Csaba Mengyán

CONSTRUCTIONAL METHODS IN FINITE PROJECTIVE GEOMETRY

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

2008

Contents

Preambulum

Overview

In finite projective geometry several methods both from geometry and algebra can be used to attain new results. In this thesis we concentrate on some methods of particular importance in the construction of minimal blocking sets and a closely related notion, strong representative systems.

The preambulum is devoted to an overview of the thesis, acknowledgement and notation.

In Chapter 1 we give some basic definitions and concepts. We prove a generalization of the Bruen-Thas upper bound in Section 1.2. In Section 1.5 we give a short overview of the methods to be discussed: embedding, partitioning, random choice, adding and deleting points and use of subsets. The description here is very general, but in subsequent chapters we provide ample examples of their uses. We also include a strong algebraic technical tool, Weil's estimate and some of its variants.

Chapter 2 is devoted to higher dimensional constructions using embedding and partitioning. In Sections 2.1 and 2.2 we give necessary definitions and a general construction. In Section 2.3 we describe the generalized Buekenhout construction, and a particular type of large minimal blocking set obtained using this embedding method. In Section 2.4 we present some results obtained by the generalized Buekenhout construction and its modifications. In subsections of Section 2.5 we show three solutions to a problem raised by Gyárfás that is equivalent to partitioning the flags of $\mathrm{PG}(2, q)$ into strong representative systems. The first two subsections give results using geometrical and partitioning arguments, while the last part of the chapter shows a solution to this problem

obtained by the generalized Buekenhout construction using minimal blocking sets described in Section 2.3, and demonstrates the power of the embedding method over the other solutions.

In Chapter 3 we consider constructions in the plane. The results here use random choice in the first part of the chapter, and mainly subsets and cosets in the second part. In Section 3.1 we show density results and that the number of such structures is in most cases more than polynomial, a question originally asked by Turán. In Section 3.2 we construct more than polynomial number of minimal blocking sets starting from the well-known triangle and Megyesi's example respectively by placing suitable subsets (of points) on lines.

In Chapter 4 we investigate Megyesi's example more thoroughly. In Section 4.1 we show a generalization of Megyesi's example, and prove that there is a strong correspondence between such constructions and some trivial equations. Finally, in Section 4.2 we introduce a simple embedding method and sketch another high dimensional embedding method, and discuss their implications to constructing non-Rédei minimal blocking sets.

Finally, we end the thesis with the Bibliography, Summary and Hungarian summary.

Acknowledgement

Above all, I am thankful to my supervisor and menthor, professor Tamás Szőnyi, who had introduced me to finite geometry in the first place, and who made my studies of this field possible and also successful.

I am very grateful to professor Andrács Gács, who was instrumental in providing help and guidance to me in writing the articles that this thesis is based on.

I would also like to thank my co-authors: M. Nóra Viola Harrach and Zsuzsa Weiner for the joint work, and everyone at the Computer Science Department of the Eötvös Loránd University for being very helpful throughout my research period there.

Notation

Finite Desarguesian projective spaces $\mathrm{PG}(n,q)$ are all formed from the underlying Galois fields $\mathrm{GF}(q)$. Hence q is a power of p, where p is prime.

Let V_{n+1} be the $(n+1)$-dimensional vector space over $\mathrm{GF}(q)$ with origin $\mathbf{O}$. Consider the following relation on $V_{n+1} \setminus \{\mathbf{O}\}$: elements $\mathbf{x} = (x_1, x_2, ..., x_{n+1})$ and $\mathbf{y} = (y_1, y_2, ..., y_{n+1})$ are in relation if there is a $0 \neq \lambda \in \mathrm{GF}(q)$ for which $x_i = \lambda y_i$ for every $i = 1, 2, ..., n+1$. This is an equivalence relation, and the equivalence classes correspond to the 1-dimensional subspaces of V_{n+1}, the points of $\mathrm{PG}(n,q)$. A point is represented by any of the vectors from the given equivalence class. (The set of equivalence classes is the set of points of $\mathrm{PG}(n,q)$).

An m-dimensional subspace or *m-space* of $\mathrm{PG}(n,q)$ is the set of points all of whose representing vectors form (together with the origin) a subspace of dimension $m+1$ of V_{n+1}. A subspace of dimension zero has already been called a point; subspaces of dimension one and two are called *line* and *plane* respectively. Subspaces of dimension $n-1$ are called *hyperplanes*. Hyperplanes are represented similarly to the points by n-tuples. A point is incident with a hyperplane if and only if the scalar product of their coordinate vectors is zero.

Throughout this paper we will work in the finite Desarguesian projective space $\mathrm{PG}(n,q)$ and its affine part $\mathrm{AG}(n,q)$. The order of the space (plane) is q. For these spaces (planes) standard representations will be used, see [26].

The points of $\mathrm{AG}(2,q)$ have *affine coordinates*, represented by pairs, where the elements of the pairs are elements of $\mathrm{GF}(q)$. The lines of $\mathrm{AG}(2,q)$ have equation $mX + b - Y = 0$ or $X = c$, where m is the slope of the line. The *infinite points* can be identified with slopes, so (m) defines the infinite point of lines with slope m. In the same way (∞) will be the infinite point of the vertical lines, that is the lines with equation $X = c$. Instead of *infinite* the term *ideal* is also used in the text. The ideal points together with $\mathrm{AG}(2,q)$ are the projective closure of $\mathrm{AG}(2,q)$, which is $\mathrm{PG}(2,q)$ defined above.

For vectors we use boldface letters. If $\mathbf{x} = (x_1, x_2, .., x_n)$ then by $\mathbf{x}^b$ we mean $\mathbf{x} = (x_1^b, x_2^b, ..., x_n^b)$. The same applies for the notation of matrices H, the exponent is considered elementwise (for each entry in the matrix).

In this paper for the multiplicative subgroup of $\mathrm{GF}(q)$ we use the notation

$(\mathrm{GF}(q), \cdot)$. Finally, we note that blocking sets are usually denoted by B, some other sets linked to blocking sets by S and ovoids by O. Generally (but not always), capital letters stand for points, lower case letters for lines and greek letters for spaces.

The thesis tries to follow the usual notation found in the literature.

Chapter 1

Introduction

1.1 Basic definitions

1.1.1 Minimal blocking set

A *blocking set* in a projective plane is a set of points which intersects every line. Lines that intersect the blocking set B in exactly one point of B are called *tangents*. A line intersecting B in k points ($k > 0$) is called a *k-secant* or simply a *secant*. A point P of a blocking set B is called *essential*, if $B \setminus \{P\}$ is not a blocking set. Geometrically, a point is essential if there is a tangent line at P, that is, a line intersecting B just at P. A blocking set is said to be *minimal*, when no proper subset of it is a blocking set, or, equivalently if each point of the blocking set is essential. Note that a minimal blocking set in a projective plane is either a line, or does not contain a line. A blocking set is called *trivial* if it contains all points from a line. It is straightforward to check that lines are the smallest blocking sets. If there is exactly one tangent t to B at P, then P is called a *critical point*, and t a *critical tangent*. Blocking sets for which there is a line l such that $|B \setminus l| = q$ are said to be *Rédei blocking sets* (or blocking sets of *Rédei-type*). Such a line l is called a *Rédei line* of the blocking set. Blocking sets are also characterized by their sizes; a blocking set is *small* if its size is less than $3(q+1)/2$, and *large* if its size is greater than $3q - 3$. Note that in this thesis we mainly investigate blocking sets in the plane, which are also called *planar* blocking sets.

1.1.2 Unital and Hermitian curve

A pointset U of $\mathrm{PG}(2,q)$ is called a *unital* if it has $q\sqrt{q}+1$ points, and every line intersects it in 1 or $\sqrt{q}+1$ points. The *Hermitian curve* is a classical unital; it is a curve projectively equivalent to the curve defined by the following equation:

$$X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1} = 0$$

or equivalently in matrix form,

$$\mathbf{x}^{\sqrt{q}} H \mathbf{x}^T = 0$$

such that $H = (H^{\sqrt{q}})^T$ is a Hermitian matrix.

The set $\mathcal{H}$ of points of such a curve form a *unital*, that is, its size is $q\sqrt{q}+1$ and it meets every line in 1 or $\sqrt{q}+1$ points. (We shall call these lines *tangents* and *secants*, respectively.)

There is a unique tangent at each point of $\mathcal{H}$, while through a point not on the curve there are $\sqrt{q}+1$ tangents.

Tangents through a point $P \notin \mathcal{H}$ meet $\mathcal{H}$ in collinear points, the corresponding secant is called the *polar* of P and denoted by $P^\perp$, and vice versa, tangents at points of a secant ℓ are concurrent at a point called the *pole* of ℓ and denoted by $\ell^\perp$.

All secants meet the curve in a Baer subline. The Baer sublines $\mathrm{PG}(1,q)$ of $\mathrm{PG}(1,q^2)$ form the blocks of a $3-(q^2+1,q+1,1)$ design, that is an inversive (or Möbius) plane. This means that three points determine a unique Baer subline, and two sublines meet in at most two points.

1.1.3 High dimensional structures

An *embedding* is an injective (one-to-one) mapping, where the (original) incidence properties are invariant under the mapping.

A projective space $\mathrm{PG}(n,q)$ embedded in $\mathrm{PG}(n,q^k)$ is called a *subgeometry*. When $n=2$ it is called a *subplane* and when $k=2$ it is the *Baer subgeometry* of dimension n. For $n=k=2$ they are the *Baer subplanes*.

A *blocking set with respect to k-dimensional subspaces* in $\mathrm{PG}(n,q)$ is a set B of points which intersects every k-dimensional subspace. Sometimes they are called k-blocking sets.

An *oval* is a set of points that every line meets in 0,1 or 2 points such that there is exactly one tangent at each of its points.

A *spread* of $\mathrm{PG}(n,q)$ is a set F of r-dimensional subspaces of $\mathrm{PG}(n,q)$, if the elements of F partition the points of $\mathrm{PG}(n,q)$.

An *ovoid* O is a set of q^2 points in $\mathrm{PG}(3,q)$ such that no three points of O are on the same line of $\mathrm{PG}(3,q)$. We will only consider classical ovoids (i.e. non-singular elliptic quadrics Q_3) in $\mathrm{PG}(3,q)$ that have q^2+1 points. These have canonical equation $Q_3 = F(x_1,x_2) + x_3x_4$ for some coordinate system, where F is an irreducible quadratic polynomial.

Consider three subspaces of $\mathrm{PG}(n,q)$, namely γ, π and a subspace V disjoint both from γ and π. Then by a *projection of a point* $P \in \gamma$ from V onto π we mean the unique intersection of π and the space spanned by P and V, $\langle P, V\rangle$. By a *projection of* γ *from* V *onto* π we mean the pointwise projection of γ.

Consider two disjoint subspaces π and V in a projective space. Let O be a substructure contained entirely in π. A *cone* with base O and vertex V is the union of the connecting lines (considered as a pointset) of the points of O to the points of V.

1.2 Upper and lower bounds

Here we are going to discuss the minimal and maximal sizes a minimal blocking set can have in the plane. For $q = 2$ we have the Fano plane, and as Neumann and Morgenstern observed in the 1940's there are no minimal blocking sets in this case. Therefore, we always consider q to be greater than 2.

A lower bound for the size of minimal blocking sets was given by Bruen [17] and Pelikán.

Theorem 1.1 (Bruen and Pelikán, [17]) *Non-trivial minimal blocking sets of* $\mathrm{PG}(2,q)$ *contain at least* $q+\sqrt{q}+1$ *points. If there is equality, then the minimal blocking set is a Baer subplane.*

Theorem 1.1 is combinatorial, that is it holds for any projective plane of order $q > 2$. There are much better lower bounds when q is not a square and the plane is Desarguesian.

Theorem 1.2 (Blokhuis, [8]) *If q is a prime, then the size of a non-trivial blocking set is at least $\frac{3(q+1)}{2}$. If $q = p^h$ is neither a square nor a prime, then the size of a non-trivial blocking set is at least $q + \sqrt{pq} + 1$.*

The lower bound was further improved by Blokhuis, Storme and Szőnyi [15].

Theorem 1.3 (Blokhius, Storme, Szőnyi, [15]) *If $q = p^h$, h is odd, then $|B| \geq q + 1 + c_p q^{2/3}$, where $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$.*

Theorem 1.4 (Szőnyi, [41]) *Let B be a non-trivial minimal blocking set in $\mathrm{PG}(2, q)$, $q = p^n$. Suppose that $|B| < 3(q+1)/2$. Then*

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

for some integer e, $1 \leq e$.

In the particular case when $q = p^2$, the previous theorem has the following corollary.

Corollary 1.5 *Let $q = p^2$ and B be a non-trivial minimal blocking set which is not a Baer subplane. Then $|B| \geq 3(q+1)/2$.*

The result about the intervals was improved by Sziklai [40], who showed that only the intervals with $e|n$ are nonempty. He also proved that the (p^e+1)-secants of the blocking set are sublines.

An upper bound for the size of minimal blocking sets was given by Bruen and Thas [19].

Theorem 1.6 (Bruen and Thas, [19]) *If B is a minimal blocking set of $\mathrm{PG}(2, q)$ then $|B| \leq q\sqrt{q} + 1$. In case of equality B is a unital (and q is square).*

PROOF. Let t be the number of tangents of B, and consider the non-tangent lines: $L_1, ..., L_N$, where $N = q^2 + q + 1 - t$. Let $n_j = |L_j \cap B|$, $j = 1, ..., N$. Counting the pairs (point of B, lines through this point) and (a pair of points of B, connecting lines through these points) we get that $\sum n_j = |B|(q+1) - t$ and $\sum n_j(n_j - 1) = |B|(|B| - 1)$. Summing these two equations gives $\sum n_j^2 = |B|^2 + |B|q - t$. Using the inequality between the geometric and arithmetic means gives

$$N \sum_{j=1}^{N} n_j^2 \geq (\sum_{j=1}^{N} n_j)^2$$

that is $(q^2 + q + 1 - t)(|B|^2 + |B|q - t) - (|B|q + |B| - t)^2 \geq 0$.

Some easy calculations give $(|B|^2 + q^2 + q + 1 - |B|q - 2|B|)t - |B|(q^3 + q^2 + q - |B|q) \leq 0$.

As B is minimal $t \geq |B|$, and the coefficient of t is positive. Replacing t by $|B|$ still gives the calculated inequality. Rearranging gives then $|B| \leq q\sqrt{q} + 1$. In case of equality $t = |B|$ and every non-tangent line meets B in exactly $\sqrt{q}+1$ points. ■

An improvement on the Bruen-Thas upper bound is possible, as we now show, see [4].

Theorem 1.7 (Szőnyi, Cossidente, Gács, Mengyán, Siciliano, Weiner, [4])
Suppose B is a minimal blocking set in $\mathrm{PG}(2, q)$, *$q \neq 5$, and denote by s the fractional part of $\sqrt{q}$. Then $|B| \leq q\sqrt{q} + 1 - \frac{1}{4}s(1-s)q$.*

Note that this always implies at least a $1/8\sqrt{q}$ improvement on the Bruen–Thas upper bound. On the other hand, it is easy to see that if q is not too close to a square, then this implies a cq improvement.

Before the proof of Theorem 1.7, we need a lemma, which is also used in the proof of Turán's theorem on graphs containing no K_r (see Lovász, [33]).

Lemma 1.8 *Let $a_1, ..., a_n$ be integers with $a_1 + ... + a_n = N$. Then $a_1^2 + ... + a_n^2 \geq N(2\alpha + 1) - n\alpha(\alpha + 1)$, where α denotes the integer part of N/n. If equality holds, then all the a_is are the same or they take two different values according as N/n is an integer or not.*

PROOF. Note that $(a-1)^2+(b+1)^2 < a^2+b^2$ whenever $a > b+1$. This shows that if we have integers $a_1, ..., a_n$ taking at least three values, we can decrease the sum of their squares (without changing their sum) by changing an appropriately chosen pair (a_i, a_j) to (a_i-1, a_j+1). So starting with $a_1 = N, a_2 = ... = a_n = 0$, after finitely many steps we end up with a multiset $\{a_1, ..., a_n\}$ consisting of at most two values, α and $\alpha+1$. It is easy to see that if N/n is integer, then we can only have one value, which is N/n; while for N/n non-integer, α has to be the integer part of N/n.

If we know that the multiset $\{a_1, ..., a_n\}$ consists of α-s and $(\alpha+1)$-s, we can determine the number k of α-s using the equation $k\alpha+(n-k)(\alpha+1) = N$. This gives $k = n(\alpha+1) - N$, hence the minimum is $k\alpha^2 + (n-k)(\alpha+1)^2 = N(2\alpha+1) - n\alpha(\alpha+1)$. ■

Proof of Theorem 1.7 The proof works only for $q \geq 53$, for smaller values see the remark after the proof.

Write $b = |B| = q\sqrt{q}+1-\epsilon$ and let $r = [\sqrt{q}]$, the integer part of $\sqrt{q}$. From the Bruen–Thas upper bound we know that $\epsilon > 0$, we need $\epsilon \geq 1/4s(1-s)q$. Denote by $a_1, ..., a_{q^2+q+1}$ the intersection sizes of B with lines. Since B is minimal, we can suppose that $a_1 = \cdots = a_b = 1$. From standard double counting, we find

$$\sum_{i=b+1}^{q^2+q+1} a_i = b(q+1) - b = bq; \tag{1.1}$$

$$\sum_{i=b+1}^{q^2+q+1} a_i(a_i-1) = b(b-1). \tag{1.2}$$

Finally, the sum of these two equations gives

$$\sum_{i=b+1}^{q^2+q+1} a_i^2 = b(b-1+q). \tag{1.3}$$

We wish to use Lemma 1.8. Here $n = q^2+q+1-b$ and $N = bq$. $N/n = \frac{bq}{q^2+q+1-b} = \frac{q}{(q^2+q+1)/b-1}$ is increasing in b and for $b = q\sqrt{q}+1$ it is $\sqrt{q}+1$, so $N/n < \sqrt{q}+1$. We prove that if $N/n \leq r+1$, then $b \leq q\sqrt{q}+1-\frac{1}{4}s(1-s)q$ automatically holds, so $\alpha = [N/n] = r+1$ can be supposed.

$N/n \leq r+1$ is equivalent to $b \leq \frac{(r+1)(q^2+q+1)}{q+r+1}$. We need that the right hand side is at most $q\sqrt{q}+1-1/4s(1-s)q$. We consider the even stronger inequality

$$\frac{(r+1)(q^2+q+1)}{q+r+1} \leq q\sqrt{q}+1-1/4sq.$$

Replacing r with $\sqrt{q}-s$ and after a little calculation we find the following equivalent form:

$$0 \leq sq(3/4q-5/4\sqrt{q}+3/4+1/4s^2),$$

this is true for $q \geq 53$.

Now Lemma 1.8 and (1.3) imply that

$$b(b-1+q) \geq (2r+3)bq-(q^2+q+1-b)(r+1)(r+2).$$

Replacing r with $\sqrt{q}-s$ and after a little manipulation, we find

$$b^2-(2q\sqrt{q}+3q+3\sqrt{q}+3)b+(q^2+q+1)(q+3\sqrt{q}+2)+$$

$$+s(2q+2\sqrt{q}+3-s)b-s(q^2+q+1)(2\sqrt{q}+3-s) \geq 0,$$

which is equivalent to

$$(b-q\sqrt{q}-1)(b-q\sqrt{q}-3q-3\sqrt{q}-2)$$

$$-s\{(q^2+q+1)(2\sqrt{q}+3-s)-(2q+2\sqrt{q}+3-s)b\} \geq 0.$$

Hence

$$\epsilon = q\sqrt{q}+1-b \geq s\frac{(q^2+q+1)(2\sqrt{q}+3-s)-(2q+2\sqrt{q}+3-s)b}{q\sqrt{q}+3q+3\sqrt{q}+2-b} =$$

$$2s\frac{(\sqrt{q}+1)(q^2+q+1)-(q+\sqrt{q}+1)b}{q\sqrt{q}+3q+3\sqrt{q}+2-b}+s(1-s)\frac{q^2+q+1-b}{q\sqrt{q}+3q+3\sqrt{q}+2-b}.$$

Replacing b with $q\sqrt{q}+1-\epsilon$ and after some calculation, we find

$$\epsilon \geq 2s\frac{\epsilon(q+\sqrt{q}+1)}{3(q+\sqrt{q}+1)+\epsilon-2}+s(1-s)\frac{q^2+q+1-q\sqrt{q}-1+\epsilon}{3q+3\sqrt{q}+1+\epsilon.} \qquad (1.4)$$

Now the best we can get from $\epsilon \geq \frac{1}{4}s(1-s)q$ is $\frac{q}{16}$, so we can suppose $\epsilon \leq \frac{q}{16}$. After this, an easy calculation shows that, if $q \geq 49$ holds, then the second term on the right hand side of (1.4) is at least $s(1-s)\frac{q}{4}$. Since the first one is non-negative, we are done. ■

Remark 1.9 *For $q < 53$, a case by case application of Lemma 1.8 yields the result of Theorem 1.7. Furthermore, the direct use of the lemma gives slightly better bounds in several cases. For $q = 5$, the union of three lines minus the intersection points is a blocking set of size 12, showing that in this case the Bruen–Thas upper bound is tight.*

Remark 1.10 *Note that the proof of Theorem 1.7 is combinatorial, so the result is true for any projective plane of order $q \geq 53$. Again using Lemma 1.8 directly, all values less than 53 can be ruled out except for 26.*

1.3 The spectrum

Under the term *spectrum* we mean a characterization of blocking sets (or other structures) with respect to their sizes. As already described previously: the smallest size for a blocking set in $\mathrm{PG}(2,q)$ after $q+1$ (the size of a line) is $q+\sqrt{q}+1$ with equality if and only if q is square and the set is a Baer subplane, and the biggest possible size is $q\sqrt{q}+1$ with equality if and only if q is square and the set is a unital. The spectrum can be divided into four major parts, into the following intervals:

I. $[q+\sqrt{q}+1, \frac{3(q+1)}{2})$ (small minimal blocking sets)

II. $[\frac{3(q+1)}{2}, 2q-2]$

III. $[2q-1, 3q-3]$

IV. $(3q-3, q\sqrt{q}+1]$ (large minimal blocking sets)

The reason the intervals are divided like this is mainly due to the different possible techniques and approaches connected to them. Small minimal blocking

sets are partly characterized, for blocking sets from the second interval mainly constructions are known. In the third interval there is a minimal blocking set for all sizes, while large minimal blocking sets are rare.

There are several survey papers about blocking sets. (See Blokhuis [9], [10], Szőnyi, Gács, Weiner [45], and Chapter 13 of the second edition of Hirschfeld's book [26] also contains a lot of recent results).

1.4 Related notions

A *tangency set* S is a set of points such that every point $P \in S$ has a tangent, in other words there exists a line l at P such that $S \cap l = \{P\}$. The tangeny set S is *maximal* if no further point can be added to it preserving the tangency property; that is none of whose supersets are tangency sets [18].

Minimal blocking sets are all maximal tangency sets. The notion of maximal tangency sets is more general than that of minimal blocking sets as was shown in [18], because for q even, an oval is a maximal tangency set, but clearly not a minimal blocking set. Note that a maximal tangency set that is a blocking set is also a minimal blocking set.

A *flag* of PG$(2, q)$ is an incident point-line pair (P, r). A set of flags $B = \{(P_1, r_1), ..., (P_k, r_k)\}$ is a *strong representative system* if and only if $P_i \in r_j$ means $i = j$. B is *maximal* if it is maximal subject to inclusion [27, 13]. By the *pointset* of a strong representative system we mean the union of the points from the pairs, that is the points $\bigcup_1^k \{P_i\}$.

It is easy to see that the idea of strong representative system is closely linked to tangency sets, namely the pointset of a strong representative system is a tangency set, and a tangency set is the pointset of some strong representative systems. There is a one to one correspondence between tangency sets and strong representative systems if all points are critical.

Furthermore, the notion of strong representative system is also a generalization of the notion of minimal blocking set: any minimal blocking set can be represented as a strong representative system by taking the set of points together with one of their tangents. We note that the representation is unique if there is exactly one tangent at each point of the minimal blocking set. On

the other hand, there are strong representative systems that do not arise from minimal blocking sets, see [27].

Some of the previous results about minimal blocking sets extend to strong representative systems or tangency sets. For example, Theorem 1.6 was proved for maximal tangency sets by Illés, Szőnyi, Wettl [27]. The lower bound (Theorem 1.1) was also extended to tangency sets, as Bruen and Drudge proved in [18] that a maximal tangency set is either a line, or an oval and q is even, or its size is at least $q + \sqrt{q} + 1$.

1.5 Constructional methods

Below we describe the constructions that are the topics of this thesis and which are often used in finite geometry. We only give an overview of these, the concrete applications will be included in the parts where we apply them to solve certain questions. Some problems require additional methods from algebra, like Weil's estimate, but these constructions themselves are geometrical in nature. We note that usually, if several of the constructions are applied in combination to solve a problem, the results tend to be stronger and more general.

1.5.1 Embeddings

Embeddings play an important role for constructions in planes (spaces) whose order is not a prime. The usual ingredient in these constructions is a certain type of structure (like a minimal blocking set) that is known to exist in the plane (space) to be embedded. By a careful embedding the resulting structure will still be of the same type as the original, although its size and other properties may be markedly different. In such a way we get new structures of the same type in the larger plane (space).

One of the simplest embeddings is that of embedding a plane $\mathrm{PG}(2, q)$ into $\mathrm{PG}(2, q^h)$. If $h = 2$ then $\mathrm{PG}(2, q)$ is a Baer subplane, for which the available literature is huge; but even for $h > 2$ a lot of trivial facts can be said, like a line of $\mathrm{PG}(2, q^h)$ intersects $\mathrm{PG}(2, q)$ in no point, one point or exactly $q + 1$ points, a line of $\mathrm{PG}(2, q)$ is contained in at most one line of $\mathrm{PG}(2, q^h)$. Even such simple

observations will prove adequate to describe some nice new results [1].

Other embedding methods are more complex, they may require several consecutive embeddings. Generally we start with a minimal blocking set (the structure of given type) and embed this into a larger space. We form a cone with base the minimal blocking set and vertex disjoint from the embedded space, and then either project the cone onto a plane of the large space or use properties of the cone to derive a new minimal blocking set. In these constructions the blocking property is usually automatically fulfilled, but minimality depends on the actual setting [4, 37, 45].

1.5.2 Partitioning with curves

In some consructions we need to partition the affine part of $\mathrm{PG}(n, q)$ with curves. A trivial way to do this in the plane is to simply consider the q vertical lines through the infinite vertical point, but more often we need this partitioning to satisfy certain conditions, like having as few elements as possible, so more elaborate structures are needed than lines. Such structures may be unitals, like disjoint Hermitian curves or parabolas according to the parabola construction of Szőnyi [43] (these are described later). Although the just mentioned examples work in the plane, it is easy to see that a partitioning of the affine part of $\mathrm{PG}(n, q)$ is always possible (using any construction that partitions the affine plane) by considering cones, whose bases are the curves and their vertex the same infinite point disjoint from the bases. As long as the bases are disjoint, the cones will be disjoint as well.

In other constructions we may need to partition the whole of $\mathrm{PG}(n, q)$, and not just the affine part. This may also be done using curves, but more often we use the concept of spread.

1.5.3 Random Choice

The probabilistic method was invented by Erdős, and the simplest form is just a counting technique for existence proofs. Standard sources for the probablistic method are the books by Alon and Spencer [5] and Erdős and Spencer [20]. One ingredient of the technique as we will use it is to find a certain blocking set

within a structure depending on the particular problem. This should be done by random choice; as this probability argument is always trivial this method is called trivial random choice. By this we mean that one simply determines the number of possible choices for a structure of a given size, then gives an upper bound on the number of "bad choices" (choices not satisfying the prescribed conditions) which is still smaller than the number of possible choices. This ensures that there is at least one structure of prescibed type; in fact as we will use the method here later, this ensures that of the "good choices" (the structures of prescribed type) there will be more than polynomial of. The interesting fact is that although trivial random choice may seem very imprecise, it still provides some strong and interesting results.

A more thorough account of the probabilistic method and a survey of its applications in finite geometry can be found in [24], where Gács and Szőnyi systematically take into account all the known applications of this method.

1.5.4 Adding and deleting points

Given a prescribed structure B one may try to add some points to it, and then delete some original points (points of B) such that the resulting structure is still of the type of B. If the added and deleted points are well chosen then this method can be considered as the non-random random choice, because we only choose from a pool of "good" choices. Therefore it is closely connected to the random choice method, and as we shall apply it to the method using subsets.

For consider a minimal blocking set B. We would like to construct a minimal blocking set of different size from this. We can investigate then points that may be added and points that consequently must be deleted. The difficulty usually lies in determining the deleted points. As we will see in certain cases, where particular subsets are used, it is quite easy to determine the set of deleted points. In other cases it is also possible that the number of added points is small, and this fact itself determines the deleted points.

More on this method can be found in an article by Béres and Illés [7].

1.5.5 The Rédei construction, subsets and cosets

Rédei blocking sets arise from a particular construction. Let $U = \{(a_i, b_i) : i = 1, ..., q\}$ denote a q-element pointset in $\mathrm{AG}(2, q)$. Given such a pointset U in $\mathrm{AG}(2, q)$, we call a point (m) on the line at infinity *determined* if $m = (b_i - b_j)/(a_i - a_j)$ for some points (a_i, b_i) and (a_j, b_j) in U. The infinite point of the vertical lines is determined if there are two points of U on any of the vertical lines. In this case we also say that U determines the direction m, and denote the set of determined directions by D; the set of non-determined directions will be denoted by D^c. A trivial way to construct a blocking set of size $q + |D|$ in $\mathrm{PG}(2, q)$ is to place q points in $\mathrm{AG}(2, q)$ and consider these together with the determined points from the line at infinity. When U is the graph of a function, this construction is called Rédei's construction. Conversely, if B is a minimal blocking set of size $q + |D|$ with $|D| < q + 1$ and there is a line l such that $|B \setminus l| = q$ then the blocking set can be obtained by Rédei's construction. This can be done by a suitable change of coordinates that makes $B \setminus l = U$ the graph of a function f, and then $B \cap l$ is the set of directions determined by U. From the definition of Rédei blocking sets we deduce that these are of size at most $2q + 1$.

Working with certain subsets of $\mathrm{GF}(q)$ that have nice and well-known algebraic properties makes calculations and constructions easier (or simply possible) in $\mathrm{PG}(n, q)$. Hereby the properties of the subsets aid in solving the given problem, provide the algebraic fabric. One example that is often used in connection to blocking sets are subgroups and their cosets. In this case instead of simply placing some points in the plane, we place points that are determined by cosets. We often say that we place some cosets on a line through the origin, and by this we mean the affine points $\{(x, y, 1) : x \in \text{some cosets of } \mathrm{GF}(q)\}$ or $\{(x, y, 1) : y \in \text{some cosets of } \mathrm{GF}(q)\}$. Doing this in some cases makes it quite simple to estimate the set of determined directions. This is so in particular if we consider the Rédei construction, and place q/s cosets on lines in the affine plane, where s is the size of the cosets (as we will show later).

1.6 Weil's theorem and its variants

A *plane curve* over a field K is the equivalence class of homogeneous polynomials in three variables, where two polynomials are equivalent if they are constant multiples of each other. This means that multiple components are allowed. The degree of the curve is just the degree of the polynomial. A curve is called *absolutely irreducible* if it is irreducible over the algebraic closure of K. A point of the curve f is called *K-rational*, if its coordinates are in K. A point of the curve f is *singular* if all three partial derivatives of f vanish at this point. Weil's theorem gives a surprisingly strong bound for the number of $\mathrm{GF}(q)$-rational points of absolutely irreducible curves defined over $\mathrm{GF}(q)$. First we state it for non-singular plane curves. Note that non-singularity obviously implies absolute irreducibility.

Theorem 1.11 (Weil, [47]) *Let C be a non-singular plane curve of degree d, defined over GF(q), and denote by N the number of its GF(q)-rational points. Then*

$$|N - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

In most of the applications, one cannot guarantee that the curve is non-singular; but in this form the result is true for singular absolutely irreducible curves, too.

In order to apply Weil's theorem a technical difficulty still remains: one has to check whether the curve is absolutely irreducible or not. In this thesis we shall always use special curves for which absolute irreducibility can be proved. One way of proving absolute irreducibility is the study of singular points and the use of Bézout's theorem, see [44]. In most of the applications in combinatorics, the character sum version of Weil's theorem is used (see Weil [47]). This has the advantage that instead of absolute irreducibility a much simpler condition has to be checked. This theorem, due essentially to Burgess, can be found as Theorem 5.41 in the book [32] by Lidl and Niederreiter.

Theorem 1.12 (Burgess, [32]) *Let χ be a multiplicative character of GF(q) of order k and let $f(x)$ be a polynomial of degree d which cannot be written as*

$f(x) = cg(x)^k$. Then

$$|\sum_{x \in GF(q)} \chi(f(x))| \leq (d-1)\sqrt{q}.$$

The biggest advantage of the character sum version of Weil's theorem is that it can easily be extended to a system of equations. We wish to prescribe that certain one variable polynomials $f_i(x)$, $(i = 1, \ldots, m)$ take square or non-square values. (This can be considered as a system of equations by putting $(f_i(x))^{(q-1)/2} = \pm 1$.) Under some light and natural conditions one can show that such a system of equations has approximately $q/2^m$ solutions, where m is the number of equations. This supports the intuitive idea that being a square is a "random event with probability 1/2".

Theorem 1.13 (Szőnyi, [43]) *Let $f_1(x), \ldots, f_m(x) \in GF(q)[x]$ be given polynomials. Suppose that no partial product $f_{i_1}(x) \ldots f_{i_j}(x)$ $(1 \leq i_1 < i_2 < \ldots i_j; j \leq m)$ can be written as a constant multiple of a square of a polynomial. If $2^{m-1} \sum_{i=0}^{m} \deg(f_i) \leq \sqrt{q} - 1$, then there is an $x_0 \in GF(q)$ such that $f_i(x_0)$ is a non-square for every $i = 1, \ldots, m$. More precisely if we denote the number of these x_0's by N, then*

$$\left| N - \frac{q}{2^m} \right| \leq \sum_{i=1}^{m} \deg(f_i) \frac{\sqrt{q}+1}{2}.$$

Another form of Weil's estimate is a result of Sziklai [39].

Theorem 1.14 (Sziklai, [39]) *Let $f_1, ..., f_m \in \mathrm{GF}(q)[X]$ be a set of polynomials such that no partial product $f_{i_1}^{s_1} f_{i_2}^{s_2} ... f_{i_j}^{s_j}$ $(1 \leq j \leq m; 1 \leq i_1 < i_2 < ... < i_j \leq m; 1 \leq s_1, s_2, ..., s_j \leq d-1)$ can be written as a constant multiple of a d-th power of a polynomial, where $d|(q-1)$, $d, m \geq 2$. Denote by N the number of solutions $\{x \in \mathrm{GF}(q) : f_i(x)$ is a d-th power in $\mathrm{GF}(q)$ for all $i = 1, ..., m\}$. Then $|N - \frac{q}{d^m}| \leq \sqrt{(}q) \sum_{i=1}^{m} deg f_i$.*

Chapter 2

Constructions in space

The main aim of the chapter is to give a demonstration of the embedding and partitioning methods by solving a problem connected to strong representative systems. We will need the following simple dimension argument of subspaces: given an r-dimensional subspace and an s-dimensional subspace, with the dimension of their intersection equal to m and the dimension of their span equal to t, we have $r + s = m + t$.

2.1 The André, Bruck-Bose representation

For the generalized Buekenhout construction (to be introduced later) that employs the embedding constructional method we need a suitable high dimensional representation of the plane that stems from spreads.

Theorem 2.1 (Bruck and Bose, [16]) *There is a spread in* $\mathrm{PG}(n, q)$ *containing* r*-dimensional subspaces if and only if* $(r + 1)|(n + 1)$.

Construction 2.2 *Let* F *be a spread of* $\mathrm{PG}(2t - 1, q)$ *comprised of* $(t - 1)$*-dimensional subspaces. Embed* $\mathrm{PG}(2t - 1, q)$ *into* $\mathrm{PG}(2t, q)$*, and consider it as the infinite hyperplane of* $\mathrm{AG}(2t, q)$*. Define the following incidence structure* A*:*

The points of A *are the points of* $\mathrm{AG}(2t, q) = \mathrm{PG}(2t, q) \setminus \mathrm{PG}(2t - 1, q)$,

The lines of A are the t-dimensional subspaces π_t of $\mathrm{PG}(2t,q)$ for which $\pi_t \cap \mathrm{PG}(2t-1,q) \subset F$ (that is the t-dimensional subspaces intersecting the ideal hyperspace in an element of F),

Incidence between points and lines of A is subset inclusion,

The infinite points of A are the spread elements.

Proposition 2.3 *The structure A defined in Construction 2.2 is a projective plane of order q^t.*

PROOF. The number of points of A and $\mathrm{PG}(2t,q)$ are both equal to $q^{2t}+q^t+1$; through every point of A there are q^{t+1} distinct lines as there are the same number of spread elements of F. On each line of A there are q^t+1 points, because π_t contains q^t affine points and there is exactly one infinite point for each corresponding to the spread element.

The dimensions imply that through any two points there is exactly one line (t-dimensional subspace) and on any two lines there is exactly one point. ■

Remark 2.4 *One always gets translation planes by Construction 2.2 (these are planes for which the affine part for a suitable line at infinity has a point-transitive translation group). In particular, the Desarguesian plane $\mathrm{PG}(2,q^t)$ can be obtained by Construction 2.2. The corresponding spreads are called* regular.

This high dimensional representation is called the *André, Bruck-Bose representation* of the plane.

2.2 A general cone construction

Construction 2.5 *Let O be an elliptic ovoid of a 3-space π, and embed π in $\mathrm{PG}(h+2,q)$ with $h \geq 2$. Construct the cone B in $\mathrm{PG}(h+2,q)$ with base O and vertex V, an $(h-2)$-space disjoint from π.*

Proposition 2.6 *The cone B in Construction 2.5 blocks all planes in* $\mathrm{PG}(h+2,q)$. *Furthermore, a plane not meeting the vertex V contains either* 1 *or* $q+1$ *points from B. Any* 3*-space disjoint from V meets B in* q^2+1 *points.*

PROOF. Choose a 3-space disjoint from V. Project the points of γ from V onto π. Since γ is also disjoint from V, the $(h-1)$-space $\langle P, V\rangle$ intersects γ in P only, hence this projection yields a one-to-one correspondence between the points of $B\cap\gamma$ and $B\cap\pi$. Since $B\cap\pi$ is the ovoid O, therefore $|B\cap\gamma| = q^2+1$.

To show that B blocks all planes of $\mathrm{PG}(h+2,q)$, choose a plane β. We may assume that $\beta\cap B=\emptyset$. Denote by β' the projection of β from V onto π. From the definition this projection is a one-to-one correspondence between the points of $B\cap\beta$ and $B\cap\beta'$. As the planes of π meet O in either 1 or $q+1$ points the statement holds. ■

The idea behind all blocking set constructions starting with the André, Bruck-Bose representation is that a point set intersecting every h-space in the underlying $\mathrm{PG}(2h,q)$ yields a blocking set in the plane $\mathrm{PG}(2,q^h)$ as the set of lines of $\mathrm{PG}(2h,q)$ is a certain subset of corresponding h-spaces. Consequently, the cone B described above is such a set, since any h-dimensional subspace of $\mathrm{PG}(2h,q)$ intersects the $(h+2)$-dimensional subspace of the cone in at least a plane. The only difficulty is in assuring the minimality of the blocking set in $\mathrm{PG}(2,q^h)$. Choosing the properties of the embedding carefully, we get minimal blocking sets. For the construction presented above, the next two remarks hold.

Proposition 2.7 *Let R be a point of $B\setminus V$. Project R from V onto π to obtain R'. Denote by α_R the unique tangent plane at R' in π. Then*

(1) the tangent planes of B at R are contained in the $(h+1)$-space $\langle\alpha_R, V\rangle$,

(2) B is a minimal blocking set with respect to planes.

PROOF. For (1) simply observe that the projection of a tangent plane at R from V onto π is α_R. For (2), first of all, note that any plane in $\langle\alpha_R, V\rangle$ through R which is not intersecting V is a tangent plane of B at R, hence the points of $B\setminus V$ are essential. Now pick a line l in π, so that it is skew to O. Then for any

point P of V, the plane $\beta := \langle l, P\rangle$ meets B in P only. Otherwise if $Q \in \beta \cap B$, $Q \neq P$, then the line $\langle Q, P\rangle$ was contained in B and so the intersection of l and $\langle Q, P\rangle$ was a point in B. Hence the points of V are also essential. ■

Proposition 2.8 *For the cone B of Construction 2.5 the following hold.*

(1) The $(h-1)$-spaces through V are either contained in B or meet B in V only.

(2) Denote by W the $(h-1)$-space spanned by the vertex V and the point T of O. Then for any h-space Z through W, $|(Z \setminus W) \cap B|$ is either 0 or q^{h-1}.

PROOF. (1) is immediate from the construction of B. For (2), note that the $(h-1)$-space W intersects π in a point exactly, and Z intersects π in a line l through T. So $Z \cap B$ consists of one or two $(h-1)$-spaces through V according as l is a 1-secant (tangent) or a 2-secant of O. ■

2.3 The generalized Buekenhout construction

The following construction is called the generalized Buekenhout construction[1].

Construction 2.9 *Consider the André, Bruck-Bose representation of the plane* $\mathrm{PG}(2, q^h)$. *Let S be the $(h-1)$-spread of the hyperplane H at infinity of* $\mathrm{PG}(2h, q)$, *defining the plane* $\mathrm{PG}(2, q^h)$. *Let O be an ovoid of a 3-space π and embed π in an $(h+2)$-space M. Construct a cone B in M with base O and vertex V, an $(h-2)$-space disjoint from π. Embed now M into* $\mathrm{PG}(2h, q)$ *in such a way that an element ρ of the spread S is generated by the vertex V and exactly one point T of the ovoid O; the hyperplane H is otherwise disjont from B.*

[1]The term generalized Buekenhout construction was implicitly used in [4]. Explicitly it appeared in [3], although referred to as a special case. Here we consider this to be the general case, although modifications exist, (see [4]), because this resembles the original Buekenhout construction the most.

The generalized Buekenhout construction is a special case of Construction 2.5, therefore the propositions from above apply. Moreover, in a series of statements (some being the reformulation of the propositions from above) we prove that B, considered as a point set of $\mathrm{PG}(2, q^h)$ is a minimal blocking set, and also derive some combinatorial properties.

Remark 2.10 *Consider a plane α in M disjoint from V. $\alpha' := \langle V, \alpha\rangle \cap \pi$ is a plane in π. It is easy to see that $\langle \alpha, V\rangle = \langle \alpha', V\rangle$. A point of α' and V generate a space meeting α in one point. This gives a one-to-one correspondence between points of α and points of α'. Hence α meets B in either 1 or $q+1$ points.*

The next lemma analyzes the embedding of M into $\mathrm{PG}(2h, q)$. Denote by M' the infinite part of M (that is, $M \cap H$). In the following two lemmas whenever we talk about an h-space through an element of S, we mean an h-space not contained in H.

Lemma 2.11 *(i) M' contains one element of S and meets the other members of the spread in a line;*

(ii) a 1 co-dimensional subspace U of M' meeting ρ in precisely V contains q^{h-2} of the lines in (i) and meets the other members of the spread in a point;

(iii) an h-space through ρ is either contained in M or their affine part is disjoint;

(iv) an h-space through a spread element different from ρ meets M in a plane;

Proof. (i) We know that M', which is an $h+1$ space, contains a spread element, namely ρ. The other members of the spread meet M' in at least a line (by a dimension argument), and since they are disjoint from ρ, the intersections must be lines (there is no room in M' for ρ and a disjoint 2-space).

For (ii) note that U either meets the spread elements in a line or in a point. U is partitioned by these points, lines and V. All in all we have $q^h + 1$ objects in the partition. A little counting shows that the number of lines is q^{h-2}.

For (iii) note that through a spread element h-spaces arise by taking the space generated by an affine point and the spread element.

By dimensions, an h-space meets M in at least a plane. On the other hand, if the h-space is through a spread element, then it has to be disjoint from ρ, hence the intersection cannot be bigger (again by dimensions). This proves (iv). ■

Putting together the remark and the previous lemma, we have the following.

Lemma 2.12 *(i) An h-space through ρ meets the affine part of M in either 0 or q^{h-1} points. The latter arises when the h-space is generated by ρ and a point of O different from T.*

(ii) An h-space not through ρ meets the affine part of M in either 1 or $q+1$ points.

(iii) Take an affine point P of O and denote by α_P the tangent plane of O at P (within π). Then h-spaces through spread elements that are tangents at an affine point of $\langle V, P\rangle$ meet M within $\langle V, \alpha_P\rangle$.

PROOF.

(i) All h-spaces through ρ within M can be generated by ρ and a point of π different from T. If this point is in O, then the affine part contains $1+(q-1)\,|V| = q^{h-1}$ points of B. Otherwise the intersection in the affine part is empty.

(ii) If an h-space is not through ρ, then by Lemma 2.11 it meets M in a plane, and by Remark 2.10 the intersection is 1 or $q+1$.

(iii) Suppose h is an h-space meeting B only in the point Q. By Lemma 2.11 h meets M in a plane α_Q, and by Remark 2.10 $\langle V, \alpha_Q\rangle = \langle V, \alpha_P\rangle$, hence $\alpha_Q \subseteq \langle V, \alpha_P\rangle$. ■

Theorem 2.13 (Szőnyi, Cossidente, Gács, Mengyán, Siciliano, Weiner, [4]) *Considering B as a point set of $\mathrm{PG}(2, q^h)$ we find a minimal blocking set B' with the following properties.*

(i) The size of B' is $q^{h+1} + 1$;

(ii) B' has a unique infinite point Y. There are q^2 lines through Y meeting B' in $q^{h-1} + 1$ points, the rest of the lines through Y are tangents;

(iii) lines not through Y are either tangents or $(q+1)$-secants;

(iv) through an affine point of B' there are q^{h-2} tangents, $q^h - q^{h-2}$ $(q+1)$-secants and one $(q^{h-1}+1)$-secant;

(v) if P' and P'' are affine points of B' on the same $(q^{h-1}+1)$-secant, then infinite points of tangents through P' are the same as infinite points of tangents through P''.

Proof. The spread element ρ (generated by V and T) becomes a point Y in $\mathrm{PG}(2, q^h)$, the only ideal point of B'. Lines through Y correspond to h-spaces through ρ, so (ii) follows from Lemma 2.12 (i).

For (iii) note that a line in $\mathrm{PG}(2, q^h)$ not through Y corresponds to an h-space through a spread element different from ρ, so we can apply Lemma 2.12 (ii).

(i) and (iv) follow from (ii) and (iii) by simple counting.

For (v) let $\langle P, V\rangle$ correspond to the $(q^{h-1}+1)$-secant with a $P \in O$ and choose a $Q \in \langle P, V\rangle$. By Remark 2.10 and Lemma 2.12 a tangent h-space through Q (corresponding to a tangent line of B') meets M in a plane α_Q within $\langle V, \alpha_P\rangle$. This plane meets M' in a line. This line is contained in the infinite part of $\langle V, \alpha_P\rangle$, a 1 co-dimensional subspace of M'. Hence the spread element within the tangent h-space in question is one of the q^{h-2} spread elements mentioned in Lemma 2.11 (ii). But by the just proved (iv) there are exactly q^{h-2} tangents through any point of $\langle P, V\rangle$ (that is, through any affine point of the $(q^{h-1}+1)$-secant in question). Hence the infinite points of tangents through any affine point of the $(q^{h-1}+1)$-secant in question are exactly the points corresponding to spread elements meeting $\langle \alpha, V\rangle$ in a line (and not in a point). ■

Remark 2.14 *If $l_1, l_2, ..., l_{q^2}$ denotes the $(q^{h-1}+1)$-secants and I_i $(i = 1, ..., q^2)$ the infinite points of tangents through points on l_i, then these I_i-s partition the infinite points different from Y into sets of cardinality q^{h-2}.*

PROOF. This is a direct consequence of (v) of the previous lemma. ■

Remark 2.15 *Since we did not use properties of the spread, the constructions work for translation planes, too. For example, Theorem 2.13 is valid for translation planes of order q^h (if the nucleus of the coordinatizing quasifield is $\mathrm{GF}(q)$).*

2.4 Some more results

Here we present some results obtained using the generalized Buekenhout construction or modifications of it.

Theorem 2.16 (Szőnyi, Cossidente, Gács, Mengyán, Siciliano, Weiner, [4])
In $\mathrm{PG}(2, q^h)$, $h \geq 3$, there are minimal blocking sets of size $q^{h+1} + q^{h-3} + 1$ and $q^{h+1} + 1$.

Let $2q^h + 2q^h \log q^h \leq b \leq q^{h+1} + 1$. Then there is a minimal blocking set B^* in $\mathrm{PG}(2, q^h)$ so that $b \leq |B^*| \leq b + q^{h-1}$.

In $\mathrm{PG}(2, q^h)$, $h > 2$, there are minimal blocking sets of size $q^{h+1}+1+b(q^{h-2}-1)$, for every $0 \leq b \leq q$.

Using non-classical ovoids as bases Mazzocca and Polverino generalized the method from [4].

Theorem 2.17 (Mazzocca and Polverino, [35]) *In $\mathrm{PG}(2, q^n)$, $n \geq 6$ and $q = 3^h$ with $h \geq 1$, there exist minimal blocking sets of size $q^{n+2} + 1$ and also of size greater than $q^{n+2} + q^{n-6}$.*

Further results can be found in the cited literature ([4, 35]).

2.5 Partitioning the flags

In the following three subsections we are going to consider a problem originally stated by András Gyárfás in [21]. The problem is equivalent to partitioning the flags of $\mathrm{PG}(2,q)$ into as few strong representative systems as possible. We show three possible solutions, the third being the nicest and most complex; for it we must use partitioning and embedding as well. Although the first two are constructions in the plane, we include them here as they clearly show the power of the embedding method. In addition, the first method, also called the trivial estimate, will be used in the final proof of the embedding method, and we also follow the idea of the second method (the Illés, Szőnyi, Wettl method) when considering the embedding method.

2.5.1 The trivial estimate

If we do not employ any of the constructional methods, simply use a geometric argument, the best we can get is the trivial estimate. This works for any q.

Lemma 2.18 (Trivial estimate) *The flags of* $\mathrm{PG}(2,q)$ *can be partitioned into* q^2+2q *strong representative systems.*

Proof. We work in $\mathrm{AG}(2,q) \subset \mathrm{PG}(2,q)$. Consider the set of flags (P_i, r_i), $i = 1, ..., q$, where the P_i-s are on the same vertical line $l(\neq l_\infty)$, and r_i is a non-vertical line through P_i, as a strong representative system. As the r_i-s run through every non-vertical line through their corresponding P_i-s, we get q disjoint strong representative systems. Repeating the procedure above for the remaining $q-1$ vertical lines $(\neq l_\infty)$ we can partition almost all flags into q^2 strong representative systems.

To finish the proof, we have to add strong representative systems partitioning the flags (P,r), where r is a vertical line or the line at infinity and the flags (P,r), where P is an infinite point and r is any line through P. To this aim we define two types of strong representative systems:

(P_i, r_i), $i = 1, ..., q$, where the P_i-s are on the same horizontal line l, and r_i is the vertical line through P_i;

(P_i, r_i), $i = 1, ..., q$, where the r_i-s are non-vertical lines through the same point P, and P_i is the infinite point of r_i.

If one lets l run through horizontal lines in the first case, and P run through points of a fixed vertical line, then these yield an additional $2q$ number of strong representative systems. In this way we have partitioned all flags except for the flag (Y, l_∞), where Y denotes the infinite point of the vertical lines, but this can be added to any of the aformentioned q^2 sets. ■

2.5.2 The Illés, Szőnyi, Wettl method

In [27] the maximal size of a strong representative system was shown to be $q\sqrt{q}+1$, which is also the maximal size of minimal blocking sets. From this upper bound follows that at least roughly $q\sqrt{q}$ strong representative systems are needed to partition all flags, as the number of flags is approximately q^3. Illés, Szőnyi and Wettl proved that this is indeed the case for q an odd square.

Theorem 2.19 (Illés, Szőnyi, Wettl, [27]) *The flags of* $\mathrm{PG}(2,q)$*, q an odd square, can be partitioned into* $(q-1)\sqrt{q}+3q$ *strong representative systems.*

To prove Theorem 2.19, Illés, Szőnyi and Wettl used unitals as large minimal blocking sets arising from the parabola construction [43]. Their method involved partitioning the affine plane with these minimal blocking sets, and mapping such a minimal blocking set into another in a way that permuted the tangents in the affine points. Finally, the uncovered flags were covered with strong representative systems resembling the ones the trivial estimate described.

It is straightforward to show that the same method of proof applied in [27] can be used to verify Theorem 2.19 for q an even square, too. If we consider the Hermitian curve given by the equation $x^{\sqrt{q}+1} + y^{\sqrt{q}}z + z^{\sqrt{q}}y = cz^{\sqrt{q}+1}$, $c \in GF(\sqrt{q})$, then this curve contains only the point $(0,1,0)$ on the line at infinity, and so the method in [27] can be applied.

Theorem 2.20 (Mengyán, [3]) *The flags of* $\mathrm{PG}(2,q)$*, q square, can be partitioned into* $(q-1)\sqrt{q}+3q$ *strong representative systems.*

PROOF. We divide the proof into three steps.

Step 1. Partition the affine points of PG$(2, q)$ into Hermitian curves.

The Hermitian curve $\mathcal{H} : x^{\sqrt{q}+1} + y^{\sqrt{q}}z + z^{\sqrt{q}}y = cz^{\sqrt{q}+1}$ in the affine plane becomes the Hermitian curve $\mathcal{H}' : x^{\sqrt{q}+1} + y^{\sqrt{q}} + y = c$, where $c \in GF(\sqrt{q})$. Then

$$\dot{\bigcup_{c \in GF(\sqrt{q})}} \mathcal{H}' = \mathrm{AG}(2, \mathrm{q})$$

Step 2. Partition almost all flags using the Hermitian curves $\mathcal{H}'$.

Here we use the fact that the tangents to the curve through the same infinite point meet the curve at points (of the curve) which all lie on the same vertical line. (This is essentially the pole-polar property of the Hermitian curve mentioned in the Introduction chapter.) Delete the y-axis from the unitals in order to be able to use the affinity $\lambda : (x, y) \to (x, \lambda y)$ for the remaining points that modifies the slope of the tangents. The affinity λ takes the Hermitian curves $\mathcal{H}'$ to Hermitian curves $\lambda(\mathcal{H}')$. If λ runs over all non-zero elements of $GF(q)$, then we obtain each flag (P, r) precisely once where P is an affine point not lying on the y-axis and r is a line through P which is neither horizontal nor vertical. These add up to $(q-1)\sqrt{q}$ number of strong representative systems.

Step 3. Partition the remaining flags of PG$(2, q)$.

The remaining flags are the following type: the flags (P, r) where P is on the y-axis or the line at infinity and r is arbitrary, and where P is an affine point not on the y-axis and r is either horizontal or vertical. We define three types of strong representative systems.

$\mathbf{A}_c = \{((u, c, 1), v_u) : u \in GF(q) \setminus 0\} \cup \{((1, v, 0), r_v) : v \neq 0, r_v \text{ is the line } y = -vx + c\} \cup \{((1, 0, 0), v_{c+1})\}$

$\mathbf{B}_c = \{((c, w, 1), h_c) : w \in GF(q)\} \cup \{((w, 1, 0), r_\infty) : w \in GF(q)\}$

$\mathbf{C}_m = \{((0, t, 1), l_t) : t \in GF(q), l_t \text{ is the line } y = mx + t\} \cup \{((0, 1, 0), v_m) \text{ :if } m \neq 0\}$

These together add up to $3q$ number of strong representative systems as c, w, t, m runs through $GF(q)$. In this way we have partitioned all flags except the flags (P, r) where $r = v_0$ is the y-axis or $P = (0, 1, 0)$, $r = l_\infty$. These flags can be added to our Hermitian curves as the number of Hermitian curves is more than $q + 2$. ■

We stress that we have used the partitioning method here.

2.5.3 The embedding method

In this section we investigate the more general case when q^h is not a prime. For this, we consider the generalized Buekenhout construction which produces minimal blocking sets of size $q^{h+1} + 1$ in $\mathrm{PG}(2, q^h)$. We repeat the trick of partitioning the affine plane with copies of the affine part of this blocking set, where each blocking set will give rise to several strong representative systems.

For the following lemma we require particular non-singular elliptic quadrics in affine form. Here we must distinguish between the q odd and the q even case when determining non-singularity.

For q odd, the affine quadratic form $z = x^2 + ky^2 + dx + ey + f$, where $d, e, f, k \in GF(q)$ and $-k$ is a fixed non-square is non-singular as can be easily deduced, since in the q odd case the general quadratic solution formula can be used. (The discriminant is then a square).

Now let $q = 2^h$. Consider the following quadric:

$$ax^2 + bxy + cy^2 + dxw + eyw + fw^2 + zw = 0$$

We want to determine values a, b, c, d, e, f for which this simplifies to the canonical form:

$$F(x, y) + wz' = 0, z' = dx + ey + fw + z$$

In this case F must be irreducible. For a, b, c this means:

$$ax^2 + bxy + cy^2 = 0$$

$$a(\frac{x}{y})^2 + b\frac{x}{y} + c = 0$$

$$ax'^2 + bx' + c = 0, x' = \frac{x}{y}$$

If $b = 0$ then $ax^2 + cy^2 = 0$ so $x = \sqrt{\frac{c}{a}}$.
Assume $b \neq 0$. Let $u = ax'/b$ and $\delta = ac/b^2$.

$$a(\frac{ub}{a})^2 + b\frac{ub}{a} + \frac{\delta b^2}{a} = 0$$

$$u^2b^2 + ub^2 + \delta b^2 = 0$$

$$u^2 + u + \delta = 0$$

Consider the trace Tr_2 of GF(q) into GF(2). Then $Tr_2(t)^2 + Tr_2(t) = 0$, where $t \in F_{2^h}$. This means $Tr_2(\delta) = 1$ is required for irreducibility. If h is odd, then $a = c = b = 1$ gives the result. If h is even, then $a = b = 1$ and c can be cosen so that $Tr_2(c) = 1$ as the Tr function is surjective. We have thus found a suitable c and consequently a suitable F. The following elliptic quadratic surface

$$x^2 + xy + cy^2 + dxw + eyw + fw^2 + zw = 0$$

is in affine coordinates

$$ax^2 + bxy + cy^2 + dx + ey + f + z = 0$$

that is

$$z = ax^2 + bxy + cy^2 + dx + ey + f$$

is a non-singular affine quadratic form. (For further details see also Hirschfeld's book [26], pages 3-4 and pages 101-102.)

Lemma 2.21 *Let $F(X,Y)$ denote a homogeneous irreducible quadratic polynomial over* $\mathrm{GF}(q)$ *and consider the following affine equation:*

$$Z = F(X,Y) + aX + bY + c.$$

As a, b and c run through all elements of $\mathrm{GF}(q)$*, we find q^3 elliptic quadrics with the following properties:*

(i) $(0,0,1,0)$ *is the unique infinite point of all the quadrics;*

(ii) every affine point is on q^2 quadrics;

(iii) for any incident (P,α) pair with P an affine point and α a plane not through $(0,0,1,0)$*, there is exactly one quadric through P for which α is a tangent plane (at P).*

Proof. It is easy to check that the q^3 elliptic quadrics have $(0,0,1,0)$ as the only point at infinity. (See [26], pages 101-102 for the fact that these are elliptic quadrics).

For (ii) note that after fixing x, y and z, the number of solutions for $z - xa - yb - F(x,y) = c$, is q^2.

For (iii) recall that the tangent plane of the quadric $Z = F(X,Y) + aX + bY + c$ at the point $(x,y,z,1)$ is the plane through the point and orthogonal to the vector $(F'_X(x,y) + a, F'_Y(x,y) + b, -1, a + b + 2c - z)$ (see [26]). It is easy to see that for fixed x, y and z this vector uniquely determines a, b and c. As all quadrics contain $(0,0,1,0)$, no tangent plane in question can pass through this point. ■

Lemma 2.22 *Suppose that in the generalized Buekenhout construction we fix everything apart from O and let O run through all ovoids from Lemma 2.21 with T corresponding to the point* $(0,0,1,0)$*. Then we find q^3 minimal blocking sets of* $\mathrm{PG}(2,q^h)$ *with the same unique infinite point that cover q^2 times the affine points of M.*

PROOF. As $\langle \pi, V \rangle = M$, and $\pi \setminus H$ was covered q^2 times this is also true for the affine part of M. (Any point in $\langle P, V \rangle$, $P \in \pi \setminus H$, is covered as many times as P.) ■

Lemma 2.23 *Pick two minimal blocking sets from Lemma 2.22 sharing the point $P \in M \setminus H$. Then the tangents to P will meet the line at infinity in disjoint pointsets (both of size q^{h-2}) for the two cases.*

PROOF. $\langle V, P \rangle$ meets π in a point P', this should be a common point of O_1 and O_2, the two ovoid bases for the two minimal blocking sets. From Lemma 2.21 we know that the tangent planes α_1 and α_2 at P' have to be different. On the other hand, by Lemma 2.12 (iii), an h-space corresponding to a common tangent through P would meet M in a plane (disjoint from V) within $\langle \alpha_1, V \rangle \cap \langle \alpha_2, V \rangle = \langle \alpha_1 \cap \alpha_2, V \rangle$. This is not possible by dimensions. ■

Corollary 2.24 *Let U denote the points of* $\mathrm{PG}(2, q^h)$ *(considered in the André, Bruck-Bose representation) corresponding to the affine points of an $(h+2)$-dimensional subspace M. Then one can partition all incident (point,line) pairs with the points chosen from U and lines not through a fixed infinite point Y, into q^{h+1} strong representative systems.*

PROOF. Take the q^3 minimal blocking sets considered in Lemma 2.22. Each of them gives rise to q^{h-2} strong representative systems as follows. Using the notations of Remark 2.14 (after fixing a blocking set) choose an infinite point from each of the I_i-s and consider all tangents (and points of tangencies) through each of them. This is a strong representative system of size q^{h+1}. Let the chosen points run through all points of the corresponding I_i-s simultaneously to find q^{h-2} strong representative systems. Finally, repeat this for all q^3 blocking sets.

By Lemmas 2.22 and 2.23 every point of U will occur in q^2 blocking sets and all tangents will be different, hence a point is in $q^2 \cdot q^{h-2} = q^h$ flags, this is the number of lines through the point (except for the one joining the point to Y). The number of strong representative systems used is $q^3 \cdot q^{h-2} = q^{h+1}$. ■

Theorem 2.25 (Mengyán, [3]) *The flags of* $\mathrm{PG}(2,q^h)$, $h \geq 2$, *can be partitioned into* $q^{2h-1}+2q^h$ *strong representative systems.*

PROOF. Denote by H the hyperplane at infinity of $\mathrm{PG}(2h,q)$ and partition the affine part with $(h+2)$-dimensional subspaces through a fixed $(h+1)$-dimensional subspace within H. This (through the André, Bruck-Bose representation) gives rise to a partitioning of the affine part of $\mathrm{AG}(2,q^h)$ into q^{h-2} sets corresponding to affine parts of $(h+2)$-spaces like in Corollary 2.24. Taking strong representative systems guaranteed by the corollary, we find a partition of almost all the flags of the affine plane (into $q^{h+1}q^{h-2}=q^{2h-1}$ strong representative systems) except for one parallel class of lines. Hence to finish the proof we have to add strong representative systems partitioning the uncovered flags as in the second part of Lemma 2.18 giving an additional $2q^h$ strong representative systems. ■

In graph theoretic terminology we can thus answer the original question of Gyárfás [21] on the strong chromatic index of the point-line incidence graph of $\mathrm{PG}(2,q)$, for q not a prime. For this we recall that a *strong colour class* in a graph G is a set of independent edges with the extra property that this set of edges is an induced subgraph of G, i.e. there are no edges in G joining two end-points of different edges in this strong colour class. Consider now the point-line incidence graph G of $\mathrm{PG}(2,q)$ (that is, the points and lines are the two colorclasses and the edges are the flags of $\mathrm{PG}(2,q)$). In G a strong colour class is a strong representative system. The *strong chromatic index* of a graph G is the minimum number of colours in an edge-colouring with the property that the edges having the same colour form a strong colour class. Geometrically, for G this chromatic index is the minimum number of strong representative systems covering the flags of $\mathrm{PG}(2,q)$, the very question we have set out to solve.

Corollary 2.26 *The strong chromatic index of the bipartite graph corresponding to* $\mathrm{PG}(2,q^h)$, q^h *a non-prime, is at most* $q^{2h-1}+2q^h$.

We note that when q is prime no methods are presently known that are better than the trivial estimate. This is connected to the limit of the application of the embedding method to the non-prime case, and lack of knowledge of large minimal blocking sets partitioning the affine plane (space).

Chapter 3

Constructions in the plane

In this chapter we will use constructional methods to answer a question originally asked by György Turán whether the number of minimal blocking sets of a given size is more than polynomial. The term more than polynomial[1] refers to a function that grows faster than any polynomial of the variable, i.e. a function of the form $f(q) = q^{g(q)}$, where $\lim_{q\to\infty} g(q) = \infty$.

3.1 Random constructions in the plane

3.1.1 The parabola construction

The arguments here are based on a paper by Szőnyi [43], where the author proves the existence of a minimal blocking set of size between $cq \log q$ and $Cq \log q$. The idea of all constructions of the paper was to take the union of parabolas and either prove that they form a minimal blocking set, or add some extra points to make the set a blocking set and consider the minimal blocking set inside the constructed set. First we summarize some easy observations from [43].

Lemma 3.1 *Let $q \equiv 1(4)$ and $T \subseteq \mathrm{GF}(q)$. Set $\mathcal{B} = \{(x, x^2 + a, 1) : x \in \mathrm{GF}(q), a \in T\} \cup (0, 1, 0)$. Then the following hold:*

- *(i) There is a tangent through every point of $\mathcal{B}$ if and only if the difference of any two elements in T is a non-square of $\mathrm{GF}(q)$;*

[1] Some authors call this superpolynomial.

- *(ii)* $\mathcal{B}$ *is a blocking set if and only if for any* $s \in \mathrm{GF}(q) \setminus T$ *there is a* $t \in T$ *such that* $t - s$ *is a square in* $\mathrm{GF}(q)$*;*

- *(iii) for an* $s \in \mathrm{GF}(q) \setminus T$ *the points of the parabola* $\{(x, x^2 + s, 1) : x \in \mathrm{GF}(q)\}$ *are either all on at least one tangent to* $\mathcal{B}$ *or none of them is on any tangent;*

- *(iv) the point* $(a, b, 1)$ *is on a tangent of* $\mathcal{B}$ *if and only if there is a* $t \in T$ *such that* $t - b + a^2$ *is a square in* $\mathrm{GF}(q)$*.*

Hence taking T to be maximal with respect to the property that the difference of any two elements of T is a non-square, we find a minimal blocking set. It is difficult to determine the size of such a T. For a lower bound one has to use Theorem 1.13.

Applying this theorem it is easy to see that if $|T| < c_1 \log_2 q$ (where $c_1 < \frac{1}{2}$ and q is large enough), then one can find an $s \in \mathrm{GF}(q)$ such that $s - t$ is a non-square for every $t \in T$, hence to make $\mathcal{B}$ become a blocking set B, we need $|B| = 1 + q\,|T| \geq 1 + c_1 q \log_2 q$. The problem is that we cannot give an upper bound on the size of $\mathcal{B}$, for instance if q is a square, then T can be taken to be a multiplicative coset of the subfield $\mathrm{GF}(\sqrt{q})$ giving a minimal blocking set of size $q\sqrt{q} + 1$. The trick sketched in Szőnyi's paper is to let $|T| = c_1 \log_2 q$ (for a fixed $c_1 < \frac{1}{2}$) and try to add points (but hopefully not whole parabolas) to $\mathcal{B}$ to complete it to a minimal blocking set. The following lemma from [22] handles a very general setting for random choice, which could be used here.

Lemma 3.2 *Let* G *be a bipartite graph with bipartition* $L \cup U$*. Suppose that the degree of vertices in* U *is at least* d*. Then there is a set* $L' \subseteq L$*,* $|L'| \leq |L|(1 + \log |U|))/d$*, such that any* $u \in U$ *is adjacent to a vertex of* L'*.*

To complete $\mathcal{B}$ to a blocking set $\mathcal{B}'$, we have to add points blocking all lines not blocked by $\mathcal{B}$. These will be found by using Lemma 3.2. We will not be able to guarantee that the resulting blocking set is minimal, all we can do is to assure that the points of $\mathcal{B}$ will still have their tangents (this will then guarantee that the minimal blocking set contained in the constructed blocking set is of

size at least $|B|$). For this, we will only choose from those points, which are on no tangents of $\mathcal{B}$.

Let the vertex class U (of a bipartite graph) correspond to the lines not blocked by $\mathcal{B}$ and the vertex class L correspond to points of $\mathrm{PG}(2,q)$ which lie on no tangents of $\mathcal{B}$. Draw an edge between a point of U and a point of L if they correspond to an incident (point,line) pair. To use Lemma 3.2, we have to bound $|U|$, $|L|$ and the minimum degree d in U.

For an upper bound on U, one can simply take $|U| \leq q^2$.

For an upper bound on L, note that by Lemma 3.1 (iii), $|L| = ql$, where l is the number of elements $s \in \mathrm{GF}(q) \setminus T$ such that $s - t$ is a non-square for all $t \in T$. By Theorem 1.13 $l \leq \frac{q}{2^{|T|}} + \frac{\sqrt{q}+1}{2}|T| < 2q^{1-c_1}$.

To find a lower bound on d, consider a line $X_1 = mX_0 + bX_2$ not blocked by $\mathcal{B}$. By Lemma 3.1 (iv) we have to count the number of points $(x, mx+b, 1)$ such that $t - (mx+b) + x^2$ is a non-square for all $t \in T$. Using Theorem 1.13 (for the polynomials $t - (mx+b) + x^2$) we have that this number is at least $\frac{q}{2^{|T|}} - (\sqrt{q}+1)|T| \geq \frac{1}{2}q^{1-c_1}$ for large enough q.

Applying Lemma 3.2 gives that we need to add at most $|L|\frac{1+\log|U|}{d} \leq c_2 q \log q$ points to $\mathcal{B}$ to find a blocking set $\mathcal{B}'$ (note that here we have $\log q$, while for the size of $\mathcal{B}$ we had $\log_2 q$, but these two are constant multiples of each other). This will have the property that through points of $\mathcal{B}$ we have tangents, hence the size of the minimal blocking set inside $\mathcal{B}'$ is between $c_1 q \log_2 q = cq \log q$ and $c_1 q \log_2 + c_2 q \log q = Cq \log q$.

Theorem 3.3 (Mengyán, [2]) *There are constants c and C such that for $q \equiv 1 \pmod 4$, the number of non-isomorphic minimal blocking sets in $\mathrm{PG}(2,q)$ of size from the interval $[cq \log q, Cq \log q]$ is more than polynomial.*

Proof. First we count the number of ways one can choose the set T. The first point of T can be arbitrary, the number of choices for the second one is exactly $\frac{q-1}{2}$,..., for the last point, by Theorem 1.13, we still have at least $\frac{q}{2^{|T|-1}} - \frac{\sqrt{q}+1}{2}(|T|-1) \geq q^{1-c_1}$ choices. Hence the number of ways to choose T is at least $(q^{1-c_1})^{|T|}$. In a resulting minimal blocking set there are at most $C \log q$ parabolas, hence at most $\binom{C\log q}{|T|} < (C \log q)^{|T|}$ different T-s can give the same minimal blocking set. Thus all in all we have constructed at least

$$(\frac{q^{1-c_1}}{C\log q})^{|T|}$$

minimal blocking sets, this is more than polynomial. ■

A similar argument (also based on a construction sketched in Szőnyi's paper) works for the case $q \equiv 3 \pmod 4$ showing that again there are more than polynomial minimal blocking sets of size approximately $cq\log q$. In this case approximately half of the points from the considered parabolas (here again Theorem 1.13 determines the parabolas) are included in the minimal blocking set.

3.1.2 Blocking sets arising from a Hermitian curve

It is easy to see that the properties of a Hermitian curve $\mathcal{H}$ (described in the Introduction) imply that if we delete all but one points from a $(\sqrt{q}+1)$-secant of $\mathcal{H}$ and add the pole of this line, then we find a minimal blocking set $\sqrt{q}-1$ smaller than $\mathcal{H}$. This is the adding and deleting points method. Throughout the section we try to iterate this procedure.

Construction 3.4 *Given a Hermitian curve $\mathcal{H}$ consider a point $P \in \mathcal{H}$ and its tangent t. Choose lines $l_1, ..., l_i$ through P different from t. Delete all points of $\mathcal{H}$ on these lines except for P and add to the set the poles $l_1^\perp, ..., l_i^\perp \in t$. If $i \leq \sqrt{q}$, then the resulting set is a minimal blocking set of size $q\sqrt{q}+1-i(\sqrt{q}-1)$.*

Theorem 3.5 (Mengyán, [2]) *There are more than polynomial minimal blocking sets in* $\mathrm{PG}(2,q)$*, q square, of size $q\sqrt{q}+1-i(\sqrt{q}-1)$, where $\log q < i \leq \sqrt{q}$.*

Proof. In Construction 3.4 we have more than $\binom{q}{\log q}$ choices for the deleted secants. This is more than polynomial. ■

Construction 3.4 works only for $i \leq \sqrt{q}$; for $i \geq \sqrt{q}+1$ we might delete all points of a $\sqrt{q}+1$ secant (not through P). This means that the adding and deleting method is insufficient by itself, and the trivial random method must be applied.

In what follows we restate and use results from [4], where the above mentioned problem is handled. First we restate Theorem 4.2 from that paper.

Theorem 3.6 (Szőnyi, Cossidente, Gács, Mengyán, Siciliano, Weiner, [4]) *For an arbitrary square prime power q there is a minimal blocking set in* $\mathrm{PG}(2,q)$ *for any size in the interval* $[4q\log q, q\sqrt{q}-q+2\sqrt{q}]$.

Now we follow the proof of this theorem with some necessary modifications.

Lemma 3.7 *Let P be a point of a Hermitian curve $\mathcal{H}$, m a $(\sqrt{q}+1)$-secant not through P. Then there exists a set A of secants through P of size at most $3\sqrt{q}\log q+1$ with the following properties:*

(1) all but one secant in A meet m in a point outside $\mathcal{H}$;

(2) the points of $\mathcal{H}$ on secants in A block all secants to $\mathcal{H}$ not through P.

Proof. We use Lemma 3.2. Choose a line l_1 through P meeting m in a point of the curve. Let the vertices in L correspond to secants through P meeting m in a point outside the curve and the vertices in U correspond to secants not through P not blocked by points of $\mathcal{H}$ on l_1. Draw an edge between a vertex of U and a vertex of L if and only if the corresponding lines meet in a point of $\mathcal{H}$. We have $|L| = q-\sqrt{q}-1$, $|U|\leq q^2$.

Next we prove that the minimum degree in U is at least $\sqrt{q}-1$. For this we recall that as $\mathcal{H}$ is classical all secants to $\mathcal{H}$ meet $\mathcal{H}$ in a Baer subline. If the degree of some vertex in U was less than $\sqrt{q}-1$, then this would correspond to a secant $m^{'}\neq m$ not through P that meets at most $\sqrt{q}-2$ secants (corresponding to vertices of L) in a point outside the curve. Consider the $\sqrt{q}+1$ lines $l_1,...,l_{\sqrt{q}+1}$ of P meeting m inside $\mathcal{H}$. Since the degree of $m^{'}$ is at most $\sqrt{q}-2$, $m^{'}$ must meet at least three of these lines in a point of $\mathcal{H}$. Using the fact that the points of $\mathcal{H}\cap m'$ form a Baer subline and that three points (respectively lines) uniquely determine a Baer subline (respectively Baer pencil), we deduce that the points in $m^{'}\cap\mathcal{H}$ are exactly the points $l_i\cap m^{'}$ $(i=1,...,\sqrt{q}+1)$. But then l_1 blocks $m^{'}$ contrary to the assumption, so we deduce $d\geq\sqrt{q}-1$. An easy calculation shows that Lemma 3.2 guarantees the existence of the set A. ■

Construction 3.8 *Let $\mathcal{H}$ be a Hermitian curve, $P \in \mathcal{H}$, t the tangent through P. Let m be a secant not through P. Let l_1 be a line through P meeting m in a point of $\mathcal{H}$. Partition all the non-tangent lines through P to sets A,B,C,D,E with the following properties:*

(1) Let A be a set coming from Lemma 3.7, $l_1 \in A$. Add to A the polar line of $m \cap t$. Hence $|A| \leq 3\sqrt{q}\log q + 2$;

(2) $B \cup C$ are the lines through P (besides l_1) meeting m in a point of $\mathcal{H}$.

Delete the point $l \cap m$ for all $l \in B$ and delete all points of $\mathcal{H}$ from the lines of C and D, except for P. Add to the set poles of deleted lines. Finally, add the pole of m.

This results in a set of size $q\sqrt{q} + 2 - |B| - |C \cup D|(\sqrt{q} - 1)$.

Lemma 3.9 *The set given in Construction 3.8 is a minimal blocking set.*

PROOF. With the introduced notation A blocks all secants not through P, secants through P are blocked by P and the added points block the tangents of deleted points. Remaining points of $\mathcal{H}$ have their original tangents except for $l_1 \cap m$ that has m as tangent and for P that has tangents from $C \cup D$. Finally, the added points have the tangents of deleted points. ■

Theorem 3.10 (Mengyán, [2]) *In* PG$(2, q)$ *there are more than polynomial non-isomorphic minimal blocking sets for any size in the interval* $\left[5q\log q, q\sqrt{q} - 2q\right]$ *whenever q is a square.*

PROOF. For a minimal blocking set of size $k \in [5q\log q, q\sqrt{q} - 2q]$ write $k = q\sqrt{q} + 2 - R(\sqrt{q} - 1) - Q$ with $0 \leq Q \leq \sqrt{q} - 2$. An easy calculation shows that here $q - 5\sqrt{q}\log q + \sqrt{q} \geq R \geq 2\sqrt{q} + 1$. If we use Construction 3.8 with $|B| = Q$ and $|C \cup D| = R$, the resulting blocking set is of size k. After choosing B and C, D can be chosen in $\binom{q-(\sqrt{q}+1)-|A|+1}{|D|} > \binom{q-4\sqrt{q}\log q}{|D|}$ ways. The bounds for R imply $\sqrt{q} + 1 \leq |D| \leq q - 5\sqrt{q}\log q + \sqrt{q}$, hence the binomial coefficient is more than polynomial in q. ■

3.2 The method of subsets and cosets

3.2.1 Blocking sets from a triangle

In this part we will use subsets. Originally, this involved the addition and deletion method, where one could determine the properties of the deleted points for certain added points. These observations were then described in the terminology of subsets. In essence (with the terminology mentioned in the first chapter) we place subsets (the added points) on lines and delete some subsets from other lines. The conditions on the added subsets ensure that these structures are minimal blocking sets. Moreover, as we add two subsets H and K for this purpose; one is used to control the size of the minimal blockig set as required, the other gives the more than polynomial choices.

Below we prove the following theorem.

Theorem 3.11 (Mengyán, [2]) *In* $\mathrm{PG}(2,q)$ *there are more than polynomial non-isomorphic minimal blocking sets for any size in the interval* $[2q-1, 3q-4]$ *whenever* q *is odd or* q *is even and* $q-1$ *is not a prime.*

For this purpose we construct minimal blocking sets of size between $2q-1$ and $3q-4$ using particular subsets. All constructions can be considered as generalizations of the IMI construction originally due to Innamorati, Maturo [28] and Illés, Szőnyi, Wettl [27]. This and all the generalizations start from the following minimal blocking set:

$$\triangle = \{(x,0,1) : x \neq 0\} \cup \{(0,y,1) : y \neq 0\} \cup \{(1,y,0) : y \neq 0\}.$$

Hence we take three sides of a triangle with the vertices removed[2].

First we recall the original construction.

Construction 3.12 *(IMI) Choose a set* $K \subset \mathrm{GF}(q) \setminus \{0\}$ *such that* $1, -1 \in K$. *The set*

$$I_K = \triangle \cup \{(1,y,1) : y \in K\} \setminus (\{(1,y,0) : y \in K\} \cup \{(0,y,1) : y \in K\})$$

[2]This is also called the *vertexless triangle*.

is a minimal blocking set of size $3q - 3 - |K|$.

The IMI construction gives minimal blocking sets for each value in the interval $[2q - 1, 3q - 4]$. It is easy to see, that whenever K has to have size between $\sqrt{q}$ and $q - \sqrt{q}$, then the number of choices is more than polynomial. Hence the construction automatically gives the following.

Theorem 3.13 *There are more than polynomial minimal blocking sets for any size in the interval* $[2q + \sqrt{q}, 3q - \sqrt{q}]$.

However, for the intervals $[3q - \sqrt{q}, 3q - 4]$ and $[2q - 1, 2q + \sqrt{q}]$ we will have to generalize the IMI construction in two different ways.

Construction 3.14 *Suppose* K, $H \subset \mathrm{GF}(q) \setminus \{0\}$ *satisfy the following conditions:*

(1) $-H = H$;

(2) $(1 - H) \cap K = \emptyset$;

(3) $K \cap H = \{1\}$.

Then

$$\triangle \cup \{(x, x, 1) : x \in H\} \cup \{(1, y, 1) : y \in K\} \setminus$$
$$(\{(1, y, 0) : y \in K\} \cup \{(0, y, 1) : y \in K \cup H\})$$

is a minimal blocking set of size $3q - 3 - |K|$.

Proof. It is straightforward to check that the constructed set blocks every line: all lines are blocked by the points of the line $X_0 = 0$, except for those through $(0, 0, 1)$ or $(1, 0, 0)$. The line $X_1 = yX_0$ through $(0, 0, 1)$ is blocked by either the point $(1, y, 1)$ or $(1, y, 0)$ according to whether $y \in K$ or not. Similarly the line $X_1 = yX_2$ through $(1, 0, 0)$ is blocked by either the point $(0, y, 1)$ or $(1, y, 1)$ or $(y, y, 1)$ according to whether $y \notin H \cup K$ or $y \in K$ or $y \in H$.

For the minimality note that for a point of the form $(1, y, 1)$ with $y \in K$ or $(y, y, 1)$ with $y \in H$ or $(0, y, 1)$ with $y \notin H \cup K$, the line $X_1 = yX_2$ is a tangent.

Through a point of the form $(1, y, 0)$, $y \notin K$, the line $X_1 = yX_0$ is a tangent. Similarly, for a point of the form $(x, 0, 1)$ with $x \notin H$, the line $X_0 = xX_2$ is a tangent. The only non-trivial part is to check, whether one has a tangent through a point of the form $(x, 0, 1)$, $x \in H$. A little calculation shows that for such a point, the line $X_1 = X_0 - xX_2$ is a tangent. ■

Theorem 3.15 *There are more than polynomial minimal blocking sets for any size in the interval* $[3q - \sqrt{q}, 3q - 4]$.

PROOF. To achieve the size $k \in [3q-\sqrt{q}, 3q-4]$, choose a set K from $\mathrm{GF}(q)\setminus\{0\}$ with $|K| = 3q - 3 - k$ and $1 \in K$, $-1 \notin K$. Apply Construction 3.14 with an appropriate H of size $\sqrt{q}$. The number of choices for such an H is at least $\binom{(q-3-4\sqrt{q})/2}{(\sqrt{q}-2)/2}$, which is more than polynomial (note that the only elements we cannot use for H are those from $K \cup (1 - K) \cup (-K) \cup (K - 1)$). ■

The following construction works for the q odd case, as then $-2 \neq 2$.

Construction 3.16 *Let the order of the plane be odd.*
Suppose K, $H \subset \mathrm{GF}(q) \setminus \{0\}$ *satisfy the following conditions:*

(1) $H \cap K = \emptyset$

(2) $2 \in H$, $-2 \in K$;

(3) $1 \in K$;

(4) $(K \setminus \{-2\}) = -(K \setminus \{-2\})$

Then

$$\triangle \cup \{(1, y, 1) : y \in K\} \cup \{(-1, y, 1) : y \in H\} \setminus$$
$$(\{(1, y, 0) : y \in (-H) \cup K\} \cup \{(0, y, 1) : y \in H \cup K\})$$

is a minimal blocking set of size $3q - 2 - |H| - |K|$.

PROOF. The proof is almost identical to the proof of Construction 3.14. It is straightforward to check that the constructed set blocks every line: all lines are blocked by the points of the line $X_0 = 0$, except for those through $(0, 0, 1)$ or $(1, 0, 0)$. The line $X_1 = yX_0$ through $(0, 0, 1)$ is blocked by either the point $(1, y, 0)$ or $(1, y, 1)$ or $(-1, y, 1)$ according to whether $y \notin H \cup K$ or $y \in K$ or $y \in H$. Similarly the line $X_1 = yX_2$ through $(1, 0, 0)$ is blocked by either the point $(0, y, 1)$ or $(1, y, 1)$ or $(-1, y, 1)$ according to whether $y \notin H \cup K$ or $y \in K$ or $y \in H$.

For the minimality note that for a point of the form $(1, y, 1)$ with $y \in K$ or $(-1, y, 1)$ with $y \in H$ or $(0, y, 1)$ with $y \notin H \cup K$, the line $X_1 = yX_2$ is a tangent. Through a point of the form $(1, y, 0)$, $y \notin H \cup K$, the line $X_1 = yX_0$ is a tangent. Similarly, for a point of the form $(x, 0, 1)$ with $x \notin \{-1, 1\}$, the line $X_0 = xX_2$ is a tangent. The only non-trivial part is to check, whether one has a tangent through the points $(-1, 0, 1)$ and $(1, 0, 1)$. A little calculation shows that at $(-1, 0, 1)$ the line through $(0, -2, 1)$ is a tangent and at $(1, 0, 1)$ the line through $(0, 1, 1)$ is a tangent. ■

Theorem 3.17 *There are more than polynomial minimal blocking sets for any size in the interval* $[2q - 1, 3q - 3 - \frac{q-1}{2}]$.

PROOF. For a $k \in [2q-1, 3q-3-\frac{q-1}{2}]$ one should choose K such that $|K| = \frac{q-1}{2}$ and then H with $|H| = 3q - 2 - \frac{q-1}{2} - k$ in Construction 3.16. The number of choices for K is roughly $\binom{q/2}{q/4}$. ■

Putting together Theorems 3.12, 3.15 and 3.17, we obtain Theorem 3.11, except for the even case. (And note that even for the $2|q$ case the only part of $[2q - 1, 3q - 4]$ where we have not been able to show more than polynomial minimal blocking sets is $[2q-1, 2q+\sqrt{q}]$.) The following construction completes the proof of Theorem 3.11, since if $q - 1$ is not a prime, we can always find an appropriate M.

Construction 3.18 *For an even prime power q let M denote a multiplicative subgroup of* GF(q) *with generator element t, with $|M| = d$, $3 \leq d \leq \sqrt{q}$.*

Suppose K,$H \subset \mathrm{GF}(q) \setminus \{0\}$ *satisfy the following conditions:*

(1) $t \in H$*;*

(2) $t+1 \notin H$, $\frac{t+1}{t} \notin K$*;*

(3) $H \cap K = \emptyset$*;*

(4) $\frac{1}{t^i} H \setminus \{t+1\} = H$ *for* $i = 0, 1, ..., d-1$.

The set H *is thus the union of cosets of* M*, except possibly for the element* $t+1$.

The set

$$\triangle \cup \{(1, y, 1) : y \in K\} \cup \{(t, y, 1) : y \in H\} \setminus$$
$$(\{(1, y, 0) : y \in H \cup K\} \cup \{(0, y, 1) : y \in H \cup K\})$$

is a minimal blocking set.

The size of the blocking set is $3q - 3 - |H| - |K|$, and since $3 \leq d \leq \sqrt{q}$, we have more than polynomial choices for a suitable H. For instance, let $|H| = [\frac{q-1}{2d}] \cdot d$ and $|K| \leq q - 3 - |H|$. To get a particular minimal blocking set of size k (from Construction 3.18) first choose H then choose K; as the size of H is fixed the size of K will determine k. That is $k = 3q - 3 - [\frac{q-1}{2d}] \cdot d - |K|$. The number of choices is $\binom{(q-1)/d-1}{[(q-1)/2d]-1}\binom{q-3-|H|}{3q-3-|H|-k}$, i.e. more than polynomial.

For the constructions above we have used certain "good" subsets, but the last construction "almost" employed cosets, which takes us to the theme of the remaining part of the present thesis.

3.2.2 Megyesi's construction

Megyesi's construction is the following Rédei construction using cosets.

Construction 3.19 (Megyesi) *Let* H *be a non-trivial multiplicative subgroup of* $(\mathrm{GF}(q), \cdot)$*. Partition* $(\mathrm{GF}(q), \cdot)$ *into two nonempty subsets* X *and* Y *in such a way that both are the union of cosets of* H*. Let* $U = \{(x, 0) : x \in X\} \cup \{(0, y) : y \in Y\} \cup \{(0, 0)\}$*. Finally, let* D *denote the determined directions of* U*. Then* $U \cup D$ *is a minimal blocking set.*

The following lemma will determine the size of the minimal blocking set in Construction 3.19.

Lemma 3.20 *The size of a minimal blocking set M using Construction 3.19 is $2q+1-|K|$, where $K = \{k : k \cdot X = X\}$.*

PROOF. We wish to prove that the non-determined directions are exactly those corresponding to elements of $-K$. A direction $(d) \notin \{(0), (\infty)\}$ is determined if and only if $d = \frac{-y}{x}$ for suitable $x \in X$ and $y \in Y$. This is equivalent to the condition $-dX \cap Y \neq \emptyset \Leftrightarrow -dX \neq X \Leftrightarrow d \notin -K$. ■

Note that K is the largest multiplicative subgroup for which X (and Y) is the union of some cosets of K and $H \subseteq K$. Hence instead of starting with H, we can start with K and the same X and Y to get the same blocking set.

Lemma 3.21 *Given a multiplicative subgroup H of $(\mathrm{GF}(q), \cdot)$ with index $h > 3$, the number of ways of choosing X and Y in Construction 3.19 to have size $2q+1-|H|$ is greater than 2^{h-1}.*

PROOF. There are $2^h - 2$ choices for X and Y. The number of choices for which the number of non-determined directions is $|K|$ for a larger group than H is at most $\sum(2^{h'} - 2)$, where the summation is over all $h'|h$, $h' \neq h$, $h' \neq 1$. This is at most $2 + 4 + \cdots + 2^{h/2} - 2 = 2^{h/2+1} - 4$. ■

Theorem 3.22 (Mengyán, [2]) *Let d be an arbitrary integer, $2 \leq d \leq \sqrt{q}$, $d|q-1$. The number of minimal blocking sets M of size $2q+1-d$ is more than polynomial.*

PROOF. Let $H \leq \mathrm{GF}(q, \cdot)$, $|H| = d$. Then the index is $h = \frac{q-1}{d} \geq \sqrt{q} - 1$. From Lemma 3.21 the number of choices for X and Y in construction 3.19 is greater than 2^{h-1}. ■

There is a similar construction due to Megyesi with additive subgroups. The only exception is that one has to put some cosets of an (additive) subgroup on

a line and the rest to a parallel line. Using this, one can prove a similar result for blocking sets of size $2q + 1 - d$, where $d|q$, $d \leq \sqrt{q}$.

We note that in $\mathrm{PG}(n, q)$ considering a cone with an $(n - 3)$-dimensional subspace as vertex V and with the minimal blocking sets constructed in this chapter as base B we get again minimal line-blocking pointsets, so equivalent statements proved in the chapter exist in higher dimensions.

Chapter 4

A generalization of Megyesi's construction

A different example than Megyesi's construction, contained in the union of four lines, was constructed by Gács [23] giving an infinite series of examples determining $7q/9$ directions approximately, thus yielding a minimal blocking set of approximate size $2q - 2q/9$.

Theorem 4.1 (Gács, [23]) *Let* 3 *be a divisor of* $q-1$*, and let* $1, \alpha, \alpha^2$ *be coset representatives of the multiplicative subgroup* G *of index* 3*. Let*

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

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

In both the Megyesi and the Gács constructions a subgroup and its cosets were placed on lines. The question arises whether a generalization would be possible when the number of cosets is larger than three, or when the number of lines from which points are taken is increased. As we show in this chapter this problem can be formulated using some trivial equations and solved by Weil's estimate.

In some sense the technique we use here is similar to techniques used by Korchmáros in [31] and Szőnyi in [42], though our method seems distinct from theirs.

4.1 Placing cosets on three lines

In this section we investigate the case when the points of the minimal blocking set are on four lines: three concurrent lines in $\mathrm{AG}(2,q)$ and the fourth the line at infinity of the projective closure of $\mathrm{AG}(2,q)$. In particular, without loss of generality, we may assume the three affine lines to be $x=0$, $y=0$ and $x=y$.

Construction 4.2 *Consider a multiplicative subgroup G of $(\mathrm{GF}(q),\cdot)$ with index s, such that α is a generator element of G. Form three non-empty subsets I,J,K from the set of integers $S=\{0,...,s-1\}$ such that $|I|+|J|+|K|=s$. Let*

$$U=\{(0,0)\}\cup\bigcup_{j\in J}(0,\alpha^jG)\cup\bigcup_{k\in K}(\alpha^kG,\alpha^kG)\cup\bigcup_{i\in I}(\alpha^iG,0).$$

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

Proof. Minimality follows from the fact that not all $q+1$ directions can be determined. ■

The size of the minimal blocking set B of Construction 4.2 can be determined by determining $|D|$. This is equivalent to determining $|D^c|$, the number of non-determined points, as $|D|+|D^c|=q+1$. Note also that S is a multiplicative subgroup, and that operations on S are considered modulo s.

Lemma 4.3 *Consider a multiplicative subgroup G of $(\mathrm{GF}(q),\cdot)$ with index s, such that α is a generator element of G and a set of integers $S=\{0,...,s-1\}$. Then*

$$\dot{\bigcup_{u\in S}}-\alpha^uG=\mathrm{GF}(q)\setminus\{0\}$$

$$\dot{\bigcup_{w\in S}}1-\alpha^wG=\mathrm{GF}(q)\setminus\{1\}$$

$$\dot{\bigcup_{v\in S}}\tfrac{1}{1-\alpha^vG}=\mathrm{GF}(q)\setminus\{0,1,\infty\}.$$

Proposition 4.4 *For B in Construction 4.2 we have:*

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

where c denotes the complement.

PROOF. Considering the directions the cosets determine, one gets D. An element of D^c must come from the intersections of the complements, as otherwise it would be determined. ■

Proposition 4.5 *From Proposition 4.4 and Lemma 4.3 it follows that*

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

Lemma 4.6 *Consider a multiplicative subgroup G of $(\mathrm{GF}(q), \cdot)$ with index s, such that α is a generator element of G. Then*

1. $-\alpha^u G \cap \frac{1}{1-\alpha^v G} \cap (1 - \alpha^w G) = \emptyset$ *if* $u + v \neq w$,
2. $-\alpha^u G \cap \frac{1}{1-\alpha^v G} = -\alpha^u G \cap (1 - \alpha^w G) = \frac{1}{1-\alpha^v G} \cap (1 - \alpha^w G)$ *if* $u + v = w$,

for any $u, v, w \in (\mathrm{GF}(q), \cdot)$.

PROOF. 1. For an element in the intersection $\frac{1}{1-\alpha^v G} \cap (1 - \alpha^w G)$ we have $\frac{1}{1-\alpha^v x} = (1 - \alpha^w y)$ for some $x, y \in G$. Then $(1 - \alpha^w y)(1 - \alpha^v x) = 1$, which implies $1 - \alpha^w y = -\frac{\alpha^w y}{\alpha^v x} = -\alpha^{w-v} \frac{y}{x} \in -\alpha^{w-v} G$. If $u + v \neq w$ then $\alpha^u \neq \alpha^{w-v}$ so $\alpha^u G$ and $\alpha^{w-v} G$ are disjoint cosets.

2. We essentially follow the proof of Lemma 3.4 of [23] showing that $-\alpha^u G \cap (1 - \alpha^w G) \subset -\alpha^u G \cap \frac{1}{1-\alpha^v G} \subset \frac{1}{1-\alpha^v G} \cap (1 - \alpha^w G) \subset -\alpha^u G \cap (1 - \alpha^w G)$.

The intersection $-\alpha^u G \cap (1 - \alpha^w G)$, means that $-\alpha^u x = 1 - \alpha^w y$ for some $x, y \in G$. Dividing by $-\alpha^u x$ one gets $1 = \frac{-1}{\alpha^u x} + \frac{\alpha^w y}{\alpha^u x}$, implying $-\alpha^u x = \frac{1}{1-\frac{\alpha^w y}{\alpha^u x}} = \frac{1}{1-\alpha^v \frac{x}{y}} \in \frac{1}{1-\alpha^v G}$.

Next let $-\alpha^u x = \frac{1}{1-\alpha^v y}$. Rearranging and using that $u+v=w$ we get $-\alpha^u x = 1-\alpha^w y \in 1-\alpha^w G$.

Finally, set $\frac{1}{1-\alpha^v x} \cap (1-\alpha^w y)$. Then $1=(1-\alpha^w y)(1-\alpha^v x)$. Again after rearranging we get $1-\alpha^w y = -\alpha^{w-v}\frac{y}{x} \in -\alpha^u G$. ■

Notation 4.7 *Denote by the pair (u,w) the intersection $-\alpha^u G \cap (1-\alpha^w G)$.*

Corollary 4.8 *D^c is the sum of intersections of the form $-\alpha^u G \cap \frac{1}{1-\alpha^v G} \cap (1-\alpha^w G)$. By Lemma 4.6 1. only those intersections are non-empty where $u+v=w$, and by Lemma 4.6 2. any of the three intersections determine the same non-empty intersection, so it is enough to consider (u,w).*

To determine the size of (u,w) for given u and w Weil's estimate is used.

Lemma 4.9 *The number of points in $-\alpha^u G \cap (1-\alpha^w G)$ is approximately $q/s^2 + O(\sqrt{q})$.*

PROOF. The elements of G are precisely the elements of the form u^s, where $0 \neq u \in \mathrm{GF}(q)$. Hence the elements of $-\alpha^u G \cap (1-\alpha^w G)$ correspond to the solutions of the equation

$$ax^s = 1 - by^s, \tag{4.1}$$

where $a=\alpha^u$ and $b=\alpha^w$ are nonzero elements of $\mathrm{GF}(q)$, and $0 \neq x,y$. Actually, for an element g of G there are s elements $u \in \mathrm{GF}(q)$ such that $g=u^s$. Hence a common element of $-\alpha^u G \cap (1-\alpha^w G)$ correspond to s^2 solutions of equation (4.1). Furthermore, (4.1) defines an affine curve whose projectivization is $ax^s = z^s - by^s$ (here (x,y,z) denotes the homogeneous coordinates). This projective curve has no singular points, since $g.c.d.(s,q)=1$. By Weil's estimate, the number of $\mathrm{GF}(q)$-rational points of the projective curve is $q+1-(s-1)(s-2)\sqrt{q} \leq N \leq q+1+(s-1)(s-2)\sqrt{q}$. The curve has s infinite points, there are at most s points on any of the lines $x=0$ and $y=0$. Therefore (4.1) has at least $q+1-(s-1)(s-2)\sqrt{q}-3s$, and at most $q+1+(s-1)(s-2)\sqrt{q}$ points. Dividing by s^2 gives that

$$|-\alpha^u G \cap (1-\alpha^w G)| \leq \frac{q}{s^2} + \frac{(s-1)(s-2)}{s^2}\sqrt{q} + \frac{1}{s^2}$$

$$|-\alpha^u G \cap (1-\alpha^w G)| \geq \frac{q}{s^2} + \frac{(s-1)(s-2)}{s^2}\sqrt{q} - \frac{3s-1}{s^2}$$

that is $|-\alpha^u G \cap (1-\alpha^w G)|$ is $q/s^2 + O(\sqrt{q})$. ■

Remark 4.10 *Note that the result is meaningful only when $q/s^2 \gg \sqrt{q}$, that is when $s \ll \sqrt[4]{q}$.*

To determine the number of nonempty (u, w) pairs the following lemma can be useful.

Lemma 4.11 *Let I, J, K be subsets of a set of integers $S = \{0, ..., s-1\}$ with $u, v, w \in S$. Then the following hold modulo s:*

$$u \notin J - I \Longrightarrow I + u \cap J = \emptyset$$

$$v \notin I - K \Longrightarrow K + v \cap I = \emptyset$$

$$w \notin J - K \Longrightarrow K + w \cap J = \emptyset$$

If furthermore $u + v = w$ then these together are equivalent to $I + u \cap J = \emptyset$, $K + w \cap I + u = \emptyset$ and $K + w \cap J = \emptyset$.

Determining D^c and D in Construction 4.2 reduces to determining $|T|$, the number of pairs (u, w) satisfying the three equations of Lemma 4.11 involving I, J, K and u, w. Each (u, w) pair then adds approximately q/s^2 to $|D^c|$, so $|B| = 2q - |T|q/s^2 + O(\sqrt{q})$.

In this way constructing a minimal blocking set B using cosets is equivalent to solving some trivial equations. The size of B depends on $|T|$ and a certain remainder term $O(\sqrt{q})$ (the remainder term in Weil's estimate); and if q is large enough then mainly on $|T|$. So if q is large enough and there is a non-empty set (u, w) then the method certainly gives minimal blocking sets of size less than $2q - 1$. (Otherwise the remainder term may be too large). Hence these minimal blocking sets are in the third interval of the spectrum.

Using the correspondence between the described trivial equations and minimal blocking sets, we can construct minimal blocking sets of many sizes.

Example 4.12 *Let* $I = \{0\}, J = \{2, 3, ..., s-1\}$ *and* $K = \{1\}$. *Then we have two pairs* $(0, 0)$ *and* $(1, s-1)$ *that satisfy Lemma 4.11. That is* $|N| = 2q/s^2 + O(\sqrt{q})$, $|B| = 2q - 2q/s^2 + O(\sqrt{q})$.

Example 4.13 *Let* $I = \{0, 2\}, J = \{1\}$ *and* $K = \{3, 4, ..., s-1\}$. *Then we have exactly one pair* $(0, 0)$ *that satisfies Lemma 4.11. That is* $|N| = q/s^2 + O(\sqrt{q})$, $|B| = 2q - q/s^2 + O(\sqrt{q})$.

Example 4.14 *Let* $s = 8k$, *for some positive integer* k, $I = \{0, 2, 4, ...\}, J = \{1, 5, 9, ...\}$ *and* $K = \{3, 7, 11, ...\}$. *Then the number of pairs that satisfy Lemma 4.11 is* $8k^2$ *giving* $|N| = (q+1)/8 + O(\sqrt{q})$, $|B| = 2q - (q+1)/8 + O(\sqrt{q})$.

Example 4.15 *Let* $s = 3k$, *for some positive integer* k, $I = \{0, 3, 6, ...\}, J = \{1, 4, 7, ...\}$ *and* $K = \{2, 5, 8, ...\}$. *Then the number of pairs that satisfy Lemma 4.11 is* $2k^2$ *giving* $|N| = 2q/9 + O(\sqrt{q})$, $|B| = 2q - 2q/9 + O(\sqrt{q})$.

A thorough generalization of the Megyesi construction was done by Nóra Viola Harrach in [1], where she investigated the general case (cosets on more than three lines), and gave a more abstract description that allows a complete characterization of minimal blocking sets obtainable from cosets on lines. For her results Sziklai's version of the Weil estimate is needed (Theorem 1.14).

4.2 Embedding and non-Rédei minimal blocking sets

From the existing minimal blocking sets some new ones can be constructed by using embeddings of $\mathrm{PG}(2, q)$ into $\mathrm{PG}(2, q^h)$ for some $h > 1$. In this section we investigate two possible methods mainly with recpect to the minimal blocking sets constructed above.

Construction 4.16 *Consider a minimal blocking set* B *of* $\mathrm{PG}(2, q)$. *Embed* $\mathrm{PG}(2, q)$ *into* $\mathrm{PG}(2, q^h)$ *for some* $h > 1$. *Denote by* l *and* m *two lines of* $\mathrm{PG}(2, q^h)$ *that intersect* $\mathrm{PG}(2, q)$ *in* $q+1$ *points, and* B *in less than* q *points*

if $Q := l \cap m$ is not a point of B. Furthermore denote by C the set of critical points of B which have their critical tangents through Q. Consider the pointset

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

We note that if B is of size less than $2q$ then all lines intersect B in at most $q-1$ points, for otherwise through any point of B on the existing q-secant there are q lines that must be blocked, consequently the size of B would be at least $2q$.

Proposition 4.17 *B' in Construction 4.16 is a minimal blocking set in $\mathrm{PG}(2,q^h)$ of size*

1. *$2q^h - 2q + |B|$ if $Q \in B$,*
2. *$2q^h - 2q + |B| + 1$ if $Q \notin B$ and C is empty.*

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

Minimality follows as at all points of B' there are tangents. At the points of B the lines containing the tangents to B in $\mathrm{PG}(2,q)$ are tangents as these intersect l and m in $l \cap \mathrm{PG}(2,q)$ and $m \cap \mathrm{PG}(2,q)$ respectively. At the points of B' on $l \setminus \mathrm{PG}(2,q)$ the lines through the points of $\{m \cap \mathrm{PG}(2,q) \setminus B\}$ are tangents, and at the points of B' on $m \setminus \mathrm{PG}(2,q)$ the lines through the points of $\{l \cap \mathrm{PG}(2,q) \setminus B\}$ are tangents. At Q all the lines of $\mathrm{PG}(2,q^h)$ intersecting $\mathrm{PG}(2,q)$ in exactly Q are tangents to B'.

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

The size of B' when $|C| > 1$ and $Q \notin B$ depends on B as some points of C must be deleted, so the precise size can be only determined given the concrete case.

Proposition 4.18 *Let $x > 1$ be an integer. If the size of B is $2q - x$ then the number of tangents at any point of B is at least $x + 1$, so there are no critical points of B.*

PROOF. We follow the argument of Blokhuis and Brouwer from [12] that is based on a result of Jamison [30]. If B is a minimal blocking set then each point of B is on at least one tangent. Let $P \in B$ be a point on t tangents, call one of them l. Form a blocking set of $\mathrm{AG}(2,q) = \mathrm{PG}(2,q) \setminus l$ with $|B|-1+(t-1)$ points by placing a point on each of the $t-1$ tangents ($\neq l$) of P and taking the points of $B \setminus \{P\}$. Then the inequality $t \geq 2q+1-|B|$ can be deduced, because in [14] Brouwer and Schrijver proved that a blocking set of $\mathrm{AG}(2,q)$ has at least $2q-1$ points. ■

Theorem 4.19 (Harrach and Mengyán, [1]) *Let $x > 1$ be an integer. If there is a minimal blocking set of size $2q-x$ in $\mathrm{PG}(2,q)$ then there are minimal blocking sets of size $2q^h - x$ and $2q^h - x + 1$ in $\mathrm{PG}(2,q^h)$.*

Note that for the minimal blocking sets of size $2q-x$ ($x>1$) constructed previously in this chapter the number of tangents at affine points is $|D^c| = x+1$ and at infinite points at least $q/s \geq x+1$. When B is such a minimal blocking set then B' of Construction 4.16 is a Rédei minimal blocking set if and only if $l \cap \mathrm{PG}(2,q)$ or $m \cap \mathrm{PG}(2,q)$ are Rédei lines of B. For this, it is enough to check the sizes of the intersection of lines with B' in $\mathrm{PG}(2,q^h)$. For B' to be Rédei this intersection size must be $q^h - x$ for some line. But this is impossible as the sizes of possible intersections are at most $q+1$ for the lines other than l or m.

Example 4.20 *In Example 4.12 let l be the x-axis and m be the line $y = x$. Then the embedding of this minimal blocking set with the method above will be a non-Rédei minimal blocking set.*

We now turn attention to another embedding method, described in [37] and [45]. Here we only repeat the construction and a theorem from these papers, and investigate what this method means for the minimal blocking sets obtained in this chapter. For further details of this construction refer to the papers [37, 45].

Construction 4.21 *Let B be a minimal blocking set in $\mathrm{PG}(2,q)$. Embed $\mathrm{PG}(2,q)$ into $\mathrm{PG}(h+1,q)$. Choose an $(h-2)$-dimensional subspace V', so that $\mathrm{PG}(2,q) \cap V' = \emptyset$. Let B' be the cone with base B and vertex V'. Embed $\mathrm{PG}(h+1,q)$*

as a subgeometry in $\mathrm{PG}(h+1,q^h)$*. Assume that* R *is an* $(h-1)$*-dimensional subspace of* $\mathrm{PG}(h+1,q)$*, and let* R^* *be the unique* $(h-1)$*-dimensional subspace of* $\mathrm{PG}(h+1,q^h)$ *that contains* R*. Choose an* $(h-2)$*-dimensional subspace* P *in* R^**, such that* P *does not intersect the subgeometry* $\mathrm{PG}(h+1,q)$*, and project* B' *from this subspace onto a plane* π *of* $\mathrm{PG}(h+1,q^h)$*, where* $\pi \cap P = \emptyset$*. The cardinality of the projection,* B'' *satisfies* $|B''| = |B'| + 1 - |R \cap B'|$*.*

Theorem 4.22 (Szőnyi, Gács, Weiner, [45]) *Let* B' *be a minimal blocking set of* $\mathrm{PG}(h+1,q)$ *with respect to lines and suppose that* $B' < 2q^h - 1$*. Then the projection* B'' *of* B' *is a minimal blocking set.*

By Theorem 4.22 the projection according to Construction 4.21 of all the minimal blocking sets constructed in this chapter will give minimal blocking sets for sufficiently large q. Moreover, it is not difficult to see that these projections will generally not be Rédei minimal blocking sets. We only have to choose the projection carefully. For simplicity let $h = 2$. (For a precise discussion on intersection numbers of B'' with respect to lines see [37], p.742.) Take R as a line through V' and the origin in $\mathrm{AG}(2,q)$. This gives three types of lines in the projection:

(i) lines that were projected from lines of B' not containing V' that intersect B'' in less than q points,

(ii) lines that were projected from lines of B' through V', which intersect B'' in 1 or $q+1$ points,

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

For B'' to be a Rédei minimal blocking set, we must have some lines intersect B'' in $q^2 - qx - q + 1$ points as the size of B'' is $(2q-x)q + 1 - q$.

For the first two cases this gives the equation $q^2 - qx - q + 1 \leq q + 1$ from which we get that $7q/9 < 2 + O(\sqrt{q})$. The third case gives $q^2 - qx - q + 1 = rq + 2 - q - 1$ from which we get $q - x = r$. But r is 1,2 or $2 + r_2|G|$, where $0 < r_2 < s - 1$ is an integer. This means that $q - x$, the number of determined

directions $|D|$ and $x+1$, the number of non-determined directions $|D^c|$ are both multiples of $|G|$ approximately. For large enough q taking the sets from Example 4.12 and Example 4.13 as B we get non-Rédei minimal blocking sets as then $7q/9 > 2 + O(\sqrt{q})$ and $|D^c| < q/s$.

Moreover it is not clear at all when the minimal blocking sets we have constructed could give Rédei minimal blocking sets with the projection method as the size of B is uncertain up to an $O(\sqrt{q})$. At present this seems only resolvable by calculating the concrete case.

Bibliography

This thesis is based on the following articles of the author.

[1] N. V. Harrach, C. Mengyán, Minimal blocking sets in PG$(2, q)$ arising from a generalized construction of Megyesi, *in preparation.*

[2] C. Mengyán, On the number of pairwise non-isomorphic minimal blocking sets in PG$(2, q)$, *Des. Codes Cryptogr.* **45** (2007), 259-267.

[3] C. Mengyán, Partitioning the flags of PG$(2, q)$ into strong representative systems, *Contr. Discr. Math. special issue dedicated to Ferenc Kárteszi* **3** (2008), 5-12.

[4] T. Szőnyi, A. Cossidente, A. Gács, C. Mengyán, A. Siciliano, Zs. Weiner, On large minimal blocking sets in PG$(2, q)$, *J. of Comb. Designs* **13** (2005), 25-41.

Further references

[5] N. Alon, J. Spencer, *The probabilistic method*, Wiley, New York, 1992.

[6] R.D. Baker, G.L. Ebert, On Buekenhout-Metz unitals of odd order, *J. Combin. Theory Ser. A.* **25** (2004), 215-421.

[7] L. Béres, T. Illés, Computational investigation of the covering number of finite projective planes with small order, *Alkalmaz. Mat. Lapok* **25** (1997), 397-411.

[8] A. Blokhuis, On the size of a blocking set in PG$(2, p)$, *Combinatorica* **14** (1994), 273-276.

[9] A. Blokhuis, Blocking sets in Desarguesian planes, in: *Paul Erdős is Eighty, Volume 2*, (D. Miklós, V.T. Sós and T. Szőnyi, eds.), Bolyai Soc. Math. Studies, **2**, Bolyai Society, Budapest, 1996, 133-155.

[10] A. Blokhuis, Combinatorial problems in finite geometry and lacunary polynomials, in: Li, Ta Tsien (ed.) et al., *Proceedings of the international congress of mathematicians, ICM 2002, Beijing, China, 2002, Vol. III: Invited lectures*, Beijing, Higher Education Press. 537-545 (2002).

[11] A. Blokhuis, S. Ball, A. Brouwer, L. Storme,T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, *J. Comb. Theory* Ser.A **86** (1999), 187-196.

[12] A. Blokhuis, A. Brouwer, Blocking sets in Desarguesian projective planes, *Bull. London Math. Soc.* **18** (1986), 132-134.

[13] A. Blokhuis, K. Metsch, Large minimal blocking sets, strong representative systems, and partial unitals, *Finite Geometries,(F. De Clerck et al. eds.)*, Cambridge Univ.,(1993), 37-51.

[14] A. Brouwer, A. Schrijver, The blocking number of an affine space, *J. Comb. Theory* Ser.A **24** (1978), 251-253.

[15] A. Blokhuis, L. Storme and T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes. *J. London Math. Soc.* (2) **60** (1999), 321-332.

[16] R. H. Bruck, R. C. Bose, The construction of translation planes from projective spaces, *J. Algebra* **1** (1964), 85-102.

[17] A. A. Bruen, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342-344.

[18] A. Bruen, K. Drudge, The Return of the Baer Suplane, *J. Combin. Theory* Ser.A**85** (1999), 228-231.

[19] A. A. Bruen, J. A. Thas, Blocking sets, *Geom. Dedicata* **6** (1977), 193-203.

[20] P. Erdős, J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, Budapest (New York), 1974.

[21] R. J. Faudree, R. H. Schelp, A. Gyárfás, Zs. Tuza, The strong chromatic index of graphs, *Ars Combinatoria* **29B** (1990), 205-211.

[22] Z. Füredi, Matchings and covers in hypergraphs, *Graphs and Combin.* **4** (1988), 115-206.

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

[24] A. Gács, T. Szőnyi, Random constructions and density results, *Des. Codes Cryptogr.*, to appear.

[25] N. Hamilton, R. Mathon On the spectrum of non-Denniston maximal arcs in $\mathrm{PG}(2,2^h)$, *European journal of Combinatorics* **25** (2004), 415-421.

[26] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford, 1979, 2nd edition, 1998.

[27] T. Illés, T. Szőnyi, F. Wettl, Blocking sets and maximal strong representative systems in finite projective planes, *Mitt. Math. Sem. Giessen* **201** (1991), 97-107.

[28] S. Innamorati, A. Maturo On irreducible blocking sets in projective planes, *Ratio Math.* **2** (1991), 151-155.

[29] I. Jagos, Gy. Kiss, A. Pór, On the intersection of Baer subgeometries of $\mathrm{PG}(n,q^2)$, *Acta Sci. Math. (Szeged)* **69** (2003), 419-429.

[30] R. Jamison, Covering finite fields with cosets of subspaces, *J. Combin. Theory Ser. A* **22** (1977), 253-266.

[31] G. Korchmáros, New Examples of k-arcs in $\mathrm{PG}(2,q)$, *Eur. J. Comb.* **4** (1983), 329-334.

[32] R. Lidl, H. Niederreiter, *Finite Fields*, Addison-Wesley, Waltham, 1983.

[33] L. Lovász, *Combinatorial problems and exercises*, American Math. Soc., Providence RI, 2007.

[34] R. Mathon, New maximal arcs in Desarguesian planes, *J. Combin. Theory Ser. A.* **97** (2002), 353-368.

[35] F. Mazzocca, O. Polverino, Blocking sets in $\mathrm{PG}(2, q^n)$ from cones of $\mathrm{PG}(2n, q)$, *J. Algebr. Comb.* **24** (2006), 61-81.

[36] F. Mazzocca, O. Polverino, L. Storme, Blocking sets in $\mathrm{PG}(r, q^n)$, *Des. Codes Cryptogr.* **44** (2007), 97-113.

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

[38] L. Rédei, *Lacunary Polynomials over Finite Fields*, North-Holland, Amsterdam, 1973.

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

[40] P. Sziklai, On small blocking sets and their linearity, *J. Combin. Th. Ser A.*, to appear.

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

[42] T. Szőnyi, Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica* **19** (1991), 91-100.

[43] T. Szőnyi, Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* **12** (1992), 227-235.

[44] T. Szőnyi, Some applications of algebraic curves in finite geometry and combinatorics, *Surveys in Combinatorics, Proc. British Comb. Conf* 1997 (ed. R.A.Bailey), 197-236.

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

[46] J.A. Thas, On semi-ovals and and semi-ovoids, *Geom. Ded.* **3** (1974), 229-231.

[47] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci* **34** (1948), 204-207.

Summary

In finite projective geometry several methods both from geometry and algebra can be used to attain new results. In this thesis we concentrate on some methods of particular importance in the construction of minimal blocking sets and a closely related notion, strong representative systems.

The preambulum is devoted to an overview of the thesis, acknowledgement and notation.

In Chapter 1 we give some basic definitions and concepts. We prove a generalization of the Bruen-Thas upper bound in Section 1.2. In Section 1.5 we give a short overview of the methods to be discussed: embedding, partitioning, random choice, adding and deleting points and use of subsets. The description here is very general, but in subsequent chapters we provide ample examples of their uses. We also include a strong algebraic technical tool, Weil's estimate and some of its variants.

Chapter 2 is devoted to higher dimensional constructions using embedding and partitioning. In Sections 2.1 and 2.2 we give necessary definitions and a general construction. In Section 2.3 we describe the generalized Buekenhout construction, and a particular type of large minimal blocking set obtained using this embedding method. In Section 2.4 we present some results obtained by the generalized Buekenhout construction and its modifications. In subsections of Section 2.5 we show three solutions to a problem raised by Gyárfás that is equivalent to partitioning the flags of $\mathrm{PG}(2, q)$ into strong representative systems. The first two subsections give results using geometrical and partitioning arguments, while the last part of the chapter shows a solution to this problem obtained by the generalized Buekenhout construction using minimal blocking sets described in Section 2.3, and demonstrates the power of the embedding

method over the other solutions.

In Chapter 3 we consider constructions in the plane. The results here use random choice in the first part of the chapter, and mainly subsets and cosets in the second part. In Section 3.1 we show density results and that the number of such structures is in most cases more than polynomial, a question originally asked by Turán. In Section 3.2 we construct more than polynomial number of minimal blocking sets starting from the well-known triangle and Megyesi's example respectively by placing suitable subsets (of points) on lines.

In Chapter 4 we investigate Megyesi's example more thoroughly. In Section 4.1 we show a generalization of Megyesi's example, and prove that there is a strong correspondence between such constructions and some trivial equations. Finally, in Section 4.2 we introduce a simple embedding method and sketch another high dimensional embedding method, and discuss their implications to constructing non-Rédei minimal blocking sets.

Finally, we end the thesis with the Bibliography, Summary and Hungarian summary.

Magyar nyelvű összefoglaló

A véges projektív geometriában különböző algebrai és geometriai módszerek használhatók, amelyekkel új eredményeket lehet elérni. Jelen dolgozatban a minimális lefogó ponthalmazokkal kapcsolatos kiemelekedően fontos konstrukciókat tekintjük át.

Az első fejezetben alapvető definiciókat adunk meg, valamint a Bruen-Thas felső becslés egy általánosítását (az 1.2 alfejezetben). Továbbá röviden áttekintjük a használandó módszereket: beágyazás, partició, véletlen választás, pontok hozzáadása-törlése és részhalmazok alkalmazása. A tárgyalás itt nagyon általános, de a további fejezetekben alaposan körbejárjuk a témát, példákkal megmutatva az alkalmazás lehetőségeit. A fejezetet a Weil becsléssel zárjuk.

A második fejezet fő témája a magasabb dimenziós konstrukciók. A 2.1 és 2.2 alfejezetekben leírjuk az André, Bruck-Bose reprezentációt, valamint megadunk egy általános kúp-konstrukciót. A 2.3 alfejezetben ennek a konstrukciónak egy speciális esetét, az általánosított Buekenhout konstrukciót fejtjük ki, amely egy érdekes nagyméretű minimális lefogó ponthalmazt ad. A következő alfejezetben további eredményeket írunk le. A 2.5 alfejezet részeiben három megoldást adunk Gyárfás egy kérdésére, amely ekvivalens $\mathrm{PG}(2,q)$ ponthalmazok egyenes párjainak erős reprezentációs rendszerekkel való particiójával. Először megadunk két megoldást, amelyek egyszerű geometriai és particiós eszmefuttatáson alapulnak. A harmadik megoldás az általánosított Buekenhout konstrukciót használva demonstrálja a beágyazásos módszer erejét.

A harmadik fejezetben a síkra térünk át. A fejezet első felében a véletlen módszert használjuk, a második felében részhalmazokat. A 3.1 alfejezetben sűrűségi eredményeket mutatunk, és bizonyítjuk, hogy bizonyos esetekben a minimális lefogók száma több, mint polinomiális. Ez utóbbi kérdést eredeti-

leg Turán tette fel. Az 3.2 alfejezetben polinomiálisnál több minimális lefogót gyártunk a jól ismert háromszögből és Megyesi konstrukcióból kiindulva azáltal, hogy megfelelő részhalmazokat helyezünk egyenesekre.

Az utolsó fejezetben a Megyesi konstrukciót vesszük górcső alá alaposabban. A 4.1 alfejezetben általánosítjuk Megyesi megoldását, és bebizonyítjuk, hogy erős megfeleltetés áll fenn ilyen konstrukciók és bizonyos egyenletek között. Végezetül, a 4.2 alfejezetben két további beágyazásos módszert írunk le röviden, azzal összefüggésben, hogy hogyan kaphatunk nem-Rédei minimális lefogókat a 4.1 alfejezetben ismertetett általánosított Megyesi konstrukció által előállított lefogókból.

A doktori dolgozatot a referenciák megadásával, valamint az angol és magyar nyelvű összefoglalóval zárjuk.