrangle Γ of order (s,t) is $st+1$, hence an ovoid of $Q(4,q)$ or $W(q)$ has size q^2+1.

Research had been done regarding the existence as well as non-existence of these partial ovoids of generalised quadrangles, in particular by J. A. Thas [99, 100]. Recently the idea of obtaining whole spectra of maximal partial ovoids [23, 24] arose. Here results were usually achieved by using computer resources. Now we found a technique to get whole spectra for the cardinality of maximal partial ovoids in $Q(4,q)$ without using computer power.

The concept is a statistical argument introduced by T. Szőnyi and collaborators in [94] and [38]. It proves the existence without an explicit construction. For convenience the theorem is cited in Corollary 2.1 below. Their argument is based on the original idea by Z. Füredi in his article on *Matchings and covers in hypergraphs* [36]. We will explain details further on. The key in their statistical approach is that it allows some freedom in several variables. This makes it possible to obtain spectra of maximal partial ovoids (or minimal blocking sets, see Chapter 4).

Spectrum results for maximal partial ovoids of $Q(4,q)$, q even, can be extended to the corresponding results:

- maximal partial ovoids of $W(q)$, q even,
- maximal partial spreads of $Q(4,q)$ and $W(q)$ for even q,
- minimal blocking sets with respect to the planes of $PG(3,q)$, q even,
- maximal partial 1-systems on the Klein quadric $Q^+(5,q)$, q even.

For details on these correspondences see [41]. Later in this chapter, beginning with Definition 2.12, we will interpret our results with respect to these structures.

The results presented in this chapter are acquired in joint work with L. Storme [83].

2.1 Idea

As announced we introduce the idea presented in the article of Szőnyi *et al* [94] for the construction of minimal blocking sets in $PG(2, q^2)$ and adapt it for maximal partial ovoids of $Q(4, q)$ where q is even. In particular the statement introduced by Füredi ([36, page 190]) is essential:

Corollary 2.1 *For a bipartite graph with bipartition $L \cup U$ where the degree of the elements in U is at least d, there is a set $L' \subseteq L$, for which $|L'| \leq |L| \frac{1+\log(|U|)}{d}$, such that any element $u \in U$ is adjacent to at least one element of L'.*

The following setting is useful for our purposes. In the next section, we will discuss it in detail. Now, we want to focus on the application of the above corollary in our context. We refer to Figure 2.1.

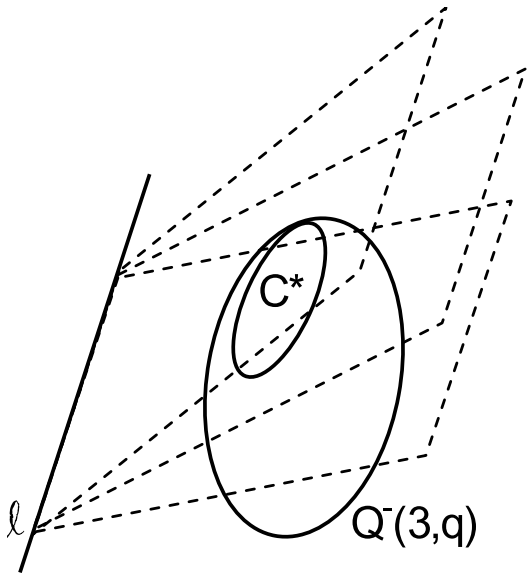

Figure 2.1: Conics of $Q^-(3, q)$ in planes through ℓ

Consider an elliptic quadric $Q^-(3, q)$ in $Q(4, q)$. Then $Q^-(3, q)$ is an ovoid of the generalised quadrangle $Q(4, q)$. Let ℓ be a line of $PG(3, q)$, external to $Q^-(3, q)$. Out of the planes containing ℓ there are two planes tangent to $Q^-(3, q)$ in the points R_1 and R_2, and $q-1$ planes intersecting $Q^-(3, q)$ in a conic. Out of these we will choose several for the construction. Then we consider another set of conics on $Q^-(3, q)$. This set consists of conics containing R_1, but not R_2, and these conics are not lying in a plane through ℓ. We will show in the next section (in particular in Lemma 2.5), that we can choose a set of conics in such a way, that these conics are intersected by the same planes through ℓ. We will later call this set of conics C^* (see Definition 2.4).

We are interested in the planes through ℓ intersecting the quadric $Q^-(3, q)$ in a conic. Among those planes, we choose $s-2$ planes out of which $r-1$ intersect the conics C^* (see Figure 2.2). We now choose for U all conics of the quadric $Q^-(3, q)$; except for a small number of conics, in particular, those conics that lie in a plane containing ℓ. We isolate a particular group of $q+1$ conics passing through R_1, but not through R_2, intersected by the same $q/2+1$ conics in planes

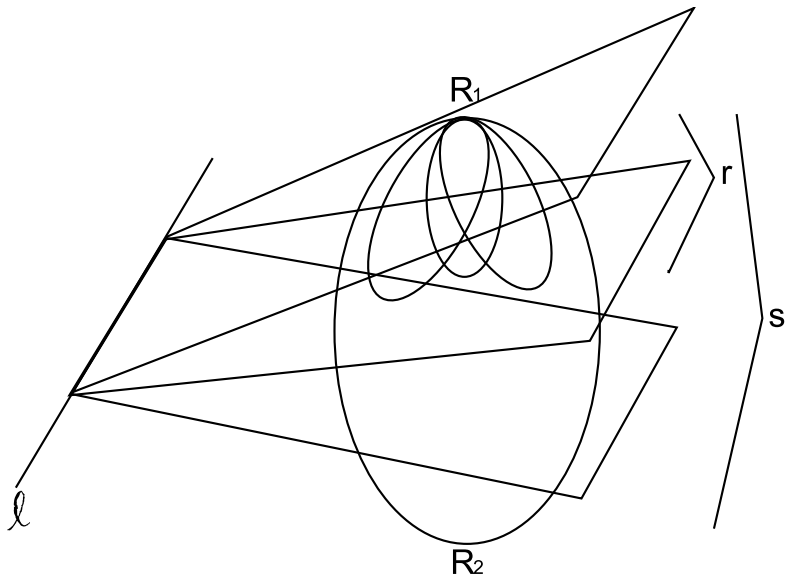

Figure 2.2: Setting for the construction

through ℓ. The $q/2$ conics of $Q^-(3,q)$ in planes through ℓ skew to this group of $q+1$ conics are the elements of L. An element of U is adjacent to an element of L when the two conics intersect in at least one point. Applying Corollary 2.1, we can reduce L to L' and still know that every conic in U intersects a conic of L'.

Then, in a first step, we can decrease the ovoid $Q^-(3,q)$ to a partial ovoid by omitting conics in planes through ℓ, but certainly not the conics in L', replacing those omitted conics by their polar points in $Q(4,q)$. Recall that q is even, thus the plane containing a conic also contains a point incident with all tangent lines to the conic, which is the nucleus of the conic.

The conics in C^* have to be intersected by the same planes containing ℓ. The following section will give the construction of these conics and show that we can replace them by their polar points without violating the properties of the partial ovoid constructed in the first step above.

2.2 Construction

Remark 2.2 A conic of $Q(4,q)$, q even, has either one or $q+1$ *polar points* on $Q(4,q)$, i.e., there are either one or $q+1$ points of $Q(4,q)$ collinear with all $q+1$ points of the conic. A conic of $Q(4,q)$ lying in a plane through the nucleus N of $Q(4,q)$ has $q+1$ polar points, while a conic of $Q(4,q)$ lying in a plane, not passing through the nucleus N, has exactly one polar point. A conic contained in an elliptic quadric $Q^-(3,q)$ of $Q(4,q)$ has therefore only one polar point.

We want to replace a number of conics of the elliptic quadric $Q^-(3,q)$ by their polar point in order to get partial ovoids of different sizes. The aim is to do this in such a way that we get many different cardinalities for the maximal partial ovoids. Thus we want to be able to replace different numbers of conics, so we have to choose these conics in a way that their polar points are not collinear in a point on $Q(4,q)$.

The polar line of ℓ with respect to $Q^-(3,q)$ is a bisecant intersecting $Q^-(3,q)$ in two points R_1 and R_2. The planes through R_1, R_2 intersect $Q^-(3,q)$ in a conic each. The nuclei of these conics are the $q+1$ points on ℓ. The planes through ℓ consist of the tangent planes to $Q^-(3,q)$ in R_1 and R_2, and of $q-1$ planes each intersecting $Q^-(3,q)$ in conics $K^i, i=1,\ldots,q-1$. There is one polar point of $Q(4,q)$ collinear with the points of such a conic K^i, $i=1,\ldots,q-1$. These $q-1$ polar points of the conics of $Q^-(3,q)$ in the planes through ℓ belong to the conic C which is the intersection of $Q(4,q)$ with the plane incident with the nucleus N of $Q(4,q)$ and the points R_1, R_2 (see Figure 2.3).

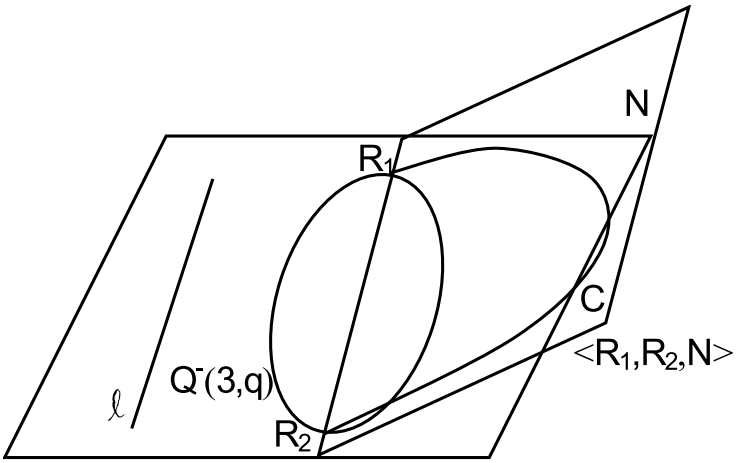

Figure 2.3: Conic C of the polar points of the conics in planes through ℓ

Now we look at the planes containing the external line ℓ. We can now replace some of these conics K^i by their polar point on C. If we keep $s-2$ conics $K^{q+2-s},\ldots,K^{q-1}$, and replace $q+1-s$ conics $K^1,\ldots,K^{q+1-s}$ by their polar point, we obtain a partial ovoid $\mathbb{O}$ containing R_1, R_2, $s-2$ conics in planes through ℓ, and $q+1-s$ points being the polar points replacing the conics. So $\mathbb{O}$ is of size $2+(s-2)(q+1)+q+1-s$.

Next we look at the other set of conics; the conics which were denoted by C^* in Figure 2.1. These are the conics which are intersected by the same planes through ℓ (the formal definition will follow in Lemma 2.5 et seq.). Out of these, we will replace some by their polar point. Let us investigate conics of $Q^-(3,q)$ incident with R_1, but not R_2. There are $q+1$ tangent lines through R_1. Each defines a pencil with carrier R_1, and each pencil contains q conics out of which one is incident with R_2. Thus we have $(q+1)(q-1)$ conics incident with R_1, but not R_2. These conics intersect $q/2+1$ planes through ℓ, one plane $\langle \ell, R_1\rangle$ tangent to the elliptic quadric in R_1 and $q/2$ planes intersecting each conic in two points. Firstly we will show that these conics form groups of $q+1$ conics which are intersected by the same $q/2+1$ planes containing ℓ. In these groups, there is exactly one conic of each pencil with carrier R_1.

Lemma 2.3 *The $(q+1)(q-1)$ conics of the elliptic quadric $Q^-(3,q)$, incident with R_1 but not with R_2, form groups of $q+1$ conics which are intersected by the same $q/2+1$ planes through the external line ℓ. Conics of the same group intersect in R_1, and every other point of such a conic is the intersection point with precisely one other conic of the same group.*

Proof: The elliptic quadric $Q^-(3,q)$ is fixed by a 3-transitive group. The subgroup fixing R_1 and R_2 has size q^2-1. This group also fixes the polar line of R_1R_2, which is the line ℓ.

The elliptic quadric can be represented by the following equation: $X_0X_1+f(X_2,X_3)=0$, where $f(X_2,X_3)=aX_2^2+bX_2X_3+cX_3^2$ is irreducible over $\mathbb{F}_q$, the Galois field of order q. Then there is a cyclic group C_{q+1} of size $q+1$ fixing the quadratic form f. This group also operates cyclically on the points of ℓ. Let R_1,R_2 have coordinates $R_1=(1,0,0,0), R_2=(0,1,0,0)$, then $\ell: X_0=X_1=0$.

If we now fix a point on ℓ, for instance $P=(0,0,0,1)$, we get the mapping $\eta:(x_0,x_1,x_2,x_3)\mapsto(a'^2x_0,x_1,a'x_2,a'x_3)$ fixing $Q^-(3,q)$. If a' is a generator of $\mathbb{F}_q^*$, then η defines a cyclic group C_{q-1} of order $q-1$. Then η fixes the elliptic quadric and also the planes $\langle\ell,R_1\rangle: X_1=0$ and $\langle l,R_2\rangle: X_0=0$, where $X_1=\alpha X_0$, for some $\alpha\neq 0$, are the secant planes to $Q^-(3,q)$ through ℓ.

If we consider the planes incident with the point P on ℓ and R_1, different from the plane through R_2 and the tangent plane in R_1, their intersection with $Q^-(3,q)$ is a conic and there are $q/2+1$ planes through ℓ intersecting this conic. In the quotient geometry $PG(1,q)=\mathbb{F}_q\cup\{\infty\}$ of ℓ, these planes correspond to a set of $q/2+1$ points where $\langle\ell,R_1\rangle$ corresponds to ∞ and the other $q/2$ planes define an additive subgroup of index 2 in $(\mathbb{F}_q,+)$, or a coset of an additive subgroup of index 2 in $(\mathbb{F}_q,+)$. The cyclic group C_{q-1} maps this subgroup of index 2 onto all subgroups of index 2 in $(\mathbb{F}_q,+)$, or this coset onto all cosets of these subgroups of index 2 in $(\mathbb{F}_q,+)$. Furthermore, C_{q-1} maps all conics in planes through the line $\langle P,R_1\rangle$, different from $\langle P,R_1,R_2\rangle$ and $T_{R_1}(Q^-(3,q))$, onto each other in a way that every subgroup occurs exactly once.

The cyclic group C_{q+1} acts transitively on ℓ, so transitively on the possible lines PR_1, with $P\in\ell$. If C_{q+1} maps $P\in\ell$ onto $P'\in\ell$, the intersection conic between a plane through the line PR_1 and $Q^-(3,q)$ is mapped onto a conic in a plane through $P'R_1$ which is intersected by the same $q/2+1$ planes through ℓ, since C_{q+1} fixes the line R_1R_2 point by point. So for every point on ℓ, there is a unique conic intersected by the same $q/2+1$ planes through ℓ.

We interrupt the proof for a short definition:

Definition 2.4 A *group* of conics of $Q^-(3,q)$ is a set C^* of $q+1$ conics $C^0,\ldots,C^q$, through R_1, but not through R_2, intersected by the same $q/2+1$ planes through ℓ.

All the conics of a group must intersect in R_1 and in another point as their planes intersect in a line incident with R_1 which cannot be in the tangent plane $\langle\ell,R_1\rangle$ to $Q^-(3,q)$ in R_1.

We now show that the other intersection points are all different, thus that every point except R_1 of every conic of a group is an intersection point, with exactly one other conic of the group. The cyclic group C_{q+1} maps a conic C^0 onto conics $C^1,\ldots,C^q$ which are intersected by the same $q/2+1$ planes through ℓ. One of these planes is the tangent plane $\langle\ell,R_1\rangle$; the other $q/2$ of those planes through ℓ are secant planes to $Q^-(3,q)$. We consider one such plane through ℓ and the intersection conic K^i with $Q^-(3,q)$. Let $R'_0,\ldots,R'_q$ be the points of K^i and let γ be the generator of the group C_{q+1}. Thus $\gamma(R'_i)=R'_{i+1} \pmod{q+1}$. This conic K^i shares two points with C^0, let's say R'_0,R'_j, so $\gamma^j(C^0)$ contains R'_j and $\gamma^{q+1-j}(C^0)$ contains R'_0.

In this way we discussed all points of $C^0\setminus\{R_1\}$, as there are $q/2$ planes through ℓ intersecting such a conic C^0 of a given group in two points, and $q/2\cdot 2=q$ is the number of points of the conic of the given group, besides R_1. □

The idea is to replace some of these conics of a given group C^* by their polar point. As this new configuration is supposed to be a maximal partial ovoid, we have to know the incidences of these

polar points. The following lemma shows that these polar points of the $q+1$ conics of a group C^* form a conic C' contained in the tangent cone $T_{R_1}(Q(4,q))$.

Lemma 2.5 *Consider a set C^* of $q+1$ conics $C^0,\ldots,C^q$ incident with the point R_1 of the elliptic quadric $Q^-(3,q)$, but not incident with R_2, intersected by the same $q/2+1$ planes through the external line ℓ. The polar points of these conics form themselves a conic C' which lies in the tangent hyperplane of $Q(4,q)$ in R_1.*

Proof: All these polar points lie in the tangent hyperplane $T_{R_1}(Q(4,q))$, since they are all incident with a line of $Q(4,q)$ through R_1.

We found the conics $C^0,\ldots,C^q$ of $Q^-(3,q)$ in the foregoing lemma using the irreducible quadratic form $f(X_2,X_3)=aX_2^2+bX_2X_3+cX_3^2$. Embedding the elliptic quadric in $Q(4,q)$, we get $X_0X_1+aX_2^2+bX_2X_3+cX_3^2+X_4^2=0$. The cyclic group C_{q+1} from the proof of Lemma 2.3 can be rescaled and extended to a mapping η'

$$\eta' : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & a' & b' & 0 \\ 0 & 0 & c' & d' & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

fixing $Q(4,q)$, where the matrix

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

fixes the quadratic form $aX_2^2+bX_2X_3+cX_3^2$. The hyperplane $T_{R_1}(Q(4,q)) : X_1=0$ is fixed by η', thus by C_{q+1}. Furthermore, the hyperplanes $X_0=0$ and $X_4=0$ are fixed as well.

If $U=(u_0,0,0,0,u_4)$ belongs to $T_{R_1}(Q(4,q)) : X_1=0$, then $U=R_1$, so we can assume that $(u_2,u_3)\neq(0,0)$. If $U=(u_0,\ldots,u_4)$, $(u_2,u_3)\neq(0,0)$, $U\in T_{R_1}(Q(4,q))$, then the images of U under C_{q+1} have coordinates

$$(u_0,u_1,A^j\begin{pmatrix} u_2 \\ u_3 \end{pmatrix},u_4).$$

An easy check shows that the images of U form a conic C' contained in $T_{R_1}(Q(4,q))\cap Q(4,q)$. The cyclic group C_{q+1} acts in one orbit on the $q+1$ conics of a group; so we have proven that the polar points of the conics of a group form a conic C' in $T_{R_1}(Q(4,q))\cap Q(4,q)$. □

The conic C' in $T_{R_1}(Q(4,q))\cap Q(4,q)$ of the preceding lemma is skew to the conic $\langle\ell,N\rangle\cap Q(4,q)$, since this conic consists of the polar points of the conics in the planes through R_1R_2. Thus we can replace conics of $Q^-(3,q)$ in planes through ℓ and conics in a given group by their polar points, under certain restrictions. Assume again that we replace $q+1-s$ conics $K^1,\ldots,K^{q+1-s}$, being the intersection of planes containing the external line ℓ with the quadric $Q^-(3,q)$. Now we replace also t conics $C^1,\ldots,C^t$ out of $\{C^0,\ldots,C^q\}$ by their polar points to get more sizes for the maximal partial ovoids of $Q(4,q)$. Some of the points on the conics $C^1,\ldots,C^t$ were already cancelled when we replaced the conics $K^1,\ldots,K^{q+1-s}$ by their polar points, so we have to know how many conics of $\{K^1,\ldots,K^{q+1-s}\}$ intersect the t conics $C^1,\ldots,C^t$ in order to determine exactly the cardinality of the newly constructed maximal partial ovoids. Assume that we kept r of the conics in the planes through ℓ that intersect the t conics $C^1,\ldots,C^t$, including the tangent

plane incident with R_1. The cardinality M of the partial ovoid $\mathbb{O}$ is then depending on how the $r-1$ conics out of $K^{q+2-s},\ldots,K^{q-1}$ intersect $C^1,\ldots,C^t$. We have $2t(r-1)-u$ points of intersection between $C^1,\ldots,C^t$ and $K^{q+2-s},\ldots,K^{q-1}$, where u is the number of intersection points of $C^1,\ldots,C^t$ and $K^{q+2-s},\ldots,K^{q-1}$ lying in two of the conics $C^1,\ldots,C^t$.

In the next section, we will investigate the intersection points among the conics $C^1,\ldots,C^t$ and the conics $K^{q+2-s},\ldots,K^{q-1}$; now we say that there are u points of intersection. Then we get partial ovoids of size

$$\begin{aligned} M &= 2+(s-2)(q+1)+q+1-s-1-2t(r-1)+t+u, \\ &= (s-1)q-2tr+3t+u, \end{aligned}$$

where certain constraints apply for s and r, and where the term -1 comes from the fact that R_1 is also cancelled from $C^1,\ldots,C^t$, and the term $+t$ comes from the fact that $C^1,\ldots,C^t$ are replaced by their polar points.

Furthermore, we have to determine the bound on the cardinality of L' from Corollary 2.1, because $s-r\geq|L'|$. Now $|L'|\leq|L|\frac{1+\log(|U|)}{d}$ where the elements of U are the conics of $Q^-(3,q)$ besides

1. the $q-1$ conics lying in a plane containing the line ℓ,
2. the $q+1$ conics in a plane through R_1R_2, and
3. the conics of the selected group $C^*=\{C^0,\ldots,C^q\}$ of conics through R_1, but not through R_2, intersected by the same $q/2+1$ planes through ℓ.

Note that $|U|\leq q^3+q^2<(q+1)^3$. These $q/2$ conics in planes through ℓ skew to the conics of the group $\{C^0,\ldots,C^q\}$ form the set L. A lower bound on the degree is given in [90, Lemma 2.12]; $d\geq\frac{1}{4}(q-1-6\sqrt{q})$. All in all we get:

$$\begin{aligned} |L'| &\leq \frac{q}{2}\cdot\frac{1+\log((q+1)^3)}{\frac{1}{4}(q-1-6\sqrt{q})} \\ &\leq 2\cdot(1+3\log(q+1))\cdot\frac{q}{q-1-6\sqrt{q}}. \end{aligned}$$

For $q\geq 50$, $q/(q-1-6\sqrt{q})\leq 8$ and we get $|L'|\leq 16(1+3\log(q+1))$.

Hence, the preceding results show that there exists, within the set of $q/2$ planes of L, a set L' of at most $16(1+3\log(q+1))$ planes, such that every conic of $Q^-(3,q)$ in U intersects at least one of the planes of L'. One of these planes could be the tangent plane $\langle\ell,R_2\rangle$. The symbol s in Step 4 of the summary of the construction stands for the planes $\langle\ell,R_1\rangle$, $\langle\ell,R_2\rangle$, and for the $s-2$ non-replaced conics in planes through ℓ. To make sure that also the plane $\langle\ell,R_2\rangle$ is counted within the symbol s, and since R_2 does not belong to the conics $C^0,\ldots,C^q$, we increase the upper bound on the size of L' to $17+48\log(q+1)$.

To be sure that every conic in U intersects at least one conic of L', we do not replace the conics in L' by their polar points, and we impose the constraint $s-r\geq 17+48\log(q+1)$.

The following also needs to be verified: We are replacing conics in planes through ℓ by their polar points, which belong to the conic C, and we are also replacing conics in a selected group C^* of

conics through R_1 by their polar points, which belong to the conic C'. We must verify, whether a selected polar point on C' can be collinear on $Q(4,q)$ with a selected polar point on C.

It is impossible that a point on C' is collinear on $Q(4,q)$ with all the points of C. For the points of $Q(4,q)$ collinear with all the points of C are the polar points of the conics through R_1R_2, and they do not belong to C'.

The points of C' form an orbit under the cyclic group C_{q+1}, which fixes the conic C pointwise. Hence, if the points of C' are collinear on $Q(4,q)$ with points of C, then they are collinear with the same points of C. They certainly are collinear with R_1 since all the conics of a group C^* pass through R_1. Assume that the points of C' are still collinear with a second point R of C. Then R is the polar point of a conic D through ℓ. We prove that this conic D is skew to all the conics of the selected group C^* of conics through R_1.

Lemma 2.6 *Assume that the points of the conic C' are collinear on $Q(4,q)$ with a point R, different from R_1, of the conic C. Assume that R is the polar point of the conic D through ℓ, then D is skew to all the conics of the selected group C^* of conics through R_1.*

Proof: Suppose that D has an intersection point with such a conic. Then there are two intersection points T_1 and T_2 since the only plane through ℓ that intersects a conic of a group in one point, is the plane $\langle \ell, R_1 \rangle$.

Assume that T_1 and T_2 belong to the conic of the selected group through R_1 with the polar point T on C'. We are assuming that this point T of C' is collinear with the point R of C; at most one of the points T_1 or T_2 can belong to the line TR. Assume that $T_2 \notin TR$, then T_2 is collinear with R since it belongs to the conic D which has R as its polar point, and T_2 is also collinear with T, but then there is a triangle of lines contained in $Q(4,q)$. This is impossible. □

Since we will be selecting points of C' and of C to belong to the newly constructed partial ovoid $\mathbb{O}$, we need to avoid that these points are collinear. They can be collinear with only one point R of C, different from R_1, which is the polar point of a conic D skew to the selected group of conics through R_1. For this reason, we increase the upper bound on the size of L' by a unit to also include the conic D in L'. This gives the constraint $s - r \geq 18 + 48\log(q+1)$.

For convenience and future reference we summarise the protracted construction and numerous proofs for completeness of the new partial ovoids and give the necessary constraints for the parameters:

1. Select an elliptic quadric $Q^-(3,q)$ contained in $Q(4,q)$, select an external line ℓ to $Q^-(3,q)$ in the solid of $Q^-(3,q)$, and let R_1R_2 be the polar line of ℓ with respect to $Q^-(3,q)$, where $R_1, R_2 \in Q^-(3,q)$.

   Let C be the conic of $Q(4,q)$ in the plane $\langle R_1, R_2, N \rangle$ containing the $q-1$ polar points of the $q-1$ conics $K^1, \ldots, K^{q-1}$ to $Q^-(3,q)$ in planes through ℓ.

2. Select a group C^* of $q+1$ conics $C^0, \ldots, C^q$ through R_1, intersected by the same $q/2+1$ planes through ℓ. Let C' be the conic in $T_{R_1}(Q(4,q))$ consisting of the polar points of the conics in C^*.

3. Let L' be the set of conics in planes through ℓ, skew to the given set of conics C^*, whose existence is guaranteed by Lemma 2.6. Note that we increased the upper bound on the size

of L' to $18+48\log(q+1)$ to guarantee that L' also includes the plane $\langle \ell, R_2 \rangle$ and the conic D.

The crucial property of the conics in the set L' is that every conic of $Q^-(3,q)$, not lying in a plane through ℓ or R_1R_2, and also different from any conic of the group C^*, intersects at least one of these conics in L' in at least one point. This follows from Corollary 2.1.

4. We construct a new partial ovoid by selecting $q+1-s$ conics of $Q^-(3,q)$ in planes through ℓ, and by replacing them by their polar points on C. This gives a new partial ovoid of size $2+(s-2)(q+1)+q+1-s$. Note that we do not replace the conics in L', including the conic D, by their polar points.

5. We now select t conics $C^1,\ldots,C^t$ out of $C^0,\ldots,C^q$, and replace them by their polar points on C'.

We can assume that exactly $r-1$ out of the $s-2$ non-replaced conics $K^{q+2-s},\ldots,K^{q-1}$ through ℓ intersect the conics $C^1,\ldots,C^t$. For our calculation we assume they intersect in total in $2t(r-1)-u$ points (recall u is the number of intersection points of $C^1,\ldots,C^t$, which are also lying in one of the planes $K^{q+2-s},\ldots,K^{q-1}$).
Then the newly constructed partial ovoid $\mathbb{O}$ has size

$$M \quad = \quad (s-1)q-2tr+3t+u.$$

It remains to be shown that such a partial ovoid $\mathbb{O}$ is complete. We know that a point in $Q^-(3,q)\backslash\mathbb{O}$ must lie on a conic which was replaced by its polar point. Thus this point is collinear with this polar point. So let us consider a point $P\in Q(4,q)$, but $P\notin Q^-(3,q)$ and $P\notin\mathbb{O}$. We assume that P extends $\mathbb{O}$ to a larger partial ovoid. The tangent cone to $Q(4,q)$ in P intersects $Q^-(3,q)$ in a conic $\varphi(P)$. The plane of $\varphi(P)$ cannot contain the external line ℓ, for since $P\notin\mathbb{O}$, this conic in this plane of $\varphi(P)$ through ℓ would not have been cancelled from $Q^-(3,q)$; so this conic contains points of $\mathbb{O}$; hence P does not extend $\mathbb{O}$. So $\varphi(P)$ can either pass through R_1 and R_2, or be a conic of the selected group C^* of conics $C^0,\ldots,C^q$ which are intersected by the same $q/2+1$ planes containing ℓ, or be a conic not intersected by the same $q/2+1$ planes through ℓ as $C^0,\ldots,C^q$. If $R_1,R_2\in\varphi(P)$, the nucleus of $\varphi(P)$ lies on ℓ. Thus every plane containing ℓ intersects $\varphi(P)$ in one point. But there are $s-2$ conics in planes through ℓ in $\mathbb{O}$, thus $\varphi(P)$ contains points of the partial ovoid $\mathbb{O}$, so P cannot extend $\mathbb{O}$ to a larger partial ovoid. If $\varphi(P)$ is intersected by $q/2+1$ planes through ℓ different from those intersecting $C^1,\ldots,C^t$, then $\varphi(P)$ intersects one of the conics in L' and P cannot extend $\mathbb{O}$. Otherwise, $\varphi(P)$ belongs to the group of conics $\{C^0,\ldots,C^q\}$, thus it intersects each of these conics $C^1,\ldots,C^t$ in R_1 and in exactly one other point. Now $\varphi(P)$ has $2(r-1)$ points, different from R_1, in common with the $r-1$ non-cancelled conics in planes through ℓ which intersect the conics $C^0,\ldots,C^q$. So if $2(r-1)>t$, then $\varphi(P)$ contains at least one point of $\mathbb{O}$, thus P cannot extend $\mathbb{O}$ to a larger partial ovoid. Hence $\mathbb{O}$ is a maximal partial ovoid, if we impose the condition $r>(t+2)/2$. □

We summarise briefly the preceding results for future references.

Corollary 2.7 *The maximal partial ovoid $\mathbb{O}$ of $Q(4,q)$ has cardinality $M=(s-1)q-2tr+3t+u$, where the following constraints apply to s and r:*

1. $2\le s\le q+1$,

2. $\frac{t+2}{2} < r \leq q/2+1$,

3. *if* $s \geq q/2$, *then* $r \geq s - q/2$,

4. $s - r \geq 18 + 48\log(q+1)$.

The restrictions follow from the construction above and the application of Corollary 2.1 in the construction.

2.3 Selection of Conics

The cardinality of the maximal partial ovoids we just constructed is $M = (s-1)q - 2tr + 3t + u$, where the parameters s, r, and u are somewhat flexible. We will need this quality to obtain maximal partial ovoids of consecutive sizes. Whenever we vary s or r we would like u to be flexible enough to bridge the emerging gap. We know from Lemma 2.3 that t conics $C^1, \ldots, C^t$ intersect in $\binom{t}{2}$ points different from R_1, out of which u are incident with a conic of $\{K^{q+2-s}, \ldots, K^{q-1}\}$. If we choose five conics $C^1, \ldots, C^t$ we get $t = 5$ thus 10 points of intersection. It is now possible to choose these in such a way that the intersection points as required belong or don't belong to $K^{q+2-s}, \ldots, K^{q-1}$ (as shown in Figure 2.4). Now we can construct maximal partial ovoids of sizes $M = (s-1)q - 10r + 15, \ldots, M = (s-1)q - 10r + 25$. Together with the variety of choices for s and r we get an uninterrupted interval for the cardinalities.

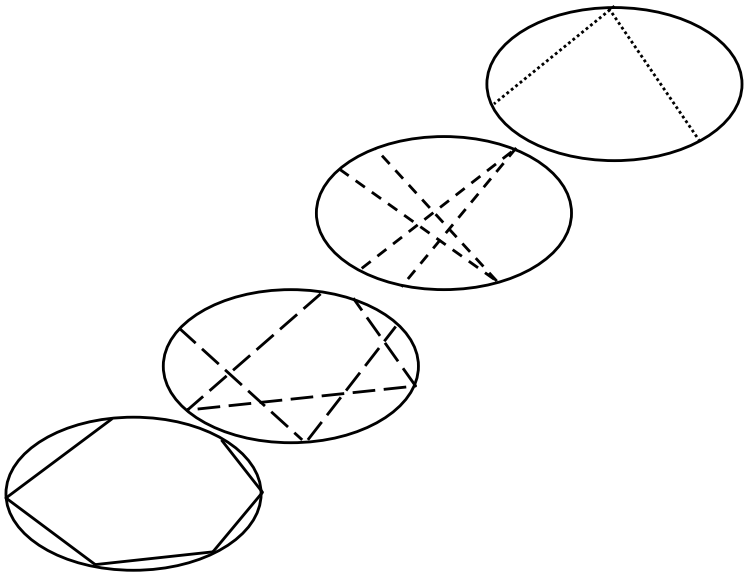

Figure 2.4: Intersection points of the 5 conics on 4 conics

Consider the $q+1$ conics $C^0, \ldots, C^q$ of the selected group. It follows from the proof of Lemma 2.3 that there is a cyclic group C_{q+1} with generator α, acting transitively on these $q+1$ conics, and fixing all conics K^i in the planes through ℓ. Assume that $\alpha(C^i) = C^{i+1}$ where the exponent is understood $\pmod{q+1}$. Now we choose five conics out of the group, let's say $C^1, \ldots, C^5$.

Note that $t = 5$ implies $r \geq 4$ (Corollary 2.7 (2)). Then 4 points of intersection are in one plane: $C^1 \cap C^2, C^2 \cap C^3, C^3 \cap C^4, C^4 \cap C^5 \in K^1$. Since the two points of C^2 in K^1 lie already in a second conic, the intersection point $C^2 \cap C^4$ lies in another conic K^2. Then, by using α and α^{-1}, the intersection points $C^1 \cap C^3, C^2 \cap C^4, C^3 \cap C^5$ are in fact incident with K^2.

We still need to determine in which conics K^i the intersection points $C^1 \cap C^4, C^2 \cap C^5$, and $C^1 \cap C^5$ lie. Again, by using α, the first two of those three intersection points lie in the same conic K^i.

Notation 2.8 The conics C^i and C^j intersect in R_1 and one other point. We address this point of intersection between the conics C^i and C^j by (ij).

Lemma 2.9 *The points* (14) *and* (25) *lie in a conic* K^3*, different from* K^1 *and* K^2*.*

Proof: The point (25) does not lie in K^1, since the two points of C^2 in K^1 already lie on C^1 and C^3. Suppose that (14) and (25) lie in K^2. Then the intersection points $(24), (13), (35), (14), (25)$ all lie in K^2. The conic K^2 is also stabilised by the cyclic group C_{q+1} generated by α. So these intersection points can be mapped onto each other by an appropriate power α^m of α. For instance, $\alpha^m(14) = (24)$, then

$$\begin{cases} 1+m & \equiv & 4 \pmod{q+1}, \\ 4+m & \equiv & 2 \pmod{q+1}. \end{cases}$$

This implies that $m \equiv 3 \pmod{q+1}$ and that $m = -2 \pmod{q+1}$. So $5 \equiv 0 \pmod{q+1}$. This is impossible, if $q \geq 64$. □

Lemma 2.10 *The point* (15) *lies in a conic* K^4*, different from* K^1, K^2, K^3*.*

Proof: The point (15) does not lie in K^1 since the two points of C^1 in K^1 already lie on the conics C^0 and C^2. Suppose that $(15) \in K^2$, then K^2 contains the points $(24), (13), (35), (15)$. Again, there must be a power α^m of α mapping one of these intersection points on another intersection point lying in K^2. Assume that $\alpha^m(13) = (15)$. Then

$$\begin{cases} 1+m & \equiv & 5 \pmod{q+1}, \\ 3+m & \equiv & 1 \pmod{q+1}. \end{cases}$$

This implies that $6 \equiv 0 \pmod{q+1}$. This is impossible, if $q \geq 64$. Suppose that (15) lies in K^3. Then K^3 contains the intersection points $(14), (25), (15)$. Assume that $\alpha^m(25) = (15)$. Then

$$\begin{cases} 2+m & \equiv & 5 \pmod{q+1}, \\ 5+m & \equiv & 1 \pmod{q+1}. \end{cases}$$

This implies that $7 \equiv 0 \pmod{q+1}$. This is impossible, if $q \geq 64$. □

We conclude that the ten intersection points of the conics $C^1, \ldots, C^5$ lie in four conics K^1, K^2, K^3, K^4, containing respectively $4, 3, 2, 1$ intersection points as shown in Figure 2.4.

With sums of the numbers $1, 2, 3, 4$, it is possible to complete the interval 0 to 10, so we can get all possibilities modulo 10. We now apply this to get a sequence for the cardinalities for the maximal partial ovoids.

- $u = 0 : M = (s-1)q - 10r + 15$. We select none of the planes through ℓ with points of intersection. Then $1 \leq r \leq q/2 - 3$. The lower bound follows from the fact that the number r also includes the plane $\langle \ell, R_1 \rangle$ intersecting $C^1, \ldots, C^5$, and the upper bound from the fact that we need to avoid the four planes containing the intersection points.

- $u = 1 : M = (s-1)q - 10r + 16$. We select the plane K^4 with one point of intersection, but none of the other planes with intersection points, thus $2 \leq r \leq q/2 - 2$. The lower bound follows from the fact that the number r also includes the plane $\langle \ell, R_1 \rangle$ intersecting $C^1, \ldots, C^5$, while the upper bound $q/2 - 2$ comes from the fact that we need to avoid the three other planes containing intersection points.

- $u = 2 : M = (s-1)q - 10r + 17$. We select the plane K^3 with two points of intersection, but none of the other planes with intersection points, thus $2 \leq r \leq q/2 - 2$.

- $u = 3 : M = (s-1)q - 10r + 18$. We select the plane K^2 with three points of intersection, but none of the other planes with intersection points, thus $2 \leq r \leq q/2 - 2$.

- $u = 4 : M = (s-1)q - 10r + 19$. We select the plane K^1 with four points of intersection, but none of the other planes with intersection points, thus $2 \leq r \leq q/2 - 2$.

- $u = 5 : M = (s-1)q - 10r + 20$. We select the planes K^1 and K^4 with respectively four and one points of intersection, but none of the other planes with intersection points, thus $3 \leq r \leq q/2 - 1$.

- $u = 6 : M = (s-1)q - 10r + 21$. We select the planes K^1 and K^3 with respectively four and two points of intersection, but none of the other planes with intersection points, thus $3 \leq r \leq q/2 - 1$.

- $u = 7 : M = (s-1)q - 10r + 22$. We select the planes K^1 and K^2 with respectively four and three points of intersection, but none of the other planes with intersection points, thus $3 \leq r \leq q/2 - 1$.

- $u = 8 : M = (s-1)q - 10r + 23$. We select the planes K^1, K^2, and K^4 with respectively four, three, and one points of intersection, but not the plane K^3 with two intersection points, thus $4 \leq r \leq q/2$.

- $u = 9 : M = (s-1)q - 10r + 24$. We select the planes K^1, K^2, and K^3 with respectively four, three, and two points of intersection, but not the plane K^4 with one intersection point, thus $4 \leq r \leq q/2$.

- $u = 10 : M = (s-1)q - 10r + 25$. We select the planes K^1, K^2, K^3, and K^4 with respectively four, three, two, and one points of intersection, thus $5 \leq r \leq q/2 + 1$.

2.4 Interval Calculation

For the spectrum, we do not wish to distinguish between the different cases for r from the above section. We impose $5 \leq r \leq q/2 - 3$ and get the interval $M = (s-1)q - 10r + 15, \ldots, M = (s-1)q - 10r + 25$, for a given pair (s, r). Together with the prior conditions from Corollary 2.7, we derive the following relevant constraints for s, r:

1. $r + 18 + \lfloor 48 \log(q+1) \rfloor \leq s$,

2. $5 \leq r \leq q/2 - 3$,

3. if $s \geq q/2$, then $r \geq s - q/2$.

For divisibility reasons we have to distinguish between $q \equiv 1, 2, 3, 4$ and $5 \pmod 5$. As q is a power of 2, it is not congruent to $0 \pmod 5$. For the remaining cases we explain the construction exemplarily for $q = 2^{4h+1}$ or in other words $q \equiv 2 \pmod 5$. The other residues follow immediately. We proceed as follows to find a non-interrupted interval of values of M for which a maximal partial ovoid of size M in $Q(4,q)$, q even, exists. We know that $5 \leq r \leq q/2 - 3$. Let's first discuss the case $s \leq q/2 + 5$. For $s \leq q/2 + 5$, r can start with 5.

For a selected pair (s,r) with $r = 5$, we find the sizes

$$\begin{aligned} M &= (s-1)q - 25, \\ &\vdots \\ M &= (s-1)q - 35. \end{aligned}$$

Consider the value $s' = s + 1$, and let r go from 5 to $(q+48)/10$, then we obtain all cardinalities M from

$$\begin{aligned} M &= sq - 25 \text{ for } r = 5, \\ &\vdots \\ M &= (s-1)q - 23 \text{ for } r = (q+48)/10, \\ &\vdots \\ M &= (s-1)q - 33 \text{ for } r = (q+48)/10. \end{aligned}$$

We get this block of values for fixed s' and flexible $r \in [5, (q+48)/10]$, and the lowest cardinality is $M = (s-1)q - 33$. The next smaller values are $M = (s-1)q - 34$ and $M = (s-1)q - 35$, but those we know from above for $(s,r) = (s,5)$. Therefore the block for the next value for s is connecting up with the previous. This enables us to get a large non-interrupted interval of integer values M for the size of maximal partial ovoids of $Q(4,q)$ in the even case.

We now discuss the case $s = q/2 + u$, with $u \geq 6$, so from the imposed conditions, $r \geq u$.

For $s = q/2 + u$ and $r = u$, we get a block of sizes

$$\begin{aligned} M &= q^2/2 + (u-1)q - 10u + 25, \\ &\vdots \\ M &= q^2/2 + (u-1)q - 10u + 15. \end{aligned}$$

For $s = q/2 + u + 1$ and $r = (q-2)/10 + u$, we get the block

$$\begin{aligned} M &= q^2/2 + (u-1)q - 10u + 27, \\ &\vdots \\ M &= q^2/2 + (u-1)q - 10u + 17. \end{aligned}$$

So for $s = q/2 + u + 1$ and $r \in [u+1, (q-2)/10 + u]$, the smallest size that is obtained, is equal to $M = q^2/2 + (u-1)q - 10u + 17$. Then, the values $(s, r) = (q/2 + u, u)$ give the next smaller values $M = q^2/2 + (u-1)q - 10u + 16$ and $M = q^2/2 + (u-1)q - 10u + 15$.

We find a large consecutive sequence of integer values M, and all are sizes of maximal partial ovoids of $Q(4, q)$ where q is even.

It remains to determine the borders of this spectrum; the smallest and the largest value of this complete sequence.

To determine the largest value, we note that we have to impose the upper bound $r = (q-2)/10+u \leq q/2-3$, since we need to use the value $r = (q-2)/10+u$ for $s = q/2+u+1$. So $u \leq (4q-28)/10$, and so $s = q/2 + u + 1 \leq (9q - 18)/10$.

For $(s, r) = ((9q-18)/10, (4q-18)/10)$, the largest size is $M = (s-1)q - 10r + 25 = (9q^2 - 68q + 430)/10$.

For the smallest value we note, that if $s = 18 + 48\lfloor \log(q+1) \rfloor + (q+48)/10$, it is possible to let r vary within $r \in [5, (q+48)/10]$. For $(s, r) = (18 + \lfloor 48 \log(q+1) \rfloor + (q+48)/10, (q+48)/10)$, the smallest cardinality is $M = (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 208q)/10 - 33$.

For $(s, r) = (17 + \lfloor 48 \log(q+1) \rfloor + (q+48)/10, 5)$, we get the sizes

$$\begin{aligned} M &= (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 208q)/10 - 25, \\ &\vdots \\ M &= (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 208q)/10 - 35. \end{aligned}$$

This block gives values smaller than $M = (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 208q)/10 - 33$; we still have no gaps in the sequence of values for M.

For $s = 17 + \lfloor 48 \log(q+1) \rfloor + (q+48)/10$, necessarily, $r \leq (q+38)/10$. For $(s, r) = (17 + \lfloor 48 \log(q+1) \rfloor + (q+48)/10, (q+38)/10)$, we derive a block of values

$$\begin{aligned} M &= (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 198q)/10 - 13, \\ &\vdots \\ M &= (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 198q)/10 - 23. \end{aligned}$$

The next block is obtained for $(s, r) = (16 + \lfloor 48 \log(q+1) \rfloor + (q+48)/10, 5)$, which gives cardinalities

$$\begin{aligned} M &= (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 198q)/10 - 25, \\ &\vdots \\ M &= (10q\lfloor 48 \log(q+1) \rfloor + q^2 + 198q)/10 - 35. \end{aligned}$$

When comparing the last two sequences, we see that the value $M = (10q\lfloor 48\log(q+1)\rfloor + q^2 + 198q)/10 - 24$ is missing.

So the value where the non-interrupted sequence ends, is equal to $(10q\lfloor 48\log(q+1)\rfloor + q^2 + 198q)/10 - 23$.

Altogether we can now state the borders of the possible spectra for all different integers q. In the following theorem the cardinality for the smallest and largest maximal partial ovoid of the interval is stated, depending on the division property of q. This non-interrupted spectrum coincides in great lines with the interval $[q^2/10, 9q^2/10]$.

Theorem 2.11 *The parabolic quadric $Q(4,q)$ and the symplectic space $W(q)$ with $q = 2^t$ and $t \geq 6$ have maximal partial ovoids for every value M in the interval*

- $q = 2^{4h}$:
$$M \in [\frac{q^2 + 194q + 10q\lfloor 48\log(q+1)\rfloor - 190}{10}, \frac{9q^2 - 69q + 440}{10}],$$
- $q = 2^{4h+1}$:
$$M \in [\frac{q^2 + 198q + 10q\lfloor 48\log(q+1)\rfloor - 230}{10}, \frac{9q^2 - 68q + 430}{10}],$$
- $q = 2^{4h+2}$:
$$M \in [\frac{q^2 + 196q + 10q\lfloor 48\log(q+1)\rfloor - 210}{10}, \frac{9q^2 - 66q + 410}{10}],$$
- $q = 2^{4h+3}$:
$$M \in [\frac{q^2 + 192q + 10q\lfloor 48\log(q+1)\rfloor - 170}{10}, \frac{9q^2 - 67q + 420}{10}].$$

Moreover, for every such integer M there exists a minimal blocking set of size M w.r.t. the planes of $PG(3,q)$.

Proof: It is proven in [24] that a maximal partial ovoid of $W(q)$, q even, defines a minimal blocking set w.r.t. the planes of $PG(3,q)$. □

Another application of our spectrum result is a spectrum result on maximal partial 1-systems of the Klein quadric $Q^+(5,q)$ [41, Section 15.4].

Definition 2.12 A *1-system* $\mathcal{M}$ on $Q^+(5,q)$ is a set of q^2+1 lines $\ell_1, \ldots, \ell_{q^2+1}$ on $Q^+(5,q)$ such that $\ell_i^\perp \cap \ell_j = \emptyset$, for all $i,j \in \{1,\ldots,q^2+1\}$, $i \neq j$.

A *partial 1-system* $\mathcal{M}$ on $Q^+(5,q)$ is a set of $s \leq q^2+1$ lines $\ell_1, \ldots, \ell_s$ on $Q^+(5,q)$ such that $\ell_i^\perp \cap \ell_j = \emptyset$, for all $i,j \in \{1,\ldots,s\}$, $i \neq j$.

A line of the Klein quadric lies in two planes of the Klein quadric. The above definition of 1-system is equivalent to the definition that a 1-system $\mathcal{M}$ on $Q^+(5,q)$ is a set of q^2+1 lines $\ell_1, \ldots, \ell_{q^2+1}$ on $Q^+(5,q)$ such that every line ℓ_j is skew to the two planes of the Klein quadric through any line ℓ_i, for all $i,j \in \{1,\ldots,q^2+1\}$, $i \neq j$. A similar observation can be made regarding the definition of a partial 1-system.

Via the Klein correspondence, points of the Klein quadric correspond to lines of $PG(3,q)$, and lines of the Klein quadric correspond to planar pencils of $PG(3,q)$, i.e. they correspond to the lines of $PG(3,q)$ through a point R in a plane Π passing through R.

A *tangency set* $\mathbb{T}$ of $PG(3,q)$ is a set of points of $PG(3,q)$, such that for every point $R \in \mathbb{T}$, there is a plane Π_R intersecting $\mathbb{T}$ only in R. It is proven in [65] that a tangency set in $PG(3,q)$ is equivalent to a partial 1-system on the Klein quadric.

A minimal blocking set B w.r.t. the planes of $PG(3,q)$ is an example of a tangency set; thus we can apply the results of Theorem 2.11.

Corollary 2.13 *For every value M belonging to one of the intervals of Theorem 2.11, there exists a maximal partial 1-system of size M on the Klein quadric $Q^+(5,q)$.*

2.5 Fringe

Our goal here was to find an uninterrupted spectrum of values for which maximal partial ovoids exist, but our construction also works outside the interval. In fact, for all parameters satisfying the conditions of Corollary 2.7, a maximal partial ovoid can be constructed. For instance: the parameters $(s,t) = (q+1,1)$ imply $r = q/2+1$ and $u = 0$, and give a maximal partial ovoid of size q^2-q+1; the parameters $(s,t) = (q+1,2)$ again imply $r = q/2+1$ and $u = 1$, and give a maximal partial ovoid of size q^2-2q+3; the parameters $(s,t) = (q,1)$ imply $u = 0$ and $r \in \{q/2, q/2+1\}$, leading to maximal partial ovoids of size q^2-2q+3 and q^2-2q+1.

Our results suggest that there exist maximal partial ovoids of size approximately q^2-iq, for small i, and their sizes lie in an interval $[q^2-iq-a_i, q^2-iq+b_i]$, where a_i and b_i are positive integers which are increasing in i. Eventually, for sufficiently large i, a non-interrupted interval of values appears for which a maximal partial ovoid exists. This idea led to the spectrum described in Theorem 2.11. The maximal partial ovoids of size q^2-q+1 and q^2-2q+3 also increase the importance of our construction method. Consider the ovoids of $Q(4,q)$ to be the largest maximal partial ovoids of $Q(4,q)$.

To complete the picture we want to mention other known results on the size of maximal partial ovoids of $Q(4,q)$ for even q. The theoretical results of [17, 24], together with the computer-aided results of [24], indicate that for the smallest possible sizes (approximately $q+1$) and the largest possible sizes (approximately q^2+1) of maximal partial ovoids there are gaps, thus not all integer values correspond to a maximal partial ovoid. We refer to [24] for the computer-aided data; here we present the main theoretical results.

Namely, Brown, De Beule, and Storme proved that q^2-q+1 is the size of the largest maximal partial ovoid (different from the ovoid itself) so our construction method finds the size of the second largest maximal partial ovoids on $Q(4,q)$.

Theorem 2.14 (Brown, De Beule, and Storme [17]) *(1) The maximal size of a partial ovoid of $Q(4,q)$, q even, is q^2+1, which is the size of an ovoid of $Q(4,q)$.*

(2) The size of the largest maximal partial ovoid of $Q(4,q)$, q even, different from an ovoid, is q^2-q+1, so there are no maximal partial ovoids with cardinality from q^2-q+2 to q^2.

The size q^2-2q+3 is particularly interesting in the problem of the construction of maximal partial ovoids on $Q(4,q)$. Here, we refer to computer-aided data on maximal partial ovoids of $Q(4,q)$, q

even. The following table shows values for which maximal partial ovoids on $Q(4,q)$, q even, were found. This is based on Table 1 of [24].

q	Spectrum found		
2*	**3,5**		
4*	**5,9,**		**11**,13,17
8	**9,17,**	21..**23**..47,49,	**51**,57,65
16	**17,33,**	**47**,49,51..163,165,	**227**,241,257

Table 2.1: Spectrum of sizes for maximal partial ovoids of $Q(4,q)$, for small even values of q. For $q = 2, 4$, the complete spectrum was obtained by exhaustive search. For larger values of q, the results are obtained by heuristic search.

The data of Table 2.1 suggests that q^2-2q+3 is the size of the third largest maximal partial ovoid. We also note that a maximal partial ovoid of size q^2-2q+3 on $Q(4,q)$, q even, was constructed in [24]. We now present some of the other known results on the size of small maximal partial ovoids of $Q(4,q)$, q even. The theoretical results of [17, 24], together with the computer-aided results of [24], indicate that for the smallest possible sizes (approximately $q+1$) of maximal partial ovoids on $Q(4,q)$, q even, there exist integer values for M for which there do not exist maximal partial ovoids of $Q(4,q)$, q even. We refer to Table 2.1 for the computer-aided data; here we present the main theoretical results.

Theorem 2.15 (Cimráková, De Winter, Fack, and Storme [24]) *(1) The smallest maximal partial ovoids of $Q(4,q)$, q even, have size $q+1$, and are equal to conics, lying in a plane not containing the nucleus N of $Q(4,q)$.*

(2) The generalised quadrangle $Q(4,q)$, $q \geq 4$ and even, has maximal partial ovoids of size $2q+1$, and of size $3q-1$.

In this article [24], also the non-existence of certain sizes in the interval $[q+2, 2q]$ for maximal partial ovoids is proven.

3 Partial Ovoids in Odd Order

Like in Chapter 2, we aim to find maximal partial ovoids of the generalised quadrangle $Q(4,q)$, and again, we are not looking for single results but for an uninterrupted interval of cardinalities, a spectrum. In this chapter we look into the case where the order of the projective space is odd. As before such a spectrum result on maximal partial ovoids implies that there is an interval, such that for every integer within this interval there exists a maximal partial ovoid with this cardinality. Since the generalised quadrangle $W(q)$ defined by a symplectic polarity of $PG(3,q)$ is isomorphic to the dual of the generalised quadrangle $Q(4,q)$ (see Definition 1.2), the same result will then hold for maximal partial spreads of $W(q)$, q odd.

The work presented in this chapter was obtained in collaboration with Valentina Pepe and Leo Storme [73].

Let's briefly recall from Chapter 1, Section 1.2, that if $Q(4,q)$ is a non-singular parabolic quadric in the projective space $PG(4,q)$, then the set of points and the set of lines of $Q(4,q)$ form a generalised quadrangle of order q. The points of $PG(3,q)$ and the self-polar lines of a symplectic polarity Δ of $PG(3,q)$ form the generalised quadrangle $W(q)$ of order q, which is isomorphic to the dual of $Q(4,q)$. The size of an ovoid of a generalised quadrangle Γ of order (s,t) is $st+1$, hence an ovoid of $Q(4,q)$ has size q^2+1.

3.1 Technique

The idea behind our construction was presented by T. Szőnyi et al in [94] where it was used to construct minimal blocking sets in $PG(2,q^2)$. They consider a particular minimal blocking set in the plane $PG(2,q^2)$, namely the Hermitian curve $H(2,q^2)$, and replace q of the points lying on a secant line ℓ of the curve by the point $\ell^\perp$. They obtain in this way a new minimal blocking set of the plane, but of a smaller size. It is clear that in this construction the polarity of the Hermitian curve plays an important role, and so it does also in ours.

The quadric $Q(4,q)$, q odd, induces a polarity $\perp$ in $PG(4,q)$ and we will widely use that polarity. The points of $Q(4,q)$ are called *singular*; if two singular points are joined by a line contained in $Q(4,q)$, we will say that they are *collinear* (in $Q(4,q)$); finally, every line ℓ not contained in $Q(4,q)$ intersects $Q(4,q)$ in $0,1$, or 2 points, and so ℓ is called *external*, *tangent*, or *secant*, respectively.

We proceed as in Chapter 2, but with certain variations, as we discuss the case of q odd. Let $Q^-(3,q)$ be an elliptic quadric of $Q(4,q)$, the intersection of $Q(4,q)$ and a hyperplane Δ of $PG(4,q)$. Here we have to show that $Q^-(3,q)$ is an ovoid of $Q(4,q)$. Every line ℓ of $Q(4,q)$ intersects Δ in at least one point, since $Q^-(3,q)$ does not contain lines, ℓ intersects $Q^-(3,q)$ in exactly one point. Hence, $Q^-(3,q)$ is an ovoid of $Q(4,q)$; $Q^-(3,q)$ is also called the *classical*

ovoid of $Q(4,q)$. Let now π be a plane of Δ that intersects $Q^-(3,q)$ in a conic c; the line $\pi^\perp$ can be either external or secant (see e.g. [41]) to $Q(4,q)$. For our approach we need to distinguish between the planes π according to this property of $\pi^\perp$. Let $\mathtt{O}$ denote the set of planes $\pi \subset \Delta$ with $\pi \cap Q^-(3,q) = c$ and $\pi^\perp \cap Q(4,q) = \emptyset$ and let $\mathtt{I}$ be the set of planes in Δ, intersecting $Q^-(3,q)$ in a conic, where the line $\pi^\perp$ intersects $Q(4,q)$ in two points. If π is a plane of $\mathtt{I}$, thus with an intersecting polar line, and we delete the points of $\pi \cap Q^-(3,q)$ from $Q^-(3,q)$ and add the points of $\pi^\perp \cap Q(4,q)$, we obtain a set Θ of size q^2-q+2. If $P \in \pi^\perp$ is a singular point, then $P^\perp \cap \Delta = \pi$, hence if a line $\ell \subset Q(4,q)$ intersects $\pi^\perp$ in P, then ℓ intersects Δ in a point of $\pi \cap Q(4,q)$, so Θ is a partial ovoid of $Q(4,q)$. Moreover, if we add a point $R \notin \pi^\perp$ to Θ, then $R^\perp \cap \Delta$ is a plane (different from π) containing a conic, so there would be lines of $Q(4,q)$ with two points. Hence, we can conclude that Θ is a maximal partial ovoid of $Q(4,q)$ of size q^2-q+2. In order to obtain a spectrum result for the size of Θ, we can delete the points of more conics of $Q^-(3,q)$ contained in planes $\pi \in \mathtt{I}$ and replace them by the singular points of $\pi^\perp$. While doing this, we need to check that:

- we only use planes $\pi \in \mathtt{I}$ in this construction,
- Θ is a partial ovoid, that is, the points we add must not be collinear in $Q(4,q)$,
- Θ is maximal.

Furthermore we need to compute the exact number of singular points of the planes $\pi \in \mathtt{I}$.

3.2 Construction

3.2.1 Setting

We first list the important elements involved in the construction. These include: (1) the parabolic quadric $Q(4,q)$, (2) in a particular hyperplane Δ, the elliptic quadric $Q^-(3,q)$ contained in $Q(4,q)$, (3) a fixed line ℓ in Δ skew to $Q^-(3,q)$, and (4) the polar points R_1 and R_2 of ℓ with respect to $Q^-(3,q)$. There is also a cyclic group C_{q+1} of order $q+1$ fixing R_1 and R_2, and stabilizing $Q^-(3,q)$ which plays an important role in the construction of the maximal partial ovoids on $Q(4,q)$.

Let $\{(x_0,x_1,x_2,x_3) \mid x_0 \in \mathbb{F}_{q^2}, x_1,x_2,x_3 \in \mathbb{F}_q\}$ be the underlying vector space of $PG(4,q)$ and let

$$X_0^{q+1} + X_1X_2 + X_3^2 = 0$$

be the equation of the particular quadric $Q(4,q)$. If $P=(a_0,a_1,a_2,a_3)$, then $P^\perp$ is the hyperplane with equation $Tr(a_0^q X_0) + a_2X_1 + a_1X_2 + 2a_3X_3 = 0$, where Tr is the trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. The hyperplane Δ has equation $X_3=0$ and $\Delta \cap Q(4,q)$ is the elliptic quadric $Q^-(3,q)$ with equation $X_0^{q+1} + X_1X_2 = 0$; the line $\ell = \{(x_0,0,0,0) \mid x_0 \in \mathbb{F}_{q^2}\}$ is an external line contained in Δ and $\ell^\perp \cap \Delta$ is a line intersecting $Q^-(3,q)$ in two points: $R_1=(0,1,0,0)$ and $R_2=(0,0,1,0)$. Let C_{q+1} be the set of the elements x of $\mathbb{F}_{q^2}$ such that $x^{q+1}=1$; C_{q+1} is a cyclic (multiplicative) group of order $q+1$ and let η be its generator. By abuse of notation, we denote by C_{q+1} also the cyclic group of collineations of $PG(4,q)$ acting as follows:

$$(x_0,x_1,x_2,x_3) \longmapsto (\eta^i x_0, x_1, x_2, x_3).$$

The group C_{q+1} clearly fixes the quadrics $Q(4,q)$ and $Q^-(3,q)$, the line ℓ, and the points R_1 and R_2. We assume that the cyclic group C_{q+1} of collineations of $PG(4,q)$ described above is generated by a collineation α. For a given plane π in Δ, we denote its image under α^i by π^i. In particular, there is one involution in C_{q+1}, the transformation $\alpha^{(q+1)/2} : (x_0, x_1, x_2, x_3) \longmapsto (-x_0, x_1, x_2, x_3)$, and then $\pi^{(q+1)/2}$ is the image of the plane π under this involution. Without confusion we can refer to a plane π and the corresponding conic $\pi \cap Q^-(3,q)$ by the same name. The two sets of planes, respectively conics, we want to use in our construction of maximal partial ovoids, are contained in the hyperplane Δ, hence we omit the equation $X_3 = 0$ each time and we just use the equations that describe them in $\Delta : X_3 = 0$.

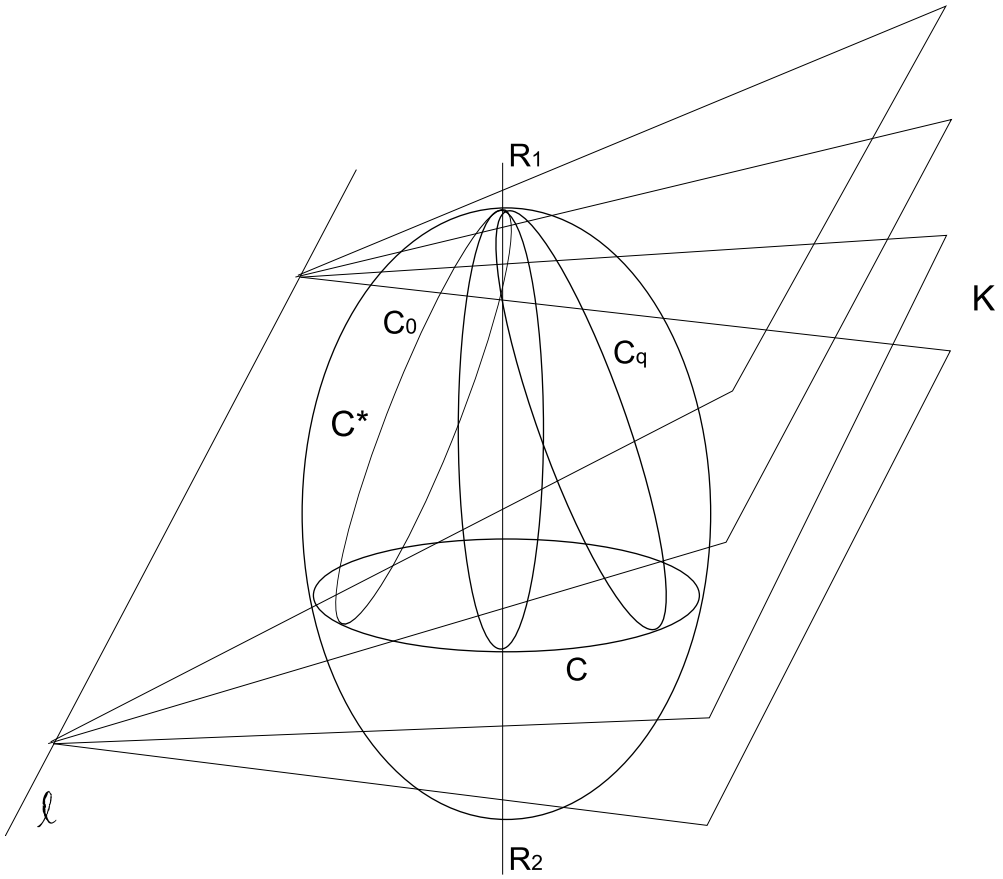

Figure 3.1: Set K of conics of $Q^-(3,q)$ in planes through ℓ and set C^*

One set contains the $q-1$ planes through ℓ intersecting $Q^-(3,q)$ in a conic. Such a set is also called a flock (see Chapter 1). Here the carriers of the flock are R_1 and R_2 and the conic C in Figure 3.1 belongs to the flock as well. A plane π of this set has equation: $X_1 + aX_2 = 0$, with $a \neq 0$, and $\pi \cap Q^-(3,q) = \{(x, -a, 1, 0) \mid x^{q+1} = a\}$. Every plane in this set is fixed by C_{q+1} and the points of such a conic form an orbit under the action of the group C_{q+1}. These planes do not intersect each other in singular points. We denote this set of planes by K.

The other set contains the planes of one orbit (of size $q+1$) under the action of C_{q+1} among the q^2-1 planes through R_1, but not through R_2, intersecting $Q^-(3,q)$ in a conic. Such planes have

an equation $Tr(A\eta^i X_0) + X_2 = 0$, with $A \in \mathbb{F}_{q^2} \setminus \{0\}$ and $i = 0, \ldots, q$. We call such a set of planes C^*.

3.2.2 Possible Intersections of the Conics in K and C^*

Firstly we investigate the conics $C^* = C^0, \ldots, C^q$ of $Q^-(3,q)$ belonging to one orbit under the cyclic group C_{q+1} of order $q+1$. How can the conics $\pi_1, \pi_2 \in C^*$ possibly intersect? For the respective planes (we can use the same notation, see page 45) π_1 and π_2, this question is equivalent to whether they intersect in a secant or a tangent line of $Q^-(3,q)$. Applying the polarity induced by $Q^-(3,q)$, this is equivalent to investigating whether the two polar points $\pi_1^\perp$ and $\pi_2^\perp$ w.r.t. $Q^-(3,q)$ lying in the plane $R_1^\perp : X_2 = 0$ generate an external or a tangent line w.r.t. $Q^-(3,q)$. If π_1 has equation $Tr(AX_0) + X_2 = 0$, then $\pi_1^\perp = (A^q, 1, 0, 0)$ and the orbit of this point under C_{q+1} consists of the points $(A^q\eta^i, 1, 0, 0)$, $i = 1, \ldots, q+1$; this is the conic of the plane $R_1^\perp$ with equation $A^{q+1}X_1^2 = X_0^{q+1}$. The only lines tangent to $Q^-(3,q)$ in these planes are the ones through $R_1 = (0,1,0,0)$ and the only tangent line through $\pi_1^\perp$ is the one joining $\pi_1^\perp = (A^q, 1, 0, 0)$ with $(-A^q, 1, 0, 0)$. Note that these two points are each others image under the involution $\alpha^{(q+1)/2}$.

This means that for every conic in C^*, there is only one other conic in C^* such that they intersect in R_1, only. From the preceding paragraph, it follows that the corresponding plane π and its image under the involution $\alpha^{(q+1)/2}$ intersect in a tangent line to $Q^-(3,q)$ through R_1. All other conics in the same orbit under C_{q+1} intersect in a second point. These intersection points are all different as the other planes under the orbit of C_{q+1} intersect π in a secant line and, since no three points $\pi_1^\perp$, $\pi_2^\perp$, and $\pi_3^\perp$ are collinear, the secant lines are all different, for every $\pi_i^\perp, i = 1, 2, 3$, in the same orbit under the cyclic group C_{q+1}.

We know that two conics of K do not intersect, but we need to investigate the intersections between conics from the set K and the set C^*:

How do conics of K in planes through ℓ intersect conics of C^* through R_1? The plane $\pi \in K$ through R_1 is tangent to all conics in C^*. Since q is odd, there is for every conic $C_i \in C^*$ another plane in K tangent to C_i. All other planes of K either intersect or miss C_i. Hence $\frac{q-1}{2}$ conics of K intersect C_i, and the remaining $\frac{q-1}{2}$ planes of K intersect the plane C_i in an external line to $Q^-(3,q)$.

3.3 Selecting Suitable Sets of Conics

We want to replace singular points of a plane, respectively conic π, by the common singular polar points, i.e. by the singular points of $\pi^\perp$. Since q is odd, the line $\pi^\perp$ with respect to the polarity induced by $Q(4,q)$ can be either a secant or an external line and, as mentioned before, we need to avoid the latter case.

A plane $\pi_1 \in K$ can be expressed as: $\begin{cases} X_1 + aX_2 = 0, \\ X_3 = 0, \end{cases}$ with $a \neq 0$, hence $\pi_1^\perp$ is the line $\langle (0,a,1,0), (0,0,0,1) \rangle$. It is easy to check that $\pi_1^\perp$ is a secant line if and only if $-a$ is a square in $\mathbb{F}_q$, hence there are $\frac{q-1}{2}$ planes in K we can use. Let K^* for now consist of these $\frac{q-1}{2}$ planes.

If π_2 is a plane of C^*, then it has as equations: $\begin{cases} Tr(AX_0) + X_2 = 0, \\ X_3 = 0, \end{cases}$ with $A \neq 0$, so $\pi_1^\perp$ is the line $\langle (A^q, 1, 0, 0), (0, 0, 0, 1) \rangle$ and this is a secant line if and only if $-A^{q+1}$ is a square in $\mathbb{F}_q$.

Hence, in one orbit under C_{q+1}, the planes are all of the same type, so we can assume that in our case all the planes of C^* have a secant polar line and can be used.

Finally, for our construction we need to know which planes in K^* intersect the planes of C^*. All other planes of K^*, skew to the conics of C^*, we want to eliminate from K^*. Again, we look at their polar points $(0,a,1,0)$ and $(A^q,1,0,0)$ w.r.t $Q^-(3,q)$, and we have the line $\langle(0,a,1,0),(A^q,1,0,0)\rangle$. The two planes intersect in two singular points if and only if this polar line $\langle(0,a,1,0),(A^q,1,0,0)\rangle$ is external to $Q^-(3,q)$. In our setting, this polar line is an external line if and only if $1-4aA^{q+1}$ is a non-square, a bisecant line if and only if $1-4aA^{q+1}$ is a non-zero square, and a tangent line if and only if $1-4aA^{q+1}$ is zero. In this last case, $a=1/(4A^{q+1})$, so $-a=1/(4(-A^{q+1}))$ is a square in $\mathbb{F}_q$ since $-A^{q+1}$ is a square in $\mathbb{F}_q$. Therefore one of the planes in K^* is tangent to all conics in C^*. We call this plane and the related tangent conic K^t.

Since we consider an element A such that $-A^{q+1}$ is a square and since $-a$ is a non-zero square for a plane of K^* in question, we firstly determine how many times $1-4(-a)(-A^{q+1})$ is a non-zero square. This is related to finding how many $x^2\neq 0$ satisfy the equation $1-x^2=y^2$. This is the equation of an affine conic that has two points at infinity if -1 is a square, i.e. $q\equiv 1 \pmod 4$, or none otherwise, when $q\equiv 3 \pmod 4$. There are always two points corresponding to $y=0$ and there are always two points corresponding to the value $x=0$, so there are $\frac{q-5}{4}$ ($\frac{q-3}{4}$ respectively) values of $x^2\neq 0$ for $q\equiv 1 \pmod 4$ (for $q\equiv 3 \pmod 4$ respectively) that satisfy the equation $1-x^2=y^2$. Hence, among the $(q-1)/2$ planes in K^*, there is one, K^t, tangent to the conics of C^* and $(q-5)/4$ skew to the conics of C^*. More precisely, if $a=\frac{1}{4A^{q+1}}$, then the corresponding plane $K^t\in K^*$ intersects all the planes in C^* in a tangent line and there are $\frac{q-1}{2}-1-\frac{q-5}{4}=\frac{q-1}{4}$ planes in K^*, intersecting the planes of C^* in two singular points if $q\equiv 1 \pmod 4$ ($\frac{q-3}{4}$ if $q\equiv 3 \pmod 4$).

We summarise the results of this paragraph in the following lemma:

Lemma 3.1 *There is one plane $K^t\in K^*$ that intersects all the planes of C^* in a tangent line and there are $\frac{q-1}{4}$ or $\frac{q-3}{4}$ planes in K^* that intersect the planes of C^* in a secant line if $q\equiv 1 \pmod 4$ (or if $q\equiv 3 \pmod 4$ respectively).*

From now on, K^* may consist of K^t and those $\frac{q-1}{4}$ (or $\frac{q-3}{4}$ respectively) planes, only.

3.3.1 Replacing the Selected Conics

When we replace the points of several conics of $Q^-(3,q)$ by their common polar points, we need to check that the new set is still a partial ovoid, meaning the points added are in $Q(4,q)$ not collinear with any other point of the new set. The conics in question are from the sets C^* and K^* we discussed in Section 3.3 and they are replaced by their polar points.

For every point $P\notin\Delta$ that we add, we know that $P^\perp\cap Q^-(3,q)$ is a conic that we have thrown away, so none of its lines of $Q(4,q)$ is collinear with a point still in Δ. We need to make sure that the points out of Δ which we add are not collinear with each other (see Figure 3.2) since we want to construct a new partial ovoid on $Q(4,q)$. The polar lines of K^* are the lines through the point $\Delta^\perp$ in the plane $\ell^\perp$ secant to the conic of $Q(4,q)$ contained in $\ell^\perp$; of course they are two by two not collinear. The polar lines of the planes in C^* are the lines in $R_1^\perp$ through the point $\Delta^\perp$ and they are secant to the tangent cone contained in $R_1^\perp$. Using coordinates, the points of intersection are $(\eta^i A^q,1,0,\pm\sqrt{-A^{q+1}})$, where $\sqrt{a}$ is one of the two elements in $\mathbb{F}_q$ whose square

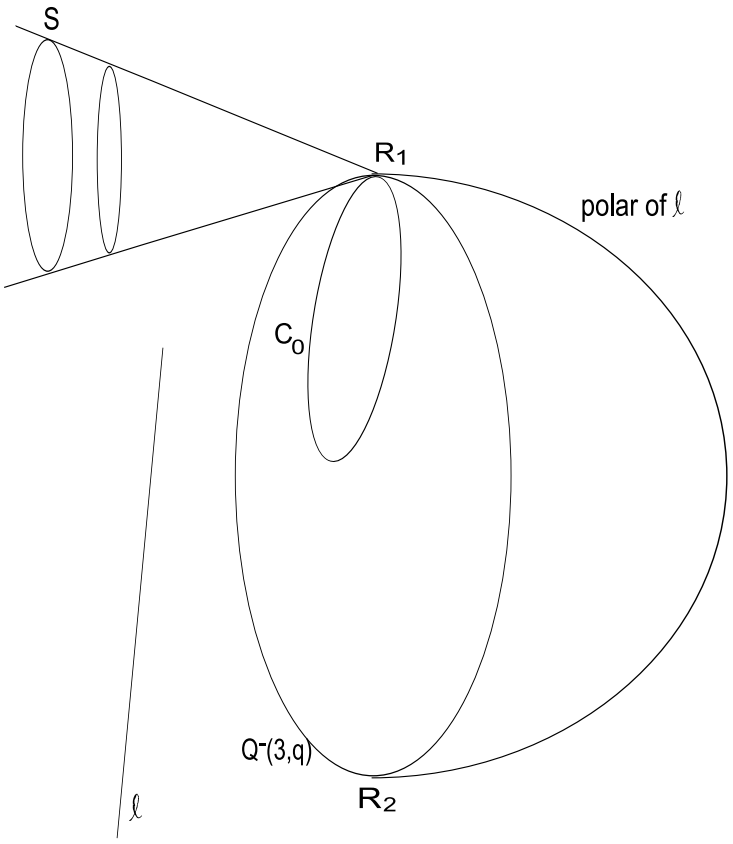

Figure 3.2: Polar points of K^* and C^*

is a. They form two conics in the hyperplane $R_1^\perp : X_2 = 0$, one in the plane $X_3 = \sqrt{-A^{q+1}}X_1$ and the other in the plane $X_3 = -\sqrt{-A^{q+1}}X_1$; a point $(\eta^i A^q, 1, 0, \sqrt{-A^{q+1}})$ of the first conic is collinear on $Q(4,q)$ with the point $(-\eta^i A^q, 1, 0, -\sqrt{-A^{q+1}})$, which means the polar points of the conic of the plane $\pi \in C^*$ are collinear with a polar point of the conic of $\pi^{(q+1)/2}$, where $\pi^{(q+1)/2}$ is the image of π under the collineation of C_{q+1} of order two. Let now $(0, a, 1, \sqrt{-a})$ be one of the polar points added in place of a conic in K^* with equations $\begin{cases} X_1 + aX_2 = 0, \\ X_3 = 0, \end{cases}$; it is collinear with $(\eta^i A^q, 1, 0, \pm\sqrt{-A^{q+1}})$ if and only if $a = \frac{1}{4A^{q+1}}$, thus when the plane in K^* intersects the planes of C^* in a tangent line.

3.3.2 Constraints

We still have to take care of the constraints on the number of conics from different sets which we can replace in order to obtain a non-interrupted interval of maximal partial ovoids of $Q(4,q)$ (or better interval of cardinalities of maximal partial ovoids).

Let s be the number of planes of K^* that we do not replace, let t be the number of planes in C^* that we replace, let r be the number of planes in K^* that we do not replace and that intersect the planes in C^* in a secant line, and let u be the number of points, different from R_1, in which

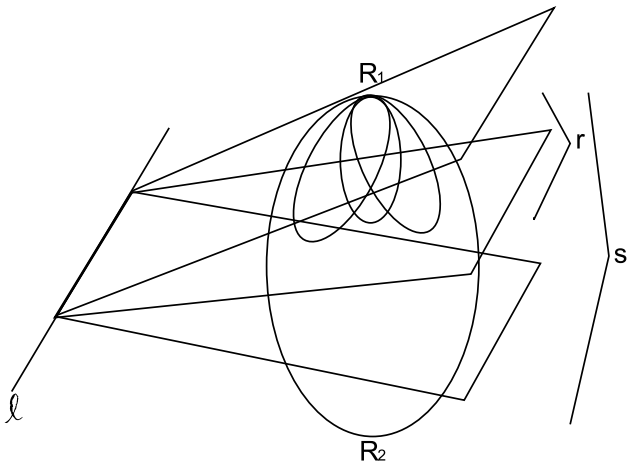

Figure 3.3: The parameters r and s in the construction

the conics in the planes of C^* thrown away intersect each other. We have indicated these s and r planes of K^* in Figure 3.3. In order to get a partial ovoid after the replacement, we need to impose:

$$1 \leq t \leq \frac{q+1}{2},$$

since C^* consists of one orbit of planes under the action of C_{q+1}. In order to avoid collinear polar points: if we replace the points of the plane $\pi \in C^*$, we can not replace the points of $\pi^{(q+1)/2}$, since they have collinear polar points on $Q(4,q)$ (Subsection 3.3.1), hence we can replace at most the points of the planes $\pi^{(i)}, i = 1, \ldots, \frac{q+1}{2}$. Moreover, we have

$$\frac{q+1}{2} \leq s \leq q-1,$$

because there are $\frac{q-1}{2}$ planes in K^*, which we do not replace, and there is also the plane K^t through ℓ that intersects the planes of C^* in a tangent line, hence the polar points added would be collinear if we would throw away this plane, so we can not replace the points of at least $\frac{q+1}{2}$ planes through ℓ.

In this way, we know that the newly constructed set Θ is a partial ovoid of $Q(4,q)$, but Θ also has to be maximal, hence for every point P of $Q(4,q) \setminus \Theta$, there exists at least one point of $P^\perp$ in Θ. This is of course true for every point of Δ; let P be a point of $Q(4,q)$ not in Δ and let π_P be the plane $P^\perp \cap \Delta$: we impose that $\pi_P \cap \Theta \neq \emptyset$. We have different cases:

1. $\ell \subseteq \pi_P$: the other planes of K do not intersect π_P in any singular point, while the planes of C^* can intersect π_P in at most two points, hence we impose that $t < \frac{q+1}{2}$ to make sure that $\pi_P \cap \Theta \neq \emptyset$.

2. $\ell \not\subseteq \pi_P$ and $R_2 \in \pi_P$: R_2 is not contained in any of the conics of $Q^-(3,q)$ that we throw away, so π_P contains always at least the point R_2 of Θ.

3. $\ell \not\subseteq \pi_P$, $R_1 \in \pi_P$ and $R_2 \notin \pi_P$; in this case we have two subcases:

3.a) π_P is one of the planes of C^*: this plane is tangent to a particular plane π of K^* in one singular point P'; the conic K^t of the plane π is not deleted (see the condition for s above) and the other planes of C^* intersect π_P in points different from P', hence we know that the point P' is never thrown away from π_P.

3.b) π_P is in another orbit under the action of C_{q+1}: Let π_P: $Tr(A'X_0)+X_2=0$. Checking the four distinct cases for $(-A'^{q+1}, q)$, $-A'^{q+1}$ is a non–zero square or a non–square, $q \equiv 1 \mod 4$ or $q \equiv 3 \mod 4$, if we impose $t < \frac{q-1}{2}$, then the planes of K^* and the t deleted conics of C^* cannot cover all the points of the conic of π_P.

4. $\ell \not\subseteq \pi_P$ and R_1, $R_2 \notin \pi_P$: the planes of K intersect π_P in at most two singular points. We consider the following two cyclic groups fixing the line ℓ: the group C_1 of size $\frac{q-1}{2}$ that acts regularly on the planes of K which have a bisecant polar line to $Q(4,q)$, and the group C_2 that acts regularly on those planes of K that intersect π_P in a secant line, so C_2 has size $\frac{q+1}{2}$ or $\frac{q-1}{2}$, according to the fact that through ℓ there are zero or two planes intersecting π_P in a tangent line. Since these two groups fix a line in a three–dimensional space, we can assume that C_1 and C_2 are subgroups of $PGL(2,q)$, so we can use Theorem 3.4, Theorem 3.5, and Corollary 3.6 of [90] and state that the planes through ℓ having a bisecant polar line and intersecting π_P in a secant line are at most $\frac{q+3\sqrt{q}}{4}$. In order to keep at least one of the points of the conic of π_P in Θ, we need to impose $2t+2+\frac{q+3\sqrt{q}}{2} < q+1$, where $2t$ comes from the at most $2t$ intersection points of the t deleted conics of C^* with π_P, and where 2 comes from the at most two tangent points of the two possible planes in K^* tangent to π_P.

To conclude, we have the following new constraint for t:

$$t < \frac{q-3\sqrt{q}-2}{4}.$$

Finally, for the parameter r we have:

a) $\frac{q-1}{4} \leq r \leq s-\frac{q-1}{4}-1$ for $q \equiv 1 \pmod 4$, and $\frac{q+1}{4} \leq r \leq s-\frac{q-3}{4}-1$ for $q \equiv 3 \pmod 4$,

b) $s=\frac{3}{4}(q-1) \Rightarrow \frac{q-1}{4} \leq r \leq \frac{q-1}{2}-1$ for $q \equiv 1 \pmod 4$, and $s=\frac{3q-1}{4} \Rightarrow \frac{q+1}{4} \leq r \leq \frac{q-1}{2}$ for $q \equiv 3 \pmod 4$,

c) $s > \frac{3}{4}(q-1)$ for $q \equiv 1 \pmod 4$, and $s > \frac{3q-1}{4}$ for $q \equiv 3 \pmod 4 \Rightarrow s-\frac{q-1}{2} \leq r \leq \frac{q-1}{2}$.

We give a brief explanation, dealing with the cases $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ simultaneously. We know that there are $\frac{q-1}{4}$ ($\frac{q+1}{4}$ for $q \equiv 3 \pmod 4$) planes in K (with an external polar line) that intersect the planes of C^* in a secant line (Lemma 3.1). These planes are never thrown away, hence we always have $\frac{q-1}{4} \leq r \leq \frac{q-1}{2}$. But the parameter r also depends on s. More precisely, these r planes are a subset of the s planes in K, which we have not replaced and among them we know that there is K^t (Lemma 3.1) and there are $\frac{q-1}{4}$ planes in K (with an external polar line) that intersect the planes of C^* in an external line ($\frac{q-3}{4}$ for $q \equiv 3 \pmod 4$), hence we have $r \leq s-\frac{q-1}{4}-1$ ($r \leq s-\frac{q-3}{4}-1$ for $q \equiv 3 \pmod 4$). Finally, from a certain value for s, as the value of s increases, also r does. There are $(q-3)/2$ conic planes in K skew to the conics of C^*, and there is K^t, tangent to all the conics of C^*. Hence, if $s-\frac{q-1}{2}$ is larger than the number of planes in K (with an external polar line) that intersect planes in C^* in a secant line,

then $r \geq s - \frac{q-1}{2}$, hence $s > \frac{3}{4}(q-1) \Rightarrow s - \frac{q-1}{2} \leq r$. The constraints mentioned before arise just by the comparison of these upper and lower bounds.

For every fixed s, t, r, and u, we get that the size of the maximal partial ovoid Θ on $Q(4,q)$ is $s(q-1)+2q-2tr+t+u-1$. This is proven in the following way.

We do not replace s of the conics of K; equivalently, we replace $q-1-s$ of the conics of K by their two polar points. This changes the size of the ovoid, i.e. the elliptic quadric $Q^-(3,q)$, from q^2+1 to $q^2+1-(q-1-s)(q+1)+2(q-1-s) = s(q-1)+2q$. We then delete the points of t conics in C^*. But some of the points of these t conics are already deleted. There are r conics in K that are not deleted and that intersect the conics of C^* in two points. Also the conic K^t is not deleted. The point R_1 belonging to all the conics in C^* has not yet been deleted. So $2r+1+1$ points in every conic of C^* still belong to the already constructed set of size $s(q-1)+2q$. The t conics in C^* that will be deleted, and replaced by their polar points, intersect, by assumption, in u points, different from R_1. So we only delete $t(2r+1)+1-u$ points from these t conics of C^*, and these $2tr+t-u+1$ points are replaced by the $2t$ polar points of these t conics of C^*. Hence, the size of the newly constructed set Θ is

$$s(q-1)+2q-2tr-1-t+u+2t = s(q-1)+2q-2tr+t+u-1.$$

3.3.3 Selection of Five Conics of C^*

In order to get a non-interrupted interval of values for the size of Θ, we proceed as in Chapter 2, i.e. we select five planes in C^* such that their ten intersection points (different from R_1) are partitioned in four planes of K^*, namely $\pi_i, i = 1, \ldots, 4$, each containing i of these 10 points of intersection. In this way, we set $t = 5$ and choosing the planes in K in a suitable way, we can let the parameter u vary from 0 to 10, so we immediately get the first non-interrupted interval

$$[(s+2)q - s + 4 - 10r, (s+2)q - s + 14 - 10r].$$

As in Chapter 2, we consider a plane π in C^* and the planes $\pi^{(i)}, i = 1, \ldots, 4$, which are the images of π under α, where α is a generator of the cyclic group C_{q+1}; the intersection points are the following: $\pi \cap \pi^{(i)} = P_i, i = 1, \ldots, 4$, $\pi^{(1)} \cap \pi^{(i)} = P_{i-1}^{(1)}, i = 2, 3, 4$, $\pi^{(2)} \cap \pi^{(i)} = P_{i-2}^{(2)}, i = 3, 4$, and $\pi^{(3)} \cap \pi^{(4)} = P_1^{(3)}$ (here, similarly, $P_j^{(k)}$ denotes the image of the point P_j under α^k). In Chapter 2, it is proven that, for $q > 5$, there exists a plane π_1 in K that contains the points $P_1, P_1^{(i)}, i = 1, 2, 3$, a plane π_2 of K that contains $P_2, P_2^{(i)}, i = 1, 2$, a plane π_3 of K that contains P_3 and $P_3^{(1)}$, and there is a plane π_4 in K that contains only the intersection point P_4. The main difference here, in comparison to Chapter 2, is that we have to check that the four planes $\pi_i, i = 1, \ldots, 4$, are also having a bisecant polar line of $Q(4,q)$. If the plane π has equation $Tr(AX_0) + X_2 = 0$, then the intersection $\pi \cap Q^-(3,q)$ is the conic $\{(A^q + A\eta^i, 1, -2A^{q+1} - Tr(A^2\eta^i), 0) \mid \eta^i \in C_{q+1}\} = \{(A^q + A^q\eta^j, 1, -2A^{q+1} - A^{q+1}Tr(\eta^j), 0) \mid \eta^j \in C_{q+1}\}$. There is one plane in C^* that intersects π in a tangent line through R_1. Every point of this conic in π, different from R_1 and different from one other particular point which is the intersection of π with the unique plane of K tangent to the conic $\pi \cap Q^-(3,q)$, is contained in just one other plane of C^*, namely the point $(A^q + A\eta^i, 1, -2A^{q+1} - Tr(A^2\eta^i), 0), \eta^i \neq A^{q-1}$, is contained in the plane with equation $Tr(\eta^{-i}A^qX_0) + X_2 = 0$ since we have that $Tr(\eta^{-i}A^q(A^q + A\eta^i)) = Tr(A(A^q + A\eta^i)) = 2A^{q+1} + Tr(A^2\eta^i)$. The plane K^t is the plane $X_1 + aX_2 = 0$, with $a = \frac{1}{4A^{q+1}}$

(see Subsection 3.3). This contains the point $(A^q + A\eta^i, 1, -2A^{q+1} - Tr(A^2\eta^i), 0), \eta^i = A^{q-1}$, so the point $(2A^q, 1, -4A^{q+1}, 0)$. The singular point in $\pi \cap \pi^{(-j)}$, $j \neq (q+1)/2$, different from R_1, is the point $P_j = (A^q + A^q\eta^{-j}, 1, -2A^{q+1} - A^{q+1}Tr(\eta^j))$. The point P_j is contained in the plane of K with equation $X_1 + aX_2 = 0$, with $a = \frac{1}{A^{q+1}(2+Tr(\eta^j))} = \frac{1}{A^{q+1}(1+\eta^j)^{q+1}}$. As we want these planes to be in K^*, we need $-a$ to be a non-zero square, that is $(1+\eta^j)^{q+1}$ is a non-zero square since $-A^{q+1}$ is a non–zero square, and this happens if and only if $1+\eta^j$ is a non-zero square in $\mathbb{F}_{q^2}$. So we need to prove the following lemma.

Lemma 3.2 *Let $C_{q+1} = \langle\eta\rangle$ be the cyclic multiplicative group of the $(q+1)$-th roots of unity in the field of odd characteristic $\mathbb{F}_{q^2}$. Then $1+\eta^i$, $\eta^i \in C_{q+1} \setminus \mathbb{F}_q$, is a non-zero square in $\mathbb{F}_{q^2}$ if and only if i is even.*

Proof: If we have $1+\eta^{2i}$, then $1+\eta^{2i} = \eta^i(\frac{1}{\eta^i} + \eta^i) = \eta^i Tr(\eta^i)$; if ξ is a primitive element of $\mathbb{F}_{q^2}$, then we can say that $\eta = \xi^{q-1}$ and that a primitive element of $\mathbb{F}_q$ is ξ^{q+1}, so every element of C_{q+1} and every element of $\mathbb{F}_q$ is a square in $\mathbb{F}_{q^2}$, so $\eta^i Tr(\eta^i)$ is a square too.
Vice versa, if we have that $1+\eta^i = d^2$, for some non-zero $d \in \mathbb{F}_{q^2}$, then $1+\eta^i = d^2 \Rightarrow \eta^i = d^2 - 1 \Rightarrow 1 = (d^2-1)^{q+1} \Rightarrow 1 = d^{2(q+1)} + 1 - d^2 - d^{2q} \Rightarrow d^{2(q+1)} = d^2 + d^{2q} \Rightarrow d^{2q} = 1 + d^{2(q-1)} \Rightarrow d^2 = 1 + d^{2(1-q)} = 1 + \eta^i$. Consequently, $d^{2(1-q)} = \eta^i$ and hence i has to be even. □

So the planes to be used are $\pi, \pi^{(2)}, \pi^{(4)}, \pi^{(6)}, \pi^{(8)}$, more precisely, for a given plane π of C^*, π has intersection points $\pi \cap \pi^{(2i)} = P_{2i}, i = 1, \ldots, 4$, $\pi^{(2)} \cap \pi^{(2i)} = P^{(2)}_{2(i-1)}, i = 2, \ldots, 4$, $\pi^{(4)} \cap \pi^{(2i)} = P^{(4)}_{2(i-2)}, i = 3, 4$, and $\pi^{(6)} \cap \pi^{(8)} = P^{(6)}_2$.

3.4 Calculation of the Interval

Now we can calculate the uninterrupted spectrum of values for the size of Θ. The case $q \equiv 1 \pmod 4$ and the case $q \equiv 3 \pmod 4$ need to be distinguished, but both follow the same argument, thus we can omit the proof for the case $q \equiv 3 \pmod 4$ and just provide the slightly different constraints for the parameters.

Maintaining the same notations as before, we know that for a fixed value of s and r, and for $t = 5$, choosing the planes in K^* in a suitable way, i.e. using the planes $\pi_i, i = 1, \ldots, 4$, of K^*, in the way described above, we can let the parameter u vary from 0 to 10, so we immediately get the first non-interrupted interval

$$[(s+2)q - s + 4 - 10r, (s+2)q - s + 14 - 10r]. \tag{3.1}$$

We now have slightly different constraints for the parameters, since we need a certain freedom to take or not take the four planes $\pi_i, i = 1, \ldots, 4$, so for $q \equiv 1 \pmod 4$, we have:

a) $\frac{q+1}{2} + 4 \leq s \leq q - 5$,

b) if $s \leq \frac{3(q-1)}{4} - 3$, then $\frac{q-1}{4} + 4 \leq r \leq s - \frac{q-1}{4} - 1$,

c) if $\frac{3(q-1)}{4} - 2 \leq s \leq \frac{3(q-1)}{4} + 3$, then $\frac{q-1}{4} + 4 \leq r \leq \frac{q-1}{2} - 4$,

d) if $s \geq \frac{3(q-1)}{4} + 4$, then $s - \frac{q-1}{2} \leq r \leq \frac{q-1}{2} - 4$.

The interval (3.1) has size 10, so if we let the parameter r vary and fix s, we still have a non-interrupted interval. Taking condition b) into consideration, we have the range

$$[s(q-11)+\frac{9q+23}{2}, s(q-1)-\frac{q+47}{2}], \tag{3.2}$$

if $s \leq \frac{3(q-1)}{4}-3$, but if we want s to be flexible too, we need to impose that $s'(q-11)+\frac{9q+23}{2} \leq s(q-1)-\frac{q+47}{2}$, where $s'=s+1$. By straightforward calculations, we get $\frac{3q+12}{5} \leq s$. Letting s vary in $[\frac{3q+12}{5}, \frac{3(q-1)}{4}-3]$, then from (3.2), we get:

$$[\frac{6q^2+3q-149}{10}, \frac{3q^2-20q-79}{4}]. \tag{3.3}$$

From condition c) follows:

$$[s(q-1)-3q+49, s(q-1)-\frac{q+47}{2}]. \tag{3.4}$$

The size of this interval is $\frac{5q-145}{2} \geq q-1$ if $q \geq \frac{143}{3}$, so s can be any integer from $\frac{3(q-1)}{4}-2$ to $\frac{3(q-1)}{4}+3$ in (3.4) and we obtain the interval:

$$[\frac{3q^2-26q+207}{4}, \frac{3q^2+4q-103}{4}]. \tag{3.5}$$

Finally, using condition d), we derive the range:

$$[s(q-1)-3q+49, s(q-11)+7q+9]. \tag{3.6}$$

In order to keep s flexible, we need to impose that $s'(q-1)-3q+49 \leq s(q-11)+7q+9$, where $s'=s+1$. In this way, we get $s \leq \frac{9q-39}{10}$, so s can vary within $[\frac{3(q-1)}{4}+4, \frac{9q-39}{10}]$ in (3.6). This gives the last interval:

$$[\frac{3q^2-2q+183}{4}, \frac{9q^2-68q+519}{10}]. \tag{3.7}$$

It is clear that the intervals (3.3), (3.5), and (3.7) overlap if $q \geq \frac{143}{3}$, so we have proven the following result.

Theorem 3.3 *For every integer in the interval* $[\frac{6q^2+3q-149}{10}, \frac{9q^2-68q+519}{10}]$, *there exists a maximal partial ovoid of* $Q(4,q)$, $q \geq 49$ *and* $q \equiv 1 \pmod 4$, *of this cardinality.*

For $q \equiv 3 \pmod 4$, we use exactly the same arguments, with the difference that the constraints for the parameters in this case are:

a) $\frac{q+1}{2}+4 \leq s \leq q-5$,

b) if $s \leq \frac{3q-1}{4}-4$, then $\frac{q+1}{4}+4 \leq r \leq s-\frac{q-3}{4}-1$,

c) if $\frac{3q-1}{4}-3 \leq s \leq \frac{3q-1}{4}+3$, then $\frac{q+1}{4}+4 \leq r \leq \frac{q-1}{2}-4$,

d) if $s \geq \frac{3q-1}{4}+4$, then $s-\frac{q-1}{2} \leq r \leq \frac{q-1}{2}-4$,

and this leads to the following uninterrupted interval.

Theorem 3.4 *For every integer in the interval* $[\frac{6q^2+3q-149}{10}, \frac{9q^2-68q+519}{10}]$, *there exists a maximal partial ovoid of* $Q(4,q)$, $q \geq 51$ *and* $q \equiv 3 \pmod 4$, *of this cardinality.*

It is known that in the dual generalised quadrangle (see Chapter 1, Section 1.2), a partial spread corresponds to a partial ovoid. So, since $W(q)$, q odd, is dual to $Q(4,q)$, q odd, it is obvious from the last two theorems, that:

Corollary 3.5 *For every integer in the interval* $[\frac{6q^2+3q-149}{10}, \frac{9q^2-68q+519}{10}]$, *there exists a maximal partial spread of the generalised quadrangle* $W(q)$, $q \geq 49$ *odd, of this size.*

4 Minimal Blocking Sets in Odd Order

Here we develop a spectrum of minimal blocking sets with respect to the planes of the 3-dimensional projective space of odd order. In a joint work with L. Storme we achieved a construction of a minimal blocking set for every cardinality between roughly $q^2/4$ and $3q^2/4$. These results have been published in [84]. They are similar to those we found for the projective space of even order in Chapter 2, and again the results translate into isomorphic structures, in particular partial 1-systems on the Klein quadric, what is shown in the last section of this chapter.

Different kinds of minimal blocking sets have been looked for. We mention now the most important results in our context.

Theorem 4.1 (Sziklai, Szőnyi, and Weiner [93, 95, 92]) *Let B be a small minimal blocking set in $PG(3,q)$, $q=p^h$, p prime, $h\geq 1$, with respect to the planes, then B intersects every plane in $1 \pmod p$ points. Let e be the maximal integer for which B intersects every plane in $1 \pmod{p^e}$ points, then e is a divisor of h.*

Here a *small* blocking set in $PG(3,q)$ with respect to the planes of $PG(3,q)$ is a blocking set of cardinality smaller than $3(q+1)/2$. The preceding integer e is called the *exponent* of the small minimal blocking set B.

The following theorem states that the cardinality of a small minimal blocking set can only lie in a number of intervals of small size. This result is originally stated in [34] for small minimal blocking sets in $PG(2,q)$, but [95, Theorem 3.5] shows that we can also formulate this result for small minimal blocking sets with respect to the planes in $PG(3,q)$.

Theorem 4.2 ([34, 95]) *Let B be a small minimal blocking set in $PG(3,q)$, $q=p^h$, p prime, $h\geq 1$, with respect to the planes, intersecting every plane in $1 \pmod{p^e}$ points. If e is the maximal integer for which B intersects every plane in $1 \pmod{p^e}$ points, then*

$$q+1+\frac{q}{p^e+2} \leq |B| \leq q+a_0\frac{q}{p^e}+a_1\frac{q}{p^{2e}}+\cdots+a_{h/e-2}p^e+1,$$

with a_n the n-th Motzkin number,

$$a_n=\frac{1}{n+1}\sum_{i=0}^{n+1}(-1)^i\binom{n+1}{i}\binom{2n+2-2i}{n-i}.$$

The following characterization of small minimal blocking sets with respect to the planes of $PG(3,q)$ by Storme and Weiner [91] points out the role of the exponent e:

Theorem 4.3 *Let B be a small minimal blocking set with respect to the planes of $PG(3,q^3)$, $q=p^h$, p prime, $p\geq 7$, $h\geq 1$. Assume that B has exponent larger than or equal to h, then B is one of the following minimal blocking sets:*

1. *a line,*
2. *a Baer subplane if q is a square,*
3. *a minimal planar blocking set of size q^3+q^2+1 projectively equivalent to the set $\{(1,x,x+x^q+x^{q^2})|x\in\mathbb{F}_{q^3}\}\cup\{(0,0,1)\}$,*
4. *a minimal planar blocking set of size q^3+q^2+q+1 projectively equivalent to the set $\{(1,x,x^q)|x\in\mathbb{F}_{q^3}\}\cup\{(0,0,1)\}$,*
5. *a subgeometry $PG(3,q)$.*

Next to studying large and small minimal blocking sets with respect to planes of $PG(3,q)$, *spectrum* results of minimal blocking sets with respect to planes of $PG(3,q)$ can be considered. We found a spectrum for q even in Chapter 2 and we want to complement this result now with a similar result for q odd. The following spectrum results on minimal blocking sets with respect to the planes of $PG(3,q)$ have been found [45, 94]. In fact, they are spectrum results on minimal blocking sets with respect to the lines of a plane $PG(2,q)$, but when this plane is embedded in $PG(3,q)$, then an equivalent spectrum result on minimal blocking sets with respect to the planes of $PG(3,q)$ is obtained.

Theorem 4.4 (Innamorati and Maturo [45]) *In $PG(2,q)$, $q\geq 4$, for every integer $k\in[2q-1,3q-3]$, there exists a minimal blocking set of size k.*

Theorem 4.5 (Szőnyi *et al* [94]) *In $PG(2,q)$, q square, a minimal blocking set of size k exists for every integer k in the interval $[4q\log q, q\sqrt{q}-q+2\sqrt{q}]$.*

4.1 Setting

We will use some ideas we already valued in Chapter 2 from the article of Szőnyi *et al* [94]. In particular, we will need again the statement introduced by Füredi in [36, p. 190]:

Corollary 4.6 *For a bipartite graph with bipartition $L\cup U$ where the degree of the elements in U is at least d, there is a set $L'\subseteq L$, for which $|L'|\leq|L|\frac{1+\log(|U|)}{d}$, such that any element $u\in U$ is adjacent to at least one element of L'.*

The following setting is crucial for our purposes. We refer to Figure 4.1.

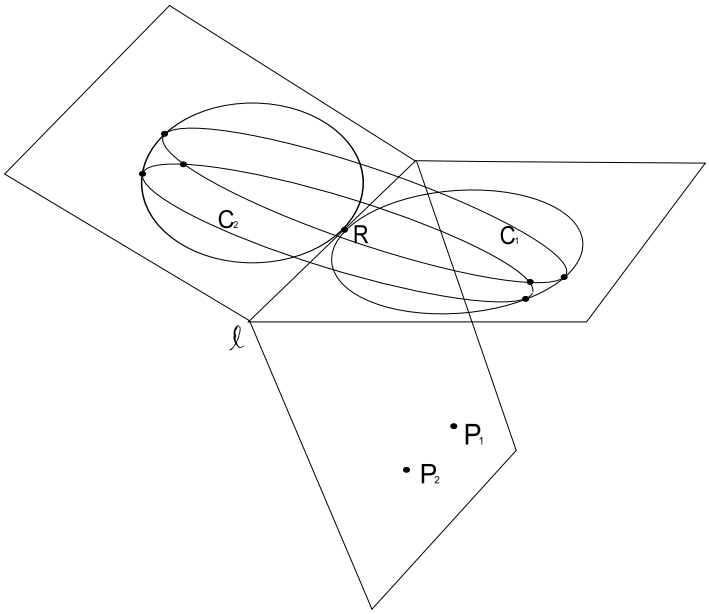

Figure 4.1: Conics of $Q^-(3,q)$ in planes through ℓ

Consider the elliptic quadric $Q^-(3,q): X_0^2 - dX_1^2 + X_2X_3 = 0$, d a non-square, in $PG(3,q)$, q odd. Consider the point $R = (0,0,0,1)$ of $Q^-(3,q)$, then its tangent plane is $T_R(Q^-(3,q)) : X_2 = 0$. Consider the tangent line $\ell : X_0 = X_2 = 0$ to $Q^-(3,q)$ passing through R, then ℓ lies in the secant planes $X_0 = 0$ and $X_0 = X_2$.

There are exactly q planes tangent to the conics $(X_0 = 0) \cap Q^-(3,q)$ and $(X_0 = X_2) \cap Q^-(3,q)$, in points of $Q^-(3,q)$ different from R (Figure 4.2).

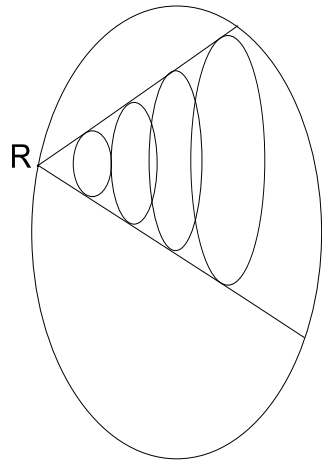

Figure 4.2: Conics of $Q^-(3,q)$, tangent to two secant planes

One of these planes is the plane $X_0 - 2dX_1 + dX_2 + X_3 = 0$, it's tangent to $Q^-(3,q)$ and $X_0 = 0$ in the point $(0,1,1,d)$ and to $Q^-(3,q)$ and $X_0 = X_2$ in the point $(1,1,1,d-1)$.

The other planes tangent to the conics $(X_0 = 0) \cap Q^-(3,q)$ and $(X_0 = X_2) \cap Q^-(3,q)$, in a point of $Q^-(3,q)$, but not R, can be obtained by applying one of the transformations

$$\alpha_c : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & c & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 2cd & dc^2 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

for $c \in \mathbb{F}_q$.

Note that the transformations α_c form an elementary abelian group of order q fixing $Q^-(3,q), R$, and all planes passing through ℓ.

Lemma 4.7 *The q planes which form the orbit of the plane $X_0 - 2dX_1 + dX_2 + X_3 = 0$ under the transformations α_c, $c \in \mathbb{F}_q$, are the only planes tangent to the conics $Q^-(3,q) \cap (X_0 = 0)$ and $Q^-(3,q) \cap (X_0 = X_2)$, in points different from R. The q conics of $Q^-(3,q)$ in these planes are intersected by the same $(q+3)/2$ planes through ℓ. Two of them, $X_0 = 0$ and $X_0 = X_2$, contain exactly one point of each of those q conics, and the other $(q-1)/2$ planes through ℓ contain exactly two points of each of those q conics.*

Every point, different from R, in $Q^-(3,q) \cap (X_0 = 0)$ and in $Q^-(3,q) \cap (X_0 = X_2)$ lies in exactly one of those q conics, and the other points of $Q^-(3,q)$, lying in at least one of those q conics, lie in exactly two of those q conics.

Proof: We first prove that there are exactly q such conics. Each such conic C is uniquely defined by its intersection point with the conic $Q^-(3,q) \cap (X_0 = 0)$. For let P be this tangent point, then the plane of C contains the tangent line to $Q^-(3,q) \cap (X_0 = 0)$ in P; it then also contains the intersection point P' of this tangent line with ℓ. This point P' lies on the tangent line ℓ to the conic $Q^-(3,q) \cap (X_0 = X_2)$ and on one other tangent line ℓ' to the conic $Q^-(3,q) \cap (X_0 = X_2)$. This line ℓ' then determines the plane of C completely.

There are exactly $(q-1)q/2$ points of $Q^-(3,q) \setminus \{R\}$ in the $(q-1)/2$ planes through ℓ intersecting these q conics in two points. Let π be one of the $(q-1)/2$ planes through ℓ intersecting these q conics in two points. The q points, different from R, in $Q^-(3,q) \cap \pi$, form one orbit under the group of transformations α_c, $c \in \mathbb{F}_q$. Assume that the conic C of $Q^-(3,q)$ in the plane $X_0 - 2dX_1 + dX_2 + X_3 = 0$ contains the points P and $\alpha_c(P)$ of $Q^-(3,q) \cap \pi$. Then $\alpha_{c'}(P)$ and $\alpha_{c'+c}(P)$ belong to $\alpha_{c'}(P)$.

But then $\alpha_c(P)$ belongs to $\alpha_c(C)$ and P belongs to $\alpha_{-c}(P)$. So every point P belongs to exactly two of those conics tangent to $X_0 = 0$ and $X_0 = X_2$ in points of $Q^-(3,q) \setminus \{R\}$.

This then accounts for the total $2(q-1)q/2 = (q-1)q$ of the incidences of the q conics tangent to $X_0 = 0$ and $X_0 = X_2$ in the planes different from $X_0 = 0$ and $X_0 = X_2$. □

The polar points of the planes tangent to $Q^-(3,q)$ in a point of $X_0 = 0$ and $X_0 = X_2$, different from R, lie in the plane $2X_0 = X_2$, in which they are the points, different from R, of the conic $\{(1/2, 1+c, 1, d(c+1)^2) | c \in \mathbb{F}_q\} \cup \{R\}$.

We will also need to consider the conic which is the intersection $(2X_0 = X_2) \cap Q^-(3,q)$. This is the conic of the points $\{(1/2, c, 1, dc^2 - 1/4) | c \in \mathbb{F}_q\} \cup \{R\}$.

Lemma 4.8 *A conic of $Q^-(3,q)$, tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$, in points different from R, shares two points with the plane $2X_0=X_2$ if and only if $q\equiv 3 \pmod 4$.*

Proof: By using the elementary abelian group of the transformations α_c, $c\in\mathbb{F}_q$, it is sufficient to check the intersection of the line

$$\begin{cases} X_0-2dX_1+dX_2+X_3 &= 0\\ 2X_0 &= X_2 \end{cases}$$

with $Q^-(3,q)$.
This leads to the quadratic equation $X_2^2(-1-4d)+8dX_1X_2-4dX_1^2=0$ having discriminant $-4d$. This is a square if and only if $q\equiv 3 \pmod 4$. □

The following result is obvious, but we state it explicitly since we will make use of the point $(1,0,0,-1)$ in the construction of the minimal blocking sets with respect to the planes of $PG(3,q)$, q odd.

Lemma 4.9 *The q planes tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$, in points different from R, all pass through the point $(1,0,0,-1)$.*
This point $(1,0,0,-1)$ is the polar point of the plane $2X_0=X_2$ with respect to $Q^-(3,q)$.

Proof: The point $(1,0,0,-1)$ lies in the plane $X_0-2dX_1+dX_2+X_3=0$. Since all transformations α_c, $c\in\mathbb{F}_q$, fix $(1,0,0,-1)$, this point lies in all these q planes tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$, in points different from R. □

4.2 Construction

From the above section, we know that there are exactly q planes tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$, in points different from R. Out of these, we select two conics C_1 and C_2 in such a way that they intersect in two points, not in the plane $2X_0=X_2$, and that the polar points of their planes are not incident with the plane of the other conic. We first prove that this indeed is possible.

Lemma 4.10 *Consider a conic C_1 of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$ in points different from R. Then if $q\equiv 1 \pmod 4$, C_1 intersects the $q-1$ other conics of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$ in points different from R, in zero or two points, and if $q\equiv 3 \pmod 4$, C_1 intersects two of the $q-1$ other conics of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$ in points different from R, in one point, and the $q-3$ other conics of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$, in points different from R, in zero or two points.*

Proof: Let C_1 be the conic of $Q^-(3,q)$ in the plane $X_0-2dX_1+dX_2+X_3=0$. Applying the elementary abelian group acting in one orbit on the q conics of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$, in points different from R, the other conics lie in the planes $X_0+(-2d+2cd)X_1+(-2cd+d+dc^2)X_2+X_3=0$.

To find the intersection with $Q^-(3,q)$ of the intersection line of the planes $X_0-2dX_1+dX_2+X_3=0$ and $X_0+(-2d+2cd)X_1+(-2cd+d+dc^2)X_2+X_3=0$, with $c\neq 0$, the quadratic equation

$$(4d^2c^2-8d^2c-dc^2+4d^2+4cd-4d)X_2^2+(8cd-8d+4)X_2X_3+4X_3^2=0,$$

needs to be solved.

The discriminant of this quadratic equation is equal to $4+4dc^2$ and is zero if and only if $c^2=-1/d$. Since d is a non-square, this has two solutions for c if and only if $q\equiv 3 \pmod 4$. □

We now use the results of Lemma 4.10 to select two conics C_1 and C_2 of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$ in points different from R. These two conics C_1 and C_2 will be used in the construction method which will lead to the non-interrupted interval for the sizes k of the minimal blocking sets with respect to the planes of $\mathrm{PG}(3,q)$ (Corollary 4.12 and Theorem 4.14). In particular, we will select these two conics C_1 and C_2 in such a way that they share two distinct points. This will give us the freedom of a new parameter u which can vary from 0 to 2, helping us to find the non-interrupted spectrum of Theorem 4.14.

So, if one selects C_1, one of the q conics of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$ in points different from R, there are always at least $(q-3)/2$ other conics of $Q^-(3,q)$ tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$ in points different from R, which intersect C_1 in two distinct points. Now the polar points of the q planes tangent to the conics $(X_0=0)\cap Q^-(3,q)$ and $(X_0=X_2)\cap Q^-(3,q)$ are in the plane $2X_0=X_2$ and C_1 shares two points with this plane when $q\equiv 3 \pmod 4$. We impose that the two intersection points of C_1 and C_2 do not lie in the plane $2X_0=X_2$. The motivation is as follows: to get a non-interrupted spectrum, we need to let vary a parameter u, where $0\leq u\leq 2$ (see (4.1)). The parameter u is the number of points in $C_1\cap C_2$ that are not deleted when constructing the new blocking set. So sometimes, they both will not be deleted ($u=2$), sometimes only one of them will be deleted ($u=1$), and sometimes both of them will be deleted ($u=0$). But we always delete the points of $Q^-(3,q)$ in the plane $2X_0=X_2$. So, to be able to let u vary from 0 to 2, we must make sure that none of the points of $C_1\cap C_2$ lies in the plane $2X_0=X_2$. The plane of C_1 intersects the plane $2X_0=X_2$ in a line containing at most two points of $Q^-(3,q)$. If this is the case, they lie on a second conic tangent to $X_0=0$ and $X_0=X_2$, so we need to exclude at most two possibilities for C_2. We also impose that the polar point of C_1 does not lie in the plane of C_2, and vice versa. These polar points lie on a conic in $2X_0=X_2$. So we exclude at most two other possibilities for C_2. We still have at least $\frac{q-11}{2}$ choices for C_2.

We would like to use Corollary 4.6 in order to obtain a spectrum of minimal blocking sets with respect to the planes of $PG(3,q)$, for q odd. Therefore, we need to introduce variables s and r, where s is the number of conics in planes through the tangent line ℓ, which are not replaced by their polar point, and out of these planes there are r which intersect C_1 and C_2 (see Figure 4.3). Thus $q-s$ conics in planes through the line ℓ are replaced by their polar points on the line $X_1=X_2=0$.

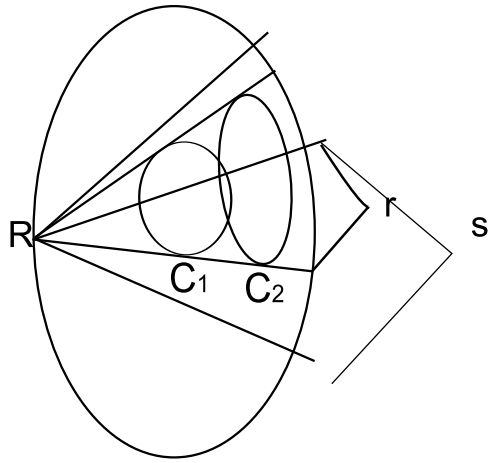

Figure 4.3: Planes through ℓ and their intersection with C_1 and C_2

We leave s conics of $Q^-(3,q)$ in the planes through ℓ in the blocking set of which r intersect C_1 and C_2. For the bipartite graph, we form sets U and L with respect to the tangent line ℓ:
The elements of L are the conics in planes through ℓ except $X_0 = 0$, $X_0 = X_2$, and except those conics in planes through ℓ intersecting the q conics of $Q^-(3,q)$ tangent to $X_0 = 0$ and $X_0 = X_2$. So $|L| = \frac{q-3}{2}$. For the elements of the set U, we use the conics of $Q^-(3,q)$ except those in a plane containing ℓ and the q conics of the quadric $Q^-(3,q)$ tangent to $X_0 = 0$ and $X_0 = X_2$, thus $|U| \leq q^3 - q < q^3$. A lower bound on the degree is given in [90] by $d \geq \frac{q-6-3\sqrt{q}}{4}$. But since we always delete the conic in the plane $2X_0 = X_2$, and this conic belongs to L when $q \equiv 1 \pmod 4$, we decrease the lower bound on d to $d \geq \frac{q-10-3\sqrt{q}}{4}$. We get as a condition for $|L'|$:

$$\begin{aligned} |L'| &\leq \frac{q-3}{2} \cdot \frac{1+\log(q^3)}{\frac{1}{4}(q-10-3\sqrt{q})} \\ &\leq 2 \cdot (1+3\log(q)) \cdot \frac{q-3}{q-10-3\sqrt{q}}. \end{aligned}$$

For $q \geq 47$, $(q-3)/(q-10-3\sqrt{q}) \leq 3$ and we get $|L'| \leq 6 + 18\log(q)$.
The result of Füredi now states that there exists, within the set of $(q-3)/2$ conics of L, a set L' of at most $6+18\log(q)$ conics such that every conic of $Q^-(3,q)$ in U intersects at least one of the conics of L'. In terms of the cardinalities of the minimal blocking sets, this implies the following condition:

$$s - r \geq 6 + 18\log(q).$$

We impose this condition for the following reason: we will not delete the conics of $Q^-(3,q)$ in the set L' in the construction of the new set B, of which we will show that it is a minimal blocking set with respect to the planes of $PG(3,q)$. Then every plane of $PG(3,q)$ intersecting $Q^-(3,q)$ in a conic of the set U intersects at least one of the conics in the set L' in a point. This point is not deleted from $Q^-(3,q)$ to construct the new set B (of which we will show that it is a minimal blocking set with respect to the planes of $PG(3,q)$), thus showing that all the planes intersecting

the elliptic quadric $Q^-(3,q)$ in a conic of the set U are blocked by a point of the newly constructed set B, and thus implying that only a small number of planes of $PG(3,q)$ still need to be verified whether they are blocked by the newly constructed set B (see also the proof of Theorem 4.13).

Altogether, we get the following construction of minimal blocking sets with respect to the planes of $PG(3,q)$, q odd, which will give an uninterrupted interval of sizes k of minimal blocking sets.

Corollary 4.11 *We construct a new minimal blocking set B with respect to the planes of $PG(3,q)$, q odd: First we replace $q-s$ conics of $Q^-(3,q)$ in planes through ℓ by their polar points, assuming that r out of the s remaining conics intersect the tangent conics C_1 and C_2. We always delete the conic of $Q^-(3,q)$ in the plane $2X_0 = X_2$, and replace it by its polar point $(1,0,0,-1)$. We add the point R back. Then we remove C_1 and C_2, and replace both by their polar points P_1 and P_2. The set B has cardinality $k = (s+1)q - s - 4r + u'$, with $3 \le u' \le 9$.*

Proof: The s non-deleted conics of $Q^-(3,q)$ in planes through ℓ, together with the $q-s$ polar points of the $q-s$ deleted conics in planes through ℓ, give a set of $1+(s+1)q-s$ points. We assume that r out of the s non-deleted conics in planes through ℓ intersect C_1 and C_2. Assume that two of these r conics are $X_0 = 0$ and $X_0 = X_2$, which are sharing only one point with C_1 and C_2. Assume that u, with $0 \le u \le 2$, of the two intersection points of C_1 and C_2 lie in one of those r conics. Then these r conics in planes through ℓ contain $(r-2)\cdot 2\cdot 2 + 2\cdot 2 - u$ points of C_1 and C_2. Then, when we delete C_1 and C_2, we delete another $4r-4-u$ points from $Q^-(3,q)$ and add two polar points back. So the new cardinality is

$$1 + (s+1)q - s - (4r-4-u) + 2 = (s+1)q - s - 4r + u + 7, \tag{4.1}$$

with $0 \le u \le 2$.

But we can also let the plane $X_0 = 0$ contain one of the deleted conics, in this case we get as cardinality $(s+1)q - s - 4r + u + 5$, with $0 \le u \le 2$. Next we can also choose to let the planes $X_0 = 0$ and $X_0 = X_2$ contain one of the deleted conics, then we get sizes $(s+1)q - s - 4r + u + 3$, with $0 \le u \le 2$. This all leads to sizes $k = (s+1)q - s - 4r + u'$, with $3 \le u' \le 9$. □

Corollary 4.12 *We need to impose the following constraints:*

1. $4 \le r \le \frac{q-7}{2}$,
2. *if* $s \ge \frac{q-1}{2}$, *then* $r \ge s - \frac{q-3}{2}$,
3. $s - r \ge 6 + 18\log(q)$.

The restrictions follow from the construction above and the application of Corollary 4.6 in the construction. For instance, the condition $r \ge 4$ follows from the fact that, depending on the cardinality desired, the two planes through ℓ containing the two intersection points of C_1 and C_2, and the two planes $X_0 = 0$ and $X_0 = X_2$ are deleted or non-deleted. To make sure that these four planes can be non-deleted, we impose $r \ge 4$. But we always delete the conic in the plane $2X_0 = X_2$, and this conic intersects C_1 and C_2 when $q \equiv 3 \pmod 4$, so when at the same time the two planes through ℓ, containing the two intersection points of C_1 and C_2, and the two planes $X_0 = 0$ and $X_0 = X_2$ are deleted, then $r \le (q-7)/2$, so we also impose $r \le (q-7)/2$.

Theorem 4.13 *The set B is a minimal blocking set with respect to the planes of $PG(3,q)$, q odd.*

Proof: Part 1. We firstly prove that B effectively is a blocking set.

Consider a tangent plane π to the elliptic quadric $Q^-(3,q)$. This tangent plane π either still contains its tangent point R of $Q^-(3,q)$ when R belongs to B, or in case R does not belong to B, then π contains the polar point of the deleted conic C of $Q^-(3,q)$ to which R belongs.

Consider a secant plane π to $Q^-(3,q)$. If π intersects $Q^-(3,q)$ in a conic which is deleted from $Q^-(3,q)$ in the construction of B, then π passes either through R or through $(1,0,0,-1)$, and these points belong to B. If the conic $\pi \cap Q^-(3,q)$ is not deleted from $Q^-(3,q)$ in the construction of B, we only discuss planes π not passing through R since $R \in B$. If the conic $\pi \cap Q^-(3,q)$ is not intersected by the same $(q+3)/2$ planes through $\ell : X_0 = X_2 = 0$ as the conics C_1 and C_2, then by the definition of the set L', the conic $\pi \cap Q^-(3,q)$ shares at least one point with one of the conics in L', and its points belong to B. If the conic $\pi \cap Q^-(3,q)$ is intersected by the same $(q+3)/2$ planes through $\ell : X_0 = X_2 = 0$, then it is one of the q conics tangent to the conics of $Q^-(3,q)$ in $X_0 = 0$ and $X_0 = X_2$. In this case, the plane π passes through $(1,0,0,-1)$, and this point belongs to B.

We have discussed all cases: every plane of $PG(3,q)$ contains at least one point of B.

Part 2. We now show that B is minimal.

We start with the necessity of the point $(1,0,0,-1)$. We selected the two conics C_1 and C_2 so that their planes do not contain the corresponding polar points P_1 and P_2. So, the only point of B that they contain is $(1,0,0,-1)$. This shows the necessity of $(1,0,0,-1)$.

We now show the necessity of a point T of $B \cap Q^-(3,q)$, with $T \neq R$. Then T lies in a plane π through ℓ in which the conic $C = \pi \cap Q^-(3,q)$ is not deleted in the construction of B. Its tangent plane π_T to $Q^-(3,q)$ intersects the line $X_1 = X_2 = 0$ in the polar point $\tilde{T}$ of C. But since C is not deleted, $\tilde{T} \notin B$. Also, P_1 and P_2 do not lie in π_T, or else $T \in C_1$ or $T \in C_2$, but then $T \notin B$. Hence, $\pi_T \cap B = \{T\}$, so T is necessary.

The point R is also necessary in B. Since $r \leq (q-7)/2$, we delete at least five conics in planes through ℓ intersecting C_1 and C_2. For at least one of those planes, R is the only point of B in that plane, so R is necessary. This concludes the necessity of the points of $B \cap Q^-(3,q)$.

We now discuss the necessity of a point T on $X_1 = X_2 = 0$, being the polar point of a deleted conic C of $Q^-(3,q)$ in a plane through ℓ. This point T lies in q tangent planes to $Q^-(3,q)$ in the points of $C \setminus \{R\}$. The only points of B that possibly could belong to these q tangent planes are P_1 and P_2. If they all contain either P_1 or P_2, then, for instance, P_1 belongs to at least $q/2$ of those tangent planes. Consider the line TP_1 and its intersection S with the plane $T^\perp$, then S would belong to at least $q/2$ tangent lines to C in $T^\perp$. This implies $q/2 \leq 2$. Note that this argument also works for the point $T = (1,0,0,-1)$ which is the polar point of the deleted conic of $Q^-(3,q)$ in the plane $2X_0 = X_2$.

Finally, the necessity of the points P_1 and P_2 in B. The point P_1 is the polar point of the conic C_1. Of the s conics in planes through ℓ that are still belonging to B, r of them intersect C_1 and C_2. Consider a tangent plane π, passing through P_1, to $Q^-(3,q)$ in the point P. Suppose that π intersects $X_1 = X_2 = 0$ in T, then $T \in T_P(Q^-(3,q))$ if and only if $P \in T^\perp$, where $T^\perp$ is a plane through ℓ. If T corresponds to one of the r non-deleted conics through ℓ intersecting C_1 and C_2, then $T \notin B$. So this tangent plane contains in this case, besides P_1, at most the point P_2. But if this is the case, then $P \in C_1 \cap C_2$. So this occurs for only two points of C_1. Since we imposed $r \geq 4$, there exists a point $P \in C_1 \setminus C_2$. So P_1 is necessary for B.

We have discussed all the points of B; we have shown that B is a minimal blocking set. □

4.3 Interval Calculation

We know from Corollary 4.11 how to construct a blocking set B and proved in Theorem 4.13 that B is a minimal blocking set with respect to the planes of $PG(3,q)$, q odd. We proceed as follows to find an uninterrupted interval of values k for which a minimal blocking set B of that size k exists in $PG(3,q)$, q odd.

For a given pair (s,r), we can construct minimal blocking sets of sizes $(s+1)q-s-4r+3,\ldots,(s+1)q-s-4r+9$. For given s, the larger r, the smaller the size of a minimal blocking set. To get a large non-interrupted interval we must make sure that for a given value s, the smallest value in the interval of sizes arising from the different values for r for this given value of s, is smaller than or equal to the largest value in the interval of sizes arising from the different values for r for the next value $s'=s-1$.

We first try to get an idea on the maximal possible value for the size of a minimal blocking set in the non-interrupted interval that can be obtained by our arguments.

The largest possible value for r that is allowed is $r=(q-7)/2$. Then the smallest value for the size of the minimal blocking set is $(s+1)q-s-4r+3=(s+1)q-s-2q+17$.

The largest value for the size of the minimal blocking set, for an allowed pair of parameters (s',r') is $(s'+1)q-s'-4r'+9$. For $s'=s-1$, this is the value $sq-s-4r'+10$. We check that

$$sq-s-4r'+10\geq(s+1)q-s-2q+17.$$

This implies that $r'\leq(q-7)/4$.

So we must be able to use the value $r'=(q-7)/4$ for $s'=s-1$.

When $q\equiv 1 \pmod 4$, we always delete the conic in the plane $2X_0=X_2$ which is skew to C_1 and C_2. So we checked $s=(q-3)/2-1+(q-9)/4$, and the values smaller than and larger than this value of s. This shows that $(3q^2-18q+71)/4$ is the maximal value for the non-interrupted interval of sizes for which a minimal blocking set is constructed. This value is obtained for $(s,r)=((q-3)/2-1+(q-5)/4,(q-5)/4)$. For $q\equiv 3 \pmod 4$, we checked the value of $s=(q-3)/2+(q-7)/4$, and the smaller and larger values of s, and found that $(3q^2-12q+57)/4$ is the maximal value of the non-interrupted interval. This value is obtained for $(s,r)=((q-3)/2+(q-3)/4,(q-3)/4)$.

Now we try to get an idea of the minimal possible value for the size of a minimal blocking set in the non-interrupted interval that can be obtained by our arguments. We know that $s-r\geq 6+18\log(q)$. We let $s=r'+6+18\log(q)$. For a given value s, the largest value for the size is obtained for $r'=4$, and is equal to $(s+1)q-s-4r'+9$. For $s=r'+6+18\log(q)$, this gives the value $r'q+7q-r'-13+18(q-1)\log(q)$.

For $r=r'$, the smallest value for the given parameter $s=r'+6+18\log(q)$ is equal to $(s+1)q-s-4r'+3$, and is equal to $r'q+7q-5r'-3+18(q-1)\log(q)$.

For $q\equiv 1 \pmod 4$, we checked the value $s=(q+7)/4+6+18\log(q)$, and the values larger than and smaller than s. This shows that the smallest value of the non-interrupted interval is $(q^2+30q-47)/4+18(q-1)\log(q)$. This value is obtained for $(s,r)=((q+7)/4+6+18\log(q),(q+7)/4)$. For $q\equiv 3 \pmod 4$, we checked the value $s=(q+5)/4+6+18\log(q)$, and the values larger than and smaller than s. This shows that the smallest value of the non-interrupted interval is $(q^2+28q-37)/4+18(q-1)\log(q)$. This value is obtained for $(s,r)=((q+5)/4+6+18\log(q),(q+5)/4)$.

Let's finally summarise the results in the next theorem.

Theorem 4.14 *There exists a minimal blocking set with respect to the planes of* $PG(3,q)$, q *odd,* $q \geq 47$, *for every integer in the following intervals*

1. $[(q^2+30q-47)/4+18(q-1)\log(q),(3q^2-18q+71)/4]$, *when* $q \equiv 1 \pmod 4$,
2. $[(q^2+28q-37)/4+18(q-1)\log(q),(3q^2-12q+57)/4]$, *when* $q \equiv 3 \pmod 4$.

Similarly as in Corollary 2.13 in Chapter 2, the preceding results are equivalent to spectrum results on maximal partial 1-systems of the Klein quadric $Q^+(5,q)$, for odd q.

Corollary 4.15 *For every value belonging to one of the intervals of Theorem 4.14, there exists a maximal partial* 1*-system of that size on the Klein quadric* $Q^+(5,q)$, q *odd.*

5 Subplanes of Inversive Planes

Finite Miquelian inversive planes and their automorphism groups are well studied, e.g. [31]. Their subplanes are known to be closely connected to certain automorphisms, so it is not surprising that their characterisation also reflects on the automorphism group. We will see that at the end of this chapter. We have to restrict this chapter to Miquelian inversive planes as precisely these planes allow an algebraic representation. First B. L. van der Waerden coordinatised these planes in his paper with L. J. Smid [107] from 1935. He used a special case of Miquel's theorem to construct a Pappus configuration in the affine plane.

A new proof was presented in [50, 55], avoiding the intermediate step of coordinatising the internal affine plane. It was motivated by a previous paper by A. Lenard [55] in which the author shows that a certain group of mappings, which are called *Drehstreckungen*, directly induces the field structure. Both proofs are suitable for our purpose and we will dedicate a short paragraph to each. We embark by gathering some known facts on subplanes and constructing an example for a plane-subplane pair.

Definition 5.1 A *subplane* $\mathbb{M}' := (P', C')$ of an inversive plane $\mathbb{M} = (P, C)$ is a substructure, $P' \subseteq P$ and $C' \subseteq C$, where $\mathbb{M}'$ has to satisfy what is called the *subplane condition*:

Any two tangent circles of $\mathbb{M}'$ are also tangent in $\mathbb{M}$.

This subplane condition is essential, it ensures that the parallelism of the affine internal plane is identical to the parallelism of the subplane.

Remark 5.2 We know that a subplane of a Miquelian inversive plane is Miquelian itself. Also M'_P is an affine subplane of M_P, for $P \in \mathbb{M}'$. If m is the order of the plane and m' the order of the subplane then $m'^2 + m' \leq m$ and in the Miquelian case we can even say $m'^3 \leq m$. Furthermore m and m' are either both even or both odd. These results can be found e.g. in [30, 31].

We will later in Theorem 5.9 see, that for a finite inversive plane $\Sigma(K, L)$ with subplane $\Sigma(K', L')$ the *index* of $\Sigma(K', L')$ corresponds to the degree of its field extension $(L : L')$. Taking this beforehand we can now construct the smallest example for a plane-subplane pair.

Example 5.3 The smallest example for an inversive plane possessing a subplane is the (Miquelian) inversive plane $\mathbb{M}$ of order 8 with a subplane $\mathbb{M}'$ of order 2.

We will construct it using the quadratic field extension $L := GF(64)$ over $K := GF(8)$ for $\mathbb{M}$, then we can induce $\mathbb{M}'$ by the quadratic field extension $L' := GF(4)$ over $K' := GF(2)$ (see Figure 5.1). As illustrated in Chapter 1, Theorem 1.25, we obtain $\Sigma = \Sigma(K, L)$ from the projective line $\mathbb{P}(L^2) = \{L(x, y) \mid (x, y) \in L^2 \setminus \{0, 0\}\}$ with $c_0 = \mathbb{P}(K^2)$, and correspondingly $\Sigma' = \Sigma(K', L')$ is $\mathbb{P}(L'^2) = \{L'(x, y) \mid (x, y) \in L'^2 \setminus \{0, 0\}\}$ with $c'_0 = \mathbb{P}(K'^2)$. Now $L'(x, y) \mapsto L(x, y)$ maps the

points of Σ' onto points of Σ and maps the circle c'_0 to c_0. As $PGL(2, L')$ is a subgroup of $PGL(2, L)$, the incidence is preserved.

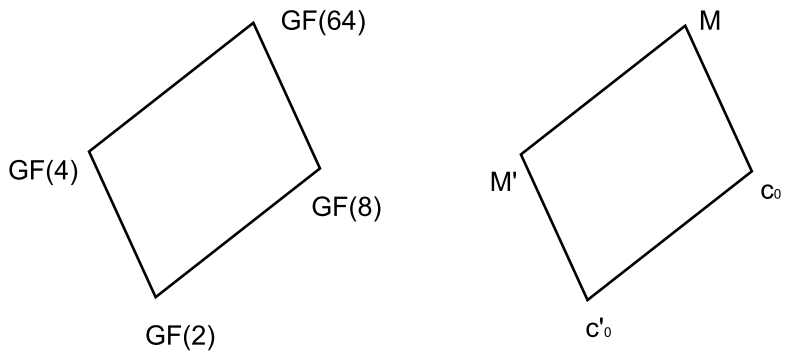

Figure 5.1: Diagram of the construction

More generally: If we look now at the projective line $PG(1, q^2)$ over $GF(q^2)$, we will see that the corresponding inversive plane Σ' of order q is embedded in the inversive plane Σ. Here Σ' is of index 3. Furthermore we will see that the points of a circle of the subplane are induced by the elements of $GF(q)$ and their images under $PG(2, q^2)$. Here $GF(q^6) : GF(q^2)$ is a Galois field extension, meaning there is an automorphism of $GF(q^6)$ fixing $GF(q^2)$ pointwise. This automorphism is of degree 3 and it induces a planar automorphism of Σ fixing Σ' pointwise.

We will now show that the subplanes of a Miquelian inversive plane follow both coordinatisations, using van der Waerden's classical as well as Lenard's newer method, and can be represented by a subfield of the field representing the inversive plane. The results of this chapter were partially published in [82].

5.1 Van der Waerden's Coordinatisation

If we want to assign coordinates to the points of a Miquelian inversive plane, it is reasonable to choose an algebraic representation for the inversive plane. Like in Example 5.3, the projective line turns out to be the most suitable way. For our purposes we will adapt the notation from Chapter 1, Corollary 1.28:

Let $\mathbb{A}(K^2) = (P, G)$ be the affine plane over a field K that allows a quadratic extension, and let $f(x, y) \in K[x, y]$ be an irreducible homogeneous quadratic form (for further details on these forms see [12, Chapter 4.7]). Then the incidence structure $(P \cup \{\infty\}, C)$ with

$$\begin{aligned} C &:= \{g \cup \{\infty\} \mid g \in G\} \cup \{c_{a,b,c} \mid a, b, c \in K\}, \quad \text{where} \\ c_{a,b,c} &:= \{(x, y) \in P \mid f(x, y) + ax + by + c = 0\}, \end{aligned}$$

is a Miquelian inversive plane $\Sigma(K, f) = (P \cup \{\infty\}, C)$.

Remark 5.4 The circles of the Miquelian inversive plane $\Sigma(K, f)$ are determined by the irreducible homogeneous quadratic form (see Corollary 1.28 in Chapter 1) $f(x, y)$. Hence the points

of the circle $c_{a,b,c}$ are the solutions of the quadratic form $f(x,y)+axz+byz+cz^2=0$, where the irreducible homogeneous quadratic form $f(x,y)$ determines the q^3-q^2 circles in $\mathbb{M}_P=\mathbb{A}(K^2)$. We will later, in Definition 5.5, call these circles the *affine circles* of $\mathbb{M}$ in $\mathbb{M}_P$. Thus the choice of $f(x,y)$ implies which inversive plane we obtain. Let's give a short example:

q odd: We choose $f(x,y)=x^2-dy^2$, with d a non-square in $GF(q)$. Together we get $x^2-dy^2+ax+by+c=0$ which leads to the condition $c\neq-\frac{b^2-da^2}{4d}$ for the non-singular conics $c_{a,b,c}$. This condition gives us the q^3-q^2 circles we need.

q even: Let's take $f(x,y)=x^2+xy+dy^2$ where $Tr(d)=1$ and we get $x^2+xy+dy^2+ax+by+c=0$. This homogeneous quadratic form defines non-singular conics if $c\neq b^2+ab+da^2$ and again we find the missing q^3-q^2 circles of $\mathbb{M}$.

If we now say $z=0$ is the line g of infinity, $\mathbb{P}\backslash g=AG(m)$, then the circle $c_{a,b,c}$ intersects g in two points, where $f(x,y)=0$. Let's say $Q=(x_1,y_1)$ satisfies $f(x_1,y_1)=0$, then for $Q'=(x_1^m,y_1^m)$, $f(x_1^m,y_1^m)=0$ holds as well.
This way we can define conjugation as a field automorphism:

$$GF(m^2)\longrightarrow GF(m^2) \text{ where } x\longmapsto x^m.$$

Then we extend it to a mapping on the point set C of $\Sigma(K,f)$:

$$\kappa: C\longrightarrow C \text{ with } (x,y,z)\longmapsto(x^m,y^m,z^m).$$

A pair of points Q,Q' is called a *conjugate point pair* if $Q'=\kappa(Q)$.

Definition 5.5 Let the Desarguesian projective plane $\mathbb{P}=PG(2,q)$ be embedded in $\mathbb{P}^*=PG(2,q^2)$, and let g be a line of $\mathbb{P}$ incident with a pair of conjugate points Q,Q' (see Remark 5.4) in $\mathbb{P}^*$. A conic incident with Q and Q' is as well a conic in $\mathbb{P}$, as it is in the affine plane $\mathbb{P}\setminus g=AG(q)$. These conics are called *affine circles*.

Theorem 5.6 *Let $\mathbb{A}$ be a Pappian affine plane and let $\mathbb{A}'$ be a subplane of $\mathbb{A}$. Then $\mathbb{A}'$ is Pappian as well. Furthermore there exists a field extension $K:K'$ and an isomorphism $\varphi:\mathbb{A}\to\mathbb{A}(K^2)$ which maps $\mathbb{A}'$ to $\mathbb{A}(K'^2)$, as it is canonically embedded in $\mathbb{A}(K^2)$.*

Proof: We would like to give the reader an idea by sketching a line-arithmetics based proof. Therefore we choose a pair of distinct, intersecting lines g_1' and g_2' in $\mathbb{A}'$ as coordinate axes. Their common intersection point is called O, and on each line we choose an additional point E_1 and E_2. During the coordinatisation process, a field K' is constructed together with an isomorphism $\varphi:\mathbb{A}'\to\mathbb{A}(K')$ such that $\varphi(O)=(0,0)$, $\varphi(E_1)=(1,0)$ and $\varphi(E_2)=(0,1)$.
If $\mathbb{A}'$ is now a subplane of the plane $\mathbb{A}$, then the original coordinate axes are restrictions of unique lines g_1 and g_2 in $\mathbb{A}$. The same coordinatisation process, applied to $\mathbb{A}$, yields a field K and an isomorphism $\overline{\varphi}:\mathbb{A}\to\mathbb{A}(K)$. Now the crucial observation is that the set of coordinates of the points of the subplane K' forms a subfield of K. In fact, addition and multiplication in K' are restrictions of the respective operations in K. This stems from the fact that they are both geometrically induced. The respective operations are defined in terms of line intersections and point connections in the respective geometries. Hence, $\overline{\varphi}$ is an extension of φ. □

Definition 5.7 (a) Let $\mathbb{A}$ be an affine plane. A *quadrilateral* is a quadruple $\square = (g_0, g_1, g_2, g_3)$ of lines of $\mathbb{A}$ such that no two are parallel and $|g_i \cap g_{i+1}| = 1$ for all $i = 0, \ldots, 3$, with scripts taken modulo 4.

(b) Two quadrilaterals (g_0, g_1, g_2, g_3) and (h_0, h_1, h_2, h_3) of an affine plane $\mathbb{A}$ are then called *similar* if $g_i \parallel h_i$ for all $i = 0, \ldots, 3$ (and a suitable choice of indices). So corresponding lines of the two quadrilaterals are parallel.

(c) Let $\mathbb{M}$ be an inversive plane, and P one of its points. We say that a quadrilateral (g_0, g_1, g_2, g_3) in $\mathbb{M}_P$ is *circular*, if there is a circle c of $\mathbb{M}$ such that

$$c \cap g_i \;=\; (g_{i-1} \cap g_i) \cup (g_i \cap g_{i+1}) \quad \text{for all } i = 0, \ldots, 3,$$

where all subscripts are taken modulo 4. Thus all four sides of the quadrilateral are chords of the circle.

The following proposition, as well as a detailed description of the special cases, i.e. where one or more sides of the quadrilateral are not chords, but tangents of the circle, can be found in [5, p. 211 ff.].

Proposition 5.8 *Let $\mathbb{M} = (P, C)$ be a Miquelian inversive plane, and let P be one of its points. Let $\square_1$ be a circular quadrilateral of $\mathbb{M}_P$, and let $\square_2$ be a quadrilateral similar to $\square_1$. Then $\square_2$ is circular (see Figure 5.2).*

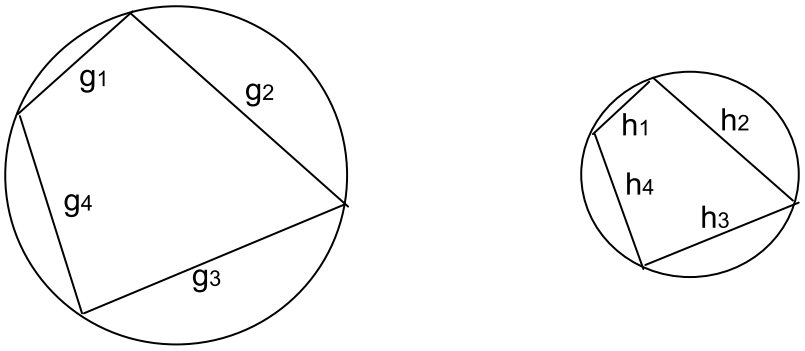

Figure 5.2: Circular quadrilaterals

Van der Waerden used this condition to characterise the affine circles of a Miquelian inversive plane in an affine internal structure, using the regular quadratic form.

Theorem 5.9 (van der Waerden) *For a Miquelian inversive plane $\mathbb{M}$, there exists a field K and an irreducible quadratic form $f(x, y) \in K[x, y]$ such that $\mathbb{M} \cong \Sigma(K, f)$.*

Proof: We will here only outline the well known proof of van der Waerden in order to refer to certain parts later on. He proved firstly that $\mathbb{M}_P$ is a Pappian affine plane for all $P \in \mathbb{M}$. A Pappian affine plane can then be coorinatised by a suitable field K using the isomorphism $\varphi : \mathbb{M}_P \to \mathbb{A}(K^2)$. He then uses Proposition 5.8 for quadrilaterals to find the affine circles. In $\mathbb{A}(K^2)$ the conics are zero sets of a quadratic form

$$px^2 + qxy + ry^2 + sx + ty + u = 0.$$

From the condition we know that every affine circle has a quadrilateral of chords such that the chords are parallel to $a_1x + a_2y + a_3 = 0$, $b_1x + b_2y + b_3 = 0$, $c_1x + c_2y + c_3 = 0$ and $d_1x + d_2y + d_3 = 0$. Thus the following equations are linearly dependent:

$$\begin{gathered} px^2 + qxy + ry^2 + sx + ty + u = 0 \\ (a_1x + a_2y + a_3)(c_1x + c_2y + c_3) = 0 \\ (b_1x + b_2y + b_3)(d_1x + d_2y + d_3) = 0 \end{gathered}$$

Therefore the matrix:

$$\begin{pmatrix} p & q & r & s & t & u \\ a_1c_1 & a_1c_2 + a_2c_1 & a_2c_2 & a_3c_1 + a_1c_3 & a_2c_3 + a_3c_2 & a_3c_3 \\ b_1d_1 & b_1d_2 + b_2d_1 & b_2d_2 & b_3d_1 + b_1d_3 & b_2d_3 + b_3d_2 & b_3d_3 \end{pmatrix}$$

has rank ≤ 2. Thus, the determinant of all its 3×3 submatrices is zero and we can say:

$$\begin{vmatrix} p & q & r \\ a_1c_1 & a_1c_2 + a_2c_1 & a_2c_2 \\ b_1d_1 & b_1d_2 + b_2d_1 & b_2d_2 \end{vmatrix} = 0$$

This equation holds for all kind of chord quadrilaterals of an affine circle. Thus we can fix at least two of the four ratios $a_1 : a_2$, $b_1 : b_2$, $c_1 : c_2$ and $d_1 : d_2$ for convenience. Van der Waerden chose $a_1 = c_1 = 0$ and $a_2 = c_2 = 0$ and obtained the following three equations:

$$\begin{aligned} q \cdot b_1d_1 &= p \cdot (b_1d_2 + b_2d_1) \\ q \cdot b_2d_2 &= r \cdot (b_1d_2 + b_2d_1) \\ p \cdot b_2d_2 &= r \cdot b_1d_1 \end{aligned}$$

with constant ratios $b_1 : b_2$ and $d_1 : d_2$ and the ratios between p, q, r being constant as well. Therefore all affine circles share a common homogeneous quadratic contribution: $f(x, y) \in K(x, y)$ with $f(x, y) = px^2 + qxy + ry^2$. Therefore the isomorphism $\varphi : \mathbb{M}_P \to \mathbb{A}(K^2)$ is extendable to $\varphi : \mathbb{M} \to \Sigma(K, f)$ with $p \mapsto \infty$. □

In order to extend an algebraic representation of a subplane of a Miquelian plane to a representation of the given plane, we need to adapt the methods of the proofs of Theorem 5.6 and Theorem 5.9 to our requirements.

Theorem 5.10 *Let $\mathbb{M}$ be a Miquelian inversive plane and let $\mathbb{M}'$ be a subplane of $\mathbb{M}$. Then there exist a field extension $K : K'$, a homogeneous quadratic form $f(x, y) \in K'[x, y]$ which is irreducible in $K[x, y]$ and an isomorphism $\varphi : \mathbb{M} \to \Sigma(K, f)$ that maps $\mathbb{M}'$ onto $\Sigma'(K', f)$.*

Proof: We choose a point $P \in \mathbb{M}'$ and observe that $\mathbb{M}'_P$ is a Pappian subplane of $\mathbb{M}_P$. Using Proposition 5.6, we can find a field extension $K : K'$ and an isomorphism $\varphi_P : \mathbb{M}_P \to \mathbb{A}(K^2)$ that maps $\mathbb{M}'_P$ onto $\mathbb{A}(K'^2)$. Following the arguments in the proof of Theorem 5.9, we also know that φ maps the circles of $\mathbb{M}'$ onto conics in $\Sigma'(K', f)$ that share a homogeneous quadratic contribution $f(x, y) \in K'(x, y)$. Likewise φ maps the circles of $\mathbb{M}$ to conics of $\mathbb{A}(K^2)$ which share the homogeneous quadratic contribution $g(x, y) \in K(x, y)$. As both f and g are uniquely determined by the algebraic description of a circular quadrilateral in the respective internal structures, we can

choose a circular quadrilateral $\square'$ in $\mathbb{M}'_P$ and use Remark 5.2 to extend it to a unique circular quadrilateral $\square$ of $\mathbb{M}_P$. But this forces g to be a multiple of an element in $K'[x,y]$, and hence, g and f must coincide up to a constant factor. This concludes the proof of the claim. $\square$

Remark 5.11 The foregoing theorem is valid also in the case where the subplane is of order 2. This stems from the fact that the desired quadratic form is still determined by a *degenerated* circular quadrilateral, i.e. a quadrilateral where three of the given sides are confluent or where two (opposite) sides coincide (cf. [5, p. 215, top]). Note that Remark 5.2 stays also valid for degenerated quadrilaterals.

5.2 Lenards' Algebraic Representation

The key idea in the algebraic representation by Lenard [55] is the *4-circle relation* (see Figure 5.3) $V \subset P^6$ where $A_{12}, A_{34}, A_{14}, A_{24}, A_{13}, A_{23}$ are at least 5 different points and $(A_{12}, A_{34}, A_{14}, A_{24}, A_{13}, A_{23}) \in V$ holds iff there are four different circles $k_1, \ldots, k_4 \in C$ and a point $Q \in P$ such that: $k_i \cap k_j = \{A_{ij}, Q\}$ for $1 \leq i < j \leq 4$.

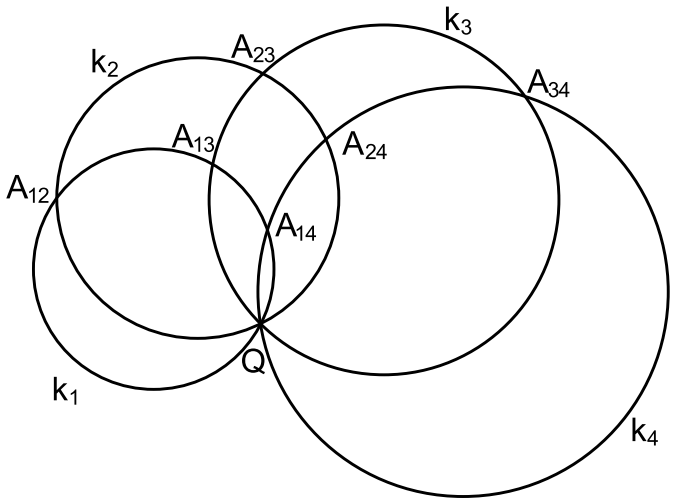

Figure 5.3: 4-circle relation

Lemma 5.12 *Let $A_{12}, A_{34}, A_{14}, A_{24} \in P$ be not incident with one circle. Then for every point $X \in P \setminus \{A_{12}, A_{34}, A_{14}\}$ there exists a unique point $X' \in P$ such that $(A_{12}, A_{34}, A_{14}, A_{24}, X, X') \in V$.*

Proof: This is proven in [50, 55] by constructing the point X'. We set $A_{13} = X$ and the circles $k_1, \ldots, k_4$ as in the definition above. Then X' is the point A_{23}. $\square$

Remark 5.13 Note that X' is unique and well defined: In the general case we get $k_1 \cap k_4 = \{A_{14}, Q\}$, $A_{12}, A_{24}, Q \in k_2$ and $A_{34}, A_{13}, Q \in k_3$ define k_2, k_3 and $k_2 \cap k_3 = \{Q, A_{23}\}$ defines $X' = A_{23}$. In case the intersection point Q is one of the points A_{34}, A_{14}, A_{24}, say $Q = A_{ij}$, the circles k_i and k_j are tangent in Q. Furthermore Q can not be A_{12}, otherwise $A_{12}, A_{34}, A_{14}, A_{24}$

would be concircular. Also no two points of $A_{12}, A_{34}, A_{14}, A_{24}$ can be identical. In the case that $X = A_{24}$, we get $k_1 \cap k_4 = \{A_{14}, X\}$, thus $Q = X$.

Using Lemma 5.12, we define a class $\Delta_{0,\infty}$ of mappings of $\mathbb{M} = (P, C)$ which are used in [50, 55] for the algebraic representation:

Definition 5.14 For chosen points $0, \infty$ of a Miquelian inversive plane $\mathbb{M} = (P, C)$, we define a mapping $\delta_{AA'} \in Aut(\mathbb{M})$ for any two points $A, A' \in P$ with $0, \infty, A, A'$ not concircular:

$$\delta_{AA'} : P \to P : \quad X \mapsto \begin{cases} X' & : \quad X \neq 0, \infty, A \\ 0 & : \quad X = 0 \\ \infty & : \quad X = \infty \\ A' & : \quad X = A \end{cases},$$

where X' is the point uniquely defined by $(0, \infty, A, A', X, X') \in V$ (see Figure 5.4).

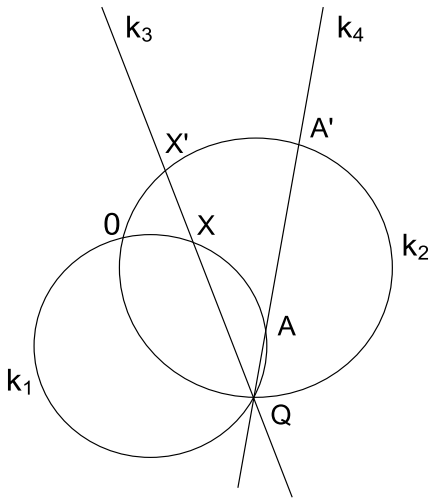

Figure 5.4: $\delta_{A,A'}$ in $\mathbb{M}_\infty$

Following [50, 55] it can be shown that the mappings $\delta_{AA'}$ generate an Abelian group $\Delta_{\infty,0}$ in a Miquelian inversive plane of order ≥ 4 which acts regularly on the points of $P \backslash \{0, \infty\}$. Furthermore there is a subgroup $\Sigma_{\infty,0} \subset \Delta_{\infty,0}$ generated by the products $\delta_{XA'}\delta_{AX}$ (called *Streckungen* in [50, 55]) where $0, \infty, A, X'$ are incident with a circle $c \in C$ and X is any point not incident with c. The restrictions of the mappings $\delta_{XA'}\delta_{AX}$ to the affine plane $\mathbb{M}_\infty$ are dilatations with fixed point 0 mapping A onto A'. Therefore, for any circle $c \in C$, with $0, \infty \in c$, the group $\Sigma_{\infty,0}$ acts regularly on $c \setminus \{0, \infty\}$. Since the dilatations of $\mathbb{M}_\infty$ with different fixed points can be constructed in the same way, it follows that $\mathbb{M}_\infty$ is a translation plane and every translation of $\mathbb{M}_\infty$ is the restriction of an automorphism of $\mathbb{M}$. We can now introduce an addition on the points of $L := P \setminus \{\infty\}$ in the following way (cf. [50, Theorem 1]): for every $A \in L$ there exists exactly one translation A^+ of $\mathbb{M}_\infty$, such that $A^+(0) = A$. We then define $A + B := A^+(B)$. For $0, \infty, A, B$ not incident with one circle, adding A and B leads to a parallelogram in $\mathbb{M}_\infty$ where k_A is the

circle incident with $0, \infty$, and A, k_B the circle through $0, \infty$, and B, k'_A shall be incident with ∞ and B but tangent to k_A in ∞, and likewise k'_B is incident with ∞ and A tangent to k_B in ∞. Then we have $A + B := k'_A \cap k'_B$ as shown in Figure 5.5.

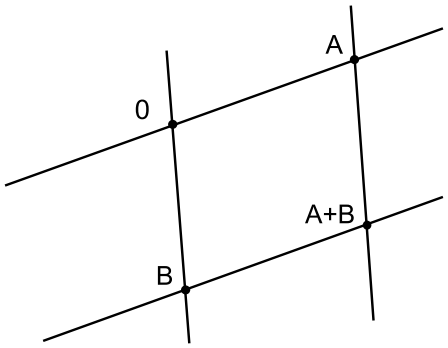

Figure 5.5: $A + B$ in $\mathbb{M}_\infty$

Now, by regularity of $\Delta_{\infty,0}$, there is precisely one $A^\bullet \in \Delta_{\infty,0}$ for every $A \in P \setminus \{0, \infty\}$, such that $A^\bullet(1) = a$ where $1 \in L \setminus \{0\}$. As $A \cdot B := A^\bullet(B)$ for every $A \neq 0$ and $A \cdot B := 0$ otherwise, we can say that this operation defines a multiplication on L. With these operations, L obtains the structure of a field, containing a subfield K with $[L : K] = 2$ induced by the points $X \neq \infty$ of the circle c with $0, 1, \infty \in c$ where $1 \in P \setminus \{0\}$. The projective group $\mathrm{PGL}(2, L)$ is a subgroup of the automorphism group that maps the circle c on all other circles. The above proves in [50, 55] the following theorem:

Theorem 5.15 *Let $\mathbb{M} = (P, C)$ be a Miquelian inversive plane of order ≥ 4, with $0, 1, \infty \in P$ and k the circle incident with $0, 1$, and ∞. For $L := P \setminus \{\infty\}$ and $K := k \setminus \{\infty\}$, there exist an addition $+$ and a multiplication $\cdot$ on L such that $L : K$ is a quadratic field extension and the mapping $\phi : x \mapsto L(x, 1)$ where $x \in L$ and $\infty \mapsto L(1, 0)$ is an isomorphism such that $\phi(\mathbb{M}) = \Sigma(K, L)$.*

Lemma 5.16 *Let $\mathbb{M} = (P, C)$ be a Miquelian inversive plane with a subplane $\mathbb{M}' = (P', C')$ and let $\Delta_{A,A'}$ be the group of mappings from the proof of Theorem 5.15. Then for $0, \infty, A, A' \in P'$, we obtain $\delta_{AA'}(P') = P'$.*

Proof: The mappings $\delta_{AA'}$ generating the group $\Delta_{A,A'}$ are defined in Definition 5.14 using intersections of circles $k_1, \ldots, k_4$. For $0, \infty, A, A', X' \in P'$ we know that $k_1, k_4 \in C'$. The intersection points of $k_1 \cap k_4 = \{A_{14}, Q\}$ are then points of P', because from $A_{14} \in P'$ follows $Q \in P'$ because of the definition of a subplane. Consequently $k_2, k_3 \in C'$ and therefore also the other points of intersection. With $\delta_{AA'}^{-1} = \delta_{A'A}$ we get $\delta_{AA'}(X') \subseteq P'$ and hence $P' \subseteq \delta_{A'A}(X') \subseteq P'$. Thus for $0, \infty, A, A' \in P'$, the mapping $\delta_{AA'}$ preserves precisely the subplane. □

In order to find an algebraic representation of the subplane we need to adapt the methods used in this section, including the mappings from Definition 5.14, to our requirements.

Theorem 5.17 *Let $\mathbb{M} = (P, C)$ be a Miquelian inversive plane and $\mathbb{M}' = (P', C')$ a (proper) subplane. Then there exist two quadratic field extensions $L : K$ and $L' : K'$ with $L' \subset L$ and $K' \subset K$ and an isomorphism $\phi : \mathbb{M} \to \Sigma(K, L)$ such that $\phi(\mathbb{M}') = \Sigma(K', L')$.*

Proof: Since $\mathbb{M}$ has a proper subplane $\mathbb{M}'$, the order of $\mathbb{M}$ is at least 6 (see [31, page 265]). For $0, \infty, 1 \in P' \subset P$ we apply Theorem 5.15 to construct a quadratic field extension $L : K$ and an isomorphism $\phi : \mathbb{M} \to \Sigma(K, L)$ such that $\phi(0) = L(0, 1)$, $\phi(\infty) = L(1, 0)$ and $\phi(1) = L(1, 1)$. Let $L' := P' \setminus \{\infty\}$ and $K' := L' \cap K$. The mappings of the group $\Delta_{\infty,0}$ from the proof of Theorem 5.15 act, because of Lemma 5.16, closed on L', meaning for $A, A' \in P'$ there holds $\delta_{AA'}(X') \in P'$ for $X' \in P'$. Defining $\Delta'_{A,A'}$ as the group generated by the mappings $\delta_{AA'}$ where $A, A' \in P'$, we find $\Delta'_{\infty,0} \subset \Delta_{\infty,0}$ acting regularly on $P' \setminus \{0\}$. Furthermore we know that also $\Delta'_{\infty,0}$ has a subgroup $\Sigma'_{\infty,0} \subset \Sigma_{\infty,0}$. Thus for $0, \infty, 1 \in P'$ the isomorphism ϕ that maps $\mathbb{M}$ onto $\Sigma(K, L)$ maps $\mathbb{M}'$ onto $\Sigma(K', L')$. □

5.3 Subplanes and Planar Automorphisms

We know from Theorem 1.31 in Chapter 1 that the automorphisms in the automorphism group of a Miquelian inversive plane have the form

$$\alpha A : \mathbb{P}(L^2) \to \mathbb{P}(L^2), \quad L(x, y) \mapsto L(x^\alpha, y^\alpha)A,$$

with $A \in \mathrm{PGL}(2, L)$ and a field automorphism α of L such that $K^\alpha = K$. Let's also recall that an automorphism π of $\mathbb{M}$ is called a *planar automorphism* if its set of fixed points contains four non-circular points.

According to [31, p. 268], a planar automorphism fixes precisely the points of a subplane. We will call a subplane *induced by a planar automorphism* if its point set is the set of fixed points of a planar automorphism.

Combining the foregoing theorem with our result in Theorem 5.17, we come to the following conclusion.

Theorem 5.18 *Let $L : K$ be a quadratic field extension, and L' a subfield of L with $K' := L' \cap K \neq K$ such that $K : K'$ is a Galois extension. Then $\Sigma(K', L')$ is a subplane of the inversive plane $\Sigma(K, L)$ which is induced by a planar automorphism.*

Proof: We know that $K : K'$ is a Galois extension and $K' = K \cap L' \subseteq L' \subset L$ as well as $K' \subset K \subset L$. Therefore (cf. Theorem 1.12. [54, p. 266]) $L : L'$ is Galois and $\mathrm{Gal}(L : L') \cong \mathrm{Gal}(K : K')$. Let $i \in L' \setminus K' \subset L \setminus K$, then $K(i)' \subseteq L'$. Also $K' \subset K(i)' \cap K \subset K(i)' \subset L$ and $\mathrm{Gal}(K : K') \simeq \mathrm{Gal}(L : K(i)')$ hence $[L : L'] = [K : K'] = [L : K(i)']$. Now as $K(i)' \subseteq L'$, it follows $K(i)' = L'$ and we get $[L' : K'] = 2$. The same Theorem 1.12. [54, p. 266] states that for $\psi \in \mathrm{Gal}(L : L')$, $\psi \to \psi \mid_K$ is an isomorphism mapping from $\mathrm{Gal}(L : L')$ onto $\mathrm{Gal}(K : K')$. It follows that there is an isomorphism ψ of L with $\psi(j) = j$ for $j \in L'$, $\psi(K) = K$ and $\psi_{K'} = id_{K'}$. Thus $\psi^* : L(x, y) \to L(x^\psi, y^\psi)$ is an automorphism of $\Sigma(K, L)$ that fixes precisely the subplane $\Sigma(K', L')$ pointwise. □

Corollary 5.19 *Every subplane of a finite Miquelian inversive plane is induced by a planar automorphism.*

Proof: By Theorem 5.17 there are quadratic field extensions $L : K$ and $L' : K'$ with $L' \subset L$ but $L' \not\subseteq K$ and $K' = L' \cap K$ such that $\Sigma(K, L)$ is a Miquelian inversive plane with a subplane

$\Sigma(K', L')$. As the inversive planes are finite, the field L is finite and $K : K'$ is a finite Galois extension. Therefore the claim follows directly from Theorem 5.18. □

We can also establish a relationship between subplanes of the same order by Möbius transforms. The following proposition prepares this general result.

Proposition 5.20 *Let L be a quadratic extension of the finite field K, and let $\mathbb{M}$ and $\mathbb{M}'$ be subplanes of the same order in $\Sigma(K, L)$. Then there exists a Möbius transform $A \in \mathrm{PGL}(2, L)$ such that $\mathbb{M}A = \mathbb{M}'$.*

Proof: From Theorems 5.19 and 1.31 we know that $\mathbb{M}$ and $\mathbb{M}'$ are the fixed structures of generalised Möbius transforms of the form αB and $\alpha' B'$ (where α and α' are automorphisms of L, and B and B' are elements of $\mathrm{PGL}(2, L)$). From this we obtain that the subplanes $\mathbb{M}B^{-1}$ and $\mathbb{M}'B'^{-1}$ are fixed structures of α and α', respectively. As these are of the same order, we conclude that α and α' fix subfields of L with the same size. By the finiteness of L it is then clear that these subfields are the same, which shows that $\mathbb{M}B^{-1} = \mathbb{M}'B'^{-1}$. Setting $A := B^{-1}B'$, we obtain $\mathbb{M}A = \mathbb{M}'$. □

Corollary 5.21 *Let L be a quadratic extension of the finite field K, and let $\mathbb{M}$ and $\mathbb{M}'$ be subplanes of the same order in $\Sigma(K, L)$. If $\mathbb{M}$ and $\mathbb{M}'$ have more than two points in common, then they are identical.*

Proof: This follows directly from Proposition 5.20 and the fact that the group of all Möbius transforms acts sharply 3-transitive on the points of $\Sigma(K, L)$. □

We have characterised subplanes using planar automorphisms. The following final statement will complement this characterization.

Theorem 5.22 *Let L be a quadratic extension of the finite field K. All planar automorphisms of the inversive plane $\Sigma(K, L)$ are of the form $B\alpha B^{-1}$, where $B \in \mathrm{PGL}(2, L)$, and $\alpha \in \mathrm{Aut}(L)$.*

Proof: Let π be a planar automorphism of $\Sigma(K, L)$. From Remark 1.30 in Chapter 1 we know that π fixes four points that are not incident with one circle, say p, q, r, and s. Furthermore, by Theorem 1.31, Chapter 1, there is a Möbius transform $A \in \mathrm{PGL}(2, L)$ and an automorphism α of L, such that $\pi = \alpha A$. We may assume that $p = L(1, 0)B$, $q = L(1, 1)B$, $r = L(0, 1)B$ and $s = L(1, x)B$ for $x \in L$ and $B \in \mathrm{PGL}(2, L)$. The automorphism $B\pi B^{-1}$ then fixes the points $L(0, 1)$, $L(1, 1)$, $L(1, 0)$ and $L(1, x)$. As $\pi = \alpha A$, we can rewrite $B\pi B^{-1} = B\alpha AB^{-1} = \alpha\alpha^{-1}B\alpha AB^{-1}$, where we note that $\alpha^{-1}B\alpha AB^{-1}$ is a Möbius transform. Now, clearly α still fixes $L(0, 1)$, $L(1, 1)$, and $L(1, 0)$. As $B\pi B^{-1}$ fixes these points as well, the Möbius transform $\alpha^{-1}B\alpha AB^{-1}$ must fix these points, too. For that reason, $\alpha^{-1}B\alpha AB^{-1} = \mathrm{id}$, and from this we immediately conclude $\pi = \alpha A = B^{-1}\alpha B$. □

6 Blocking Sets in Inversive Planes

In this chapter we investigate blocking intersection sets in inversive planes. Blocking sets, or intersection sets (see Definition 1.16 in Chapter 1) play an important role in contemporary finite geometry. They have extensively been studied in projective planes and other line geometries. Little is known however for circle geometries, like inversive planes. There are cryptographic applications for inversive planes depending on their construction and combinatorial properties, e.g. the size of possible blocking sets. It has been proposed by C. Mitchell and F. Piper [66, 67, 68] for example to use the structure of inversive planes in order to reduce storage requirements for cryptographic key distribution in secure networks. For this application the question of minimal cardinalities of blocking sets is directly related to the security of the underlying network communication. The question here is: how many points of an inversive plane do we need, to have at least one point incident with each circle? Before we find a bound for this cardinality, we will discuss a preceding question: how many circles will be blocked by a d-element set of points that has been constructed successively using a greedy type algorithm? We derive a lower bound for this number and thus obtain an upper bound for the cardinality of a blocking set of smallest size. Defining a coefficient called *greedy index*, we finally give an asymptotic analysis for the blocking capabilities of subplanes of inversive planes. So in this chapter the aim is to construct blocking sets, or sets that intersect as many blocks as possible, of minimal cardinality. The results of this chapter are joint work with M. Greferath and were published in [39].

As a preparation for the study of blocking capabilities of circles, we need to investigate the possible incidences of circles. In particular the circles of a bundle and a flock with the same carrier can intersect in different ways and therefore have different blocking numbers.

6.1 Bundles and Flocks

The intersection between the circles of a bundle and a corresponding flock depends on the order of the inversive plane. Therefore we have to investigate even and odd order planes separately.

In an inversive plane of even order, the following correspondence between the circles of a bundle and a flock with same carrier P and Q is known:

Theorem 6.1 *If there is a flock $\mathbb{S}$ with carrier P, Q in an inversive plane of even order, then the following holds for the circles of $\mathbb{S}$ and the bundle $\mathbb{B}$ with carrier P, Q:*

$$\forall b \in \mathbb{B} \text{ and } \forall s \in \mathbb{S} \text{ there holds } |b \cap s| = 1\,.$$

In other words, we can say that every circle of the flock touches every circle of the bundle, and the other way around (see Figure 6.1). The proof can be found in [10].

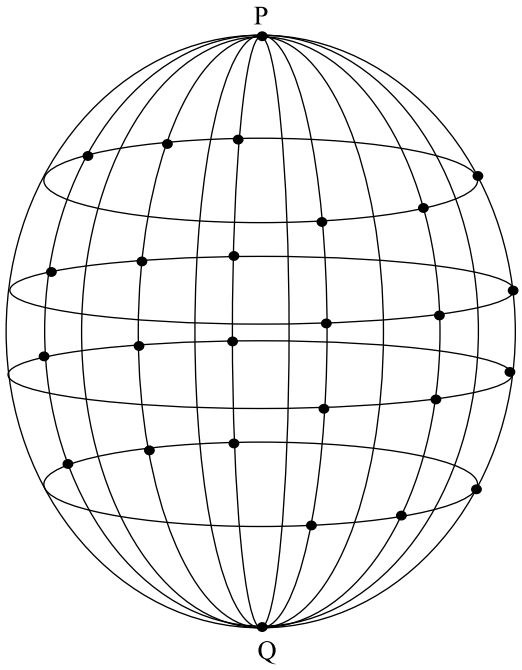

Figure 6.1: Bundle-flock configuration in even order

We now want to find a similar correspondence for inversive planes of odd order. First we need the Theorem of Bruck, which is based on inversive planes $\Sigma(K, L)$ constructed over the projective line (see Chapter 1, Theorem 1.25).

Theorem 6.2 *(Theorem of Bruck) Let $\mathbb{M} := \Sigma(K, L)$ be a Miquelian inversive plane of order m, $m > 2$, $\mathbb{B}$ a bundle with carrier P, Q, and $\mathbb{F}$ the set of all circles such that the inversion (see Chapter 1, Remark 1.30) on one of the circles maps P upon Q. Now let H be the subgroup of $Aut(\mathbb{M})$ (or more precisely $PGL(2, L)$, see Theorem 1.31 in Chapter 1) which maps $\mathbb{F}$ onto $\mathbb{F}$. Let the inversions on the circles of $\mathbb{F}$ form a subgroup $S \subseteq H$ and let the inversions on the circles of $\mathbb{B}$ similarly form the subgroup $B \subseteq H$. Then the following hold:*

1. *$\mathbb{F}$ is a flock, so we call the set $\mathbb{S}$,*
2. *$|H| = 4 \cdot (m^2 - 1)$, $|B| = 2 \cdot (m + 1)$ and $|S| = 2 \cdot (m - 1)$,*
3. *S and B are normal in H and $S \circ B$ has index 1 in H if m is even and index 2 for m odd. Furthermore every element of S commutes with every element of B,*
4. *B consists of all collineations (see again Remark 1.30 in Chapter 1) in H which fix every circle of $\mathbb{S}$ and B contains a cyclic normal subgroup of order $m + 1$, index 2 which acts transitively on the points of every circle in $\mathbb{S}$,*

5. *H/B has order $2(m-1)$ and acts isomorphically on the $m-1$ circles of $\mathbb{S}$ according to the group of permutations: $s_i \mapsto s_{i+t}\ \forall i \pmod{m-1}$ where $s = \pm 1$, with s_i referring to a suitable numbering on the circles of $\mathbb{S}$ and t a positive integer taken $\pmod{m-1}$.*

6. *S induces on the circles of $\mathbb{S}$ the permutations with t even.*

This is Theorem 7.5 in [18, page 456].

The following theorem gives a similar result for inversive planes of odd order. It is not surprising, that the circles here are either intersecting or disjoint. We will show that half of the circles of the bundle intersect with half of the circles of the flock, conversely half of the circles of the bundle avoid half of the circles of the flock. We can think of two separate nets, of incident bundle and flock circles as shown in Figure 6.2:

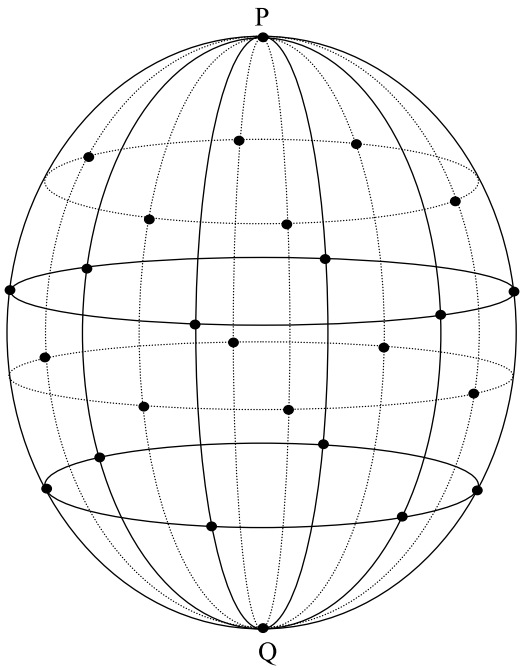

Figure 6.2: Bundle-flock configuration in odd order

Theorem 6.3 *For an inversive plane $\mathbb{M} := \Sigma(K, L)$ of odd order m, let $\mathbb{B}$ be a bundle and $\mathbb{S}$ a flock with carrier P, Q. Then there exists a partition $\mathbb{B}_e, \mathbb{B}_o$ of $\mathbb{B}$ and $\mathbb{S}_e, \mathbb{S}_o$ of $\mathbb{S}$ where $|\mathbb{B}_e| = |\mathbb{B}_o|$ and $|\mathbb{S}_e| = |\mathbb{S}_o|$ satisfying the following property:*

$$\forall b \in \mathbb{B}_e, s \in \mathbb{S}_e : |b \cap s| = 2 \; and \forall b \in \mathbb{B}_o, s \in \mathbb{S}_o : |b \cap s| = 2.$$

Conversely,

$$\forall b \in \mathbb{B}_e, s \in \mathbb{S}_o : b \cap s = \emptyset \; and \forall b \in \mathbb{B}_o, s \in \mathbb{S}_e : b \cap s = \emptyset.$$

Proof: We start this proof by showing that the circles of $\mathbb{B}$ and $\mathbb{S}$ can not be tangent:

The order of $\mathbb{M}$ is the same as the order of the affine internal structure $\mathbb{M}_P$ (see Chapter 1, Definition 1.18), thus odd. As P is a carrier, we know that the circles of $\mathbb{B}$ are the lines intersecting

with Q, while the circles of $\mathbb{S}$ are affine circles (see Chapter 5, Definition 5.5). Because the order is odd we know that in $\mathbb{M}_P$ there are either two or no tangents of a circle $\mathbb{S}$ incident with Q (see Chapter 1, Theorem 1.9). Thus if a circle of $\mathbb{S}$ would have a tangent circle, there would be another circle tangent in $\mathbb{B}$. Let's assume that there are two circles in $\mathbb{B}$ touching a circle $s \in \mathbb{S}$, let's say at points S_1, S_2. Using part *6.* of Bruck's Theorem 6.2, there would be an inversion mapping S_1 not onto S_2 but fixing $\mathbb{S}$ pointwise. Then this inversion would map a circle of $\mathbb{B}$ tangent to s onto a circle of $\mathbb{B}$ intersecting s, which is a contradiction. Thus the point Q is in $\mathbb{M}_P$ an inner point of every circle of $\mathbb{S}$ (see Figure 6.3). (Remark: For even order Q is the nucleus.)

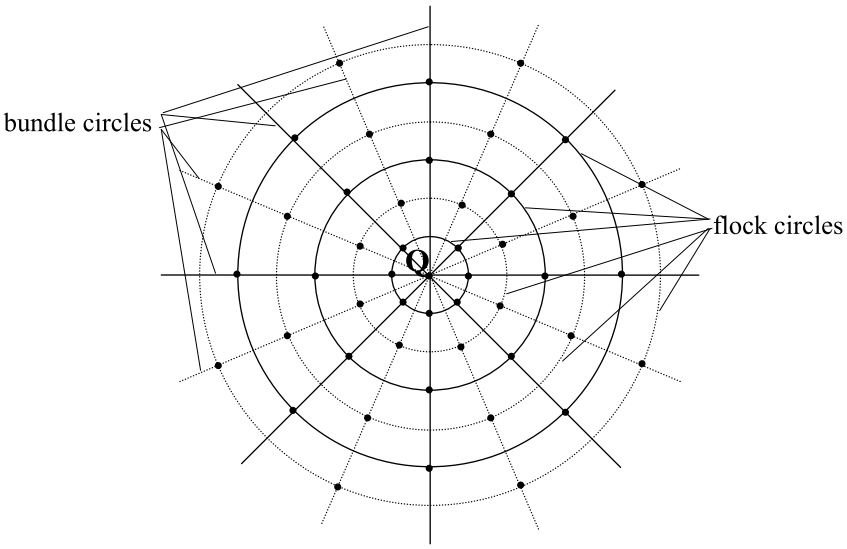

Figure 6.3: Inner point of a flock

We now have to find a partition on the bundle and flock circles into two classes each, such that the incidence between a class of the circles of the flock and one of the circles of the bundle is the same for all circles in either class. Depending on the choice, all circles will then intersect or avoid each other.

Let $b_1, \ldots, b_{m+1}$ be a numbering on the circles of $\mathbb{B}$ such that

$$B_e := \{b_i \mid i \text{ is even}\} \text{ and } B_o := \{b_i \mid i \text{ is odd}\}, i = 1, \ldots, m+1$$

and accordingly let $s_1, \ldots, s_{m-1} \in \mathbb{S}$ be a numbering of $\mathbb{S}$ with

$$S_e := \{s_i \mid i \text{ is even}\} \text{ and } S_o := \{s_i \mid i \text{ is odd}\}, i = 1, \ldots, m-1.$$

Then we have to show that

$$|b \cap s| = 2 \text{ for } b \in B_e \text{ and } s \in S_e, \text{ or } b \in B_o \text{ and } s \in S_o$$

and vice versa

$$|b \cap s| = 0 \text{ for } b \in B_o \text{ and } s \in S_e, \text{ or } b \in B_e \text{ and } s \in S_o.$$

From the definition we know that $|S_e| = |S_o| = \frac{1}{2}(m-1)$ and $|B_e| = |B_o| = \frac{1}{2}(m+1)$, and we know from part *6.* of Bruck's Theorem 6.2 that the inversions in S induce even order permutations

of the circles of $\mathbb{S}$. Thus we can find a numbering $s_1, \ldots, s_{m-1}$ for the circles such that S_e and S_o are invariant. Furthermore we know that S fixes the circles of the bundle, thus it leaves also B_e and B_o invariant.

S operates transitively on S_e and S_o respectively. So let's now look at the orbit of the intersection points under S: For two circles $b_i \in B_e, s_i \in S_e$ we have two points of intersection $b_i \cap s_i$. These points are mapped by S onto the points where b_i intersects the other circles of S_e. Thus we get $2 \cdot \frac{1}{2}(m-1)$ points. If we now include the carrier P, Q, we have all points of the circle b_i. Thus circles of B_e can only intersect with circles of S_e. Conversely circles of B_o can only intersect circles of S_o.

We also know that a circle $s_i \in S_e$ intersects all $\frac{1}{2}(m+1)$ circles of B_e (see again Bruck's Theorem 6.2 part *6.*). Therefore s_i is disjoint to B_o, and also S_o to B_e. Accordingly is $\mathbb{B}_e, \mathbb{B}_o$ and $\mathbb{S}_e, \mathbb{S}_o$ the wanted partition. □

Next we can count the number of circles incident with two circles of a flock. This number depends on whether the order is even or odd.

Corollary 6.4 *In an inversive plane of even order m, $m > 2$, two circles s_1, s_2 of a flock are incident with $\frac{1}{4} \cdot (m^3 + 5m^2 + 8m + 4)$ circles.*

Proof: We have to distinguish between the following possibilities of incidence:

$$\begin{aligned} a_{11} &= |\{k : |k \cap s_1| = 1, |k \cap s_2| = 1\}|, \\ a_{12} &= |\{k : |k \cap s_1| = 1, |k \cap s_2| = 2\}|, \\ a_{21} &= |\{k : |k \cap s_1| = 2, |k \cap s_2| = 1\}|, \\ a_{22} &= |\{k : |k \cap s_1| = 2, |k \cap s_2| = 2\}|. \end{aligned}$$

We first calculate the number of circles touching s_1 and s_2. This can be easily done in the affine internal structure taken in a point of s_1. Here s_1 is a line and s_2 an affine circle (see Chapter 5, Definition 5.5). By Theorem 1.9 we know that there is precisely one tangent of s_2 parallel to s_1. This holds for every point of s_1 we use to get the internal structure. Thus we get $a_{11} = m + 1$ and from Theorem 6.1 follows that these are the circles of the bundle with the same carrier as the flock of s_1, s_2.

If we stay in the affine plane, we see that the other lines parallel to s_1 are either secants of s_2 or do not intersect. There are $\frac{1}{2} \cdot m$ lines intersecting s_2, thus they need to be counted in a_{12}. Again we get different lines for each internal structure taken in a point of s_1. Therefore $a_{12} = \frac{1}{2} \cdot m(m+1)$ and because of symmetry we have the same cardinality for a_{21}.

The case where both circles are intersected in two points is left. We will use double counting to find this cardinality: The number of circles incident with a point on s_1 and a point on s_2 multiplied by the number of possible pairs of points (where one point is incident with s_1 and the other with s_2) is equivalent to the number of circles incident with s_1 and s_2 multiplied by the number of intersection points.

We know that the number of circles incident with two points is $m + 1$ so we get the following equation:

$$(m+1)^2 \cdot (m+1) = 1 \cdot a_{11} + 2 \cdot a_{12} + 2 \cdot a_{21} + 4 \cdot a_{22}.$$

Together with our preceding results we derive a_{22}:

$$\begin{aligned}(m+1)^3 &= m+1+2\frac{1}{2}m(m+1)+2\frac{1}{2}m(m+1)+4a_{22}\\ a_{22} &= \frac{1}{4}m^2(m+1).\end{aligned}$$

Now we can sum up the different types of circles intersecting s_1 and s_2:

$$\begin{aligned}\sum_{i,j=1}^{2} a_{ij} &= m+1+\frac{1}{2}m(m+1)+\frac{1}{2}m(m+1)+\frac{1}{4}m^2(m+1)\\ &= (m+1)(\frac{1}{4}m^2+m+1)\\ &= \frac{1}{4}(m^3+5m^2+8m+4).\end{aligned}$$

□

Similarly we get the following result for inversive planes of odd order.

Corollary 6.5 *Let s_1, s_2 be two circles of a flock $\mathbb{S}$ in an inversive plane of odd order m, and let $\mathbb{S}_e, \mathbb{S}_o$ be a partition of $\mathbb{S}$ in the sense of Theorem 6.3. Then the number of circles intersecting with both $\mathbb{S}_e$ and $\mathbb{S}_o$ depends on the choice of s_1 and s_2:*
For s_1, s_2 both in S_e or S_o we have $\frac{1}{4}(m^3+5m^2+7m+3)$ such circles.
For $s_1 \in S_o$ and $s_2 \in S_e$ or vice versa $s_1 \in S_e$ and $s_2 \in S_o$, there are $\frac{1}{4}(m^3+5m^2+9m+5)$ circles incident with s_1 and s_2.

Proof: The proof uses the same approach as in the foregoing Corollary 6.4, therefore we use the same notation. In the affine internal structure taken in a point of s_1 we see again a line s_1 and an affine circle s_2. An oval, so in particular an affine circle, has either two or no tangent lines out of a parallel class (according to Chapter 1, Theorem 1.9) when the order is odd. Thus for every point of s_1 there are either two circles tangent to s_2 or none. At the end of this proof we will see that only one or the other is possible, but no mixture. Up to then we have to treat both possibilities as ultra.

Case 1. Let's assume that every point of s_1 is incident with two circles which are tangent to s_1 and s_2. Then we would get:

$$a_{11} = 2 \cdot (m+1).$$

Consequently we would know for the cardinality a_{12} that the other $m-1$ points of s_2 are intersecting with circles touching s_1 and intersecting s_2 in two points:

$$a_{12} = a_{21} = (m+1)\frac{1}{2}(m-1).$$

With the same double counting we used in Theorem 6.4, we derive a_{22}:

$$\begin{aligned}(m+1)^3 &= 2(m+1)+2\frac{1}{2}(m-1)(m+1)+2\frac{1}{2}(m-1)(m+1)+4a_{22}\\ a_{22} &= \frac{1}{4}(m+1)(m^2+1).\end{aligned}$$

And get as number of intersecting circles:

$$\begin{aligned}\sum_{i,j=1}^{2} a_{ij} &= 2(m+1)+\frac{1}{2}(m-1)(m+1)+\frac{1}{2}(m-1)(m+1)+\frac{1}{4}(m+1)(m^2+1)\\ &= (m+1)(\frac{1}{4}m^2+m+\frac{5}{4})\\ &= \frac{1}{4}(m^3+5m^2+9m+5).\end{aligned}$$

Case 2. We now assume the least possible number of intersecting circles. Thus no point of s_1 is incident with a circle that is tangent to s_1 and s_2. Here we get:

$$a_{11}=0.$$

For a_{12} we then know that all circles tangent to s_1 intersect s_2 in two points:

$$a_{12}=a_{21}=(m+1)\frac{1}{2}(m+1).$$

With a double counting principle like in Theorem 6.4 we obtain a_{22}:

$$\begin{aligned}(m+1)^3 &= 0+2\frac{1}{2}(m+1)^2+2\frac{1}{2}(m+1)^2+4a_{22}\\ a_{22} &= \frac{1}{4}(m+1)^2(m-1).\end{aligned}$$

Here the number of circles incident with s_1 and s_2 is:

$$\begin{aligned}\sum_{i,j=1}^{2} a_{ij} &= 0+\frac{1}{2}(m+1)^2+\frac{1}{2}(m+1)^2+\frac{1}{4}(m+1)^2(m-1)\\ &= (m+1)^2\frac{1}{4}(m+3)\\ &= \frac{1}{4}(m^3+5m^2+7m+3).\end{aligned}$$

Finally we have to show why precisely these two cases can occur, but no mixture. For this observation we look at the difference of the two cardinalities:

$$\frac{1}{4}(m^3+5m^2+9m+5)-\frac{1}{4}(m^3+5m^2+7m+3) = \frac{1}{2}(m+1).$$

So $\frac{1}{2}(m+1)$ makes this difference, but with Theorem 6.3 we know exactly which ones these circles are.

If the circles s_1 and s_2 are in the same partition, meaning $s_1,s_2\in S_o$ or $s_1,s_2\in S_e$, we know that they are intersecting with the circles of only one partition class of the bundle that has the same carrier as the flock containing s_1 and s_2. These are $\frac{1}{2}(m+1)$ circles. If we have one circle out of each of the two classes, $s_1\in S_o, s_2\in S_e$ or $s_1\in S_e, s_2\in S_o$, then s_1 and s_2 intersect all circles of the bundle. Thus we know that the number of intersecting circles is either $\frac{1}{4}(m^3+5m^2+7m+3)$ or $\frac{1}{4}(m^3+5m^2+9m+5)$, but not in between. □

6.2 Blocking Efficiency

Different point sets, even with the same cardinality, can intersect with different numbers of circles. We are interested in point sets of small cardinality intersecting with all, or almost all circles. We say that the points *block* these circles. At the end of this chapter we want to be able to compare different point sets regarding their ability to block as many circles as possible. In order to do so, we will now investigate different sets, such as points on circles, points of a subplane or points which are spread throughout the plane and then compare the number of circles they block. We call this number the *blocking number* of the point set.

Definition 6.6 For a set D of points in an incidence structure we call the number of blocks that are incident with at least one point of D the *blocking number* of D, and write $b(D)$.

Examples 6.7 1. In an inversive plane of order m, we know from Theorem 1.21 in Chapter 1 the blocking number of one, two and three points:

- $b(P_1) = m(m+1)$,
- $b(P_1, P_2) = 2m(m+1) - (m+1) = 2m^2 + m - 1$ and
- $b(P_1, P_2, P_3) = 3m(m+1) - 3(m+1) + 1 = 3m^2 - 2$.

2. The blocking number of the points on a circle of the inversive plane is:

$$\begin{aligned} b(k) &= (m+1)(b(P \in k) - 1) - \binom{m+1}{2}(b(P_1, P_2) - 1) + 1 \\ &= (m+1)(m(m+1) - 1) - \binom{m+1}{2}m + 1 = \frac{1}{2}m^2(m+3). \end{aligned}$$

We can also find the number of circles blocked by the points of two circles, but the exact number already depends on whether the two circles are intersecting and also on the order of the inversive plane.

Corollary 6.8 *In an inversive plane of order m, $m \geq 3$, let k_1, k_2 be two circles of a flock. Then the number of circles blocked by the points of $k_1 \cup k_2$ is:*

$$b(k_1 \cup k_2) = \begin{cases} \frac{1}{4}(3m^3 + 7m^2 - 8m - 4), & \text{if } m \text{ is even;} \\ \frac{1}{4}(3m^3 + 7m^2 - 9m - 5) & \text{or} \\ \frac{1}{4}(3m^3 + 7m^2 - 7m - 3), & \text{if } m \text{ is odd.} \end{cases}$$

Proof: For even m, we know from Corollary 6.4 the number of circles that are incident with both k_1 and k_2. Thus we can count the total number of circles as:

$$\begin{aligned} b(k_1 \cup k_2) &= b(k_1) + b(k_2) - b(k_1 \cap k_2) \\ &= m^2(m+3) - \frac{1}{4} \cdot (m^3 + 5m^2 + 8m + 4) \\ &= \frac{3}{4}m^3 + \frac{7}{4}m^2 - 2m + 2. \end{aligned}$$

If m is odd, Corollary 6.5 states that we have two possibilities depending on the choice of k_1 and k_2. Hence we get two slightly different blocking numbers:

$$\begin{aligned} b(k_1 \cup k_2) &= b(k_1) + b(k_2) - b(k_1 \cap k_2) \\ &= m^2(m+3) - \frac{1}{4} \cdot (m^3 + 5m^2 + 9m - 5) \\ &= \frac{1}{4}(3m^3 + 7m^2 - 9m - 5), \text{ or} \\ b(k_1 \cup k_2) &= b(k_1) + b(k_2) - b(k_1 \cap k_2) \\ &= m^2(m+3) - \frac{1}{4} \cdot (m^3 + 5m^2 + 7m - 3) \\ &= \frac{1}{4}(3m^3 + 7m^2 - 7m - 3). \end{aligned}$$

□

Another attempt would be to spread out points in such a way that not more than three are incident with a common circle. Of course, the existence of such a set, depending on the cardinality, is a different question.

Corollary 6.9 *Let $\mathbb{U}$ be a set of points of an inversive plane $\mathbb{M}$ of order m with the property that no four points are concircular. For such a set $\mathbb{U}$, with $|\mathbb{U}| = n$, the blocking number would be:*

$$b(\mathbb{U}) = n \cdot m(m+1) - \binom{n}{2}(m+1) + \binom{n}{3}.$$

Proof: For the calculation of $b(\mathbb{U})$, we only have to use the blocking numbers of one, two and three points from the Examples 6.7. □

An example for such a set can be found via the correspondence between generalised quadrangles and inversive planes. If we take a hyperbolic line in a generalised quadrangle then we obtain in the inversive plane a set of points such that no four points are concircular.

Corollary 6.10 *The points of a hyperbolic line (see Chapter 1 in Section 1.2, Definition 1.13) of the generalised quadrangle $W(q)$ (see Chapter 1 in Section 1.2, Examples 1.12) correspond to a set of $q+1$ points in the inversive plane of order q such that no four of these points are concircular.*

Proof: From Definition 1.13 in Chapter 1, Section 1.2, we know that the hyperbolic line of two points x, y, which are not collinear, is defined as $\{x,y\}^{\perp\perp} = \{u \in \mathbb{P} \mid u \in z^{\perp}, \forall z \in x^{\perp} \cap y^{\perp}\}$. □

Recalling Theorem 1.21 of Chapter 1, we know that $\mathbb{M}$ has $m(m^2+1)$ circles and that every point is incident with $m(m+1)$ of them. Thus the upper bound for $n = |\mathbb{U}|$ is:

$$n \leq \frac{3 \cdot m(m^2+1)}{m(m+1)} = \frac{3(m^2+1)}{(m+1)} \leq 3m - 2.$$

Proposition 6.11 *Let $\mathbb{M}'$ be a subplane of order m' (see Definition 5.1 in Chapter 5) of the inversive plane $\mathbb{M}$ of order m. Then the number of circles blocked by the subplane is:*

$$b(\mathbb{M}') = (m'^2+1)\,(m^2 + m - \frac{1}{2}m^2\,m' + \frac{1}{2}m'^3 - m'^2).$$

Proof: For the blocking number of a subplane, we have to distinguish between circles of the subplane, circles intersecting the subplane, and circles tangent to the subplane. The subplane has $m' \cdot (m'^2 + 1)$ circles. For the number of intersecting and tangent circles, we look at the affine internal structure taken in any point P of the subplane (see Definition 1.18 in Chapter 1). Then $\mathbb{M}'_P$ is an affine subplane of $\mathbb{M}_P$ (see [31]).

The lines tangent to the affine subplane are the circles intersecting $\mathbb{M}'$ in P and in one other point. But all lines that are not lines of the subplane can only be tangent, as they are already intersecting the subplane in two points. Thus every point of $\mathbb{M}'_P$ has $m - m'$ tangent lines. Every point of the affine subplane is incident with $m'^2 \cdot (m - m')$ tangent lines. So we get a number of $\frac{1}{2} \cdot (m'^2 + 1) \cdot m'^2 \cdot (m - m')$ circles that are incident with $\mathbb{M}'$ in two points.

The circles touching the subplane in P are the lines in $\mathbb{M}_P$ not intersecting with $\mathbb{M}'_P$. These lines are neither lines of $\mathbb{M}'_P$, nor tangent to $\mathbb{M}'_P$. Their number is therefore: $(m^2 + m) - (m'^2 + m') - m'^2(m - m') = m^2 + m - m'^2 m + m'^3 - m'^2 - m'$. The number of circles that are tangent to $\mathbb{M}'$ is then $(m'^2 + 1) \cdot (m^2 + m - m'^2 m + m'^3 - m'^2 - m')$. Together we get the blocking number of a subplane:

$$\begin{aligned} b(\mathbb{M}') &= m'\,(m'^2 + 1) + \frac{1}{2}(m'^2 + 1)m'^2(m - m') + (m'^2 + 1)(m^2 + m - m\,m'^2 + m'^3 - m'^2 - m') \\ &= (m'^2 + 1)\,(m^2 + m - \frac{1}{2}m\,m'^2 + \frac{1}{2}m'^3 - m'^2). \end{aligned}$$

□

6.3 Cardinality of a Blocking Set

In order to find a lower bound for the cardinality of a blocking set, we look first of all for a lower bound for the maximal blocking number that can be achieved by a set of given cardinality.

From the last paragraph we know examples of blocking numbers for certain point sets. Here we will now show that for a chosen cardinality there exists a set of points which blocks at least a certain number of points. Knowing that this blocking number can be achieved, we can then derive a bound for the cardinality of a blocking set.

Theorem 6.12 *In an inversive plane $\mathbb{M} = (P, C)$ of order m, for every d with $0 \leq d \leq m^2 + 1$, there exists a d-element set D of points such that*

$$b(D) \;\geq\; m\,(m^2 + 1)\left(1 - \frac{\binom{m^2+1-d}{m+1}}{\binom{m^2+1}{m+1}}\right).$$

Proof: We will inductively construct the desired point set D for given d and first observe that our claim obviously holds for $d = 0$ and $D = \emptyset$. If D is a d-element set of points satisfying our claim, and if $d < m^2 + 1$, then there is a point P not contained in D that is contained in at most

$$\frac{b(D)\,(m + 1) - d\,m\,(m + 1)}{m^2 + 1 - d}$$

circles which are already blocked by D. This results from the double counting of the set of pairs

$$Q_D \;:=\; \{(P, c) \in P \times C \mid c \cap D \neq \emptyset\}.$$

On the one hand, the cardinality of this set is obviously given by $(m+1)\,b(D)$. On the other hand, we have

$$|Q_D| \;=\; d\,m\,(m+1) + \sum_{P \notin D} |\{c \in C \mid P \in c \text{ and } c \cap D \neq \emptyset\}|.$$

So, the number of pairs on the right hand side of the last expression, averaged over the points outside of D, is given by

$$\frac{1}{m^2+1-d} \sum_{P \notin D} |\{c \in C \mid P \in c \text{ and } c \cap D \neq \emptyset\}| \;=\; \frac{b(D)\,(m+1) - d\,m\,(m+1)}{m^2+1-d},$$

and hence there must exist a point P outside of D that is contained in at most this number of circles blocked by D. Adding this point to D, we obtain

$$b(D \cup \{P\}) \;\;\geq\;\; b(D) + m\,(m+1) \;-\; \frac{b(D)\,(m+1) - d\,m\,(m+1)}{m^2+1-d}.$$

With our assumption on D, we obtain the lower bound:

$$\begin{aligned}
b(D \cup \{P\}) &\geq b(D) - \frac{b(D)\,(m+1) - (m^2+1)\,m\,(m+1)}{m^2+1-d} \\
&\geq m\,(m^2+1)\left[1 - \frac{1}{\binom{m^2+1}{m+1}}\left(\binom{m^2+1-d}{m+1} - \frac{\binom{m^2+1-d}{m+1}(m+1)}{m^2+1-d}\right)\right] \\
&\geq m\,(m^2+1)\left[1 - \frac{1}{\binom{m^2+1}{m+1}}\left(\binom{m^2+1-d}{m+1} - \frac{(m^2-d)!(m+1)}{(m+1)!(m^2-m-d)!}\right)\right] \\
&\geq m\,(m^2+1)\left[1 - \frac{1}{\binom{m^2+1}{m+1}} \cdot \frac{(m^2+1-d)! - (m^2-d)!(m+1)}{(m+1)!(m^2-m-d)!}\right] \\
&\geq m\,(m^2+1)\left[1 - \frac{1}{\binom{m^2+1}{m+1}} \cdot \frac{(m^2-d-m)(m^2-d)!}{(m+1)!(m^2-m-d)!}\right] \\
&\geq m\,(m^2+1)\left[1 - \frac{1}{\binom{m^2+1}{m+1}} \cdot \frac{(m^2-d)!}{(m+1)!(m^2-m-d-1)!}\right] \\
b(D \cup \{P\}) &\geq m\,(m^2+1)\left[1 - \frac{\binom{m^2+1-(d+1)}{m+1}}{\binom{m^2+1}{m+1}}\right].
\end{aligned}$$

□

This bound is met by one-, two- and three-element point sets. For a set of four points, not incident with a circle, this bound is slightly weaker than the blocking number that is actually achieved. The next statement shows consequences for the cardinality of a blocking set.

Theorem 6.13 *In an inversive plane of order m, there exists a blocking set of at most*

$$m^2 + 1 - \sqrt[m+1]{\binom{m^2}{m}(m-1)!}$$

elements.

Proof: We define

$$g(d) := m\,(m^2+1)\,(1 - \frac{\binom{m^2+1-d}{m+1}}{\binom{m^2+1}{m+1}})$$

as the number of circles which can be blocked by a d-element point set. As we know from Theorem 6.12, this is possible. Now we have to find out from which d on this point set would block all circles: $g(d) \geq m\,(m^2+1)$. We obtain:

$$\begin{aligned} m\,(m^2+1)\left(1 - \frac{\binom{m^2+1-d}{m+1}}{\binom{m^2+1}{m+1}}\right) &\geq m\,(m^2+1) \\ m\,(m^2+1)\left(1 - \frac{\binom{m^2+1-d}{m+1}}{\binom{m^2+1}{m+1}}\right) &> m\,(m^2+1) - 1. \end{aligned}$$

Furthermore

$$\binom{m^2+1-d}{m+1} \leq \frac{(m^2+1-d)^{m+1}}{(m+1)!}$$

holds. Hence, a cardinality d satisfying

$$m\,(m^2+1)\left(1 - \frac{\frac{(m^2+1-d)^{m+1}}{(m+1)!}}{\binom{m^2+1}{m+1}}\right) > m\,(m^2+1) - 1$$

would satisfy $g(d) > m(m^2+1) - 1$ as well. In other words, for this d there would exist a point set $D \subseteq P$ of the inversive plane with $|D| = d$, such that $b(D)$ is (at least) $m(m^2+1)$. Finally

we obtain the claim using the inequalities

$$\begin{aligned}
m\,(m^2+1)\left(1-\frac{\frac{(m^2+1-d)^{m+1}}{(m+1)!}}{\binom{m^2+1}{m+1}}\right) &> m\,(m^2+1)-1\\
m\,(m^2+1)\,\frac{\frac{(m^2+1-d)^{m+1}}{(m+1)!}}{\binom{m^2+1}{m+1}} &< 1\\
m\,(m^2+1)\,\frac{(m^2+1-d)^{m+1}}{(m+1)!} &< \binom{m^2+1}{m+1}\\
(m^2+1-d)^{m+1} &< \binom{m^2+1}{m+1}\frac{(m+1)!}{m\,(m^2+1)}\\
m^2+1-d &< \sqrt[m+1]{\binom{m^2+1}{m+1}\frac{(m+1)!}{m\,(m^2+1)}}\\
d &> m^2+1-\sqrt[m+1]{\binom{m^2}{m}(m-1)!}.
\end{aligned}$$

□

Corollary 6.14 *A power series expansion of the latter bound in Theorem 6.13 yields an asymptotic result that an inversive plane of order m contains a blocking set of at most*

$$3\,m\ln(m)+\frac{1}{2}m+\frac{1}{24}-\frac{9}{2}\ln(m)-\frac{9}{2}\ln(m)^2+O(\frac{1}{m}) \;=\; 3\,m\ln(m)+\frac{1}{2}m+O(1)$$

points.

Greedy-Index

In the last paragraph, we showed that for a given cardinality there exists a set of points which will block at least a certain number of circles. So in the proof, we consider a hypothetical algorithm that successively adds points to a given set of points in such a way, that a maximal number of circles will be intersected by the enriched set. As this algorithm does not revise its past choices, it works according to a greedy principle. In this way we define a function g that assigns to every element $d \in \{1,\ldots,m^2-1\}$ a lower bound for the number of circles of the inversive plane, that can be blocked by a d-element subset of points. Having this function, we define the *greedy index* of a given point set D as the ratio of the number of circles actually blocked by D to the number $g(|D|)$.

Definition 6.15 In an inversive plane of order m let $D \subseteq P$ be a point set of cardinality $|D|$. The function $r : 2^P \to \mathbb{R}$, defined by

$$r(D) := \frac{b(D)}{g(|D|)}, \quad \text{where } g(|D|) = m\,(m^2+1)\left(1-\frac{\binom{m^2+1-|D|}{m+1}}{\binom{m^2+1}{m+1}}\right).$$

is called the *greedy index* of D.

Proposition 6.16 *From Examples 6.7, the blocking number of a circle of an inversive plane of order* m *is* $\frac{1}{2}m^2(m+3)$. *As* m *grows, the greedy index decreases monotonically and converges to* $\frac{1}{2}\frac{e}{e-1} \approx 0.79$ *where* e *is the Eulerian number.*

This greedy index is designed to measure what could be called the blocking quality of a given set. A greedy index of 1 would mean that the given point configuration has the same quality as the theoretically best set. A configuration with greedy index less than 1 would have a lower quality. It would be desirable to find point sets with asymptotically high greedy indices. We conclude our investigation with an analysis of the blocking capability of a (maximal) subplane.

Proposition 6.17 *For a (maximal) subplane* $\mathbb{M}'$ *of order* m' *in an inversive plane of order* m, *with* $m = m'^3$, *the blocking number is (see Proposition 6.11)*

$$b(\mathbb{M}') = (m'^2+1)\,(m^2+m-\frac{1}{2}m^2\,m'+\frac{1}{2}m'^3-m'^2)$$

and the greedy index converges for m *growing to* 1 *(see Figure 6.4).*

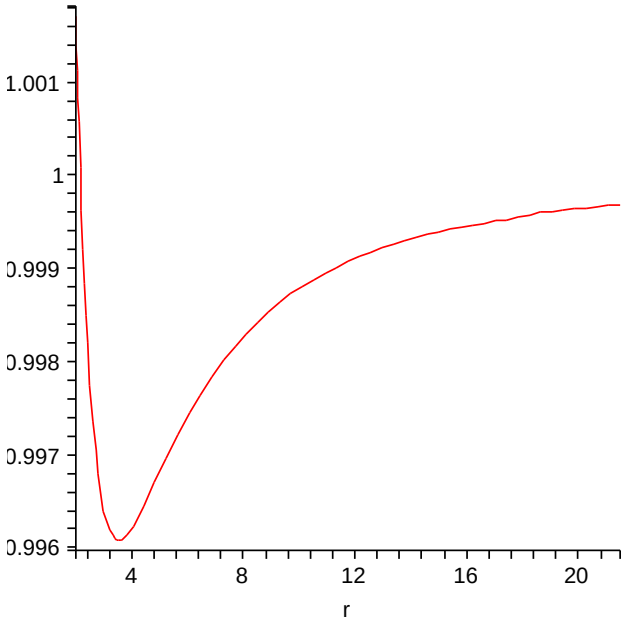

Figure 6.4: Greedy index of a maximal subplane (asymptotic)

7 Low-Density Parity-Check Codes

In cryptography as well as in coding theory, certain features of inversive planes, respectively inversive spaces, are applied. In cryptography the research on *secret sharing schemes* and *key distribution* makes use of inversive planes [66, 67, 68]. This chapter discusses an application of inversive planes in coding theory which yields a promising family of *low-density parity-check (LDPC) codes*. First we will give briefly an overview of the goals and problems in coding theory. This is to position LDPC codes in contemporary coding theory. Finally we elaborate the design of the codes we discovered. The resulting LDPC codes, which are based on inversive spaces, were discovered in joint work with M. Greferath and later including M. Flanagan [35]. This chapter profited substantially from the joint work with M. Greferath and L. Storme which can be found in [40].

7.1 The Idea of Coding

In modern life, communication is of great importance. Generally, communication is any transmission of information: a source (called the sender) is passing a message to a recipient (called the receiver) through a channel (where the channel is the way of sending). There are countless types of communication. For example a person talking to someone on the telephone, a computer transferring a file to a memory stick, verification of a PIN for a debit card, a satellite sending a picture back to earth, etc. Hence there is a diversity of possible senders and receivers of information, not only a person or a computer, also a bar-code and a register in a supermarket. There is also a huge variety of channels, the information can be transmitted, e.g. through a phone line, a bluetooth connection, a card reader or wireless. Now most likely the transmission is not completely accurate, the information is altered or in other words the received message is not exactly the same as the one which was sent: it contains what is called *noise*. Obviously reliable communication is in great demand at present, in particular for digital communication. The receiver wants to be able to recover the original message from the data received via a noisy channel. To achieve this goal, a scheme to add redundancy to the message in an efficient way is used. This makes it possible to ensure a certain level of security for the transmission. Codes are studied for this purpose: designing efficient and reliable information transfer schemes. The science of finding these schemes for reliable transmission through a noisy channel is called *coding theory*.

In general a code is a rule for converting a message into a format suitable for transmission, e.g. the morse code where our common alphabet is translated into an alphabet consisting of just two symbols, long and short. Other non digital examples are semaphore or sign language.

Now in coding theory, error-correcting codes are targeting fast and reliable recovery of the original message. Thus error-correcting codes pursue two competing goals: reliability and efficiency.

Common applications require high bandwidth communication using devices consuming less and less energy without compromising reliability. Commonly known examples are CDs/DVDs and other digital data storage devices, wireless signal transmission, e.g. mobile phones, or data transfer to and from a satellite.

The foundations of the theory of reliable communication were developed by Claude E. Shannon. In his landmark paper "A mathematical theory of communication" [88], he describes amongst other things a communication scheme (see Figure 7.1) and introduces the term *bit* for a unit of information.

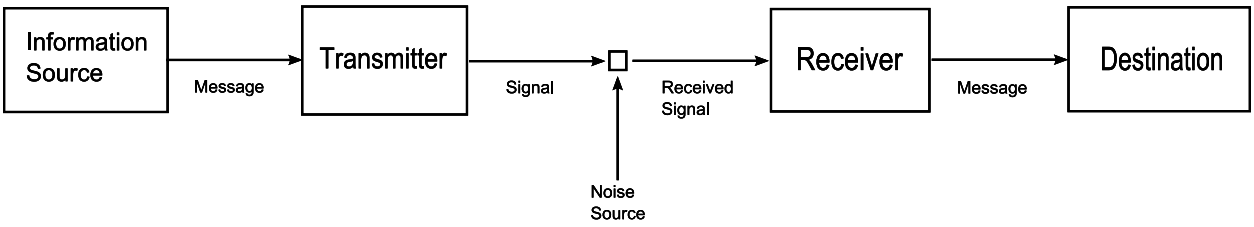

Figure 7.1: General Shannon-Weaver communication model (1949)

7.2 Communication Setting

The original model for information transfer distinguishes between five elements. The *information source* giving a message to the *transmitter*, which turns the message into a signal. The signal is then sent over the *channel* to the *receiver*. There the message is reconstructed from the received signal and forwarded to the *destination*. As a disruptive factor the channel is exposed to noise, which varies in strength and character.

In order to make it possible for the receiver to regain the correct message despite the noise in the channel the sender encodes the message. Usually encoding means adding redundancy in one way or another to the message. During the transmission over a channel the information might get altered by noise. The added information is then used by the receiver to possibly detect and correct errors. To retrieve the original information vector from the received signal is called *decoding* of a message. There is a huge variety of codes with different qualities regarding, e.g. error detection/correction or size, which makes them suitable for different applications. Here we can focus on binary linear codes, which belong to the class of block codes.

For example a *binary code* is a mapping which adds redundancy to a message. If the message is a binary sequence of length n, the encoded message will be a sequence of $m > n$ zeros and ones. Thus the code maps blocks of size n onto blocks of size m where the blocks of size m are called *codewords* and the set of all possible codewords is the *block code*. The algorithm used by the receiver to recover the original message is called the *decoder*.

There is *hard decision* and *soft decision* decoding. Hard decision decoding means that each received bit is interpreted as valid information. In a binary system for example, the output of a *digital channel* is either 0 or 1, for every transmitted bit. A hard decision decoder then assigns valid codewords to the received signal. For example a hard decision *maximum-likelihood decoder* assigns to every received sequence the most likely original information, being the one which is closest to

the received signal. In other words, this widely used decoder retrieves the original information by changing a minimal number of bits. This type of decoder matches the communication model where the information is transmitted via a binary symmetric channel. In this channel bits, meaning 0 and 1, are switched with probability p thus they are transmitted correctly with probability $1-p$. A *binary symmetric channel* (see Figure 7.2) with probability p, where $0 \leq p \leq 1$, is a binary mapping satisfying:

- the probability for 1 being mapped onto 0 is the same as the probability for 0 being mapped onto 1: $p(1|0) = p(0|1) = p$.
- the probability that a bit is not altered is $1-p$: $p(1|1) = p(0|0) = 1-p$.

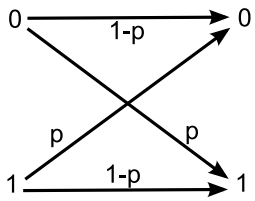

Figure 7.2: Binary symmetric channel

For LDPC codes decoding methods using soft decision are used. Soft decision decoding associates a certain probability to each received bit. Therefore the model of an *additive white Gaussian noise channel* (see Figure 7.3 for an AWGN channel) is used for the simulations. The received signal is expressed as $p(0)$ and $p(1)$ with $p(0)+p(1) = 1$ for each received bit. These probabilities are then used as input for the decoder using a *message-passing algorithm*.

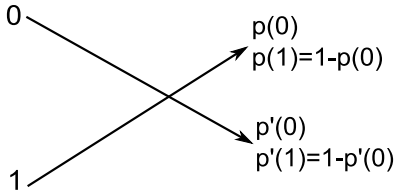

Figure 7.3: Additive white Gaussian noise channel

The message is encoded by the transmitter using a code C, then the encoded message is transmitted via a noisy channel and at the other end of the channel the receiver uses a decoder D to recover the original message. Depending on the code, there are disparate ways of decoding.

Figure 7.4: Standard communication system

7.3 Basic Concept of Codes

The codewords of a block code are n-tuples over an alphabet, thus we can identify them with vectors of the n-dimensional vector space V_n over a field $GF(q)$, corresponding to the alphabet. The structure of the vector space enables us to define a *linear block code* C of *length* n and *dimension* k as a subspace of dimension k of the n-dimensional vector space over $GF(q)$. A linear block code C has then a *generator matrix* G being a $k \times n$ matrix of linearly independent rows such that:

$$C = \{x\,G \mid x \in GF(q)^k\}.$$

The benefit of linear codes is obviously that we can encode a message vector simply by multiplying it by a generator matrix of the code. For some applications matrix multiplication is considered too complex, in these applications encoding schemes of lower complexity are required.

The check digit is the sum over of a pre-specified set of information digits. These formation rules for each check digit can be represented conveniently by a parity-check matrix [37]. When a code C has a parity-check matrix H, then C is the null space of H. The parity-check matrix of a linear code is the generator matrix of its dual code [79].

Definition 7.1 The *parity-check matrix* H of the code C is a $J \times n$ matrix of rank $n-k$ (where $J \geq (n-k)$) satisfying:

$$H \cdot c = 0, \quad \forall\, c \in C,$$

where 0 denotes the 0-vector.

Hence the code C consists of the set of solutions of the equations above. Each codeword satisfies the parity-check equations with regard to the rows of H. Therefore it is straightforward to check whether a received vector is corrupted: If you multiply it with the parity-check matrix and the result is not the 0-vector, the message contains an error. Linear block codes are often described by their parity-check matrix but both, the generator as well as the parity-check matrix, define the linear code uniquely.

The *Hamming distance* between two strings $x = (x_1 \ldots x_n)$ and $y = (y_1 \ldots y_n)$ is defined as the number of positions in which the n-tuples differ:

$$d(x, y) := |\{1 \leq i \leq n \mid x_i \neq y_i\}|\,.$$

The *Hamming weight* w of a binary codeword x is the number of positions with a nonzero entry: $w(x) := d(x, 0)$ where 0 is the 0-vector. The *minimum distance* d of a code is then

$$d = \min\{d(x, y) \mid x, y \in C, x \neq y\}.$$

If a linear code C has length n, dimension k and minimum distance d, we write C as an $[n, k, d]$ *code*.

When we follow the communication system in Figure 7.4, we see that an $[n, k, d]$ code will encode a message of length k into a codeword of length n. This information is sent over the channel. The received message is then decoded, this means that it is, if possible interpreted as a valid piece of information, which is passed on to the receiver. Generally, up to $d-1$ errors can be detected and up to $(d-1)/2$ errors can be corrected (see [79]). The ratio between the length n of the transmitted signal to the length k of the original information is called the *rate* k/n of the code.

For a $m \times n$ matrix we define the *row and column weight* as the sum of the entries:
A row $i \in \{1, \ldots, m\}$ has weight $\rho := \sum_{j=1}^{n} x_{ij}$, a column $j \in \{1, \ldots, n\}$ has weight $\gamma := \sum_{i=1}^{m} x_{ij}$.
The matrix is called *regular* if every row has the same weight and the column weight is the same for every column.

7.4 What are LDPC Codes?

LDPC codes were developed in 1963 by Robert G. Gallager in his doctoral thesis at the Massachusetts Institute of Technology [37]. Impractical to implement at the time, they were forgotten until their rediscovery by D. MacKay and R. Neal [60] in 1995. Decoding had been a major problem but with the graphical approach to LDPC codes introduced by R. Tanner [97] in 1981, an algorithm called *message-passing decoding*, in particular its version as *sum-product algorithm*, could now be used.

The LDPC codes investigated so far were pseudo random constructions; these codes already perform quite close to the Shannon limit (see page 104). The Shannon limit is a theoretical value depending on the capacity of the channel. Reliable codes and decoding algorithms are possible at a rate below this limit; above the Shannon limit, meaning at a higher rate, coding is not effective. With the new interest in LDPC codes grew the demand in more efficient encoding and decoding algorithms (e.g. [80]), and in particular in systematic constructions. In Section 7.7 we will show the various ways LDPC codes have been constructed, but so far only few outperform random constructions.

Please note: From now on we are talking about binary codes. Momentarily this class of codes is in the center of discussion.

Low-density parity-check codes are described by their parity-check matrix:

Notation 7.2 Let H be the regular $J \times n$ parity-check matrix of a code C in the binary vector space, thus C is the zero space of H. We call H a *low-density parity-check matrix or LDPC matrix* if it satisfies:

1. Any two rows have at most one 1 at the same position: $|\{x_{ij} = 1 = x_{hj} \mid i, h \in \{1, \ldots, J\}, i \neq h, j \in \{1, \ldots, n\}\}| \leq 1$.
2. The row weight ρ and column weight γ, in comparison to the number of rows and columns is small: $\rho << J, \gamma << n$.

The code C is then a *(binary, regular) low-density parity-check code or LDPC code*, also referred to as *binary, (ρ, γ)-regular LDPC code*. Is H an LDPC matrix, then H^T is, because of $G \cdot H^T = 0$, also an LDPC matrix.

The first condition provides some geometric structure which we will need for our constructions. The second needs further explanation. The matrix H with a small number of $1's$ compared to the number of $0's$ is called a *sparse* matrix. In order to address what sparse means in this context, we need to define a term to compare the number of 1 and 0 entries in the matrix.

Definition 7.3 The *density* δ of a $J \times n$ LDPC matrix H with row weight ρ and column weight γ is:

$$\delta := \frac{\rho}{n} = \frac{\gamma}{J}.$$

Practical applications are interested in densities which scale roughly linear with n rather than quadratic, like $\delta \approx 6/n$, where $256 \leq n \leq 8192$.

The rows of H can be linearly dependent, then the parity-check matrix for the LDPC code is not of full rank. In fact, it turns out that for actual applications a moderate set of extra rows in the check matrix of an LDPC code can contribute to an improved performance of the implemented decoder. We will discuss later that most parity-check matrices based on the geometric structures are highly redundant and that these binary, regular parity-check matrices are nothing but incidence matrices of *combinatorial designs*.

Example 7.4 Consider the binary code of length $n = 7$ and dimension $k = 4$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

A generator matrix for this code is

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Particularly interesting for applications is the following algebraic property for block codes. Even if only parts satisfy this condition, the encoding process (see Section 7.5) is already much faster.

Definition 7.5 A linear block code C is called *cyclic* if for every codeword $(c_0, \ldots, c_{n-1})$ all cyclic shifts, e.g. $(c_1, \ldots, c_{n-1}, c_0)$, give a codeword as well.

LDPC codes can also be described non-algebraically by Tanner graphs [97]. These graphs do not only describe the LDPC code, but furthermore visualise the decoding process. We will use them in the following Section 7.5 to explain the decoding algorithm.

Definition 7.6 The *Tanner graph* of a $k \times n$ parity-check matrix H is a bipartite graph on the vertex set $S \cup T$ where S is a set of k vertices called *check vertices* and T is a set of n vertices called *bit vertices*. An edge is drawn between check vertex $s \in S$ and bit vertex $t \in T$ iff the (s, t)-entry of the parity-check matrix H is nonzero.

The length of the shortest cycle is referred to as the *girth* g of the graph.

Figure 7.5 shows the corresponding Tanner graph for the matrix H in Example 7.4. From Definition 7.1 we already know the difference between check digits and information, or bit digits. The corresponding vertices are here squares for the check vertices and circles for the bit vertices.

One of the main conditions regarding the performance of a code is its minimum distance d: the minimum number of digits any two codewords differ. There is not much known about the minimum distance of LDPC codes. We will collect, enhance and compare new and known attempts.

Lemma 7.7 *The number $Z(\ell)$ of non-zero entries in a linear combination of ℓ columns of the check matrix of girth at least 6 with constant column weight γ satisfies*

$$Z(\ell) \;\geq\; \ell\,\gamma - \ell(\ell - 1).$$

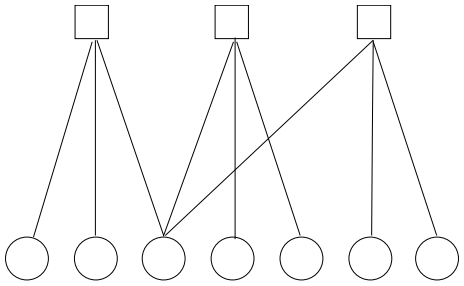

Figure 7.5: Tanner graph

Proof: We will proceed by induction and first observe that $Z(1) = \gamma$ in accordance with the claim. Assume that $Z(\ell) \geq \ell\,\gamma - \ell(\ell-1)$ for some $\ell \geq 1$, and assume that $\ell + 1$ distinct columns are given. Then by the assumption on the girth of the underlying matrix, the $(\ell+1)$st column shares at most one 1-entry with each of the preceding ℓ columns, and hence the number of 1's in the sum is given by $Z(\ell+1) \geq Z(\ell) + \gamma - 2\,\ell \geq \ell\gamma + \gamma - 2\,\ell - \ell(\ell-1) = (\ell+1)\,\gamma - (\ell+1)\ell$ which finishes the proof. □

Proposition 7.8 *For a parity-check matrix of girth at least* 6 *with column weight* γ*, a non-empty set of linearly dependent columns has at least* $\gamma + 1$ *elements.*

Proof: Assume there are ℓ linearly dependent columns in the matrix where ℓ is assumed to be minimal. Then $0 \geq Z(\ell) \geq \ell\,\gamma - \ell(\ell-1)$ according to the preceding proposition. Solving this for ℓ yields $\ell \geq \gamma + 1$. □

Similar statements can be made about the rows of a regular parity-check matrix. The preceding statement has an immediate consequence for the minimum distance of the LDPC code in question.

Theorem 7.9 *The minimum distance of an LDPC code of girth at least* 6 *with column weight* γ *is at least* $\gamma + 1$.

Proof: It is well known that the minimum distance of a linear code is d, if every choice of $d-1$ columns of a parity-check matrix for this code is linearly independent but there are d linearly dependent columns. With Proposition 7.8 we conclude that the minimum distance of an LDPC code under the above assumptions is at least $\gamma + 1$. □

This result is a slight improvement for girth up to 8, otherwise we refer to the minimum distance analysis made by Tanner in [97].

7.5 Encoding and Decoding

As mentioned before, LDPC codes had no practical potential at the time they were discovered; the encoding and decoding process was a non-feasible task. The encoding of information using a code defined by a generator matrix, like LDPC codes, is theoretically simple but does involve high computational power and time. Encoding an information vector using a linear code is generally a straightforward algorithm involving a matrix multiplication. In the case of cyclic LDPC codes (see Definition 7.5) the encoding by now is simple and fast.

Example 7.10 If we want to encode the information vector $v := (1,0,1,0)$ for example, we send the encoded vector c where $v \cdot G = c$:

$$c = (1,0,1,0) \cdot \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Now the encoded information, $(1,0,1,0,1,0,1)$, is sent over the channel (see Figure 7.4).

Sum-Product Algorithm

It is known (see e.g. [7]) that in general the decoding problem for block codes using maximum-likelihood decoding is computationally hard. Linearity of a code can reduce this complexity but does not do so in general. Using the idea to describe LDPC codes by bipartite graphs made it possible to develop fast and sufficient decoding algorithms like message-passing decoders. The message-passing decoder we will use is called *sum-product algorithm*. We give here a very brief presentation of this algorithm. The sum-product algorithm iterates between the two types of nodes of the Tanner graph, the check nodes S and bit nodes T. The check nodes are represented by squares and the bit nodes (also referred to as variable nodes or information nodes) by circles. First the checks collect information from their adjacent bits. For each bit node, the check calculates the probabilities he retrieved from other bits it is connected to and sends this information to the bit, see Figure 7.6.

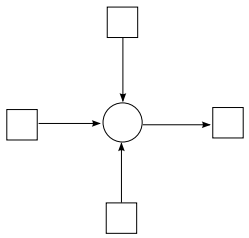

Figure 7.6: Bit node

If, e.g. a bit is connected to three checks and receives from one check the information (a,b) and from the other (a',b') where a and a' are $p(0)$ and b and b' are $p(1)$. Then the bit calculates the information for the third check $p(0) = a'' = aa' + bb'$ and $p(1) = b'' = ab' + a'b$ and sends it. If there are more adjacent nodes the probability is calculated associatively. It is important that the information the check node gets is independent from what it had sent to the bit. In the next step the check node calculates the probabilities for the bits and again, the information for each bit is independent from what it had sent. If again, a check is connected to three bits (see Figure 7.7) and receives from the one bit (c,d) and from the other (c',d'), then it will calculate the information to be sent to the third bit (c'',d'') as follows: $c'' = \frac{cc'}{cc'+dd'}$ and $d'' = \frac{dd'}{cc'+dd'}$ where the denominator insures the probability laws.

Depending on the girth of the Tanner graph the original information will after a number of iterations get back to the node and influence the result. Thus the reliability of the sum-product algorithm is

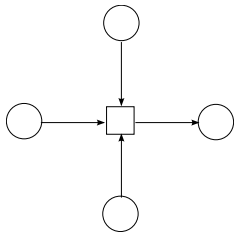

Figure 7.7: Check node

proved if the Tanner graph is a tree. In practice the algorithm turns out to converge if the girth is large enough, and it is extremely efficient.

Let us now clarify this process using Example 7.4: Assume that at the receiving end of the communication channel, a vector r of soft information about a binary word is given in the form

$$r \;=\; \big[[.9,.1],[.6,.4],[.1,.9],[.1,.9],[.8,.2],[.8,.2],[.6,.4]\big].$$

Under hard decision, r yields the binary word $[0,0,1,1,0,0,0]$ and it is easily checked that

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \;=\; \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \;\neq\; \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

which shows that $[0,0,1,1,0,0,0]$ is not a codeword, thus cannot be the transmitted word. The resulting vector $[1,0,1]$ is also referred to as the *syndrome*. In this example two conditions fail. The syndrome contains two non-zero entries, this shows that at least one error occurred.

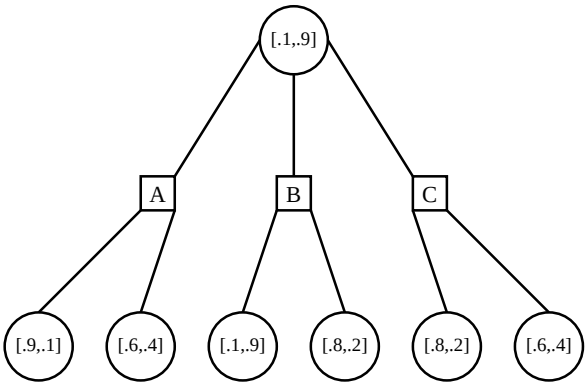

Figure 7.8: Sum-product algorithm – initialization

Figure 7.8 shows the initialization, the received vector r is stored in the bit vertices r_t, $t \in T$.

The first step of the sum-product algorithm applies to r: these distributions pass as messages $p_{t,s}$ from bit vertex $t \in T$ to check vertex $s \in S$ along the edges, as is depicted in Figure 7.9.

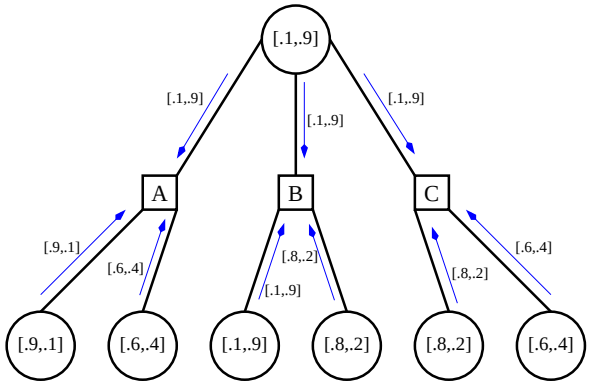

Figure 7.9: Sum-product algorithm – passing bit messages to the checks

Next, as depicted in Figure 7.10, for each check vertex the algorithm computes convolutions of the distributions that reach the check, and passes the results back to the bit vertices.

More precisely: let $T(s)$ be the neighborhood of check vertex $s \in S$, and denote by $p_{t,s}$ the distribution that reaches s from bit vertex $t \in T(s)$. Let $q_{s,t}$ denote the distribution that is passed back from s to t. Then

$$q_{s,t} \;:=\; \bigotimes_{\substack{u \in T(s) \\ u \neq t}} p_{u,s} \quad \text{for all } t \in T(s).$$

The symbol $\otimes$ denotes the (additive) convolution of two distributions, which means

$$\big(a \otimes b\big)(0) := a(0)\,b(0) + a(1)\,b(1) \quad \text{and} \quad \big(a \otimes b\big)(1) := a(0)\,b(1) + a(1)\,b(0).$$

For example check vertex A receives information from bit vertices $1, 2, 3$. The information $p_{1,A} = [.9, .1]$ and $p_{2,A} = [.6, .4]$ is convolved to $.9 \cdot .6 + .1 \cdot .4 = .58$ and $.1 \cdot .6 + .9 \cdot .4 = .42$ and passed as $q_{A,3} = [.58, .42]$ to bit 3.

After convolution and passing the messages $q_{s,t}$ to the bit vertices, the latter computed Hadamard products (componentwise multiplication) of the distributions is passed along with the initial distribution. These products are normalised, to make them distributions again, and then passed back to the check vertices. A (normalised) copy of the Hadamard product of all incoming distributions with the received information is kept as an update of the bit vertex distribution. All this can be seen in Figure 7.11.

More precisely: let $S(t)$ be the neighborhood of bit vertex $t \in T$, and denote by $q_{s,t}$ the distribution that reaches t from check vertex $s \in S(t)$. First an updated distribution vector $\hat{r}$ is computed, and has value

$$\hat{r}_t \;:=\; \frac{1}{N}\, r_t \cdot \prod_{v \in S(t)} q_{v,t} \qquad \text{with} \quad N := r_t(0) \prod_{v \in S(t)} q_{v,t}(0) + r_t(1) \prod_{v \in S(t)} q_{v,t}(1),$$

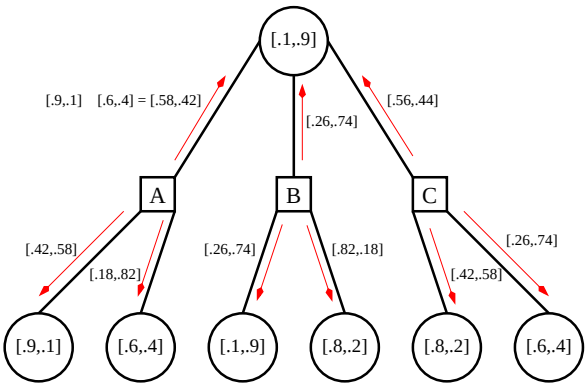

Figure 7.10: Sum-product algorithm – convolution step

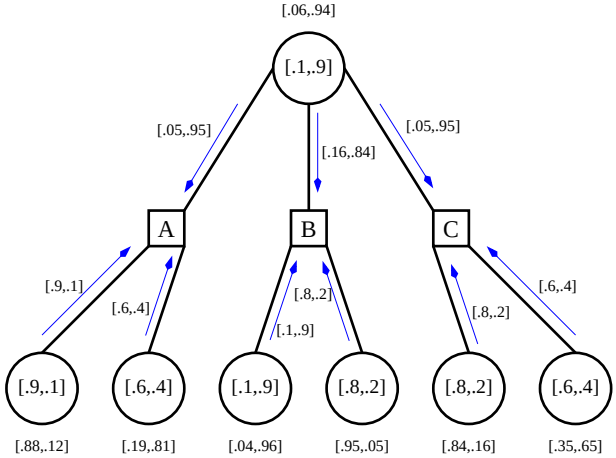

Figure 7.11: Sum-product algorithm – update and begin of second iteration

for all $t \in T$.

Here $\prod$ (resp. $\cdot$) denotes the pointwise Hadamard product of two vectors, which means

$$\big(a \cdot b\big)\,(0) := a(0)\,b(0) \quad \text{and} \quad \big(a \cdot b\big)\,(1) := a(1)\,b(1).$$

If we take for example bit vertex 3 which received $q_{A,3} = [.58, .42]$ from check A, $q_{B,3} = [.26, .74]$ from B and $q_{C,3} = [.56, .46]$ from C, we get for $N = .1 \cdot .58 \cdot .26 \cdot .56 + .9 \cdot .42 \cdot .74 \cdot .44 = .0084 + .1230 = .1314$, so we get the distribution $\hat{r}_3(0) = \frac{.0084}{.1314} = .06$ and $\hat{r}_3(1) = \frac{.1230}{.1314} = .94$ for bit vertex 3.

At this stage we could already decode the correct codeword, but for the sake of this example we will add a second iteration: Let $p_{t,s}$, as above, denote the distribution that is passed back from t to s. We set for all $s \in S(t)$:

$$p_{t,s} \;:=\; \frac{1}{N}\, r_t \cdot \prod_{\substack{v \in S(t) \\ v \neq s}} q_{v,t} \qquad \text{with} \quad N := r_t(0) \prod_{\substack{v \in S(t) \\ v \neq s}} q_{v,t}(0) + r_t(1) \prod_{\substack{v \in S(t) \\ v \neq s}} q_{v,t}(1).$$

and send this information to the check vertex.

The information sent from bit vertex 3 back to check vertex A would then be:

$$p_{3,A}(0) = \frac{.1 \cdot .26 \cdot .56}{.1 \cdot .26 \cdot .56 + .9 \cdot .74 \cdot .44} = \frac{.0146}{.0146 + .2930} = \frac{.0146}{.3076} = .05$$

$$p_{3,A}(1) = \frac{.9 \cdot .74 \cdot .44}{.3076} = \frac{.2930}{.3076} = .95$$

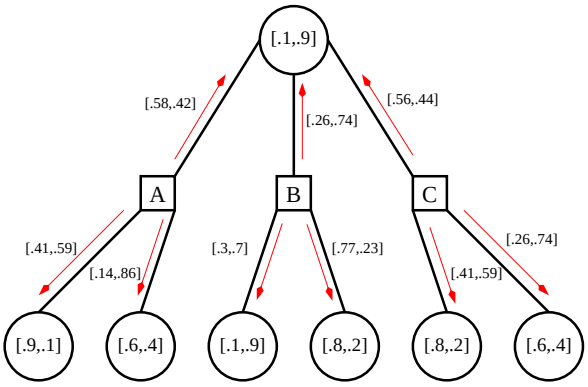

Figure 7.12: Sum-product algorithm – check-to-bit communication in second iteration

This procedure is repeated a number of times. After each iteration the vector $\hat{r}$ of updated probability distributions is decoded by hard decision into a binary vector. Once this yields a codeword, the algorithm is terminated.

In Figure 7.13 we can see this: at the end of the second iteration we obtain from the vector

$$\hat{r} \;=\; \big[[.86, .14], [.2, .8], [.06, .94], [.05, .95], [.74, .26], [.93, .07], [.3, .7]\big]$$

of updated distributions the binary word $[0, 1, 1, 1, 0, 0, 1]$, and it is easily checked that

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

showing that our resulting word is a codeword. We will now terminate the algorithm.

7.6 Performance

For an LDPC code, given by a parity-check matrix, there are limitations for predicting its performance. Some characteristics, the girth of the corresponding Tanner graph or the minimum distance,

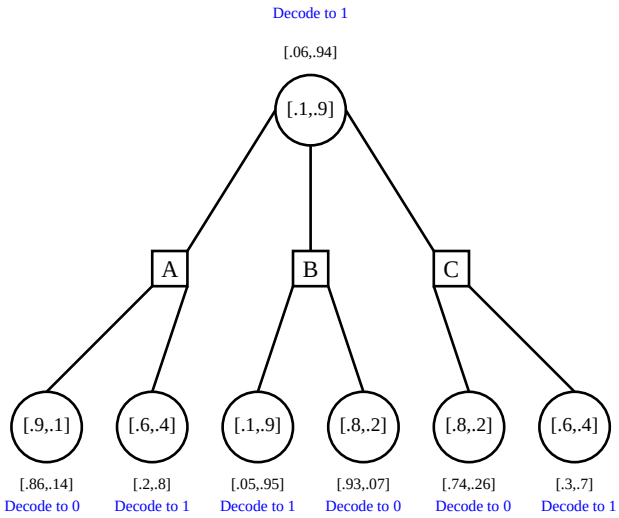

Figure 7.13: Sum-product algorithm – terminating step

are known to support a good performance. Further structural features of the graph like *stopping sets*, *trapping sets*, *absorbing sets* of vertices are relevant as well. A quite extensive theory of what are called *pseudo codewords* has been developed to enhance this understanding (cf. [70, 104, 105]). So far the common method of demonstrating the quality of an LDPC code is an extensive simulation of its behavior in a noisy communication channel. The error correcting performance of the code is usually compared with a not coded transmission over the channel, a randomly generated LDPC code, and as the case may be, other LDPC codes.

7.6.1 Simulation

To test a code and a decoder at a specific *signal-to-noise ratio* (SNR) of the channel, the simulation procedure is as follows: a message vector is randomly generated, the message is encoded to produce a codeword, which is modulated to create the desired signal strength. Noise is generated randomly according to the channel's noise level and added to the codeword to simulate the channel. The resulting vector of distributions is considered as received word, and then decoded. In each case decoding continues until either a valid codeword was detected (via syndrome check) or a maximum of 64 iterations is completed. This procedure is repeated under the same conditions, that is, the same code, the same noise level and the same decoder until at least 100 frame errors are simulated to determine the *bit error rate* (BER). We consider that for a good code the performance must be simulated for values of BER that range from 1 to 10^{-7}, and for higher rate of the code to 10^{-8} and sometimes even down to 10^{-12} and less. Note that for values of BER around 10^{-8}, the decoder makes an error (decides for a message different from the transmitted one) on average every one hundred thousand received messages, where we assume a block length of $n = 1000$. The larger the SNR is, or in other words, the lower the noise, the longer it will take until the algorithm finds enough errors to proceed to the next simulation point. So billions of simulations must be carried out to get realistic representation of the performance of a code. Using a computer cluster this might take days of computing.

7.6.2 Comparison

As already mentioned, there is a threshold for the feasibility of coding, the *Shannon limit*. This constant gives the theoretical bound depending on the channel quality and the transmission rate. No reliable communication is possible using a code whose rate is higher than the Shannon limit. On the other hand the existence of codes having a vanishing error probability at a rate below the Shannon limit has been proven [88]. The Shannon limit determines the correspondence between the noise level of the channel and the communication rate. For a given degree of noise contamination of a communication channel, it is possible to send information nearly error free (up to a maximum rate given by the Shannon limit) using longer codes. We can also say that the Shannon limit of a communication channel is the maximum rate for a particular noise level. The actual limit is evaluated involving more or less complex computations and numerical integration, what we do not need to discuss here.

The goal in coding is to find implementable codes performing at a rate close to the Shannon limit. If we take the Shannon limit as the theoretical optimum to compare the performance of a code, we compare it on the other side against the behavior of a communication system in which no coding is performed at all. Within these curves we expect the results of the simulation. This is not obvious, on the contrary, a code can as well worsen the communication! In addition it is customary to check the performance of a certain LDPC code against a random code. As mentioned before, it is challenging to compete with such a code. In the last section of this chapter (Section 7.9) the simulations for the codes constructed will be held against each other.

7.6.3 Presentation

It is common practice to illustrate the bit error rate performance of LDPC codes in a diagram, called a *waterfall-diagram*.

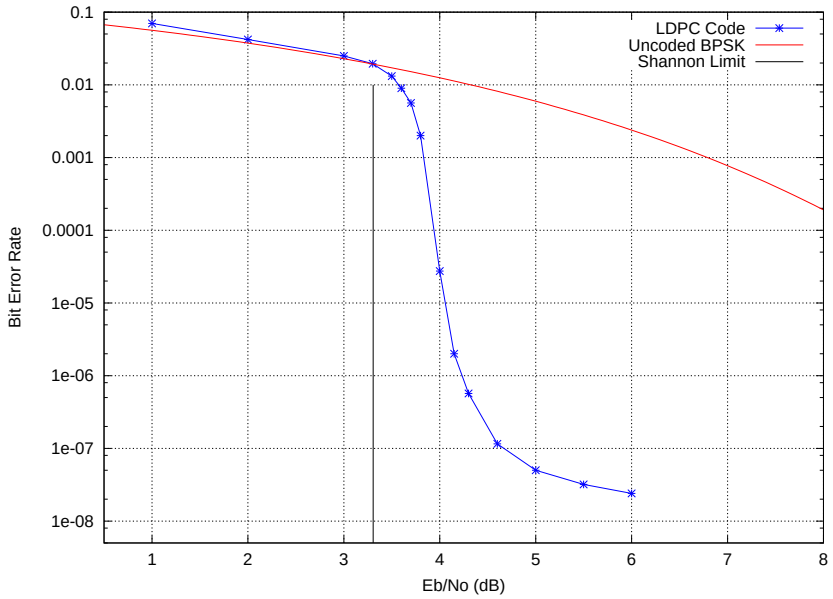

Figure 7.14: Example of a waterfall diagram

This is a chart representing the *bit error ratio* (BER) as function of the *signal-to-noise ratio* (SNR). Here, the bit error ratio is the fraction of erroneous bits in a stream of received bits, and the signal-to-noise ratio is a quantity measuring the quality of the channel. On the x-axis of the diagram you see the signal to noise ratio in decibel. The higher the signal to noise ratio, the better the quality of the channel. The y-axis shows the bit error rate. Each waterfall diagram presents the performance of a code or several, at a certain rate. Then the curve of the LDPC code represents how many errors the code can correct depending on the noise level in the channel. Now, the lower the bit error rate is, the higher signal to noise ratio is required to correct all errors.

In a waterfall diagram the Shannon limit marks a point on the x-axis shown by a vertical line. Only to the right of this line, we can expect the benefit of coding. Often you find other graphs in the same diagram for comparison. Useful here is the graph plotting the behavior of a communication system in which no coding is performed at all. This curve is of very moderate slope. It essentially maps the signal-to-noise ratio (SNR) of the channel in a one-to-one manner to the bit-error-ratio (BER) in the received word. One might consider it as a guideline.

7.6.4 Analysis

For the performance graph of the LDPC code in question, there are few characteristics to mention. Obviously, the steeper this curve, and the closer it is to the vertical Shannon limit, the better. For the known LDPC codes we observe a point where the error rate gets so high that the graph of the code changes its direction and turns into an almost horizontal line. This point of change is called the *error floor* and hence, an improvement of the channel quality does not yield any further improvement in bit error ratio that results from using the code. Regarding possible applications, it is considered to be ineffective to use a given code on a channel with SNR where the code has the error floor, or even worse, to use a code that exhibits an error floor at too high BER. Developers

therefore strive for the construction of codes exhibiting error floors only at a very low bit error ratio.

7.7 Examples for Codes from Geometries

As mentioned before, the common method of construction is to take the incidence matrix of the finite geometry as the parity-check matrix of the code. In terms of incidence geometry, points correspond then to bits and blocks to parity-check equations (see Definition 7.11 below).

Code constructions based on finite geometries were first proposed in 2000 by Kou, Lin and Fossorier [51]. They started with projective and affine planes over a Galois field of even order. Inversive spaces, our main focus, as well as generalised quadrangles are very different from these classical examples. Generalised quadrangles belong to the more general concept of partial linear spaces (see Definition 1.1 in Chapter 1). Also the geometry derived from an inversive space (see Corollary 7.12) is a partial linear space. We can also classify them more precisely as (α, β)-geometries (see Definition 1.14 in Chapter 1). These concepts allow triangle free incidence structures, thus not every two points are incident. From a geometry with no triangles it is easier to construct a code such that the girth of the corresponding Tanner graph is at least 8. As we saw earlier, this property supports the performance of the decoder.

Let's start with a standard example:

Taking the point-line incidence matrix H of a projective 3-space of order q, H is a $((q^2+1)(q^2+q+1) \times (q^3+q^2+q+1))$ matrix with row weight $\rho = q+1$, column weight $\gamma = q^2+q+1$, and density $\delta = \frac{1}{q^2+1}$. The condition that two rows can have at most one 1 entry in the same place is satisfied because two lines of a projective space can intersect in at most one point. Therefore we can say that H is a binary, regular LDPC matrix.

In the first paper of Fossorier et al [51]: "Low Density Parity-Check Codes Based on Finite Geometries: A Rediscovery", the authors use incidence matrices of projective and affine planes which are punctured in the origin, in the sense, that the 0 point and all lines incident with 0 are excluded. This is done in a way that for the affine plane over $GF(2^s)$, they use a primitive element of $GF(2^{2s})$ whose powers produce all points of the plane. This enables the authors to generate a cyclic parity-check matrix H of size $(2^{2s}-1) \times (2^{2s}-1)$ with row and column weight 2^s. The generator polynomial is characterised by its roots in $GF(2^{2s})$ and the code has minimum distance $d = 2^s+1$. One can find the definitions of cyclic codes and their generator polynomial e.g. in [61] or a similar coding theory book.

In two followup papers [52, 53], the authors extended this approach into type-I and type-II parity-check matrices (see Definition 7.11 below) for affine and projective planes. Then they generalise these four codes using lines in even order affine and projective spaces of dimension m over $GF(2^s)$. These codes have length $2^{ms}-1$. The row weight is 2^s, column weight is $(2^{ms}-1)/(2^s-1)-1$, thus the density is $2^s/(2^{ms}-1)$. The minimum distance is at least $(2^{ms}-1)/(2^s-1)$, this bound is sharp for $m = 2$.

Then Lin, Tang and Kou [57] used the same construction for affine and projective spaces of even order taking a subspace and its hyperplanes. Together with Abdel-Ghaffar [109] they generalised this result for even order affine and projective spaces and the incidence between subspaces of any dimension. The associated Tanner graphs of all the finite geometry based LDPC code constructions discussed so far have a comparably modest girth (namely 6). Nevertheless, on the Gaussian channel

under the sum-product algorithm they show a performance close enough to the Shannon limit, and may hence considered to be good LDPC codes.

The following distinction between two types of incidence matrices for one incidence structure was introduced:

Definition 7.11 Let $\mathbb{G} := (P, B)$ be a finite incidence structure consisting of a set P of n points and a set B of k blocks.

(a) We define the *type-I matrix* of $\mathbb{G}$ as a binary $k \times n$ matrix $H^{(1)}$, where entry $H^{(1)}_{ij} = 1$ if point $j \in P$ is incident with block $i \in B$ and where $H^{(1)}_{ij} = 0$ otherwise.

(b) The *type-II matrix* of $\mathbb{G}$ is defined as the binary $n \times k$ matrix $H^{(2)}$ where $H^{(2)}_{ij} = 1$ if point $i \in P$ is incident with block $j \in B$ and where $H^{(2)}_{ij} = 0$ otherwise.

Obviously, $H^{(2)}$ is the transpose of $H^{(1)}$, and hence, their densities in the sense of Definition 7.3 are the same. The null space of $H^{(1)}$ is called the *type-I LDPC code* of $\mathbb{G}$. It is a code of length n. Accordingly, the null space of $H^{(2)}$ is called the *type-II LDPC code* of $\mathbb{G}$, and it is a code of length k.

The girth of the associated Tanner graph of $H^{(1)}$ or $H^{(2)}$ should be larger than 4 in order to make the sum-product algorithm performing well. In the language of geometry, this means that the incidence structure in question should not contain 2-gons, e.g. a set of two distinct blocks that meet in more than one point.

Affine and Projective Geometries

For the finite field $GF(q)$, consider the n-dimensional affine space $AG(n, q)$. Forming the matrices $H^{(1)}$ and $H^{(2)}$ in the fashion described above, we see that these are of density $\delta = \frac{1}{q^{n-1}}$. The LDPC code checked by $H^{(1)}$ is a code of length $l = q^n$ and the code has dimension n. According to Theorem 7.9 its minimum distance is lower bounded by $d_{min} \geq \frac{q^n-1}{q-1} + 1$. The type-II LDPC code checked by $H^{(2)}$ is of length $l = \frac{q^{n-1}(q^n-1)}{q-1}$ and dimension n. Again by Theorem 7.9, its minimum distance is lower bounded by $d_{min} \geq q + 1$.

An alternative construction was based on punctured affine spaces, or the internal structure (see Definition 1.18 in Chapter 1) with respect to a point P of $AG(n, q)$. It yields a space $AG_0(n, q)$. The according check matrices $H^{(1)}_0$ and $H^{(2)}_0$ are of density $\delta = \frac{q}{q^n-1}$. The LDPC code checked by $H^{(1)}_0$ is of length $n = q^n - 1$ with a minimum distance of at least $\frac{q^n-1}{q-1}$. It turns out that this code is equivalent to a cyclic code, and therefore allows for particularly efficient encoding.

The code checked by $H^{(2)}_0$ is of length $l = \frac{(q^{n-1}-1)(q^n-1)}{q-1}$ and has minimum distance at least $q+1$. This code is equivalent to a quasicyclic code with $\frac{q^{n-1}-1}{q-1}$ cyclic blocks of length q^n-1. We mention this again because of the resulting advantage in the encoding procedure. For the n-dimensional projective space $PG(n, q)$, the check matrices $H^{(1)}$ and $H^{(2)}$ are of density $\delta = \frac{q^2-1}{q^{n+1}-1}$. The LDPC code checked by $H^{(1)}$ is a code of length $l = \frac{q^{n+1}-1}{q-1}$ and dimension m. By Theorem 7.9, its minimum distance is lower bounded by $d_{min} \geq \frac{q^n-1}{q-1} + 1$. This code was known and studied as projective geometry code long before the interest in LDPC coding arose, namely in the framework

of what are called *majority-logic* decodable codes (cf. [13, 63]). It can be seen that this code is equivalent to a cyclic code and hence the encoding procedure is of accordingly low complexity. The performance of such a code is shown in section 7.9 in the waterfall diagram 7.15.

The type-II LDPC code checked by $H^{(2)}$ is of length $l = \frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)}$. Again by Theorem 7.9, its minimum distance is lower bounded by $d_{min} \geq q+2$. This code can be taken into quasi-cyclic form which again decreases the encoding complexity.

Generalised Quadrangles

In 2001, Vontobel and Tanner [106] introduced codes derived from generalised quadrangles (see in Chapter 1, Definition 1.2). An example of a generalised quadrangle of order (q,q) which is based on a symplectic generalised quadrangle in $PG(3,q)$ is shown in section 7.9. The performance of the code constructed from a generalised quadrangle of order $(7,7)$ is shown there in diagram 7.16. More details on the construction are in [22].

A further immediate generalization of these ideas (see [58] for details) is the use of generalised polygons which were introduced by J. Tits [101]. The girth of the incidence graph of a generalised n-gon is twice its diameter, namely $2n$. As mentioned earlier, this is an indicator for potentially better performance of these codes under iterative decoding algorithms. Please note that the dual incidence structure $GQ^{\perp}(L,P)$, equipped with the inverse incidence, is a generalised quadrangle. If GQ is of order (s,t), then $GQ^{\perp}$ is of order (t,s), but even if $s=t$, this does not imply that these two quadrangles are isomorphic. In recent years, Kim, Mellinger, Pepe, Storme and Van de Voorde [49, 74, 75] found the minimum distance for several of these codes. Please note that the dual incidence structure $GQ^{\perp}(L,P)$, equipped with the inverse incidence, is also a generalised quadrangle. Mellinger investigated LDPC codes from triangle free line sets. These sets are related to caps (see [64]) and generalised quadrangles. He used type-I matrices for his codes while Storme et al ([49, 74, 75]) studied the related type-II matrices. For both cases, examples of codewords of minimum weight were found and characterised. Also the bounds could be explicitly shown by examples.

7.8 Codes Constructed from Inversive Spaces

The main goal of this chapter is to introduce an incidence structure based on inversive spaces and to show the performance of the derived LDPC codes. We start presenting our construction in an inversive plane and will then move on to higher dimensions.

Inversive Planes

We will use the incidence structure consisting of pencils (see Chapter 1, Definition 1.20) and circles of an inversive plane. This way we can take advantage of a characteristic of inversive planes of even order (see Chapter 1, Theorem 1.22): there are no three circles touching pairwise in three different points. This characteristic ensures that the girth of the Tanner graph (see Definition 7.6) for our codes is at least 8.

Corollary 7.12 *The pencils and circles of an inversive plane of even order m form an incidence structure with the following incidence: we say that a circle and a pencil are incident when the circle is an element of the pencil. Then the incidence matrix H has the following properties:*

- *H is a $(m(m^2+1) \times (m^2+1)(m+1))$ matrix.*
- *The row weight is $\rho = m+1$, and the column weight is $\gamma = m$. The density is $\delta = \frac{1}{m^2+1}$.*
- *Two rows can have at most one 1 entry in the same place.*

Thus H is an LDPC matrix.

Proof: An inversive plane has $m(m^2+1)$ circles and every point is carrier of $m+1$ different pencils. Every circle is an element of $m+1$ pencils and a pencil consists of m circles. Two different pencils can share at most one circle, two circles can be in at most one pencil. □

Inversive Spaces

We will base the LDPC codes discussed in the following on the inversive spaces (see Definition 1.33 in Chapter 1) constructed in Example 1.34 in Chapter 1. In the case of an inversive space of even order, or when the dimension u and the order m are both odd (see Theorem 7.17 below), we can construct a $(0,1)$-geometry (see Definition 1.14 in Chapter 1) and derive a parity-check matrix directly as the incidence matrix of this geometry. Note that the properties of these LDPC codes result from the structure of the given inversive space; non-isomorphic classes of inversive spaces might give rise to differently behaving LDPC codes.

Then $\mathbb{M}$ forms a 3-design with parameters $(m^u+1, m+1, 1)$. Thus an inversive space of dimension u contains exactly m^u+1 points. Each point is incident with exactly $m^{u-1}\frac{m^u-1}{m-1}$ circles, and for this reason $\mathbb{M}$ contains $m^{u-1}\frac{m^{2u}-1}{m^2-1}$ circles.

Again, as in inversive planes, also in inversive spaces of even order or when the dimension and the order are both odd there holds: two distinct pencils have at most one circle in common.

The next step will be to thin out the pencils to partial pencils and test the new codes for their performance.

Lemma 7.13 *Let $\mathbb{M} = (P, C)$ be an inversive space of order m, let P be one of its points, and let U be an affine subspace of dimension $v \geq 1$ of $\mathbb{M}_P$. For a circle c that contains P and the pencil $\pi(P,c)$, consider*

$$\pi_U(P,c) \;:=\; \{v \in \pi(P,c) \mid v \setminus \{P\} \subseteq U\}.$$

If $\pi_U(P,c) \neq \emptyset$, then it contains m^{v-1} elements.

Proof: In $\mathbb{M}_P$, the set $\{l \setminus \{P\} \mid l \in \pi(P,c)\}$ forms a full parallel class of lines. If U is a v-dimensional affine subspace of $\mathbb{M}_P$, then either no lines of this class are fully contained in U, or exactly m^{v-1} such lines. □

Definition 7.14 In an inversive space $\mathbb{M}$, let P be a point and let c be a circle such that $P \in c$. A subset $\sigma \subset \pi(P,c)$ is called a *partial pencil of degree v*, if there is a v-dimensional affine subspace of $\mathbb{M}_P$ such that $\sigma = \pi_U(P,c)$.

Remark 7.15 (a) In an u-dimensional inversive space, every pencil is a partial pencil of degree u.

(b) For every circle c of an inversive space, the set $\{c\}$ is a partial pencil of degree 1.

The fact that two circles are tangent in a point can also be used to define the *touching* relation in $\mathbb{M}(\mathbb{L}:\mathbb{K})$, which can be nicely expressed in terms of the cross-ratio (see Definition 1.26 in Chapter 1).

Lemma 7.16 *Let c, d be circles in $\mathbb{M}(\mathbb{L}:\mathbb{K})$ that both contain the point P. Then c and d touch in P if and only if for all $A, A' \in c \setminus \{P\}$ and $B, B' \in d \setminus \{P\}$ there holds*

$$\begin{bmatrix} P & A \\ B & A' \end{bmatrix} - \begin{bmatrix} P & A \\ B' & A' \end{bmatrix} \in \mathbb{K}.$$

For details see [4, p. 114].

It is easy to see that if c is defined by the points $P = \mathbb{L}(0,1)$, $A = \mathbb{L}(1,0)$ and $A' = \mathbb{L}(1,1)$ and d by the points P, $B = \mathbb{L}(1,s)$ and $B' = \mathbb{L}(1,t)$ then c and d touch in P if and only if $s - t \in \mathbb{K}$. We will refer to this in the next proof.

We need one further element of preparation. For the proof of the following statement the author is indebted to A. Blokhuis.

Theorem 7.17 *Let $\mathbb{M} = \mathbb{M}(\mathbb{L}:\mathbb{K})$ be an inversive space of dimension u and order m. If m is even, or m and u are odd, and π is a pencil in $\mathbb{M}$ and c a circle that does not belong to π, then there exists at most one circle $c' \in \pi$ that touches c.*

Proof: Without loss of generality we may assume that we have two circles c, c' of a pencil with carrier $P = \mathbb{L}(0,1)$, and that both touch a circle e that does not belong to this pencil. From Chapter 1, Theorem 1.32, we may further assume that c contains the points $A = \mathbb{L}(1,0)$ and $A' = \mathbb{L}(1,1)$, that c' contains the points $B = \mathbb{L}(1,t)$ and $B' = \mathbb{L}(1,t+1)$ where $t \notin \mathbb{K}$. Finally, we may assume that e contains the points A, B and $U = \mathbb{L}(1,t')$. Evaluating the corresponding cross-ratios (see Definition 1.26 in Chapter 1), we conclude from c touching e in A that $tt'/(t-t') \in \mathbb{K}$. Likewise, we obtain from c' touching e in B that $t(t'-t)/t' \in \mathbb{K}$, but then the product of these numbers which is given by $-t^2$ must be contained in $\mathbb{K}$. If m is even, this means $t \in \mathbb{K}$, a contradiction. If m and u are odd, then $t \in \mathbb{L}$ and $t^2 \in \mathbb{K}$ again implies $t \in \mathbb{K}$, which is a contradiction. Altogether the claim follows. □

An equivalent statement within an inversive plane is: there do not exist three circles in $\mathbb{M}$ which touch each other pairwise in different points. For this statement we refer to Theorem 1.22 in Chapter 1.

We now apply the same construction as before in Corollary 7.12: first we will use an inversive space of even order to construct a $(0,1)$-geometry $\mathbb{S}$, then we will take the incidence matrix of this geometry $\mathbb{S}$ as the parity-check matrix H for the LDPC code.

Theorem 7.18 *Let $\mathbb{M} = (P, C)$ be an inversive space of even order. We define an incidence structure $\mathbb{S} := (\Pi_v, C)$ by*

$$\Pi_v := \{\pi \mid \pi \text{ is a partial pencil of degree } v \text{ in } \mathbb{M}\},$$

where $\pi \in \Pi_v$ is incident with $c \in C$ if and only if $c \in \pi$. Then $\mathbb{S}$ is a $(0,1)$-geometry of order $(m-1, m^{v-1}-1)$.

Proof: This follows directly from Definition 7.14 and Theorem 7.17. □

Now, we first observe that the number of lines in the $(0,1)$-geometry $\mathbb{S}$ over the inversive space of order m and dimension u is equal to

$$k \;=\; \frac{m^{2u}-1}{m^2-1}\, m^{u-1}$$

and the number of partial pencils of degree v is given by

$$n \;=\; \frac{m^{u}-1}{m-1}\, m^{u-v}(m^u+1).$$

As before, we have the incidence matrix $H^{(1)}$, a $(k \times n)$-matrix, and the $(n \times k)$-incidence matrix $H^{(2)}$. The ratio $k/n = \frac{m^{u-1}}{m+1}$ is larger than 1 iff $u \geq 3$. Therefore, for $u = 2$, we take $H^{(1)}$ as parity-check matrix; this type-I LDPC code has length n and a target rate of $1-k/n = 1/(m+1)$. For higher dimensions typically only the type-II LDPC codes, checked by $H^{(2)}$, are of interest. These LDPC codes have length k, a target rate of $1 - n/k = 1 - \frac{m+1}{m^{v-1}}$, and a minimum distance of at least $m+2$.

Example 7.19 Let $\mathbb{M}(GF(4) : GF(2))$ be the smallest Möbius space of order 2 and dimension 2. Then the induced $(0,1)$-geometry $\mathbb{S}(\mathbb{M})$ has 15 points and 10 lines. The derived parity-check matrix $H^{(1)}$ is given by

$$H^{(1)} \;=\; \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}.$$

This matrix checks a binary $[15, 6, 5]$-code as the rank of $H^{(1)}$ is 9 rather than 10.

7.9 Waterfall Diagrams

The first diagram shows the performance of an LDPC code constructed from a projective geometry. This code is equivalent to a cyclic code, which eases encoding.

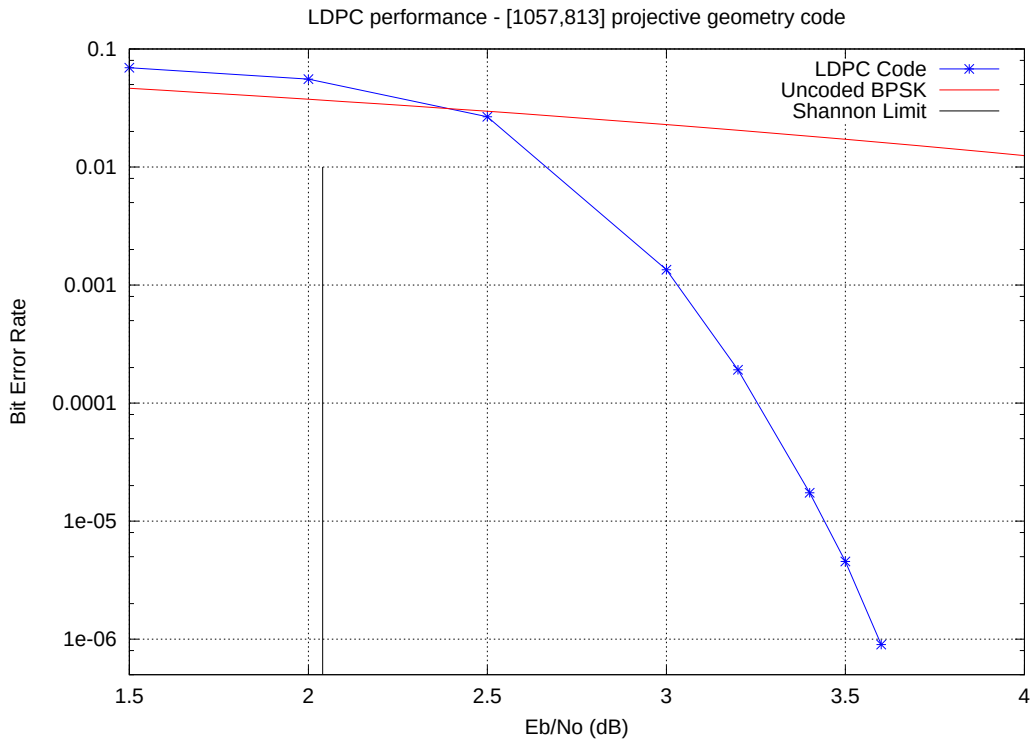

Figure 7.15: LDPC code from a projective geometry

A code constructed from a generalised quadrangle as discussed in Section 7.7 is shown in Figure 7.16. The generalised quadrangle is of order 7 and thus the code obtained is a $[400, 175, 116]$-code which performs as shown.

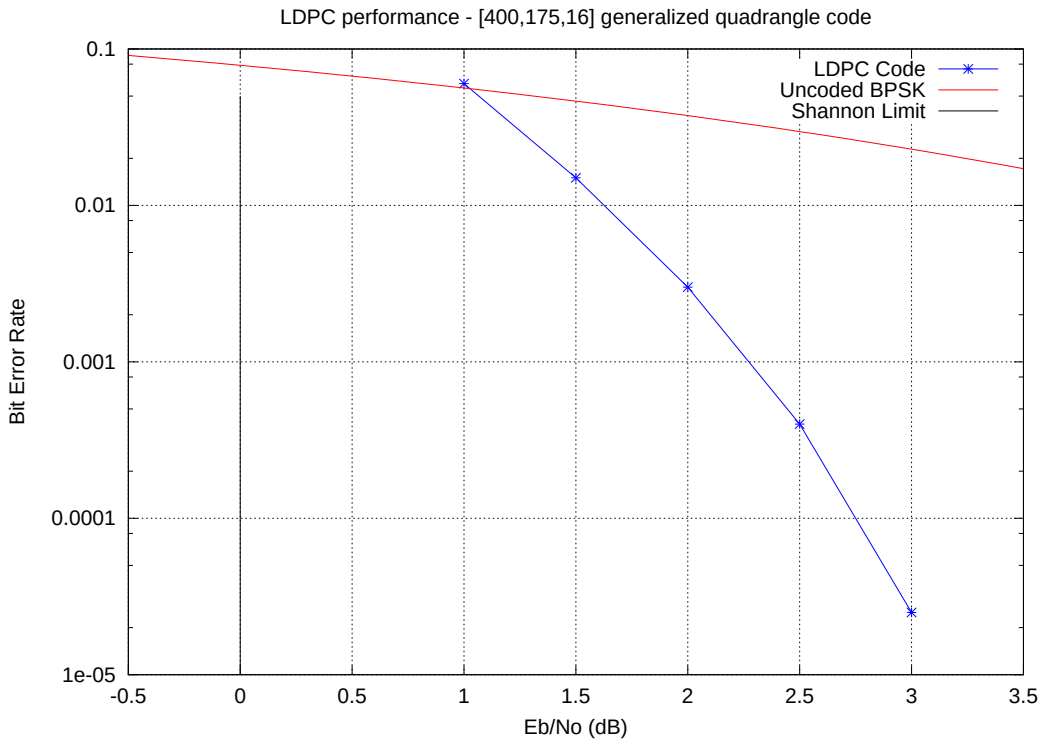

Figure 7.16: LDPC code from the generalised quadrangle of order 7

The first set of results is from an LDPC code constructed using an inversive space of dimension $n = 5$ and order $m = 2$. This yields a 1023×5456 parity-check matrix with a rank of 1008. The Tanner graph has a girth of 10 and a diameter of 6. The bit error rate (BER) performance of this $(5456, 4448)$ LDPC code is shown in Figure 7.17. The performance of this code is 1.15 dB from the Shannon limit at a BER of 10^{-6}.

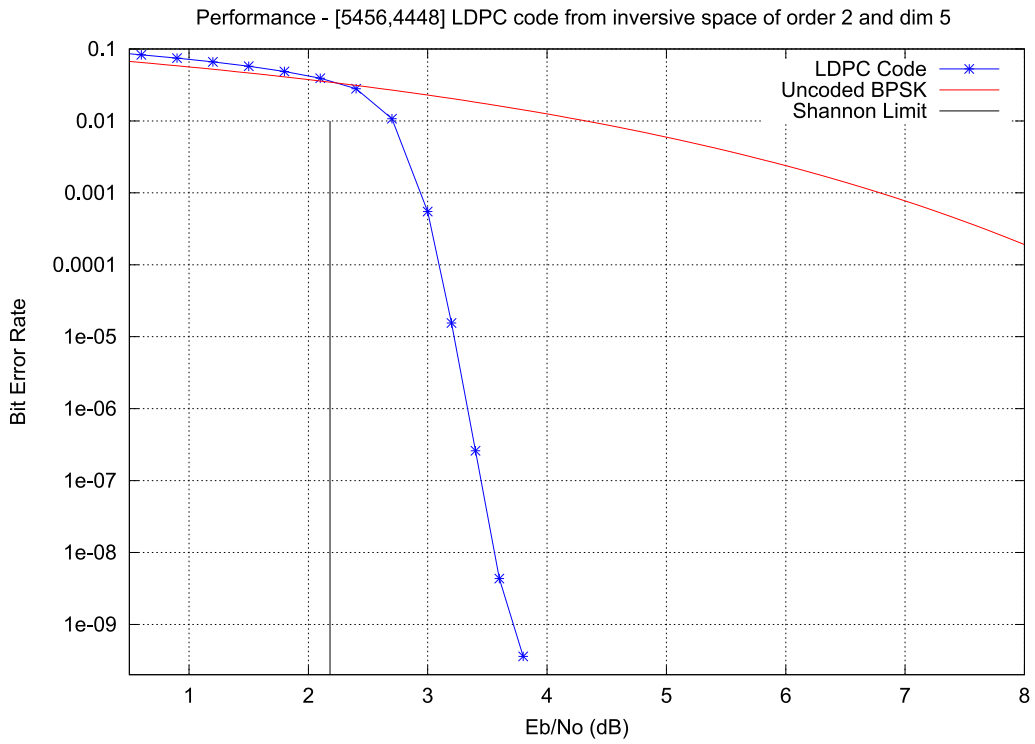

Figure 7.17: LDPC code from an inversive space of dimension 5

The second set of results shows the performance of an LDPC code constructed via an inversive space of order $m = 2$ and dimension $u = 6$. This diagram shows a performance of only 0.7 dB from the Shannon limit at a BER of 10^{-7}.

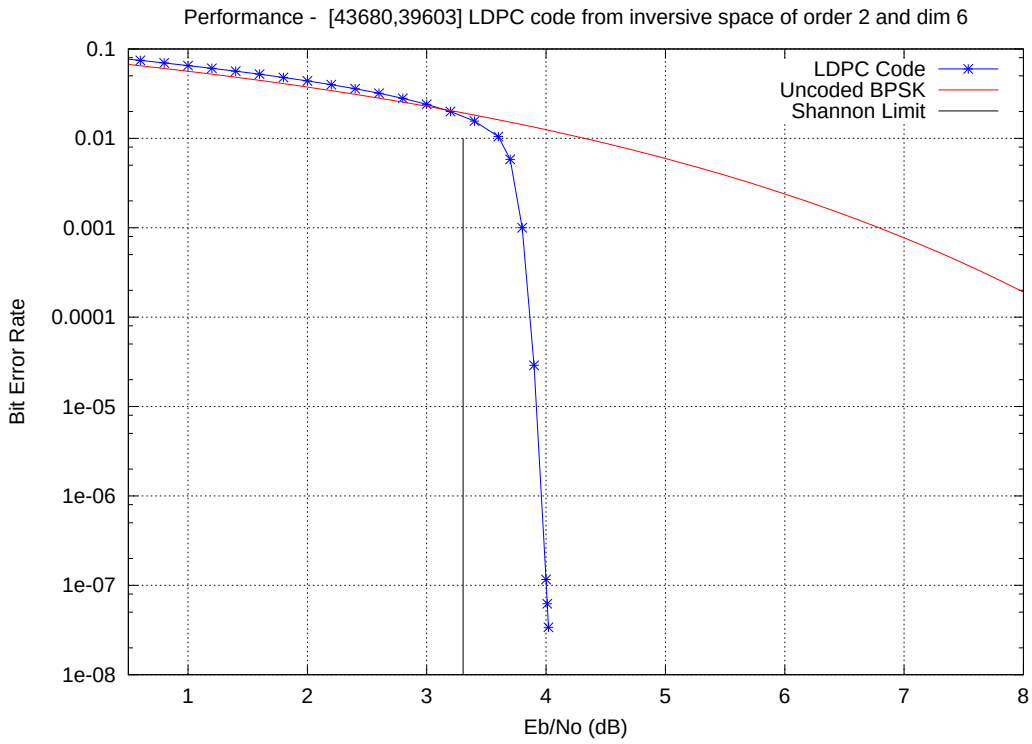

Figure 7.18: LDPC code from an inversive space of dimension 6

Bibliography

[1] A. Aguglia, G. L. Ebert, and D. Luyckx, *On partial ovoids of Hermitian surfaces*, Bull. Belg. Math. Soc. Simon Stevin **12** (2005), 641–650.

[2] E. Artin, *Geometric Algebra*, Wiley, New York, 1988.

[3] A. Barlotti, *Un' estensione del teorema di Segre–Kustaanheimo*, Boll. Un. Mat. Ital. **10** (1955), 96–98.

[4] W. Benz, *Über Möbiusebenen*, Jhber. D.M.V. **63** (1960), 1–27.

[5] W. Benz, *Geometrie der Algebren*, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[6] L. Berardi, F. Eugeni, and O. Ferri, *Sui Blocking Sets Nei Sistemi Di Steiner*, Bollettino U.M.I. Algebra e Geometria Serie VI, Vol. III-D, No. 1 (1984).

[7] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Trans. Inf. Theory, IT-**24** (1978), 384–386.

[8] J. De Beule, *Blocking sets and partial spreads in finite polar spaces*, PhD Thesis, Ghent University, Belgium 2004.

[9] J. De Beule and A. Gács, *Complete arcs on the parabolic quadric* $\mathcal{Q}(4,q)$, Finite Fields Appl. **14** (2008), no. 1, 14–21.

[10] A. Beutelspacher, *Einführung in die endliche Geometrie II*, BI Wissenschaftsverlag, Mannheim 1983.

[11] A. Beutelspacher, *Kryptologie*, Verlag Vieweg, Wiesbaden, 1993.

[12] A. Beutelspacher and U. Rosenbaum, *Projektive Geometrie: Von den Grundlagen bis zu den Anwendungen*, Verlag Vieweg, Wiesbaden, 1992.

[13] R. E. Blahut, *Theory and practice of error control codes*, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983.

[14] A. Blunck and A. Herzer, *Kettengeometrien*, Shaker Verlag, Aachen, 2005.

[15] J. Bond, S. Hui, and H. Schmidt, *Linear-congruence constructions of low-density parity-check codes*, in Codes, systems, and graphical models (Minneapolis, MN, 1999), 2001.

[16] R. C. Bose and R. C. Burton, *A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the McDonald codes*, J. Combin. Theory **1** (1966), 96-104.

[17] M. R. Brown, J. De Beule, and L. Storme, *Maximal partial spreads of $T_2(\mathcal{O})$ and $T_3(\mathcal{O})$*, European J. Combin. **24** (2003), no. 1, 73–84.

[18] R. H. Bruck, *Construction Problems of Finite Projective Planes*, Proceedings of the Conference in Combinatorics held at the University of North Carolina at Chapel Hill **10.-14.** Apr. 67, Univ. of North Carolina Press (1969), 426–514.

[19] A. A. Bruen, *Blocking sets and skew subspaces of projective space*, Canad. J. Math. **32** (1980), 628–630.

[20] A. A. Bruen and B. L. Rothschild, *Lower bounds on blocking sets*, Pacific J. Math. **118** (1985), 303–311.

[21] A. A. Bruen and J. A. Thas, *Hyperplane coverings and blocking sets*, Math. Z. **181** (1982), 407–409.

[22] F. Buekenhout, ed., *Handbook of incidence geometry*, North-Holland, Amsterdam, 1995.

[23] M. Cimráková and V. Fack, *Clique algorithms for finding substructures in generalized quadrangles*, J. Combin. Math. and Combin. Computing, to appear.

[24] M. Cimráková, S. De Winter, V. Fack, and L. Storme, *On the smallest maximal partial ovoids and spreads of the generalized quadrangles $W(q)$ and $Q(4,q)$*, European J. Combin. **28** (2007), 1934–1942.

[25] H. S. M. Coxeter, *Projective Geometry*, Springer-Verlag, New York, 1987.

[26] H. S. M. Coxeter, *The Real Projective Plane*, Springer-Verlag, New York, 1993.

[27] H. S. M. Coxeter, *The inversive plane and hyperbolic space*, Abh. Hamburg **29** (1966), 217–242.

[28] H. S. M. Coxeter, *Geometry Revisited*, New Mathematical Library 19, The Mathematical Association of America, Washington, 1967.

[29] P. Dembowski, *Möbiusebenen gerader Ordnung*, Math. Ann. **157** (1964), 179–205.

[30] P. Dembowski, *Automorphismen endlicher Möbius-Ebenen*, Math. Z. **87** (1965), 115–136.

[31] P. Dembowski, *Finite Geometries*, Ergebnisse der Mathematik und ihrer Grenzgebiete **44**, Springer Berlin, 1968.

[32] G. L. Ebert and J. W. P. Hirschfeld, *Complete systems of lines on a Hermitian surface over a finite field*, Des. Codes Cryptogr. **17** (1999), 253–268.

[33] http://www.encyclopediaofmath.org

[34] V. Fack, Sz. L. Fancsali, L. Storme, G. Van de Voorde, and J. Winne, *Small weight codewords in the codes arising from Desarguesian projective planes*, Des. Codes Cryptogr. **46** (2008), 25–43.

[35] M. Flanagan, M. Greferath, and C. Rößing, *On LDPC codes from* $(0,1)$*-geometries induced by finite inversive spaces of even order*, in Proceedings of the WCC 2007, Versailles, 2007.

[36] Z. Füredi, *Matchings and covers in hypergraphs*, Graphs and Combin. **4** (1988), 115–206.

[37] R. Gallager, *Low density parity check codes*, MIT press, Cambridge, MA, 1963.

[38] A. Gács and T. Szőnyi, *On Maximal Partial Spreads in PG(n,q)*, Des. Codes Cryptogr. **29**, (2003), 123–129.

[39] M. Greferath and C. Rößing, *On the cardinality of intersection sets in inversive planes.* J. Combin. Theory Ser. A **100** (2002), no. 1, 181–188.

[40] M. Greferath, C. Rößing, and L. Storme, *Galois Geometries and Low-Density Parity-Check Codes*, Chapter 10 in *Current Research Topics in Galois Geometry* (J. De Beule and L. Storme, Eds.), NOVA Academic Publishers (2012), 245–270.

[41] J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, 1985.

[42] J. W. P. Hirschfeld, *Projective Geometry over Finite Fields*, Oxford Mathematical Monographs, Oxford University Press, New York, 1998.

[43] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, *Developments in Mathematics*, Vol. **3**, Kluwer Academic Publishers *Finite Geometries*, Proceedings of the *Fourth Isle of Thoms Conference* (Chelwood Gate, July 16.–21. 2000) (Eds. A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas), 201–246.

[44] J. W. P. Hirschfeld and J. A. Thas *General Galois Geometries*, Oxford Sci. Publ., Clarendon Press, 1991.

[45] S. Innamorati and A. Maturo, *On irreducible blocking sets in projective planes*, Ratio Math. **2** (1991), 151–155.

[46] S. J. Johnson and S. R. Weller, *Codes for iterative decoding from partial geometries*, in Proc. IEEE Int. Sym. Inform. Theory, Switzerland, June 30-July 5, 2002.

[47] J. Kahn, *Finite inversive Planes satisfying the bundle Theorem*, Geom. Dedicata **12** (1982), 171–187.

[48] J. Kahn, *Inversive Planes satisfying the bundle Theorem*, J. Combin. Theory, Ser. A **29** (1980), 1–19.

[49] J.-L. Kim, K. E. Mellinger, and L. Storme, *Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles*, Des. Codes Cryptogr. **42** (2007), 73–92.

[50] H.-J. Kroll and S. G. Taherian, *Bemerkungen zum Beweis des Darstellungssatzes für miquelsche Möbius-Ebenen von A. Lenard*, Abh. Math. Sem. Univ. Hamburg **69** (1999), 159–166.

[51] Y. Kou, S. Lin and M. P. C. Fossorier, *Low Density Parity Check Codes Based on Finite Geometries: A Rediscovery*, Proc. 2000 IEEE Int. Symp. Inf. Theory, Sorrento, Italy, June 25-30, 2000.

[52] Y. Kou, S. Lin, and M. P. C. Fossorier, *Low Density Parity Check Codes: Construction Based on Finite Geometries*, Global Telecom. Conf. 2000, GLOBECOM '00 IEEE **2** (2000), 825-829.

[53] Y. Kou, S. Lin, and M. P. C. Fossorier, *Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results*, IEEE Trans. Inform. Theory **47** (2001), 2711–2736.

[54] S. Lang, *Algebra Third Edition*, Addison-Wesley Publishing Company, 1993.

[55] A. Lenard, *Ein neuer Beweis des Darstellungssatzes für Miquelsche Möbius-Ebenen*, Abh. Math. Sem. Univ. Hamburg **65** (1995), 57–82.

[56] X. Li, C. Zhang, and J. Shen, *Regular LDPC codes from semipartial geometries*, Acta Appl. Math **102** (2008), 25–35.

[57] S. Lin, H. Tang, and Y. Kou, *On a Class of Finite Geometry Low Density Parity Check Codes*, ISIT 2001, Washington DC, June 24–29, 2001.

[58] Z. Liu and D. A. Pados, *LDPC codes from generalized polygons*, IEEE Trans. Inform. Theory **51** (2005), 3890–3898.

[59] D. MacKay, *Good Error-Correcting Codes Based on Very Sparse Matrices*, IEEE Trans. Inform. Theory **45**, No. 2 (1999), 399–431.

[60] D. MacKay and R. Neal, *Good codes based on very sparse matrices*, in Cryptography and Coding, 5th IMA Conference, 1995, 100–111.

[61] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1978.

[62] G. Margulis, *Explicit constructions of graphs without short cycles and low density codes*, Combinatorica **2** (1982), 71–78.

[63] J. L. Massey, *Threshold decoding*, Massachusetts Institute of Technology, Research Laboratory of Electronics, Tech. Rep. **410**, Cambridge, Mass., 1963.

[64] K. E. Mellinger, *LDPC codes from triangle-free line sets*, Des. Codes Cryptogr. **32** (2004), 341–350.

[65] K. Metsch and L. Storme, *Tangency sets in* $PG(3,q)$, J. Combin. Des. **16** (2008), 462–476.

[66] C. Mitchell and F. Piper, *The Cost of Reducing Key-Storage Requirements in Secure Networks*, Computers and Security **6** (1987), 339–341.

[67] C. Mitchell and F. Piper, *Key Storage in Secure Networks*, Discrete Applied Math. **21** (1988), 215–228.

[68] C. Mitchell and F. Piper, *Combinatorial Techniques for Key Storage Reduction in Secure Networks*. Hewlett-Packard Laboratories, Technical Memo, 1987.

[69] A. F. Möbius, *Der barycentrische Calcul* (Nachdruck), Georg Olms Verlag Hildesheim - New York, 1976.

[70] A. Orlitsky, R. Urbanke, K. Vishwanathan, and J. Zhang, *Stopping sets and the girth of Tanner graphs*, in Proc. IEEE International Symposium on Information Theory, Lausanne, Switzerland, 2002, 2.

[71] M. O'Sullivan, M. Greferath, and R. Smarandache, *Construction of LDPC codes from affine permutation matrices*, in Proceedings of the 40th Annual Allerton Conference on Communication, Control and Computing, 2002.

[72] S. E. Payne and J. A. Thas, *Finite generalized quadrangles*, EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, second ed., 2009.

[73] V. Pepe, C. Rößing, and L. Storme, *A spectrum result on maximal partial ovoids of the generalized quadrangle $Q(4,q)$, q odd*. Finite fields: theory and applications, 349–362, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

[74] V. Pepe, L. Storme, and G. Van de Voorde, *Small weight codewords in the LDPC codes arising from linear representations of geometries*, J. Combin. Des. **17** (2009), 1–24.

[75] V. Pepe, L. Storme, and G. Van de Voorde, *On codewords in the dual code of classical generalized quadrangles and classical polar spaces*, Discr. Math. **310** (2010), 3132–3143.

[76] O. Polverino and L. Storme, *Small minimal blocking sets in $PG(2,p^3)$*, European J. Combin. **23** (2002), 83-92.

[77] K. A. S. Quinn, *Combinatorial Structures with Applications to Information Theory*, PhD Thesis, RHBNC, University of London, 1991.

[78] B. Qvist, *Some remarks concerning curves of the second degree in a finite plane*, Ann. Acad. Sci. Fenn. **134** (1952), 1-27.

[79] R. Hill, *A First Course in Coding Theory*, Clarendon Press Oxford, ISBN 0198538030.

[80] T. J. Richardson and R. L. Urbanke, *Efficient encoding of low-density parity-check codes*, IEEE Trans. Inform. Theory **47** (2001), 638–656.

[81] J. Rosenthal and P. Vontobel, *Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis*, in Proc. of the 38th Allerton Conference on Communication, Control, and Computing (2000), 248–257.

[82] C. Rößing, *On subplanes of Miquelian inversive planes*. J. Geom. **91** (2009), no. 1-2, 140–149.

[83] C. Rößing and L. Storme, *A spectrum result on maximal partial ovoids of the generalized quadrangle $\mathcal{Q}(4,q)$, q even*, European J. Combin. **31** (2010), 349-361.

[84] C. Rößing and L. Storme, *A spectrum result on minimal blocking sets with respect to the planes of $PG(3,q)$, q odd*, Des. Codes Cryptogr. **55** (2010), 2-3, 107-119.

[85] E. M. Schröder, *Vorlesungen über Geometrie*, Band 1: Möbiussche, elliptische und hyperbolische Ebenen. BI-Wissenschafts-Verlag, Mannheim, 1991.

[86] B. Segre, *Ovals in a finite projective plane*, Canad J. Maths. **7** (1955) 414-416.

[87] B. Segre, *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, Acta Arith. **5** (1959), 315-332.

[88] C. E. Shannon, *A mathematical theory of communication*, Bell System. Tech. J. **27** (1948), 379-423, 623-656.

[89] L. Storme, *Projective Geometry and Coding Theory*, Combinatorial and Computational Center Pohang University of Science and Technology, 2003.

[90] L. Storme and T. Szőnyi, *Intersection of arcs and normal rational curves in spaces of even characteristic*, J. Geom. **51** (1994), 150–166.

[91] L. Storme and Zs. Weiner, *On 1-blocking sets in PG(3,q), $n \geq 3$*, Des. Codes Cryptogr. **21** (2000), 235–251.

[92] P. Sziklai, *On small blocking sets and their linearity*, J. Combin. Theory, Ser. A **115** (2008), 1167–1182.

[93] T. Szőnyi, *Blocking sets in Desarguesian affine and projective planes*, Finite Fields Appl. **3** (1997), 187–202.

[94] T. Szőnyi, A. Cossidente, A. Gács, C. Mengyán, A. Siciliano, and Zs. Weiner, *On Large Minimal Blocking Sets in $PG(2, q)$*, J. Combin. Des. **13** (2005), 25–41.

[95] T. Szőnyi and Zs. Weiner, *Small blocking sets in higher dimensions*, J. Combin. Theory, Ser. A **95** (2001), 88–101.

[96] H. Tang, J. Xu, Y. Kou, S. Lin, and K. Abdel-Ghaffar, *On algebraic construction of Gallager and circulant low-density parity-check codes*, IEEE Trans. Inform. Theory **50** (2004), 1269–1279.

[97] R. M. Tanner, *A recursive approach to low complexity codes*, IEEE Trans. Inform. Theory **27** (1981), 533–547.

[98] D. E. Taylor, *The Geometry of the Classical Groups*. Heldermann Verlag, Berlin, 1992.

[99] J. A. Thas, *Old and new results on spreads and ovoids of finite classical polar spaces*, Combinatorics '90 (Gaeta, 1990), Ann. Discrete Math. **52** (1992), 529-544.

[100] J. A. Thas, *Ovoids, spreads and m-systems of finite classical polar spaces*, Survey in combinatorics, (2001) (Sussex), 241–267, London Math. Soc. Lecture Note Ser. **288**, Cambridge Univ. Press, Cambridge (2001).

[101] J. Tits, *Ovoides et groupes de Suzuki*, Arch. Math. **13** (1962), 187–198.

[102] J. Tits, *Buildings of spherical type and finite BN-pairs*. Springer-Verlag, Berlin, 1974. Lecture Notes in Mathematics, Vol. **386**.

[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.

[104] P. Vontobel, *http://www.pseudocodewords.info*.

[105] P. Vontobel, R. Smarandache, N. Kiyavash, J. Teutsch, and D. Vukobratovic, *On the minimal pseudo-codewords of codes from finite geometries*, in Proc. IEEE Intern. Symp. on Inform. Theory 2005, Adelaide, Australia, 2005, 980–984.

[106] P. Vontobel and R. Tanner, *Construction of codes based on finite generalized quadrangles for iterative decoding*, in Proc. IEEE Intern. Symp. on Inform. Theory, Washington, D.C., USA, 2001, 223.

[107] B. L. van der Waerden and L. J. Smid, *Eine Axiomatik der Kreisgeometrie und der Laguerregeometrie*, Math. Ann. **110** (1935), 753–776.

[108] N. Wiberg, *Codes and Decoding on General Graphs*, PhD thesis, Linköping University, Sweden, 1996.

[109] J. Xu, H. Tang, Y. Kou, S. Lin, and K. Abdel-Ghaffar, *A General Class of LDPC Finite Geometry Codes and their Performance*, ISIT 2002, Lausanne, Switzerland, June 30-July 5, 2002.