Blocking sets in projective and affine planes

Notes for the intensive course
Ghent, April 14–24, 1998

Aart Blokhuis *

1. Introduction

1.1. What is a blocking set

A *blocking set* in a projective or affine plane is a set of points intersecting every line. In case of a projective plane we assume in addition that it does not contain a line. The name blocking set originates from game theory, where we have a set of individuals, and certain subsets called coalitions, with the property that a coalition can force a particular decision. A blocking set then is a subset that is not a coalition, but contains at least one member of each coalition, so that it can block any decision without being able to force one. Von Neumann and Morgenstern [35] gave the Fano plane, $PG(2,2)$, with coalitions the collinear triples, as an example of a structure without a blocking set. This is the only projective plane without a blocking set however.

Richardson was the first one to look at larger planes [40]. He showed that the minimal size of a blocking set in $PG(2,3)$ is 6, and noted that Baer subplanes are examples of blocking sets of size $q+\sqrt{q}+1$ in projective planes of square order. After that things were quiet for 13 years until di Paola [36] introduced the idea of a projective triangle, which gives an example of a blocking set of size $3(q+1)/2$ in Desarguesian planes of odd order. That projective triangles exist in these planes was shown by Bruen, who also obtained the general lower bound $q+\sqrt{q}+1$ for the size of a blocking set in an arbitrary projective plane of order q.

Further early results were obtained by Bruen and Thas in [24], where they give the upper bound $q\sqrt{q}+1$ for a minimal blocking set in any projective plane of order q, and make the connection with Rédei's work on lacunary polynomials [39]. How fundamental his results are for the structure of blocking sets however was only realized much later and in

*Eindhoven University of Technology, P.O. Box 513, 5600 MB, Eindhoven, The Netherlands, and Free University Amsterdam

this course the emphasis will be to explain in some detail the recent developments and the connection between Rédei's work on lacunary polynomials and small blocking sets and multiple blocking sets in Desarguesian projective planes.

1.2. Examples of small blocking sets

Let Π_q denote an arbitrary projective plane of order q, and denote the Desarguesian plane by $PG(2,q)$. A *Baer subplane* B of Π_q is a collection of $q+\sqrt{q}+1$ points with the property that every line joining two points of B contains precisely $\sqrt{q}+1$ points of B. The points of B together with the $q+\sqrt{q}+1$ secants thus obtained form the structure of a $\Pi_{\sqrt{q}}$. Every non-secant intersects B in exactly one point. Hence a Baer subplane is a blocking set. A Desarguesian plane of square order contains a Baer subplane. If we fix any coordinate frame $P_1=(1:0:0)$, $P_2=(0:1:0)$, $P_3=(0:0:1)$, $P_4=(1:1:1)$ then the unique Baer subplane containing P_1, P_2, P_3, P_4 consists of the points $\{(a:b:c:)\,|\,a,b,c\in GF(\sqrt{q})\}$. Baer subplanes are the smallest possible blocking sets.

Theorem 1.1 (Bruen [18]). *Let B be a blocking set in Π_q. Then $|B|\geq q+\sqrt{q}+1$ with equality if and only if B is a Baer subplane.*

Before proving this we first make an observation. If B has size $q+m$, then for any line L we have $|L\cap B|\leq m$. Indeed, let P be a point on L not in B, then

$$q+m=|B|=\sum_{M:P\in M}|B\cap M|\geq|B\cap L|+q\cdot 1.$$

In the case of equality we say that B is of Rédei type (with respect to L).

Proof : We assume that B is a blocking set of size $q+m$, with $m\leq\sqrt{q}+1$ and we will show that B is a Baer subplane. We have $|B\cap L|\leq m\leq\sqrt{q}+1$ for each line L by the observation above. Let l_i denote the number of lines containing precisely i points of B. Counting lines, incident point line pairs, and triples (P,Q,L), $P,Q\in L\cap B$, we obtain

$$\begin{aligned}\sum_{i=1}^{m} l_i &= q^2+q+1;\\ \sum_{i=1}^{m} il_i &= |B|(q+1);\\ \sum_{i=1}^{m} i(i-1)l_i &= |B|(|B|-1).\end{aligned}$$

It follows that

$$(|B|-q-\sqrt{q}-1)(|B|-q\sqrt{q}-1)=\sum_{i=1}^{m}(i-1)(i-\sqrt{q}-1)l_i\leq 0.$$

Hence $|B| \geq q + \sqrt{q} + 1$.

In case of equality, all lines intersect the blocking set either in 1, or in precisely $\sqrt{q} + 1$ points, and B is a Baer subplane. □

Bruen's bound implies that a blocking set in $PG(2,3)$ has at least 6 points. Since the complement of a blocking set is again a blocking set, and since there are 13 points altogether, the only possible sizes are 6 and 7. In order to find all of them it sufficies to consider the case $|B| = 6$. From the equations $l_1 + l_2 + l_3 = 13$, $l_1 + 2l_2 + 3l_3 = 24$ and $2l_2 + 6l_3 = 15$, we get $l_1 = 6$, $l_2 = 3$ and $l_3 = 4$. The four 'three-lines' intersect pairwise in a point of B, and no three are concurrent. Hence they form a dual arc, and B consists of the 6 exterior points of a conic.

The next example, a projective triangle, is essentially due to di Paola [36]. Existence in general odd order Desarguesian planes was shown by Bruen [19]. Fix a coordinate frame, and let $B_1 = \{(0 : 1 : -a^2) \,|\, a \in GF(q)\}$; B_2 and B_3 are obtained by cyclicly rotating the coordinates of the points in B_1, so $B_2 = \{(-a^2 : 0 : 1) \,|\, a \in GF(q)\}$. Claim: $B = B_1 \cup B_2 \cup B_3$ is a blocking set of size $3(q+1)/2$.

Proof of the claim. Consider a line L. If L contains any of the points $(0:0:1)$, $(0:1:0)$ or $(1:0:0) \in B$, then L intersects B, otherwise L contains points $(0:1:a)$, $(b:0:1)$ and $(1:c:0)$, $a,b,c \neq 0$. The collinearity of these three points implies that as vectors they are dependent, which is equivalent to $abc + 1 = 0$, or equivalently $(-a)(-b)(-c) = 1$. Since 1 is a square this implies that either 1 or 3 of $-a$, $-b$, $-c$ are squares.

Note that the above example is of Rédei type.

In [36] di Paola says that it might be the case that for q an odd prime this is best possible. Later in this course we shall see that she was right. It might even be true that for $q \neq 7$ prime, the example is (projectively) unique. In the plane of order 7 there is another blocking set of size 12. This set can be described as follows: Consider the set B defined above, but remove the 'corners' $(1:0:0)$, $(0:1:0)$, $(0:0:1)$. What is left is a set of 9 points. Now look at the 12 lines that meet this set in 3 points. These lines cover the points of the plane, so they form a dual blocking set. This set is not of Rédei type. On the other hand it was shown by Gács [28] that for $q = 11$ the projective triangle is the unique minimal example.

The Baer subplanes and the projective triangles give blocking sets of the smallest possible size in the planes of order at most 31, with the exception of $PG(2,8)$ and $PG(2,27)$. Examples in these planes will follow from more general constructions later on in the course.

1.3. Large blocking sets

The complement of a blocking set is again a blocking set, so large blocking sets are just complements of small blocking sets. The question of finding upper bounds for the size of a blocking set becomes more interesting if we require the set to be minimal, in the sense that no subset of it is still a blocking set. Being minimal is equivalent to having a tangent at every point. Before stating and proving the main result on large minimal blocking sets, first a definition.

A *unital* in Π_q is a set U of $q\sqrt{q}+1$ points, such that every line joining two points of U intersects U in precisely $\sqrt{q}+1$ points.

Again straightforward counting gives that all other lines of the plane intersect U in precisely one point, and in fact at each point of U there is a unique tangent. So a unital is a minimal blocking set. In fact it turns out to be the largest one.

Theorem 1.2 (Bruen, Thas [24]). *Let B be a minimal blocking set in Π_q. Then $|B| \leq q\sqrt{q}+1$ with equality if and only if B is a unital.*

Proof : Let $|B| = bq+1$. We may compute $\sum l_i$, $\sum il_i$ and $\sum i(i-1)l_i$ as before, and this enables us to compute

$$s = \sum_i (i-b-1)^2 l_i.$$

Since B is minimal, every point is on a tangent, so $l_1 \geq |B|$, and $s \geq |B|b^2$. Hence

$$0 \leq s - |B|b^2 = (b+1)q(q-b^2).$$

This gives that $b \leq \sqrt{q}$ and as before, in case of equality all lines intersect B in either 1 or $\sqrt{q}+1$ points, so that B must be a unital. □

1.4. Possible sizes of blocking sets

So far we have looked at small and large minimal blocking sets. Here we will briefly survey what is known for the spectrum of cardinalities of minimal blocking sets. If q is not a square then it should be possible to essentially improve the Bruen-Thas upper bound $q\sqrt{q}+1$, but this seems to be a difficult problem. In [11] it is shown that if $q \geq 25$ is a square, then there is no minimal blocking set of size $q\sqrt{q}$.

One would expect the situation to be roughly the following: For a large interval, say roughly from $2q$ to $q\sqrt{q} - c \cdot q$ for some (possibly large) constant c there exist minimal blocking sets of every possible size. So the excluded cardinalities are some small ones, all at most $2q$, and on the other hand some large ones, all close to $q\sqrt{q}$.

The following result of Innamorati and Maturo [31] indicates that at least the lower bound of this interval is more or less correct:

Theorem 1.3 *In a Desarguesian plane of order at least 4 there exists a blocking set of order k if $2q-1 \leq k \leq 3q-3$.*

The blocking sets they construct are contained in the union of 4 lines. For small planes the result is quite useful: If $q = 4$ or 5 this interval coincides with the entire interval from lower to upper bound. For $q = 7$ the interval contains all numbers except the lower bound 12 (realized by the projective triangle, and the sporadic example described earlier) and the upper bound 19, realized by an interesting configuration found by Brouwer [15], and also by Biliotti and Korchmáros [4] (the points form an orbit of a subgroup of index 3 of a Singer cycle). A discussion of these cases can also be found in the nice paper by Cameron [25].

For $q = 8$ there is a construction giving the lower bound 13. The interval in the theorem is $[15, 21]$. There is no blocking set of size 14 of Rédei type in $PG(2, 8)$. For $q = 9$, the lower bound 13 is realized by a Baer subplane, size 14 does not occur by a result of Bruen and Silverman [22], constructions for 15,16 and 17 can be found in [25]. The interval [17,24] is taken care of by the theorem. Constructions for 25 and 26 were given by Illés, Szőnyi and Wettl [30]. Non-existence of a minimal blocking set of size 27 is still open. The upper bound 28 is realized by an arbitrary unital (there are at least 2 non-isomorphic ones).

For large q not too much is known. Using a theorem of Ughi [45], saying that the union of a constant number of conics can not be a blocking set if q is large enough, Szőnyi [43] showed the existence of minimal blocking sets of size $c \cdot q \log q$. Later, together with Hirschfeld he constructed minimal blocking sets of size $c \cdot q^{1+\lambda}$, $1/4 < \lambda \leq 1/2$, $q > q_0(\lambda)$, in the case that q is a square [29].

This shows that in the entire range between lower and upper bound there are cardinalities belonging to the spectrum.

1.5. Related concepts

We finish this introduction by mentioning two related concepts. In [30] a *strong representative system* (short: s.r.s.) in Π_q is defined as a set of flags (incident point-line pairs) (P_i, L_i), such that for $i \neq j$, $P_i \notin L_j$. A s.r.s. is maximal if it is not contained in a larger one. From a minimal blocking set or a line (or a dual blocking set, or the collection of lines through a point) a s.r.s. of the same size may be constructed by taking the pairs (P, L), P a point of the blocking set and L a fixed tangent through P (or dually). In this way we get s.r.s.'s of size $q + 1$, and $\geq q + \sqrt{q} + 1$ respectively. The upper bound for the size of a s.r.s. is again $q\sqrt{q} + 1$, as it was for minimal blocking sets, with the same proof. The best known lower bound, assuming the system does not have all points collinear, or lines concurrent, is only $q + \frac{1}{2}\sqrt{q}$. [11]

Another related concept is that of a *tangency set*. This is a set of points such that through each of them there is at least one tangent. Again minimal blocking sets are examples of maximal tangency sets, and Bruen and Drudge recently showed that the size of a maximal tangency set in Π_q that is not a line, is at least that of a minimal blocking set. The upper bound $q\sqrt{q} + 1$ can be obtained, with the same proof as for blocking sets.

2. Lacunary polynomials

2.1. What is a lacunary polynomial

Most of us have been pleasantly surprised by the factorization $x^2 - a^2 = (x+a)(x-a)$ at some point in life. We ask ourselves now more generally, what are the polynomials $f(x) = x^n + g(x)$, with $g(x)$ a polynomial of small degree (compared to n), that factor into linears over some field K (equivalently, all zeroes of f are in K). Over the field $\mathbf{C}$ of complex numbers every polynomial factors into linears, so there the question is not interesting. Over the field $\mathbf{R}$ it is a nice exercise to show that g has to have degree at least $n-2$, which can hardly be called small. As it turns out however for finite fields the problem is much more interesting, and moreover it is intimately related to the theory of blocking sets. (Irrelevant side remark: what about fields like $\mathbf{Q}[i]$?) The basic results are due to Rédei [39]. We start with some notation and a definition.

The degree of a polynomial $f(x)$ will be denoted by f°. So $f(x) = f_0 x^{f^\circ} + g(x)$ for some polynomial g of smaller degree. Occasionally we need the *second degree* $f^{\circ\circ} = g^\circ$. We say that f is *lacunary* if $f^{\circ\circ} < f^\circ - 1$. Let K be a field. We say that $f(x) \in K[x]$ is *fully reducible* if f factors into linear factors over $K[x]$ (equivalently, all zeroes of f are in K).

Theorem 2.1 (Rédei) *Let $f(x) = x^q + g(x) \in GF(q)[x]$, and assume f is fully reducible over $GF(q)$. Then $g(x) = -x$ or $g'(x) = 0$ or $g^\circ \geq \frac{q+1}{2}$.*

This is (by far) the easiest of a number of similar theorems. We include the proof since it is so nice.

Proof : Write $f = s.r$ where s contains the different linear factors of f, all exactly once, and r the rest. Since all zeroes of f are in $GF(q)$ one has $s \mid x^q - x$. Combined with $s \mid x^q + g(x)$ we conclude $s \mid x + g(x)$. For r we get the divisibility $r \mid f'(x) = g'(x)$. Combining this we get

$$f = s.r \mid (x+g)g'.$$

Now the right hand side is either zero, and then $g(x) = -x$ or $g'(x) = 0$, or it has degree at least $f^\circ = q$, so that $g^\circ \geq (q+1)/2$. □

Most of Rédei's book is about the classification of the fully reducible polynomials f with $g^\circ = \frac{q+1}{2}$, for us however the case $g'(x) = 0$ is more interesting. In this case g is a p-th power, where p is the characteristic of the field $GF(q)$, so $q = p^h$ say. If e is maximal such that g is in fact a p^e-th power, then Rédei shows $g^\circ \geq (q + p^e)/(p^e + 1)$ (by a reasoning similar to the above).

In the next paragraph we will see what all this has to do with blocking sets.

2.2. Blocking sets of Rédei type

Consider the projective plane $\Pi_q = A_q \cup \ell_\infty$. Let U be a set of q points of $A = A_q$. We want to construct a (minimal) blocking set B, such that $B \cap A = U$. The points of ℓ_∞ correspond to the parallel-classes of lines of the affine plane A. Consider two points u, $v \in U$. Among the q lines in the parallel class of lines containing uv, there must be at least one having empty intersection with U, since $|U| = q$, and $|U \cup uv| \geq 2$. In order to block those lines we are forced to add the point $uv \cap \ell_\infty$ to our blocking set.

Doing this for all pairs in U we obtain a set of size $q + m$ say, with m points on the line at infinity, where m is the number of directions determined by U. The blocking set B obtained this way is of Rédei type. Conversely, every minimal blocking set of Rédei type is obtained in this way.

In practice we choose U in such a way that it does not determine the vertical direction, so that it has exactly one point on each vertical line. If $A = AG(2, q)$ we may consider U as the graph of a function $f : GF(q) \to GF(q)$. We will now compute the number of directions determined by some particularly nice functions. So in all examples $U = U_f = \{(x, f(x)) \mid x \in GF(q)\}$, $A = AG(2, q)$. The set D_f of directions determined by f is given by

$$D_f = \left\{ \frac{f(x) - f(y)}{x - y} \mid x \neq y \in GF(q) \right\}.$$

1. Let $q = q_1^n$ and $f : x \to \mathrm{Tr}_{q \to q_1}(x)$. By linearity of the trace we have

$$\frac{f(x) - f(y)}{x - y} = \frac{\mathrm{Tr}(x) - \mathrm{Tr}(y)}{x - y} = \frac{\mathrm{Tr}(z)}{z}$$

for $z = x - y$. Now $\mathrm{Tr}(z_1)/z_1 = \mathrm{Tr}(z_2)/z_2$ if and only if either $\mathrm{Tr}(z_1) = \mathrm{Tr}(z_2) = 0$ or $z_1/z_2 = \mathrm{Tr}(z_1)/\mathrm{Tr}(z_2) (\in GF(q_1))$. Hence every nonzero value of $\mathrm{Tr}(z)/z$ is assumed $q_1 - 1$ times and zero is assumed q/q_1 times. This implies

$$|D_f| = 1 + \frac{q - q/q_1}{q_1 - 1} = 1 + \frac{q}{q_1}.$$

2. As before let $q = q_1^n$ and now $f : x \to x^{q_1}$. Again by 'linearity' we have

$$\frac{f(x) - f(y)}{x - y} = \frac{x^{q_1} - y^{q_1}}{x - y} = z^{q_1 - 1},$$

for $z = x - y$. So D_f consists of all (nonzero) $q_1 - 1$-st powers, and

$$|D_f| = \frac{q - 1}{q_1 - 1} = 1 + q_1 + q_1^2 + \ldots + q_1^{n-1}.$$

3. Let q be odd, and $f : x \to x^{(q+1)/2}$. Note that $f(x) = \pm x$, the sign depending on whether x is a square or not. By considering the four different possibilities for x and y one can show that
$$|D_f| = \frac{q+3}{2}.$$

The first two examples are of a very special nature. If $q = q_1^n$ then the affine plane $AG(2, q)$ can be interpreted as $AG(2n, q_1)$, and the graphs of the q_1-linear functions correspond to n-subspaces. The extension of those n-spaces to blocking sets can also be done in the more general setting of translation planes [17].

As an application of the results in the previous paragraph on lacunary polynomials we now present Rédei's original theorem on the possible number of directions. Write $K = GF(q)$.

Theorem 2.2 *Let $f : K \to K$ be any function, and let $m := |D_f|$. Then either $m = 1$, or $m \geq (q+3)/2$, or $2 + (q-1)/(p^e+1) \leq m \leq (q-1)/(p^e-1)$ for some e, $1 \leq e \leq [n/2]$.*

Proof : We may assume that $1 < m < q$. Let
$$H(x,y) := \prod_{w \in K} (x + yw - f(w)) = \sum_{j=0}^{q} h_j(y)x^j,$$
and for $a \in K$, let $H_a(x) := H(x, a)$. Then $H_a(x) = x^q - x$ if and only if $\{f(w) - aw \mid w \in K\} = K$, that is, if and only if $a \notin D_f$. Thus, if $1 < j < q$, then $h_j(y)$ vanishes for at least $q - m$ values of y. But in h_j no higher powers of y than y^{q-j} occur, and y^{q-j} has coefficient
$$\sum_{S \subset K, |S| = q-j} \prod_{w \in S} w = 0 \quad (\text{ for } 1 < j < q).$$
Hence h_j has degree at most $q - j - 1$, and if $m \leq j < q$ then $h_j = 0$. Now choose $a \in D_f$. We have $H_a(x) = \sum_j h_j(a)x^j$ and $(H_a)^{\circ\circ} \leq m - 1$. Choose $e_a \geq 0$ in such a way that $H_a \in K[x^{p^{e_a}}] \setminus K[x^{p^{e_a+1}}]$ (so that $H_a(x) = g(x)^{p^{e_a}}$ for some $g \in K[x] \setminus K[x^p]$). Let us remark that the definition of e_a guarantees that the lines with direction a intersect the graph of f in a multiple of p^{e_a} points, but not all in a multiple of p^{e_a+1}. Using Rédei's degree estimates we find that
$$m \geq 1 + (H_a)^{\circ\circ} \geq 2 + (q-1)/(p^{e_a} + 1).$$

As e is just $\min\{e_a \mid a \in D_f\}$, this is the lower bound in the theorem. We leave the derivation of the upper bound on m to the reader. It is a combination of combinatorial and geometrical arguments. $\square$

Recently far more has been deduced. The following result is proved in [9]. It classifies the functions that determine less than $(q+3)/2$ directions. The proof is heavily based on

Rédei's ideas, but is far more technical and involved. Again let $K = GF(q)$. Then K^2 may be mapped to $L = GF(q^2)$ by $(a, b) \mapsto \alpha a + \beta b$, for arbitrary α, $\beta \in L^*$ with $\alpha/\beta \notin K$. If F is a subfield of K, then K and hence also L is a vector space over F. A subset V of K^2 will be called F-linear, if it is mapped in this way to a F-subspace of L. It is easy to check that this property is well-defined, that is, it is independent of the choice of α and β defining the mapping.

Theorem 2.3 *Let $U \subset K^2$ be a point set of size q containing the origin, let D be the set of slopes of secants of U, and put $m := |D|$. Let e (with $0 \leq e \leq n$) be the largest integer such that each line with slope in D meets U in a multiple of p^e points. Then we have one of the following:*

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

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

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

(iv) $e = n$ *and* $m = 1$.

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

Let us say that a blocking set in $PG(2, q)$ is *small* if it has less than $3(q+1)/2$ points. This theorem classifies the small blocking sets of Rédei type, except in planes of even order. For a time it was believed (at least by me) that small blocking sets (in Desarguesian planes) were necessarily of Rédei type. This is (completely) false however. Only if $q = p$ is prime (then there are no small blocking sets), if $q = p^2$ (this follows from results of Szőnyi [44]) and if $q = p^3$ [37] small minimal blocking sets are of Rédei type. More about this in the next paragraph.

3. Extensions of Rédei's theorem

3.1. Recent bounds for general blocking sets

One of the most intrigueing problems in the area of blocking sets was di Paola's question whether the projective triangle is minimal among all blocking sets in $PG(2, p)$, p prime. It would mean that there is a tremendous gap between Bruen's general bound, $p + \sqrt{p} + 1$, and the size of the examples, $\frac{3}{2}(p + 1)$. As it turned out, di Paola was right, and the proof only needed a little generalization of Rédei's lemma on lacunary polynomials, and an obvious extension of the Rédei polynomial. For a detailed proof we refer to [8].

Theorem 3.1 *Let $f \in GF(q)[x]$ be fully reducible, and suppose that $f(x) = x^q g(x) + h(x)$, where g and h have no common factor. Let k be the maximum of the degrees of g and h. Then $k = 0$, or $k = 1$ and $f(x) = a(x^q - x)$, or q is prime and $k \geq (q+1)/2$, or q is a square and $k \geq \sqrt{q}$, or $q = p^{2e+1}$ and $k \geq p^{e+1}$.*

For blocking sets this result implies the following bounds:

Theorem 3.2 *Let S be a blocking set in $PG(2,q)$, where q is a power of the prime p. Then*

$$|S| \geq \begin{cases} p + (p+3)/2 & \text{if} \quad q = p; \\ p^n + p^{\lceil n/2 \rceil} + 1 & \text{if} \quad q = p^n, \ n > 1. \end{cases}$$

For q is prime, and for n is even, or $n = 3$ this result is best possible, so the first open case is $q = p^5$, where the correct lower bound should be $p^5 + p^4 + 1$ in stead of $p^5 + p^3 + 1$ as guaranteed by the theorem.

The bound for $q = p^3$ was conjectured by Bruen [19].

We repeat here the conjecture that the lower bounds coincide with the bounds we get for blocking sets of Rédei type:

Conjecture 3.3 *Let S be a blocking set in $PG(2,q)$, (q not a prime) and let $GF(q_1)$ be the largest subfield of $GF(q)$. Then $|S| \geq q + q/q_1 + 1$, and in case of equality S is projectively equivalent to the blocking set of Rédei type obtained from the trace function $GF(q) \to GF(q_1)$.*

The truth of the conjecture for q a square follows from Bruen's characterization of the Baer subplane as the minimal blocking set.

For $q = p^3$, ($p \geq 7$) Polverino [37] has shown that small blocking sets are of Rédei type, so that it follows from Theorem 2.3.

3.2. Small blocking sets

Recall that a blocking set in $PG(2,q)$ is small if it has less than $3(q+1)/2$ points. An important problem still is the classification of minimal small blocking sets. We already saw that small blocking sets of Rédei type are classified except if q is even. There exist however small blocking sets that are not of Rédei type. The examples are due to Lunardon [34], Polito and Polverino [38].

Let $q = q_1^n$, $n > 1$. The projective plane $\Pi = PG(2,q)$ has as its points and lines the 1- and 2- dimensional subspaces of $V = GF(q)^3$. Let V' be just V, but viewed as a $3n$-dimensional space over $GF(q_1)$. Points P and lines L then correspond to certain n- and $2n$-

dimensional subspaces (P', resp. L') of V'. Two subspaces are disjoint if their intersection is just the origin, otherwise they intersect. The n-spaces P' corresponding to the points of Π partition V' (minus the origin). Also if P' intersects L' then $P \in L$. Let W be an arbitrary $(n+1)$-dimensional subspace of V'. Since $n+1+2n > 3n$, W intersects every $2n$-dimensional subspace of V', in particular the $2n$-spaces corresponding to lines of Π. Define the set $B = B(W)$ to be the set of those points in $P \in \Pi$ for which P' intersects W.

Claim: B is either a line, or a blocking set of Π.

Proof of the claim: Let L be a line of Π, then the $2n$-space L' intersects W. Let $w \in L' \cap W$ ($w \neq \mathbf{0}$). The spaces P' partition V' hence cover W, so there is a point Q such that $w \in Q'$. Hence $Q \in L \cap B$. So we have shown that B intersects all lines. Suppose now that B contains a line L. This means that W intersects the $q_1^n + 1$ n-spaces in the $2n$-space L' that correspond to points, each in at least $q_1 - 1$ nonzero points. In total the subspace $L' \cap W$ then contains at least $q_1^{n+1} - q_1^n + q_1$ points, so it must be (at least) $n+1$-dimensional, and therefore $W \subset L'$. $\square$

The size of B depends a on the position of the $(n+1)$-space W with respect to the n-spaces P' of 'point-type'. If W contains the n-space P' corresponding to the point P, then intersections with other n-spaces of point-type Q' can be at most one-dimensional, since n-spaces of point-type are disjoint. So W intersects

$$1 + \frac{q_1^{n+1} - q_1^n}{q_1 - 1} = q_1^n + 1$$

n-spaces, and $|B| = q_1^n + 1 = q + 1$, i.e. B is a line. We also can see this as follows: If W contains P' of dimension n and intersects Q', then, being of dimension $n+1$, W is contained in the $2n$-space $< P', Q' >$, but this is exactly L', for the line L joining P and Q.

Next suppose $W \cap P'$ is $(n-1)$-dimensional for some point P. If for some point Q the intersection of Q' is two-dimensional then we may reason as above and get $W \subset < P', Q' >$ and B is again a line. Otherwise the intersection of W with point-type subspaces is at most one-dimensional, and we get

$$|B| = 1 + \frac{q_1^{n+1} - q_1^{n-1}}{q_1 - 1} = 1 + q_1^{n-1} + q_1^n.$$

A similar computation shows that the number of points of B on a line through P is either 1 or $q^{n-1} + 1$, so in fact B is of Rédei type.

The size of B will be maximal if $\dim(W \cap P') \leq 1$ for all P. In this case

$$|B| = \frac{q_1^{n+1} - 1}{q_1 - 1}.$$

The last example and the ones corresponding to most other intersection patterns of W will be not of Rédei type in general. Except when $n = 2$ or 3. For $n = 2$ we either get that B is a line or a Baer subplane. But also for $n = 3$ the resulting blocking set is necessarily of Rédei type.

In fact there is the following nice result by Polverino [37]

Theorem 3.4 *If B is a small minimal blocking set in $PG(2, p^3)$, where $p \geq 7$ is prime, then B is of Rédei type.*

As mentioned earlier, an important open problem is the classification of small blocking sets. The strongest result about the structure of small blocking sets is due to Szőnyi [44]

Theorem 3.5 *If B is a small minimal blocking set in $PG(2, q)$, where $q = p^n$. Then*

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

for some integer $e \geq 1$.

The proof combines the ideas in the original blocking set proofs, involving lacunary polynomials and the Rédei polynomial with estimates on the number of rational points on the intersection of two curves.

3.3. Multiple blocking sets

A subset B of a projective of affine plane is called a t-fold blocking set if B intersects every line in at least t points [20]. For $t > 1$ it makes no difference for the bounds we get whether we require in addition that B does not contain a line. For $t = 2$ or 3 we speak of *double* or *triple* blocking sets. An obvious idea to construct multiple blocking sets is to take unions of ordinary blocking sets. If q is a square we get a t-fold blocking set of size $t(q + \sqrt{q} + 1)$ in Π_q provided we can find t disjoint Baer subplanes. It was observed by a lot of people (for example in [27]) that $PG(2, q)$ can be partitioned into $q - \sqrt{q} + 1$ Baer subplanes, so here the construction works for all relevant t.

For very large t it makes more sense to look at the complement of B. If $k = q + 1 - t$, then the complement of B is a set intersecting every line in at most k points, and finding small t-fold blocking sets is equivalent to finding (n, k)-arcs with n large.

Using combinatorial arguments, similar to those in Bruen's proof of the lower bound for the size of an ordinary blocking set Ball [1] obtained the general lower bound $tq + \sqrt{tq} + t$ for the size of a t-fold blocking set in Π_q. For the Desarguesian plane it turned out that the theory of lacunary polynomials gives again much stronger results. In [3] it is shown that a double blocking set in $PG(2,q)$ contains at least the expected number of $2(q+\sqrt{q}+1)$ points. This result was improved by Gács and Szőnyi who characterized the minimal examples as the union of two Baer subplanes for large q.

For q prime the result we obtain is again much stronger.

Theorem 3.6 (Ball, [1]) *Let B be a t-fold blocking set in $PG(2,p)$. If $t \leq (p-1)/2$ then*

$$|B| \geq (t+\frac{1}{2})(p+1).$$

If $t \geq (p+1)/2$ then

$$|B| \geq (t+1)p.$$

For $t=1$ this is of course just the bound for ordinary blocking sets in Theorem 3.2. For $t=(p-1)/2$ and for $t=(p+1)/2$ the bounds are best possible, in view of the following examples: For $t=(p-1)/2$ we may take for S the set of exterior points of an irreducible conic. For $t=(p+1)/2$ we take the same set, together with all but one points of the conic.

For samll t the bound does not seem to be sharp. I conjecture that a double blocking set in $PG(2,p)$, p prime contains at least $3p$ points. For $p=2,3,5,7$ this is true, but this is not very impressing. A proof for $p=11$ would really convince me.

For the general case there is the following theorem.

Theorem 3.7 (B., Storme, Szőnyi,[13]) *Let B be a t-fold blocking set in $PG(2,q)$ of size $s(q+1)+c$. Let $c_2=c_3=2^{-1/3}$ and $c_p=1$ for $p>3$.*

1. *If $q=p^{2d+1}$ and $s<q/2-c_pq^{2/3}/2$ then $c \geq c_pq^{2/3}$*
2. *If $4<q$ is a square, $s<q^{1/4}/2$ and $c<c_pq^{2/3}$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*
3. *If $q=p^2$ and $s<q^{1/4}/2$ and $c<p\lceil\frac{1}{4}+\sqrt{\frac{p+1}{2}}\rceil$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*

In order to prove this we needed the following nice Rédei-type theorem on lacunary polynomials.

Theorem 3.8 *Let $f=x^{\sqrt{q}}g+h \in GF(q)[x]$, q square, be fully reducible with $(g,h=1$, $f' \neq 0$ and $k=\max(g^\circ,h^\circ)$. Then either $f(x)=a\,Tr(bx+c)+d$ or $f(x)=a\mathrm{Norm}(bx+c)+d$ for suitable constants a, b, c, d or $t \geq \frac{1}{4}+\sqrt{\frac{\sqrt{q}+1}{2}}$.*

4. Blocking sets in affine planes

4.1. Introduction

For an affine blocking set we usually don't require that it does not contain a line. An easy way to construct a blocking set of size $2q-1$ in A_q is then to take a line, together with one point on each of the $q-1$ parallels. Another way to obtain blocking sets for the affine plane is to start with a projective blocking set, remove one point, and add a point on all but one of the tangents through the removed point. Starting for example with a Baer subplane, or with a projective triangle will give a set of size $2q-1$ again.

In a lecture at Oberwolfach [26] Doyen asked whether this was the best one could do for the Desarguesian plane $PG(2,q)$. The surprising answer (yes) was given soon after that by Brouwer and Schrijver [16], but in fact a more general result had already been proved by Jamison [32] about half a year before.

Theorem 4.1 (Jamison, Brouwer/Schrijver). *A blocking set in $AG(2,q)$ has at least $2q-1$ points.*

The proofs are similar and only use elementary linear algebra. The contrast with the situation for projective planes is striking. First of all the bound is much larger, and in the second place, the bound only depends on the size of the field, not it's structure.

I will present a different proof here, since it gives me an excuse to introduce one of my favourite polynomials. But first we make a little detour and discuss nuclei.

4.2. Nuclei

In [41] Segre and Korchmáros prove that a set of $q+1$ points outside a conic in $PG(2,q)$, q odd, with the property that it intersects all secants and tangents of the conic, is necessarily a line. In [23] Bruen and Thas prove the same for q even. These results motivated the following question by Mazzocca:

Let B be a set of $q+1$ points in Π_q, not a line. A point P is called a *nucleus* of B if every line through P contains exactly one point of B (in other words, B is a blocking set of the lines through P). Question: How many nuclei can there be? This question was answered in [14]:

Theorem 4.2 *The number of nuclei of a $(q+1)$-set B in $AG(2,q)$ is at most $q-1$.*

Note that this indeed answers the question, because if B is not a line, then there is a line ℓ disjoint from B. This line does not contain any nuclei, so all nuclei of B are in the affine plane $PG(2,q)\setminus\ell$.

Much later I realized that this result could be generalized as follows: let B be a set of points in the affine plane $AG(2,q)$, of size $q+t$ say. A point P is called a nucleus of B if every line through P contains at least one point of B (so B is still a blocking set of the lines through P).

Theorem 4.3 [6] *The number of nuclei of a $(q+t)$-set B in $AG(2,q)$ is at most $t(q-1)$.*

Proof : We restrict to the case $t<q$, since otherwise everything is obvious.

We may identify the points of $\mathcal{A}=AG(2,q)$ with the elements of $GF(q^2)$ in a suitable way. Through every point of $\mathcal{A}$ there are $q+1$ lines, one from each parallel class. There is a natural correspondence between the $q+1$ different parallel classes, and the $q+1$-st roots of unity in $GF(q^2)$. For two points a and b, the direction of the line joining them corresponds to the value of $(a-b)^{q-1}$.

With the set B, considered as a subset of $GF(q^2)$, we associate the following polynomial in two variables

$$F(X,T)=\prod_{b\in B}(T-(X-b)^{q-1}).$$

Consider now a nucleus x of B. This means, that every line through x contains a point of B. If we consider the multiset

$$\{(x-b)^{q-1}\mid b\in B\},$$

then every $q+1$-st root of unity occurs. This implies that the polynomial $F(x,T)\in GF(q)[T]$ is divisible by $T^{q+1}-1$ whenever x is a nucleus of B. Let $\sigma_j(X)\in GF(q)[X]$ denote the j-th elementary symmetric function of the set of polynomials:

$$\{(X-b)^{q-1}\mid b\in B\}.$$

Note that σ_j has degree at most $j(q-1)$, and the degree equals $j(q-1)$, precisely if the binomial coefficient $\binom{|B|}{j}$ doesn't vanish. If the polynomial F is expanded in powers of the variable T, we get

$$F(X,T)=\sum_{j=0}^{|B|}(-1)^j\sigma_j(X)T^{|B|-j}.$$

If we now substitute for the variable X a nucleus x of B, and use the divisibility property above, we get (with $|B|=q+t$):

$$F(x,T)=(T^{q+1}-1)(T^t+\text{ terms of lower degree }).$$

Expanding this again, we note that the coefficient of T^q is zero, since $t<q$. Since this coefficient equals $(-1)^t\sigma_t(x)$, we see that $\sigma_t(x)=0$, for all nuclei x of B. Since

$$\binom{q+t}{t}\neq 0,$$

$\sigma_t(X)$ has degree $t(q-1)$, and hence the number of nuclei of B is at most this number. $\square$

There are several nice aspects about these theorems. First of all the bounds are all best possible: A set B consisting of a line and t points on different parallels has exactly $t(q-1)$ nuclei. For $t = 1$ only one other example with $q - 1$ nuclei is known, a set of 6 points in the plane of order 5.

The second nice aspect is that if B of size $q+t$ is an affine blocking set then the remaining $q^2 - q - t$ points are nuclei, so we must have $q^2 - q - t \leq t(q-1)$, which is the same as $t \geq q - 1$. So the affine blocking set theorem is a corollary.

4.3. Multiple blocking sets in affine planes

Just as for projective planes we now consider the problem of t-fold blocking sets for affine planes.

Using essentially the methods of Jamison and Brouwer-Schrijver, Bruen [21] obtained the lower bound $(t+1)q - t$, for the size of t-fold blocking set in $AG(2,q)$.

Again generalizing the notion of a nucleus I was able to improve the lower bound to $(t+1)q - 1$, but only if $(t,q) = 1$. Both results are part of the following more general very recent result by Ball [2].

Theorem 4.4 *Let B be a t-fold blocking set in $AG(2,q)$, and let $p^e = (q,t)$. Then $|B| \geq (t+1)q - p^e$.*

The proof consists of a clever observation added to the proof in [6], which in fact is a straightforward generalization of the proof in the previous paragraph.

Note that this bound is sharp for $AG(2, q = 2^h)$ and $t = q - 2^e$. Let B be the complement of a Denniston arc $(2^e q - q + 2^e, 2^e)$.

Analogous results for affine blocking sets in higher dimensional affine spaces have been obtained by Sziklai [42] and Ball [2].

References

[1] S. Ball, On sets of points in finite planes, Ph.D.-thesis, Sussex (1994).

[2] S. Ball, On nuclei and blocking sets in Desarguesian spaces, manuscript (1998).

[3] S. Ball and A. Blokhuis, On the size of double blocking set in $PG(2,q)$, *Finite Fields and their applications*, **2** (1996), 125–137.

[4] M. Biliotti and G. Korchmáros, Transitive blocking sets in cyclic projective planes, *Mitteilungen aus dem mathem. Seminar Giessen*, **201**, (1991), 35–38.

[5] A. Blokhuis, On nuclei and affine blocking sets, *J. Combin. Theory (A)* **67** (1994), 273–275.

[6] A. Blokhuis, On multiple nuclei and a conjecture of Lunelli and Sce, *Bull. Belg. Math. Soc.* **3**, (1993), 349–353.

[7] A. Blokhuis, On the size of a blocking set in $PG(2, p)$, *Combinatorica*, **14**, (1994), 111-114.

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

[9] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes of the graph of a function defined on a finite field, *J. Combin. Theory A*, to appear.

[10] A. Blokhuis, A.E. Brouwer and H.A. Wilbrink, Heden's Bound on Maximal Partial Spreads, *Discrete Mathematics*, **74**, (1989), 335–339.

[11] A. Blokhuis and K. Metsch, Large minimal blocking sets, strong representative systems and partial unitals, in: *Finite Geometries*, (eds: F. De Clerck and J. Hirschfeld), Cambridge University Press. (1993), 37–52.

[12] A. Blokhuis, R. Pellikaan and T. Szőnyi, Blocking Sets of Almost Rédei Type, *J. Combin. Theory (A)*, **78** (1997), 141–150.

[13] A. Blokhuis, L. Storme and T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes, manuscript

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

[15] A.E. Brouwer, A Series of Separable Designs with Application to Pairwise Orthogonal Latin Squares. *Europ. J. Combinatorics*, **1**, (1980), 39–41.

[16] A.E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combin. Theory (A)*, **24**, (1978), 251–253.

[17] A.E. Brouwer and H.A. Wilbrink, Blocking sets in translation planes, *J. of Geometry*, **19**, (1982), 200.

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

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

[20] A.A. Bruen, Arcs and multiple blocking sets, in: *Proc. Conf. Finite Geometries, I.N.d.A.M.*, Rome (Italy), 1983.

[21] A.A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory (A)*, **60**, (1992), 19–33.

[22] A.A. Bruen and R. Silverman, Arcs and Blocking Sets II, *Europ. J. Combinatorics*, **8**, (1987) 351–356.

[23] A.A. Bruen and J.A. Thas, Flocks, chains and configurations in finite geometries. *Atti Accad. Naz. Lincei Rend.*, **59**, (1975), 744-748.

[24] A.A. Bruen and J.A. Thas, Blocking Sets, *Geom. Ded.* **6** (1977), 193–203.

[25] P.J. Cameron, Four lectures on projective geometry, in: *Finite geometries*, (eds.: C.A. Baker and L.M. Batten), Lecture notes in pure and applied mathematics **103**, Marcel Dekker, New York, Basel, 1985, 27–65.

[26] J. Doyen, Lecture at Oberwolfach, May 1976.

[27] J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas, Complete arcs in planes of square order, *Annals of Discrete Mathematics*, **30**, (1986), 243–250.

[28] A. Gács, Ph.D.-Thesis, Eötvös Lórand Un. (1997).

[29] J.W.P. Hirschfeld and T. Szőnyi, Constructions of Large Arcs and Blocking Sets in Finite Planes, *Europ. J. Combinatorics*, **12**, (1991), 499–511.

[30] T. Illés, T. Szőnyi and F. Wettl, Blocking Sets and Maximal Strong Representative Systems in Finite Projective Planes, *Mitteilungen aus dem mathem. Seminar Giessen*, **201**, (1991), 97–107.

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

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

[33] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Scientiarum Mathematicarum Hungarica*, **16**, (1981), 449–454.

[34] G. Lunardon, Normal spreads, *Forum Mathematicum*, submitted (1997).

[35] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, 2nd ed., Princeton Univ. Press, Princeton (1947).

[36] J. di Paola, On minimum blocking coalitions in small projective plane games, *SIAM J. Appl. Math.*, **17**, (1969), 378–392.

[37] O. Polverino, Small blocking sets in $PG(2, p^3)$, manuscript (1998).

[38] P. Polito and O. Polverino, On small blocking sets, manuscript (1997).

[39] L. Rédei, *Lückenhafte Polynome über endlichen Körpern,* Birkhäuser Verlag, Basel, 1970.

[40] M. Richardson, On finite projective games, *Proc. Amer. Math. Soc.*, **7**, (1956), 458–465.

[41] B. Segre and G. Korchmáros, Una proprietà degli insiemi di punti di un piano di Galois caratterizzante quelli formati dai punti delle singole rette esterne ad una conica. *Atti Accad. Naz. Lincei Rend.*, **62**, (1977), 1–7.

[42] P. Sziklai, Nuclei of point sets in $PG(n, q)$, *Discrete Math.*, **174**, (1997), 323–327.

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

[44] T. Szőnyi, Blocking sets in desarguesian affine and projective planes, manuscript (1996).

[45] E. Ughi, On (k, n)-blocking sets which can be obtained as a union of conics, *Geom. Ded.*, **26** (1988), 241–246.