

Zsuzsa Weiner

**GEOMETRIC AND ALGEBRAIC METHODS IN
GALOIS-GEOMETRIES**

PhD thesis

Supervisor: Prof. Tamás Szőnyi

Mathematics PhD School of the Eötvös Loránd University

Director: Prof. Miklós Laczkovich

Pure Mathematics PhD Program

Director: Prof. János Szenthe

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

and

Central European University, Budapest, Hungary

2002

Contents

Introduction	3
Acknowledgements	4
Notation and definitions	5
An overview on blocking sets	7
Blocking sets in Galois planes	7
Blocking sets in higher dimensions	12
1 Planar blocking sets	13
1.1 Constructing blocking sets in $\text{PG}(2, q^2)$	13
1.1.1 The construction	13
1.1.2 Examples obtained by projections of cones	17
1.2 Generalization of the construction	20
1.2.1 The geometric description	20
1.2.2 The algebraic description	26
1.3 Another application	29
2 Blocking sets in higher dimensions	33
2.1 Intersection with subspaces	34
2.2 Applications	38
2.2.1 An observation	38
2.2.2 Spectra of blocking sets	39
2.2.3 An attempt to characterize blocking sets	43
3 Algebraic background	47
3.1 A bound on the degree of the g.c.d.	47
3.2 An important observation	50

4	(k, p^e)-arcs	53
4.1	Introduction	53
4.2	The main result	55
4.3	Remarks	64
5	A conjecture of Metsch	67
	Bibliography	71
	Summary	77
	Magyar nyelvű összefoglaló	79

Introduction

Concerning finite geometry, several methods can be used from other fields of mathematics. The first two chapters contain mostly combinatorial and geometric reasonings, while the last two chapters give examples of how algebraic results can be applied.

In Chapter 1 a geometric construction for various minimal planar blocking sets is presented. Section 1.1 appeared as [2], here we construct minimal planar blocking sets using 3-dimensional projective spaces. Section 1.2 is the generalization of the previous section. With minor alteration, the idea of Section 1.2 can be used to construct $(q + t, t)$ -arcs of type $(0, 2, t)$, see Section 1.3. The results of the latter two sections are from [3] and [1].

Chapter 2 is devoted to higher dimensional blocking sets and it appeared as [4]. In $\text{PG}(2, q)$, $q = p^h$, Szőnyi proved that a small minimal blocking set intersects each line in $1 \pmod p$ point. The main result of Chapter 2 is that we generalize this result to higher dimensions. Furthermore, we use this generalization to characterize blocking sets.

In Chapter 3 we summarize the common algebraic background used in the next two chapters.

In Chapter 4, that is [5], Szőnyi's embeddability result on (k, p) -arcs is improved, it is shown that there are no complete (k, p^e) -arcs of size a little bit smaller than the size of the maximal arc.

Finally, in Chapter 5 a conjecture of Metsch on the number of lines intersecting a point set is proved.

Acknowledgements

I would like to thank my co-authors, Aart Blokhuis, András Gács, Olga Polverino, Leo Storme and Tamás Szőnyi for the joint work and Klaus Metsch for the problem which is the topic of the last chapter, furthermore, I thank Péter Sziklai for his constructive suggestions during the preparation of this thesis.

Finally, above all, I am most grateful to my supervisor, Tamás Szőnyi, for his enthusiastic supervising, introducing me to several interesting problems and for the many valuable discussions, from which I learnt a lot.

Notation and definitions

In this section we give the most important definitions and notation that will be used throughout this thesis.

Notation

We will work on the Desarguesian affine and projective spaces $\text{AG}(n, q)$ and $\text{PG}(n, q)$; see [33]. Hence q is a prime power, the letter q will always denote the order of the Galois plane, while p will always denote the characteristic of the field $\text{GF}(q)$. Throughout this thesis we use the usual representation of $\text{AG}(2, q)$ and $\text{PG}(2, q)$.

Affine coordinates. The points of $\text{AG}(2, q)$ have *affine coordinates* (x, y) , where x and y are elements of $\text{GF}(q)$. The lines of $\text{AG}(2, q)$ have equation $mX + b - Y = 0$ or $X = c$, where m is the slope of the line. The *infinite points* or *ideal points* can be identified with slopes, so (m) will denote the infinite point of lines with slope m . Similarly (∞) will be the infinite point of the vertical lines, the lines with equation $X = c$.

Homogeneous coordinates. In $\text{PG}(2, q)$ the points are represented by *homogeneous triples* (x, y, z) , where x, y and z are elements of $\text{GF}(q)$, and $(x, y, z) \neq (0, 0, 0)$. Two triples represent the same point iff one is the scalar multiple of the other. Lines are represented similarly, by triples $[x, y, z]$. A point is incident with a line iff the scalar product of their coordinate vectors is 0.

Similarly, the points of $\text{PG}(n, q)$ are represented by homogeneous vectors (x_0, x_1, \dots, x_n) , where the x_i 's are elements of $\text{GF}(q)$, and $(x_0, x_1, \dots, x_n) \neq (0, \dots, 0)$. Hyperplanes are represented similarly, by vectors $[x_0, x_1, \dots, x_n]$. A point is incident with a hyperplane iff the scalar product of their coordinate vectors is 0. The $(n - k)$ -dimensional subspaces can be obtained as the intersection of k hyperplanes.

Definitions

Subgeometry. A projective space $\text{PG}(n, q)$ embedded in $\text{PG}(n^s, q^k)$ is called a subgeometry. When $n = 2$ and $s = 1$, it is also called a *subplane* and when

$k = 2$, it is the *Baer subgeometry* of dimension n . For $n^s = n = k = 2$, they are the *Baer subplanes*.

Blocking sets. A *blocking set with respect to k -dimensional subspaces* (or an $(n - k)$ -*blocking set*) in $\text{PG}(n, q)$, is a set B of points which intersects every k -dimensional subspace. Of course, this notion is trivial for $k = n$ or 0 , hence we will always suppose that $0 < k < n$. A point P of B is called *essential* if there exists a k -dimensional subspace that intersects B in P only. Such a subspace will be called a *tangent* of B at P . This means that the point P is essential if and only if $B \setminus P$ is not a k -blocking set. When the points of B are all essential, B is called *minimal* (or *irreducible*). In other words, B is minimal if no proper subset of it is an $(n - k)$ -blocking set. The blocking set B is *trivial* if it contains an $(n - k)$ -dimensional subspace, otherwise it is called *non-trivial*. A blocking set with respect to k -dimensional subspaces in $\text{PG}(n, q)$ is *small* if its size is less than $3(q^{n-k} + 1)/2$. A t -fold $(n - k)$ -blocking set in $\text{PG}(n, q)$, is a set B of points which intersects every k -dimensional subspace in at least t points.

When $n = 2$, blocking sets are called *planar blocking sets*. Observe that here a blocking set is small if it has size less than $3(q + 1)/2$.

Arcs. A (k, n) -*arc* in the projective plane $\text{PG}(2, q)$ is a set of k points such that each line intersects it in at most n points. It is *complete* if it cannot be extended to a $(k + 1, n)$ -arc. It is not difficult to see that $k \leq qn - q + n$. When equality holds, a (k, n) -arc is called *maximal*.

Note that blocking sets and (k, n) -arcs are similar objects. More precisely, the complement of a (k, n) -arc in $\text{PG}(2, q)$ is a $(q + 1 - n)$ -fold blocking set in $\text{PG}(2, q)$.

An overview on blocking sets

In this section we summarize the known results concerning blocking sets in Galois planes and in higher dimensional projective spaces.

Blocking sets in Galois planes

After the definition of minimal blocking sets, the very first question is whether there are other blocking sets than lines. For $\text{PG}(2, 2)$, the answer is negative, which was already observed in 1947 by von Neumann and Morgenstern. Note that for $q > 2$, the vertexless triangle (that is $(\ell_1 \cup \ell_2 \cup \ell_3) \setminus \{\ell_1 \cap \ell_2, \ell_1 \cap \ell_3, \ell_2 \cap \ell_3\}$ for three non-concurrent lines ℓ_1, ℓ_2, ℓ_3) is always a minimal blocking set of size $3q - 3$. Similarly, if $P_1 \in \ell_1$, $P_2 \in \ell_2$, $P_1, P_2 \notin \ell_1 \cap \ell_2$, and P_3 is a point on the line joining P_1 and P_2 , $P_3 \neq P_1, P_2$, then $(\ell_1 \cup \ell_2 \cup \{P_3\}) \setminus \{P_1, P_2\}$ is a minimal blocking set of size $2q$.

In this subsection first we list a few constructions for planar blocking sets, then we survey some results on the possible sizes of minimal planar blocking sets.

Known constructions

The construction below yields a huge class of blocking sets, but before introducing this class we need a definition.

Definition 0.1 *Let U be a subset of $\text{AG}(2, q)$. An infinite point (m) is determined by U , if there are two different points $P_1, P_2 \in U$ so that P_1, P_2 and (m) are collinear.*

Assume that U is a set of q points in $\text{AG}(2, q)$. Denote by D the set of directions determined by U . It is not difficult to see that if $|D| < q + 1$, then $B = U \cup D$ is a minimal blocking set. Hence by this construction we obtain minimal blocking sets of size at most $2q$. It is also not difficult to prove that if B is a minimal blocking set of size at most $2q$ and if there is a line ℓ so that $|B \setminus \ell| = q$, then B can be obtained by the construction above.

Definition 0.2 *A blocking set of size $q + m$ in $\text{PG}(2, q)$ is of Rédei type if it has an m -secant line. Such a line is called a Rédei line.*

In applications, the set U is often the graph of a function f from $\text{GF}(q)$ to $\text{GF}(q)$. Hence it can be written in the form of $U = \{(x, f(x)) : x \in \text{GF}(q)\}$. Note that now a direction (m) is determined, when there are x, u such that $(f(x) - f(u))/(x - u) = m$. Furthermore, for any set $U \subset \text{AG}(2, q)$ of size q , determining at most q directions, one can always choose the coordinate system so that U will be the graph of a function from $\text{GF}(q)$ to $\text{GF}(q)$.

The next examples are some important cases of this construction. Each example is given by the function f .

Example 0.3 (1) *Suppose that q is odd and let f be the function $f(x) = x^{(q+1)/2}$. Then $|B| = 3(q+1)/2$. This example is called the projective triangle.*

(2) *Let f be the trace function from $\text{GF}(q)$ to a subfield $\text{GF}(q')$, that is $f(x) = x + x^{q'} + \dots + x^{q/q'}$. Then $|B| = q + 1 + q/q'$. For $q' = 2$ this is called the projective triad.*

(3) *Let $f(x) = x^{q'}$, where again $\text{GF}(q')$ is a subfield of $\text{GF}(q)$. Then $|B| = q + (q-1)/(q'-1)$. For $q' = \sqrt{q}$, this gives a Baer subplane.*

For a while it seemed that the minimal blocking sets of size less than $3(q+1)/2$ are all of Rédei type. A wider class of small blocking sets, called *linear* ones, were constructed by Lunardon [39], [40], Polito and Polverino [43]. They showed (see [39]) that this class contains all blocking sets of Rédei type, and proved that this class contains some (actually a lot of) non-Rédei type blocking sets (see [43]).

Now we give a definition of linear point sets, which is compatible with the definition introduced by Lunardon.

Definition 0.4 *Assume that S is a point set in $\text{PG}(2, q)$, $q = p^h$. Embed $\text{PG}(2, q)$ in $\text{PG}(n, q)$ as a subspace. Then S is $\text{GF}(p^e)$ -linear if it is the projection of a subgeometry (in $\text{PG}(n, q)$) isomorphic to $\text{PG}(n', p^e)$, from a subspace disjoint from the subgeometry.*

Note that a $\text{GF}(p^e)$ -linear point set is not necessarily a blocking set. A linear blocking set is a linear point set that is a blocking set.

Moving towards larger blocking sets, there are many blocking sets of size between $2q - 1$ and $3q - 3$, but no examples of minimal blocking sets of size cq are known, where c is a constant larger than 3. Several constructions give minimal blocking sets of size $cq \log q$, see Szőnyi [51], this seems to be the “typical cardinality” of a minimal blocking set. Large blocking sets are difficult to construct. Very recently in $\text{PG}(2, q^h)$, Szőnyi constructed minimal blocking sets of size $q^{h+1} + 1$. Finally, on planes of square order the points of a Hermitian curve, that is defined by the equation $X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0$, is a minimal blocking set of size $q\sqrt{q} + 1$.

In Chapter 1 we construct various minimal blocking sets, among them there are also linear but non-Rédei type ones. In $\text{PG}(2, q^h)$, we also construct relatively large blocking sets of size roughly $q^h \sqrt{q}$.

Characterization-type results

One of the most interesting questions on blocking sets is to determine the possible sizes of the minimal ones. A much harder task is to characterize them.

The first result in this direction is due to Bruen [23], who proved that a non-trivial minimal blocking set has size at least $q + \sqrt{q} + 1$. When q is a square, minimal blocking sets of that size exist; these are exactly the point sets of Baer subplanes. Concerning the other end of the spectrum Bruen and Thas [26] showed that the largest minimal blocking sets have size at most $q\sqrt{q} + 1$. Again when q is a square, this bound is sharp and in case of equality the set has to be a unital, that means that there are a unique tangent at each point of the set and the non-tangent lines meet the set in $\sqrt{q} + 1$ points. Unitals do exist, e.g. the points of a Hermitian curve form a unital.

There has been a lot of attention paid on minimal blocking sets of Rédei type. Blokhuis, Ball, Brouwer, Storme and Szőnyi showed that the size of a Rédei type blocking set lies in certain, relatively short intervals depending on q . Furthermore, they gave an almost complete characterization of these blocking sets. Before stating the result we need a definition. Let K denote the field $\text{GF}(q)$, $q = p^n$. K^2 may be mapped to $L = \text{GF}(q^2)$ by $(a, b) \mapsto \alpha a + \beta b$, for arbitrary $\alpha, \beta \in L^*$ with $\alpha/\beta \notin K$. If F is a subfield of K (that is $F = \text{GF}(p^e)$, where e divides n), then K and hence also L is a vector space over F . A subset V of K^2 will be called F -linear, if it is mapped in this way to an F -subspace of

L. It is easy to check that this property is well-defined, that is, it is independent of the choice of α and β defining the mapping.

Result 0.5 (Blokhuis, Ball, Brouwer, Storme, Szőnyi [17]) *Let $U \subset \text{AG}(2, q)$ be a point set of size q , let D be the set of directions determined by U , and put $N := |D|$. Let e (with $0 \leq e \leq n$) be the largest integer such that each line with slope in D meets U in a multiple of p^e points. Then one of the following holds:*

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

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

(iii) $p^e > 2$, $e|n$, and $q/p^e + 1 \leq N \leq (q - 1)/(p^e - 1)$,

(iv) $e = n$ and $N = 1$.

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

It follows from the result above easily that $U \cup D$ is a linear blocking set. Considering Rédei type blocking sets, for planes of prime order, Gács proved the following theorem.

Result 0.6 (Gács [29]) *Let B be a Rédei type blocking set of $\text{PG}(2, p)$, p prime. Then either B is the projective triangle or $|B| \geq p + [2(p - 1)/3] + 1$.*

For general prime powers not much is known, except for the case $q = p^2$. In this case, using a lemma of Lovász and Szőnyi, Gács also showed that any Rédei type blocking set in $\text{PG}(2, p^2)$ of size $3(p^2 + 1)/2$ has to be equivalent to the projective triangle. Furthermore, he proved that if a Rédei type blocking set has more than this number of points, then it has at least $1 + (3p^2 + p)/2$ points. In Chapter 1 Rédei type blocking sets of size $1 + (3p^2 + p)/2$ are constructed; which shows that the above bound is sharp.

In the general case, for arbitrary small minimal blocking sets, Szőnyi proved a similar theorem to Result 0.5. The difference is that here the sizes of the intervals are roughly double of those in Result 0.5. Furthermore, he also showed that a small minimal blocking set intersects each line in $1 \pmod{p^e}$ points, for some e depending on the size of the blocking set. More precisely, he proved the following theorem.

Result 0.7 (Szőnyi, [52]) *Let B be a non-trivial, minimal blocking set in $\text{PG}(2, q)$, $q = p^n$. Suppose that $|B| < 3(q + 1)/2$. Then*

$$q + 1 + \frac{q}{p^e + 2} \leq |B| \leq \frac{qp^e + 1 - \sqrt{(qp^e + 1)^2 - 4q^2p^e}}{2}, \quad (0.1)$$

for some integer e , $1 \leq e$. If $|B|$ lies in the interval belonging to e and $p^e \geq 9$ (or $e = 1$), then each line intersects B in 1 modulo p^e points.

Later this result will be referred as the 1 mod p result. The upper bound of this interval was improved by Polverino [45].

There is a hope to characterize small minimal blocking sets. In some cases this is already done.

Result 0.8 (1) (Blokhuis, [16]) *If $q = p$ prime, then there are no small minimal non-trivial blocking sets in $\text{PG}(2, p)$ at all;*

(2) (Szőnyi, [52]) *If $q = p^2$, p prime, then small minimal non-trivial blocking sets in $\text{PG}(2, p^2)$ are Baer subplanes;*

(3) (Polverino, [45]) *If $q = p^3$, p prime, then small minimal non-trivial blocking sets in $\text{PG}(2, p^3)$ have size $p^3 + p^2 + 1$ or $p^3 + p^2 + p + 1$ and they are of Rédei type.*

Case (3) is generalized to planes of order q^3 , see Polverino, Storme [46]. The bound in Theorem 0.8 (1) was conjectured by Di Paola [42], who studied the smallest non-trivial blocking sets in planes of small order. The lower bound in Theorem 0.8 (3) was conjectured by Bruen [24], and proved by Blokhuis [15].

Concerning the upper end of the spectrum, there are not too many results. We have already seen the result from Bruen and Thas, which characterizes the largest minimal blocking sets as unitals. Blokhuis and Metsch [19] showed that in $\text{PG}(2, q)$, q square, there are no minimal blocking sets of size $q\sqrt{q}$, when $q \geq 49$. Hence the gap between the largest and the second largest minimal blocking sets is at least 2.

A set U of points in the projective plane of order q is called a *partial unital*, if (1) every point of U lies on at least one tangent line, (2) no line contains more than $\sqrt{q} + 1$ points of U , and (3) there is at least one line meeting U in $\sqrt{q} + 1$ points. Ball [9] showed that if a partial unital in $\text{PG}(2, q)$ has more than

$q\sqrt{q} + 1 - \sqrt{q}$ points, then it must be a subset of a unital; so it cannot be a minimal blocking set. Hence if we only consider minimal blocking sets that are partial unitals as well, then the above mentioned gap is at least \sqrt{q} .

In a joint result with Szőnyi [8], we proved that for arbitrary blocking sets this gap tends to infinity as q tends to infinity.

Theorem 0.9 ([8]) *A minimal blocking set in $\text{PG}(2, q)$, q square, of size less than $q\sqrt{q} + 1$ have size less than $q\sqrt{q} + 1 - \frac{1}{3}q^{\frac{1}{6}}$.*

Blocking sets in higher dimensions

Concerning higher dimensional blocking sets, again the interesting question is to determine the possible sizes, the possible intersection numbers with subspaces and describing the structure of certain small blocking sets. At the moment it seems that there is only chance to handle small minimal $(n - k)$ -blocking sets.

Regarding blocking sets in higher dimension much less is known than in the planar case. The smallest minimal $(n - k)$ -blocking sets in $\text{PG}(n, q)$ were characterized as k -dimensional subspaces (these are the trivial blocking sets) by Bose and Burton in the sixties. Blocking sets in higher dimensions were studied by Beutelspacher [14], Tallini [54] and others. Udo Heim [31] proved that the minimum size of a 1-blocking set in $\text{PG}(n, q)$ ($n > 2$, $q > 3$) is the same as in $\text{PG}(2, q)$. He also showed that 1-blocking sets of this cardinality (or 1 bigger) are necessarily planar. Furthermore he characterized the second smallest minimal $(n - k)$ -blocking sets for $q > 2$, see [32]. Such a blocking set is a cone with vertex an $(k - 2)$ -dimensional subspace and with base of a minimal cardinality non-trivial planar blocking set. A particular class of blocking sets, the *linear blocking sets*, was studied systematically by Lunardon [40] and his students.

In Chapter 2 we generalize the 1 modulo p result of Szőnyi (see Result 0.7) for blocking sets in $\text{PG}(n, q)$ with respect to k -dimensional subspaces.

Chapter 1

Planar blocking sets

In this chapter first we give a geometric construction yielding various minimal blocking sets in Galois planes. Then we show that these blocking sets can be obtained also by algebraic construction. Finally, as an application, the idea of the construction is used to obtain $(q + t)$ -arcs of type $(0, 2, t)$.

This chapter is based on [2], [1] and [3].

1.1 Constructing blocking sets in $\text{PG}(2, q^2)$

In this section our main construction is presented. Before doing this, some properties of Baer subgeometries are needed.

1. Each plane of $\text{PG}(3, q^2)$ intersects $\text{PG}(3, q)$ in a line or a plane.
2. Dually: each point P of $\text{PG}(3, q^2) \setminus \text{PG}(3, q)$ lies on a unique line $r = r_P$ of $\text{PG}(3, q)$.
3. If a plane through $P \in \text{PG}(3, q^2) \setminus \text{PG}(3, q)$ is a plane of $\text{PG}(3, q)$, then it contains r_P .

In the rest of this section P always denotes a point of $\text{PG}(3, q^2) \setminus \text{PG}(3, q)$ and r the line r_P .

1.1.1 The construction

Construction 1.1 *Let B' be a blocking set in $\text{PG}(3, q)$ with respect to lines, that is a set of points which intersects every line. Embed $\text{PG}(3, q)$ as a sub-*

geometry in $\text{PG}(3, q^2)$. Choose a point P not in $\text{PG}(3, q)$ and project B' from this point onto a plane π . Then the projection B'' will be a blocking set in $\text{PG}(2, q^2) = \pi$.

The cardinality of B'' satisfies

$$|B''| = |B'| + 1 - |r \cap B'|.$$

Proof: Take any line ℓ of $\text{PG}(2, q^2)$ and consider the plane α of $\text{PG}(3, q^2)$ generated by ℓ and P . This plane intersects $\text{PG}(3, q)$ in a line or a plane (see 1. of the list above). Since any line (or plane) intersects B' , ℓ must intersect B'' .

To compute the size of B'' consider a point $U' \in B'$, $U' \notin r$. The line PU' is not a line of $\text{PG}(3, q)$ (see 2. above), hence there is a one-to-one correspondence between these points U' and their projection $U'' \in \pi$. The points of $r \cap B'$ are projected onto the same point $R'' = r \cap \pi$. \square

Of course, it is not at all obvious that the projection of a minimal blocking set is also a minimal one, but under some mild conditions we are able to prove it.

Proposition 1.2 *Let P be a point not in $\text{PG}(3, q)$ and let r be the unique line of $\text{PG}(3, q)$ passing through P . Let B' be a blocking set of $\text{PG}(3, q)$ with respect to lines and suppose that through a point S' of $B' \setminus r$ there is a tangent line which does not intersect r . Let S'' be the projection of S' onto π , and as usual let B'' be the projection of B' . Then S'' is an essential point of B'' .*

If this condition holds for each point of $B' \setminus r$, then B'' is minimal. The point $R'' = r \cap \pi$ is always an essential point of B'' .

Proof: Denote by R'' the common point of π and r . Let S' be our point, and denote its projection to π by S'' . Then $S'' \in B''$, $S'' \neq R''$. By assumption there is a tangent $t_{S'}$ of B' through S' which does not intersect r . Consider the line $t'' = \langle t_{S'}, P \rangle \cap \pi$. We are going to show that t'' is a tangent of B'' at S'' . Since a plane through P which is a plane of $\text{PG}(3, q)$ must contain r , the plane $\langle t_{S'}, P \rangle$ intersects $\text{PG}(3, q)$ in $t_{S'}$; in other words, it meets B' only in S' . This proves that S'' is essential.

Now consider the point R'' . Take a point $R' \in r \cap B'$ that is mapped to R'' and any plane through r which is not a plane of $\text{PG}(3, q)$. This plane intersects

B' only in the points of $r \cap B'$, hence its intersection with π will be a tangent of B'' at R'' . \square

It is not easy to check the condition in the previous proposition, but there are some particular cases when it holds automatically. Theorem 1.3 and Proposition 1.7 give such conditions.

Theorem 1.3 *Let B' be a minimal blocking set of $PG(3, q)$ with respect to lines and suppose that $|B'| \leq 2q^2 - 1$. Then the projection B'' of B' is minimal.*

Before proving this, one needs some lemmas. The first one is essentially due to Blokhuis and Brouwer [18].

Result 1.4 (Blokhuis, Brouwer) *Let B be a blocking set in $PG(2, q)$, $|B| = 2q - s$ and let P be an essential point of B . Then there are at least $s + 1$ tangents through P .*

Proof: Let t denote the number of tangents through P . Delete P and put one-one point on each of these tangents with one exception. Choosing the line at infinity as this exceptional tangent, one gets an affine blocking set of size $|B| - 2 + t$. By [22], this affine blocking set has size at least $2q - 1$, whence the result follows. \square

We extend this result to blocking sets in 3 dimensions.

Proposition 1.5 *Let K be a minimal blocking set in $PG(3, q)$ (with respect to lines). If $|K| = 2q^2 + q - s$, then there are at least $s + 1$ tangent lines through each point of K .*

Proof: Take a point $P \in K$ and a tangent ℓ of K at P (such a line exists because of the minimality of K). Consider the planes π_1, \dots, π_{q+1} through ℓ . Let $K_i = \pi_i \cap K$. K_i is a blocking set in π_i and P is an essential point of it. Let s_i be defined such that $|K_i| = 2q - s_i$. The previous lemma implies that the number of tangents of K_i in π_i at P is at least $s_i + 1$ (this is trivial if $s_i < 0$). Counting points of $\cup K_i$ gives that

$$\sum_{i=1}^{q+1} (2q - s_i) = |K| + q,$$

and the total number of tangents through P is at least $\sum s_i + 1$. Substituting $|K| = 2q^2 + q - s$ yields $\sum s_i = s$. \square

The same proof shows that the same assertion holds for essential points of a not necessarily minimal blocking set in $\text{PG}(3, q)$ if its size is $2q^2 + q - s$.

Proof of Theorem 1.3: Each plane intersects $\text{PG}(3, q)$ in a line or a plane, hence it intersects B' . This proves that B'' is indeed a blocking set. To prove its minimality pick a point $Q'' \in B''$. If the line PQ'' is a line of $\text{PG}(3, q)$, then there is a plane through this line which is not a plane of $\text{PG}(3, q)$. This plane gives the desired tangent at Q'' .

If PQ'' is not a line of $\text{PG}(3, q)$, then there is a unique point $Q' \in B'$ which projects onto Q'' (see the proof for the cardinality of B'' in Construction 1.1). By the previous proposition there are at least $q + 2$ tangents of B' at Q' , hence there is one that does not intersect r . So Proposition 1.2 applies and B'' is minimal. \square

For the other proposition a particular case of Construction 1.1 is necessary.

Construction 1.6 *Let B be a minimal blocking set in $\text{PG}(2, q)$ and let B' be the cone with base B and vertex $V' \in \text{PG}(3, q) \setminus \text{PG}(2, q)$. Project B' from the point $P (\notin \text{PG}(3, q))$ onto a plane π to obtain B'' .*

Note that the cone B' is always a minimal blocking set in $\text{PG}(3, q)$ if the base of the cone was minimal.

Proposition 1.7 *Let B'' be the blocking set obtained from B using Construction 1.6. Let V' denote the vertex of the cone and B' the cone itself.*

- *Any point U' of the cone B' which is projected from V' onto a point $U \in B$ having at least two tangents, is projected from P onto an essential point U'' of B'' .*
- *If the line r does not pass through V' , then any point U' of B' not belonging to the plane $\langle r, V' \rangle$, is projected from P onto an essential point U'' of B'' . If the plane $\langle r, V' \rangle$ intersects B' in more than $q + 1$ points, then also the points of this plane are projected from P onto essential points.*

- If the line r passes through V' , and the point $U' \in B'$ is such that the plane $\langle r, U' \rangle$ intersects B' in other points than the points of the line $U'V'$, then U' is projected from P onto an essential point U'' of B'' .
- The point R'' is always essential.

Proof of Proposition 1.7: Note first that for a tangent t of B the plane $\psi = \langle t, V' \rangle$ intersects B' in a line through V' , and if $U' \neq V'$ is a point of that line, then the lines of ψ through U' different from $U'V'$ are all tangents of B' . The first assertion follows immediately from Proposition 1.2, since there are more than $q + 1$ tangents through U' . The last assertion was proved in Proposition 1.2. So we need to consider a point whose projection from V' has a unique tangent t . Denote by ψ the plane $\langle t, V' \rangle$. If the line r is not contained in the plane ψ , from Proposition 1.2 it follows that U' is projected from P in an essential point of B'' . Hence the second assertion holds, as r cannot be a line of ψ . The third assertion follows similarly. \square

1.1.2 Examples obtained by projections of cones

Now we use Construction 1.6 to construct various examples of blocking sets in $PG(2, q^2)$. Some of them will have 0, 1 or more Rédei lines, and also their size will be in some cases smaller than $3(q + 1)/2$, close to $3(q + 1)/2$, and much bigger than q regarding its order of magnitude. The notation introduced in the previous section will be used throughout.

Let us repeat that by Construction 1.1, $|B''| = |B'| + 1 - |r \cap B'|$, and $|B'| = q|B| + 1$, since it is a cone.

The advantage of Construction 1.6 is that it is very easy to control the intersection numbers of B'' with respect to lines. What we have to do is to control intersections of B' with planes through P . Since a plane through P intersects $PG(3, q)$ either in a plane through r or in a line, we have to find intersections of B' with lines and with planes containing r . As B' is a cone, a line not passing through the vertex V' of the cone can be projected onto the plane containing the base of the cone, thus the intersection numbers for B' are the same as for B . The only exceptions are the lines through V' , which intersect

B' in either 1 or $q + 1$ points. For planes containing r the situation depends on r . Suppose first that r passes through the vertex V' of the cone. Then it intersects $\text{PG}(2, q)$ in a point W . The planes through r intersect $\text{PG}(2, q)$ in lines through W . When such a line ℓ through W intersects B in s points, then the corresponding plane $\langle \ell, r \rangle$ intersects B' in $sq + 1$ points. This means that the corresponding line of π meets B'' in $sq + 2 - |r \cap B'|$ points.

The situation is similar, if r does not contain V' . Of course, for lines everything remains the same. For planes through r the only difference is that the planes not containing V' meet B' in exactly $|B|$ points. The corresponding line of π meets B'' in $|B| + 1 - |r \cap B'|$ points. The plane $\langle r, V' \rangle$ intersects $\text{PG}(2, q)$ in a line ℓ . If this line ℓ meets B in s points, then again the intersection of $\langle r, V' \rangle$ with B' has size $sq + 1$. The corresponding intersection number for B'' is again $sq + 2 - |r \cap B'|$.

These observations can be used to prove the following corollary, which was (actually, more generally) proved by Polito and Polverino [43].

Corollary 1.8 *Let $q = p^h$, $h > 1$. Then $\text{PG}(2, q^2)$ contains a minimal blocking set of size less than $3(q^2 + 1)/2$, which is not of Rédei type.*

Proof: Start from any non-trivial minimal blocking set B of $\text{PG}(2, q)$, whose size is less than $q + (q + 1)/2$. Choose a line ℓ in $\text{PG}(2, q)$ which is a tangent of B . Let r be a line of $\langle \ell, V' \rangle$, not through V' . If $P \notin \text{PG}(3, q)$ is a point on r , then the line r_P will be just r , and by the discussion before the corollary, the largest intersection number of B'' is $|B|$. Denote this by $q + k$. Comparing the largest intersection number with the cardinality of B'' , and supposing that B'' is of Rédei type, one gets

$$|B|q + 1 = q^2 + |B|, \quad \text{that is} \quad kq + 1 = q + k,$$

which implies $k = 1$, a contradiction. □

In [2] we prove that starting from a linear B , one always gets a linear B'' , that is for small minimal blocking sets no new examples are obtained. On the other hand, one can actually see the existence of non-Rédei type blocking sets which were not mentioned explicitly in [43], although they can be obtained by the general construction for linear blocking sets.

The same construction can also be used for larger minimal blocking sets. For example, one can start from the projective triangle, and obtain various minimal blocking sets. For a description and some properties of the projective triangle, see [33], Chapter 12, [15], p. 138, and [47], Chapter 36, p. 228.

Corollary 1.9 *In $PG(2, q^2)$ there are minimal blocking sets of size $\frac{3}{2}(q+1)q+1$, which are not of Rédei type. There are minimal blocking sets of size $\frac{3}{2}(q+1)q+1-q$, which have exactly one or exactly two Rédei lines.*

Proof: Let B be a projective triangle, B' be a cone with base B and vertex V' as in Construction 1.6. Take r as a line through V' . If r passes through one of the vertices of B , then a blocking set B'' of size $3(q+1)q/2+1-q$ is obtained and it has two Rédei lines (corresponding to the sides containing the vertex). If r intersects $PG(2, q)$ in a point on one of the sides of B which is not a vertex, then the resulting blocking set B'' will have just one Rédei line. The cardinality of B'' is $3(q+1)q/2+1-q$ or $3(q+1)q/2+1$, according as r passes through a point of B or not. Finally, if r intersects $PG(2, q)$ in a point not lying on the sides of the projective triangle, then the cardinality of B'' is $3(q+1)q/2+1$, and it has no Rédei line at all. \square

As we mentioned earlier using a lemma of Lovász and Szőnyi, Gács showed that if a Rédei type blocking set in $PG(2, p^2)$, p prime, has size greater than $3(p^2+1)/2$, then it has at least $1+(3p^2+p)/2$ points. Note that when q is a prime, then the above example shows that this bound is sharp.

Finally, let us mention that one can obtain much larger minimal blocking sets using Proposition 1.7. For example starting from a unital one can obtain minimal blocking sets of size $q^2\sqrt{q}+1$ —something. The potential number of non-essential points is small as the next proposition shows.

Proposition 1.10 *Let B be a unital, B' be the cone over B with vertex V' and B'' be the projection of B' from P . Let B^* be a minimal blocking set contained in B'' .*

1. *If $V' \notin r$ and $|r \cap B'| = 1$, then $q^2\sqrt{q}+1 \leq |B^*| \leq q^2\sqrt{q}+q+1$,*
2. *If $V' \in r$ and $|r \cap B'| = \sqrt{q}+1$, then $|B^*| = |B''| = q^2\sqrt{q}+q-\sqrt{q}+1$,*

3. If $V' \in r$ and $|r \cap B'| = 1$, then $q^2\sqrt{q} + 1 - q\sqrt{q} \leq |B^*| \leq q^2\sqrt{q} + q + 1$,
4. If $V' \in r$ and $|r \cap B'| = q + 1$, then $|B^*| = |B''| = q^2\sqrt{q} + 1$.

Proof: (Sketch.) In Case 1, the non-essential points are among the projections of the points of $(\langle r, V' \rangle \cap B') \setminus r$. Case 2 follows immediately from Proposition 1.7. In Case 3 let Q be a non-essential point of B'' . It has to be a projection of a point of $B' \setminus r$ contained in a plane containing the line r and a tangent line to B through the point $W = r \cap \Pi$, where Π is the plane in which B is contained. Since $|r \cap B'| = 1$, $W \notin B$; so there are $\sqrt{q} + 1$ tangents to B passing through W . Hence the number of non-essential points is at most $q(\sqrt{q} + 1)$. A similar reasoning gives the minimality of B'' in Case 4. \square

1.2 Generalization of the construction

In this section first we give a possible generalization of the results in Section 1.1, that is we construct blocking sets using higher dimensional projective spaces. Then we give an algebraic description of these blocking sets.

1.2.1 The geometric description

Our first aim is to extend Construction 1.1 to higher dimensions. To do this, first we need to extend the idea of projecting from a point to projecting from a subspace.

Definition 1.11 *Let β be an m -dimensional and Q an $(n - m - 1)$ -dimensional subspace in $\text{PG}(n, q)$, $\beta \cap Q = \emptyset$. Take a point S from $\text{PG}(n, q) \setminus Q$. The $(n - m)$ -dimensional subspace $\langle Q, S \rangle$ intersects β in a unique point S' , that will be called the projection of S from Q onto β .*

It turns out that, in general, it is very difficult to repeat the construction of the previous section in higher dimensions. The main difficulty lies in controlling the projection of a subgeometry from a subspace, since in the general case it is not easy to tell which points will project onto the same point. The next lemma shows that in some special cases this can be done easily.

Lemma 1.12 *Let M be an $(h + 1)$ -dimensional subgeometry of order q in $\text{PG}(h + 1, q^h)$. Assume that R is an $(h - 1)$ -dimensional subspace of M and let R^* be the unique $(h - 1)$ -dimensional subspace of $\text{PG}(h + 1, q^h)$ that contains R .*

- (i) *There exists an $(h - 2)$ -dimensional subspace P in R^* such that P does not intersect the subgeometry M .*
- (ii) *An $(h - 1)$ -dimensional subspace containing P , different from R^* intersects the subgeometry M in 0 or 1 point.*
- (iii) *Project the subgeometry M from P onto a plane π ($\pi \cap P = \emptyset$) of $\text{PG}(h + 1, q^h)$ to obtain M' . Then there is a one-to-one correspondence between the points of $M \setminus R$ and their projections. The subspace R projects onto the unique common point R' of R^* and π .*
- (iv) *Let l be a line in π . Then the pre-image of $l \cap M'$ is a hyperplane (of the subgeometry M) containing R or a line (of M) skew to R , according as the point R' was on the line l or not.*

Proof: Note that to block every hyperplane of R^* we need at least $q^h + 1$ points. Now (i) is straightforward, since R has only $\frac{q^h - 1}{q - 1}$ points.

Let L be an $(h - 1)$ -dimensional subspace containing P and different from R^* . Assume to the contrary, that there are two different points, Q and S , lying in $L \cap M$. Since P, Q and S are in L , the line $\langle Q, S \rangle$ intersects P and so S is in the hyperplane $H = \langle Q, R^* \rangle$. The hyperplane H intersects M in a hyperplane h of the subgeometry (since the intersection contains R and the point Q not in R). Considering h only, we get that the subline containing Q and S must intersect R . Hence $R^* \cap \langle Q, S \rangle$ contains a point of R and a point of P , too. This means that the line $\langle Q, S \rangle$ is in R^* and so $L \equiv R^*$, which contradicts our assumption.

Pick a point S' of M' . The pre-image of S' is the intersection of $\langle S', P \rangle$ and M ; hence (iii) follows from (ii).

The points of M that project onto a line l of π are the points of $\langle l, P \rangle \cap M$. Remark that this intersection always contains a line of M . To see this note that over $\text{GF}(q)$, $\langle l, P \rangle$ is an $(h + 1)h$ -dimensional, M is an $(h + 2)$ - and $\text{PG}(h + 1, q^h)$ is an $(h + 2)h$ -dimensional vector space, hence the intersection of $\langle l, P \rangle$ and M

is at least a 2-dimensional vector space over $\text{GF}(q)$. To show (iv) note that if $\langle l, P \rangle \cap M$ contains a point of R^* , then it contains the entire R . \square

Now we are ready to generalize Construction 1.1.

Construction 1.13 *Let B' be a blocking set in $\text{PG}(h+1, q)$ with respect to lines. Embed $\text{PG}(h+1, q)$ as a subgeometry M in $\text{PG}(h+1, q^h)$. Assume that R is an $(h-1)$ -dimensional subspace of M and let R^* be the unique $(h-1)$ -dimensional subspace of $\text{PG}(h+1, q^h)$ that contains R . Choose an $(h-2)$ -dimensional subspace P in R^* , such that P does not intersect the subgeometry M , (for the existence of such a subspace see Lemma 1.12 (i)), and project B' from this subspace onto a plane π of $\text{PG}(h+1, q^h)$, where $\pi \cap P = \emptyset$.*

Then the projection B'' will be a blocking set in $\text{PG}(2, q^h) = \pi$. The cardinality of B'' satisfies

$$|B''| = |B'| + 1 - |R \cap B'|.$$

Proof: Since B' is a blocking set in M with respect to lines, it follows from Lemma 1.12 (iv) that B'' is a planar blocking set. Using (iii) the size of B'' can be calculated. \square

Generalizing Construction 1.1 this way allows us to repeat most of the results of the previous section almost literally.

As before, in some cases the minimality of B'' follows automatically.

Proposition 1.14 *The point $R'' = R^* \cap \pi$ is always an essential point of B'' . Suppose that through a point S' of $B' \setminus R$ there is a tangent line which does not intersect R . Let S'' be the projection of S' onto π . Then S'' is an essential point of B'' . If this condition holds for each point of $B' \setminus R$, then B'' is minimal.*

Proof: Take a point $R' \in R \cap B'$ that is mapped to R'' and any hyperplane through R^* which is not a hyperplane of $\text{PG}(h+1, q^h)$. This hyperplane intersects B' only in the points of $R \cap B'$, hence its intersection with π will be a tangent of B'' at R'' .

Now pick a point S' of $B' \setminus R$. Denote its projection by S'' ($\neq R''$). By assumption there is a tangent $t_{S'}$ of B' through S' which does not intersect R . Consider the line $t'' = \langle t_{S'}, P \rangle \cap \pi$. From Lemma 1.12 (iv) it follows that t'' is a tangent of B'' at S'' , hence S'' is essential. \square

Theorem 1.15 *Let B' be a minimal blocking set of $\text{PG}(h+1, q)$ with respect to lines and suppose that $|B'| \leq 2q^h - 1$. Then the projection B'' of B' (see Construction 1.13) is a minimal blocking set.*

This theorem is a generalization of Theorem 1.3. In Section 1.1 the essential lemma for proving Theorem 1.3 was a 3-dimensional extension of Result 1.4 due to Blokhuis and Brouwer. Now we extend this result to arbitrary dimensions.

Lemma 1.16 *Let K be a blocking set in $\text{PG}(h+1, q)$ with respect to lines. If $|K| = 2q^h + q^{h-1} + \dots + q - s$, then there are at least $s+1$ tangent lines through each essential point of K .*

Proof: Take an essential point $P \in K$ and a tangent ℓ of K at P . Consider the planes $\pi_1, \dots, \pi_{q^{h-1}+q^{h-2}+\dots+1}$ through ℓ . Let $K_i = \pi_i \cap K$. Then K_i is a blocking set in π_i and P is an essential point of it. Let s_i be defined such that $|K_i| = 2q - s_i$. The previous lemma implies that the number of tangents of K_i in π_i at P is at least $s_i + 1$ (this is trivial if $s_i < 0$). Counting points of $\cup K_i$ gives that

$$\sum_{i=1}^{q^{h-1}+q^{h-2}+\dots+1} (2q - s_i) = |K| + q^{h-1} + \dots + q,$$

and the total number of tangents through P is at least $\sum s_i + 1$. Substituting $|K| = 2q^h + q^{h-1} + \dots + q - s$ yields $\sum s_i = s$. \square

Proof of Theorem 1.15: By Construction 1.13 we only have to show that B'' is minimal. Pick a point T'' of B'' . When $\langle T'', P \rangle = R^*$, then T'' is essential by Proposition 1.14. Otherwise, by Lemma 1.12 (iii), there is a unique point T' , which projects onto T'' . By the previous lemma there are at least $q^{h-1} + \dots + q + 2$ tangents of B' at T' , hence there is at least one that does not intersect the subspace R . Applying Proposition 1.14 the result follows immediately. \square

Next we generalize Construction 1.6.

Construction 1.17 *Let B be a minimal blocking set in the plane α of $\text{PG}(h+1, q)$, $h > 1$. Choose an $(h-2)$ -dimensional subspace V' , so that $\alpha \cap V' = \emptyset$. Let B' be the cone with base B and vertex V' . Remark that the cone B' is a blocking set in $\text{PG}(h+1, q)$ with respect to lines, hence using Construction 1.13 we can construct the blocking set B'' of $\text{PG}(2, q^h)$.*

Note that the cone B' is always a minimal blocking set in $\text{PG}(h+1, q)$ if the base of the cone is minimal. Note also that, $|B''| = |B'| + 1 - |R \cap B'|$, and $|B'| = q^{h-1}|B| + \frac{q^{h-1}-1}{q-1}$.

Remark 1.18 *When the size of B is less than $2q$, then $|B'| < 2q^h$ holds; hence by Proposition 1.15, B'' is a minimal blocking set.*

Now we will use the remark above to construct minimal blocking sets of $\text{PG}(2, q^h)$, $h \geq 2$, with cardinality a little bit bigger than the size of a projective triangle.

Let B be a projective triangle of $\text{PG}(2, q)$ and use Construction 1.17 to obtain the cone B' and the blocking set B'' . The cone B' has size $\frac{3}{2}(q+1)q^{h-1} + \frac{q^{h-1}-1}{q-1}$, hence, by Remark 1.18, B'' is minimal. To calculate the size of B'' (see above) we have to determine $|R \cap B'|$. Since R is an $(h-1)$ -dimensional subspace, the intersection of the vertex V' of the cone and R contains an $(h-4)$ -dimensional subspace of the subgeometry M .

First assume that $\dim(R \cap V') = (h-4)$. Then there exists a plane β in R skew to V' and so R intersects B' in a cone with base $\beta \cap B'$ and with vertex $R \cap V'$. Let Q be a point of B . Then $\langle Q, V' \rangle$ intersects β in exactly one point, hence $\beta \cap B'$ is a projective triangle and the size of $R \cap B'$ is $\frac{3}{2}(q+1)q^{h-3} + \frac{q^{h-3}-1}{q-1}$.

Now let $\dim(R \cap V') = (h-3)$. Then there exists a line ℓ in R skew to V' . As before, $R \cap B'$ is a cone with base $\ell \cap B'$ and with vertex $R \cap V'$. A line skew to V' can be projected onto the plane containing the base of the cone B' , hence the intersection numbers for B' are the same as for B . Hence $|R \cap B'| = a_i q^{h-2} + \frac{q^{h-2}-1}{q-1}$, where $a_i = 1, 2, 3$ or $\frac{1}{2}(q+3)$.

Finally, assume that $\dim(R \cap V') = (h-2)$, hence $V' \subset R$. Then there are only two possibilities, R is either fully contained in B' or $R \cap B' = V'$. Hence $|R \cap B'| = b_i q^{h-1} + \frac{q^{h-1}-1}{q-1}$, where $b_i = 0$ or 1 .

As in Corollary 1.9 in some of the examples above one can control the existence of Rédei lines.

Corollary 1.19 *There are minimal blocking sets in $\text{PG}(2, q^h)$ of size $\frac{3}{2}(q+1)q^{h-1} + 1 - q^{h-1}$, which have exactly one or two Rédei lines. There are minimal blocking sets of size $\frac{3}{2}(q+1)q^{h-1} + 1$, which are not of Rédei type. Furthermore, there exist minimal blocking sets with cardinality $\frac{3}{2}(q+1)q^{h-1} + 1 - \frac{1}{2}(q^{h-1} + q^{h-2})$, $\frac{3}{2}(q+1)q^{h-1} + 1 - 2q^{h-2}$, $\frac{3}{2}(q+1)q^{h-1} + 1 - q^{h-2}$ and $\frac{3}{2}(q+1)q^{h-1} + 1 - \frac{1}{2}(q^{h-2} + q^{h-3})$.*

When $|B| \geq 2q$, it is not easy to control the minimality of B'' . Though there is a very special case, where it can be done without difficulties.

Construction 1.20 *Suppose that B' is the cone obtained by Construction 1.17. Assume that Q is a point of the plane α in Construction 1.17. Let R be the subspace spanned by Q and V' , and again use Construction 1.13 to obtain the blocking set B'' of $\text{PG}(2, q^h)$. This construction will be called the generalized cone construction.*

Proposition 1.21 *Let B be a minimal blocking set of $\text{PG}(2, q)$ and assume that Q is a point of $\text{PG}(2, q)$, such that through each point of $B \setminus Q$ there passes at least one tangent line of B , not passing through Q . Then the blocking set B'' obtained by the generalized cone construction is minimal.*

Proof: By Proposition 1.14, it is enough to show that through each point of $B' \setminus R$ there passes at least one tangent line skew to R .

Let S' be a point of $B' \setminus R$ and denote the projection of S' from V' onto $\text{PG}(2, q)$ by S . According to our assumption there is a tangent line t_S of B that passes through S and that is skew to Q . Hence the hyperplane $\langle V', t_S \rangle$ of the subgeometry M intersects the cone B' in $\langle V', S \rangle$ and it intersects R in V' , only. Therefore any line of the hyperplane $\langle V', t_S \rangle$ through S' not contained in $\langle V', S \rangle$ is a tangent line of B' skew to R . \square

Corollary 1.22 *Let B be a minimal blocking set of $\text{PG}(2, q)$ and assume that Q is a point of B . Then the blocking set B'' obtained by the generalized cone construction is minimal.*

Proof: From the previous proposition it follows that the points of $B'' \setminus Q$ are essential, since a tangent line of $B \setminus Q$ cannot pass through Q . Proposition 1.14 proves the essentiality of Q . \square

Now we will show how the observations above can be used to construct larger blocking sets. For planes of square order the following theorem was proved by Hirschfeld and Szőnyi.

Result 1.23 (Hirschfeld, Szőnyi [34]) *For every λ with $1/4 < \lambda \leq 1/2$, there are constants c_1 and c_2 such that in $\text{PG}(2, q)$, q square, there are minimal blocking sets of size k with $c_1 q^{1+\lambda} \leq k \leq c_2 q^{1+\lambda}$ for $q > q_0(\lambda)$.*

Combining this with the general cone construction, for planes of fourth power order we get a similar result, but for $1/8 < \lambda \leq 1/2$. The process can be iterated: for planes of eighth power order one can get minimal blocking sets of size q^λ , where $1/16 < \lambda \leq 1/2$, and so on. As an illustration, the next theorem, that is the generalization of Proposition 1.10 can be proved. It is stated for planes of order q^h , not only for planes of order q^2 .

Proposition 1.24 *Let B be a unital of the plane $\text{PG}(2, q)$, q square. Embed $\text{PG}(2, q)$ into $\text{PG}(h + 1, q)$ and choose an $(h - 2)$ -dimensional subspace V' according to Construction 1.17. As in that construction, let B' be the cone over B with vertex V' and let B'' be the projection of B' from P . Let B^* be a minimal blocking set contained in B'' .*

- 1 *If $V' \subset R$ and $R \cap B = \emptyset$, then $q^h \sqrt{q} + 1 - q^{h-1} \sqrt{q} \leq |B^*| \leq q^h \sqrt{q} + q^{h-1} + 1$.*
- 2 *If $V' \subset R$ and $R \cap B \neq \emptyset$, then $|B^*| = |B''| = q^h \sqrt{q} + 1$. □*

Case 2. of this Proposition shows how the generalized cone construction works for large blocking sets. According to Corollary 1.22 the subspace V' and the point Q can always be chosen in such a way that B'' is a minimal blocking set. The size of B'' is $q^{h-1}(|B| - 1) + 1$. When $|B| \sim q^{1+\alpha}$, then $|B''| \sim (q^h)^{1+\alpha/h}$. For $h = 1$, this means that the exponents can roughly be halved, as remarked after Theorem 1.23. When $|B| \sim cq$, then $|B''| \sim cq^h$, so this does not give anything new about the spectrum.

1.2.2 The algebraic description

In this section we give an algebraic description of the blocking sets obtained by the generalized cone construction.

First we write up the coordinates of the minimal blocking set obtained by the generalized cone construction. The next remark shows that in some cases it is enough to give the coordinates of the affine part of the blocking set, since it uniquely determines the entire blocking set.

Remark 1.25 *Assume that B is a minimal blocking set in $\text{PG}(2, q)$. Choose a line ℓ of $\text{PG}(2, q)$, so that ℓ is a secant line of B or if ℓ is tangent to B , then*

there exists another line tangent to B through $B \cap \ell$. Delete the points of $B \cap \ell$. Note that the unique way to extend $B \setminus \ell$ to a minimal blocking set is to add the points of ℓ to B , through that there passes 0-secant of $B \setminus \ell$ (different from ℓ), and so we get back B .

Assume that B'' is a blocking set obtained by the generalized cone construction and suppose also that the line ℓ is a secant line of B'' . Our aim is to coordinatize $B'' \setminus \ell$.

Without loss of generality we may assume that $\alpha \subset \pi$. We use the usual homogeneous coordinate representation of $\text{PG}(2, q^h)$. With a suitable linear transformation we can achieve the following:

$$\begin{aligned} M &= \{(Z_0, \dots, Z_{h+1}) : Z_i \in \text{GF}(q)\}; \\ \pi &= \{(X_0, X_1, X_2, 0, \dots, 0) : X_i \in \text{GF}(q^h)\}; \\ \alpha &= \pi \cap M = \{(Z_0, Z_1, Z_2, 0, \dots, 0) : Z_i \in \text{GF}(q)\}; \\ V' &= \{(0, 0, 0, Z_3, \dots, Z_{h+1}) : Z_i \in \text{GF}(q)\}; \\ Q &= (0, 1, 0, 0, \dots, 0). \\ \ell &= \{(X_0, X_1, 0, 0, \dots, 0) : X_i \in \text{GF}(q^h)\}; \end{aligned}$$

$X_2 = 0$ will be the hyperplane at infinity. Note that since the hyperplane $X_2 = 0$ is mapped to the ideal line of π (that is $\ell = \pi \cap \{X_2 = 0\}$), we are allowed to consider only the affine part of B (that is $B \setminus \ell$).

Finally write $\{(x_k, y_k, 1, 0, \dots, 0) : k\}$ for the affine part of B and let \bar{B} denote the affine part of the cone B' .

These conditions imply the following:

$$\begin{aligned} \bar{B} &= \{(x_k, y_k, 1, z_1, \dots, z_{h-1}) : (x_k, y_k, 1, 0, \dots, 0) \in B, z_i \in \text{GF}(q)\}. \\ R &= \{(0, Z_1, 0, Z_3, \dots, Z_{h+1}) : Z_i \in \text{GF}(q)\}; \\ R^* &= \{(0, X_1, 0, X_3, \dots, X_{h+1}) : X_i \in \text{GF}(q^h)\}. \end{aligned}$$

One can choose a base for P of the following form:

$\{(0, b_1, 0, 1, 0, \dots, 0), (0, b_2, 0, 0, 1, 0, \dots, 0), \dots, (0, b_{h-1}, 0, 0, \dots, 0, 1)\}$. To see this, take an arbitrary generating point set of P that lies in $R^* \setminus V^*$, where V^* is the unique $(h-2)$ -dimensional subspace of R^* that contains V' . Any linear combination of the generating points is still in the subspace P , hence using Gauss elimination one gets the required form. Note that $P \cap M = \emptyset$ implies $b_i \neq 0$.

An easy calculation shows that projecting \bar{B} from P onto π , we get

$\{(x_k, y_k + \sum_{i=1}^{h-1} \lambda_i b_i, 1, 0, \dots, 0) : (x_k, y_k, 1, 0, \dots, 0) \in B, \lambda_i \in \text{GF}(q)\}$. Let $I = \{\sum_{i=1}^{h-1} \lambda_i b_i : \lambda_i \in \text{GF}(q)\}$. Hence the affine part of B'' is :

$$B'' \setminus \ell = \{(x_k, y_k + i, 1, 0, \dots, 0) : (x_k, y_k, 1, 0, \dots, 0) \in B, i \in I\} \quad (1.1)$$

We show that I is a direct complement of $\text{GF}(q)$ in the additive group of $\text{GF}(q^h)$. Here the direct complement means a vector subspace I (over $\text{GF}(q)$) of $\text{GF}(q^h)$, where $|I| = q^{h-1}$ and $I \cap \text{GF}(q) = \{0\}$. One sees immediately, that I is a $\text{GF}(q)$ -linear additive subgroup in $\text{GF}(q^h)$. To prove $|I| = q^{h-1}$ and $I \cap \text{GF}(q) = 0$, suppose $\sum z_i b_i \in I \cap \text{GF}(q)$. This means that the point $(0, \sum z_i b_i, 0, z_1, z_2, \dots, z_{h-1})$ is in $P \cap M$, implying $z_1 = \dots = z_{h-1} = 0$.

The next construction shows that I in (1.1) can be replaced by an arbitrary direct complement of $\text{GF}(q)$ in $(\text{GF}(q^h), +)$.

Construction 1.26 *Let B be a minimal blocking set in $\text{PG}(2, q)$ and let $\ell_\infty = [0, 0, 1]$ be the line at infinity. For sake of simplicity, suppose that ℓ_∞ is secant to B . Choose a coordinate system, such that $(0, 1, 0) \in B$. The points of $B \setminus \ell_\infty$ can be written in the form of $(x_k, y_k, 1)$. Assume that $h > 1$ is an integer and I is a direct complement of $\text{GF}(q)$ in the additive group of $\text{GF}(q^h)$. Let B^* be the following subset of $\text{AG}(2, q^h)$:*

$$B^* := \{(x_k, y_k + i, 1) : (x_k, y_k, 1) \in B \setminus \ell_\infty, i \in I\}.$$

To B^ add the points of the line $[0, 0, 1] \subset \text{PG}(2, q^h)$, through that there passes an affine 0-secant of B^* , and denote the resulting point set by \bar{B} . Then \bar{B} is a minimal blocking set. \square*

Proof: We show that $\bar{B} \setminus \ell$ can be obtained by the generalized cone construction starting from the minimal blocking set B , choosing Q to be the point $(0, 1, 0)$ and at the end deleting the points that were projected onto ℓ . It is easy to show that I must be $\text{GF}(q)$ -linear, hence there are elements $b_1, \dots, b_{h-1} \in \text{GF}(q^h)$ such that every element of I can be written as $\sum_{i=1}^{h-1} z_i b_i$, where $z_i \in \text{GF}(q)$. Now we coordinatize $\text{PG}(h+1, q^h)$ as we did after Remark 1.25, we build the ‘same’ cone B' on B in order to get back the same setting as we had there. Choosing P to be the subspace generated by the points $(0, b_1, 0, 1, 0, \dots, 0), (0, b_2, 0, 0, 1, 0, \dots, 0), \dots, (0, b_{h-1}, 0, 0, \dots, 0, 1)$ we are done.

Let B'' be the blocking set above obtained by the generalized cone construction. By Corollary 1.22, B'' is minimal. Now Remark 1.25 yields that B'' and \bar{B} coincide, hence the result follows. \square

From the arguments above we have the following consequence.

Corollary 1.27 *The minimal blocking sets obtained by the generalized cone construction are exactly the minimal blocking sets constructed by Construction 1.26.* \square

1.3 Another application

In this section we assume that q is even. A *hyperoval* in $\text{PG}(2, q)$ is a set of $q+2$ points intersecting each line in 0 or 2 points. A $(q+t, t)$ -arc of type $(0, 2, t)$ is a set of $q+t$ points in $\text{PG}(2, q)$ meeting every line in 0, 2 or t points. It can be considered as a generalization of hyperovals or as a small example for a set without tangents. We also suppose $t > 2$ (the $t = 2$ case is just the class of hyperovals).

Korchmáros and Mazzocca constructed an infinite series of $(q+t, t)$ -arcs of type $(0, 2, t)$, whenever the field $\text{GF}(\frac{q}{t})$ is a subfield of $\text{GF}(q)$.

Construction 1.28 (Korchmáros, Mazzocca [38]) *Assume that q is even. Suppose g is an o -polynomial over $\text{GF}(q)$, that is the point set $\mathcal{H} = \{(g(x), x, 1) : x \in \text{GF}(q)\} \cup \{(1, 0, 0), (0, 1, 0)\}$ forms a hyperoval in $\text{PG}(2, q)$ and let T be the following point set of $\text{AG}(2, q^h)$, $h > 1$:*

$$T := \{(g(\text{Tr}(a)), a, 1) : a \in \text{GF}(q)\},$$

where $\text{Tr}(a) = a + a^q + a^{q^2} + \dots + a^{q^{h-1}}$.

Then T together with the q^{h-1} directions not determined by T forms a $(q^h + q^{h-1}, q^{h-1})$ -arc of type $(0, 2, q^{h-1})$ in $\text{PG}(2, q^h)$.

In [1] we give a more general construction for $(q+t, t)$ -arcs of type $(0, 2, t)$ including the Korchmáros-Mazzocca arcs by using the idea of the construction in the previous section. This idea can be repeated for arbitrary point sets.

Construction 1.29 [1] *Choose a plane α in $\text{PG}(h+1, q)$, where $h > 1$. Let \mathcal{D} be a point set in α . Choose an $(h-2)$ -dimensional subspace V in $\text{PG}(h+1, q) \setminus \alpha$. Construct the cone \mathcal{C} with vertex V and base \mathcal{D} . Now embed $\text{PG}(h+1, q)$ into $\text{PG}(h+1, q^h)$ as a subgeometry. Let Q be a point of α and let R be the $(h-1)$ -dimensional subspace in $\text{PG}(h+1, q)$ spanned by V and Q . Denote by R^* the unique $(h-1)$ -dimensional subspace in $\text{PG}(h+1, q^h)$ that contains R . Assume that P is an $(h-2)$ -dimensional subspace in $R^* \setminus \text{PG}(h+1, q)$. (For the existence of such a subspace, see Proposition 1.12 (i).) Project $\mathcal{C} \setminus R$ from P onto an arbitrary plane π of $\text{PG}(h+1, q^h)$ to obtain \mathcal{D}' . \square*

As before the advantage of this construction is that knowing the intersection numbers of \mathcal{D} with respect to lines, it is very easy to control the intersection multiplicities of \mathcal{D}' with lines, so the next construction can be proved easily.

Construction 1.30 [1] *Let $q = 2^r$ and let the point set \mathcal{D} in Construction 1.29 be a hyperoval of the plane α or a $(q+t, t)$ -arc of type $(0, 2, t)$. Now use Construction 1.29 to obtain the point set \mathcal{D}' of the plane $\pi \cong \text{PG}(2, q^h)$.*

- (1) *When \mathcal{D} is a hyperoval and Q (in Construction 1.29) is a point of the hyperoval, then the point set \mathcal{D}' is a $(q^h + q^{h-1}, q^{h-1})$ -arc of type $(0, 2, q^{h-1})$.*
- (2) *When \mathcal{D} is a hyperoval and Q is a point of $\alpha \setminus \mathcal{D}$, then the point set \mathcal{D}' is a $(q^h + 2q^{h-1}, 2q^{h-1})$ -arc of type $(0, 2, 2q^{h-1})$.*
- (3) *When \mathcal{D} is a $(q+t, t)$ -arc of type $(0, 2, t)$ and Q is the t -nucleus of \mathcal{D} , then the point set \mathcal{D}' is a $(q^h + tq^{h-1}, tq^{h-1})$ -arc of type $(0, 2, tq^{h-1})$. \square*

As in the previous section this geometric construction can be described algebraically.

Construction 1.31 [1] *Let I be a direct complement of $\text{GF}(q)$ in the additive group of $\text{GF}(q^h)$, $h > 1$. Let $\mathcal{H} = \{(x_k, y_k, 1) : x_k, y_k \in \text{GF}(q)\} \subseteq \text{PG}(2, q)$ be the affine part of a hyperoval or of a $(q+t, t)$ -arc of type $(0, 2, t)$. Construct the following point set of $\text{AG}(2, q^h)$:*

$$\mathcal{J} := \{(x_k, y_k + i, 1) : (x_k, y_k, 1) \in \mathcal{H}, i \in I\}.$$

- (A) When \mathcal{H} is a hyperoval and $(0, 1, 0) \in \mathcal{H}$, then \mathcal{J} can be uniquely extended to a $(q^h + q^{h-1}, q^{h-1})$ -arc of type $(0, 2, q^{h-1})$ in $\text{PG}(2, q^h)$.
- (B) When \mathcal{H} is a hyperoval and $(0, 1, 0) \notin \mathcal{H}$, then \mathcal{J} can be uniquely extended to a $(q^h + 2q^{h-1}, 2q^{h-1})$ -arc of type $(0, 2, 2q^{h-1})$ in $\text{PG}(2, q^h)$.
- (C) When \mathcal{H} is a $(q + t, t)$ -arc of type $(0, 2, t)$ and $(0, 1, 0)$ is the t -nucleus of \mathcal{H} , then \mathcal{J} can be uniquely extended to a $(q^h + tq^{h-1}, tq^{h-1})$ -arc of type $(0, 2, tq^{h-1})$ in $\text{PG}(2, q^h)$. \square

Corollary 1.32 [1] *The classes of arcs obtained by Construction 1.30 (1), (2) and (3) are exactly the classes of arcs of Construction 1.31 (1), (2) and (3), respectively.* \square

This algebraic description shows that Construction 1.30 is the generalization of the Korchmáros-Mazzocca arcs: among new examples, (1) contains the arcs in question, while the arcs coming from (2) are all new examples. (3) only gives new examples if we start with an arc not arising from our construction.

Chapter 2

Blocking sets in higher dimensions

The main result of this chapter is that we generalize the 1 modulo p result of Szőnyi (see Result 0.7) for blocking sets in $PG(n, q)$ with respect to k -dimensional subspaces. This chapter appeared as [4].

For proving this result, algebraic curves associated to the blocking sets were used. A natural way of the generalization would be to associate hypersurfaces to higher dimensional blocking sets, so that it has the same properties as in the planar case and so one could “copy” the proof. Until now it has not been done. For a while we were also trying this approach, but though it is very straightforward how one should associate a “good” hypersurface we could not repeat the proof in higher dimensions. The difficulty seems to lie in the fact that it is not easy to control the intersection numbers of two hypersurfaces, while in the planar case we have the Bézout theorem.

Instead of an algebraic approach, we used a purely geometric approach to generalize the 1 mod p result. Let B be a blocking set of $PG(2k, q)$, $k > 1$, with respect to k -dimensional subspaces. Consider a $(k - 1)$ -spread W of $H_\infty = PG(2k - 1)$. It defines a plane π^W . Let B' be the point set of π^W , whose affine points are the points of $B \setminus H_\infty$ and whose ideal points are the elements of W that intersect B . We will call B' *the image of B in π^W* . Note that B' is a blocking set of π^W . When our blocking set B is a cone over a blocking set in a subspace, the 1 modulo p result for π^W yields that k -dimensional subspaces intersect B in 1 modulo p points. Using this, we first prove the result for 1-

blocking sets (Proposition 2.5). The result for k -blocking sets (Theorem 2.7) follows by embedding $\text{PG}(n, q)$ in $\text{PG}(n, q^{n-k})$ as a subgeometry. This result can also be used to characterize certain non-trivial blocking sets in higher dimensions (Theorems 2.21, 2.26).

2.1 Intersection with subspaces

First of all we recall how spreads define translation planes. Take a $(k-1)$ -spread S of $\text{PG}(2k-1, q)$, that is a partition of $\text{PG}(2k-1, q)$ into disjoint $(k-1)$ -dimensional subspaces. Embed $\text{PG}(2k-1, q) = H_\infty$ in $\text{PG}(2k, q)$ as a hyperplane. Then an affine translation plane π^S can be defined as follows.

1. The *points* of π^S are the points of $\text{PG}(2k, q) \setminus H_\infty$.
2. The *lines* of π^S are the k -dimensional subspaces of $\text{PG}(2k, q)$ which meet H_∞ in an element of S .

This affine plane can be extended to a projective plane with the elements of the spread as ideal points. The *regular* $(k-1)$ -spreads are the $(k-1)$ -spreads that define the plane $\text{PG}(2, q^k)$ in this way, see [10]. For more details see [33], Section 4.1, or [39]. An important property of $(k-1)$ -spreads of $\text{PG}(2k-1, q)$ is that they are also dual spreads, that is every hyperplane contains exactly one element of the $(k-1)$ -spread.

A collineation of $\text{PG}(2k-1, q)$ can be prescribed on $2k$ projectively independent points. Hence given any two not intersecting $(k-1)$ -dimensional subspaces w_1 and w_2 of $\text{PG}(2k-1, q)$ and a $(k-1)$ -spread, one can find a collineation, so that w_1 and w_2 will be elements of the image of this given $(k-1)$ -spread.

Remark 2.1 *Any set of two non-intersecting $(k-1)$ -dimensional subspaces of $\text{PG}(2k-1, q)$ can be extended to a regular $(k-1)$ -spread of $(k-1)$ -dimensional subspaces.*

Our first aim is to say something about the possible intersection numbers of hyperplanes and minimal blocking sets with respect to hyperplanes. For $n = 2$ the following theorem completes our task.

Theorem 2.2 [52] *A minimal blocking set in $\text{PG}(2, q)$, $q = p^h$, of size less than $\frac{3}{2}(q+1)$ intersects every line in $1 \pmod p$ points. \square*

Throughout this chapter we will rather use the following corollary of Theorem 2.2.

Corollary 2.3 *Let B be a blocking set in $\text{PG}(2, q)$, $q = p^h$, p prime, of size less than $\frac{3}{2}(q + 1)$. Let ℓ be a line of $\text{PG}(2, q)$, so that each point of B on the line ℓ is essential to B . Then ℓ intersects B in $1 \pmod p$ points.*

Proof: Delete the non-essential points one by one until a minimal blocking set is obtained. The result follows from Theorem 2.2 as none of the points of the line ℓ will be removed. \square

To be able to use the idea mentioned at the beginning of this chapter, we will need the following construction to obtain a blocking set with respect to k -dimensional subspaces from a given blocking set with respect to hyperplanes.

Construction 2.4 *Let B be a blocking set of $\text{PG}(n, q)$ with respect to hyperplanes. Embed $\text{PG}(n, q)$ in $\text{PG}(m, q)$ as a subspace. Choose an arbitrary $(m - n - 1)$ -dimensional subspace P , not intersecting $\text{PG}(n, q)$, and construct the cone C with base B and vertex P . Then $C \cap \text{PG}(n, q) = B$. The cone C is a blocking set in $\text{PG}(m, q)$ with respect to $(n - 1)$ -dimensional subspaces. Furthermore, if B is minimal, then C is minimal as well.*

Proof: First we show that any $(n - 1)$ -dimensional subspace S of $\text{PG}(m, q)$ intersects C . If S intersects P , then there is nothing to prove, otherwise S and P generate a hyperplane H of $\text{PG}(m, q)$. A hyperplane intersects $\text{PG}(n, q)$ in an $(n - 1)$ -dimensional subspace. Hence H must contain a point Q of B , as B blocks every hyperplane of $\text{PG}(n, q)$. Since the $(m - n)$ -dimensional subspace $\langle P, Q \rangle$ is contained in the hyperplane H , it intersects S , and so S intersects the cone C . If C contained a point x of $\text{PG}(n, q) \setminus B$, then there would be a point $b \in B$, for which $\langle b, P \rangle \cap \text{PG}(n, q)$ contains x ; this is impossible since $\langle b, P \rangle \cap \text{PG}(n, q)$ has dimension 0.

Now assume that B is minimal. For the minimality of C , we only have to show that any point R of $C \setminus B$ is essential. Let R' be the projection of R from P onto B . Since B is minimal, there is an $(n - 1)$ -dimensional subspace $S_{R'}$ in $\text{PG}(n, q)$ through R' , that is tangent to B and so tangent to C . Hence any $(n - 1)$ -dimensional subspace in $\langle S_{R'}, P \rangle$ through R not intersecting P proves that R is essential. \square

Proposition 2.5 *A minimal blocking set in $\text{PG}(n, q)$, $q = p^h$, with respect to hyperplanes and of size less than $\frac{3}{2}(q + 1)$ intersects every hyperplane in 1 mod p points.*

Proof: The proof goes by induction on n . For $n = 2$ it is Theorem 2.2. Now assume that it is true for $(n - 1)$. We wish to show that an arbitrary hyperplane H intersects the minimal blocking set B in 1 mod p points. Embed $\text{PG}(n, q)$ in $\text{PG}(2n - 2, q)$ as a subspace and construct the cone C , as in Construction 2.4. Now $m = 2n - 2$, so the vertex P of the cone C will be an $(n - 3)$ -dimensional subspace and $H \cap C = H \cap B$, by Construction 2.4.

By the induction hypothesis we may assume that B is not in H , which means that there is an $(n - 2)$ -dimensional subspace $L \subset H$, that does not intersect B . Let H^* be an $(n - 1)$ -dimensional subspace of $\text{PG}(n, q)$ through L , so that there is only one point Q of B on H^* . Such a subspace exists, otherwise counting the number of points of B on the hyperplanes of $\text{PG}(n, q)$ through L , we would get at least $2(q + 1)$ points; which contradicts our assumption made on the size of B . By Remark 2.1, there exists a regular $(n - 2)$ -spread W of the hyperplane $\langle H^*, P \rangle$, so that it contains $\langle P, Q \rangle$ and L . Let π^W denote the plane defined by the $(n - 2)$ -spread W and C' denote the image of C in π^W .

Since $|B|$ is an integer $|B| < \frac{3}{2}(q + 1)$ means that $|B| \leq \frac{3}{2}q + 1$. Now, $\langle P, Q \rangle$ is the only element of the $(n - 2)$ -spread that intersects the cone C , hence $|C'| \leq \frac{3}{2}q^{(n-1)} + 1$.

Note that on the plane π^W , the subspace H will correspond to a line h , so we only have to show that the points of $h \cap C'$ are all essential to C' , as Corollary 2.3 would then finish the proof. To see this take a point R of $H \cap B$. Since B is minimal, there exists an $(n - 1)$ -dimensional subspace H_R through R , that is in $\text{PG}(n, q)$ and tangent to B . The hyperplane $\langle H_R, P \rangle$ intersects $\langle H^*, P \rangle$ in a $(2n - 4)$ -dimensional subspace, hence it contains exactly one element w of W . We show that $\langle w, R \rangle \cap C = R$ and hence $\langle w, R \rangle$ corresponds to a tangent line of C' in the plane π^W , and so R corresponds to an essential point of C' . If P does not intersect $\langle w, R \rangle$, then the projection from P is a 1 - 1 correspondence between the the points of $C \cap \langle w, R \rangle$ and $H_R \cap C$ and hence the result follows. Otherwise, let S denote a point of $P \cap \langle w, R \rangle$ (note that $S \neq R$). The line RS is contained in the cone C and it intersects w as well. Hence w intersects the cone. From above, this means that $w = \langle P, Q \rangle$, so Q is in $\langle P, H_R \rangle \cap \text{PG}(n, q)$

and so it lies in H_R ; which is a contradiction. \square

Now we extend the result of Proposition 2.5 to arbitrary subspaces.

Proposition 2.6 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to hyperplanes, $q = p^h$, $p > 2$ prime, and assume that $|B| < \frac{3}{2}(q + 1)$. Then any subspace that intersects B , intersects it in $1 \pmod p$ points.*

Proof: For $(n - 1)$ -dimensional subspaces this is Proposition 2.5. First we prove that the statement is true for $(n - 2)$ -dimensional subspaces. On the contrary, suppose that an $(n - 2)$ -dimensional subspace Z intersects B , but not in $1 \pmod p$ points.

If $|B \cap Z| \not\equiv 0 \pmod p$, then since a hyperplane intersects B in $1 \pmod p$ points, each hyperplane through Z must contain at least two points of $B \setminus Z$. Counting the number of points of $B \setminus Z$ on the hyperplanes through Z , gives that B has at least $2(q + 1)$ points, which is a contradiction.

When $0 \neq |B \cap Z| \equiv 0 \pmod p$, the earlier reasoning works if each hyperplane through Z contains at least two points of $B \setminus Z$. Assume that there is a hyperplane H through Z containing only one point P of $B \setminus Z$. Let Q be a point in $Z \cap B$. Since B is minimal, there exists a hyperplane H_Q through Q that is tangent to B . The $(n - 2)$ -dimensional subspace $\langle H_Q \cap Z, P \rangle$ intersects B in exactly two points. Since $p > 2$, this is a contradiction by the proof in the previous case.

Finally, assume that the theorem is true for any k -dimensional subspace, $(2 \leq) k \leq n - 2$. We prove that it is true for $(k - 1)$ -dimensional subspaces too. Take any $(k - 1)$ -dimensional subspace U . If it intersects B , but not in $1 \pmod p$ points, then as before each subspace through U contains at least one point of $B \setminus U$. Since through a $(k - 1)$ -dimensional subspace ($k \leq n - 2$) there are more than q^2 k -dimensional subspaces, counting the number of points of $B \setminus U$ on the k -dimensional subspaces through U , we get a contradiction. \square

Theorem 2.7 *Let B be a minimal blocking set B of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $q = p^h$, $p > 2$ prime, and assume that $|B| < \frac{3}{2}(q^{n-k} + 1)$. Then any subspace that intersects B , intersects it in $1 \pmod p$ points.*

Proof: Case $k = n - 1$ is proved in Proposition 2.6. Now let $k < n - 1$. Embed $\text{PG}(n, q)$ in $\text{PG}(n, q^{n-k})$ as a subgeometry. Consider $\text{PG}(n, q^{n-k})$ as

an $(n + 1)(n - k)$ -dimensional vectorspace V over $\text{GF}(q)$. A hyperplane of $\text{PG}(n, q^{n-k})$ is an $n(n - k)$ -dimensional and $\text{PG}(n, q)$ is an $(n + 1)$ -dimensional vectorspace in V . Hence a hyperplane of $\text{PG}(n, q^{n-k})$ contains at least a k dimensional subspace of $\text{PG}(n, q)$, therefore B is a blocking set of $\text{PG}(n, q^{n-k})$ with respect to hyperplanes.

To show that B is minimal, take a point P of B . Since B was minimal in $\text{PG}(n, q)$, there exists a k -dimensional subspace K of $\text{PG}(n, q)$ that is tangent to B . Any hyperplane of $\text{PG}(n, q^{n-k})$ through K that intersects $\text{PG}(n, q)$ in K proves that P is essential.

To prove the theorem, take an arbitrary subspace of $\text{PG}(n, q)$. This subspace can be extended to a subspace of $\text{PG}(n, q^{n-k})$ of the same dimension. Hence the result follows from Proposition 2.6. \square

2.2 Applications

In this section we will show how Theorem 2.7 can be used to obtain more information on blocking sets in an n -dimensional projective space.

2.2.1 An observation

Lemma 2.8 *Let B be a blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $q = p^h$, p prime, and suppose that $|B| \leq 2q^{n-k}$. Assume that each k -dimensional subspace of $\text{PG}(n, q)$ intersects B in $1 \pmod p$ points. Then B is minimal.*

Proof: Suppose on the contrary that B is not minimal. Let P be a non-essential point of B . This means that each k -dimensional subspace through P contains at least one point of $B \setminus P$. Since every k -dimensional subspace intersects B in $1 \pmod p$ points, each k -dimensional subspace through P must contain at least two points of $B \setminus P$. If there exists a $(k - 1)$ -dimensional subspace M through P , so that $M \cap B = P$, then by counting the number of points of B on the k -dimensional subspaces through M , we get more than $2q^{n-k}$ points; which is a contradiction.

Now we show that the above mentioned subspace M exists. When $k = 1$ we take M to be the point P itself. If $k > 2$, then since there are more than q^{n-1}

lines through P and since each of these lines contain no point or at least two points of $B \setminus P$, there must be a line l through P , so that it does not intersect $B \setminus P$. The same argument shows that if there is a $(t-1)$ -dimensional subspace (where $t < k$) through P with no point of $B \setminus P$ on it, then one can find a t -dimensional one (through P) with the same property. Consequently, there is a $(k-1)$ -dimensional subspace through P , that does not intersect $B \setminus P$. \square

Next, we give a corollary of the previous lemma.

Corollary 2.9 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $q = p^h$, $p > 2$ prime. Assume that $|B| \leq \frac{3}{2}(q^{n-k} + 1)$. Choose a t -dimensional subspace P , not intersecting B , and an $(n-t-1)$ -dimensional subspace H , not intersecting P . Project B from P onto H and denote the projection by B' . Then B' is a minimal blocking set of H with respect to $(k-t-1)$ -dimensional subspaces.*

Proof: Take any $(k-t-1)$ -dimensional subspace α of H and consider the k -dimensional subspace generated by P and α . Since B is a blocking set with respect to k -dimensional subspaces, $\langle \alpha, P \rangle$ contains a point Q of B , and so the intersection point of $\langle P, Q \rangle$ and α is a point of B' in α , whence B' is a blocking set in H with respect to $(k-t-1)$ -dimensional subspaces.

Now we prove that B' is minimal. A point R' of B' is the projection of the points of $\langle P, R' \rangle \cap B$, hence by Theorem 2.7 R' is the projection of $1 \pmod p$ points. So an arbitrary $(k-t-1)$ -dimensional subspace β of H intersects B' mod p the same number of points as $\langle P, \beta \rangle$ intersects B , and this is $1 \pmod p$ again by Theorem 2.7. So by Lemma 2.8 B' is minimal. \square

2.2.2 Spectra of blocking sets

Note that Theorem 2.2 says that the possible values for the size of a minimal blocking set in $\text{PG}(2, q)$, $q = p^h$, p prime, are those that are equal to $1 \pmod p$. (To see this, one has to count the points of B on the lines through a given point.) For simplicity, we introduce the following notation.

Notation 2.10 *Let $S(q)$ be the set of the possible sizes of minimal blocking sets in $\text{PG}(2, q)$ with cardinality less than $\frac{3}{2}(q+1)$.*

Our goal is to show that the possible sizes of minimal blocking sets in $\text{PG}(n, q)$ with respect to k -dimensional subspaces and with cardinality less than $\frac{3}{2}(q^{n-k} + 1)$ depend on the possible sizes of minimal blocking sets of projective planes.

First we handle the case $k = n - 1$; to do that the following lemma is needed.

Lemma 2.11 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to hyperplanes, $n > 2$, $q = p^h$, p prime.*

1. *Suppose that $|B| < \sqrt{2}q$. Then there exists a point Q in $\text{PG}(n, q)$, so that Q does not lie on any of the secants of B .*
2. *Assume that $p > 2$ and assume also that $|B| < \frac{3}{2}(q + 1)$. Then there exists a point Q in $\text{PG}(n, q)$, so that Q does not lie on any of the secants of B .*

Proof: (1) comes from simple counting. There are at most $\binom{|B|}{2}$ secants of B , each contains at most $(q - 1)$ points not from B . Therefore there are less than q^3 such points in $\text{PG}(n, q) \setminus B$, that lie on a secant of B .

(2) can be proved by repeating the same argument, taking into account Theorem 2.7. When $p > 2$, we know that each secant of B contains at least $(3 + 1)$ points. Hence there are only at most $\binom{|B|}{2} / \binom{4}{2}$ secants of B and so, as before, we are done. \square

Now we give two propositions that determine the possible sizes of minimal blocking sets in $\text{PG}(n, q)$ with respect to hyperplanes in terms of the possible sizes of minimal blocking sets in projective planes of different order. The first one extends Heim's result mentioned in Section for small blocking sets.

Proposition 2.12 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to hyperplanes, $q = p^h$, p prime. If $p = 2$ let $|B| < \sqrt{2}q$, otherwise let $|B| < \frac{3}{2}(q + 1)$. Then $|B| \in S(q)$.*

Proof: The proof is again by induction on n . For $n = 2$, we just get the definition of $S(q)$ back. Suppose that the proposition is true for $n - 1$. Let Q be a point in $\text{PG}(n, q) \setminus B$, not lying on any of the secants of B . Then by Corollary 2.9 projecting B from Q onto a hyperplane H , not through Q , we obtain a minimal blocking set B' of H with respect to hyperplanes (of H).

Since each line through Q contains at most 1 point of B , $|B| = |B'|$; hence the result follows from the induction hypothesis. \square

Proposition 2.13 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to hyperplanes, $q = p^h$, $p > 2$ prime. Suppose that $|B| < \frac{3}{2}(q + 1)$. Then $((|B| - 1)q^{n-2} + 1) \in S(q^{n-1})$.*

Proof: To prove the proposition we just have to recall the proof of Proposition 2.5 again. By Construction 2.4, the cone C is a minimal blocking set of $\text{PG}(2n - 2, q)$ with respect to $(n - 1)$ -dimensional subspaces. So from Theorem 2.7 every $(n - 1)$ -dimensional subspace intersects C in $1 \pmod p$ points. Note that since the way of constructing the cone C , we can determine the size of the blocking set C' on the plane π^W . The points of $\langle P, Q \rangle$ correspond to the same point, while the rest of the points of C correspond to different points, so $|C'| = (|B| - 1)q^{n-2} + 1$. Note also that π^W was isomorphic to $\text{PG}(2, q^{n-1})$ and the lines of π^W correspond to $(n - 1)$ -dimensional subspaces of $\text{PG}(2n - 2, q)$. So from above, each line of π^W intersects C' in $1 \pmod p$ points; hence by Lemma 2.8 C' is a minimal blocking set on the plane π^W . \square

Now let B be a blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces. As in the proof of Theorem 2.7, by embedding $\text{PG}(n, q)$ into $\text{PG}(n, q^{n-k})$ B becomes a 1-blocking set of $\text{PG}(n, q^{n-k})$. So, as before, we can extend the results of the two propositions above.

Corollary 2.14 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $q = p^h$, p prime. If $p = 2$ let $|B| < \sqrt{2}q^{n-k}$, otherwise let $|B| < \frac{3}{2}(q^{n-k} + 1)$. Then*

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

In the planar case it was proved that the possible sizes for a minimal blocking set of $\text{PG}(2, q)$ with cardinality less than $\frac{3}{2}(q + 1)$ (i.e. the elements of $S(q)$) should lie in some intervals.

Notation 2.15 *Let $l(q, e)$ ($u(q, e)$) denote the biggest (smallest) integer so that for any minimal blocking set B of $\text{PG}(2, q)$, $q = p^h$, p prime, and of size $l(q, e) \leq$*

$|B| \leq u(q, e)$, e is the largest integer such that each line intersects B in 1 mod p^e points.

Szönyi proved (see Result 0.7) that for a fixed q , these intervals are disjoint unless $p^e = 2, 4, 8$, and for $q = p^h$, $e \leq h/2$. It was also mentioned in [52] that for $p^e \neq 2, 4, 8$ Blokhuis' lower bound is valid, that is $q+1+p^e \lceil (q/p^e + 1)/(p^e + 1) \rceil \leq l(q, e)$. The best bound for $u(q, e)$ is due to Polverino [44].

Theorem 2.16 For $p^e \neq 2, 4, 8$

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

This means that asymptotically

$$|B| \leq q + \frac{q}{p^e} + \frac{q}{p^{2e}} + 2\frac{q}{p^{3e}} \cdots.$$

□

Note also, that $|B| \leq u(q, e)$ means that the blocking set B lies in an interval belonging to e' , where $e' \geq e$, and so B intersects every line in 1 mod $p^{e'}$ points; whence B intersects every line in 1 mod p^e points.

Now we generalize the previous theorems for blocking sets with respect to hyperplanes.

Proposition 2.17 Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to hyperplanes, $q = p^h$, $p > 2$ prime. Assume that $|B| < \frac{3}{2}(q + 1)$. Let e be the integer, for which $l(q^{n-1}, e) \leq (|B| - 1)q^{n-2} + 1 \leq u(q^{n-1}, e)$. Then each subspace that intersects B , intersects it in 1 mod p^e points.

Proof: The same reasoning as in the proof of Proposition 2.5 proves that an arbitrary hyperplane H intersects B in 1 mod p^e points. To see this we just have to note that the blocking set C' in π^W (in the proof of Proposition 2.5) is minimal and has size of $(|B| - 1)q^{n-2} + 1$ (see the proof of Lemma 2.13). Hence each line of the plane π^W intersects C' in 1 mod p^e points.

To prove that any subspace, of dimension less than $(n - 1)$, that intersects B , intersects it in 1 mod p^e points, we just have to copy the proof of Proposition 2.6 again by writing p^e instead of p . □

Again by embedding $\text{PG}(n, q)$ into $\text{PG}(n, q^{n-k})$, from a blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces we obtain a blocking set of $\text{PG}(n, q^{n-k})$ with respect to hyperplanes. Hence we can generalize the above proposition.

Corollary 2.18 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $q = p^h$, $p > 2$ prime. Assume that $|B| < \frac{3}{2}(q^{n-k} + 1)$. Let e be the integer, for which $l((q^{n-k})^{n-1}, e) \leq (|B| - 1)(q^{n-k})^{n-2} + 1 \leq u((q^{n-k})^{n-1}, e)$. Then each subspace that intersects B , intersects it in $1 \pmod{p^e}$ points. \square*

2.2.3 An attempt to characterize blocking sets

In this subsection we attempt to characterize blocking sets of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $n > 2$, $q = p^h$, p prime. First let us see a few examples for blocking sets.

A k -dimensional subspace intersects a t -dimensional subspace T at least in a $(k + t - n)$ -dimensional subspace (now let $t \geq n - k$). Hence a blocking set of T with respect to its $(k + t - n)$ -dimensional subspaces is obviously a blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces. So the interesting blocking sets in $\text{PG}(n, q)$ are those, that are not contained in a smaller dimensional subspace of $\text{PG}(n, q)$. Here we follow [49] and call these blocking sets *non-degenerate*. The next remark shows that the converse is also true.

Remark 2.19 *If B is a blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces and if B is contained in a t -dimensional subspace T , then B is a blocking set of T with respect to its $(k + t - n)$ -dimensional subspaces. Furthermore, if B is a minimal blocking set in $\text{PG}(n, q)$, then B is minimal in T as well. \square*

The next lemma provides us with a series of examples.

Lemma 2.20 *A subgeometry S of dimension $h(n - k)$ and of order p is a minimal blocking set with respect to k -dimensional subspaces in $\text{PG}(n, p^h)$.*

Proof: $\text{PG}(n, p^h)$ can be identified with an $((n+1)h)$ -dimensional vector space V over $\text{GF}(p)$ in a natural way. Then a k -dimensional subspace in $\text{PG}(n, p^h)$ is a

$((k+1)h)$ -dimensional subspace in V , and the subgeometry S is an $(h(n-k)+1)$ -dimensional linear subspace in V . Since $(h(n-k)+1) + (k+1)h > (n+1)h$, S blocks every k -dimensional subspaces in $\text{PG}(n, p^h)$. The minimality of S comes from an easy counting argument. \square

Some special cases were already studied in [7]. Here, when h is even and $p > 3$, the blocking sets with respect to hyperplanes of cardinality at most the size of the second smallest minimal blocking set in $\text{PG}(2, q)$ are characterized as planar blocking sets. When $h = 3s$, $p \geq 5$, $q > 5$, the blocking sets with respect to hyperplanes and of cardinality at most the size of the second smallest minimal blocking sets of $\text{PG}(2, q)$ are characterized as planar blocking sets or as a subgeometry $\text{PG}(3, p^s)$.

Theorem 2.21 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $q = p^h$ and $p > 2$ prime. Suppose that $|B| < \frac{3}{2}(q^{n-k} + 1)$ and $h(n-k) \leq n$. Assume that B is not contained in an $(h(n-k) - 1)$ -dimensional subspace of $\text{PG}(n, q)$, then B is projectively equivalent to $\text{PG}(h(n-k), p)$.*

Before proving Theorem 2.21, let us have a closer look at it. It says, that for $h(n-k) < n$ the only small (that is $|B| < \frac{3}{2}(q^{n-k} + 1)$) minimal blocking sets of $\text{PG}(n, q)$ with respect to k -dimensional subspaces are the degenerate ones. When $h(n-k) = n$, the only non-trivial minimal blocking set with respect to k -dimensional subspaces is the subgeometry of order p .

Note that this theorem also implies that the blocking sets in question are *linear*. In [49] it is proved that every small $(n-k)$ -blocking set of Rédei type (i.e. a blocking set with q^{n-k} affine points) is linear, and also their shape is described. The proof of Storme and Sziklai uses the result of [17], where the case $n = 2, k = 1$ is established.

Proof of Theorem 2.21: First we prove that every secant of B contains $(p+1)$ points. On the contrary, suppose that there is a secant ℓ , so that $|\ell \cap B| \neq p+1$. Then by Theorem 2.7 ℓ contains at least $(2p+1)$ points of B . Since B is not contained in an $(h(n-k) - 1)$ -dimensional subspace, there is a point P_1 of $B \setminus \ell$. The lines connecting a point of $\ell \cap B$ and P_1 by Theorem 2.7 should also contain at least $p+1$ points of B . Hence the plane $\langle P_1, \ell \rangle$ contains at least $2p^2 + p + 1$

points of B . Now, repeating the above arguments first we find a point P_2 in $B \setminus \langle P, \ell \rangle$, then a point P_3 in $B \setminus \langle P_3, \langle P_2, \ell \rangle \rangle \dots$ and so on. Hence B must have at least $2p^{h(n-k)} + p^{h(n-k)-1} + \dots + p + 1$ points, which is a contradiction.

Next we show, that if a plane contains three non-collinear points of B , then it contains exactly $p^2 + p + 1$ points of it. From above, we know that such a plane must contain at least $p^2 + p + 1$ points. Assume that it contains more than that, that is at least $p^2 + 2p + 1$ points. As before, this implies that $|B| \geq p^{h(n-k)} + 2p^{h(n-k)-1} + \dots + p + 1$, but this contradicts the upper bound on $|B|$ coming from Theorem 2.16 by taking $e = 1$. Hence if α is a plane of $\text{PG}(n, q)$ containing three non-collinear points of B , then $\alpha \cap B$ is a subplane of order p .

Every plane of $\text{PG}(n, q)$ intersects B in 1 point or in $(p+1)$ collinear points or in a subplane of order p , so Veblen's theorem (see [13], p.806) implies that B is a projective subgeometry of order p . The result follows, since such a subgeometry is a minimal blocking set by Lemma 2.20. \square

In particular when $h = 1$, $h = 2$ and $h = 3$, the theorem above implies the following corollaries.

Corollary 2.22 *A non-trivial minimal blocking set of $\text{PG}(n, p)$ with respect to k -dimensional subspaces, $p > 2$ prime, has size at least $\frac{3}{2}(p^{n-k} + 1)$. \square*

Corollary 2.23 *A non-trivial minimal blocking set of $\text{PG}(n, p^2)$ with respect to hyperplanes and of size less than $\frac{3}{2}(p^2 + 1)$, $p > 2$ prime, is a Baer subplane. \square*

Corollary 2.24 *A non-trivial minimal blocking set of $\text{PG}(n, p^3)$ with respect to hyperplanes and of size less than $\frac{3}{2}(p^3 + 1)$, $p > 2$ prime, is a planar blocking set or a subgeometry of dimension three and order p . \square*

Since the blocking sets of $\text{PG}(2, p^3)$ are characterized by Polverino (see Result 0.8 (3)), the corollary above gives a full description of the small minimal blocking sets of $\text{PG}(n, p^3)$ with respect to hyperplanes.

Now, we try to say something about the possible non-degenerate blocking sets when $h(n-k) > n$. Similarly to Lemma 2.20 one easily proves the following.

Lemma 2.25 *Assume that e is a divisor of h . Then a subgeometry S of dimension $\frac{h}{e}(n-k)$ and of order p^e is a minimal blocking set with respect to k -dimensional subspaces in $\text{PG}(n, p^h)$. \square*

When our blocking set is such that each secant of it contains $1 \bmod p^e$ points, then similarly to Theorem 2.21 the following theorem can be proved.

Theorem 2.26 *Let B be a minimal blocking set of $\text{PG}(n, q)$ with respect to k -dimensional subspaces, $q = p^h$ and $p > 2$ prime. Assume that e is an integer, $1 \leq e \leq \frac{h}{2}$, and $\frac{h}{e}(n - k) \leq n$. Suppose also that $(|B| - 1)(q^{n-k})^{n-2} + 1 \leq u((q^{n-k})^{n-1}, e)$ (where $u((q^{n-k})^{n-1}, e)$ is defined in Notation 2.15). Then B is contained in an $(\lceil \frac{h}{e}(n - k) \rceil - 1)$ -dimensional subspace of $\text{PG}(n, q)$ or B is projectively equivalent to $\text{PG}(\frac{h}{e}(n - k), p^e)$. \square*

Proof: Note that by Corollary 2.18 and by the remark after Theorem 2.16 every subspace that intersects B , intersects it in $1 \bmod p^e$ points.

Firstly, suppose that e is not a divisor of h . Starting from a secant line of B , similarly as in the proof of Theorem 2.21, one can prove that if B is not contained in an $(\lceil \frac{h}{e}(n - k) \rceil - 1)$ -dimensional subspace, then B has at least $p^{e \lceil \frac{h}{e}(n-k) \rceil} + p^{e \lceil \frac{h}{e}(n-k) \rceil - 1} + \dots + p^e + 1$ points. Since, now $e \lceil \frac{h}{e}(n - k) \rceil > h(n - k)$, this means that B would have too many points, hence B must lie in a subspace of dimension $(\lceil \frac{h}{e}(n - k) \rceil - 1)$.

Secondly, assume that e is a divisor of h . Then as before one may prove that each secant of B contains $1 \bmod p^e$ points and each plane intersects B in 1 point or in $(p^e + 1)$ collinear points or in a subplane of order p^e . Hence again by Veblen's theorem we get that B is projectively equivalent to $\text{PG}(\frac{h}{e}(n - k), p^e)$. \square

Chapter 3

Algebraic background

This chapter summarizes the algebraic background and methods used in the next two chapters.

The Rédei polynomial

Let ℓ be the line at infinity in $\text{PG}(2, q)$ and let $U = \{(a_i, b_i, 1) : i = 1, \dots, n\}$ be a set of points in $\text{PG}(2, q) \setminus \ell$. Then the *Rédei polynomial* of U is the following polynomial in three variables:

$$H(X, Y, Z) = \prod_{i=1}^n (X + a_i Y - b_i Z) = \sum_{j=0}^n h_j(Y, Z) X^{n-j}.$$

Note that $h_j(Y, Z)$ is a homogeneous polynomial of degree j . It is not difficult to see that this polynomial encodes the intersection numbers of U and the affine lines.

Lemma 3.1 *For a fixed $(z, y, 0) \in \ell$, the element $x \in \text{GF}(q)$ is an r -fold root of $H(X, y, z)$ if and only if the line with equation $zY = yX + xZ$ intersects U in exactly r points. \square*

3.1 A bound on the degree of the g.c.d.

In this section, first we recall Szőnyi's results from [53], Section 3. There a condition was given which guarantees that the greatest common divisor of two given polynomials has a prescribed degree.

Result 3.2 (Szőnyi [53]) *Let $u(X) = u_0X^n + u_1X^{n-1} + \dots$ ($u_0 \neq 0$) be a polynomial of degree n and $v(X) = v_0X^{n-1} + v_1X^{n-2} + \dots$ be a polynomial of degree at most $n - 1$. Denote by R_k the following $2k \times 2k$ matrix:*

$$R_k = \begin{pmatrix} u_0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ u_1 & u_0 & 0 & \dots & 0 & -v_0 & 0 & \dots & 0 \\ u_2 & u_1 & u_0 & \dots & 0 & -v_1 & -v_0 & \dots & 0 \\ \vdots & & \vdots & & & & & \vdots & \\ u_{k-1} & u_{k-2} & u_{k-3} & \dots & u_0 & -v_{k-2} & -v_{k-3} & \dots & -v_0 & 0 \\ u_k & u_{k-1} & u_{k-2} & \dots & u_1 & -v_{k-1} & -v_{k-2} & \dots & & -v_0 \\ \vdots & & \vdots & & & & & \vdots & & \\ \vdots & & \vdots & & & & & \vdots & & \\ u_{2k-1} & \dots & & \dots & u_k & -v_{2k-2} & -v_{2k-3} & \dots & & -v_{k-1} \end{pmatrix}$$

where u_j , $j > n$ and v_i , $i > n - 1$ supposed to be zero.

If the degree of the greatest common divisor of u and v is $n - k$, then the determinant of R_k is non-zero. When the degree of the greatest common divisor is greater than $n - k$, then $\det R_k = 0$.

Note that $\det R_k$ plays a very similar role to the resultant. Actually, deleting the first row and the first column of R_k we get back a submatrix of the resultant, for $n = k$ it is the resultant of the two polynomials. The advantage now is that when the greatest common divisor of the two polynomials is large, then the matrix R_k is small.

Proof: Let $r(x)$ be the greatest common divisor of u and v . Denote by \bar{c} the quotient u/r and let $\bar{a} = v/r$. Since $\deg(r) = n - k$, we can suppose that $\bar{c}(x) = x^k + \bar{c}_1x^{k-1} + \dots$ and $\bar{a}(x) = \bar{a}_0x^{k-1} + \dots$. For these polynomials we have $r(x) = u(x)/\bar{c}(x) = v(x)/\bar{a}(x)$. In other words, this means that:

$$u(x)\bar{a}(x) - v(x)\bar{c}(x) = 0, \quad (3.1)$$

and this polynomial equation can be interpreted as a system of linear equations for the coefficients.

More precisely, if we compute the coefficient of x^{n+k-1} in $u(x)\bar{a}(x) - v(x)\bar{c}(x)$, then it is just $u_0\bar{a}_0 - v_0 \cdot 1$, and since this is zero, we get the first equation $u_0\bar{a}_0 = v_0$. Now the coefficient of x^{n+k-2} is $u_1\bar{a}_0 + u_0\bar{a}_1 - v_1 \cdot 1 - v_0\bar{c}_1$. Since this is zero, we get the equation $u_1\bar{a}_0 + u_0\bar{a}_1 - v_0\bar{c}_1 = v_1$. Continuing in this way, we

obtain a system of linear equations. The last equation comes from comparing the coefficients of x^{n-k} .

$$\underline{R}_k(\bar{a}_0, \dots, \bar{a}_{k-1}, \bar{c}_1, \dots, \bar{c}_k)^T = (v_0, \dots, v_{2k-1})^T \quad (3.2)$$

Note that the right-hand side is non-zero when the greatest common divisor has degree at least $n-k$, since $v_0 = \dots = v_{k-1} = 0$ would imply that the degree of r is at most $n-k-1$.

It is important to note that the solutions of the system of linear equations correspond to solutions of the polynomial equation, if we know in advance that the greatest common divisor has degree at least $n-k$. Indeed, if $\bar{a}_0, \dots, \bar{a}_{k-1}, \bar{c}_1, \dots, \bar{c}_k$ is a solution of our system of linear equations, then the polynomials $\bar{c}(x) = x^k + \bar{c}_1 x^{k-1} + \dots$ and $\bar{a}(x) = \bar{a}_0 x^{k-1} + \dots$ will have the property that $u(x)\bar{a}(x) - v(x)\bar{c}(x)$ has degree less than $n-k$. Since this polynomial is divisible by $r(x)$, it must be identically zero. Now the polynomial equation (and hence the system of linear equations) has a unique solution if r has degree exactly $n-k$. To see this, first observe that $u/r = \bar{c}$ is a solution of the polynomial equation of degree exactly k , so we can normalize it; this means that there is at least one solution. Suppose that there are two: \bar{a}', \bar{a}'' and \bar{c}', \bar{c}'' . Then from $u\bar{a}' - v\bar{c}' = 0$ and $u\bar{a}'' - v\bar{c}'' = 0$ we get $u(\bar{a}' - \bar{a}'') - v(\bar{c}' - \bar{c}'') = 0$. Now the degree of $\bar{c}' - \bar{c}''$ is less than k ; so we get a contradiction after dividing by r . Therefore the solution is unique if $\deg(r) = n-k$, and it can be obtained by Cramer's rule. If the degree of r is strictly bigger than $n-k$, then the above determinant is zero, since the polynomial equation $u(x)\bar{a}(x) - v(x)\bar{c}(x) = 0$ cannot have a unique solution. Indeed, we can determine \bar{a}, \bar{c} with smaller degree and then multiply it by anything. \square

In the applications we will suppose that the coefficient u_j is a homogeneous polynomial in two variables (Y and Z) which satisfies $\deg(u_j) = tj$ for a fixed $t \geq 1$ or it is the zero polynomial, furthermore, we will also suppose that the same holds for v_j .

Similarly as in Result 3.2, we construct the matrix $R_k(Y, Z)$. Replace the m -th column of $R_k(Y, Z)$ by $(v_0(Y, Z), \dots, v_{2k-1}(Y, Z))^T$ to obtain $R_{k,m}(Y, Z)$. (We imitate the idea of Cramer's rule.) Let us introduce the polynomial $a^{(k)}(X, Y, Z) = \sum_{i=0}^{k-1} a_i(Y, Z)X^{k-1-i}$, where $a_i(Y, Z) = \det R_{k,(i+1)}(Y, Z)$ and let $c^{(k)}(X, Y, Z) = \sum_{i=0}^k c_i(Y, Z)X^{k-i}$ be the polynomial such that $c_0(Y, Z) =$

$\det R_k(Y, Z)$ and $c_i(Y, Z) = \det R_{k, (k+i)}(Y, Z)$, when $i > 0$. Note that if for the fixed values $Y = y$ and $Z = z$, the degree of the greatest common divisor of $u(X, y, z)$ and $v(X, y, z)$ is $n - k$ exactly (so $\det R_k(y, z) \neq 0$), then it follows from the previous arguments that $a^{(k)}(X, y, z) = \frac{v(X, y, z)}{\gcd(u(X, y, z), v(X, y, z))} \det R_k(y, z)$ and $c^{(k)}(X, y, z) = \frac{u(X, y, z)}{\gcd(u(X, y, z), v(X, y, z))} \det R_k(y, z)$.

Now for the polynomials $a^{(k)}$ and $c^{(k)}$ a similar proposition to [53, Proposition 3.2] (where u_j and v_j were polynomials in one variable) holds.

Proposition 3.3 *Suppose that the polynomials $u(X, Y, Z) = \sum_{i=0}^n u_i(Y, Z)X^{n-i}$ and $v(X, Y, Z) = \sum_{i=0}^{n-1} v_i(Y, Z)X^{n-1-i}$, satisfy $\deg u_i(Y, Z) = ti$ or $u_i = 0$ and $\deg v_i(Y, Z) = ti$ or $v_i = 0$, for a fixed $t \geq 1$, and $u_0 \neq 0$. Then the determinant of $R_k(Y, Z)$ in Result 3.2 is a homogeneous polynomial (in Y and Z) of degree $tk(k-1)$ or it is 0. Furthermore, all the subdeterminants of $R_k(Y, Z)$ are homogenous polynomials.*

The coefficient of X^{k-i} in the polynomial $c^{(k)}(X, Y, Z)$ and the coefficient of X^{k-1-i} in the polynomial $a^{(k)}(X, Y, Z)$ are homogeneous polynomials (in Y and in Z) of degree $tk(k-1) + ti$ or they are 0.

Proof: To calculate the degree of the determinant of $R_k(Y, Z)$, observe that the degree of the (l, m) -th entry ($l, m = 1, \dots, 2k$) is $t(l-m)$ (or it is 0) if we are in the left-hand side, and it is $t(l-m+k-1)$ if we are in the right-hand side of $R_k(Y, Z)$ (or again that entry is 0). So each term in the expression of the determinant has degree exactly $tk(k-1)$. Similarly, one can prove easily that all the subdeterminants of $R_k(Y, Z)$ are homogenous polynomials. If we put $(v_0(Y, Z), \dots, v_{2k-1}(Y, Z))^T$ in place of the m -th column of $R_k(Y, Z)$, then the degree will be bigger than that of $R_k(Y, Z)$ by $t(m-1)$ or $t(m-k)$ according as m is in the left or right part of the matrix, from which the second part of the result follows. \square

3.2 An important observation

From Result 3.2 it follows that if for the fixed value $Y = y$ and $Z = z$ the degree of the greatest common divisor of $u(X, y, z)$ and $v(X, y, z)$ is bigger than $n - k$, then the determinant of $R_k(y, z)$ is 0. Since $\det R_k(Y, Z)$ is a homogeneous polynomial, this means that $(zY - yZ)$ is a factor of $R_k(Y, Z)$.

As Proposition 3.5 shows a bit more is true, but to prove that the next lemma is needed.

Lemma 3.4 (Sziklai) *Let $M(Y, Z)$ be an $m \times m$ matrix with entries of polynomials depending on Y and Z . Assume that for the fixed values y and z , $(zY - yZ)^r$ divides all $(m - 1) \times (m - 1)$ subdeterminants of $M(Y, Z)$, then $(zY - yZ)^{r+1}$ is a factor of $\det M(Y, Z)$.*

Proof: The lemma is true when $\det M(Y, Z) = 0$, hence we may assume that it is not the zero polynomial. Let $M^*(Y, Z)$ be the matrix obtained by replacing each element m_{ij} of $M(Y, Z)$ by $(-1)^{i+j}$ times the corresponding $(m-1) \times (m-1)$ subdeterminant of $M(Y, Z)$. Note that $(M^*(Y, Z))^T M(Y, Z) = (\det M(Y, Z))I$, where I is the $m \times m$ identity matrix; hence $\det M^*(Y, Z) = (\det M(Y, Z))^{m-1}$. By assumption the elements of $M^*(Y, Z)$ are divisible by $(zY - yZ)^r$, therefore $(zY - yZ)^{rm}$ divides $\det M^*(Y, Z) = (\det M(Y, Z))^{m-1}$ and so the lemma follows. \square

Proposition 3.5 *Assume that the polynomials $u(X, Y, Z) = \sum_{i=0}^n u_i(Y, Z)X^{n-i}$ and $v(X, Y, Z) = \sum_{i=0}^{n-1} v_i(Y, Z)X^{n-1-i}$ are such that $u_i(Y, Z)$ and $v_i(Y, Z)$ are homogeneous polynomials, furthermore, suppose that $\deg u_i(Y, Z) = ti$ or $u_i = 0$ and $\deg v_i(Y, Z) = ti$ or $v_i = 0$, for a fixed $t \geq 1$, and $u_0 \neq 0$. For $Y = y$ and $Z = z$, let $n - k'$ be the degree of the greatest common divisor of $u(X, y, z)$ and $v(X, y, z)$. Assume that k is a non-negative integer such that $n - k' \geq n - k$ and construct the matrix $R_k(Y, Z)$ of Result 3.2. Then $(zY - yZ)^{k-k'}$ divides $\det R_k(Y, Z)$.*

Proof: As before, we want to determine the coefficients of the polynomials $\bar{a}(X)$ and $\bar{c}(X)$, for that $u(X, y, z)\bar{a}(X) - v(X, y, z)\bar{c}(X) = 0$, $\deg \bar{c} = k$, (the coefficient of X^k is normalized to 1 again) and $\deg \bar{a} \leq k - 1$ hold. Again the previous equation can be interpreted as a system of linear equations with matrix $R_k(y, z)$, for the coefficients of \bar{a} and \bar{c} .

Since the degree of the greatest common divisor of the polynomials $u(X, y, z)$ and $v(X, y, z)$ is $n - k' (\geq n - k)$, the polynomials \bar{a} and \bar{c} are the products $\bar{a}(X) = \frac{v(X, y, z)}{\gcd(u(X, y, z), v(X, y, z))} (X^{k-k'} + d_1 X^{k-k'-1} + \dots + d_{k-k'})$ and $\bar{c}(X) = \frac{u(X, y, z)}{\gcd(u(X, y, z), v(X, y, z))} (X^{k-k'} + d_1 X^{k-k'-1} + \dots + d_{k-k'})$, where d_i can be chosen arbitrary. This means that the $2k \times 2k$ matrix $R_k(y, z)$ has rank $2k - (k - k') = k + k'$.

Hence the $(k + k' + 1) \times (k + k' + 1)$ subdeterminants of $R_k(y, z)$ are all 0. By Proposition 3.3, all the subdeterminants of $R_k(Y, Z)$ are homogeneous polynomials, hence $(zY - yZ)$ divides all $(k + k' + 1) \times (k + k' + 1)$ subdeterminants of $R_k(Y, Z)$. The result follows by applying Lemma 3.4 $(k - k')$ times. \square

As we will see the above proposition will be crucial in the next two chapters.

Chapter 4

(k, p^e) -arcs

4.1 Introduction

Recall that a (k, n) -arc in a projective plane is a set of k points such that each line intersects it in at most n points. It is *complete* if it cannot be extended to a $(k + 1, n)$ -arc.

Considering (k, n) -arcs Barlotti [12] showed that for $1 < n < q + 1$, we have $k \leq qn - q + n$ and equality can only hold when n divides q . Arcs of size $qn - q + n$ are called *maximal*. In the Desarguesian projective plane of order q , Denniston [27] constructed maximal arcs for every divisor of q , when q is even. Ball, Blokhuis and Mazzocca [11] proved that for q odd, there is no maximal arc.

There are several improvements on Barlotti's bound, when n is not a divisor of q . Lunelli and Sce [41] showed that $k \leq (n - 1)q + n - 3$ and if q is large enough compared to n , then $k \leq (n - 1)q + 8n/13$.

Let \mathcal{K} be an arbitrary $(qn - q + n - \varepsilon, n)$ -arc in $\text{PG}(2, q)$. When n divides q , a natural question is whether \mathcal{K} is incomplete if ε is small enough, that is whether it can be completed to a maximal arc. For $\varepsilon = 1$, this was shown by Thas [55]. Ball, Blokhuis [10] showed it for $\varepsilon < n/2$ when $q/n > 3$, for $\varepsilon < 0.476n$ when $n = q/3$ and for $\varepsilon < 0.381n$ when $n = q/2$. This result was improved by Hadnagy and Szőnyi [30], namely they proved it for $\varepsilon \leq 2n/3$, if q/n is large enough. In the previous two results the bound on ε depended on n , while in the next theorem this is not the case.

Result 4.1 (Szőnyi [53]) *Assume that \mathcal{K} is a $(qp - q + p - \varepsilon, p)$ -arc in $\text{PG}(2, q)$, $q = p^h$, p prime. Suppose also that $\varepsilon \leq \frac{1}{2}\sqrt[4]{q}$. Then \mathcal{K} can be embedded in a maximal arc.*

For large $n = p$, the results of Ball-Blokhuis and Hadnagy-Szőnyi turn out to be better, while for small p , Result 4.1 is stronger.

When $n = 2$, (k, n) -arcs are simply called k -arcs and maximal arcs are called hyperovals. In this case Segre [48] showed that a $(q + 2 - \varepsilon)$ -arc, $\varepsilon \leq \sqrt{q}$, can be extended to a hyperoval. When $4 < q$ is a square, this result is sharp, since then there are complete $(q + 1 - \sqrt{q})$ -arcs, see Boros and Szőnyi [21] and Fischer, Hirschfeld and Thas [28] and Kestenband [37].

In this chapter we improve on Result 4.1, that is we prove the following theorem.

Theorem 4.16 *Assume that \mathcal{K} is a $(qp^e - q + p^e - \varepsilon, p^e)$ -arc in $\text{PG}(2, q)$, $q = p^h$, p prime. Suppose also that $\varepsilon \leq \frac{1}{4}\sqrt{q}$ and $p^e \leq \frac{1}{2}\sqrt{q}$. Then \mathcal{K} can be embedded in a maximal arc.*

The improvement on the result comes from studying [53]. One of the main observations is that Proposition 3.5 and so Proposition 4.4 can be used to improve on Result 4.1. Szőnyi's method is similar to Segre's one in the sense that he associates an algebraic envelope to the (k, p) -arc. It turns out that a similar envelope can be associated to the (k, p^e) -arc, when $e > 1$. This envelope is reintroduced in Section 3. In [53] it is proved that the above envelope factors into linear components, i.e. line pencils, and the arc in question can be completed by adding the vertices of these line pencils. Unfortunately, when $\varepsilon > \sqrt[4]{q}/2$, we cannot use the idea of factorizing this envelope, instead we show that certain linear components must be factors of it and this will be enough to complete the proof.

In general, probably \sqrt{q} is not the right order of magnitude for ε , except for the case $p^e = 2$. As we saw earlier, in this case Segre showed that ε can be as big as \sqrt{q} and this is sharp. Note that the sharpness of Segre's result shows that if ε does not depend on p^e , the best order of magnitude of ε we can get is \sqrt{q} . In Section 4.3 we give a new proof of Segre's result.

4.2 The main result

From now on assume that \mathcal{K} is a $(qp^e - q + p^e - \varepsilon, p^e)$ -arc in $\text{PG}(2, q)$, $q = p^h$, p prime. Assume also that $0 < \varepsilon \leq \sqrt{q}/4$.

The aim is to prove that \mathcal{K} can be embedded in a $(qp^e - q + p^e, p^e)$ -arc.

By Thas [55], the $(qp^e - q + p^e - 1, p^e)$ -arcs are incomplete, hence we can assume that $q \geq 64$. Note that when $p^e > \sqrt{q}/2$, then the embeddability follows by the results of Ball-Blokhuis [10] and by Hadnagy-Szőnyi [30], hence we may suppose that $p^e \leq \sqrt{q}/2$.

A line intersecting \mathcal{K} in j points is called a j -secant. Denote by i the greatest integer for that each line intersects \mathcal{K} in $0 \pmod{p^i}$ point. Counting the points of \mathcal{K} on the lines through a point, we get that $p^i | \varepsilon$. Since \mathcal{K} is not maximal, $p^i < p^e$ and so $p^i \leq \sqrt{q}/4$.

Lines intersecting \mathcal{K} in not $0 \pmod{p^{i+1}}$ points will be called *irregular*. (Note that such a line contains less than p^e points but more than 0 point.) The *index* of a point is the number of irregular lines passing through it. Let l be the line at infinity, then the *affine index* of a point P on l is the number of affine irregular lines passing through P . (Hence when l is irregular then the affine index of P is one less than its index, otherwise the affine index and the index are equal.) Note that through a point of \mathcal{K} there pass at most ε/p^i irregular lines. Denote by δ the total number of irregular lines of \mathcal{K} . The next lemma gives an upper bound on δ .

At the beginning of this section we follow the proof of Result 4.1.

Lemma 4.2 *The number δ , of lines containing at least 1 but less than p^e points of \mathcal{K} , is*

- at least $(q + 1 - p^e)$;
- at most $\frac{p^e - 1}{p^e - p^i} \frac{\varepsilon}{p^i} (q + 1)$, that is less than $\frac{2\varepsilon}{p^i} (q + 1)$, furthermore, when $p^i = 1$, it is at most $\varepsilon(q + 1)$.

Proof: To see that there are at least $q + 1 - p^e$ irregular lines, take a line ℓ , so that $\mathcal{K} \setminus \ell$ is not divisible by p^{i+1} . (When \mathcal{K} is not divisible by p^{i+1} , then ℓ can be a p^e -secant, otherwise it can be an irregular line.) Then through each point of $\mathcal{K} \setminus \ell$ there pass at least one irregular line.

For the upper bound, let $r_j(P)$ denote the number of $(p^e - j)$ -secants through the point P of \mathcal{K} . We have that $\sum_{j=1}^{p^e-1} jr_j(P) = \varepsilon$. When s_j denotes the number of $(p^e - j)$ -secants, then $s_j(p^e - j) = \sum_{P \in \mathcal{K}} r_j(P)$. Note that now $s_j = 0$ for $p^i \nmid (p^e - j)$, hence for $p^i \nmid j$. So:

$$p^i(p^e - p^i) \sum_{j=p^i}^{p^e-p^i} s_j \leq \sum_{j=p^i}^{p^e-p^i} j(p^e - j)s_j = \sum_j j \sum_{P \in \mathcal{K}} r_j(P) = \sum_{P \in \mathcal{K}} \sum_j jr_j(P) = \varepsilon|\mathcal{K}|$$

Hence $\delta = \sum_j s_j \leq (\varepsilon|\mathcal{K}|)/(p^i(p^e - p^i))$ and since $|\mathcal{K}| \leq (q+1)(p^e - 1)$, we are done. \square

Let ℓ be the line at infinity in $\text{PG}(2, q)$, for the affine points of \mathcal{K} write $\mathcal{K} \setminus \ell = \{(a_i, b_i, 1)\}$ and consider the Rédei polynomial of $\mathcal{K} \setminus \ell$ introduced in Chapter 3:

$$H(X, Y, Z) = \prod_{i=1}^{|\mathcal{K} \setminus \ell|} (X + a_i Y - b_i Z) = \sum_{j=0}^{|\mathcal{K} \setminus \ell|} h_j(Y, Z) X^{|\mathcal{K} \setminus \ell| - j}$$

Recall that $h_j(Y, Z)$ is a homogeneous polynomial of degree j . Furthermore, let us introduce the following polynomial:

$$U(X, Y, Z) = \sum_{j=0}^{|\mathcal{K} \setminus \ell|/p^i} u_j(Y, Z) X^{(|\mathcal{K} \setminus \ell|/p^i) - j}, \text{ where } u_j(Y, Z) = h_{jp^i}(Y, Z).$$

Remark that u_j is homogeneous and its total degree is jp^i . Assume that $(z, y, 0) \in \ell \setminus \mathcal{K}$. Then since each line intersects \mathcal{K} in $0 \pmod{p^i}$ point, the lemma above implies that $H(X, y, z)$ is a p^i -th power of a polynomial. Furthermore, $H(X, y, z) = U(X^{p^i}, y, z)$ holds. For any element w of $\text{GF}(q)$, there is a unique element $x \in \text{GF}(q)$, such that $x^{p^i} = w$. Hence there is a 1 – 1 correspondence between the $\text{GF}(q)$ -rational points of $H(X, y, z)$ and $U(X, y, z)$. Furthermore, if (w, y, z) is a point of U , then the intersection multiplicity of the line $zY = yZ$ and H at the point (x, y, z) is exactly p^i times the intersection multiplicity of the line $zY = yZ$ and U at the point (w, y, z) . So at this point considering U instead of H makes no essential difference.

For any $(z, y, 0) \in \ell \setminus \mathcal{K}$, the multiplicity of the roots of $H(X, y, z)$ are divisible by p^i (see Lemma 3.1). So when $i > 0$, the derivative of $H(X, y, z)$ (with respect to X) is zero, since the characteristic is p . By the choice of i , it is not always the case for the polynomial $U(X, y, z)$; this will be the advantage of using U instead of H .

From now on $U'_X(X, Y, Z)$ will denote the partial derivative of $U(X, Y, Z)$ with respect to X . The fact that through a point $(z, y, 0) \in (\ell \setminus \mathcal{K})$ there pass exactly s irregular lines can be interpreted by the polynomial $U(X, Y, Z)$.

Lemma 4.3 *The affine index of a point $(z, y, 0) \in (\ell \setminus \mathcal{K})$ is s if and only if the greatest common divisor of $U(X, y, z)$ and $U'_X(X, y, z)$ has degree exactly $\deg_X(U) - s$, that is $(|\mathcal{K} \setminus \ell|/p^i) - s$.*

Proof: By Lemma 3.1, the multiplicity of a root x of $H(X, y, z)$ is not divisible by p^{i+1} , if and only if x corresponds to an irregular line through $(z, y, 0)$. From the argument above it follows that the roots of $U(X, y, z)$ will have multiplicity divisible by p or they will correspond to irregular lines. The characteristic is p , so considering $U'_X(X, y, z)$, the roots (of $U(X, y, z)$) that had multiplicity divisible by p will have at least this multiplicity, while the multiplicity of the other roots will decrease by 1. Thus the greatest common divisor of $U(X, y, z)$ and $U'_X(X, y, z)$ has degree exactly $\deg_X(U) - s$. \square

Assume that there is a point in $\ell \setminus \mathcal{K}$ with affine index s . For the parameter s and for the polynomials $U(X, Y, Z)$ and $U'_X(X, Y, Z)$ construct the matrix $R_s(Y, Z)$ and the polynomial $c^{(s)}(X, Y, Z)$ introduced in Section 2. Observe that the coefficients of U and U'_X can be expressed using the coefficients $u_0(Y, Z), u_1(Y, Z) \dots$ of $U(X, Y, Z)$, that is using the coefficients $h_0(Y, Z), h_{p^i}(Y, Z) \dots$ of $H(X, Y, Z)$. First of all note that for any $(z, y, 0) \in (\ell \setminus \mathcal{K})$ with affine index s :

$$c^{(s)}(X, y, z) = \frac{U(X, y, z)}{\gcd(U(X, y, z), U'_X(X, y, z))} \det R_s(y, z).$$

By Result 3.2 and by Lemma 4.3, $\det R_s(y, z)$ is not zero. Hence an element x is a root of $c^{(s)}(X, y, z)$ if and only if x corresponds to an irregular line through $(z, y, 0)$. Note that the multiplicity of the roots of $c^{(s)}(X, y, z)$ is always 1.

Our aim is to find a typical index on ℓ , such that most of the points on $\ell \setminus \mathcal{K}$ have affine index s . The next lemma is crucial for finding such an index.

Lemma 4.4 *Let ℓ be a line and assume that the point P in $\ell \setminus \mathcal{K}$ has affine index k . Denote by n_{k-h} the number of points of $\ell \setminus \mathcal{K}$ that have affine index $(k - h)$. Then $\sum_{h=1}^k h n_{k-h} \leq p^i k(k - 1)$.*

In [53] $e = 1$ and so $i = 0$. There it was showed that the number of points in $\ell \setminus \mathcal{K}$ that has index less than k is at most $k(k - 1)$. The lemma above is very similar to this, the only difference is that now the points are counted with weights. This will be one of the main observations that helps to improve on Result 4.1.

Proof: Let ℓ be the line at infinity and for the affine point set $\mathcal{K} \setminus \ell$ construct the polynomial $U(X, Y, Z)$. Assume that $P = (z, y, 0)$. By Lemma 4.3, $\deg(\gcd(U(X, y, z), U'_X(X, y, z)))$ is $\deg_X(U) - k$. For the polynomials $U(X, Y, Z)$ and $U'_X(X, Y, Z)$ and for the value k , construct the matrix $R_k(Y, Z)$ introduced in Section 3.1. By Result 3.2, $\det R_k(y, z) \neq 0$ and so $\det R_k(Y, Z) \neq 0$. Furthermore, by Proposition 3.5, if $(z', y', 0) \in \ell \setminus \mathcal{K}$ has index $k - h$, $h > 1$, then $(z'Y - y'Z)^h$ is a factor of $\det R_k(Y, Z)$. So $\sum_{h=1}^k hn_{k-h} \leq \deg(\det R_k(Y, Z))$ and by Proposition 3.3 it is at most $p^i k(k - 1)$. \square

Proposition 4.5 *For every line ℓ , there is a unique value $s = s(\ell)$ such that:*

- (1) $s \leq \frac{\delta}{q+1} + \frac{1}{2}$;
- (2) at least $q + 1 - \frac{q}{4p^i} - \sqrt{q}$ points on $\ell \setminus \mathcal{K}$ have affine index $s(\ell)$;
- (3) if a point of $\ell \setminus \mathcal{K}$ has affine index larger than s , then its affine index is at least $\frac{q+1-\sqrt{q}}{p^i}$.

Proof: Let k be a value such that there exists a point on $\ell \setminus \mathcal{K}$ with affine index k . Let n_{k-h} be the number of points on $\ell \setminus \mathcal{K}$ having affine index $(k - h)$, $h \geq 0$. Then the number δ of irregular lines of \mathcal{K} is at least $(q+1 - |\ell \cap \mathcal{K}|)k - \sum_{h=1}^k hn_{k-h}$. By Lemma 4.4, it is at least $(q + 1 - |\ell \cap \mathcal{K}|)k - p^i k(k - 1)$. Hence:

$$(q + 1 - |\ell \cap \mathcal{K}|)k - p^i k(k - 1) \leq \delta \quad (4.1)$$

Since $|\ell \cap \mathcal{K}| \leq \sqrt{q}/2$ and $\varepsilon, p^i \leq \sqrt{q}/4$, estimating the discriminant in (4.1) by $(q + 1 - |\ell \cap \mathcal{K}| + p^i - (2p^i(\delta/q + 1) + p^i))^2$ from below, we get that $k \leq \frac{\delta}{q+1} + \frac{1}{2}$ or $k \geq \frac{q+1-2\varepsilon-|\ell \cap \mathcal{K}|}{p^i}$.

Let s be the greatest value such that it is at most $\frac{\delta}{q+1} + \frac{1}{2}$ and there exists a point on $\ell \setminus \mathcal{K}$ having index s . The number of irregular lines is less than $\frac{2\varepsilon}{p^i}(q+1)$, so there are at most 2ε points having index bigger than s (hence index at least $\frac{q+1-\sqrt{q}}{p^i}$). By Lemma 4.4 the number of points on $\ell \setminus \mathcal{K}$ with index smaller than

s is at most $p^i s(s-1) \leq \frac{4\varepsilon^2}{p^i}$; so the number of points on $\ell \setminus \mathcal{K}$ with affine index $s(\ell)$ is at least $q+1 - |\ell \cap \mathcal{K}| - \frac{4\varepsilon^2}{p^i} - 2\varepsilon$. \square

The value $s(\ell)$ above will be called the *typical affine index* on ℓ . Furthermore, a *typical point* of ℓ is a point of $\ell \setminus \mathcal{K}$ with typical affine index. Until this point we followed the proof of Result 4.1, now we leave that way.

By Lemma 4.2, there are less than $2\varepsilon(q+1)/p^i$ lines containing at least 1 but less than p^ε points of \mathcal{K} . Hence for any line ℓ , there are at least $(q+1)/2 - \sqrt{q}/2$ points of $\ell \setminus \mathcal{K}$, so that the number of not p^ε - or 0-secants (of \mathcal{K}) through these points is less than $(4\varepsilon)/p^i$. Through such points there pass at least $\frac{q+5\varepsilon}{p^\varepsilon} - \frac{4\varepsilon}{p^i} \geq \sqrt{q}$ lines not intersecting \mathcal{K} , since a j -secant, $0 < j < p^\varepsilon$, contains at least p^i points.

Remark 4.6 *There are points through which there pass at least \sqrt{q} skew lines to \mathcal{K} .*

Next we will make the bound in Proposition 4.5 (1) more accurate.

Lemma 4.7 *The typical affine index of an irregular line is at most $\frac{\delta}{q+1} - \frac{1}{2}$.*

Proof: Take a typical point P on an irregular line g and denote by $s(g)$ the typical affine index on g , thus the total number of irregular lines through P is $s(g) + 1$. Note that by Proposition 4.5, there is a gap between the values of the typical affine index and the next possible affine index after it, so on a line through P , which is not irregular, the typical affine index is at least $s(g) + 1$; hence the result follows from Proposition 4.5 (1). \square

By Lemma 4.2, $\delta/(q+1) \leq 2\varepsilon/p^i$, furthermore since $2\varepsilon/p^i$ is an integer, the lemma above says that the typical affine index of a line is at most $2\varepsilon/p^i$ while the typical affine index of an irregular line is less than $2\varepsilon/p^i$. Proposition 4.5 and Lemma 4.7 yields the following corollary.

Corollary 4.8 \bullet *The index of a point is either at most $2\frac{\varepsilon}{p^i}$ or at least $\frac{q+1-\sqrt{q}}{p^i}$. The latter index will be called big.*

- \bullet *The typical affine index on an irregular line is less than $2\frac{\varepsilon}{p^i}$, on the remaining lines it is at most $2\frac{\varepsilon}{p^i}$.*

The next lemma is a very important corollary of Lemma 4.7.

Lemma 4.9 *On each irregular line there is at least one point with big index.*

Proof: Assume to the contrary, that there exists an irregular line ℓ such that none of its points have big index. By Lemma 4.7 and by Lemma 4.5 (3), the affine index of any point in $\ell \setminus \mathcal{K}$ is at most $\frac{\delta}{q+1} - \frac{1}{2}$. Since ℓ is irregular, the affine index of a point in $\ell \cap \mathcal{K}$ is at most $\varepsilon/p^i - 1$. Hence by counting the number of irregular lines through the points of ℓ we get at most:

$$\delta \leq 1 + \left(\frac{\varepsilon}{p^i} - 1\right)|\ell \cap \mathcal{K}| + \left(\frac{\delta}{q+1} - \frac{1}{2}\right)|\ell \setminus \mathcal{K}| \quad (4.2)$$

Substituting $q+1 - |\ell \cap \mathcal{K}|$ in $|\ell \setminus \mathcal{K}|$, we get a contradiction. \square

In [53] a curve was associated to (k, p) -arcs, so that the points of this curve corresponded to irregular lines. Now we introduce almost the same curve.

Proposition 4.10 *Let s be the typical affine index for the line at infinity. Then there is a curve $c^\ell(X, Y, Z)$ such that:*

- (1) $\deg_X(c^\ell) = p^i s$, $\deg(c^\ell) \leq p^i s^2 \leq (q/4p^i)$;
- (2) *when the point $(z, y, 0) \in \ell \setminus \mathcal{K}$ has index s , then x is a root of the polynomial $c^\ell(X, y, 1)$ if and only if the line $zY = yX + xZ$ is irregular.*

Proof: For the polynomials $U(X, Y, Z)$ and $U'_X(X, Y, Z)$ construct the polynomial $c^{(s)}(X, Y, Z)$ introduced in Section 3.1. By Proposition 3.3, the coefficient of X^{s-j} in $c^{(s)}$ is homogeneous and if it is not zero, then its total degree is $p^i s(s-1) + p^i j$. In the polynomials $c^{(s)}$ substitute X^{p^i} in place of X to obtain the homogeneous polynomial c^ℓ . Hence the result follows by Corollary 4.8 and by Proposition 3.3. \square

In [53] using Bézout's theorem it was shown that the curve associated to the (k, p) -arc does not depend on the choice of the line at infinity and so it splits into linear factors, that is into line pencils. Finally, it was proved that by adding to the (k, p) -arc the vertices of these line pencils we get a maximal arc. Unfortunately when $\varepsilon \geq \sqrt[4]{q}/2$, the degree of c^ℓ is too large so we cannot use Bézout's theorem, hence we have to do something else.

In the rest of this chapter we show that by adding the points with big index to \mathcal{K} we obtain a maximal arc. Of course, now this will be done without factorizing c^ℓ . Note that Lemma 4.9 was the first step in this direction. Though we cannot factorize c^ℓ , some of its components are known. From now on often c^ℓ will be considered as a dual curve, that is an envelope.

Proposition 4.11 *For any line ℓ construct the curve c^ℓ . Consider c^ℓ as a dual curve, so as an envelope. Let $P = (a_i, b_i, 1)$ be a point in $\text{PG}(2, q) \setminus \ell$, such that it has big index. Then the line pencil $(X + a_i Y - b_i Z)$ corresponding to P is a component of c^ℓ .*

Proof: By Proposition 4.5, there are at least $\frac{q+1-\sqrt{q}}{p^i} - \frac{q}{4p^i} - \sqrt{q}$ irregular lines through P which intersect ℓ in typical points. Hence by Proposition 4.10 (2), there are at least this many common lines of c^ℓ and the line pencil corresponding to P . When $q \geq 16$, this is bigger than $\deg c^\ell$, so by Bézout's theorem we are done. \square

Proposition 4.12 *The value i must be 0.*

Proof: Pick a point P with big index and for a line ℓ not through P construct the curve c^ℓ . By Proposition 4.11, the line pencil corresponding to P is a component of c^ℓ . By Proposition 4.5, there are at least $q + 1 - q/(4p^i) - \sqrt{q}$ points on $\ell \setminus \mathcal{K}$ with typical index, hence Proposition 4.10 (2) implies that through P there pass at least this many irregular lines. On an irregular line there are at most $p^e - p^i$ points. So when $p^i > 1$, counting the points of \mathcal{K} on the lines through P we get much less points than $|\mathcal{K}|$. Therefore i is either 0 or there is no point with big index at all. Hence when $i > 0$, then by Lemma 4.9, there is no irregular line, which contradicts the choice of i . \square

Note that by Lemma 4.2 and by Proposition 4.5, $i = 0$ means that the index of any point is at most ε or at least $q + 1 - \sqrt{q}$. This latter index was called big. Furthermore, the curve c^ℓ in Proposition 4.10 has degree at most $q/4$, its X -degree is at most the typical index (that is at most ε) and the polynomial $U(X, Y, Z)$ is just the polynomial $H(X, Y, Z)$.

Corollary 4.13 *The number of points with big index is at most ε .*

Proof: Let ℓ be the line at infinity and construct the envelope c^ℓ . By Proposition 4.11, a line pencil corresponding to an affine point having big index must be a component of c^ℓ . The X -degree of such a component is 1, hence by Proposition 4.10 (1) and by Proposition 4.12, there are at most ε affine points with big index. If there are no points with big index on ℓ , then we are done.

Otherwise, there are at most ε such points on ℓ , so in total there are at most 2ε points with big index. The result follows by choosing another ℓ , so that it does not contain points with big index. \square

Corollary 4.14 *Let ℓ be the line at infinity. Then a line different from ℓ and passing through a typical point of ℓ contains exactly 1 affine point with big index when it is irregular and 0 otherwise.*

Proof: Assume that $(z, y, 0)$ is a typical point on ℓ and choose g to be a line through $(z, y, 0)$. First we show that g is irregular if and only if g contains an affine point with big index. Note that by Lemma 4.9, we only have to show that if g passes through a point having big index, then g must be irregular. This follows from Proposition 4.10 (2), since by Proposition 4.11, any line pencil corresponding to an affine point having big index is a component of the envelope c^ℓ . We only left to show that when g is irregular, then it cannot contain more than 1 point with big index; but this follows from the fact that the multiplicity of any root of $c^\ell(X, y, 1)$ is 1. \square

Observe that the lemma above can be translated in terms of the envelope constructed in Proposition 4.10. For any line ℓ at infinity, the envelope c^ℓ contains $\deg_X(c^\ell)$ linear factors corresponding to the affine points having big index. The rest of the components of c^ℓ do not depend on X .

Lemma 4.15 *On any line ℓ there exists a typical point P , such that the affine irregular lines through P are all $(p^e - 1)$ -secants.*

Proof: Denote by B the set of points having big index. Note that B is not empty, since otherwise by Lemma 4.9, there would be no irregular line, which contradicts the choice of i . For a point $b \in B$, denote by $r(b)$ the number of p^e -secants and by $t(b)$ the number of at most $(p^e - 2)$ -secants passing through b . Let $R = \sum_{b \in B} r(b)$ and $T = \sum_{b \in B} t(b)$. Counting the points of \mathcal{K} from each

point of B , we get $|B|(qp^e - q + p^e - \varepsilon)$ points (with multiplicity). On the other hand, we count at most $Rp^e + T(p^e - 2) + (|B|(q + 1) - R - T)(p^e - 1)$ points. Hence $T \leq R + |B|(\varepsilon - 1)$ and since there are at most ε points with big index we get that $T \leq R + \varepsilon(\varepsilon - 1)$. Our aim is to show that T is less than the number of typical points on ℓ (so it is less than $\frac{3}{4}q + 1 - \sqrt{q}$, see Proposition 4.5); from which the result follows. To do this we prove that R is at most $\varepsilon(\varepsilon - 1)$; hence T is at most $2\varepsilon(\varepsilon - 1)$, that is less than $q/8$.

Take a line g that is skew to B . By Proposition 4.5 (3) and by Corollary 4.14, the typical affine index on g is B and a non-typical point has index less than $|B|$. Pick a point G of $g \setminus \mathcal{K}$ that has index $|B| - h$, $h \geq 0$, and count the p^e -secants through G , each with multiplicity the number of points with big index on it. This value is at most h , since on each irregular line there must be at least 1 point with big index. Now adding up this value for the points on $g \setminus \mathcal{K}$ we get R , on the other hand by Lemma 4.4, we get at most $|B|(|B| - 1)$, that is at most $\varepsilon(\varepsilon - 1)$. \square

Theorem 4.16 *Assume that \mathcal{K} is a $(qp^e - q + p^e - \varepsilon, p^e)$ -arc in $\text{PG}(2, q)$, $q = p^h$, p prime. Suppose also that $\varepsilon \leq \frac{1}{4}\sqrt{q}$ and $p^e \leq \frac{1}{2}\sqrt{q}$. Then \mathcal{K} can be embedded in a maximal arc.*

Proof: Denote by \mathcal{K}' the union of the points of \mathcal{K} and the points with big index. We show that each line intersects \mathcal{K}' in $0 \pmod{p^e}$ point. Pick a line ℓ . By Lemma 4.15, there is at least one typical point P on ℓ such that the irregular lines of \mathcal{K} through P are all $(p^e - 1)$ -secants. By Corollary 4.14, each line through P contains 1 or 0 point with big index according as it is irregular or not, whence they intersect $\mathcal{K}' \setminus \ell$ in $0 \pmod{p^e}$ point; so $|\mathcal{K}' \setminus \ell| \equiv 0 \pmod{p^e}$ holds. By Remark 4.6 and by Corollary 4.13, there exists a line g that is skew to \mathcal{K}' . When g plays the role of ℓ , then the argument above implies that $|\mathcal{K}'| \equiv 0 \pmod{p^e}$, from which $|\ell \cap \mathcal{K}'| \equiv 0 \pmod{p^e}$ follows.

Since there are at most ε points with big index, $|\mathcal{K}'| \leq qp^e - q + p^e$. Take a point of \mathcal{K}' . The lines through this point intersect \mathcal{K}' in at least p^e points, hence $\mathcal{K}' \geq qp^e - q + p^e$. So $|\mathcal{K}'| = qp^e - q + p^e$ and any line intersects \mathcal{K}' in 0 or in p^e points, thus \mathcal{K}' is maximal. \square

Combining Theorem 4.16 with the result of Ball, Blokhuis and Mazzocca on

non-existence of maximal arcs (and with the results of [10] and [30]), the next corollary follows:

Corollary 4.17 *A (k, p^e) -arc in $\text{PG}(2, q)$, $q = p^h$, $p > 2$ prime, has size less than $qp^e - q + p^e - \frac{1}{4}\sqrt{q}$. \square*

4.3 Remarks

For sake of simplicity we proved our main theorem for the constant $1/4$. The same proof, but a bit more complicated counting shows that the constant can be slightly improved. But since in general, except when $p^e = 2$, the right order of magnitude is probably not \sqrt{q} , the constant is not really relevant.

For $p^e = 2$, Segre showed (see [48]) that $(q + 2 - \varepsilon)$ -arcs, $\varepsilon \leq \sqrt{q}$, are incomplete. On the other hand, when $4 < q$ is a square, then there exist complete arcs of size $q - \sqrt{q} + 1$ (see [21], [28] and [37]), which shows that in this case the result is sharp.

We give a new proof for Segre's result using the idea of the previous sections. The reason why now the constant can be improved to 1 is that in this special case everything turns out to be much simpler. Note that for $\varepsilon \leq \sqrt{q}$, Lemma 4.4 remains still true.

Theorem 4.18 *Any arc in $\text{PG}(2, q)$, q even, of size greater than $q - \sqrt{q} + 1$ can be embedded in a hyperoval.*

Proof: If there is a point, not in the arc, through that there pass only 0- and 1-secants, then adding this point to the arc we still get an arc. Repeating this process until there is no more such a point, we obtain an arc \mathcal{K} . We show that \mathcal{K} is a hyperoval.

Assume to the contrary, that \mathcal{K} is not a hyperoval, hence $|\mathcal{K}| = q + 2 - \varepsilon$, where $1 \leq \varepsilon \leq \sqrt{q}$. First of all observe that there are exactly ε 1-secants passing through a point of \mathcal{K} , hence the total number of 1-secants is $\varepsilon(q + 2 - \varepsilon) \neq 0$.

We show that the index s of a point on any 0-secant ℓ is at most ε . As before by Lemma 4.4, counting the 1-secants through the points of ℓ we get at least $(q+1)s - s(s-1)$, that is at most $\varepsilon(q+2-\varepsilon)$; from which $s \leq \varepsilon$ or $s \geq q+2-\varepsilon$ follows. Note that there can be no point with index at least $q+2-\varepsilon$, since

such a point would have index $q + 2 - \varepsilon$ exactly and it could have been added to \mathcal{K} . Furthermore, since through each point outside \mathcal{K} there passes at least one 0-secant, the argument above implies that the index of any point is at most ε .

Hence the 1-secants form a dual $(\varepsilon(q + 2 - \varepsilon), \varepsilon)$ -arc and so when $1 \leq \varepsilon \leq \sqrt{q}$, the contradiction follows by Barlotti's bound. \square

Chapter 5

A conjecture of Metsch

After I had finished the first draft of this thesis, I participated in the conference “Combinatorics 2002”, where Klaus Metsch presented the conjecture below. Realizing that this was one of the most elegant applications of the ideas in Sections 3.1 and 3.2, I felt that its proof cannot be left out from the thesis.

Conjecture 5.1 (Metsch) *Let B be a point set in $\text{PG}(2, q)$. Pick a point P not from B and assume that through P there pass exactly r lines meeting B (that is containing at least 1 point of B). Then the total number of lines meeting B is at most $1 + rq + (|B| - r)(q + 1 - r)$.*

First of all observe that there are point sets for which the given bound is sharp. Assume that $r - 1$ is the order of a subplane π in $\text{PG}(2, q)$ and let B be the proper subset of π containing r collinear points, hence B blocks all the lines of π . So the number of lines meeting B is $((r - 1)^2 + (r - 1) + 1) + |B|(q + 1 - r)$, where the first part is the number of lines in π , the second counts the lines through the points of B which does not contain a line of π . Choose P to be in $\pi \setminus B$, hence the number of lines through P meeting B is r and so the bound in the conjecture is sharp. Note that the following well-known result of Jamison [36] and Brouwer and Schrijver [22] is a consequence of the statement of the conjecture.

Theorem 5.2 (Jamison, Brouwer and Schrijver) *A blocking set in $\text{AG}(2, q)$ contains at least $2q - 1$ points.*

Proof: Assume to the contrary that there is a blocking set B in $\text{AG}(2, q)$, of size $|B| \leq 2q - 2$. Embed $\text{AG}(2, q)$ into $\text{PG}(2, q)$ and let P be an ideal point.

Now the value r in the conjecture above is q and so the total number of lines meeting B is at most $1 + qq + (|B| - q)(q + 1 - q) \leq q^2 + q - 1$; which is a contradiction, since B blocks all the $q^2 + q$ affine lines. \square

There are blocking sets of size less than $2q - 1$ on certain non-Desarguesian affine planes of order q , see [25]. This shows that the conjecture cannot be true over arbitrary projective planes. For the proof of the conjecture the following lemma is crucial.

Lemma 5.3 *Let ℓ_∞ be the line at infinity in $\text{PG}(2, q)$ and let S be a point set in $\text{PG}(2, q) \setminus \ell_\infty$. Assume that $|S| \neq q$ and suppose that through the ideal point $(z, y, 0)$ there pass t (affine) lines meeting S . Denote by n_{t+h} the number of ideal points through that there pass exactly $t + h$ (affine) lines meeting S . Then $\sum_{h=1}^{q-t} hn_{t+h} \leq (|S| - t)(q - t)$.*

Proof: For the points of S write $\{(a_i, b_i, 1)\}$ and consider the three-variable Rédei polynomial of S , that is $H(X, Y, Z) = \prod_{i=1}^{|S|} (X + a_i Y - b_i Z) = \sum_{j=0}^{|S|} h_j(Y, Z) X^{|S|-j}$. Recall that $\deg h_j = j$ or $h_j = 0$. It follows from Lemma 3.1, that $\deg_X \gcd(H(X, y, z), X^q - X) = t$.

For the polynomials H and $X^q - X$ and for the value $k = \max(\deg_X H, q) - t$, construct the matrix $R_k(Y, Z)$ introduced in Section 3.1. By Proposition 3.5, if through $(z', y', 0) \in \ell_\infty$ there pass $t + h$, $h \geq 1$, lines meeting S , then $(z'Y - y'Z)^h$ is a factor of $\det R_k(Y, Z)$. Hence $\sum_{h=1}^{q-t} hn_{t+h} \leq \deg(\det R_k(Y, Z))$.

To write up the matrix $R_k(Y, Z)$ we have to distinguish two cases according as $|S|$ is smaller or bigger than q . Here we only consider the case $|S| < q$, the other case can be handled similarly and so it is left to the reader. Let $|S| = q - a$ (note that $t \leq q - a$), hence R_k is the following $2(q - t) \times 2(q - t)$ matrix:

$$\left(\begin{array}{c|cccc} & 0 & 0 & \dots & 0 \\ & \vdots & & & \\ \underline{\underline{I_{q-t}}} & -h_0(Y, Z) & 0 & \dots & 0 \\ & -h_1(Y, Z) & -h_0(Y, Z) & \dots & 0 \\ & \vdots & & \ddots & \\ & -h_{q-t-a-1}(Y, Z) & -h_{q-t-a-2}(Y, Z) & \dots & \vdots \\ \hline & -h_{q-t-a}(Y, Z) & -h_{q-t-a-1}(Y, Z) & \dots & \\ & \vdots & & & \\ \underline{\underline{A}} & \vdots & & & \vdots \\ & -h_{2(q-t)-a-1}(Y, Z) & -h_{2(q-t)-a-2}(Y, Z) & \dots & -h_{q-t-a}(Y, Z) \end{array} \right)$$

where $\underline{\underline{A}}$ is the zero matrix, when $2(q-t) \leq q-1$; otherwise the zeros at the $(t-1+i, i)$ -th entries of $\underline{\underline{A}}$, $i = 1 \dots q+1-2t$, are replaced by -1 . It is not difficult to see that the degree of each term of the determinant is at most $(q-t-a)(q-t) = (|S|-t)(q-t)$, hence the degree of the determinant is also at most this value. \square

Proof of Metsch' conjecture: For the line at infinity ℓ_∞ choose an m -secant, $m > 0$, of B passing through P . Note that now the line at infinity meets B , hence through P there pass $(r-1)$ affine lines containing at least 1 point from B . Again denote by $n_{(r-1)+h}$ the number of ideal points through which there pass exactly $(r-1)+h$ affine lines meeting B . Let us sum up the number of affine lines meeting B through the ideal points, in total we get at most $qm + [(q+1-m)(r-1) + \sum_{h=1}^{q-(r-1)} hn_{(r-1)+h}]$; where the first part corresponds to the points of $\ell_\infty \cap B$, the second to the points of $\ell_\infty \setminus B$. When $|B \setminus \ell_\infty| \neq q$, then the result follows from Lemma 5.3 immediately.

Now assume that for each line ℓ through P , for that ℓ contains at least 1 point of B , $|B \setminus \ell| = q$ holds. Then either each line through P contains exactly 1 point of B , hence $r = q+1$ and so Metsch' bound gives $1 + q + q^2$ (which is just the total number of lines of $\text{PG}(2, q)$) or it follows that $|B| \geq 2r$. Note that in the latter case $r < q+1$, hence there is a line ℓ' through P so that it is skew to B . Since now $|B| \geq 2r$, choosing ℓ' to be the line at infinity, Lemma 5.3 gives a stronger bound than it is in Metsch' conjecture. \square

Bibliography

This thesis based on the following publications of the author

- [1] A. GÁCS AND ZS. WEINER, On $(q + t, t)$ -arcs of type $(0, 2, t)$, *Designs, Codes and Cryptography*, submitted.
- [2] O. POLVERINO, T. SZŐNYI AND ZS. WEINER, Blocking sets in Galois planes of square order, *Acta Sci. Math. (Szeged)* **65** (1999), 737–748.
- [3] T. SZŐNYI, A. GÁCS AND ZS. WEINER, On the spectrum of minimal blocking sets in $PG(2, q)$, *Proc. Combinatorics'2002*, Univ. Basilicata, 242–265.
- [4] T. SZŐNYI AND ZS. WEINER, Small Blocking sets in Higher Dimensions, *J. Comb. Theory Ser. A* **95** (2001), 88–101.
- [5] ZS. WEINER, On (k, p^e) -arcs in Galois planes of order p^h , *Finite Fields and Appl.*, submitted.

Other publications of the author

- [6] A. BLOKHUIS, T. SZŐNYI AND ZS. WEINER, On sets without tangents on Galois planes of even order, *Designs, Codes and Cryptography*, to appear.
- [7] L. STORME AND ZS. WEINER, On 1-blocking sets in $PG(n, q)$, $n \geq 3$, *Designs, Codes and Cryptography* **21** (2000), 235–251.
- [8] T. SZŐNYI AND ZS. WEINER, Large minimal blocking sets, manuscript, 2002.

References

- [9] S. BALL, Partial unitals and related structures in Desarguesian planes, *Designs, Codes and Cryptography* **15** (1998), 231–236.
- [10] S. BALL AND A. BLOKHUIS, On the incompleteness of (k, n) -arcs in Desarguesian planes of order q where n divides q , *Geom. Dedicata* **74** (1999), 325–332.
- [11] S. BALL, A. BLOKHUIS AND F. MAZZOCCA, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica* **17** (1997), 31–41.
- [12] A. BARLOTTI, Sui $\{k, n\}$ -archi di un piano lineare finito, *Boll. Un. Mat. Ital.* **11** (1956), 553–556.
- [13] T. BETH, D. JUNGnickel AND H. LENZ, *Design theory*, 2nd Edition, Cambridge Univ. Press, 1999.
- [14] A. BEUTELSPACHER, Blocking sets and partial spreads in finite projective spaces, *Geom. Dedicata* **9** (1980), 425–449.
- [15] A. BLOKHUIS, *Blocking sets in Desarguesian Planes*, in: Paul Erdős is Eighty, vol. **2** (1996), 133–155. eds.: D. Miklós, V.T. Sós, T. Szőnyi, Bolyai Soc. Math. Studies.
- [16] A. BLOKHUIS, On the size of a blocking set in $PG(2, p)$, *Combinatorica* **14** (1994), 273–276.
- [17] A. BLOKHUIS, S. BALL, A. BROUWER, L. STORME AND T. SZŐNYI, On the number of slopes determined by a function on a finite field, *J. Comb. Theory Ser. (A)* **86** (1999), 187–196.
- [18] A. BLOKHUIS AND A. E. BROUWER, Blocking sets in Desarguesian projective planes, *Bull. London Math. Soc.* **18** (1986), 132–134.
- [19] A. BLOKHUIS AND K. METSCH, Large minimal blocking sets, strong representative systems and partial unitals, in: *Finite Geometries*, (F. De Clerck et al. eds), Cambridge Univ. Press, Cambridge, 1993, 37–52.

- [20] A. BLOKHUIS, R. PELLIKAAN AND T. SZŐNYI, Blocking sets of almost Rédei type, *J. Comb. Theory Ser. A* **78** (1997), 141–150.
- [21] E. BOROS AND T. SZŐNYI, On the sharpness of the theorem of B. Segre, *Combinatorica* **6** (1986), 261–268.
- [22] A. E. BROUWER AND A. SCHRIJVER, The blocking number of an affine space, *J. Comb. Theory Ser. A* **24** (1978), 251–253.
- [23] A. A. BRUEN, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.
- [24] A. A. BRUEN, Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.
- [25] A. A. BRUEN AND M. J. DE RESMINI, Blocking sets in affine planes, In *Combinatorics '81*, **18** of *Ann. Discrete Math.*, North-Holland, Amsterdam-New York (1983), 169–175. (Rome, 1981)
- [26] A. A. BRUEN AND J. A. THAS, Blocking Sets, *Geom. Dedicata* **6** (1977), 193–203.
- [27] R. H. F. DENNISTON, Some maximal arcs in finite projective planes, *J. Comb. Theory* **6** (1969), 317–319.
- [28] J. C. FISCHER, J. W. P. HIRSCHFELD AND J. A. THAS, Complete arcs on planes of square order, *Ann. Discrete Math.* **30** (1986), 243–250.
- [29] A. GÁCS, On a generalization of Rédei's theorem, *Combinatorica*, to appear.
- [30] É. HADNAGY AND T. SZŐNYI, On the embedding of large (k, n) -arcs and partial unitals, *Ars Combinatoria*, to appear.
- [31] U. HEIM, Proper blocking sets in projective spaces, *Discrete Math.* **174** (1997), 167–176.
- [32] U. HEIM, Blockierende Mengen in endliche projektiven Räumen, *Mitt. Math. Semin. Giessen* **226** (1996), 4–82.

- [33] J. W. P. HIRSCHFELD, Projective geometries over finite fields, *Clarendon Press, Oxford*, 1979, 2nd edition, 1998.
- [34] J. W. P. HIRSCHFELD AND T. SZŐNYI, Constructions of large arcs and blocking sets in finite planes, *European J. Comb.* **12** (1991), 499–511.
- [35] T. ILLÉS, T. SZŐNYI AND F. WETTL, Blocking sets and maximal strong representative systems in finite projective planes, *Mitt. Math. Sem. Giessen* **201** (1991), 97–107.
- [36] R. E. JAMISON, Covering finite fields with cosets of subspaces, *J. Comb. Theory Ser. A* **22** (1977), 253–266.
- [37] B. C. KESTENBAND, A family of complete arcs in finite projective planes, *Colloq. Math.* **LVII** (1987), 59–67.
- [38] G. KORCHMÁROS AND F. MAZZOCCA, On $(q + t)$ -arcs of type $(0, 2, t)$ in a desarguesian plane of order q , *Math. Proc. Camb. Phil. Soc.* **108** (1990), 445–459.
- [39] G. LUNARDON, Normal spreads, *Geom. Dedicata* **75** (1999), 245–261.
- [40] G. LUNARDON, Linear k -blocking sets, *Combinatorica* **21** (2001), 571–581.
- [41] L. LUNELLI AND M. SCE, Considerazioni aritmetiche e risultati sperimentali sui $\{K, n\}_q$ -archi, *Ist. Lombardo Accad. Sci. Rend. A* **98** (1964), 3–52.
- [42] J. DI PAOLA, On minimum blocking coalitions in small projective plane games, *SIAM J. Appl. Math.* **17** (1969), 378–392.
- [43] P. POLITO AND O. POLVERINO, On small blocking sets, *Combinatorica* **18** (1998), 133–137.
- [44] O. POLVERINO, Small minimal blocking sets and complete k -arcs in $\text{PG}(2, p^3)$, *Discrete Math.* **208/9** (1999), 469–476.
- [45] O. POLVERINO, Small blocking sets in $\text{PG}(2, p^3)$, *Designs, Codes and Cryptography* **20** (2000), 319–324.

- [46] O. POLVERINO AND L. STORME, Small minimal blocking sets in $PG(2, q^3)$, *Eur. J. Comb.* **23** (2002), 83–92.
- [47] L. RÉDEI, *Lückenhafte Polynome über endlichen Körpern*, Akadémiai Kiadó, Budapest, and Birkhäuser Verlag, Basel, 1970 (English translation: *Lacunary polynomials over finite fields*, Akadémiai Kiadó, Budapest, and North Holland, Amsterdam, 1973).
- [48] B. SEGRE, Introduction to Galois geometries (ed. J.W.P. Hirschfeld), *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur I* **8** (1967), 133–236.
- [49] L. STORME AND P. SZIKLAI, Linear pointsets and Rédei type k -blocking sets in $PG(n, q)$, *J. Alg. Comb.* **14** (2001), 221–228.
- [50] P. SZIKLAI AND T. SZŐNYI, Blocking sets and algebraic curves, *Rend. Circ. Mat. Palermo* **51** (1998), 71–86.
- [51] T. SZŐNYI, Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* **12** (1992), 227–235.
- [52] T. SZŐNYI, Blocking sets in Desarguian affine and projective planes, *Finite Fields and Appl.* **3** (1997), 187–202.
- [53] T. SZŐNYI, On the embeddability of (k, p) -arcs, *Designs, Codes and Cryptography* **18** (1999), 235–246.
- [54] G. TALLINI, On blocking sets in finite projective and affine spaces, in: *Combinatorics'86*, volume **37** of *Ann. of Discrete Math.*, North-Holland, Amsterdam, 1988, 433–450.
- [55] J. A. THAS, Some results concerning $\{(q + 1)(n - 1), n\}$ -arcs and $\{(q + 1)(n - 1) + 1, n\}$ -arcs in finite projective planes of order q , *J. Comb. Theory Ser. A* **19** (1975), 228–232.

Summary

Concerning finite geometry, several methods can be used from other fields of mathematics. The first two chapters of the thesis contain mostly combinatorial and geometric reasonings, while the last two chapters give examples of how algebraic results can be applied.

In Chapter 1 a geometric construction for various minimal planar blocking sets is presented. In Section 1.1 we construct minimal planar blocking sets using 3-dimensional projective spaces. Section 1.2 is the generalization of the previous section. With minor alteration, the idea of Section 1.2 can be used to construct $(q+t, t)$ -arcs of type $(0, 2, t)$, see Section 1.3. The results of this chapter are from the works with Gács, Polverino and Szőnyi.

In $\text{PG}(2, q)$, $q = p^h$, Szőnyi proved that a small minimal blocking set intersects each line in $1 \pmod p$ point. The main result of Chapter 2 is that together with Szőnyi, we generalize this result to higher dimensions.

In Chapter 3 the common algebraic background used in the next two chapters is summarized.

In planes of order $q = p^h$, the largest (k, p^e) -arc has size at most $qp^e - q + p^e$; arcs of that size are called maximal. Szőnyi showed that when $e = 1$ and $\varepsilon \leq \sqrt[4]{q}/2$, a $(qp^e - q + p^e - \varepsilon, p^e)$ -arc can be extended to a maximal arc. In Chapter 4, this result is improved for $p^e \leq \sqrt{q}/2$ and for $\varepsilon \leq \sqrt{q}/4$. When p is odd, by Ball-Blokhuis, maximal arcs do not exist; hence the result above say that for the largest (k, p^e) -arc, $k < qp^e - q + p^e - \sqrt{q}/4$ hold.

Finally, in Chapter 5 a conjecture of Metsch on the number of lines intersecting a point set is proved.

Magyar nyelvű összefoglaló

A véges geometriákban a matematika különböző területeinek módszerei alkalmazhatóak: a disszertáció első két fejezete nagyrészt geometriai és kombinatorikus módszereket használ, míg a második részben az algebrai módszerek alkalmazhatóságára látunk példákat.

Az 1. fejezetben magasabb dimenziós projektív terek segítségével minimális lefogó ponthalmazokat konstruálunk Galois síkokon. Az itt szereplő eredmények Gácscsal, Polverinival és Szőnyivel közös munkákból származnak. A konstruált példák sok szempontból érdekesek. A fejezet végén megmutatjuk, hogy a konstrukció ötletével nem csak lefogó halmazokat, hanem (az ötletet kicsit módosítva) $(0, 2, t)$ típusú $(q + t, t)$ -íveket is előállíthatunk.

A 2. fejezetben Szőnyivel közösen, Szőnyi síkbeli lefogó halmazokra vonatkozó $1 \pmod p$ eredményét terjesztjük ki $2 < n$ dimenzióba. Majd ezt n dimenziós lefogó halmazok karakterizálására használjuk.

A 3. fejezet az utolsó két fejezet algebrai ötletét foglalja össze.

$\text{PG}(2, q)$ -ban, a legnagyobb (k, p^e) -ív mérete legfeljebb $qp^e - q + p^e$, az ilyen méretű íveket maximálisnak nevezik. Szőnyi megmutatta, hogy $e = 1$ és $\varepsilon \leq \sqrt[4]{q}/2$ esetén, egy $(qp^e - q + p^e - \varepsilon, p^e)$ -ív beágyazható egy maximális ívbe. A 4. fejezetben ezt az eredményt terjeszttem ki $\varepsilon \leq \sqrt{q}/4$ -re és $e = 1$ -ről $p^e \leq \sqrt{q}/2$ -re. Ball-Blokhuis megmutatta, hogy páratlan q esetén nincsenek maximális ívek; ilyenkor a fenti eredményből a (k, p^e) -ívek méretére kapunk felső korlátot.

Végül a 5. fejezetben Metsch egy sejtésére adok bizonyítást.