PhD thesis

BLOCKING SETS IN FINITE PROJECTIVE SPACES

Nóra Viola Maloschikné Harrach

Supervisor:

Tamás Szőnyi
Professor, DSc

PhD School of Mathematics
School Leader: Miklós Laczkovich
Professor, Member of the Hungarian Academy of Sciences

Theoretical Mathematics Programme
Head of the programme: András Szűcs
Professor, Corresp. Member of the Hungarian Academy of Sciences

Department of Computer Science
Faculty of Science, Eötvös Loránd University,
Budapest, Hungary

2013

Contents

Introduction **5**

Overview 5

Acknowledgments 6

1 Preliminary results **7**

1.1 Definitions, notation 7

1.2 Projections in $\mathrm{PG}(n, q)$ 8

1.3 Linear point sets 9

1.4 Blocking sets 10

1.5 Blocking sets of Rédei type 11

1.6 Small minimal blocking sets 13

1.7 Multiple blocking sets 18

2 Small point sets of $\mathrm{PG}(n, q^3)$ intersecting each k-space in $1 \bmod q$ points **21**

2.1 The main theorem 21

2.2 $\mathrm{GF}(q)$-linear blocking sets of $\mathrm{PG}(n, q^3)$ 23

2.3 Proof of Theorem 2.1.1 for $k = 1$, $n = 3$ 30

2.4 Proof of Theorem 2.1.1 for $k = 1$, $n \geq 4$ 41

2.5 Proof of Theorem 2.1.1 for $1 < k < n$, $n \geq 3$ 45

2.6 Blocking sets PG$(6, q)$ in PG(n, q^3) 53

3 Unique reducibility of multiple blocking sets 61

3.1 The main theorem 61

3.2 t-fold $(n-k)$-blocking sets which contain two minimal t-fold $(n-k)$-blocking sets 62

3.3 t-fold nuclei 64

3.4 Proof of Theorem 3.1.3 68

3.5 Examples 71

3.5.1 The case $t = 1$ 71

3.5.2 The case $t \geq 2$ 72

4 Generalizing the Megyesi construction 75

4.1 Placing the cosets on three lines 75

4.2 Placing the cosets on $n \geq 4$ lines 82

4.3 Constructions in PG$(2, q^h)$ 85

Bibliography 89

This thesis is based on 89

Further refrences 92

Magyar nyelvű összefoglaló 93

Magyar nyelvű összefoglaló 95

Introduction

Overview

In this thesis we present results about blocking sets in the finite projective space $\mathrm{PG}(n, q)$. The results presented here are based on articles [1] [2], [3] and [4].

In Chapter 1 the notation, definitions, and most important preliminary results are presented. We aim at using standard notation.

Chapter 2 deals with small minimal $(n-k)$-blocking sets of $\mathrm{PG}(n, q)$. These blocking sets are of special interest, as there is hope to characterize them. Sziklai's Linearity Conjecture claims that all small minimal $(n-k)$-blocking sets are linear. Szőnyi and Weiner prove in [45] that small minimal $(n-k)$-blocking sets meet every k-space in 1 mod p points, where $q = p^h$ is the order of the projective space. It is also proved that the sizes of small minimal blocking sets are contained in disjoint intervals. In Chapter 2 we prove the Linearity Conjecture in one of these intervals. The proof is separated into 3 cases ($n = 3$, $k = 1$; $n \geq 4$, $k = 1$ and $n \geq 3$, $k \geq 2$) and a section is devoted to every case. The first two cases are solved by the same method, while the last case is solved by a slightly different technique. Section 2.2 collects some properties of linear point sets of the projective space, and Section 2.6 gives a classification of a class of blocking sets in $\mathrm{PG}(3, q^3)$.

In Chapter 3 we turn our attention to multiple blocking sets. In a multiple blocking set one can always find a minimal multiple blocking set by throwing away the points that are not necessary to the set. In this chapter we prove that if B is a weighted t-fold $(n-k)$-blocking set of $\mathrm{PG}(n, q)$ with size at most $(t+1)q^{n-k} + q^{n-k-1} + \cdots + q + 1$, then the minimal t-fold $(n-k)$-blocking set contained in B is unique. Our result is a generalization of the one given by Szőnyi in [43] and of a result by Lavrauw, Storme and Van de Voorde in [29]. Examples of the last section show that our result is sharp in certain cases.

In Chapter 4 planar blocking set constructions are presented. The first construction is a generalization of the Megyesi construction and also of a construction given by Gács in [22]. We consider $\mathrm{PG}(2, q)$ as $\mathrm{AG}(2, q) \cup \ell_\infty$. A set of q points is selected in $\mathrm{AG}(2, q)$ with the aid of a subgroup of the multiplicative group $\mathrm{GF}(q)^*$, and the ideal points determined by the set are added, which make it a minimal blocking set. The size of the resulting set is estimated, and some examples are given for sizes which can be achieved. The blocking set constructed this way will have the property that it is contained in the union of 4 lines, three of which are concurrent. The next construction of Chapter 4 is a generalization of the first to more than 4 lines. The resulting blocking set is contained in the union of $n + 1$ lines, precisely n of which are concurrent. The last section of this chapter presents two constructions which produce blocking sets of $\mathrm{PG}(2, q^h)$ starting from a blocking set of $\mathrm{PG}(2, q)$.

Acknowledgments

Above all, I am most grateful to my supervisor Tamas Szőnyi for all his help and encouragement throughout the years of my doctoral studies, and in writing this thesis. I am very grateful to Leo Storme and Klaus Metsch for the joint work, and for their kind hospitality when visiting Ghent University and the Justus-Liebig-Universität Gießen. I would like to thank my co-authors Zsuzsa Weiner and Csaba Mengyán for the joint work. My work was funded by the Hungarian National Foundation for Scientific Research (OTKA) grants T 67867 and K 81310. I am also grateful to the Alfréd Rényi Institute of Mathematics for providing excellent working conditions.

Chapter 1

Preliminary results

In this chapter we will introduce the geometrical objects and the most important results that will be used in the following chapters. For more details, please turn to books [26], [25] and [27].

1.1 Definitions, notation

In this thesis we will mostly be working in $\mathrm{PG}(n,q)$ and $\mathrm{AG}(n,q)$, the n-dimensional projective and affine spaces over the Galois field $\mathrm{GF}(q)$, of order q, where $q = p^h$ and p is a prime.

Let $V = V(n+1,q)$ denote the $(n+1)$-dimensional vector space over $\mathrm{GF}(q)$. Then $\mathrm{PG}(n,q)$ can be derived from V, if we view subspaces of V of rank 1 as points, subspaces of rank 2 as lines, subspaces of rank $k+1$ as k-dimensional subspaces, and subspaces of rank n as hyperplanes. A point of $\mathrm{PG}(n,q)$ can be represented by *homogeneous coordinates,* which is any $\neq \mathbf{0}$ vector of the subspace of V of rank 1 corresponding to that point. Thus, if $\lambda \in \mathrm{GF}(q) \setminus \{0\}$, then $(x_1, x_2, \ldots, x_{n+1}) \neq (0, \ldots, 0)$ and $(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1})$ represent the same point.

The number of points of an m-dimensional subspace of $\mathrm{PG}(n,q)$ will be denoted by θ_m, and clearly $\theta_m = \frac{q^{m+1}-1}{q-1} = q^m + q^{m-1} + \cdots + 1$.

If we select a hyperplane H_∞ of $\mathrm{PG}(n,q)$, then $\mathrm{PG}(n,q) \setminus H_\infty$ is an n-dimensional affine space of order q, denoted by $\mathrm{AG}(n,q)$. The points of $\mathrm{AG}(n,q)$ can be represented by affine coordinates $(x_1, x_2, \ldots, x_n)$, with $x_i \in \mathrm{GF}(q)$. A natural correspondence can be defined between the points of $\mathrm{AG}(n,q)$ and the elements of $\mathrm{GF}(q^n)$. With this representation, three points A, B and C of $\mathrm{AG}(n,q)$ are collinear if and only if $(a-b)^{q-1} = (a-c)^{q-1}$ for the corresponding elements $a, b, c \in \mathrm{GF}(q)$. Thus, to every line of $\mathrm{AG}(n,q)$ a θ_{n-1}-st root of unity of $\mathrm{GF}(q^n)$ can be associated, and parallel lines are associated with the same root of unity. This gives a one to one correspondence between the points of H_∞ and the θ_{n-1}-st roots of unity of $\mathrm{GF}(q^n)$.

When $n = 2$, it is more convenient to use the notation (x, y) (or any other two letters) for the points of $\mathrm{AG}(2,q)$. In this case lines can be given by the equations $Y = mX + b$ and $X = c$, where in the first case the *slope* of the line is m, and in the second case we have a vertical line with slope ∞. We will denote by (m) and (∞) the *ideal (or infinite) points* and $l_\infty = \{(m) | m \in \mathrm{GF}(q)\} \cup \{(\infty)\}$ is the *ideal line* or *line at infinity.*

1.2 Projections in $\mathrm{PG}(n,q)$

If a point set $S \subset \mathrm{PG}(n,q)$ with the subsets

$$\{\Sigma \cap S | \Sigma \text{ is a subspace of } \mathrm{PG}(n,q)\}$$

forms a projective space $\mathrm{PG}(n', q')$, then we say that S is an *embedded* $\mathrm{PG}(n', q')$ *subgeometry* in $\mathrm{PG}(n,q)$. The order of the embedded subgeometry is either q, or $\mathrm{GF}(q')$ is a subfield of $\mathrm{GF}(q)$, so $(q')^m = q$ for a certain integer m. If $S = \{(x_1, x_2, \ldots, x_{n+1}) | x_i \in \mathrm{GF}(q')\}$, then S is a *canonical subgeometry* of $\mathrm{PG}(n,q)$. If q is square and $q' = \sqrt{q}$, then the subgeometry is called a *Baer subgeometry* (a *Baer subline* when $n' = 1$, and a *Baer subplane* when $n' = 2$).

If $S_1, S_2, \ldots$ are point sets or subspaces of $\mathrm{PG}(n,q)$ then $\langle S_1, S_2, \ldots \rangle$ will denote the *subspace generated* by $S_1, S_2, \ldots$, which is the meet of all the subspaces of $\mathrm{PG}(n,q)$ containing these sets. For two points P and Q the unique line connecting them can be denoted by $\langle P, Q \rangle$, but often we will simply write PQ.

Let Σ_r be an r-dimensional subspace of $\mathrm{PG}(n,q)$. Consider the vector space V associated to $\mathrm{PG}(n,q)$, and the subspace N of rank $r+1$ associated to Σ_r. Then the projective space defined by the quotient space V/N will be called the *quotient geometry* $\mathrm{PG}(n,q)/\Sigma_r$, and isomorphic to $\mathrm{PG}(n-r-1,q)$. Another way of viewing $\mathrm{PG}(n,q)/\Sigma_r$ is to consider the $(r+1+k)$-dimensional subspaces of $\mathrm{PG}(n,q)$ containing Σ_r as k-dimensional subspaces for $-1 \leq k \leq n-r-2$. If we select an $(n-r-1)$-dimensional subspace Σ_{n-r-1} of $\mathrm{PG}(n,q)$, which is disjoint from Σ_r, then every $(r+1)$-dimensional subspace on Σ_r meets Σ_{n-r-1} in exactly one point. This gives a one to one correspondence between the points of Σ_{n-r-1} and the $(r+1)$-dimensional subspaces on Σ_r. For any point $P \notin \Sigma_r$, the point $P' = \Sigma_{n-r-1} \cap \langle P, \Sigma_r \rangle$ is called the *projection* of P from Σ_r to Σ_{n-r-1}. For any point set $S \subset \mathrm{PG}(n,q) \setminus \Sigma_r$, the set of projected points is the projection of S from Σ_r to Σ_{n-r-1}.

Note that it may happen that more than one points are projected onto the same point. If a point of the resulting set is the image of one point only, then it will be called an *ordinary point* of the projected point set.

If $q = p^h$ and $e|h$, and we choose S to be a canonical subgeometry $S = \mathrm{PG}(s,p^e)$, then the resulting set will be called a *projected* $\mathrm{PG}(s,p^e)$ *subgeometry.* An embedded subgeometry can also be regarded as a projected subgeometry: in this case the vertex of the projection is the empty set, the subspace of dimension -1.

1.3 Linear point sets

Definition 1.3.1 (Lunardon [30], Polito and Polverino [33])**.** Let $\mathrm{GF}(p^e)$ be a subfield of $\mathrm{GF}(q)$.

(a) A point set S of $\mathrm{PG}(n,q)$ is said to be $\mathrm{GF}(p^e)$*-linear*, if there is a projective space $\mathrm{PG}(n',q)$ containing $\mathrm{PG}(n,q)$ such that S is the projection of a subgeometry $\mathrm{PG}(s,p^e) \subset \mathrm{PG}(n',q)$ from a suitable subspace (vertex) onto $\mathrm{PG}(n,q)$.

(b) A point set S of $\mathrm{PG}(n,q)$ is said to be $\mathrm{GF}(p^e)$*-linear*, if the $(n+1)$-dimensional $\mathrm{GF}(q)$ vector space V defining $\mathrm{PG}(n,q)$ has a $\mathrm{GF}(p^e)$-linear subspace W such that a point of $\mathrm{PG}(n,q)$ belongs to S if and only if it is defined by a vector of W.

Result 1.3.2 (Lundardon, Polito, Polverino, [31])**.** *The two definitions above are equivalent.*

Thus, $\mathrm{GF}(p^e)$-linear point sets are exactly the projected $\mathrm{PG}(s, p^e)$ subgeometries. When the subfield and the dimension is obvious, then S will simply be called a linear point set or a projected subgeometry.

The intersection of a subspace of $\mathrm{PG}(n, q)$ and a $\mathrm{PG}(s, p^e)$ projected subgeometry is a $\mathrm{PG}(t, p^e)$ projected subgeometry with $-1 \leq t \leq s$. For the dimensions of these subgeometries the following result holds.

Lemma 1.3.3. *Let $q = (p^e)^m$. If a subspace of dimension k of $\mathrm{PG}(n, q)$ meets a projected $\mathrm{PG}(s, p^e)$ in a projected $\mathrm{PG}(t, p^e)$, then*

$$s - (n - k)m \leq t \leq (k + 1)m - 1.$$

Proof. A k-dimensional subspace can be viewed as $\mathrm{PG}(k, q) \cong V(k + 1, q) \cong V((k+1)m, p^e) \cong \mathrm{PG}((k+1)m-1, p^e)$, so $t \leq (k+1)m-1$. Similarly $\mathrm{PG}(n, q) \cong \mathrm{PG}((n + 1)m - 1, p^e)$, and if a $((k + 1)m - 1)$-dimensional subspace and an s-dimensional subspace of $\mathrm{PG}((n + 1)m - 1, p^e)$ meet in a t-dimensional subspace, then

$$(k + 1)m - 1 + s \leq (n + 1)m - 1 + t,$$

from which the lower bound follows. ■

1.4 Blocking sets

Definition 1.4.1 (Blocking set)**.** A set B of points in $\mathrm{PG}(n, q)$, which intersects each k-dimensional subspace is called an $(n - k)$*-blocking set* or a *blocking set with respect to k-spaces.*

To exclude trivial cases, $0 < k < n$ will always be assumed. When $n = 2$ (and so $k = 1$), blocking sets are called *planar blocking sets.* A 1-blocking set (i.e. a blocking set with respect to hyperplanes) is often simply called a blocking set.

Result 1.4.2 (Bose and Burton, [13])**.** *An $(n-k)$-blocking set of $\mathrm{PG}(n, q)$ has at least θ_k points. In case of equality the $(n-k)$-blocking set is an $(n-k)$-dimensional subspace.*

An $(n - k)$-blocking set containing an $(n - k)$-dimensional subspace is called *trivial.*

A point P of B is *essential* to B, if there exists a k-space through P intersecting B in P only. Such a k-space is called a *tangent* of B at P. The blocking set B is *minimal*, if each point of it is essential.

Following [17] we will call a point P a *critical point* of the blocking set B, if there is exactly one tangent k-space to B at P. Such a subspace then will be called a *critical tangent* of B. If a subspace Σ meets B in t points, then we say that Σ is a *t-secant* of B.

Result 1.4.3 (Bruen, [15, 16])**.** *In* $\mathrm{PG}(2,q)$ *a non-trivial blocking set has size at least* $\geq q+\sqrt{q}+1$*. In case of equality the blocking set is a Baer subplane.*

Actually, Bruen's proof is combinatorial, so Result 1.4.3 is valid for any projective plane of order q, not only for $\mathrm{PG}(2,q)$. A Baer subplane of $\mathrm{PG}(2,q)$ is an embedded $\mathrm{PG}(2,\sqrt{q})$ subgeometry. Projected subgeometries can also be blocking sets, such sets are called linear blocking sets. See Result 1.3.3 for the correctness of the following construction.

Construction 1.4.4 (Linear blocking sets)**.** A projected $\mathrm{PG}(m(n-k),q)$ subgeometry in $\mathrm{PG}(n,q^m)$ is a minimal $(n-k)$-blocking set.

1.5 Blocking sets of Rédei type

Now we present a different construction of blocking sets in $\mathrm{PG}(2,q)$.

Definition 1.5.1. Consider the projective plane $\mathrm{PG}(2,q)$ as the union $\mathrm{AG}(2,q)\cup\ell_\infty$. We say that *the ideal point* $Q\in\ell_\infty$ *is determined* by the affine points $P_1,P_2\in\mathrm{AG}(2,q)$, if the line $\langle P_1,P_2\rangle$ meets ℓ_∞ in Q. If $P_1=(a_1,b_1)$, $P_2=(a_2,b_2)$ and $Q=(m)$, with $a_1,a_2,b_1,b_2\in\mathrm{GF}(q)$ and $m\in\mathrm{GF}(q)\cup\{\infty\}$, then Q is determined by P_1 and P_2 if and only if $(b_2-b_1)/(a_2-a_1)=m$. Note that if $a_1=a_2$, then $m=\infty$. Sometimes m will be called the *direction determined by* P_1 and P_2.

Construction 1.5.2 (Rédei's construction)**.** Select a q-element point set $U=\{(a_i,b_i):i=1,...,q\}$ in $\mathrm{AG}(2,q)$. Denote by D the set of ideal points determined by the points of U. If $|D|<q+1$ then the set $U\cup D$ is a minimal blocking set of $\mathrm{PG}(2,q)$.

Proof. Clearly all lines meeting the line at infinity in a point of D are blocked by $U \cup D$. Now consider a pencil of lines through a point $P \in l_\infty \setminus D$. Since P is not determined by U, every such line can contain at most one point of U. Since $|U| = q$ and the pencil consists of q lines other than l_∞, each line has to contain exactly one point of U. ■

Simple counting argument shows that the following statement is true in all projective planes.

Proposition 1.5.3. *If B is any blocking set of a projective plane of order q, then for any line l not contained in B, we have $|B \setminus l| \geq q$.*

The blocking set in Construction 1.5.2 has a line for which equality holds.

Definition 1.5.4 (Rédei type blocking set of the plane)**.** Let B be a minimal blocking set of a projective plane of order q. If there is a line l for which

$$|B \cap l| = |B| - q,$$

then B is called a *Rédei type blocking set.* Such a line is called a *Rédei line* of the set.

The following proposition shows, that the notion Rédei type blocking set is more or less equivalent to a q-element set together with its determined directions.

Proposition 1.5.5. *Let B be a minimal blocking set of Rédei type with Rédei line l. With $U := B \setminus l$, the determined ideal points in Construction 1.5.2 will be exactly the points $B \cap l$.*

There are several different methods for constructing Rédei type minimal blocking sets with Construction 1.5.2 (see for example [42],[22],[37]). One well-known and basic example is due to Megyesi.

We will use the notation $\mathrm{GF}(q)^*$ for the multiplicative group $\mathrm{GF}(q) \setminus \{0\}$.

Result 1.5.6 (Megyesi)**.** *Let d be a divisor of $q - 1$ and let G be a multiplicative subgroup of $\mathrm{GF}(q)^*$ of size d. Consider the set*

$$U = \{(0, 0)\} \cup \{(0, h) : h \notin G\} \cup \{(g, 0) : g \in G\}.$$

Then U determines exactly $q + 1 - d$ directions, and $B = U \cup D$ is a minimal blocking set of size $2q + 1 - d$. Similarly, if d divides q, then using additive subgroups and two parallel lines we get a minimal blocking set B of size $2q+1-d$.

Note that the points of the resulting blocking set will be on three lines. The first blocking set is often referred to as the *projective triangle* when $d = (q-1)/2$, while the second is the *projective triad* when $d = q/2$.

A different example, contained in the union of four lines, was constructed by Gács in [22], giving an infinite series of examples determining $7q/9$ directions approximately, and yielding a minimal blocking set with size approximately $(2 - 2/9)q$.

Result 1.5.7 (Gács [22]). *Let* 3 *be a divisor of* $q-1$*, and let* $1, \alpha, \alpha^2$ *be coset representatives of the multiplicative subgroup* G *of* $\mathrm{GF}(q)^*$ *of index* 3*. Let*

$$U_i = \{(0,0)\} \cup \{(x,0) : x \in \alpha^i G\} \cup \{(x,x) : x \in G\} \cup \{(0,x) : x \in \alpha^i G\}.$$

Denote by $|D_i|$ *the number of directions determined by* U_i*. Then* $|D_1| + |D_2| + |D_3| = 3q + 1 - 2(q-1)/3$*, and* $|D_i| = 7q/9 + O(\sqrt{q})$*.*

In both the Megyesi and the Gács constructions the cosets of a subgroup of $\mathrm{GF}(q)^*$ were used to select the points of U. We will say, that the cosets were *placed* on lines. In Chapter 4 we present a more general construction, where the number of cosets can be larger than three, and the number of lines from which points are taken can also be increased.

The definition of a Rédei type blocking set can be generalized to higher dimensions also.

Definition 1.5.8 (Rédei type $(n-k)$-blocking set). Let B be a minimal $(n-k)$-blocking set of $\mathrm{PG}(n,q)$. If there is a hyperplane H for which

$$|B \cap H| = |B| - q^{n-k}$$

(which is equivalent to $|B \setminus H| = q^{n-k}$), then B is called a *Rédei type* $(n-k)$*-blocking set.* Such a hyperplane is called a *Rédei hyperplane* of the set.

1.6 Small minimal blocking sets

Definition 1.6.1 (Small blocking set). An $(n-k)$-blocking set B is *small* if $|B| < 3(q^{n-k}+1)/2$.

Small minimal $(n-k)$-blocking sets are of special interest, since there is hope to classify them, as all the known examples of small minimal blocking sets are linear. Linear blocking sets have the property that every subspace meets them in $1 \bmod p$ points. Szőnyi shows in [43], that the same is true for small minimal blocking sets of $\mathrm{PG}(2,q)$, and this result is generalized to higher dimensions by Szőnyi and Weiner in [45].

Result 1.6.2 (Szőnyi [43], Szőnyi and Weiner [45]). *Let B be a small minimal $(n-k)$-blocking set in $\mathrm{PG}(n,q)$, $q=p^h$, p prime. Then each subspace of dimension at least k intersects B in $1 \bmod p$ points.*

Conjecture 1.6.3 (Linearity Conjecture, Sziklai [40]). *All small minimal $(n-k)$-blocking sets of $\mathrm{PG}(n,q)$ are linear.*

In the following case the conjecture is proved to be true.

Result 1.6.4 (Lunardon [30], Storme and Sziklai [41]). *Small minimal blocking sets of Rédei type are linear.*

For a small minimal $(n-k)$-blocking set B of $\mathrm{PG}(n,q)$ we can define the *exponent* of B as the largest integer such that B intersects each k-space in 1 modulo p^e points.

Result 1.6.5 (Sziklai [40]). *Let B be a small minimal $(n-k)$-blocking set in $\mathrm{PG}(n,q)$, $q=p^h$, $2<p$ prime.*

(1) *Let e be the largest integer such that B intersects each k-space in 1 modulo p^e points (from above $1 \leq e \leq h$). Then $e|h$, so $\mathrm{GF}(p^e)$ is a subfield of $\mathrm{GF}(q)$.*

(2) *Furthermore, if the k-space L intersects B in p^e+1 points, then $L \cap B$ is isomorphic to $\mathrm{PG}(1,p^e)$.*

Result 1.6.6 (Szőnyi and Weiner [45]). *Denote by*

$$[l_q(n,k,e), u_q(n,k,e)]$$

the smallest interval containing the sizes of all the small minimal $(n-k)$-blocking sets of $\mathrm{PG}(n,q)$, $q=p^h$, $2<p$ prime, with exponent e. These intervals are disjoint, furthermore, if $e'|m$ and $e'<e$, then $u_q(n,k,e)<l_q(n,k,e')$.

Thus, minimal $(n-k)$-blocking sets with size in the interval $[l_q(n,k,e), u_q(n,k,e)]$ intersect each k-space in 1 mod p^e points. The next statement summarizes some corollaries of the 1 mod p result.

Result 1.6.7 (Szőnyi and Weiner [45]). *Assume that B is a point set in* $\mathrm{PG}(n,q)$, *$q = p^h$, $2 < p$ prime. Let e and k be integers, so that $0 < k < n$ and suppose that $|B| < 3(q^{n-k}+1)/2$. Then the following statements are equivalent:*

(1) *B is a minimal $(n-k)$-blocking set and $|B| \leq u_q(n,k,e)$.*

(2) *B intersects each k-space in* 1 mod p^e *points.*

(3) *Every subspace with dimension at least k intersects B; and any subspace that intersects B intersects it in* 1 mod p^e *points.*

The best bounds for $l_q(2,1,e)$ and $u_q(2,1,e)$ are due to Blokhuis and Polverino, and the case $n > 2$ was studied in [45].

Result 1.6.8. *Assume that $p^e \neq 2, 4, 8$, then*

(1) (Blokhuis [10]) $q + 1 + p^e\lceil (q/p^e+1)/(p^e+1)\rceil \leq l_q(2,1,e)$.

(2) (Polverino [34]) $u_q(2,1,e) \leq \frac{1+(p^e+1)(q+1)-\sqrt{[1+(p^e+1)(q+1)]^2-4(p^e+1)(q^2+q+1)}}{2}$.

(3) (Szőnyi and Weiner, [45]) $l_q(n,k,e) \geq l_{q^{n-k}}(2,1,e)$ *and* $u_q(n,k,e) \leq u_{q^{n-k}}(2,1,e)$.

Result 1.6.9 (Polverino [34]). *A small minimal blocking set of* $\mathrm{PG}(n,q)$, *$q = p^{mh}$ intersecting each line in* 1 mod p^h *points has size at most*

$$u_q(n,1,h) < q^{n-1} + \frac{q^{n-1}}{p^h} + \frac{q^{n-1}}{p^{2h}} + 3\frac{q^{n-1}}{p^{2h}}.$$

By Result 1.6.6, the sizes of the minimal $(n-k)$-blocking sets of $\mathrm{PG}(n,q)$, $q = p^h$, $2 < p$ prime, are contained in disjoint intervals

$$[l_q(n,k,e_1), u_q(n,k,e_1)], \ldots, [l_q(n,k,e_i), u_q(n,k,e_i)],$$

where $e_1 > \cdots > e_i$ are the divisors of h, and $u_q(n,k,e_j) < l_q(n,k,e_{j+1})$.

Starting from the smallest one, the first interval consists of one value only, $l_q(n,k,h) = u_q(n,k,h) = \theta_{n-k}$, because an $(n-k)$-dimensional subspace is the only $(n-k)$-blocking set with the property that every subspace of dimension at least k intersects it in 1 mod q points.

When q is a square (hence $2|h$), then $[l_q(n,k,h/2), u_q(n,k,h/2)]$ is the second interval, and it contains the sizes of the $(n-k)$-blocking sets intersecting each $(n-k)$-space in 1 mod $\sqrt{q}$ points. Weiner proves in [47], that all minimal $(n-k)$-blocking sets of this interval are linear.

Result 1.6.10 (Weiner [47])**.** *Small minimal $(n-k)$-blocking sets of* $\mathrm{PG}(n,q)$*, $q=p^{2m}$, $2<p$ prime, $81 \leq q$, intersecting each k-space in* 1 mod $\sqrt{q}$ *points are linear.*

These blocking sets are so called *Baer-cones.*

A *cone* with base a set S and vertex a subspace Σ is the union of all subspaces $\langle \Sigma, P\rangle$, where P is a point of S. A Baer-cone is a cone with base an embedded $\mathrm{GF}(\sqrt{q})$-linear subgeometry. It is not hard to see that projected $\mathrm{PG}(m,\sqrt{q})$ subgeometries are always Baer-cones.

The next interval to be observed is $[l_q(n,k,h/3), u_q(n,k,h/3)]$, if h is divisible by 3. The next result solves the planar case.

Result 1.6.11 (Polverino [34], Polverino and Storme [35])**.** *A non-trivial blocking set in* $\mathrm{PG}(2,p^{3m})$*, $p \geq 7$, meeting every line in* 1 mod p^m *points is either a Baer subplane* (*and m is even*) *or one of the following sets:*

(1) *a minimal blocking set of size $p^{3m}+p^{2m}+1$, projectively equivalent to the set*

$$\{(x, Tr(x), 1) | x \in \mathrm{GF}(p^{3m})\} \cup \{(x, Tr(x), 0) | x \in \mathrm{GF}(p^{3m}) \setminus \{0\}\},$$

where Tr is the trace function from $\mathrm{GF}(p^{3m})$ *to* $\mathrm{GF}(p^m)$ (*i.e. Tr :* $\mathrm{GF}(p^{3m}) \rightarrow \mathrm{GF}(p^m) : x \mapsto x + x^{p^m} + x^{p^{2m}}$);

(2) *a minimal blocking set of size $p^{3m}+p^{2m}+p^m+1$, projectively equivalent to the set*

$$\{(x, x^{p^m}, 1) || x \in \mathrm{GF}(p^{3m})\} \cup \{(x, x^{p^m}, 0) || x \in \mathrm{GF}(p^{3m}) \setminus \{0\}\}.$$

The next remark summarizes some properties of the blocking sets of Result 1.6.11. For more details the reader is referred to [34] and [35].

Remark 1.6.12. (Polverino [34], Polverino and Storme [35]) All three types of blocking sets in Result 1.6.11 are linear (and hence each line intersects them in a linear point set). Furthermore, they are all of Rédei type.

The Baer subplane has $p^{3m} + p^{3m/2} + 1$ points and every line meets it in 1 or $p^{3m/2} + 1$ points.

The minimal blocking set of size $p^{3m}+p^{2m}+p^m+1$ has exactly one $(p^{2m}+p^m+1)$-secant, and all other lines are 1-secants (i.e. *tangents*) or (p^m+1)-secants. Every (p^m+1)-secant meets the $(p^{2m}+p^m+1)$-secant in a point belonging to the set.

The minimal blocking set of size $p^{3m} + p^{2m} + 1$ has a unique point lying on $(p^{2m} + 1)$-secants and tangents only. There are $p^m + 1$ $(p^{2m} + 1)$-secants on this point. All other lines are (p^m+1)-secants or tangents. A (p^m+1)-secant contains one point from each of the $(p^{2m} + 1)$-secants.

It will be the main result of Chapter 2, to prove a similar result for higher dimensional projective spaces. We prove that point sets of $\mathrm{PG}(n, p^{3m})$, $n > 2$, $p \geq 7$ prime, with size less than $3(p^{3m(n-k)} + 1)/2$ and intersecting each k-space in 1 mod p^m points are linear blocking sets.

In certain projective spaces the Linearity Conjecture has been proved to be true.

Result 1.6.13 (Heim, [24]). *For $q = p$ prime, there are no small minimal non-trivial $(n-k)$-blocking sets in* $\mathrm{PG}(n,p)$ *at all. For $n = 2$ this was proved by Blokhuis in* [9].

The next result is a corollary of Result 1.6.10. For $n = 2$ it was proved by Szőnyi in [43].

Corollary 1.6.14 (Weiner, [47]). *If $q = p^2$, $11 \leq p$ prime, then all small minimal $(n-k)$-blocking sets in* $\mathrm{PG}(n,p^2)$ *are linear.*

The following result is a corollary of Result 1.6.11.

Corollary 1.6.15. *If $q = p^3$, $p \geq 7$ prime, then all small minimal non-trivial blocking sets in* $\mathrm{PG}(2,p^3)$ *are one of the linear sets described in (1) and (2) of Result 1.6.11.*

The case $n \geq 3$ will be proved in Chapter 2.

1.7 Multiple blocking sets

Definition 1.7.1 (t-fold $(n-k)$-blocking set)**.** A *t-fold $(n-k)$-blocking set* of $\mathrm{PG}(n,q)$ is a set of points which meets every k-dimensional subspace in at least t points. If the points of the set are not all different, so the set is a *multiset* of points, then it is called a *weighted* t-fold $(n-k)$-blocking set.

To exclude trivial cases, $0 < k < n$ will always be assumed.

A *weight function* w of $\mathrm{PG}(n,q)$ is a mapping from the point set of $\mathrm{PG}(n,q)$ to the set of nonnegative integers. For a point P the integer $w(P)$ is the *weight* of P.

There is a natural correspondence between multisets and weight functions of $\mathrm{PG}(n,q)$: let the weight of a point be the multiplicity of that point in the set. For a given weight function the weight of a set M of points is by definition the sum of the weights of all its points, denoted by $w(M)$. We will call $w(\mathrm{PG}(n,q))$ the *total weight* of w, and denote it by $|w|$.

We will use the following notation: for the multisets B_1 and B_2, with associated weight functions w_1 and w_2 respectively, $B_1 \cup B_2$ will denote the multiset defined by the weight function $\max\{w_1, w_2\}$, while $B_1 + B_2$ will denote the multiset defined by the weight function $w_1 + w_2$.

The multiset associated to a weight function w is a t-fold $(n-k)$-blocking set if and only if the weight of every k-dimensional subspace is at least t. If this is the case, then we will call the weight function w a *t-fold $(n-k)$-blocking set* for short. When we speak of weighted t-fold $(n-k)$-blocking sets, we will use both notations B and w, always choosing the one which makes descriptions simpler.

If w is a t-fold $(n-k)$-blocking set, then a point P will be called an *essential point* of w, if $w(P) \geq 1$ and there is a k-subspace Σ_k containing P such that $w(\Sigma_k) = t$. The point P is a *nonessential* point of w, if $w(P) \geq 1$ and the weight of every k-subspace containing P is at least $t+1$. In this case the weight function w' defined by

$$w'(Q) = \begin{cases} w(Q) & \text{if } Q \neq P; \\ w(P) - 1 & \text{if } Q = P \end{cases}$$

is also a t-fold $(n-k)$-blocking set.

If w and w' are weight functions, then we will say that w' is *contained* in w, and denote this by $w' \leq w$, if $w'(P) \leq w(P)$ for all points $P \in \mathrm{PG}(n,q)$.

The t-fold $(n-k)$-blocking set w is said to be *minimal* if $w' \equiv w$ for any t-fold $(n-k)$-blocking set w' contained in w. Clearly a t-fold $(n-k)$-blocking set is not minimal if and only if it has nonessential points.

Definition 1.7.2. A t-fold blocking set of $\mathrm{PG}(2,q)$, $q=p^h$, p prime, is called *small*, if it has less than $tq+(q+3)/2$ points.

Result 1.7.3 (Blokhuis, Lovász, Storme and Szőnyi, [11])**.** *Let B be a small minimal t-fold blocking set in $\mathrm{PG}(2,q)$, $q=p^h$, p prime, $h \geq 1$. Then B intersects every line in $t \bmod p$ points.*

Conjecture 1.7.4 (General Linearity Conjecture, Sziklai [40])**.** *If t is small enough, then a small minimal t-fold $(n-k)$-blocking set in $\mathrm{PG}(n,q)$ is the sum of $\mathrm{GF}(p^{e_i})$-linear $(n-k)$-blocking sets.*

Result 1.7.5 (Ferret, Storme, Sziklai and Weiner, [21])**.** *Let B be a minimal weighted t-fold $(n-k)$-blocking set of $\mathrm{PG}(n,q)$, $q=p^h$, p prime, $h \geq 1$, of size $|B| = tq^{n-k}+t+k'$, with $t+k' \leq (q^{n-k}-1)/2$. Then B intersects every k-dimensional subspace in $t \bmod p$ points.*

Using this result, a characterization result similar to Result 1.6.10 was proved in [20].

Result 1.7.6 (Ferret, Storme, Sziklai and Weiner, [20])**.** *Let B be a minimal t-fold $(n-k)$-blocking set of $\mathrm{PG}(n,q)$, q square, of size at most $|B| \leq tq^{n-k} + 2tq^{n-k-1}\sqrt{q} < tq^{n-k}+q^{n-k-1/3}$.*

Then B is the union of pairwise disjoint Baer-cones.

Chapter 2

Small point sets of $\mathrm{PG}(n, q^3)$ intersecting each k-space in $1 \bmod q$ points

This chapter is based on joint work with Zsuzsa Weiner, Klaus Metsch and Tamás Szőnyi and appeared in [4] and [3].

2.1 The main theorem

There has been a lot of work aiming at finding a proof for Sziklai's Linearity Conjecture, yet only partial results have been achieved. According to Result 1.6.6, the sizes of the minimal blocking sets of $\mathrm{PG}(n, q)$, $q = p^h$, $p > 2$ prime, are contained in disjoint intervals

$$[l_q(n, k, e_1), u_q(n, k, e_1)], \ldots, [l_q(n, k, e_i), u_q(n, k, e_i)],$$

where $e_1 > \cdots > e_i$ are the divisors of h, and $u_q(n, k, e_j) < l_q(n, k, e_{j+1})$.

Starting from the smallest one, the first interval where the Linearity Conjecture has not been proved yet is $[l_q(n, k, h/3), u_q(n, k, h/3)]$, if h is divisible by 3. In this chapter we prove that the Linearity Conjecture is valid here also, that is all minimal $(n - k)$-blocking sets with size belonging to the interval $[l_q(n, k, h/3), u_q(n, k, h/3)]$ are linear.

Notation. Throughout this chapter we will be working in projective spaces of order p^{3h}, p prime, $h \geq 1$, and with point sets meeting certain subspaces in $1 \bmod p^h$ points. For the sake of simplicity, instead of q, we will use q^3 for the order of the space, and have $q = p^h$, p prime, $h \geq 1$. So please keep in mind, that *from here on, throughout this chapter, we will be working in the projective space* $\mathrm{PG}(n, q^3)$.

The aim of this chapter is to prove the following theorem, which can be found in [4] ($k = n - 1$) and [3] (arbitrary k).

Theorem 2.1.1. *Let B be a point set of* $\mathrm{PG}(n, q^3)$*, $q = p^h$, $1 \leq h$, $7 \leq p$ prime, intersecting each k-space in* $1 \bmod q$ *points, and with size $|B| < \frac{3}{2}(q^{3(n-k)} + 1)$. Then B is a linear $(n - k)$-blocking set.*

In [29] Lavrauw, Storme and Van de Voorde prove the same result using an approach different from ours.

A corollary of Theorem 2.1.1 and Result 1.6.7 is that all minimal $(n-k)$-blocking sets of size in the interval $[l_{q^3}(n, k, h), u_{q^3}(n, k, h)]$ are linear. Moreover, the upper bound of this interval can be raised until the lower bound of the next interval. Thus, any improvement on the bound of the lower end of the fourth interval leads to an immediate improvement of the next corollary.

Corollary 2.1.2. *Let s be the smallest integer such that $3 < s \leq 3h$ and $s|3h$. Then the minimal $(n - k)$-blocking sets of size $< l_{q^3}(n, k, 3h/s)$ are linear.*

Another important corollary of Theorem 2.1.1 is that it proves the Linearity Conjecture in projective spaces of order p^3, with $p \geq 7$ prime.

Corollary 2.1.3. *Small minimal blocking sets of* $\mathrm{PG}(n, p^3)$*, $p \geq 7$ prime are linear.*

2.2 GF(q)-linear blocking sets of PG(n, q^3)

In this section some important properties of GF(q)-linear sets of PG(n, q^3) are collected. Most of these results are simple corollaries of Lemma 1.3.3.

Lemma 2.2.1. *If a point meets a projected subgeometry in a projected* PG(m, q), *then* $0 \leq m \leq 2$.

If $m = 0$, then the point is an *ordinary* point of the projection. We will call the point *special*, if $m = 1$ and *superspecial*, if $m = 2$.

Notation. Consider a PG(m, q) subgeometry embedded in PG(n, q^3). For every subspace U of PG(m, q), we call the subspace of PG(n, q^3) generated by the points of U the *extension* of U, and denote this subspace by $e(U)$. In other words, $e(U)$ is the unique subspace of PG(n, q^3) containing U and having $\dim(U) = \dim(e(U))$.

Now we examine the linear point sets of a line PG($1, q^3$).

Lemma 2.2.2. *Let S be a projected* PG(m, q) *subgeometry contained in a line $l =$* PG($1, q^3$), *and not contained in a point.*

(1) *Then $1 \leq m \leq 5$.*

(2) *If $m = 1$, then $|S| = q + 1$ and S is an embedded* PG($1, q$) *subgeometry* (*a subline of l*).

(3) *If $m = 2$, then S is a projected* PG($2, q$) *subplane. There are two cases: either $|S| = q^2 + q + 1$ and all points of S are ordinary, or $|S| = q^2 + 1$ and one point of S is special, while all the other are ordinary.*

(4) *If $m \geq 3$, then $|S| = q^3 + 1$, so every point of the line belongs to S.*

(5) *If $m = 3$, then there are two cases: either S has one superspecial point and q^3 ordinary points, or S has $q + 1$ special points and $q^3 - q$ ordinary points.*

(6) *If $m = 4$, then S has 1 superspecial point and q^3 special points.*

(7) *$m = 5$, then all points of S are superspecial.*

Proof. The preimages of the points of S yield a partition of PG(m, q) into disjoint subspaces of dimension 0, 1, or 2. The statements above follow from this and Lemma 1.3.3. ■

Corollary 2.2.3. *If S is a projected* $\mathrm{PG}(m,q)$ *subgeometry in* $\mathrm{PG}(n,q^3)$*, and the line l is a $(q+1)$-secant of S, then every point of $S\cap l$ is ordinary.*

Corollary 2.2.4. *If S is a projected* $\mathrm{PG}(m,q)$ *subgeometry in* $\mathrm{PG}(n,q^3)$*, and P is a special point of S, then a non-tangent line on P is either contained in S, or is a (q^2+1)-secant of S. If P is superspecial, then every non-tangent line on P is contained in S.*

Corollary 2.2.5. *If S is a projected* $\mathrm{PG}(m,q)$ *subgeometry in* $\mathrm{PG}(n,q^3)$*, and $P_1,P_2,\ldots$ are the superspecial points of S, then either S is the subspace $\langle P_1,P_2,\ldots\rangle$, or S is a cone with vertex the subspace $\langle P_1,P_2,\ldots\rangle$.*

Suppose that $\mathrm{PG}(m,q)$ is projected to $\mathrm{PG}(n,q^3)$ and the resulting set is S. Now clearly there can be several ways we can choose a set $S'\cong\mathrm{PG}(m,q)$ in $\mathrm{PG}(N,q^3)\supseteq\mathrm{PG}(n,q^3)$ and a subspace C, with $C\cap S'=\emptyset$, such that S is the projection of S' from C to $\mathrm{PG}(n,q^3)$. For a point $P\in S$, can the dimension of the subgeometry projected to P be different for different choices of S' and C? For the case $|S|=q^2+1$, this question is answered in [19].

Result 2.2.6 (Fancsali and Sziklai, [19])**.** *Let S be a linear point set of* $\mathrm{PG}(1,q^3)$*, $|S|=q^2+1$. Then the special point of S is unique, that is, for any construction of S the special point is always the same.*

Corollary 2.2.7. *Let S be a projected* $\mathrm{PG}(m,q)$ *subgeometry in* $\mathrm{PG}(n,q^3)$*, such that S is not a subspace, and let $P\in S$ be any point. Then for any construction of S the dimension of the subgeometry projected to P is the same.*

Proof. If there is a line l on P which is a $(q+1)$-, a (q^2+1)- or a (q^2+q+1)-secant of S, then the dimension of the subgeometry projected to P is clear. If all non-tangent lines on P are contained in S, and S is not a subspace, then we can find a plane π on P which meets S in $q+1$, q^2+1 or q^2+q+1 concurrent lines. With inspection of the possibilities of the preimages of these lines, and by Lemma 1.3.3, we have that in the first case π meets S in a projected $\mathrm{PG}(4,q)$ subgeometry, and in the second and third cases a projected $\mathrm{PG}(5,q)$ subgeometry. In all cases P is superspecial. ■

Remark. Let S be a projected $\mathrm{PG}(m,q)$ subgeometry in $\mathrm{PG}(n,q^3)$ and assume that a construction of S has been selected. In other words, a set $S'\cong\mathrm{PG}(m,q)$ in $\mathrm{PG}(N,q^3)\supseteq\mathrm{PG}(n,q^3)$ and a subspace C of $\mathrm{PG}(N,q^3)$, with $C\cap S'=\emptyset$ and

$\dim(C) = N - n - 1$ has been given, such that S is the projection of S' from C to $\mathrm{PG}(n, q^3)$. Another way of looking at this, is to view S as a subset of the quotient geometry $\mathrm{PG}(N, q^3)/C$. In this case S corresponds to the set of subspaces $\langle P, C\rangle$ where P is a point of S'. It is not hard to see, that if we replace C by $e(S') \cap C$ and the sets $\langle P, C\rangle$ by $\langle P, e(S') \cap C\rangle$, then the set we obtain in $e(S') \cong \mathrm{PG}(m, q^3)$ is projectively equivalent to S. Thus, we can assume that in the construction we choose for S we have $N = m$ and $\dim(C) = m - n - 1$.

Definition 2.2.8. A nonempty set $\mathcal{R}$ of skew lines of a 3-dimensional projective space $\mathrm{PG}(3, q)$ is called a *regulus*, if the following are true:

(1) Through each point of each line of $\mathcal{R}$ there is a transversal of $\mathcal{R}$ (i.e. a line which meets every element of $\mathcal{R}$).

(2) Through each point of a transversal of $\mathcal{R}$ there is a line of $\mathcal{R}$.

It is clear that the set of all transversals of a regulus $\mathcal{R}$ again form a regulus. We call it the *opposite regulus* of $\mathcal{R}$. And it is also clear that $|\mathcal{R}| = q + 1$. Any three skew lines of $\mathrm{PG}(3, q)$ are contained in a unique regulus.

Lemma 2.2.9. *Let S be a projected $\mathrm{PG}(m, q)$ subgeometry on a line $l = \mathrm{PG}(1, q^3)$. Let $b \cong \mathrm{PG}(1, q)$ be a line of $\mathrm{PG}(m, q)$, which is projected to the points P_1, $P_2, \ldots,$ $P_{q+1} \in l$. Then if at least three of the points P_i are not ordinary points, then neither of them are.*

Proof. By Lemma 2.2.2, the only case which needs to be observed is when $m = 3$, and S has $q + 1$ special points, and $q^3 - q$ ordinary points. Then the preimages of the special points are $q + 1$ skew lines $l_1, l_2, \ldots, l_{q+1}$ of the $\mathrm{PG}(3, q)$ subgeometry. We will prove that they form a regulus. Then any line which meets at least 3 of them, has to meet all.

By the Remark above, we can consider the following construction of S: embed l into a projective space $\mathrm{PG}(3, q^3)$, and select 3-dimensional subgeometry $S' \subset \mathrm{PG}(3, q^3)$, and a line $t \subset \mathrm{PG}(3, q^3)$, t skew to l, $t \cap S' = \emptyset$, such that S is the projection of S' from t to l. Then the extensions of the lines l_i are skew lines $e(l_1)$, $e(l_2), \ldots,$ of the space $\mathrm{PG}(3, q^3)$, and all of them meet t and l.

Now let $\mathcal{R}$ be the regulus of S' determined by three of the lines, say l_1, l_2 and l_3. Let $\mathcal{R}^e$ be the regulus of $\mathrm{PG}(3, q^3)$ determined by $e(l_1)$, $e(l_2)$ and $e(l_3)$. For every line of $\mathcal{R}$, the extension is an element of $\mathcal{R}^e$. Clearly t and l are elements of the opposite of $\mathcal{R}^e$, so every element of $\mathcal{R}^e$ meets both l and t. This proves that every element of $\mathcal{R}$ corresponds to a special point P_i, so $\mathcal{R} = \{l_1, l_2, \ldots, l_{q+1}\}$. ■

The following lemma collects some of the properties of GF(q)-linear point sets of PG$(2, q^3)$.

Lemma 2.2.10. *Let S be a projected* PG(m, q) *subgeometry in a plane $\pi \cong$* PG$(2, q^3)$*, but not contained in a line.*

(1) *Then $2 \leq m \leq 8$.*

(2) *If S is a blocking set of π, then $m \geq 3$.*

(3) *If $m = 3$, then S is one of the sets in Result 1.6.11 (1) and (2).*

(3) *If $m = 4$, and P is an ordinary point of S, then there are no tangents on P to S. There are two cases: either there is one line on P which is contained in S and all other lines are $(q+1)$-secants to S, or there are $q+1$ lines that are (q^2+1)- or (q^2+q+1)-secants of S and all the other lines are $(q+1)$-secants.*

(4) *If $m \geq 5$, then S has no $(q+1)$-secants in π.*

(5) *If $m \geq 6$, then S contains every point of π.*

Proof. (3) Let P be an ordinary point of S and $l_1, \ldots, l_{q^3+1}$ the lines on P in π. By Lemma 1.3.3, every line l_i contains a projected PG(t, q) with $t \geq 1$. These are all subspaces of PG$(4, q)$ and they all meet in one point (the preimage of P). Counting the points of PG$(4, q)$ in these subspaces yields that either one line l_i contains a projected 3-dimensional subspace, and all others contain projected lines, or $q+1$ have projected planes and all others lines.

The other statements are direct consequences of Lemma 1.3.3. ■

Lemma 2.2.11. *Let S be a projected* PG$(4, q)$ *subgeometry in a plane $\pi \cong$* PG$(2, q^3)$*. Let $P \in S$ be an ordinary point of S such that there are $q+1$ lines l_1, $l_2, \ldots, l_{q+1}$ on P, which meet S in projected* PG$(2, q)$ *subgeometries, and all other lines on P are $(q+1)$-secants to S. Let $b \cong$* PG$(1, q)$ *be a line of the* PG$(4, q)$ *subgeometry, which is projected to the points P_1, $P_2, \ldots$, P_{q+1}. Then if at least 3 of these points lie on the lines l_i, then all of them do.*

Proof. Embed the plane π in a projective space $\mathrm{PG}(4, q^3)$, and select a 4-dimensional subgeometry $S' \cong \mathrm{PG}(4, q)$, and a line $t \subset \mathrm{PG}(4, q^3)$, such that S is the projection of S' from t to π. The points of π correspond to planes on t, and the lines of π correspond to 3-dimensional spaces on t.

The preimages of $l_i \cap S$ are planes $\pi_1, \pi_2, \ldots, \pi_{q+1}$ of $\mathrm{PG}(4, q)$ meeting in one point P', which is the preimage of P.

Select lines $r_1 \subset \pi_1$ and $r_2 \subset \pi_2$ such that $P' \notin r_i$. Then $e(r_1)$ and $e(r_2)$ are skew lines, which meet the plane $\langle t, P' \rangle$ in different points R_1 and R_2. Let $\Sigma = \langle r_1, r_2 \rangle$ be the 3-dimensional subspace generated by r_1 and r_2. Then $e(\Sigma) = \langle e(r_1), e(r_2) \rangle$. Σ does not contain P', so $\Sigma \cap \langle t, P' \rangle$ is a line, in fact, it is the line $r := \langle R_1, R_2 \rangle$. And Σ meets every plane π_i in a line r_i, such that $e(r_i)$ meets $\langle t, P' \rangle$ in a point of r.

We will prove that the planes π_i form a cone with vertex P' and base a regulus of Σ. Then the assertion follows, because any line of $\mathrm{PG}(4, q)$ which meets at least 3 of these planes, will meet them all.

Let $\mathcal{R}$ be the unique regulus of Σ which contains the lines r_1, r_2 and r_3. Then the regulus $\mathcal{R}^e$ of $e(\Sigma)$, which contains $e(r_1)$, $e(r_2)$ and $e(r_3)$ will contain the extension of every element of $\mathcal{R}$. Clearly, r is an element of the opposite of $\mathcal{R}^e$. We will show that

$$\{\pi_1, \ldots, \pi_{q+1}\} = \{\langle P', l \rangle | l \in \mathcal{R}\}.$$

If $l \in \mathcal{R}$, then $e(l)$ meets the line r, thus it meets the plane $\langle t, P' \rangle$, which means that the plane $\langle P', l \rangle$ is contained in a 3-dimensional subspace on t, and so corresponds to a line on P meeting S in a projected $\mathrm{PG}(2, q)$. ■

Lemma 2.2.12. *Let S be a projected $\mathrm{PG}(m, q)$ subgeometry of $\mathrm{PG}(n, q^3)$, and $H \cong \mathrm{PG}(2, q)$ a subplane of S such that the points of H are projected onto the concurrent lines $t_1, t_2, \ldots, t_{q+1}$. Then either $|t_i \cap S| \geq q^2 + 1$ for each t_i or this is true only for at most two of these lines.*

Proof. The lines t_i span a plane π of $\mathrm{PG}(n, q^3)$ which meets S in a projected $\mathrm{PG}(t, q)$ subgeometry. By Corollary 2.2.4 and Lemma 2.2.10, we may assume that $t = 4$, and the lines t_i meet in an ordinary point P. We may also assume that there are $q + 1$ lines on P, say $l_1, l_2, \ldots, l_{q+1}$, which meet S in projected $\mathrm{PG}(2, q)$ subgeometries, and all other lines on P are $(q + 1)$-secants to S. Let

$b \cong \mathrm{PG}(1,q)$ be a line of H with $P' \notin b$. Then the number of lines belonging to both $\{l_1,\dots,l_{q+1}\}$ and $\{t_1,\dots,t_{q+1}\}$ equals the number of points of b on the lines $l_1,\dots,l_{q+1}$, and we can use Lemma 2.2.11. ■

In the following lemmas S is not only a GF(q)-linear set of $\mathrm{PG}(n,q^3)$, but also a minimal $(n-k)$-blocking set. Thus, $m = 3(n-k)$.

Lemma 2.2.13. *Let S be a projected $\mathrm{PG}(3(n-k),q)$ subgeometry of $\mathrm{PG}(n,q^3)$, and suppose that S is not a subspace.*

(a) *Every point that meets S in a projected $\mathrm{PG}(s,q)$, $0 \le s \le 2$, lies on a line meeting S in a projected $\mathrm{PG}(s+1,q)$.*

(b) *Every line l that meets S in a projected $\mathrm{PG}(s,q)$, $2 \le s \le 5$, lies in a plane that meets S in a projected $\mathrm{PG}(s+1,q)$. If $k \ge 2$, this also holds for $s \le 1$.*

Proof. If $\langle S\rangle$ is an n'-dimensional subspace of $\mathrm{PG}(n,q^3)$, then S meets every $(n'+k-n)$-dimensional subspace of $\langle S\rangle$, i.e. S is an $(n-k)$-blocking set of $\langle S\rangle$. Thus, we may assume that S generates $\mathrm{PG}(n,q^3)$.

Let Σ_t be a t-subspace ($t \le n-2$) that meets S in a projected $\mathrm{PG}(s,q)$ and suppose that every $(t+1)$-subspace on Σ_t which meets S not only in the points of $\Sigma_t \cap S$ meets S in at least a projected $\mathrm{PG}(s+2,q)$. Consider a $(t+2)$-subspace Σ_{t+2} spanned by two of these $(t+1)$-subspaces. Then Σ_{t+2} meets S in at least a $\mathrm{PG}(s+4,q)$. Therefore by Lemma 1.3.3, every $(t+1)$-subspace of Σ_{t+2} meets S in at least a $\mathrm{PG}(s+1,q)$. Applying this to the $(t+1)$-subspaces of Σ_{t+2} on Σ_t, the assumption implies that all these meet S in at least a $\mathrm{PG}(s+2,q)$.

This argument shows that the union of the $(t+1)$-subspaces on Σ_t that meet S not only in $\Sigma_t \cap S$ is a subspace. As S generates $\mathrm{PG}(n,q^3)$, it follows that each $(t+1)$-subspace on Σ_t meets S in at least a $\mathrm{PG}(s+2,q)$. As S is a projected $\mathrm{PG}(m,q)$, it follows that $|\mathrm{PG}(m,q)|$ is at least the number of $(t+1)$-subspaces on Σ_t times $q^{s+2}+q^{s+1}$. This implies that $m \ge 3(n-1-t)+s+2$. Using $m = 3(n-k)$ and $k \ge 1$, this gives $s \le 3(t-k)+1$. In the situation of (a) and (b), this is a contradiction. ■

Lemma 2.2.14. *Let S be a projected $\mathrm{PG}(3(n-k),q)$ subgeometry of $\mathrm{PG}(n,q^3)$, and suppose that S is not a subspace. If P is an ordinary point of S, then there are at least $q^{3(n-k-1)+2} - q^{3(n-k-1)}$ $(q+1)$-secants on P to S.*

Proof. We will proceed by induction on k. The case $k = 1$ follows from Lemma 2.4.7, where it is proved that if B is a non-trivial blocking set of $\mathrm{PG}(n, q^3)$ of size $< \frac{3}{2}(q^{3(n-1)} + 1)$ and meeting every line in 1 mod q points, but not having a $(q^{3/2} + 1)$-secant, and P is a point of B which is on a $(q + 1)$-secant to B, then the number of $(q+1)$-secants on P is at least $q^{3n-4} - q^{3n-6}$. The set S has these properties, and by Lemma 2.2.13(1) we can find a $(q + 1)$-secant on an ordinary point P.

For the induction step suppose that $k \geq 2$. Again by Lemma 2.2.13(1) we can find a $(q+1)$-secant on any ordinary point. Consider a tangent on the ordinary point P and project S form a point $T \neq P$ of this tangent to a hyperplane H. This results in a set S' that is a projected $\mathrm{PG}(m, q)$ meeting all $(k - 1)$-subspaces of H. The image P' of P is an ordinary point of S' and clearly, every $(q+1)$-secant of S' is the image of a (unique, which we do not need) $(q + 1)$-secant of S. As the assertion is true for $k - 1$, it follows for general k. ■

2.3 Proof of Theorem 2.1.1 for $k = 1$, $n = 3$

Throughout this section it will be assumed that B is a point set of $\mathrm{PG}(3, q^3)$*, $q = p^h$, $1 \leq h$, $7 \leq p$ prime, intersecting each line in* $1 \bmod q$ *points, and $|B| < \frac{3}{2}(q^6 + 1)$.*

The following lemma is a direct consequence of Result 1.6.9.

Lemma 2.3.1. $|B| < q^6 + q^5 + q^4 + 3q^3$.

The next lemma is crucial when we characterize these point sets.

Lemma 2.3.2. *A plane π either intersects B in a small minimal blocking set, or contains more than $q^4 - q^3$ points from B.*

Proof. Let $x = |B \cap \pi|$, where π is a plane of $\mathrm{PG}(3, q^3)$. Let b_i be the number of lines of π meeting B in exactly i points. As π has $b := q^6 + q^3 + 1$ lines and $r := q^3 + 1$ lines on each point, standard counting arguments give the following three equations.

$$\begin{aligned} \sum_i b_i &= b \\ \sum_i b_i i &= xr \\ \sum_i b_i i(i-1) &= x(x-1) \end{aligned}$$

Combining these we find

$$\sum_i b_i (i-1)(i-q-1) = x(x-1) - (q+1)xr + (q+1)b. \tag{2.1}$$

As every line meets B in 1 mod q points, the left-hand side is non-negative. As the right-hand side is quadratic in x and negative for $x = \frac{3}{2}q^3 + 1$ and $x = q^4 - q^3$, the assertion follows. ■

Corollary 2.3.3. *On any line l of* $\mathrm{PG}(3, q^3)$ *there has to be a plane which intersects B in a small minimal blocking set. Thus, $l \cap B$ is a linear set of size 1, $q + 1$, $q^2 + 1$, $q^2 + q + 1$, $q^3 + 1$, or $q^{3/2} + 1$ (then q is a square).*

Proof. Suppose on the contrary, that all the planes on l contain more than $q^4 - q^3$ points from B. Then counting the points of B on these planes we get

$$|B| > (q^3+1)(q^4 - q^3 - |l \cap B|) + |l \cap B| > q^7 - q^6 - |l \cap B|q^3,$$

but $|l \cap B| \leq q^3 + 1$, which contradicts the bound of Lemma 2.3.1, as $p \geq 7$.

Every secant of B has to be a secant of a small minimal planar blocking set. The secants of these sets are described in Remark 1.6.12. ∎

The following is a technical lemma which will be useful for us.

Lemma 2.3.4. (1) *On a $(q+1)$-secant there are less than 4 planes intersecting B in more than $q^4 - q^3$ points.*

(2) *On a (q^2+1)- or a (q^2+q+1)-secant there are less than $2q$ planes intersecting B in more than $q^4 - q^3$ points.*

(3) *On a line totally contained in B there are less than $q^2 + 3q$ planes containing further points of B.*

Proof. Let l be a line and denote by K the number of planes on l which intersect B in more than $q^4 - q^3$ points.

(1) If l is a $(q+1)$-secant, then counting the points of B on the planes through l gives

$$|B| > K(q^4 - q^3 - q - 1) + (q^3 + 1 - K)(q^3 + q^2 - q).$$

For $K \geq 4$ this is in contradiction with Lemma 2.3.1.

(2) Summing the number of points on the planes through a (q^2+1)- or a (q^2+q+1)-secant gives

$$|B| > K(q^4 - q^3 - q^2 - q - 1) + (q^3 + 1 - K)q^3.$$

For $K \geq 2q$ this is in contradiction with Lemma 2.3.1.

(3) A plane on a line totally contained in B and containing a further point of B intersects B in at least $q^4 + q + 1$ points, as B intersects every line in 1 mod q points. Having at least $q^2 + 3q$ such planes on a line totally contained in B would lead to a contradiction with Lemma 2.3.1. ∎

In case $2|h$ we will now characterize the blocking sets having a $(q^{3/2}+1)$-secant.

Lemma 2.3.5. *If $2|h$ and B has a $(q^{3/2}+1)$-secant, then a line can intersect B in 1, $q^{3/2}+1$ or q^3+1 points only. In this case B is linear.*

Proof. If B has a $(q^{3/2}+1)$-secant, then by Corollary 2.3.3 and Result 1.6.11 there has to be a plane π intersecting B in a Baer subplane. Through a point $P \in \pi \cap B$, there are $q^{3/2}+1$ $(q^{3/2}+1)$-secants in π. Suppose now that there is a line l through P, not in π, which intersects B in $q+1$, q^2+1 or q^2+q+1 points. The planes containing l and a $(q^{3/2}+1)$-secant have to intersect B in more than q^4-q^3 points (see Result 1.6.11 that a small minimal planar blocking set having a $(q^{3/2}+1)$-secant can have tangents or $(q^{3/2}+1)$-secants only), but there are $q^{3/2}+1$ such planes, which is in contradiction with (1) and (2) of Lemma 2.3.4.

Thus, B meets all lines in 1 mod $q^{3/2}$ points, so by Result 1.6.10 B is linear. ■

For the rest of this section we will assume that B has no $(q^{3/2}+1)$-secants, and thus no Baer plane sections. All lines intersect B in a linear set of size 1, $q+1$, q^2+1, q^2+q+1, or q^3+1. A plane can intersect B in a line, a small minimal blocking set described in (1) or (2) of Result 1.6.11 or in more than q^4-q^3 points.

Definition 2.3.6. We will call a point $P \in B$ *a special point of B*, if there is a plane π through P for which $\pi \cap B$ is the small minimal blocking set described in (1) of Result 1.6.11, and P is the *special point* of this point set.

The following lemma summarizes some properties of special points of B.

Lemma 2.3.7. (1) *On every (q^2+1)-secant there is exactly one special point.*

(2) *The lines through a special point can be tangents, lines totally contained in B, or (q^2+1)-secants only.*

(3) *Two special points are always connected by a line contained in B.*

Proof. (1) Result 2.2.6.

(2) Let P be a special point, l a (q^2+1)-secant through P. According to Lemma 2.3.4, more than q^3+1-2q of the planes on l intersect B in the small minimal blocking set (1) of Result 1.6.11, thus more than $(q^3+1-2q)q+1$ of the lines through P have to be (q^2+1)-secants.

If m is a (q^2+q+1)-secant on P, then because of Corollary 2.3.3 there has to be a plane on m in which there are $(q+1)$-secants on P.

Now let m be a $(q+1)$-secant on P. Assume that a plane π on m intersects B in the small minimal blocking set (1) of Result 1.6.11. From Remark 1.6.12 it is clear that in this blocking set, on a special point there are tangents or (q^2+1)-secants only. Thus, the special point of $\pi \cap B$ has to be a point Q, different from P and the line PQ is a (q^2+1)-secant of $\pi \cap B$. But this would be in contradiction with (1), because P and Q would be two special points of the line PQ. Thus, all the planes on m intersect B in the small minimal blocking set (2) of Result 1.6.11 or in more than $q^4 - q^3$ points. By (1) of Lemma 2.3.4, there can be at most 3 planes meeting B in more than $q^4 - q^3$ points, and thus, there can be at most 3 planes on m containing (q^2+1)-secants on P, which means that the number of (q^2+1)-secants on P can be at most $3q^3$, a contradiction. Thus, there are no $(q+1)$- or (q^2+q+1)-secants on P.

(3) is a direct consequence of (1) and (2). ∎

Proposition 2.3.8. *If π is a plane of* $\mathrm{PG}(3, q^3)$ *such that* $|\pi \cap B| > q^4 + 3q^3$, *then B is of Rédei type and π is a Rédei plane.*

Proof. First observe that there are no special points outside π. If $S \in B$ were a special point, $S \notin \pi$, then according to Lemma 2.3.7(2), all lines connecting S with a point of $B \cap \pi$ would intersect B in at least q^2+1 points. This would give $|B| > (q^4 + 3q^3)q^2 + 1$, contradicting Lemma 2.3.1.

Now we will prove that there are no $(q+1)$-secants in π. Suppose on the contrary that l is a $(q+1)$-secant in π. If a plane through l intersects B in a small minimal blocking set, it has to be the one given in (2) of Result 1.6.11, as there are no special points outside π. But even if all the planes through l (other than π) would intersect B in small minimal blocking sets, we would reach contradiction with Lemma 2.3.1, because counting the points of B in these planes would give $|B| > q^4 + 3q^3 + q^3(q^3 + q^2)$. Thus, $\pi \cap B$ has no $(q+1)$-secants.

Let $l \not\subset \pi$ be a line meeting π in the point $P \in \pi \setminus B$. Assume $|l \cap B| > 1$, that is (as there are no special points outside π) $|l \cap B| = q+1$ or q^2+q+1. Let α be a plane on l, and let $m := \alpha \cap \pi$. If l is a $(q+1)$-secant of B and m a (q^2+q+1)-secant, then the plane α meets B in more than $q^4 - q^3$ points, because in a small minimal planar blocking set every $(q+1)$-secant has to meet the (q^2+q+1)-secant in a point belonging to the set (see Result 1.6.11), but $P = l \cap m \notin B$. With similar arguments $|\alpha \cap B| > q^4 - q^3$ if l is a $(q+1)$-secant and m a (q^2+1)-secant, and clearly $|\alpha \cap B| > q^4 - q^3$ if l is a (q^2+q+1)-secant and m a (q^2+1)-secant or a (q^2+q+1)-secant.

By Lemma 2.3.4, as l is a $(q+1)$-secant or a (q^2+q+1)-secant, then there are less than $2q$ planes on l intersecting B in more than $q^4 - q^3$ points. By these reasonings there are less than $2q$ lines on P meeting $B \cap \pi$ in more than one point. As every line of π on P contains at most q^2+q+1 points of B, we have $|B \cap \pi| < q^3 + 1 + 2q(q^2+q)$, but this is in contradiction with the lower bound on $|B \cap \pi|$.

Thus, for the point $P \in \pi \setminus B$, all the lines through P, but not in π are tangents to B, and this means that $|B \setminus \pi| = q^6$, and so B is of Rédei type with π a Rédei plane. ■

Corollary 2.3.9. *If there is a line contained in B and a special point of B not on this line, then B is a Rédei type blocking set.*

Proof. If a plane contains a line of B and a special point of B not on the line, then it contains at least $q^2(q^3+1)+1$ points of B, because by (2) of Lemma 2.3.7 any line on a special point which intersects B in at least 2 points, has to intersect it in at least q^2+1 points. ■

The following is a technical lemma, which will be useful for us.

Lemma 2.3.10. *Let $P \in B$ be a non-special point and t a tangent on P. Denote by N the number of planes on t which intersect B in the small minimal blocking set of type (1) of Result 1.6.11 and M is the number of planes on t which intersect B in a line. Suppose that $M \leq q$ and $N \leq q^2$. Then all the planes on t intersect B in small minimal blocking sets and*

$$|B| = (q^3+1)(q^3+q^2+q) + 1 - M(q^2+q) - Nq.$$

Proof. Having a plane on t which intersects B in more than $q^4 - q^3$ points would result in

$$|B| > q^4 - q^3 + q^3(q^3+q^2+q) + 1 - q(q^2+q) - q^2q,$$

which is in contradiction with the bound of Lemma 2.3.1. Thus, $|B| = N(q^3+q^2) + Mq^3 + (q^3+1-N-M)(q^3+q^2+q)+1$. ■

Lemma 2.3.11. *At least one line is totally contained in B.*

Proof. Suppose on the contrary that there are no lines contained in B. Then by Lemma 2.3.7(3), there can be at most one special point in B. Let P be a nonspecial point of B and t a tangent on P. By Lemma 2.3.10,

$$|B| = (q^3 + 1)(q^3 + q^2 + q) - Nq + 1,$$

where $N \leq 1$ is the number of special points in B.

Now if $N = 1$, then let l be a $(q + 1)$-secant of B in a plane which intersects B in the small minimal blocking set (1) of Result 1.6.11, while if $N = 0$ then let l be any $(q + 1)$-secant of B. Counting the points of B in the planes on l yields that one plane π has to intersect B in exactly $q^4 + q^3 + q^2 + q + 1$ points. By the choice of l, there is no special point in π. From this it follows, that there are no $(q^2 + 1)$-secants on π. There are no tangents on π either, because having a tangent t would lead to a contradiction with Lemma 2.3.10 (with $P := t \cap B$, $N \leq 1$, $M = 0$, and $\pi \cap B$ not being a small minimal blocking set).

Thus, through a point of π not belonging to B there can be $(q + 1)$-secants or $(q^2 + q + 1)$-secants in π only. Denote by L the number of $(q^2 + q + 1)$-secants in π on a point $Q \in \pi \setminus B$. We have:

$$|B \cap \pi| = L(q^2 + q + 1) + (q^3 + 1 - L)(q + 1),$$

from which $L = 1$. Now denote by K the number of $(q^2 + q + 1)$-secants in π. Double-counting the number of pairs (Q, m), $Q \in \pi \setminus B$, m a $(q^2 + q + 1)$-secant on Q, we get:

$$(q^6 + q^3 + 1 - |\pi \cap B|) \cdot 1 = K \cdot (q^3 - q^2 - q),$$

which has no integer solutions for K. ∎

Proposition 2.3.12. *If there are at least two lines contained in B, then B is of Rédei type.*

Proof. Any two lines totally contained in B must intersect, as two skew lines would contradict Lemma 2.3.4(3). Let l_1 and l_2 be lines contained in B and let $P = l_1 \cap l_2$. If there is a special point in $B \setminus \{P\}$ or if P is special and there are further lines in B that are not on P, then by Corollary 2.3.9, B is of Rédei type.

Case 1: Suppose now that P is the only special point of B and all the lines of B go through P. Let Q be any point on a line of B through P. From Lemma

2.3.10,

$$|B| = (q^3+1)(q^3+q^2+q)+1-q^2-q.$$

Now let R be any point of B which is on a (q^2+1)-secant through P. Then again from Lemma 2.3.10,

$$|B| = (q^3+1)(q^3+q^2+q)+1-q,$$

but this is a contradiction. Thus, there are no (q^2+1)-secants through P, and P is not a special point.

Case 2: Suppose now that there are no special points in B at all and again $P = l_1 \cap l_2$, where l_1 and l_2 are lines contained in B. If there is a $(q+1)$- or a (q^2+q+1)-secant on P then by (1) and (2) of Lemma 2.3.4 we can find a $(q+1)$-secant l on P which is not in the plane $\langle l_1, l_2 \rangle$. As the planes $\langle l, l_1 \rangle$ and $\langle l, l_2 \rangle$ both contain at least q^4+q^3+1 points of B, we have $|B| \geq 2(q^4+q^3-q)+(q^3-1)(q^3+q^2)+q+1$, which is in contradiction with Lemma 2.3.1. Thus, there are no $(q+1)$- or (q^2+q+1)-secants on P and B has to be a cone with vertex P. The base of this cone is a plane section of B, but from Lemma 2.3.1 $|B| \geq q^3(q^4-q^3)+1$ is not possible. Thus, the base is a small minimal blocking set, which is either a line, or a blocking set of type (2) of Result 1.6.11. This planar blocking set is of Rédei type, and so the cone is of Rédei type also. ■

Proposition 2.3.13. *B is either of Rédei type, or is a blocking set with the following properties:*

- *$|B| = q^6+q^5+q^4+q^3+1$;*
- *There is exactly one line l contained in B. There are $q+1$ special points in B and all are on the line l.*
- *On a nonspecial point of l there are tangents and $(q+1)$-secants only. On a special point of l there are tangents and (q^2+1)-secants only.*
- *There are q^2+q+1 planes on l containing further points of B. These planes meet B in q^4+q^3+1 points.*
- *On a $(q+1)$-secant meeting the line l, there is one plane meeting B in q^4+q^3+1 points (the plane on l), and all other planes intersect B in the small minimal blocking set (2) of Result 1.6.11.*

Proof. By Lemma 2.3.11, Proposition 2.3.12 and Corollary 2.3.9, we can assume that there is exactly one line l totally contained in B and all the special points of B (if there are any) are on l. If there are at least $4q$ special points on l, then a plane on l which contains further points of B will contain at least $4qq^2+(q^3+1-4q)q+1$ points of B, and thus by Proposition 2.3.8, B is of Rédei type.

Suppose now, that the number of special points is less than $4q$. Let P be any non-special point of the line l containing the special points and let t be a tangent of P such that the plane $\langle t, l\rangle$ intersects B in the points of l only. By Lemma 2.3.10,

$$|B| = q^3(q^3+q^2+q)+q^3+1.$$

Now let P be a point of B not on the line l, and t a tangent of P. Again by Lemma 2.3.10, we have

$$|B| = (q^3+1)(q^3+q^2+q) - Nq + 1,$$

with N the number of special points in B. From this $N = q+1$.

Let π be a plane on the line l and containing further points of B. As there are $q+1$ special points on l, counting the points of $B \cap \pi$ on the lines through a point of $\pi \cap B$ not on l we have: $|B \cap \pi| \geq (q+1)q^2+(q^3-q)q+1$. Counting the points of B in the planes on any $(q+1)$-secant m of π, we have $|B| \geq q^3(q^3+q^2)+|B\cap\pi|$, because there are no special points outside π, and so the small sections on m can be of type (2) of Result 1.6.11 only. From the size of B we have $|B \cap \pi| = q^4+q^3+1$, and equality has to hold above. From this it is clear that a point of $\pi \setminus l$ is connected to the special points of l by (q^2+1)-secants, and to the non-special points by $(q+1)$-secants. It is also clear, that on a $(q+1)$-secant which intersects l, all the planes not containing l will intersect B in the small minimal blocking set (2) of Result 1.6.11. Counting the points of B in the planes on l, we see that there are exactly q^2+q+1 planes containing q^4+q^3+1 points of B, and all other planes meet B in l. ∎

Remark 2.3.14. The blocking set with the properties above is not a Rédei type blocking set. The Rédei plane would have to contain $|B| - q^6 = q^5+q^4+q^3+1$ points and (by the proof of Proposition 2.3.8) would have to contain all the special points of B. But the planes containing the special points of B all contain q^4+q^3+1 points of B.

Notation: Let V be the GF(q^3)-vector space of rank 4 defining PG$(3,q^3)$. For a line e we will use the notation $e^B := e \cap B$. Suppose that P is a point of B and $e_1, \dots, e_s$ are lines on P such that all sets e_i^B are sublines isomorphic to PG$(1,q)$. Let $v \in V$ be any vector representing P. Then V has a unique GF(q)-subspace V_i of rank two containing v and representing exactly the points of e_i^B. Consider the GF(q)-span of the vectors in $V_1 \cup \dots \cup V_s$. The set of all points of PG$(3,q^3)$ generated by vectors in this GF(q)-span will be denoted by $\langle e_1^B, \dots, e_s^B \rangle_q$. Notice that this definition does not depend on the choice of the vector v representing P: using a vector $v' = \lambda v$ with $\lambda \in$ GF(q^3), $\lambda \neq 0$, will result in the set of all points of PG$(3,q^3)$ generated by the GF(q)-span of vectors in $\lambda V_1 \cup \dots \cup \lambda V_s$, which is the same set. If the V_i subspaces are GF(q)-independent, then $\langle e_1^B, \dots, e_s^B \rangle_q$ is an s-dimensional GF(q)-linear subspace.

Lemma 2.3.15. *Suppose that B is as described in Proposition 2.3.13. Let P be a point not on l and consider two $(q+1)$-secants l_1 and l_2 on P such that l_1 meets l. Then $\langle l_1^B, l_2^B \rangle_q$ is contained in B.*

Proof. Case 1: l_2 is skew to l. Then the plane $\langle l_1, l_2 \rangle$ meets B in a small blocking set and the assertion follows by inspection of the small blocking sets. Alternatively, the small blocking set is GF(q)-linear, which also proves the claim.

Case 2: l_2 meets l, that is the plane $\pi = \langle l_1, l_2 \rangle$ contains l. Then $E_1 := l \cap l_1$ and $E_2 := l \cap l_2$ are non-special points of l. It suffices to show for all points $R \in l_2^B$ that the set $E_1 R \cap \langle l_1^B, l_2^B \rangle_q$ is contained in B. This holds for $R = P$ and $R = E_2$ (because the line $E_1 E_2 = l$ is contained in B). Suppose therefore that $R \neq P, E_2$.

As stated in Proposition 2.3.13, all planes on l_2 other than π intersect B in small minimal blocking sets (2) of Result 1.6.11. Thus, we can find a point E_3 outside π such that $l_3 := PE_3$ and $E_3 R$ are $(q+1)$-secants. By Proposition 2.3.13, the line $E_1 E_3$ is a $(q+1)$-secant also.

From Case 1 we see that $\langle l_1^B, l_3^B \rangle_q$ is contained in B. As $E_1 E_3$ contains the points E_1, E_3 of this set, it follows that

$$(E_3 E_1)^B \subseteq \langle l_1^B, l_3^B \rangle_q.$$

Similarly

$$(E_3 R)^B \subseteq \langle l_2^B, l_3^B \rangle_q \quad \text{and} \quad (E_1 R)^B \subseteq \langle (E_3 E_1)^B, (E_3 R)^B \rangle_q.$$

Hence $(E_1R)^B \subseteq \langle l_1^B, l_2^B, l_3^B\rangle_q$. As E_1R is also contained in π, it follows that $(E_1R)^B \subseteq \langle l_1^B, l_2^B\rangle_q$. ■

Lemma 2.3.16. *Let B be a point set with the properties given in Lemma 2.3.13. Then B is a linear blocking set.*

Proof. Let P be any point of B not on the line l containing the special points, and let π be the plane on P and l. Take any two $(q+1)$-secants e_1, e_2 through P in π, let $E_1 := e_1 \cap l$ and $E_2 := e_2 \cap l$. By the previous lemma, we have $\langle e_1^B, e_2^B\rangle_q \subseteq B$. Let e_3 be a third $(q+1)$-secant of π on P meeting the set $\langle e_1^B, e_2^B\rangle_q$ only in point P, and let $E_3 := e_3 \cap l$.

We will now prove that $\langle e_1^B, e_2^B, e_3^B\rangle_q$ is also contained in B. Because of Lemma 2.3.15, $\langle e_1^B, e_3^B\rangle_q$ and $\langle e_2^B, e_3^B\rangle_q$ are contained in B, thus, for any point $R \in e_3^B$ it is true that $\langle e_1^B, e_2^B, e_3^B\rangle_q \cap RE_1 \subseteq RE_1 \cap B$ and $\langle e_1^B, e_2^B, e_3^B\rangle_q \cap RE_2 \subseteq RE_2 \cap B$. Equality holds, if and only if $R \notin l$, because in this case RE_1 and RE_2 are $(q+1)$-secants of $B \cap \pi$. Applying Lemma 2.3.15 to R and the $(q+1)$-secants RE_1 and RE_2, we have that $\langle (RE_1)^B, (RE_2)^B\rangle_q \subset B$. Every point of $\langle e_1^B, e_2^B, e_3^B\rangle_q$ is contained in one of the sets $\langle (RE_1)^B, (RE_2)^B\rangle_q$ with $R \in e_3^B$, and thus $\langle e_1^B, e_2^B, e_3^B\rangle_q \subset B$ follows.

With this we have found a 3-dimensional GF(q)-linear subspace containing P and contained in B. The number of $(q+1)$-secants a 3-dimensional subspace can generate on a point is at most q^2+q+1, but in π the number of $(q+1)$-secants on P is q^3-q (see Proposition 2.3.13) and thus there have to be further $(q+1)$-secants of π on P. Take one and denote it by e_4, and let $E_4 := e_4 \cap l$. We will prove $\langle e_1^B, e_2^B, e_3^B, e_4^B\rangle_q \subset B \cap \pi$. By Lemma 2.3.15 we have that $\langle e_1^B, e_4^B\rangle_q$, $\langle e_2^B, e_4^B\rangle_q$ and $\langle e_3^B, e_4^B\rangle_q$ are contained in B. Thus, for any point $R \in e_4^B \setminus E_4$ the set $\langle e_1^B, e_2^B, e_3^B, e_4^B\rangle_q$ meets the lines RE_1, RE_2 and RE_3 in the sets $RE_1 \cap B$, $RE_2 \cap B$ and $RE_3 \cap B$ respectively (these are all $(q+1)$-secants). Clearly from the reasonings of the previous paragraph $\langle (RE_1)^B, (RE_2)^B, (RE_3)^B\rangle_q \subset B$ if $R \in e_4^B$. (Note that $(RE_3)^B \not\subset \langle (RE_1)^B, (RE_2)^B\rangle_q$, but we don't need it in the proof.) From this $\langle e_1^B, e_2^B, e_3^B, e_4^B\rangle_q \subset B \cap \pi$ clearly follows.

The number of (q^2+1)-secants on P in π is $q+1$ and the number of $(q+1)$-secants on P in π is q^3-q, thus the lines on P in π can contain at most $(q^3-q)+(q+1)(q+1)$ sublines, and this proves $\langle e_1^B, e_2^B, e_3^B, e_4^B\rangle_q = B \cap \pi$.

Now let α be a plane on e_1 different from π. By the properties of B, $\alpha \cap B$ is the small minimal blocking set (2) of Result 1.6.11. This is a linear blocking set, thus there are $(q+1)$-secants e_5 and e_6 on P such that $\langle e_1^B, e_5^B, e_6^B\rangle_q = \alpha \cap B$. We will now prove that $\langle e_1^B, e_2^B, e_3^B, e_4^B, e_5^B, e_6^B\rangle_q \subset B$.

There is exactly one (q^2+q+1)-secant on α, and we may suppose that P is not contained in it (if it were, then choose another point as P). Thus, for any point $R \in \alpha \cap B$ the line PR is a $(q+1)$-secant. By Lemma 2.3.15, $\langle (PR)^B, e_i^B\rangle \subset B$ for all $i = 1, \ldots, 4$ and all $R \in \alpha \cap B$, $R \neq E_1$. Then the lines RE_i all meet the set $\langle e_1^B, e_2^B, e_3^B, e_4^B, e_5^B, e_6^B\rangle_q$ in exactly the points of $RE_i \cap B$, as these are all $(q+1)$-secants of B. We can apply the reasonings of the previous paragraphs of this proof to R in place of P, and then we obtain $\langle (RE_1)^B, (RE_2)^B, (RE_3)^B, (RE_4)^B, \rangle_q \subset B$. But from this $\langle e_1^B, e_2^B, e_3^B, e_4^B, e_5^B, e_6^B\rangle_q \subset B$ follows.

Thus, B contains a 6-dimensional GF(q)-linear subspace, in other words a projected PG$(6,q)$ subgeometry. Such a projected subgeometry blocks all the lines of PG$(3,q^3)$, and so if B contained further points, it would be in contradiction with the minimality of B. ■

Proof of Theorem 2.1.1 for $n = 3$ and $k = 1$. In this section, through a series of lemmas we proved the following theorem.

Theorem 2.3.17. *Let B be a point set of* PG$(3,q^3)$*, $q = p^h$, $p \geq 7$ prime, intersecting each line in* 1 mod q *points, and with size $|B| < \frac{3}{2}(q^{3(n-1)}+1)$. Then B is a linear blocking set.*

Proof. Clearly by Result 1.6.7, B is a small minimal blocking set of PG$(3,q^3)$. If $2|h$ and B has a $(q^{3/2}+1)$-secant, then B is linear by Lemma 2.3.5. If B has no $(q^{3/2}+1)$-secants, then by Proposition 2.3.13, B is either a blocking set of Rédei type, and thus linear by Result 1.6.4, or B is the blocking set described in Lemma 2.3.13, and linear by Lemma 2.3.16. ■

2.4 Proof of Theorem 2.1.1 for $k = 1$, $n \geq 4$

Throughout the section it will be assumed that B is a point set of $\mathrm{PG}(n, q^3)$, $q = p^h$, $1 \leq h$, $7 \leq p$ *prime, and* $n \geq 4$. *Furthermore,* $|B| < \frac{3}{2}(q^{3(n-1)} + 1)$ *and* B *intersects every line of* $\mathrm{PG}(n, q^3)$ *in* $1 \bmod q$ *points.*

Our technique will be to prove that the plane sections of such point set are always linear, and then prove the linearity of the whole set similarly as in Lemma 2.3.16. For the size of B, we will again use an upper bound which follows from Result 1.6.9.

Lemma 2.4.1. $|B| < q^{3(n-1)} + q^{3(n-2)+2} + q^{3(n-2)+1} + 3q^{3(n-2)}$.

Lemma 2.4.2. *A 3-dimensional subspace of* $\mathrm{PG}(n, q^3)$ *either intersects* B *in a small minimal blocking set, or contains more than* $q^7 - q^6$ *points from* B.

Proof. A 3-dimensional subspace has $b := (q^6 + 1)(q^6 + q^3 + 1)$ lines, and $r := q^6 + q^3 + 1$ lines on every point. With these values for b and r, equation (2.1) in the proof of Lemma 2.3.2 remains true in our situation. As the right-hand side of this equation is negative for $x = \frac{3}{2}q^6 + 1$ and $x = q^7 - q^6$, the assertion follows. ■

Corollary 2.4.3. *On any plane of* $\mathrm{PG}(n, q^3)$ *there has to be a 3-dimensional subspace which intersects* B *in a small minimal blocking set.*

Proof. If all 3-spaces on a plane π contained more than $q^7 - q^6$ points from B, then counting the points of B in these 3-spaces would yield

$$|B| \geq (q^{3(n-3)} + q^{3(n-4)} + \cdots + 1)(q^7 - q^6 - |\pi \cap B|) + |\pi \cap B|,$$

which is in contradiction with Lemma 2.4.1, as $|\pi \cap B| \leq q^6 + q^3 + 1$. ■

Corollary 2.4.4. *Every plane* π *of* $\mathrm{PG}(n, q^3)$ *intersects* B *in a linear point set. Thus,* $\pi \cap B$ *is either a line, a projected* $\mathrm{PG}(m, q)$ *subgeometry, with* $3 \leq m \leq 8$, *or a Baer subplane* (*then* q *is a square*).

Proof. By Corollary 2.4.3, every plane π is contained in a 3-dimensional space which intersects B in a small minimal blocking set. Theorem 2.3.17 proves that the intersection is a linear point set, and thus $\pi \cap B$ is also a linear point set.

By Lemma 2.2.10, if $\pi \cap B$ is a GF(q)-linear blocking set of π, then it has to be a projected PG(m, q), with $3 \leq m \leq 8$. If $\pi \cap B$ is GF($q^{3/2}$)-linear, then it is a Baer subplane. ■

Corollary 2.4.5. *An arbitrary line intersects B in a linear point set of size 1, $q+1$, q^2+1, q^2+q+1, q^3+1, or $q^{3/2}+1$ (then q is a square).*

In case $2|h$ we will now characterize the blocking sets which have a $(q^{3/2}+1)$-secant.

Lemma 2.4.6. *If $2|h$ and B has a $(q^{3/2}+1)$-secant, then B intersects every line in $1 \bmod q^{3/2}$ points. In this case B is linear.*

Proof. If B has a $(q^{3/2}+1)$-secant m and a $(q+1)$-, a (q^2+1)- or a (q^2+q+1)-secant l, then these lines have to be skew by Corollary 2.4.4. Now for any points $P \in l \setminus B$ and $Q \in m$ the line PQ has to be a tangent to B, as any other intersection number would lead to contradiction. Thus, the plane $\langle P, m \rangle$ meets B in q^3+1 points which are not collinear, contradicting Corollary 2.4.4. This proves that if B has a $(q^{3/2}+1)$-secant, then B has no $(q+1)$-, (q^2+1)- or (q^2+q+1)- secants. B meets every line in $1 \bmod q^{3/2}$ points, and is linear by Result 1.6.10. ■

Lemma 2.4.7. *Suppose now that B has no $(q^{3/2}+1)$-secants. If there is a $(q+1)$-secant on a point $P \in B$, then the number of $(q+1)$-secants on P is at least $q^{3n-4} - q^{3n-6}$.*

Proof. Let l be a $(q+1)$-secant on the point $P \in B$. By Corollary 2.4.4 and Lemma 2.2.10, a plane on l meets B in a projected PG($3, q$) or a projected PG($4, q$). In both cases P is an ordinary point by Corollary 2.2.3. In the first case there are at least q^2-1 further $(q+1)$-secants on P (see Remark 1.6.12). In the latter case there are at least q^3-q further $(q+1)$-secants on P by Lemma 2.2.10(4). Thus, in any plane on l there are at least q^2-1 further $(q+1)$-secants on P, and the number of $(q+1)$-secants on P is at least $(q^2-1)(q^{3(n-2)}+q^{3(n-3)}+\cdots+1) \geq q^{3n-4} - q^{3n-6}$. ■

We are now ready to prove the main theorem. We will again use the notation $\langle e_1^B, \ldots, e_s^B \rangle_q$ given before Lemma 2.3.15.

Theorem 2.4.8. *Let B be a point set of* $\mathrm{PG}(n, q^3)$*,* $q = p^h$*,* $1 \le h$*,* $7 \le p$ *prime,* $n \ge 4$*. Let* $|B| < \frac{3}{2}(q^{3(n-1)} + 1)$ *and assume that B intersects every line of* $\mathrm{PG}(n, q^3)$ *in* $1 \bmod q$ *points. Then B is a linear point set.*

Proof. By Result 1.6.7, B is a minimal blocking set of $\mathrm{PG}(n, q^3)$. If B is a hyperplane, or B has a $(q^{3/2} + 1)$-secant, then B is a linear point set (Corollary 2.4.6).

Now we may assume that B has no $(q^{3/2} + 1)$-secants, and so by Corollary 2.4.4, every plane meets B in a projected $\mathrm{PG}(m, q)$, with $3 \le m \le 8$. If B has a (q^2+1)- or a $(q^2 + q + 1)$-secant, then B has to have $(q + 1)$-secants also, or else all the planes on such a secant would meet B in a projected $\mathrm{PG}(5, q)$, which would be in contradiction with the size of B.

Let $P \in B$ be a point on a $(q + 1)$-secant. By Lemma 2.4.7, there are many $(q+1)$-secants on P. Let e and f be two $(q+1)$-secants of B meeting in the point P. The plane $\langle e, f\rangle$ meets B in a projected $\mathrm{PG}(m, q)$ subgeometry, and P is an ordinary point of $\langle e, f\rangle \cap B$ (Corollary 2.2.3). Thus, e^B and f^B are projections of intersecting lines of $\mathrm{PG}(m, q)$. Then the subplane $\langle e^B, f^B\rangle_q$ generated by them is the image of the plane of $\mathrm{PG}(m, q)$ generated by the pre-images, so $\langle e^B, f^B\rangle_q \subset B$.

Now suppose that $e_1, e_2, \ldots, e_s$ are $(q + 1)$-secants through $P \in B$, such that $e_i^B \notin \langle e_1^B, \ldots, e_{i-1}^B\rangle_q$ for $i = 2, \ldots, s$ and $\langle e_1^B, \ldots, e_s^B\rangle_q \subset B$. If $s < 3(n - 1)$ then we can find further $(q+1)$-secants through P, as the subspace $\langle e_1^B, \ldots, e_s^B\rangle_q$ has at most $q^{s-1} + q^{s-2} + \cdots + 1$ $(q + 1)$-secants through P, and from Lemma 2.4.7 there are more. Let e_{s+1} be any further $(q+1)$-secant through P, such that $e_{s+1} \cap \langle e_1^B, \ldots, e_s^B\rangle_q = \{P\}$.

Let Σ be a 3-dimensional $\mathrm{GF}(q)$-linear subspace of $\langle e_1^B, \ldots, e_s^B, e_{s+1}^B\rangle_q$ containing $\langle e_1^B, e_{s+1}^B\rangle_q$. Σ meets $\langle e_1^B, \ldots, e_s^B\rangle_q$ in a subplane on e_1 which contains by Lemma 2.2.12 further lines f_i $(i = 1, \ldots, q - 2)$ which are all $(q + 1)$-secants of B going through P. From the reasonings above, the subplane $\langle e_{s+1}, e_1\rangle_q$ and the subplanes $\langle e_{s+1}, f_i\rangle_q$ are all contained in B. Suppose now that $Q \in \Sigma$ is not on any of these planes. Again by Lemma 2.2.12, among the q further $\mathrm{GF}(q)$-linear subplanes on the line PQ in Σ we can find a subplane which intersects two of the subplanes $\langle e_{s+1}, f_i\rangle_q$ in sublines which are both $(q + 1)$-secants of B. Then the subplane generated by these two $(q + 1)$-secants is contained in B and Q is an element of this subplane.

With this we have proved that any 3-dimensional GF(q)-linear subspace of the subgeometry $\langle e_1^B, \ldots, e_s^B, e_{s+1}^B \rangle_q$ containing e_1^B and e_{s+1}^B is contained in B, thus $\langle e_1^B, \ldots, e_s^B, e_{s+1}^B \rangle_q$ is contained in B.

From this it is clear that B contains a projected PG$(3(n-1), q)$ subgeometry. This projected subgeometry is a blocking set of PG(n, q^3), and so it is equal to B by the minimality of B. ■

2.5 Proof of Theorem 2.1.1 for $1 < k < n$, $n \geq 3$

The strategy used in the previous two sections was to prove that every plane section of the blocking set B is a linear point set, find a point P with many $(q+1)$-secants on it, and then 'build' a linear point set in B. This last case ($k \geq 2$, $n \geq 3$) can also be proved this way, but now we present a different method. We will project the blocking set B into a hyperplane, use induction on k to represent the projected set B' in the hyperplane as a linear set, and finally lift the linear structure back to B. In [29] Lavrauw, Storme and Van de Voorde present a third method to solve the same problem.

Our methods have the advantage that one needs to study only the plane sections of the blocking set. There is hope that these techniques may be generalized in order to help solving similar problems. For example in the classification of small blocking sets in $\mathrm{PG}(n, q^h)$ for $h > 3$, or even in the classification of sets of points in $\mathrm{PG}(n, q^h)$ that meet every plane in a linear set.

Throughout this section it will be assumed that B is a point set of $\mathrm{PG}(n, q^3)$, with $q = p^h$, $1 \leq h$, $7 \leq p$ prime and $2 \leq k \leq n-1$, meeting all k-subspaces in $1 \bmod q$ points and $|B| < \frac{3}{2}(q^{3(n-k)} + 1)$.

We will be using the fact that every subspace of $\mathrm{PG}(n, q^3)$ that meets B, meets it in $1 \bmod q$ points by Result 1.6.7.

Lemma 2.5.1. *If U is a point not in B, then projecting B from U into a hyperplane H produces a small minimal blocking set B' of H with respect to $(k-1)$-subspaces. If B' is a subspace, then B is a linear blocking set.*

Proof. As B meets all k-subspaces, so B' meets all $(k-1)$-subspaces of H. Every subspace that meets B meets it in $1 \bmod q$ points, so the same is true for B'. Result 1.6.7 implies that B' is a minimal $(n-k)$-blocking set of H.

Assume that B' is a subspace Σ of H. Then Σ has dimension $n-k$, and the subspace $\langle U, \Sigma \rangle$ of dimension $n-k+1$ contains B. As B meets every k-subspace, it follows that B meets every line of $\langle U, \Sigma \rangle$. The case $k = 1$ being handled in the previous section, it follows that B is linear. ■

Lemma 2.5.2. *Let T be a $(t-1)$-dimensional subspace meeting B in at least q^r points, with $2r$ an integer. If $r > 3(t-k) - 1$, then there is a t-dimensional subspace on T meeting B in the points $T \cap B$ only.*

Proof. Assume that this is not true. Every line that meets B in 2 points, meets it in at least $q+1$ points. Thus, every t-dimensional subspace on T contains at least $q^r(q-1)+1$ points of B outside $T \cap B$. The number of t-subspaces on T is more than $q^{3(n-t)}$, and thus: $\frac{3}{2}(q^{3(n-k)}+1) > |B| > q^{3(n-t)}(q-1)q^r$, which is a contradiction if $r+1 > 3(t-k)$ and $q \geq 7$. ■

Lemma 2.5.3. *Every line meets B in a linear point set. Let $\mathcal{S} = \{1, q+1, q^2+1, q^2+q+1, q^3+1\}$, and $\mathcal{T} = \{1, q^{3/2}+1, q^3+1\}$. Then either for all lines l of* $\mathrm{PG}(n, q^3)$ *it is true that $|l \cap B| \in \mathcal{S}$ or for all lines $|l \cap B| \in \mathcal{T}$. In the latter case B is linear.*

Proof. We will prove this by induction on k. The case $k=1$ is proved in Corollary 2.4.5 and Lemma 2.4.6. By Lemma 2.5.2, on any line l such that $|l \cap B| \geq q+1$, we can find a plane π such that $\pi \cap B = l \cap B$. Projecting B from a point $U \in \pi \setminus l$, the resulting point set is a blocking set with respect to $(k-1)$-spaces and having an $|l \cap B|$-secant. By the induction hypothesis $l \cap B$ is a linear point set, and $|l \cap B| \in \mathcal{S} \cup \mathcal{T}$.

Assume that there exist intersecting lines s and t such that $|t \cap B| = q^{3/2}+1$ and $|s \cap B| \in \mathcal{S} \setminus \mathcal{T}$. By the 1 mod q property of B, we have $|\langle s, t\rangle \cap B| \geq (q^{3/2}+1)q$, and so we can use Lemma 2.5.2 to find a 3-dimensional subspace on $\langle s, t\rangle$ which meets B in the points $B \cap \langle s, t\rangle$ only. Projecting B from a point of this 3-space not on $\langle s, t\rangle$ results in a blocking set of H with respect to $(k-1)$-spaces of H and having an $|s \cap B|$-secant and a $|t \cap B|$-secant, which is in contradiction with the induction hypothesis.

Now assume that there are lines s and t such that $|t \cap B| = q^{3/2}+1$ and $|s \cap B| \in \mathcal{S} \setminus \mathcal{T}$, but only skew lines s, t have these intersection numbers. Then all the lines connecting points of $s \cap B$ and $t \cap B$ have to be contained in B. Thus, in the 3-space generated by s and t there are more than $(q^{3/2}+1)(q+1)(q^3-1)$ points of B. Using Lemma 2.5.2 we find a 4-space on $\langle s, t\rangle$ which intersects B in the points of $\langle s, t\rangle \cap B$ only. Projecting B from a point of this 4-space not on $\langle s, t\rangle$ results in a blocking set with respect to $(k-1)$-spaces and having an $|s \cap B|$-secant and a $|t \cap B|$-secant, which is in contradiction to the induction hypothesis.

If B meets all lines in 1 mod $q^{3/2}$ points, then B meets all k-spaces in 1 mod $q^{3/2}$ points, and is linear by Result 1.6.10. ■

For the rest of this section we will assume that B has no $(q^{3/2}+1)$-secants, so all lines intersect B in a linear set of 1, $q+1$, q^2+1, q^2+q+1 or q^3+1 points. Also, for the rest of the section we fix a point U not in B and a hyperplane H not on U and consider the projection B' of B into H. In view of the preceding lemmas and the induction hypothesis, we may assume that B' is a linear minimal blocking set, a projected $\mathrm{PG}(3(n-k),q)$ subgeometry and that B' is not a subspace. Recall that a point P of a linear point set is *ordinary*, it is the projection of one point only.

Lemma 2.5.4. *Every ordinary point P' of B' is the projection of only one point of B.*

Proof. As every line meets B in no point or in 1 mod q points, every point of B' is the image of exactly one or at least $q+1$ points of B. Suppose that the ordinary point P' is the projection of $x \geq q+1$ points of B. By Lemma 2.2.14, the number of $(q+1)$-secants of B' on P' is at least $q^{3(n-k)-1} - q^{3(n-k-1)}$. The number of points of B that are projected onto a point $Q' \in B'$, which is connected to P' by a $(q+1)$-secant is at least x. To prove this, assume that $P_i \in B$, $i = 1, \ldots, x$ are the points projected onto P' and $R \in B$, $R \neq P_i$ is a point projected onto the $(q+1)$-secant connecting P' with Q'. Then the lines RP_i are all $(q+1)$-secants of B, which have to meet the line $\langle Q', U\rangle$ in a point of B. This proves $|B| \geq (q^{3(n-k)-1} - q^{3(n-k)-3})qx$, which leads to a contradiction with the upper bound on $|B|$. Hence $x = 1$. ■

Lemma 2.5.5. *If a line l' meets B' in a $\mathrm{PG}(1,q)$, then the plane $\langle l', U\rangle$ meets B in a $\mathrm{PG}(1,q)$.*

Proof. By Corollary 2.2.3, the points of $l' \cap B'$ are ordinary and then the previous lemma shows that the plane $\langle l', U\rangle$ meets B in exactly $q+1$ points. The 1 mod q property proves that they have to be collinear and thus form a $\mathrm{PG}(1,q)$. ■

Lemma 2.5.6. *Let l' be a line of H such that the points of B in the plane $\tau := \langle l', U\rangle$ are not collinear.*

(a) *If l' meets B' in a projected $\mathrm{PG}(2,q)$, then τ meets B in a $\mathrm{PG}(2,q)$.*

(b) *If the line l' meets B' in a projected $\mathrm{PG}(3,q)$, then τ meets B in a projected $\mathrm{PG}(3,q)$.*

Proof. (a) If $|l' \cap B'| = q^2 + q + 1$, then by Lemma 2.2.2, all points of $l' \cap B'$ are ordinary, so $|\tau \cap B| = q^2 + q + 1$ by Lemma 2.5.4. The 1 mod q result for B implies that $\tau \cap B$ is a projective plane of order q, an embedded PG$(2, q)$ subplane. The other possibility is that $|l' \cap B'| = q^2 + 1$ and that q^2 points of $l' \cap B'$ are ordinary and one point $S' \in B'$ is not. Then the plane $\langle l', U \rangle$ meets B in $x + q^2$ points, where x is the number of points of B on the line US'. In view of the 1 mod q result for B, we see that $B \cap \langle l', U \rangle$ must have at least $xq + 1$ points. From $x + q^2 = |B \cap \langle l', U \rangle| \geq xq + 1$ it follows that $x \leq q + 1$. The 1 mod q result shows therefore that $x = q + 1$ and that the plane $\langle l', U \rangle$ meets B in a PG$(2, q)$.

(b) In this case, every point of l' lies in B' and so $|\tau \cap B| \geq q^3 + 1$. By Lemma 2.5.2, we can find a 3-space Σ on τ which meets B only in points of τ. Choose a point in $\Sigma \setminus \tau$ and project B from this point into a hyperplane. From Lemma 2.5.1 and the induction hypothesis we have that this gives a projected PG(m, q). The image of the plane τ meets this projected PG(m, q) in a projected PG(t, q) for some t, and thus τ meets B in a projected PG(t, q). We have to show that $t = 3$. On the line l' we have a projected PG$(3, q)$ and this has ordinary points X'. The corresponding lines UX meet B then in only one point. This implies that $t \leq 3$, since for $t > 3$ a projected PG(t, q) in a plane meets every line of that plane in more than one point (Lemma 1.3.3). As $|\tau \cap B| \geq |l'| = q^3 + 1$, we have $t = 3$. ■

Notation. Let W be the vector space of rank $n + 1$ over GF(q^3) defining PG(n, q^3). As B' is a projected PG$(3(n - k), q)$ subgeometry, there exists a GF(q)-subspace V' of W of rank $3(n - k) + 1$ such that B' consists of the points which are represented by vectors $0 \neq v' \in V'$; also a point of B' is represented by a subspace of GF(q)-rank $s + 1$ of V' if and only if it meets B' a projected PG(s, q).

For the remaining of this section we will use the following notation: for any vector $0 \neq v \in W$, the point of PG(n, q^3) represented by this vector will be denoted by $\langle v \rangle$.

Let $u \in W$ with $U = \langle u \rangle$, and define V to be the set of all vectors $v \in W$ with the following properties

- $v = v' + \lambda u$ with $\lambda \in$ GF(q^3) and $0 \neq v' \in V'$,

- $\langle v\rangle$ is a point of B, and
- $\langle v\rangle$ projects from U to an ordinary point of B' (which is $\langle v'\rangle$).

We also put

$$\bar{V} := \{v + w \mid v, w \in V \cup \{0\}\}$$

As V' is GF(q)-homogeneous, the same is true for V and $\bar{V}$. We shall show that $\bar{V}$ is a GF(q)-subspace of W representing exactly the points of B. We start by showing that the vectors $\neq 0$ in $\bar{V}$ represent points of B. For this, the following notation is convenient.

Notation. A line h' of H will be called *suitable*, if it has the property that the point $\langle v+w\rangle$ lies in B for any two vectors $v, w \in V$ that represent distinct points $\langle v\rangle, \langle w\rangle$ in the plane $\langle h', U\rangle$.

It will be showed in the next two lemmas that all lines of H are suitable.

Remark. Notice that $\langle v + w\rangle \in B$ is trivial, if v and w represent the same point, since $v = v' + \lambda u$ and $w = w' + \mu u$ with $v', w' \in V'$ and $\lambda, \mu \in \mathrm{GF}(q^3)$ implies $v + w = (v' + w') + (\lambda + \mu)u$ (notice that $v' + w'$ represents a point of B' by the definition of V'). Therefore we will consider only the case when v and w represent different points, which implies that their projections to B' are also different (because $v, w \in V$ implies by definition that $\langle v'\rangle$ and $\langle w'\rangle$ are ordinary points and thus the projection of a unique point of B).

Lemma 2.5.7. *Let l' be a line of H and suppose that the points of B in the plane $\langle l', U\rangle$ are collinear. Then l' is suitable.*

Proof. Consider two different points $\langle v\rangle$ and $\langle w\rangle$ with $v, w \in V$ of the plane $\langle l', U\rangle$ and write $v = v' + \lambda u$ and $w = w' + \mu u$ with $v', w' \in V'$ and $\lambda, \mu \in \mathrm{GF}(q^3)$. Then the line on $\langle v + w\rangle$ and U meets l' in the point $\langle v' + w'\rangle$. As $v', w' \in V'$, then $v' + w' \in V'$ and hence $X' := \langle v' + w'\rangle \in B'$. Thus, the line on this point and U meets B in a point X. But as the points of B in the plane $\langle l', U\rangle$ are collinear, X is the intersection of the line on $\langle v\rangle$ and $\langle w\rangle$ with $X'U$, so $X = \langle v + w\rangle$. This shows that $\langle v + w\rangle \in B$. ■

Lemma 2.5.8. *All lines of H are suitable.*

Proof. This is trivial for lines of H meeting B' in at most one point. Thus, it suffices to consider lines l' of H that meet B' in at least two points, so they meet B' in a projected $\mathrm{PG}(s,q)$ with $s \geq 1$. If $s \geq 4$, then l' does not contain ordinary points and then there is nothing to show. Notice that $|l' \cap B|$ can be $q+1$, q^2+1, q^2+q+1 or q^3+1. We handle these cases separately. We always use the following technique.

Technique. Assume that $v', w' \in V'$ represent ordinary points of l' and let the vectors $v = v' + \lambda u$ and $w = w' + \mu u$ of V represent the points of B that are projected to these. We use a point $T' = \langle t' \rangle \in B'$, with $T' \notin l'$ and $t' \in V'$, and the points $R' = \langle v' + t' \rangle$ and $S' = \langle w' - t' \rangle$ of B'. We shall choose t' in such a way that R', S', T' will be ordinary points, and that the three lines $R'S', R'T', S'T'$ are already known to be suitable. Then we consider the pre-images T, R, S under the projection from U, and write $T = \langle t \rangle$ with $t = t' + \nu u$. As RT and ST are suitable, then $r := v + t$ and $s := v - t$ are vectors of V. Thus, r and s represent the points of B projecting to R' and S'. As the line RS is suitable, it follows that $r + s = v + w$ lies in V and we are done.

(1) $|l' \cap B| = q+1$. It follows from Lemmas 2.5.5 and 2.5.7 that all $(q+1)$-secants of B' are suitable.

(2) $|l' \cap B| = q^2 + q + 1$. By Lemma 2.2.13, there exists a plane π' in H on l' such that $\pi' \cap B'$ is a projected $\mathrm{PG}(3,q)$. Then all lines other than l' of π' meet B' in one or $q+1$ points, so all lines other than l' of π' are suitable by (1). All points of $\pi' \cap B'$ are ordinary by Lemma 2.2.3 and Corollary 2.2.2. Thus, the above technique applies and shows that $\langle v + w \rangle \in B$. Hence, all lines meeting B' in $q^2 + q + 1$ points are suitable.

(3) $|l' \cap B'| = q^2+1$. In view of Lemma 2.5.7, we may assume that the points of B in the plane $\langle U, l' \rangle$ are not collinear, so that these points form a $\mathrm{PG}(2,q)$ by Lemma 2.5.6.

As in (2), there exists a plane π' on l' meeting B' in a projected $\mathrm{PG}(3,q)$ subgeometry. See Remark 1.6.12 that $\pi' \cap B'$ has a unique non-ordinary (special) point N', and every line of π' on N' is either a tangent, or a (q^2+1)-secant of B', while all lines of π' that do not pass through N' are either tangents, or meet B' in a $\mathrm{PG}(1,q)$. Clearly, $N' \in l'$. As the $(q+1)$-secants are suitable by (1), the general technique therefore shows the following.

If $v, w \in V$ such that the points $\langle v\rangle$ and $\langle w\rangle$ project to distinct ordinary points of $l' \cap B'$ and such that $\langle v+w\rangle$ does not project to N', then $\langle v+w\rangle \in B$. As λw also represents $\langle w\rangle$, we see that $\langle v+\lambda w\rangle \in B$ for all except exactly one value λ of $\mathrm{GF}(q) \setminus \{0\}$. If we now take three non-collinear points $\langle v\rangle$, $\langle w\rangle$ and $\langle t\rangle$ of $\langle l', U\rangle$ that project to ordinary points of $l' \cap B'$, then it follows that the subplane $\mathrm{PG}(2, q)$ obtained from the $\mathrm{GF}(q)$-linear combinations of v, w, t shares at least q^2 points with the subplane $\langle l', U\rangle \cap B$. Then clearly both subplanes are equal ($q \geq 3$), and thus, $\langle v+\lambda w\rangle \in B$ for all $\lambda \in \mathrm{GF}(q)$. Hence, $\langle v+w\rangle \in B$.

We have shown that all (q^2+1)-secants are suitable.

(4) $|l' \cap B'| = q^3+1$ and l' meets B in a projected $\mathrm{PG}(3, q)$. In view of Lemma 2.5.7, we may assume that the points of B in the plane $\langle U, l'\rangle$ are not collinear, so that these points form a projected $\mathrm{PG}(3, q)$ by Lemma 2.5.6.

As $l' \cap B'$ is a projected $\mathrm{PG}(3, q)$, then by Lemma 2.2.13 l' lies in a plane π' meeting B' in a projected $\mathrm{PG}(4, q)$. Then all points of B' in $\pi' \setminus l'$ are ordinary. There are two possibilities.

The first is that π' has $q+1$ non-ordinary (special) points. In this case, l' is the only line of π' contained in B. Hence, all other lines of π' are suitable and the general technique can be used to show that l' is suitable.

The second possibility is that π' has a unique non-ordinary point N' (a superspecial point). In this case, N' lies on $q+1$ lines of π' that are contained in B', and all lines of π' that do not pass through N' are $(q+1)$-secants and hence suitable. The general technique therefore shows the following.

If $v, w \in V$ such that the points $\langle v\rangle$ and $\langle w\rangle$ project to distinct ordinary points of $l' \cap B'$ and such that $\langle v+w\rangle$ does not project to N', then $\langle v+w\rangle \in B$. As λw also represents $\langle w\rangle$, we see that $\langle v+\lambda w\rangle \in B$ for all except exactly one value λ of $\mathrm{GF}(q) \setminus \{0\}$.

As the points of B in the plane $\langle l', U\rangle$ form a projected $\mathrm{PG}(3, q)$, we find four points $\langle v_i\rangle$, $1 \leq i \leq 4$ of $\langle l', U\rangle \cap B$ that project to ordinary points of $l' \cap B'$, where $v_1, v_2, v_3, v_4 \in V$ are $\mathrm{GF}(q)$-independent. Then the $\mathrm{GF}(q)$-linear combinations of the v_i define a projected $\mathrm{PG}(3, q)$ in the plane $\langle l', U\rangle$. Our arguments show that this shares at least q^3 points with the projected $\mathrm{PG}(3, q)$ that is formed by the points of B in $\langle l', U\rangle$. Hence, both projected

PG$(3,q)$ subgeometries are equal and thus, $\langle v+\lambda w\rangle \in B$ for all $\lambda \in \mathrm{GF}(q)$. Hence, $\langle v+w\rangle \in B$. ■

Proposition 2.5.9. *Every vector* $\neq 0$ *of* $\bar{V}$ *represents a point of* B.

Proof. This means for any $v, w \in V$ with $v+w \neq 0$ that $\langle v+w\rangle$ is a point of B. This is clear, if v and w represent the same point. For different points, it follows from the fact that all lines are suitable. ■

Lemma 2.5.10. $\bar{V}$ *is closed under addition.*

Proof. It suffices to consider $v, w, t \in V$ and show that $v+w+t \in \bar{V}$.

Case 1: If two of the vectors, say v and w represent the same point of B, then we have $v = v' + \lambda_v u$ and $w = w' + \lambda_w u$ with w' being a GF(q) multiple of v'. Thus, either $v+w=0$ or $v+w = v'+w'+(\lambda_v+\lambda_w)u = (1+\lambda)v' + (\lambda_v+\lambda_w)u \in V$ by the definition of V. In both cases $v+w+t \in \bar{V}$, also by definition.

Case 2: We may suppose now that the points $v, w, t \in V$ represent different points of B. We have $v = v' + \lambda_v u$ and $w = w' + \lambda_w u$ and $t = t' + \lambda_t u$ with $v', w', t' \in V'$ and $\lambda_v, \lambda_w, \lambda_t \in \mathrm{GF}(q^3)$. Then v', w' and t' represent ordinary points of B'. The two points v and t define a subline with points t and $v+\lambda t$, $\lambda \in \mathrm{GF}(q)$. So the point $v'+\lambda t'$ is not ordinary for at most two values $\lambda \neq 0,1$, see Lemma 2.2.9. Similarly, the point $w'+(1-\lambda)t'$ is not ordinary for at most two values $\lambda \neq 0,1$. As $q \geq 7$, we find $0,1 \neq \lambda \in \mathrm{GF}(q)$ such that $v'+\lambda t'$ and $w'+(1-\lambda)t'$ correspond to ordinary points of B'. They are projected from the points of B belonging to the vectors $v+\lambda t$ and $w+(1-\lambda)t$; notice that these vectors represent in fact points of B, as $v, w, \lambda t, (1-\lambda)t \in V$ (Proposition 2.5.9). Hence, $v+\lambda t \in V$ and $w+(1-\lambda)t \in V$, so their sum $v+w+t$ is in $\bar{V}$.

Lemma 2.5.11. *The* GF(q)*-vector space* $\bar{V}$ *represents exactly the points of* B.

Proof. We already know that $\bar{V}$ is a GF(q)-vector space and that all its vectors represent points in B. Let $P = \langle v\rangle$ be any point of B with $v \in V$, and let P' be its projection to B'. Then the number of $(q+1)$-secants to B' on the point P' is at least $q^{3(n-k)-1} - q^{3(n-k)-3}$ by Lemma 2.2.14. The points on these lines are ordinary points of B' (Corollary 2.2.3) and thus project from exactly one point of B (Lemma 2.5.4); by definition, these are represented by vectors of V. It follows that V represents at least $q^{3(n-k)} - q^{3(n-k)-2}$ points of B, and so $\bar{V}$ has rank at least $3(n-k)+1$. But such a vector space represents a blocking set with respect to k-spaces, and so has to represent exactly the points of B, because of the minimality of B. ∎

Thus, we have proved that B is a linear point set, which proves Theorem 2.1.1 for $2 \leq k \leq n-1$ and $n \geq 3$.

2.6 Blocking sets $\mathrm{PG}(6,q)$ in $\mathrm{PG}(n,q^3)$

In the previous sections we proved that all small minimal $(n-k)$-blocking sets of $\mathrm{PG}(n,q^3)$, $q=p^h$, $1 \leq h$, $7 \leq p$ prime, with size in the interval $[\theta_{n-k}, u_{q^3}(n,k,h)]$ are linear.

For $n-k=1$ this means that such a blocking set is either a line, a projected $\mathrm{PG}(3,q)$ subgeometry, or an embedded $\mathrm{PG}(2,q^{3/2})$ subgeometry, if q is a square. These are all well-known sets: an embedded $\mathrm{PG}(2,q^{3/2})$ subgeometry is a Baer subplane, while a projected $\mathrm{PG}(3,q)$ subgeometry can either be a $\mathrm{PG}(3,q)$ subgeometry embedded in a 3-space of $\mathrm{PG}(n,q^3)$ or one of the planar blocking sets described in Result 1.6.11, contained in a plane of $\mathrm{PG}(n,q^3)$.

If $n-k=2$, then our result shows that a small minimal 2-blocking set of $\mathrm{PG}(n,q^3)$, $n \geq 3$, with size in the given interval is either a plane, a projected $\mathrm{PG}(6,q)$ subgeometry, or a projected $\mathrm{PG}(4,q^{3/2})$ subgeometry, if q is a square. Simple calculations reveal that a projected $\mathrm{PG}(4,q^{3/2})$ subgeometry is either an embedded $\mathrm{PG}(4,q^{3/2})$ subgeometry ($n \geq 4$), or a cone with base a Baer-subplane, vertex a point. The situation is much more interesting in the case of projected $\mathrm{PG}(6,q)$ subgeometries. In this section we will give a complete classification of the projections of $\mathrm{PG}(6,q)$ into $\mathrm{PG}(3,q^3)$. This classification is of special interest, because one case will lead to a linear blocking set which is not of Rédei type, and the existence of such a set was not known for some time.

As for $n-k \geq 3$: the projected $\mathrm{PG}(2(n-k),q^{3/2})$ subgeometries are again either embedded subgeometries or cones (see [47]), and the projected $\mathrm{PG}(3(n-k),q)$ subgeometries can be examined with the techniques of this section, but with the growth of $n-k$ the number of cases to be examined increases.

Notation. Consider a $\mathrm{PG}(m,q)$ subgeometry embedded in $\mathrm{PG}(m,q^3)$. Recall that for every subspace S of $\mathrm{PG}(m,q)$, we call the subspace of $\mathrm{PG}(m,q^3)$ generated by the points of S the *extension* of S. For every subspace U of $\mathrm{PG}(m,q^3)$ consider the smallest subspace of $\mathrm{PG}(m,q)$ whose extension contains U; this is the meet of all subspaces whose extension contains U. We will denote this subspace by $S(U)$.

For a point P, the dimension of $S(P)$ can be 0, 1 or 2, and clearly $\dim S(P) = 0$ if and only if P is a point of $\mathrm{PG}(m,q)$. A point of $\mathrm{PG}(m,q^3)$ will be called a *stabbing point*, if $\dim S(P) = 1$. These are the points on the extensions of the lines of $\mathrm{PG}(m,q)$ which are not in $\mathrm{PG}(m,q)$.

Note that if $P_1, P_2, \ldots, P_k$ are points generating the subspace U, then $S(U) = \langle S(P_1), \ldots, S(P_k)\rangle$. The next lemma follows from this fact, but it can also be easily seen algebraically.

Lemma 2.6.1. *For any subspace U of* $\mathrm{PG}(m,q^3)$

$$\dim S(U) \leq 3\dim(U) + 2.$$

Lemma 2.6.2. *Consider* $\mathrm{PG}(m,q)$ *embedded in* $\mathrm{PG}(m,q^3)$*, $m \geq 4$. If the line l of* $\mathrm{PG}(m,q^3)$ *is disjoint from* $\mathrm{PG}(m,q)$*, then the number of stabbing points on l is 0, 1, $q+1$, or q^2+q+1, with* $\dim S(l)$ *being 5, 4, 3 or 2 respectively.*

Proof. By Lemma 2.6.1, $2 \leq \dim S(l) \leq 5$.

If $\dim S(l) = 5$, then for any two points P, Q of l we have $S(l) = \langle S(P), S(Q)\rangle$ and thus, $\dim S(P) = \dim S(Q) = 2$. This is true for any point of l. Hence, in this case l has no stabbing point.

If $S(l)$ is a plane, then the q^2+q+1 lines of this plane all meet l and therefore l has q^2+q+1 stabbing points.

When $\dim S(l) = 3$, then the extension of $S(l)$ is a solid on l. The q^3+1 planes on l of this solid all meet $S(l)$ (see Lemma 1.3.3) and thus provide a partition of $S(l)$ in q^3+1 parts. Clearly every part is a line or a point, so a counting argument shows that exactly $q+1$ planes meet $S(l)$ in lines, and and q^3-q meet $S(l)$ only in points. The extensions of these $q+1$ lines will be meeting l in different points, and thus the number of stabbing points is $q+1$.

The last case to consider is $\dim S(l) = 4$. First select a plane π on the line l, such that π is contained in $e(S(l))$, the extension of $S(l)$, but disjoint from $S(l)$. We can select such a plane, since $e(S(l))$ is a 4-dimensional subspace of $\mathrm{PG}(m, q^3)$, so l lies in $q^6 + q^3 + 1$ planes contained in this subspace, which is more than the number of points of $S(l)$, which is a 4-dimensional subspace of $\mathrm{PG}(m, q)$. By Lemma 1.3.3 $\dim S(\pi) \geq 4$, so $\dim S(\pi) = 4$.

Again by Lemma 1.3.3, each 3-space on π contained by $e(S(l))$ meets $S(l)$ in at least a line. Then counting the intersection of these $q^3 + 1$ solids with $S(l)$ shows that exactly one of these intersections is a plane while all other intersections are lines. This implies that π has a line h containing $q^2 + q + 1$ stabbing points ($\dim(S(h)) = 2$) and q^3 further stabbing points not on h.

Now we prove that these $q^3 + q^2 + q + 1$ stabbing points form a minimal blocking set in π. Suppose that g is a line of π which contains no stabbing points. Then $P = h \cap g$ is not a stabbing point. Consider the $q^3 - 1$ lines of π on P other than h and g. One of them, say f has to contain at least 2 stabbing points by the pigeonhole principle. Then $\dim S(f) = 3$, because if Q_1 and Q_2 are the stabbing points, then $S(Q_1)$ and $S(Q_2)$ are skew lines, and $S(f) = \langle S(Q_1), S(Q_2) \rangle$. But then $\dim\langle S(f), S(h) \rangle = 4$ implies that $\dim S(P) = \dim S(h \cap f) = \dim(S(h) \cap S(f)) = 1$. This is a contradiction. ■

Lemma 2.6.3. *Consider* $\mathrm{PG}(m, q)$ *embedded in* $\mathrm{PG}(m, q^3)$, $m \geq 6$. *There are six types of planes in* $\mathrm{PG}(m, q^3)$, *skew to the embedded* $\mathrm{PG}(m, q)$, *and they have the following properties:*

(1) $\dim S(\pi) = 4$, *and there are* $q^3 + q^2 + q + 1$ *stabbing points on* π, *which form a blocking set of type* (2) *of Result 1.6.11.*

(2) $\dim S(\pi) = 5$, *and there are* $q^2 + q + 1$ *collinear stabbing points on* π.

(3) $\dim S(\pi) = 5$, *and there are* $q^2 + q + 1$ *stabbing points on* π, *which form a* $\mathrm{PG}(2, q)$.

(4) $\dim S(\pi) = 6$, *and there are* $q + 1$ *collinear stabbing points on* π.

(5) $\dim S(\pi) = 7$, *and there is* 1 *stabbing point on* π.

(6) $\dim S(\pi) = 8$, *and there are no stabbing points on* π.

Proof. As π is disjoint from $\mathrm{PG}(m,q)$, then Lemma 1.3.3 shows that $\dim S(\pi) \geq 4$. The case $\dim S(\pi) = 4$ follows from Result 1.6.11 and the last case of the proof of Lemma 2.6.2.

We may thus assume that $\dim S(\pi) \geq 5$.

We will first show that π has a line l with $\dim S(l) = 5$. Assume that this is not true. Then, by Lemma 2.6.2, the stabbing points in π form a blocking set. If there is a line m containing q^2+q+1 stabbing points, then $\dim S(m) = 2$ and with $P \notin m$ a stabbing point of π we have $\dim S(\pi) = \dim\langle S(m), S(P)\rangle \leq 4$, a contradiction. Thus, every line of π has 1 or $q+1$ stabbing points. But it is easy to see that $\mathrm{PG}(2,q^3)$ has no point-set meeting every line in 1 or $q+1$ points. This is a contradiction.

Hence, π has a line l with $\dim S(l) = 5$, which means that there are no stabbing points on l. The planes $S(P)$ with $P \in l$ are mutually skew planes, which form a plane-spread of $S(l)$. Let $Q \in \pi \setminus l$ be a point with $\dim S(Q) = 2$. For any point $P \in l$ the line PQ contains 0, 1, $q+1$ or q^2+q+1 stabbing points, which is equivalent to $\dim S(PQ)$ being 5, 4, 3 or 2 respectively, which is equivalent to $\dim(S(P) \cap S(Q))$ being -1, 0, 1 or 2 respectively (see Lemma 2.6.2). Thus, the number of stabbing points on the line PQ is equal to the number of points in $S(P) \cap S(Q)$. As the $S(P)$ with $P \in l$ partition $S(l)$, it follows that the number of stabbing points in π is equal to $|S(l) \cap S(Q)|$. This is q^2+q+1 if $\dim S(\pi) = 5$, $q+1$ if $\dim S(\pi) = 6$, 1 if $\dim S(\pi) = 7$, and 0 if $\dim S(\pi) = 8$.

The proposition follows from this, as q^2+q+1 or $q+1$ points meeting every line in 0, 1, $q+1$ or q^2+q+1 points have to form one of the sets given in (2), (3) or (4). ■

Now let us examine the projected $\mathrm{PG}(6,q)$ subgeometries of $\mathrm{PG}(3,q^3)$. Consider $\mathrm{PG}(6,q)$ embedded in $\mathrm{PG}(6,q^3)$ as a subgeometry, and let the plane π be the vertex of the projection. A point, a line, or a plane of $\mathrm{PG}(3,q^3)$ corresponds to a 3-space, a 4-space or a 5-space on π respectively. Clearly the structure of the resulting point set depends only on the relation of the $\mathrm{PG}(6,q)$ subgeometry and the vertex of the projection.

Lemma 2.6.4. *There are four types of projected* $\mathrm{PG}(6,q)$ *subgeometries in* $\mathrm{PG}(3,q^3)$*, which have the following properties:*

	number of points	*Rédei*	*cone*
(1)	$q^6 + q^5 + q^3 + 1$	*yes*	*yes*
(2)	$q^6 + q^5 + q^4 + q^3 + 1$	*yes*	*yes*
(3)	$q^6 + q^5 + q^4 + 1$	*yes*	*no*
(4)	$q^6 + q^5 + q^4 + q^3 + 1$	*no*	*no*

Proof. First observe that $\dim S(\pi) \leq 6$. Clearly the projection is of Rédei type, if and only if $\dim S(\pi) \leq 5$, because then we can find a 5-space on π meeting the $\mathrm{PG}(6,q)$ in a 5-dimensional subspace. Then every point of $\mathrm{PG}(6,q) \setminus \mathrm{PG}(5,q)$ is projected once, which is equivalent to $\mathrm{PG}(3,q^3)$ having a plane which contains all but q^6 points of the projection.

The projection is a cone if and only if it has a point having a $\mathrm{PG}(2,q)$ projected onto it. (see Corollaries 2.2.4 and 2.2.5 and Lemma 2.2.13(a)). This is equivalent to $\mathrm{PG}(6,q)$ having a plane whose extension meets π in a line, which is equivalent to π having a line containing (q^2+q+1) stabbing points.

(1) Suppose that π has properties as in (1) of Lemma 2.6.3. As $\dim S(\pi) = 4$, then all the points of $S(\pi)$ are projected onto a line, that is onto q^3+1 points, which gives the number of points stated in (1). Clearly the projection will be of Rédei type and a cone.

(2) Suppose now that π has properties as in (2) of Lemma 2.6.3. Clearly the projection is of Rédei type and a cone. It has one point having a $\mathrm{PG}(2,q)$ projected onto it, and all other points are ordinary. From this the number of points of the projection is clear.

(3) Assume that π has properties as in (3) of Lemma 2.6.3. The projection will be of Rédei type, but not a cone. For the stabbing points $P \in \pi$, the lines $S(P)$ are all skew, and every 3-space on π can contain at most one (or else a 3-space on π would meet the $\mathrm{PG}(6,q)$ subgeometry in a $\mathrm{PG}(3,q)$, which is impossible by Lemma 1.3.3). From this the number of the points of the projection is clearly $q^6 + q^5 + \cdots + 1 - (q^2+q+1)q$.

(4) Assume that π has properties as in (4) of Lemma 2.6.3. For m the only line of π containing stabbing points, $S(m)$ is projected onto a line, and thus the given number of points in the projection follows. The projection will not be of Rédei type and it will not be a cone. ■

Some more properties of these sets:

The sets given in (1) and (2) are the cones with base the plane blocking sets described in (1) and (2) of Result 1.6.11.

The set given in (3) has a Rédei plane in which the special points form a $\mathrm{PG}(2,q)$ subgeometry, and the lines of this $\mathrm{PG}(2,q)$ subgeometry are all lines contained in B. A line of the Rédei plane either meets the set in q^2+q+1 points (if it does not contain a special point), in q^2+1 point (if it contains one special point) or in q^3+1 points (if it contains $q+1$ special points). Every line not in the Rédei plane can meet the set in 1, $q+1$ or q^2+1 points.

The properties of the set given in (4) can be found in Lemma 2.3.13. It contains a unique line l. There are $q+1$ non-ordinary points on l, all other points of the set are ordinary. Every point not on l is connected to the ordinary points of l by $(q+1)$-secants, and to the non-ordinary points of l by (q^2+1)-secants. This example is of special interest, because the existence of linear blocking sets that are not of Rédei type were unknown for some time.

In [4] a different construction was given for finding the vertex of projection for this last linear blocking set. For the sake of completeness, we include this construction also.

Construction 2.6.5. Let $\mathrm{PG}(6,q)$ be embedded in $\mathrm{PG}(6,q^3)$ as a subgeometry. Suppose that $\Sigma = \mathrm{PG}(3,q)$ is a 3-dimensional subspace of the embedded subgeometry, denote by $e(\Sigma)$ the extension of Σ. Let $\mathcal{R}$ be a regulus of Σ. The extensions of the lines of $\mathcal{R}$ are elements of a regulus $\mathcal{R}^*$ of $e(\Sigma)$. Let v be a line of the opposite regulus of $\mathcal{R}^*$ such that v is skew to Σ (that is v is not the extension of an element of $\mathcal{R}^{OPP}$). Let Q be a further point of $\mathrm{PG}(6,q^3)\setminus\mathrm{PG}(6,q)$ such that Q is not contained in the extension of any of the 5-dimensional subspaces of $\mathrm{PG}(6,q)$ containing Σ. We can find such a point, because the number of 5-dimensional subspaces of $\mathrm{PG}(6,q)$ containing Σ is q^2+q+1, the extension of such a 5-dimensional subspace contains $q^{15}+q^{12}$ points from $\mathrm{PG}(6,q^3)\setminus e(\Sigma)$ and thus even if these were all different points, the extensions would be covering at most $(q^2+q+1)(q^{15}+q^{12})+|e(\Sigma)|$ points, but the number of points in $\mathrm{PG}(6,q^3)\setminus\mathrm{PG}(6,q)$ is larger than q^{18}. Let $\pi := \langle v, Q\rangle$. Then $\dim S(\pi)=6$. The lines of $\mathcal{R}$ are the only lines of $\mathrm{PG}(6,q)$ with the property that their extension meets π. All other properties can be derived from these. ■

Remark. Starting with the same line v, but choosing the point Q to be a point contained in the extension of a 5-space on Σ, but not contained in the extension of a 4-space on Σ will result in the blocking set (3) of Lemma 2.6.4.

Chapter 3

Unique reducibility of multiple blocking sets

3.1 The main theorem

Consider a weight function which corresponds to a t-fold $(n-k)$-blocking set that is not minimal. If we start reducing the weight of the non-essential points one by one, always checking carefully that the resulting weight function is still a t-fold $(n-k)$-blocking set, then after some steps we will arrive at a minimal t-fold $(n-k)$-blocking set. Thus, every t-fold $(n-k)$-blocking set contains a minimal t-fold $(n-k)$-blocking set. It is a natural question to ask if there are conditions which guarantee the uniqueness of this minimal t-fold $(n-k)$-blocking set. This chapter is based on [1].

In [43] such a condition is given for non-weighted 1-fold 1-blocking sets of $\mathrm{PG}(2,q)$.

Result 3.1.1 (Szőnyi, [43])**.** *A non-weighted 1-fold 1-blocking set of* $\mathrm{PG}(2,q)$ *with size smaller than* $2q+1$ *contains a unique minimal 1-fold 1-blocking set.*

This result was recently generalized to non-weighted 1-fold $(n-k)$-blocking sets of $\mathrm{PG}(n,q)$ in [29].

Result 3.1.2 (Lavrauw, Storme and Van de Voorde, [29])**.** *A non-weighted 1-fold* $(n-k)$*-blocking set of* $\mathrm{PG}(n,q)$ *with size smaller than* $2q^{n-k}$ *contains a unique minimal 1-fold* $(n-k)$*-blocking set.*

In this chapter we will prove the following theorem.

Theorem 3.1.3. *A weighted t-fold $(n-k)$-blocking set of* $\mathrm{PG}(n,q)$*, with total weight smaller than*

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

contains a unique minimal weighted t-fold $(n-k)$-blocking set.

Note that Theorem 3.1.3 is stronger than Result 3.1.2. Examples in section 3.5 show that the bound is sharp if $t=1$, or if $k=n-1$.

In this chapter a t-fold $(n-k)$-blocking set will sometimes be denoted by B, and then be viewed as a multiset of points, while at other times we will use the notation w and view the blocking set as a weight function. These two notions are equivalent, and we will switch between them according to our needs.

3.2 t-fold $(n-k)$-blocking sets which contain two minimal t-fold $(n-k)$-blocking sets

Let w be a t-fold $(n-k)$-blocking set. We will now define a new weight function s_w on the points of $\mathrm{PG}(n,q)$. For a point P let $s_w(P)$ be the largest integer for which the weight function w' defined by

$$w'(Q) = \begin{cases} w(Q) & \text{if } Q \neq P, \\ w(P) - s_w(P) & \text{if } Q = P \end{cases}$$

is also a t-fold $(n-k)$-blocking set. Then $w(P) \geq s_w(P) \geq 0$, so if $w(P)=0$, then $s_w(P)=0$. It is also clear that w is minimal if and only if $s_w \equiv 0$.

Lemma 3.2.1. *For a t-fold $(n-k)$-blocking set w and $P \in \mathrm{PG}(n,q)$ the following are true.*

(1) $s_w(P) = \min\{w(P), \min_{P\in\Pi_k}(w(\Pi_k)-t)\}$*, where Π_k runs along the k-dimensional subspaces containing P;*

(2) $s_w(P) = \max_{w'\leq w}\{w(P)-w'(P)\}$*, where w' runs along the t-fold $(n-k)$-blocking sets contained in w.*

Lemma 3.2.2. *If w is a t-fold $(n-k)$-blocking set which contains two different minimal t-fold $(n-k)$-blocking sets, then there is a weight function $v \leq w$ and a line l^* with the following properties:*

(1) *$v(\Pi_k) \geq t$ for any k-subspace Π_k not containing l^*;*

(2) *$v(\Pi_k) \geq t-1$ for any k-subspace Π_k containing l^*;*

(3) *there is a k-subspace Π_k^* containing l^* for which $v(\Pi_k^*) = t-1$;*

(4) *and $w(\mathrm{PG}(n,q)) \geq v(\mathrm{PG}(n,q)) + 2$.*

Proof. Let w' and w'' be two different minimal t-fold $(n-k)$-blocking sets contained in w. Then there is a point $P^* \in \mathrm{PG}(n,q)$, such that $w'(P^*) > w''(P^*)$. Define $\tilde{w}$ as follows:

$$\tilde{w}(Q) = \begin{cases} w(Q) & \text{if } Q \neq P^*, \\ w'(P^*) & \text{if } Q = P^*. \end{cases}$$

Then $\tilde{w}$ is a t-fold $(n-k)$-blocking set and $w', w'' \leq \tilde{w}$. Lemma 3.2.1(b) yields that $s_{\tilde{w}}(P^*) \geq \tilde{w}(P^*) - w''(P^*) = w'(P^*) - w''(P^*) > 0$. (*)

As $\tilde{w}$ contains the minimal t-fold $(n-k)$-blocking set w', we can start reducing the weight of the points with $\tilde{w}(P) > w'(P)$, one at a time, until we arrive at w'. Formally, let $\tilde{w} = w_1 \geq w_2 \geq \cdots \geq w_m = w'$ be a sequence of t-fold $(n-k)$-blocking sets, such that for $i \in \{1, 2, \ldots, m-1\}$ the t-fold $(n-k)$-blocking sets w_i and w_{i+1} only differ in one point P_i, and $w_{i+1}(P_i) = w_i(P_i) - 1$. Clearly $P_i \neq P^*$, and the points P_i are not necessarily all different. It is also clear that $\tilde{w} \neq w'$, because $\tilde{w} = w'$ would mean that w'' is contained in w', which is a contradiction, so $m \geq 2$ follows.

By Lemma 3.2.1(a), $s_{w_{i+1}} \leq s_{w_i}$, in fact, for any point Q, either $s_{w_{i+1}}(Q) = s_{w_i}(Q)$ or $s_{w_{i+1}}(Q) = s_{w_i}(Q) - 1$. For the point P^*, we have $s_{\tilde{w}}(P^*) > 0$ by (*), and $s_{w'}(P^*) = 0$ by the minimality of w'. So there will be an $i \in \{1, 2, \ldots, m-1\}$ such that $s_{w_i}(P^*) = 1$ and $s_{w_{i+1}}(P^*) = 0$. The weight functions w_i and w_{i+1} only differ in the point P_i. Then by Lemma 3.2.1(a), there is a k-space Π_k^* which contains P_i and P^*, and has weight $w_i(\Pi_k^*) = t+1$. Also by Lemma 3.2.1(a), this yields $s_{w_i}(P_i) \leq 1$, and as $w_{i+1}(P_i) = w_i(P_i) - 1$, so P_i is a non-essential point of w_i, then $s_{w_i}(P_i) = 1$ follows. Thus, for any k-dimensional subspace Π_k, which contains P^* and/or P_i we have $w_i(\Pi_k) \geq t+1$.

Let l^* be the line connecting P_i and P^*, and define v to be the following weight function:

$$v(Q) = \begin{cases} w_i(Q) & \text{if } Q \notin \{P^*, P_i\}; \\ w_i(Q) - 1 & \text{if } Q \in \{P^*, P_i\}. \end{cases}$$

Clearly $w(\mathrm{PG}(n,q)) \geq w_i(\mathrm{PG}(n,q)) = v(\mathrm{PG}(n,q)) + 2$, and v is a weight function contained in w.

For any k-subspace Π_k,

$$v(\Pi_k) = \begin{cases} w_{i-1}(\Pi_k) - 2 & \text{if } \Pi_k \text{ contains both of } P^* \text{ and } P_i; \\ w_{i-1}(\Pi_k) - 1 & \text{if } \Pi_k \text{ contains one of } P^* \text{ and } P_i; \\ w_{i-1}(\Pi_k) & \text{if } \Pi_k \text{ contains neither of } P^* \text{ and } P_i. \end{cases}$$

Thus, v, l^* and Π_k^* satisfy the properties given in the lemma. ■

3.3 t-fold nuclei

If $t = 1$, $n = 2$, $k = 1$, then Lemma 3.2.2 yields that if w is a 1-fold 1-blocking set of $\mathrm{PG}(2,q)$ containing two different minimal 1-fold 1-blocking sets, then w contains a weight function v, which defines a blocking set of the affine plane $\mathrm{AG}(2,q) := \mathrm{PG}(2,q) \setminus l^*$. Thus, $w(\mathrm{PG}(2,q)) \geq s(q) + 2$, where $s(q)$ denotes the size of the smallest 1-blocking set of $\mathrm{AG}(2,q)$. There are several independent proofs for $s(q) = 2q - 1$, from which Result 3.1.1 follows (see Jamison [28], Brouwer and Schrijver [14], Blokhuis [8], Szőnyi [43]).

In [8] Blokhuis proves $s(q) = 2q - 1$ as a corollary of a theorem on *nuclei* of point sets. Now we generalize the notion of *nucleus* to multisets/weight functions.

Definition 3.3.1. (1) Let S be a multiset of $\mathrm{PG}(n,q)$. A point $P \notin S$ will be called a *t-fold nucleus* of S if every line through P meets S in at least t points, counted with multiplicities.

(2) Let w be a weight function of $\mathrm{PG}(n,q)$. A point $P \in \mathrm{PG}(n,q)$ with $w(P) = 0$ will be called a *t-fold nucleus* of w if every line through P has weight at least t.

For S to have nuclei, clearly $|S| \geq t\theta_{n-1}$ is needed. Let $|S| = t\theta_{n-1} + r$, $r \geq 0$.

Note that for $|S| = t\theta_{n-1} - r$, $r \geq 0$, a 'symmetric' version of the definition can be: a point $P \notin S$ is a t-fold nucleus of S, if every line through P meets S in at most t points, counted with multiplicities.

The notion of *nucleus* was first introduced by Mazzocca for affine sets for $n = 2$, $t = 1$ and $r = 0$. Blokhuis extended the notion to $r \geq 0$ in [8] and $t \geq 1$ in [7], and Sziklai generalized the definition for sets of the projective space $\mathrm{PG}(n, q)$ in [38]. (The 'symmetric' version was introduced in [23] and [38].)

Denote by $N^t(S)$ the set of t-fold nuclei of S, and let p be the characteristic of the field $\mathrm{GF}(q)$.

Result 3.3.2. (Sziklai, [38]) *Let S be a set of points in $\mathrm{PG}(n, q)$ with $|S| = t\theta_{n-1} + r$, $r \geq 0$. Let H_∞ be a given hyperplane, $|S \cap H_\infty| = m_\infty$. Then*

$$|N^t(S) \setminus H_\infty| \leq (r + 1)(q - 1),$$

provided that $\binom{t\theta_{n-1}+r-m_\infty}{r+1} \neq 0 \pmod{p}$.

Result 3.3.2 was proved in the case when $m_\infty = 0$, $n = 2$ by Blokhuis and Wilbrink ($r = 0$, $t = 1$, see [12]) and by Blokhuis (for $r \geq 0$, $t = 1$, see [8], and for $r \geq 0$, $t \geq 1$ see [7]). The 'symmetric' version was also settled by Sziklai in [38].

As Result 3.3.2 is not applicable when $\binom{t\theta_{n-1}+r-m_\infty}{r+1} = 0 \pmod{p}$, to obtain an upper bound in this case, Ball presented the following theorem.

Result 3.3.3. (Ball, [6]) *Let S be a set of points in $\mathrm{PG}(n, q)$ with $|S| = t\theta_{n-1} + r$, $r \geq 0$, and let H_∞ be a given hyperplane, $|S \cap H_\infty| = m_\infty$. Then*

$$|N^t(S) \setminus H_\infty| \leq (r + 1 + j)(q - 1),$$

provided that the binomial coefficient

$$\binom{t\theta_{n-1} + r - m_\infty}{r + 1 + j} \neq 0 \pmod{p}$$

for some $j \geq 0$.

The proof of Results 3.3.2 and 3.3.3 can be easily copied for multisets/weight functions and we obtain the following lemma.

Lemma 3.3.4. *Let w be a weight function on* $\mathrm{PG}(n,q)$ *and H_∞ a given hyperplane with $w(H_\infty) = m_\infty$. Suppose that $w(\mathrm{PG}(n,q)) = t\theta_{n-1} + r$, with $r \geq 0$. If*

$$\binom{t\theta_{n-1} + r - m_\infty}{r+1+j} \not\equiv 0 \pmod{p}$$

for some $j \geq 0$, then the number of t-fold nuclei of w in $\mathrm{PG}(n,q) \setminus H_\infty$ *is at most* $(r+1+j)(q-1)$.

Proof. If the binomial coefficient is nonzero, then $w(\mathrm{PG}(n,q) \setminus H_\infty) > 0$, so the number of t-fold nuclei in $\mathrm{PG}(n,q) \setminus H_\infty$ is at most $q^n - 1$. Thus, the statement is trivially true for $r + 1 \geq \theta_{n-1}$, so from now on we will suppose $r < \theta_{n-1} - 1$.

Identify the points of $\mathrm{AG}(n,q) := \mathrm{PG}(n,q) \setminus H_\infty$ with the elements of $\mathrm{GF}(q^n)$, and the points of H_∞ with the θ_{n-1}-st roots of unity of $\mathrm{GF}(q^n)$ in the usual way. The points of $\mathrm{PG}(n,q)$ will be denoted by capital letters, and the corresponding elements of $\mathrm{GF}(q^n)$ by the same lowercase letters. Then for points $A \neq B \in \mathrm{AG}(n,q)$, the line AB contains the ideal point $C \in H_\infty$ if and only if $(a-b)^{q-1} = c$ holds.

Let $\mathcal{S} = \{a_1, a_2, \ldots, a_{t\theta_{n-1}+r-m_\infty}\} \cup \{c_1, \ldots, c_{m_\infty}\}$ be the multiset of elements of $\mathrm{GF}(q^n)$ corresponding to the points of nonzero weight of $\mathrm{PG}(n,q) \setminus H_\infty$ and H_∞ respectively, such that $a \in \mathcal{S}$ has multiplicity $w(A)$ in $\mathcal{S}$ for the corresponding point $A \in \mathrm{PG}(n,q)$.

Let X and Y be variables, and define

$$\mathcal{B}(X) = \{(X - a_i)^{q-1} | i = 1, \ldots, t\theta_{n-1} + r - m_\infty\} \cup \{c_1, \ldots, c_{m_\infty}\},$$

and

$$F(Y,X) = \prod_{b \in \mathcal{B}(X)} (Y - b).$$

Then

$$F(Y,X) = \sum_{j=0}^{t\theta_{n-1}+r} (-1)^j \sigma_j(\mathcal{B}(X)) Y^{t\theta_{n-1}+r-j},$$

where $\sigma_j(\mathcal{B}(X))$ denotes the jth elementary symmetric polynomial of the set $\mathcal{B}(X)$.

Suppose that $x \in \mathrm{GF}(q^n)$ is an element corresponding to a t-fold nucleus of w. Then $\mathcal{B}(x)$ contains every θ_{n-1}-st root of unity with multiplicity at least t, so

$$F(Y,x) = (Y^{\theta_{n-1}} - 1)^t (Y^r + \text{terms of lower degree}).$$

As $r < \theta_{n-1} - 1$, the coefficients of the terms

$$Y^{t\theta_{n-1}-1}, Y^{t\theta_{n-1}-2}, \dots, Y^{(t-1)\theta_{n-1}+r+1}$$

are 0 in $F(Y, x)$. Thus, $\sigma_{r+1+j}(\mathcal{B}(x)) = 0$ for $0 \leq j \leq \theta_{n-1} - r - 2$.

The degree of $\sigma_{r+1+j}(\mathcal{B}(X))$ as a polynomial of X is at most $(r+1+j)(q-1)$, with equality precisely if the binomial coefficient

$$\binom{t\theta_{n-1} + r - m_\infty}{r+1+j}$$

does not vanish. In this case $\sigma_{r+1+j}(\mathcal{B}(X))$ is not the zero polynomial, and every nucleus is a root of it, hence the number of nuclei is at most its degree: $(r+1+j)(q-1)$. ■

We will now use Lemma 3.3.4 for $n = 2$, $j = 0$ and $m_\infty = t - 1$.

Lemma 3.3.5. *Suppose that v is a weight function of* $\mathrm{PG}(2, q)$ *such that there is a line l^*, with $v(l^*) = t - 1$, while all other lines have weight at least t. Then $|v| \geq (t+1)q - 1$.*

Proof. Assume first that $t \leq q - 2$. Suppose on the contrary that v is such a weight function, yet the total weight of v is less than $(t+1)q - 1$. We may suppose $|v| = (t+1)q - 2$ (or else increase the weight of some of the points of $\mathrm{PG}(2, q) \setminus l^*$). All lines other than l^* have weight at least t, which means that all the points of $\mathrm{PG}(2, q) \setminus l^*$ with weight 0 are t-fold nuclei of v. As $v(\mathrm{PG}(2, q) \setminus l^*) = (t+1)q - 2 - (t-1) = tq + q - t - 1$, $\mathrm{PG}(2, q) \setminus l^*$ has at most $tq + q - t - 1$ points with positive v weight (and exactly this many if every point of $\mathrm{PG}(2, q) \setminus l^*$ has weight ≤ 1). So v has at least $q^2 - (tq + q - t - 1) = q^2 - tq - q + t + 1$ t-fold nuclei.

We will use Lemma 3.3.4 to prove that this is not possible. As

$$|v| = (t+1)q - 2 = t(q+1) + q - t - 2$$

and

$$\binom{t(q+1) + q - t - 2 - (t-1)}{q - t - 2 + 1} = \binom{tq + q - t - 1}{q - t - 1} \neq 0 \pmod{p}$$

by Lucas' theorem, so Lemma 3.3.4 yields that the number of t-fold nuclei of v is at most $(q - t - 1)(q - 1) = q^2 - tq - 2q + t + 1$, a contradiction. The same arguments prove that, if $|v| = (t+1)q - 1$, then $v(P) \leq 1$ for all points $P \in \mathrm{PG}(2,q) \setminus l^*$.

For $t \geq q-1$, the assertion can be proved by summing the weights of all lines through a carefully selected point P. If we can find a point $P \in \mathrm{PG}(2,q) \setminus l^*$ with $v(P) = 0$, then $|v| \geq t(q+1) = tq + t \geq tq + q - 1$, and we are done. If we choose a point $P \in l^*$ with $v(P) = 0$, then we have $|v| \geq tq + t - 1$. If $t \geq q$, then we are done again. If $t = q-1$ and all points of $\mathrm{PG}(2,q) \setminus l^*$ have positive weight, then $v(\mathrm{PG}(2,q) \setminus l^*) \geq q^2$, so $|v| \geq q^2 + t - 1 > (t+1)q - 1$. This proves that if we can select a point $P \in \mathrm{PG}(2,q)$ with $v(P) = 0$, then the assertion is true.

Assume now that $v(P) > 0$ for every point. Let $m = \min_P v(P)$ and define a new weight function $\tilde{v}$, by $\tilde{v}(P) := v(P) - m$. Then $\tilde{v}(l^*) = t - m(q+1) - 1$ and $\tilde{v}(l) \geq t - m(q+1)$ for any line $l \neq l^*$. If $t - m(q+1) \leq q-2$ then we can use the first part of the proof to prove $|\tilde{v}| \geq (t - m(q+1) + 1)q - 1$. If $t - m(q+1) \geq q-1$ then we can use the second part, as there will be a point with zero $\tilde{v}$ weight. Then

$$|v| = |\tilde{v}| + m(q^2+q+1) \geq (t - m(q+1)+1)q - 1 + m(q^2+q+1) = (t+1)q - 1 + m.$$

Hence the result is established. ■

3.4 Proof of Theorem 3.1.3

Proof. Assume that w is a weighted t-fold $(n-k)$-blocking set of $\mathrm{PG}(n,q)$ which contains two different minimal t-fold $(n-k)$-blocking sets. We will prove $|w| \geq (t+1)q^{n-k} + \theta_{n-k-1}$. By Lemma 3.2.2, there is a weight function $v \leq w$, a line l^* and a k-subspace Π_k^* containing l^*, such that

(1) $v(\Pi_k) \geq t$, for every k-subspace Π_k not containing l^*;

(2) $v(\Pi_k) \geq t-1$ for every k-subspace Π_k containing l^*;

(3) $v(\Pi_k^*) = t-1$;

(4) $|w| \geq |v| + 2$.

Case 1 Assume first that $k = 1$. Then $\Pi_k^* = l^*$ is a line, and $v(l^*) = t-1$, while the v weight of any other line is at least t. If $n = 2$, then $|v| \geq (t+1)q - 1$ by Lemma

3.3.5, which proves the theorem in this case. Now assume $n \geq 3$ and let Π be a plane containing the line l^*. Then the weight function v restricted to the plane Π fulfills the requirements of Lemma 3.3.5, so $v(\Pi) \geq (t+1)q-1$. This is true for all the planes containing the line l^*, so clearly $|v| \geq \theta_{n-2} \cdot ((t+1)q - 1 - (t-1)) + t - 1 = (t+1)q^{n-1} + \theta_{n-2} - 2$.

Case 2 For $n \geq 3$ and $k \geq 2$ we will use induction on n to prove that

$$|v| \geq (t+1)q^{n-k} + \theta_{n-k-1} - 2.$$

Case 2a Let $V \in \Pi_k^* \setminus l^*$ be a point with $v(V) = 0$. Consider the quotient space $\mathrm{PG}(n,q)/V \cong \mathrm{PG}(n-1,q)$, and the weight function $\tilde{v}$ induced by v on $\mathrm{PG}(n-1,q)$. Clearly $\tilde{v}(\mathrm{PG}(n-1,q)) = v(\mathrm{PG}(n,q))$. The plane $\langle V, l^* \rangle$ corresponds to a line, and a k-space containing V corresponds to a $(k-1)$-space. It is not hard to check that $\tilde{v}$ fulfills requirements (a)-(c) with $\langle V, l^* \rangle / V$ as l^* and Π_k^*/V as Π_{k-1}^*, and so by induction

$$\tilde{v}(\mathrm{PG}(n-1,q)) \geq (t+1)q^{n-k} + \theta_{n-k-1} - 2.$$

Case 2b Suppose now that for all $P \in \Pi_k^* \setminus l^*$: $v(P) > 0$, but there is a point $v(V) = 0$. Then $t - 1 \geq \theta_k - (q+1)$. Increase the weight of one point ($\neq V$) of l^* by one to obtain the new weight function v', which is now a t-fold $(n-k)$-blocking set of $\mathrm{PG}(n,q)$. We will prove that $|v'| \geq tq^{n-k} + \theta_{n-k} - 1$. This is generally not true for t-fold $(n-k)$-blocking sets of $\mathrm{PG}(n,q)$, only if t is large enough.

Assume on the contrary, that $|v'| \leq tq^{n-k} + \theta_{n-k} - 2$. Then we can find a line Σ_1 containing V, such that

$$v'(\Sigma_1) \leq \frac{t - (q^{k-1} + q^{k-2} + \cdots + q)}{q^{k-1}},$$

because if all lines through V had v' weight more than

$$\frac{t - (q^{k-1} + q^{k-2} + \cdots + q)}{q^{k-1}},$$

then all these weights would be at least $\geq \dfrac{t-(q^{k-1}+q^{k-2}+\cdots+q)}{q^{k-1}}+\dfrac{1}{q^{k-1}}$, and then the total weight of v' would be

$$
\begin{aligned}
|v'| &\geq \left(\frac{t-q^{k-1}-q^{k-2}-\cdots-q}{q^{k-1}}+\frac{1}{q^{k-1}}\right)\cdot\theta_{n-1}\\
&= tq^{n-k}+\left(\frac{t}{q^{k-1}}-\frac{q^k+q^{k-1}+\cdots+q^2}{q^{k-1}}\right)\theta_{n-2}-\frac{q^{k-1}+q^{k-2}+\cdots+q}{q^{k-1}}+\frac{\theta_{n-1}}{q^{k-1}}\\
&\qquad > tq^{n-k}+\frac{q^{n-1}+q^{n-2}+\cdots+q^k}{q^{k-1}}=tq^{n-k}+\theta_{n-k}-1.
\end{aligned}
$$

We will now prove that if $1\leq j\leq k-2$ and Σ_j is a j-space with

$$
v'(\Sigma_j)\leq\frac{t-(q^{k-j}+q^{k-j-1}+\cdots+q)}{q^{k-j}},
$$

then we can find a $(j+1)$-space $\Sigma_{j+1}\supset\Sigma_j$, with

$$
v'(\Sigma_{j+1})\leq\frac{t-(q^{k-j-1}+\cdots+q)}{q^{k-j-1}}.
$$

If this were not true, then we would have

$$
\begin{aligned}
|v'| &> \left(\frac{t-(q^{k-j-1}+\cdots+q)}{q^{k-j-1}}-v'(\Sigma_j)\right)\cdot\theta_{n-j-1}+v'(\Sigma_j)\\
&\geq \left(\frac{t-(q^{k-j-1}+\cdots+q)}{q^{k-j-1}}-\frac{t-(q^{k-j}+q^{k-j-1}+\cdots+q)}{q^{k-j}}\right)\cdot\theta_{n-j-1}\\
&\qquad +\frac{t-(q^{k-j}+q^{k-j-1}+\cdots+q)}{q^{k-j}}=tq^{n-k}+\theta_{n-k}+1.
\end{aligned}
$$

Thus, we can find a $(k-1)$-space Σ_{k-1}, with $v'(\Sigma_{k-1})\leq\frac{t-q}{q}$. But all k-spaces containing Σ_{k-1} have v' weight at least t, so

$$
|v'|\geq(t-\frac{t}{q}+1)\cdot\theta_{n-k}+\frac{t-q}{q}=tq^{n-k}+\theta_{n-k}-1,
$$

a contradiction.

Case 2c There is one more case remaining to be proved: if $v(P)>0$ for all points $P\in\mathrm{PG}(n,q)$. Then let $m:=\min_P v(P)$ and let $\tilde{v}:=v-m$. Then $\tilde{v}$ fulfills requirements (a)-(c) with $\tilde{t}:=t-m\cdot\theta_k$. Cases 2a and 2b prove $|\tilde{v}|\geq\tilde{t}q^{n-k}+\theta_{n-k}-2$ and then

$$
\begin{aligned}
|v|=|\tilde{v}|+m\cdot\theta_n &\geq (t-m\cdot\theta_k)q^{n-k}+\theta_{n-k}-2+m\cdot\theta_n\\
&= tq^{n-k}+\theta_{n-k}-2+m\theta_{n-k-1}.
\end{aligned}
$$

■

3.5 Examples

In this section we investigate the sharpness of Theorem 3.1.3. We are looking for weighted t-fold $(n-k)$-blocking sets of size $(t+1)q^{n-k} + \theta_{n-k-1}$, which contain two different minimal t-fold $(n-k)$-blocking sets.

3.5.1 The case $t = 1$

Example 3.5.1. Let Σ^1 and Σ^2 be two $(n-k)$-dimensional subspaces of $\mathrm{PG}(n, q)$ meeting in an $(n-k-1)$-dimensional subspace. Then $B := \Sigma^1 \cup \Sigma^2$ contains two different minimal 1-fold $(n-k)$-blocking sets, Σ_1 and Σ_2, and $|B| = 2q^{n-k}+\theta_{n-k-1}$.

Corollary 3.5.2. *Theorem 3.1.3 is sharp, if* $t = 1$.

The following proposition is a corollary of Theorem 3.1.3, but in fact equivalent to it if $t = 1$ and $k = 1$. Corollary 3.5.4 can also be found in [44].

Proposition 3.5.3. *Let B be a minimal 1-fold $(n-1)$-blocking set of* $\mathrm{PG}(n, q)$, *and $P \in B$. Then there are at least $\geq 2q^{n-1} + \theta_{n-2} - |B|$ tangents through P.*

Proof. Suppose that there are k tangents through P. Take points P_1, P_2, ..., P_k, one from each of the tangents, $P_i \neq P$. Clearly $(B \setminus \{P\}) \cup \{P_1, \dots, P_k\}$ is a 1-fold $(n-1)$-blocking set. It contains a minimal 1-fold $(n-1)$-blocking set B', and $B \neq B'$. Thus, $B \cup \{P_1, \dots, P_k\}$ contains two different minimal 1-fold $(n-1)$-blocking sets, so $|B| + k \geq 2q^{n-1} + \theta_{n-2}$. ■

Corollary 3.5.4. *Let B be any 1-fold $(n-1)$-blocking set of* $\mathrm{PG}(n, q)$, *and $P \in B$ an essential point of B. Then there are at least $\geq 2q^{n-1} + \theta_{n-2} - |B|$ tangents through P.*

Construction 3.5.5. (1) Let B be a 1-fold $(n-1)$-blocking set which has a point $P \in B$, through which there are exactly $2q^{n-1} + \theta_{n-2} - |B|$ tangents to B. Then adding a point to every tangent will result in a 1-fold $(n-1)$-blocking set of size $2q^{n-1} + \theta_{n-2}$, which contains two different minimal 1-fold $(n-1)$-blocking sets.

(2) Embed S in an $(n-k+1)$-dimensional subspace of $\mathrm{PG}(n, q)$ to obtain 1-fold $(n-k)$-blocking sets of size $2q^{n-k} + \theta_{n-k-1}$, which contain two different minimal 1-fold $(n-k)$-blocking sets. ■

Note that blocking sets used in the construction above exist: let B be a blocking set of Rédei type with Rédei hyperplane H, and $P \in B \setminus H$. Then for a point $Q \in H$ the line $\langle P, Q\rangle$ is a tangent to B if and only if $Q \notin B$. Thus, P is on exactly $\theta_{n-1} - (|B| - q^{n-1}) = 2q^{n-1} + \theta_{n-2} - |B|$ tangents (see [41]).

3.5.2 The case $t \geq 2$

Note that the proof of Lemma 3.3.5 yields that for $n = 2$, $k = 1$ it is not possible to have $v(\mathrm{PG}(2, q)) = (t+1)q - 1$, if $t \geq q+1$, and so the proof of Theorem 3.1.3 yields that the bound cannot be sharp if $t \geq q+1$. Also from the proofs of Lemma 3.3.5 and Theorem 3.1.3 it follows that if $t \leq q - 2$ and B is a weighted t-fold $(n-k)$-blocking set which contains two different minimal t-fold $(n-k)$-blocking sets and $|B| = (t+1)q^{n-k} + \theta_{n-k-1}$, then only points on one line (the line l^*) can be multiple points.

Example 3.5.6. Let π be a plane of $\mathrm{PG}(n, q)$, let $l_1, l_2, \ldots, l_t$ be different lines in π through a common point P, and l_{t+1} a further line of π, with $P \notin l_{t+1}$. Then the multiset $B := (l_1 + l_2 + \cdots + l_t) \cup l_{t+1}$ is a t-fold $(n-1)$-blocking set in $\mathrm{PG}(n, q)$, $|B| = t(q+1) + (q+1-t) = (t+1)q + 1$, and $l_1 + l_2 + \cdots + l_t$ and $l_1 \cup (l_2 + \cdots + l_t) \cup l_{t+1}$ are two minimal t-fold $(n-1)$-blocking sets contained in B; the latter one differs from B only in the point P.

Corollary 3.5.7. *Theorem 3.1.3 is sharp if* $k = n-1$, $2 \leq t \leq q$.

The following proposition is again a corollary of Theorem 3.1.3, which is in fact equivalent to it if $k = 1$.

Proposition 3.5.8. *Let B be a minimal t-fold $(n-1)$-blocking set of* $\mathrm{PG}(n, q)$, *and $P \in B$. Then there are at least $\geq (t+1)q^{n-1} + \theta_{n-2} - |B|$ t-secants through P.*

Proof. Suppose that there are k t-secants through P. Take points $P_1, P_2, \ldots, P_k$, one from each of the t-secants, $P_i \neq P$. Clearly the t-fold $(n-1)$-blocking set $B \setminus \{P\} + \{P_1, \ldots, P_k\}$ contains a minimal t-fold $(n-1)$-blocking set B', and $B \neq B'$. Thus, $B + \{P_1, \ldots, P_k\}$ contains two different minimal t-fold $(n-1)$-blocking sets, so $|B| + k \geq (t+1)q^{n-1} + \theta_{n-2}$. ■

Corollary 3.5.9. *Let B be a any t-fold $(n-1)$-blocking set of* $\mathrm{PG}(n,q)$*, and $P \in B$. Then there are at least $\geq (t+1)q^{n-1} + \theta_{n-2} - |B|$ t-secants through P.*

Proof. Let B' be a minimal t-fold $(n-1)$-blocking set contained in B. Then $P \in B'$. There are at least $\geq (t+1)q^{n-1} + \theta_{n-2} - |B'|$ t-secants through P to the set B'. At most $|B \setminus B'|$ of these are not t-secants to B. ∎

For $n = 2$ this proposition can also be found in papers by Ferret, Storme, Sziklai and Weiner [21], and Bacsó, Héger and Szőnyi [5]. A somewhat better result for non-weighted sets has been presented by Blokhuis, Lovász, Storme and Szőnyi in [11], where it is proved that every essential point of a non-weighted t-fold blocking set B of $\mathrm{PG}(2,q)$ lies on at least $(t+1)q + t - |B|$ t-secants.

Construction 3.5.10. (1) Let B be a minimal t-fold $(n-1)$-blocking set which has a point $P \in B$, through which there are exactly $(t+1)q^{n-1} + \theta_{n-2} - |B|$ t-secants to B. Adding a point to every t-secant will result in a t-fold $(n-1)$-blocking set S of size $(t+1)q^{n-1} + \theta_{n-2}$ and containing two different minimal t-fold $(n-1)$-blocking sets.

(2) Embed the set S in an $(n-k+1)$-dimensional subspace of $\mathrm{PG}(n,q)$ to obtain t-fold $(n-k)$-blocking sets of size $(t+1)q^{n-k} + \theta_{n-k-1}$, which contain two different minimal t-fold $(n-k)$-blocking sets. ∎

For $n = 2$, $k = 1$ and $2 \leq t \leq q$ one can find t-fold 1-blocking sets in $\mathrm{PG}(2,q)$ which have points that are on exactly $(t+1)q + 1 - |B|$ t-secants to B. The sum of t Rédei type blocking sets which have a common Rédei line, and share exactly one point, which is not on the Rédei line will have this property. Using such a planar t-fold 1-blocking set and Construction 3.5.10(2), we get examples for $n \geq 3$, $k = n-1$ and $1 \leq t \leq q$. Example 3.5.6 is a special case of this: the sum of t lines sharing a common point.

Unfortunately, for $t \geq 2$, $n \geq 3$ and $k = 1$, in the minimal t-fold $(n-1)$-blocking sets we examined, all points have at least $t\theta_{n-1} - (q+1-t)q^{n-2} - |B|$ t-secants to B. Thus, it may be conjectured that the correct bound in Theorem 3.1.3 should be

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

Chapter 4

Generalizing the Megyesi construction

In Rédei's blocking set construction (see Construction 1.5.2) a set U of q points is selected in $\mathrm{AG}(2,q)$, and U together with the ideal points determined by U form a minimal blocking set of $\mathrm{PG}(2,q) := \mathrm{AG}(2,q) \cup l_\infty$. The Megyesi construction (Result 1.5.6) is a special case of this, where a multiplicative subgroup of $\mathrm{GF}(q)^* := \mathrm{GF}(q) \setminus \{0\}$ is selected, and the points of U are chosen from two lines of $\mathrm{AG}(2,q)$ according to certain cosets of this subgroup. We say that the cosets were *placed* on the lines. The resulting minimal blocking sets have size $2q + 1 - |G|$. Gács generalized this method to three lines giving an infinite series of minimal blocking sets of size approximately $2q - \frac{2}{9}q$ (see Result 1.5.7). In a joint work with Csaba Mengyán we generalized this method, and presented it in [2]. Sections 4.1 and 4.3 can also be found in Mengyán's PhD dissertation [32], but for the sake of completeness, it is included here also.

4.1 Placing the cosets on three lines

First we investigate the case when the points are selected from three concurrent lines in $\mathrm{AG}(2,q)$. Without loss of generality, we may assume that the lines are $x = 0$, $y = 0$ and $x = y$.

Construction 4.1.1. Let $s \geq 3$ be a divisor of $q-1$ and consider a multiplicative subgroup G of $\mathrm{GF}(q)^*$ with index s. Let $\alpha \in \mathrm{GF}(q)^*$ be an element for which

G, αG, $\alpha^2 G$, $\ldots$, $\alpha^{s-1}G$ are the cosets of G. Form three non-empty subsets $I, J, K \subset \mathbb{Z}_s$ such that $|I| + |J| + |K| = s$. Let

$$U = \{(0, x) : x \in \alpha^i G, i \in I\} \cup \{(x, 0) : x \in \alpha^j G, j \in J\} \cup \\ \cup \{(x, x) : x \in \alpha^k G, k \in K\} \cup \{(0, 0)\}.$$

If D denotes the set of ideal points determined by U, and $|D| < q + 1$, then $B = U \cup D$ is a minimal blocking set, by Result 1.5.2.

The size of the minimal blocking set B of Construction 4.1.1 can be determined by determining $|D|$. First we will consider the question of determined ideal points in general, and calculate the set of directions determined by two cosets placed on two lines with slope m_1 and m_2.

Remark. A *direction* determined by two points is by definition a point (m) on the ideal line. With misuse of notation we will say that m is the direction (or ideal point) determined and omit the brackets. Thus, the set of directions (ideal points) determined by a point set will be a subset of $\mathrm{GF}(q) \cup \{\infty\}$.

Notation. For K a subset of $\mathrm{GF}(q)$ and $a, b \in \mathrm{GF}(q)$, we will use $aK + b = \{ax + b : x \in K\}$ and $1/K = \{1/x : x \in K\}$. For any element $x \in \mathrm{GF}(q)^*$, note that $x/0 = \infty$ and $x + \infty = \infty$.

Lemma 4.1.2. *Let $m_1, m_2 \in \mathrm{GF}(q)$, $m_1 \neq m_2$, $i_1, i_2 \in \mathbb{Z}_s$.*

- *The set of directions determined by the sets*

  $$\{(x, m_1 x) : x \in \alpha^{i_1} G\} \text{ and } \{(x, m_2 x) : x \in \alpha^{i_2} G\}$$

  (apart from m_1, m_2) is

  $$\left\{\frac{m_1 - m_2 x}{1 - x} : x \in \alpha^{i_2 - i_1} G\right\} = m_1 + \frac{m_2 - m_1}{1 - \alpha^{i_1 - i_2} G} = m_2 + \frac{m_1 - m_2}{1 - \alpha^{i_2 - i_1} G}.$$

- *The set of directions determined by the sets*

  $$\{(x, m_1 x) : x \in \alpha^{i_1} G\} \text{ and } \{(0, x) : x \in \alpha^{i_2} G\}$$

  (apart from m_1, ∞) is

  $$\{m_1 - x : x \in \alpha^{i_2 - i_1} G\} = m_1 - \alpha^{i_2 - i_1} G.$$

Proof. Basic calculations. ■

Corollary 4.1.3. *The set of directions determined in Construction 4.1.1 is*

$$D = \{0,1,\infty\} \cup \Big(\bigcup_{i\in I, j\in J} -\alpha^{i-j}G\Big) \cup \Big(\bigcup_{i\in I, k\in K} 1-\alpha^{i-k}G\Big) \cup \Big(\bigcup_{j\in J, k\in K} \frac{1}{1-\alpha^{j-k}G}\Big).$$

Notation. For $m_1, m_2 \in \mathrm{GF}(q)\cup\{\infty\}$, $m_1 \neq m_2$, $u \in \mathbb{Z}_s$ the notation

$$f(m_1,m_2,u) := \begin{cases} m_2 + \dfrac{m_1-m_2}{1-\alpha^u G} & \text{if } m_1, m_2 \neq \infty \\ m_1 - \alpha^u G & \text{if } m_2 = \infty \\ m_2 - \alpha^{-u} G & \text{if } m_1 = \infty \end{cases}$$

will be used. Thus, $f(m_1,m_2,u)$ is a subset of $\mathrm{GF}(q)\cup\{\infty\}$.

Lemma 4.1.4. *For $m_1, m_2, m_3 \in \mathrm{GF}(q)\cup\{\infty\}$ all different, and $u, v, w \in \mathbb{Z}_s$:*

(1) $f(m_1,m_2,u) = f(m_2,m_1,-u)$;

(2) $f(m_1,m_2,u) \cap f(m_1,m_2,v) = \emptyset$, *if* $u \neq v$;

(3) $\bigcup_{u=0}^{s-1} f(m_1,m_2,u) = (\mathrm{GF}(q)\cup\{\infty\}) \setminus \{m_1,m_2\}$;

(4) $f(m_1,m_2,u) \cap f(m_2,m_3,v) \subset f(m_1,m_3,u+v)$;

(5) $f(m_1,m_2,u) \cap f(m_2,m_3,v) \cap f(m_1,m_3,w) =$

$$= \begin{cases} \emptyset & \text{if } u+v \neq w, \\ f(m_2,m_3,v) \cap f(m_1,m_3,w) & \text{if } u+v = w. \end{cases}$$

Proof. (1) follows from the definition of f, as $1/G = G$. (2) and (3) are direct consequences of the facts $\alpha^u G \cap \alpha^v G = \emptyset$ if $u \neq v$ and $\bigcup_{u=0}^{s-1} \alpha^u G = \mathrm{GF}(q) \setminus \{0\}$.

(4) If $m_1, m_2 \neq \infty$, then for any element in the left set there are $x, y \in G$ such that

$$\frac{m_1 - m_2\alpha^u x}{1-\alpha^u x} = \frac{m_2 - m_3\alpha^v y}{1-\alpha^v y}.$$

Thus,

$$m_1 - m_2\alpha^u x - m_1\alpha^v y + m_2\alpha^{u+v}xy = m_2 - m_3\alpha^v y - m_2\alpha^u x + m_3\alpha^{u+v}xy.$$

Simplifying with $-m_2\alpha^u x$, switching the place of $m_2\alpha^{u+v}xy$ and $m_3\alpha^{u+v}xy$ and adding $m_3\alpha^{u+2v}xy^2$ to both sides yields

$$(m_1 - m_3\alpha^{u+v}xy)(1-\alpha^v y) = (m_2 - m_3\alpha^v y)(1-\alpha^{u+v}xy),$$

from which

$$\frac{m_1 - m_3\alpha^{u+v}xy}{1-\alpha^{u+v}xy} = \frac{m_2 - m_3\alpha^v y}{1-\alpha^v y} \in f(m_1, m_3, u+v).$$

If $m_3 = \infty$, then there are $x, y \in G$ such that

$$\frac{m_1 - m_2\alpha^u x}{1-\alpha^u x} = m_2 - \alpha^v y,$$

from which

$$m_1 - m_2\alpha^u x = m_2 - \alpha^v y - m_2\alpha^u x + \alpha^{u+v}xy.$$

Simplify with $-m_2\alpha^u x$ and take $\alpha^{u+v}xy$ to the other side to get

$$m_1 - \alpha^{u+v}xy = m_2 - \alpha^v y \in f(m_1, \infty, u+v).$$

In the case of $m_1 = \infty$, similar calculations give the result (or the use of (1) several times). As for $m_2 = \infty$: there are $x, y \in G$ such that

$$m_1 - \alpha^u x = m_3 - \alpha^{-v} y.$$

Taking $-\alpha^u x$ to the other side, and adding $-m_3\alpha^{u+v}x/y$ to both sides yields

$$m_1 - m_3\alpha^{u+v}x/y = m_3 - \alpha^{-v}y - m_3\alpha^{u+v}x/y + \alpha^u x = (m_3 - \alpha^{-v}y)(1-\alpha^{u+v}x/y).$$

(5) As a consequence of (4) and (2) the intersection is empty when $u + v \neq w$. In the case of $u + v = w$, (1) and (4) yield that any of the three terms can be omitted: $f(m_1, m_2, u) \cap f(m_2, m_3, v) \cap f(m_1, m_3, w) = f(m_2, m_3, v) \cap f(m_3, m_1, -w) \cap f(m_2, m_1, -u) = f(m_2, m_3, v) \cap f(m_1, m_3, w)$. ■

Notation. Let I, J, K be non-empty subsets of $\mathbb{Z}_s$, such that $|I| + |J| + |K| = s$. Denote by $T(I, J, K)$ the set of ordered pairs $(u, v) \in \mathbb{Z}_s \times \mathbb{Z}_s$, for which I, $J + u$ and $K + v$ are pairwise disjoint (that is $\mathbb{Z}_s$ is a disjoint union of I, $J + u$ and $K + v$).

It will be more convenient to calculate $|D^c|$, the number of non-determined points, and clearly $|D| = q + 1 - |D^c|$.

Theorem 4.1.5. *If D^c is the set of directions not determined in Construction 4.1.1, then*

$$D^c = \bigcup_{(u,v)\in T(I,J,K)} (-\alpha^u G \cap 1 - \alpha^v G),$$

with the sets $(-\alpha^u G \cap 1 - \alpha^v G)$ being pairwise disjoint.

Proof. From Corollary 4.1.3,

$$D^c = \left(\{0, 1, \infty\} \cup (\bigcup_{u\in I-J} -\alpha^u G) \cup (\bigcup_{v\in I-K} 1 - \alpha^v G) \cup (\bigcup_{w\in J-K} \frac{1}{1-\alpha^w G}) \right)^c .$$

Because of (2) and (3) of Lemma 4.1.4, we have

$$D^c = (\bigcup_{u\notin I-J} -\alpha^u G) \cap (\bigcup_{v\notin I-K} 1 - \alpha^v G) \cap (\bigcup_{w\notin J-K} \frac{1}{1-\alpha^w G}).$$

Thus, D^c is the union of intersections of the form

$$-\alpha^u G \cap (1 - \alpha^v G) \cap \frac{1}{1-\alpha^w G} = f(0,\infty,u) \cap f(1,\infty,v) \cap f(1,0,w),$$

with $u \notin I-J$, $v \notin I-K$, $w \notin J-K$. By Lemma 4.1.4(5), only those intersections are non-empty where $w + u = v$, and for such an intersection

$$-\alpha^u G \cap (1 - \alpha^v G) \cap \frac{1}{1-\alpha^w G} = -\alpha^u G \cap (1 - \alpha^v G).$$

Thus,

$$D^c = \bigcup \{-\alpha^u G \cap (1 - \alpha^v G) | u \notin I - J, v \notin I - K, v - u \notin J - K\}.$$

Because of Lemma 4.1.4(2) these sets are pairwise disjoint, and the following lemma finishes the proof. ∎

Lemma 4.1.6. *Let A, B be non-empty subsets of $\mathbb{Z}_s$, $x \in \mathbb{Z}_s$. Then*

$$x \notin A - B \Longleftrightarrow B + x \cap A = \emptyset.$$

Proof. $x \notin A - B$ means $x \neq a - b$ for any $a \in A$, $b \in B$, that is $b + x \neq a$ for any $a \in A$, $b \in B$. ∎

The determination of $|D^c|$ now comes down to determining $|T(I, J, K)|$ and the size of a set $-\alpha^u G \cap (1 - \alpha^v G)$.

Proposition 4.1.7. *Let I, J, K be non-empty subsets of $\mathbb{Z}_s$, such that $|I| + |J| + |K| = s$. Denote by $T(I, J, K)$ the set of ordered pairs $(u, v) \in \mathbb{Z}_s \times \mathbb{Z}_s$, for which I, $J + u$ and $K + v$ are disjoint. Then*

$$|T(I, J, K)| \leq 2s^2/9.$$

Equality holds if and only if s is divisible by 3 and $I, J, K \in \{H, H + 1, H + 2\}$ where $H = \{0, 3, 6, ..., s - 3\} = 3 \cdot \mathbb{Z}_s$.

Proof. As $|T(I, J, K)|$ is invariant under translations of I, J, K and permutations of (I, J, K), we may assume I, J, K to be disjoint, and $|I| \geq |J| \geq |K|$, which yields $|K| \leq s/3$ and $|J \cup K| \leq 2s/3$. Here equality holds if and only if $|I| = |J| = |K| = s/3$.

The number of u's satisfying $J + u \cap I = \emptyset$ is clearly at most $|J \cup K|$ (as an element of J can only be translated to elements of $J \cup K$) and for such a u the number of v's satisfying $K + v \cap (I \cup J + u) = \emptyset$ is at most $|K|$. Thus $|T(I, J, K)| \leq 2s^2/9$.

In the case of equality $3|s$ and $|I| = |J| = |K| = s/3$ clearly holds. But $|T(I, J, K)| = 2s^2/9$ means that for any u for which $J + u \cap I = \emptyset$, there are $s/3$ translations mapping K onto itself, which proves that K has to be a coset of a subgroup of $\mathbb{Z}_s$. The same is true for I and J. ∎

For the estimation of the size of the set $-\alpha^u G \cap (1 - \alpha^v G)$, a result from Sziklai [39] will be used, which is a variant of the Weil estimate. First we define the d-power independence of polynomials.

Definition 4.1.8. Let $f_1, ..., f_m \in \mathrm{GF}(q)[X]$ be given polynomials. We say that their system is *d-power independent*, if no partial product $f_{i_1}^{s_1} f_{i_2}^{s_2} ... f_{i_j}^{s_j}$ $(1 \leq j \leq m; 1 \leq i_1 < i_2 < ... < i_j \leq m; 1 \leq s_1, s_2, ..., s_j \leq d - 1)$ can be written as a constant multiple of a d-th power of a polynomial (that is $f_{i_1}^{s_1} f_{i_2}^{s_2} \dots f_{i_j}^{s_j} \neq cg^d$).

Lemma 4.1.9 (Sziklai, [39]). *Let $f_1, ..., f_m \in \mathrm{GF}(q)[X]$ be a set of d-power independent polynomials, where $d|(q - 1)$; $d, m \geq 2$. Denote by N the number of solutions $\{x \in \mathrm{GF}(q) : f_i(x)$ is a d-th power in $\mathrm{GF}(q)$ for all $i = 1, ..., m\}$. Then*

$$|N - \frac{q}{d^m}| \leq \sqrt{q} \sum_{i=1}^{m} \deg f_i.$$

Corollary 4.1.10. *The number of elements in $-\alpha^u G \cap (1 - \alpha^v G)$ is approximately q/s^2.*

Proof. $x \in G$ is equivalent to $x = y^s$ for some $y \in \mathrm{GF}(q)^*$. Thus, $x \in m - \alpha^u G$ is equivalent to $x = m - \alpha^u y^s$, which is equivalent to $\alpha^{-u}(m - x)$ being an s-th power. But then $|-\alpha^u G \cap (1 - \alpha^v G)|$ equals the number of solutions

$$\{x \in \mathrm{GF}(q) : -\alpha^{-u}X \text{ and } \alpha^{-v}(1 - X) \text{ are both } s\text{-th powers in } \mathrm{GF}(q)\}.$$

The number of such solutions is $q/s^2 + C\sqrt{q}$, with $|C| \leq 2$. ■

Thus, Theorem 4.1.5, Proposition 4.1.7 and Corollary 4.1.10 prove the following theorem.

Theorem 4.1.11. *Let D^c be the set of non-determined directions by the set U in Construction 4.1.1. Then*

$$|D^c| = \frac{|T(I, J, K)|}{s^2} q + C\sqrt{q} \leq \frac{2}{9} q + C\sqrt{q},$$

with $|C| \leq 4s^2/9$. If $s = o(\sqrt[4]{q})$, then

$$|B| \geq \left(2 - \frac{2}{9}\right) q + O(\sqrt{q}s^2).$$

This is a result is in harmony with the result of Gács [22]. And now we present some constructions:

Theorem 4.1.12. *Let s be a divisor of $q-1$, $s \geq 3$. In $\mathrm{PG}(2, q)$ minimal blocking sets of sizes $(2 - \frac{t}{s^2})q + C\sqrt{q}$ exist, where $t \in \{1, 2, k, kl\}$ with $k|s$, and $l|s$ such that $kl < s$, and $|C| \leq 2t$.*

Proof. Here are some examples for the given t's:

$t = 1$: For $I = \mathbb{Z}_s \setminus \{0, 1, 2\}$, $J = \{1\}$, $K = \{0, 2\}$,
$T(I, J, K) = \{(0, 0)\}$, $D^c = -G \cap (1 - G)$, $|D^c| \leq q/s^2 + 2\sqrt{q}$.

$t = 2$: For $I = \mathbb{Z}_s \setminus \{u, v\}$, $J = \{u\}$, $K = \{v\}$,
$T(I, J, K) = \{(0, 0), (v - u, u - v)\}$,
$D^c = (-G \cap 1 - G) \cup (-\alpha^{v-u}G \cap 1 - \alpha^{u-v}G)$,
$|D^c| \leq 2q/s^2 + 4\sqrt{q}$.

$t = k$: Let H be a proper subgroup of $\mathbb{Z}_s$, $|H| = k$ (note that $1 \notin H$).
For $I = \mathbb{Z}_s \setminus (H \cup \{1\})$, $J = H$, $K = \{1\}$,
$T(I, J, K) = \{(0, 0), (h, 0), (2h, 0), \dots\}$, with h a generator element of H. $D^c = \bigcup_{h \in H} \left(-\alpha^h G \cap (1 - G)\right)$,
$|D^c| \leq k(q/s^2 + 2\sqrt{q})$.

$t = k$: Let H be a proper subgroup of $\mathbb{Z}_s$, $|H| = k$, $a \in H$.
For $I = \mathbb{Z}_s \setminus H$, $J = H \setminus \{a\}$, $K = \{a\}$,
$T(I, J, K) = \{(0, 0), (h, h), (2h, 2h), \dots\}$, with h a generator element of H. $D^c = \bigcup_{h \in H} \left(-\alpha^h G \cap (1 - \alpha^h G)\right)$,
$|D^c| \le k(q/s^2 + 2\sqrt{q})$.
Note that instead of H the union of some cosets of H could be used, and for K an arbitrary subset of the union, while $J = \cup H \setminus K$ and $I = \mathbb{Z}_s \setminus (J \cup K)$. This and the previous case are the same in this sense (switch I and J).

$t = kl$: Let H_1 and H_2 be proper subgroups of $\mathbb{Z}_s$, $H_1 \ne H_2$, $|H_1| = k$, $|H_2| = l$, such that $kl < s$. Then there is an element $x \in \mathbb{Z}_s$ such that $H_1 \cap (H_2 + x) = \emptyset$ (because if none of the sets $H_1 \cap (H_2 + x)$, $x = 0, \dots, s/l - 1$ were empty, it would lead to $k \ge s/l$). For $I = \mathbb{Z}_s \setminus (J \cup K)$, $J = H_1$, $K = H_2 + x$,
$T(I, J, K) = H_1 \times H_2$, $D^c = \cup_{h_1 \in H_1, h_2 \in H_2} (-\alpha^{h_1} G \cap 1 - \alpha^{h_2} G)$ and $|D^c| \le lk(q/s^2 + 2\sqrt{q})$. ■

In our examples when $T(I, J, K) > 2$, at least one of I, J or K is a union of some cosets of a subgroup of $\mathbb{Z}_s$. If I, J, K are the unions of some cosets of the same subgroup $H \subset \mathbb{Z}_s$, then in Construction 4.1.4 G can be replaced by the subgroup $\bigcup_{h \in H} \alpha^h G$ of index $s/|H|$.

4.2 Placing the cosets on $n \ge 4$ lines

Now we investigate the case when the points of U are selected from n concurrent lines of AG$(2, q)$. Without loss of generality, we may assume that the lines are $x = 0$ and $y = m_i x$, $i = 2, \dots, n$. The theorems and proofs will be very much the same as when $n = 3$.

Construction 4.2.1. Consider a multiplicative subgroup G of GF$(q)^*$ with index s ($s \ge n$) and an $\alpha \in$ GF$(q)^*$ such that $\alpha^i G$, $i = 0, ..., s-1$ are the cosets of G. Let $m_1 = \infty$ and $\{m_2, m_3, \dots, m_n\} \subset$ GF(q) be the set of slopes. Form n non-empty subsets $A_1, A_2, ..., A_n$ in $\mathbb{Z}_s$ such that $|A_1| + |A_2| + ... + |A_n| = s$. Let

$$U = \{(0, 0)\} \cup \{(0, x) : x \in \alpha^a G, a \in A_1\} \cup \bigcup_{i=2}^{n} \{(x, m_i x) : x \in \alpha^a G, a \in A_i\}.$$

If D is the set of directions determined by U and $|D| < q + 1$, then the set $B = U \cup D$ is a minimal blocking set.

Notation. For $A_1, A_2, \ldots, A_n$ non-empty subsets of $\mathbb{Z}_s$, such that $\sum_{i=1}^{n} |A_i| = s$, denote by $T(A_1, \ldots A_n)$ the set of ordered $(n-1)$-tuples $(u_2, u_3, \ldots, u_n) \in \mathbb{Z}_s \times \cdots \times \mathbb{Z}_s$, for which $A_1, A_2 + u_2, \ldots, A_n + u_n$ are pairwise disjoint.

Theorem 4.2.2. *With the previous notation, D^c is the union of pairwise disjoint sets*

$$D^c = \bigcup \left\{ (m_2 - \alpha^{u_2} G) \cap \cdots \cap (m_n - \alpha^{u_n} G) | (u_2, \ldots, u_n) \in T(A_1, A_2, ..., A_n) \right\}.$$

Proof. From Lemma 4.1.2,

$$D = \{\infty\} \cup \{m_i : i = 2, \ldots, n\} \cup \bigcup_{1 \leq i < j \leq n} \left(\bigcup_{u \in A_i - A_j} f(m_j, m_i, u) \right).$$

By Lemma 4.1.4 (2) and (3),

$$D^c = \bigcap_{1 \leq i < j \leq n} \bigcup_{u \notin A_i - A_j} f(m_j, m_i, u) = \bigcup \bigcap_{1 \leq i < j \leq n} f(m_j, m_i, u_{j,i}).$$

By Lemma 4.1.4 (5), only those intersections

$$f(m_2, m_1, u_{2,1}) \cap f(m_3, m_1, u_{3,1}) \cap f(m_4, m_1, u_{4,1}) \cap \cdots \cap f(m_n, m_{n-1}, u_{n,n-1})$$

are non-empty for which for any 3 indices $i > j > k$: $u_{i,j} + u_{j,k} = u_{i,k}$ holds, and if this is the case, then for any three terms $f(m_i, m_j, u_{i,j})$, $f(m_j, m_k, u_{j,k})$, $f(m_i, m_k, u_{i,k})$ one can be omitted. Thus, for any two indices $i > j$ the intersection:

$$f(m_i, m_1, u_{i,1}) \cap f(m_j, m_1, u_{j,1}) \cap f(m_i, m_j, u_{i,j})$$

can be replaced by

$$f(m_i, m_1, u_{i,1}) \cap f(m_j, m_1, u_{j,1})$$

with $u_{i,1} \notin A_1 - A_i$, $u_{j,1} \notin A_1 - A_j$ and $u_{i,j} = u_{i,1} - u_{j,1} \notin A_j - A_i$, which is equivalent to the sets A_1, $A_i + u_{i,1}$ and $A_j + u_{j,1}$ being pairwise disjoint. ■

Proposition 4.2.3. *Let $A_1, A_2, ..., A_n$ be non-empty subsets of $\mathbb{Z}_s$ such that $|A_1| + |A_2| + ... + |A_n| = s$. Denote by $T(A_1, A_2, ..., A_n)$ the ordered $(n-1)$-tuples*

$(u_2, ..., u_n)$, with $u_2, ..., u_n \in \mathbb{Z}_s$, for which $A_1, A_2 + u_2, \ldots, A_n + u_n$ are pairwise disjoint. Then

$$|T(A_1, A_2, ..., A_n)| \leq \frac{(n-1)!s^{n-1}}{n^{n-1}}.$$

Equality holds if and only if s is divisible by n and $A_i \in \{H, H+1, H+2, ..., H+(n-1)\}$ where $H = \{0, n, 2n, ..., s-n\}$ (that is the A_i's are cosets of the subgroup $n \cdot \mathbb{Z}_s$).

Proof. The proof is exactly as in Proposition 4.1.7:

$$|T(A_1, A_2, ..., A_n)| \leq \left(\sum_{i=2}^{n} |A_i|\right) \cdot \left(\sum_{i=3}^{n} |A_i|\right) \ldots \left(\sum_{i=n}^{n} |A_i|\right).$$

If $|A_1| \geq |A_2| \geq ... \geq |A_n|$ holds, then $\sum_{i=k+1}^{n} |A_i| \leq (n-k)s/n$. ■

Proposition 4.2.4.

$$|(m_2 - \alpha^{u_2} G) \cap \cdots \cap (m_n - \alpha^{u_n} G)| \leq \frac{q}{s^{n-1}} + (n-1)\sqrt{q}.$$

Proof. Identical to that of Proposition 4.1.10. Use Lemma 4.1.9 for the polynomials $f_i(X) = \alpha^{-u_i}(m_i - X)$. ■

Theorem 4.2.2, Proposition 4.2.3 and Proposition 4.2.4 together prove the following theorem.

Theorem 4.2.5. *If D^c is the set of directions not determined by the set U in Construction 4.2.1, then*

$$|D^c| = \frac{|T(A_1, \ldots, A_n)|}{s^{n-1}} q + C\sqrt{q} \leq \frac{(n-1)!}{n^{n-1}} q + C\sqrt{q},$$

with $|C| \leq \frac{(n-1)!}{n^{n-2}} s^{n-1}$.

If s and n are fixed, such that $C_{s,n} := \frac{(n-1)!}{n^{n-2}} s^{n-1} << \sqrt{q}$, then

$$|B| \geq \left(2 - \frac{(n-1)!}{n^{n-1}}\right) q + O(\sqrt{q} C_{s,n}).$$

For s, n relatively small compared to q minimal blocking sets of sizes $2q - \frac{t}{s^{n-1}} q + O(\sqrt{q} C_{s,n})$ exist, where t is a number depending on some elementary equations.

4.3 Constructions in $\mathrm{PG}(2, q^h)$

From the existing minimal blocking sets some new ones can be constructed using embeddings of $\mathrm{PG}(2, q)$ into $\mathrm{PG}(2, q^h)$ for some $h > 1$. In this section we investigate two possible methods and use them on the minimal blocking sets constructed in this chapter and in a paper by Danielsson [18].

Construction 4.3.1. Consider a minimal blocking set B of $\mathrm{PG}(2, q)$. Embed $\mathrm{PG}(2, q)$ into $\mathrm{PG}(2, q^h)$ for some $h > 1$. Denote by l and m two lines of $\mathrm{PG}(2, q^h)$ which are extensions of lines of $\mathrm{PG}(2, q)$. If $Q := l \cap m$ is not a point of B, then suppose also that $|B \cap l| < q$ and $|B \cap m| < q$, and in this case denote by C the set of critical points of B which have their critical tangents through Q. Consider the point set

$$B' = B \cup \{l \setminus \mathrm{PG}(2, q)\} \cup \{m \setminus \mathrm{PG}(2, q)\} \cup \{Q\} \setminus C.$$

Remark. If B is a nontrivial blocking set of size less than $2q$, then by Proposition 1.5.3 all lines intersect B in at most $q - 1$ points.

Proposition 4.3.2. *In Construction 4.3.1, if $|C| \leq 1$, then B' is a minimal blocking set of* $\mathrm{PG}(2, q^h)$ *of size*

(1) $2q^h - 2q + |B|$, *if $Q \in B$;*

(2) $2q^h - 2q + |B| + 1 - |C|$, *if $Q \notin B$.*

Proof. Observe that any line of $\mathrm{PG}(2, q^h)$ through a point of $l \cap \mathrm{PG}(2, q)$ is blocked by the points of B, $m \setminus \mathrm{PG}(2, q)$ or the point Q, and the points of B' on $l \setminus \mathrm{PG}(2, q)$ block the remaining lines. Thus, B' is a blocking set.

To prove minimality, we will show that there is a tangent at every point of B'. At a point of B the extension of the line which is tangent to B in $\mathrm{PG}(2, q)$ will be a tangent to B', as such a line intersects l and m in $l \cap \mathrm{PG}(2, q)$ and $m \cap \mathrm{PG}(2, q)$, respectively. If through a point of B there is only one tangent, which is on $Q \notin B$, then by definition this point is not in B'. At the points of B' on $l \setminus \mathrm{PG}(2, q)$ the lines through the points of $\{m \cap \mathrm{PG}(2, q) \setminus B\}$ are tangents, and at the points of B' on $m \setminus \mathrm{PG}(2, q)$ the lines through the points of $\{l \cap \mathrm{PG}(2, q) \setminus B\}$ are tangents. At Q all the lines of $\mathrm{PG}(2, q^h)$ intersecting $\mathrm{PG}(2, q)$ in exactly Q are tangents to B'.

The size of B' is simply $|l \setminus \mathrm{PG}(2,q)| + |m \setminus \mathrm{PG}(2,q)| + |B|$ if $Q \in B$ and $|l \setminus \mathrm{PG}(2,q)| + |m \setminus \mathrm{PG}(2,q)| + |B| + 1 - |C|$ if $Q \notin B$. ■

When $Q \notin B$ and $|C| > 1$, then the set B' in Construction 4.3.1 may not be a blocking set at all, because in B a line through two points of C may have been blocked by only these points. In this case some of the points of C have to be added to B', and thus the size of the resulting blocking set can be only determined given the concrete case. But as the next proposition shows, this problem does not arise when $|B| < 2q$.

Proposition 4.3.3. *Let $x \geq 1$ be an integer. If the size of the minimal blocking set B is $2q - x$, then the number of tangents at any point of B is at least $x + 1$. Hence there are no critical points of B.*

Proof. Direct consequence of Proposition 3.5.3. ■

Theorem 4.3.4. *Let $x \geq 1$ be an integer. If there is a minimal blocking set of size $2q - x$ in* $\mathrm{PG}(2,q)$*, then there are minimal blocking sets of size $2q^h - x$ and $2q^h - x + 1$ in* $\mathrm{PG}(2,q^h)$*. If we start from a Rédei type minimal blocking set, then the resulting blocking sets can be chosen to be of Rédei type, and also not to be of Rédei type.*

Proof. Use Construction 4.3.1. Note that $m \cap \mathrm{PG}(2,q)$ (or equivalently $l \cap \mathrm{PG}(2,q)$) is a Rédei line of B if and only if m is a Rédei line of B', as $|B' \setminus m| = |B \setminus m| + q^h - q$. All other lines intersect B' in less than q points. ■

In [18] Danielsson proves the existence of Rédei type minimal blocking sets of size $2p - 3$ and $2p - 2$.

Theorem 4.3.5 (Danielsson, [18]). *Let $p > 5$ be a prime. If $p \equiv 1 \pmod 4$, then there are Rédei type minimal blocking sets of size $2p - 3$. If $p \equiv 3 \pmod 4$, then there are Rédei type minimal blocking sets of size $2p - 2$.*

Using the previous constructions the following can be proved:

Corollary 4.3.6. *Let $q = p^h$ with $h > 1$ and $p > 5$ a prime. In* $\mathrm{PG}(2,q)$ *there are minimal blocking sets of size $2q - 2$ (both of Rédei type and not of Rédei type). If $p \equiv 1 \pmod 4$, then in* $\mathrm{PG}(2,q)$ *there are minimal blocking sets of size $2q - 3$ (both of Rédei type and not of Rédei type).*

We now turn attention to another embedding method, which is described in [36] and [44]. Here we only repeat the construction and a theorem from these papers, and investigate what this method means for the minimal blocking sets obtained in this chapter. For further details of this construction we refer to the papers [36, 44].

Construction 4.3.7. Let B be a minimal blocking set in $\mathrm{PG}(2,q)$. Embed $\mathrm{PG}(2,q)$ into $\mathrm{PG}(h+1,q)$. Choose an $(h-2)$-dimensional subspace Σ, so that $\mathrm{PG}(2,q)\cap\Sigma=\emptyset$. Let B' be the cone with base B and vertex Σ. Embed $\mathrm{PG}(h+1,q)$ as a subgeometry in $\mathrm{PG}(h+1,q^h)$. Assume that R is an $(h-1)$-dimensional subspace of $\mathrm{PG}(h+1,q)$, and let R^* be the extension of R. Choose an $(h-2)$-dimensional subspace P in R^*, such that P does not intersect the subgeometry $\mathrm{PG}(h+1,q)$, and project B' from this subspace onto a plane π of $\mathrm{PG}(h+1,q^h)$, where $\pi\cap P=\emptyset$. The cardinality of the projection, B'' satisfies $|B''|=|B'|+1-|R\cap B'|$.

Note that B' is a minimal blocking set of $\mathrm{PG}(h+1,q)$ with respect to lines and $|B'|=q^{h-1}|B|+\frac{q^{h-1}-1}{q-1}$, thus if $|B|<2q$ then $|B'|<2q^h$.

Theorem 4.3.8. *Let B' be a minimal blocking set of $\mathrm{PG}(h+1,q)$ with respect to lines and suppose that $|B'|\le 2q^h-1$. Then the projection B'' of B' is a minimal blocking set of $\mathrm{PG}(2,q^h)$.*

By Theorem 4.3.8, starting from any of the minimal blocking sets constructed in this chapter and using Construction 4.3.7 will result in minimal blocking sets for q sufficiently large. The size of the resulting blocking set B'' depends on the choice of R. Following the reasonings of [44] (page 262) it can be proved that, depending on the dimension of $R\cap\Sigma$ (which can vary between $h-2$ and $h-4$), the size of $|R\cap B'|$ can be: $\frac{q^{h-1}-1}{q-1}$, $q^{h-1}+\frac{q^{h-1}-1}{q-1}$, $rq^{h-2}+\frac{q^{h-2}-1}{q-1}$ (where B has an r-secant in $\mathrm{PG}(2,q)$) and $|B|q^{h-3}+\frac{q^{h-3}-1}{q-1}$.

Theorem 4.3.9. *Let B be a minimal blocking set of $\mathrm{PG}(2,q)$ with $|B|=2q-x$, where $x\ge 1$. Using Construction 4.3.7 one can obtain blocking sets of $\mathrm{PG}(2,q^h)$, $h>1$ with sizes*

$$2q^h-xq^{h-1}+1,$$

$$2q^h-(x+1)q^{h-1}+1,$$

$2q^h - xq^{h-1} - q^{h-2} + (x+1)q^{h-3} + 1$

$2q^h - xq^{h-1} - (r-1)q^{h-2} + 1$, *where B has an r-secant in* $\mathrm{PG}(2,q)$.

It is not difficult to see that starting from a Rédei type minimal blocking set, we can choose R in such a way that the projection will be of Rédei type, or not. For simplicity let $h = 2$, so R is a line of $\mathrm{PG}(h+1,q)$ and Σ is a point (with either $\Sigma \in R$ or $\Sigma \notin R$). Let B be a minimal blocking set of size $2q - x$ with $x \geq 1$. There will be three types of lines in the projection:

(i) lines that were projected from lines of $\mathrm{PG}(h+1,q)$: these intersect B'' in at most $q+1$ points;

(ii) lines that were projected from a plane β through R, with $\Sigma \notin \beta$ (only if $\Sigma \notin R$): these intersect B'' in $|B| + 1 - |R \cap B'|$ points;

(iii) lines that were projected from a plane β through R, with $\Sigma \in \beta$: these intersect B'' in $rq + 2 - |R \cap B'|$ points, where $r = |\beta \cap B|$.

(For a precise discussion on intersection numbers of B'' with respect to lines see [36], p.742.) For B'' to be a minimal blocking set of Rédei type we must have some lines intersect B'' in $|B|q + 2 - |R \cap B'| - q^2 = q^2 - qx + 2 - |R \cap B'|$ points. For the lines of type (i) this is impossible. For a line of type (ii) to be a Rédei line, the equation $|B|q + 2 - |R \cap B'| - q^2 = |B| + 1 - |R \cap B'|$ has to hold, which leads to $|B| = q + 1$, a contradiction. For a line of type (iii) to be a Rédei line, the equation $|B|q + 2 - |R \cap B'| - q^2 = rq + 2 - |R \cap B'|$ has to hold, from which $|B| - q = r$, which is equivalent to $\beta \cap \mathrm{PG}(2,q)$ being a Rédei line of B. Thus, B'' will be of Rédei type if and only if there is a plane on R and Σ intersecting $\mathrm{PG}(2,q)$ in a Rédei line of B.

Bibliography

This thesis is based on

[1] N. V. Harrach. Unique reducibility of multiple blocking sets. *J. Geom.*, 103:445–456, 2012.

[2] N. V. Harrach and C. Mengyán. Minimal blocking sets in $\mathrm{PG}(2, q)$ arising from a generalized construction of megyesi. *Innov. Incidence Geom.*, 6/7:211–226, 2007/2008.

[3] N. V. Harrach and K. Metsch. Small point sets of $\mathrm{PG}(n, q^3)$ intersecting each k-subspace in 1 mod q points. *Designs, Codes and Cryptography*, 56(2-3):235–248, 2010.

[4] N. V. Harrach, K. Metsch, T. Szőnyi, and Zs. Weiner. Small point sets of $\mathrm{PG}(n, p^{3h})$ intersecting each line in 1 mod p^h points. *Journal of Geometry*, 98(1-2):59–78, 2010.

Further references

[5] G. Bacsó, T. Héger, and T. Szőnyi. The 2-blocking number and the upper chromatic number of $\mathrm{PG}(2, q)$. *J. Comb. Des.*, 21:585–602, 2013.

[6] S. Ball. On nuclei and blocking sets in Desarguesian spaces. *J. Combin. Theory Ser. A*, 85:232–236, 1999.

[7] A. Blokhuis. On multiple nuclei and a conjecture of Lunelli and Sce. *Bull. Belg. Math. Soc.*, 3:349–353, 1994.

[8] A. Blokhuis. On nuclei and affine blocking sets. *J. Combin. Theory Ser. A*, 67:273–275, 1994.

[9] A. Blokhuis. On the size of a blocking set in $\mathrm{PG}(2,p)$. *Combinatorica*, 14:111–114, 1994.

[10] A. Blokhuis. Blocking sets in desarguesian planes. *Bolyai Soc. Math. Studies*, 2:133–155, 1996. Paul Erdős is Eighty.

[11] A. Blokhuis, L. Lovász, L. Storme, and T. Szőnyi. On multiple blocking sets in Galois planes. *Adv. Geom.*, 7:39–53, 2007.

[12] A. Blokhuis and H. A. Wilbrink. A characterization of exterior lines of certain sets of points in $\mathrm{PG}(2,q)$. *Geom. Dedicata*, 23:253–254, 1987.

[13] R. C. Bose and R. C. Burton. A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald Codes. *J. Comb. Theory*, 1:96–104, 1966.

[14] A. E. Brouwer and A. Schriver. The blocking number of an affine space. *J. Combin. Theory Ser. A*, 24:251–253, 1978.

[15] A. Bruen. Baer subplanes and blocking sets. *Bull. Amer. Math. Soc.*, 76:342–344, 1970.

[16] A. Bruen. Blocking sets in finite projective planes. *SIAM J. Appl. Math.*, 21:380–392, 1971.

[17] A. Bruen and K. Drudge. The return of the Baer subplane. *J. Comb. Theory Ser. A*, 85:228–231, 1999.

[18] J. Danielsson. Minimal blocking sets of size $2p-2$ and $2p-3$ in $\mathrm{PG}(2,p)$, p prime and $p>5$. *J. Geom.*, 88:15–18, 2008.

[19] Sz. L. Fancsali and P. Sziklai. Description of the clubs. *Ann. Univ. Sci. Budapest Eötvös Sect.Math.*, 51:141–146, 2009.

[20] S. Ferret, L. Storme, P. Sziklai, and Zs. Weiner. A $t \pmod p$ result on weighted multiple $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$. *Innov. Incidence Geom.*, 6/7:169–188, 2007/2008.

[21] S. Ferret, L. Storme, P. Sziklai, and Zs. Weiner. A characterization of multiple $(n-k)$-blocking sets in projectiove spaces of square order. *Adv. Geom.*, 14:739–756, 2012.

[22] A. Gács. On the number of directions determined by a point set in $\mathrm{AG}(2,p)$. *Discrete Math.*, 208/209:299–309, 1999.

[23] A. Gács, P. Sziklai, and T. Szőnyi. Two remarks on blocking sets and nuclei in planes of prime order. *Des. Codes Cryptogr.*, 10:29–39, 1997.

[24] U. Heim. Blockierende Mengen in endlichen projektiven Räumen. *Mitt. Math. Semin. Giessen*, 226:4–82, 1996.

[25] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions.* Clarendon Press, Oxford, 1985.

[26] J. W. P. Hirschfeld. *Projective geometries over finite fields.* Clarendon Press, Oxford, second edition edition, 1998.

[27] J. W. P. Hirschfeld and J. Thas. *General Galois geometries.* Oxford University Press, 1991.

[28] R. Jamison. Covering finite fields with cosets of subspaces. *J. Combin. Theory Ser. A*, 22:253–266, 1977.

[29] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$ and its dual. *Finite Fields Appl.*, 14:1020–1038, 2008.

[30] G. Lunardon. Linear k-blocking sets. *Combinatorica*, 21:571–581, 2001.

[31] G. Lunardon, P. Polito, and O. Polverino. A geometric characterisation of linear k-blocking sets. *J. of Geometry*, 74:120–122, 2002.

[32] C. Mengyán. *Constructional methods in finite projective geometry.* PhD thesis, Mathematics PhD School of the Eötvös Loránd University, 2008.

[33] P. Polito and O. Polverino. On small blocking sets. *Combinatorica*, 18:133–137, 1998.

[34] O. Polverino. Small minimal blocking sets and complete k-arcs in $\mathrm{PG}(2,p^3)$. *Discrete Math.*, 208/209:469–476, 1999.

[35] O. Polverino and L. Storme. Small minimal blocking sets in $\mathrm{PG}(2, q^3)$. *European J. Combin.*, 23(1):83–92, 2002.

[36] O. Polverino, T. Szőnyi, and Zs. Weiner. Blocking sets in Galois planes of square order. *Acta Sci. Math. (Szeged)*, 65:737–748, 1999.

[37] L. Rédei. *Lacunary Polynomials over Finite Fields.* North-Holland Publishing Co., Amsterdam, American Elsevier Pub. Co., New York, 1973.

[38] P. Sziklai. Nuclei of point sets in $\mathrm{PG}(n, q)$. *Discrete Math.*, 174:323–327, 1997.

[39] P. Sziklai. A lemma on the randomness of d-th powers in $\mathrm{GF}(q)$, $d|q-1$. *Bull. Belg. Math. Soc. Simon Stevin*, 8(1):95–98, 2001.

[40] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory Ser. A*, 115(7):1167–1182, 2008.

[41] P. Sziklai and L. Storme. Linear pointsets and Rédei type k-blocking sets in $\mathrm{PG}(n, q)$. *J. Alg. Comb.*, 14:221–228, 2001.

[42] T. Szőnyi. Combinatorial problems for Abelian groups arising from geometry. *Period. Polytechnica*, 19:91–100, 1991.

[43] T. Szőnyi. Blocking sets in Desarguesian affine and projective planes. *Finite Fields Appl.*, 3(3):187–202, 1997.

[44] T. Szőnyi, A. Gács, and Zs. Weiner. On the spectrum of minimal blocking sets in $\mathrm{PG}(2, q)$. *J. of Geometry*, 76:256–281, 2003.

[45] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory Ser. A*, 95(1):88–101, 2001.

[46] G. Van de Voorde. *Blocking sets in finite projective spaces and coding theory.* PhD thesis, Universiteit Gent, 2011.

[47] Zs. Weiner. Small point sets of $\mathrm{PG}(n, q)$ intersecting each k-space in 1 modulo $\sqrt{q}$ points. *Innov. Incidence Geom.*, 1:171–180, 2005.

Summary

In this thesis we present results about blocking sets in the finite projective space $\mathrm{PG}(n, q)$. The results presented here are based on articles [1], [2], [3] and [4].

In Chapter 1 the notation, definitions, and most important preliminary results are presented. We aim at using standard notation.

Small minimal $(n-k)$-blocking sets of $\mathrm{PG}(n, q)$ are of special interest, as there is hope to characterize them. Sziklai's Linearity Conjecture claims that all small minimal $(n-k)$-blocking sets are linear. Szőnyi and Weiner prove in [45] that small minimal $(n-k)$-blocking sets meet every k-space in 1 mod p points, where $q = p^h$ is the order of the projective space. It is also proved that the sizes of small minimal blocking sets are contained in disjoint intervals. In Chapter 2 we prove the Linearity Conjecture in one of these intervals.

In Chapter 3 we turn our attention to multiple blocking sets. In a multiple blocking set one can always find a minimal multiple blocking set. In this chapter we prove that if B is a weighted t-fold $(n-k)$-blocking set of $\mathrm{PG}(n, q)$ with size at most $(t+1)q^{n-k} + q^{n-k-1} + \cdots + q + 1$, then the minimal t-fold $(n-k)$-blocking set contained in B is unique. Examples of the last section show that our result is sharp in certain cases.

In Chapter 4 planar blocking set constructions are presented. The main construction of this chapter is a generalization of the Megyesi construction and also of a construction given by Gács in [22]. A set of q points is selected with the aid of a subgroup of the multiplicative group $\mathrm{GF}(q)^*$. This set, together with the ideal points determined by it forms a minimal blocking set, which is contained in the union of $n + 1$ lines, precisely n of which are concurrent. The last section of this chapter presents constructions which produce blocking sets of $\mathrm{PG}(2, q^h)$ starting from a blocking set of $\mathrm{PG}(2, q)$.

Magyar nyelvű összefoglaló

Doktori értekezésemben véges projektív terek lefogó ponthalazaival kapcsolatos állítások és konstrukciós eljárások szerepelnek. Eredményeim az [1], [2], [3] és [4] cikkekben jelentek meg.

Az 1. fejezetben a szükséges definíciókat, jelöléseket, valamint a korábbi eredményeket mutatom be.

Az utóbbi években megkülönböztetett figyelem övezi a $\mathrm{PG}(n,q)$ projektív tér kicsi minimális lefogó ponthalmazait, mivel ezek karakterizációja reményteljes vállalkozásnak tűnik. Sziklai fogalmazta meg az ún. Linearitási Sejtést, mely szerint minden kicsi minimális lefogó ponthalmaz lineáris. Szőnyi és Weiner a [45] cikkben bizonyította, hogy egy kicsi minimális lefogó ponthalmaz minden k-dimenziós alteret $1 \bmod p$ pontban metsz. Azt is belátták, hogy a kicsi minimális lefogó ponthalmazok méretei diszjunkt intervallumokba tartoznak. A 2. fejezetben az egyik interallumban bizonyítjuk a Linearitási Sejtést.

A 3. fejezetben többszörösen lefogó ponthalmazokat vizsgálunk. Egy súlyozott t-szeres $(n-k)$-lefogó ponthalmazban mindig találhatunk minimális súlyozott t-szeres $(n-k)$-lefogó ponthalmazt. A 3. fejezetben belátjuk, hogy ha a súlyozott t-szeres $(n-k)$-lefogó ponthalmaz mérete legfeljebb $(t+1)q^{n-k}+q^{n-k-1}+\cdots+q+1$, akkor egyértelmű a bennefoglalt minimális rész.

A 4. fejezet lefogó ponthalmaz konstrukciókat mutat be. A legfontosabb konstrukciónk a Megyesi féle konstrukció, illetve Gács [22] cikkben bemutatott konstrukciójának általánosítása. A $\mathrm{GF}(q)^*$ multiplikatív csoport egy részcsoportja segítségével választunk ki egy q elemű ponthalmazt a $\mathrm{PG}(2,q)$ projektív tér $\mathrm{AG}(2,q)$ affin részében, majd ehhez hozzávéve a meghatározott ideális pontokat, minimális lefogó ponthalmazt nyerünk. Az így kapott minimális lefogó ponthalmazok $n+1$ egyenesen helyezkednek el, melyből n konkurrens.