On the spectrum of minimal blocking sets in PG$(2, q)$

Tamás Szőnyi, András Gács, and Zsuzsa Weiner

November 15, 2002

Abstract

The spectrum problem for minimal blocking sets means that we wish to determine the possible cardinalities of minimal blocking sets. Besides surveying the results on this problem some new results (or new proofs) are given.

1 Introduction

A *blocking set* in a projective or affine plane is a set of points which intersects every line. Actually, these are particular cases of 1-covers in hypergraphs; for a survey of these more general results on matchings and covers in hypergraphs the reader is referred to Füredi [31].

Throughout this paper, we will work in the Desarguesian affine and projective planes AG$(2, q)$ and PG$(2, q)$, see [39]. Hence $q = p^n$, where p is prime, $n \geq 1$. The letters q, p, n will always be used in this sense. For these planes, standard representations will be used.

For projective planes, the smallest blocking sets are just the lines. Blocking sets containing a line will be called *trivial*. 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 in just P. A blocking set is said to be *minimal* when no proper subset of it is a blocking set. It is equivalent to saying that each point of the blocking set is essential. Some authors call them *irreducible* instead of minimal. Note that a minimal blocking set in a projective plane is either a line, or does not contain a line. The terminology is not standard; sometimes it is supposed that a blocking set contains no line.

It was observed already in 1947 by von Neumann and Morgenstern that $\mathrm{PG}(2,2)$ does not contain non-trivial blocking sets. For $q > 2$, the vertexless triangle (that is $(\ell_1 \cup \ell_2 \cup \ell_3) \setminus \{\ell_1 \cap \ell_2, \ell_1 \cap \ell_3, \ell_2 \cap \ell_3\}$ for three non-concurrent lines ℓ_1, ℓ_2, ℓ_3) is always a minimal blocking set of size $3q-3$. Similarly, if $P_1 \in \ell_1$, $P_2 \in \ell_2$, $P_1, P_2 \neq \ell_1 \cap \ell_2$, and P_3 is a point on the line joining P_1 and P_2, $P_3 \neq P_1, P_2$, then $(\ell_1 \cup \ell_2 \cup \{P_3\}) \setminus \{P_1, P_2\}$ is a minimal blocking set of size $2q$.

In this paper we survey the results about possible sizes of minimal blocking sets. Since there are other survey papers about blocking sets, and Chapter 13 of the second edition of Hirschfeld's book [39] also contains recent developments, we concentrate on results that are not contained in that chapter. The results are grouped according to different intervals in the spectrum of minimal blocking sets, and the last section is devoted to planes of small order. The general picture is roughly the following: small and large minimal blocking sets are difficult to construct. A blocking set is called *small* if it has size less than $3(q+1)/2$. There is hope that small minimal blocking sets can be characterized. For example, by a famous theorem of Aart Blokhuis [12], in desarguesian planes of prime order there are no small minimal blocking sets. There seems to be some structure in blocking sets of size between $3(q+1)/2$ and $2q-1$, particularly when the cardinality is close to the lower end of this interval. There are many blocking sets of size between $2q-1$ and $3q-3$, but no examples of minimal blocking sets of size cq are known, where c is a constant larger than 3. There are several constructions giving minimal blocking sets of size $cq \log q$, and this seems to be the "typical cardinality" of a minimal blocking set. Very few constructions give larger blocking sets; a new construction is sketched here, see [28]. For planes of square order there are unitals and one can locally modify unitals by adding points not in the unital and deleting points of the unital to obtain a minimal blocking set. Essentially the same picture is described in Cameron [26], together with some experience in planes of small order.

In the next section two general constructions, giving minimal blocking sets, are discussed. These can be used in more than one interval of the spectrum.

Blocking sets in non-desarguesian planes, in higher dimensions, or in other geometric structures; or multiple blocking sets are also very interesting, but this paper focuses only on blocking sets in $\mathrm{PG}(2,q)$. Previous surveys on blocking sets are Berardi–Eugeni [6] (in Italian), Blokhuis [13], Szőnyi [71], Sziklai–Szőnyi [69]. Other surveys also contain information on blocking sets, see Hirschfeld–Storme [40], [74]. Some of these surveys contain information on non-desarguesian planes, higher dimensions, multiple blocking sets, as well.

2 General constructions

2.1 The Rédei construction

Let us begin with the so-called *Rédei construction.* Take a subset U of size q in $\mathrm{AG}(2,q)$. An infinite point (m) is *determined by* U if there are two points $P_1, P_2 \in U$, such that $P_1, P_2, (m)$ are collinear. In most constructions the set U is the graph of a function f from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$, that is, $U = \{(x, f(x)) : x \in \mathrm{GF}(q)\}$. In this case (m) is determined when there are x, u such that $(f(x) - f(u))/(x - u) = m$. Let D denote the set of directions determined by U. Then $B = U \cup D$ is a minimal blocking set, if D is not the entire line at infinity. Since $|U| = q$, $|D| \leq q$, we obtain blocking sets of size at most $2q$ this way. When U is the graph of a function, this construction will be called *Rédei's construction.* Conversely, if B is a minimal blocking set of size $q + m$, $m \leq q$, and there is a line ℓ so that $|B \setminus \ell| = q$, then the blocking set can be obtained by Rédei's construction. Indeed, after a suitable change of coordinates one can always choose U as a graph of a function f and $B \cap l$ has to be the set of directions determined by U. Blocking sets of size $q + m$ that have an m-secant line will be called *blocking sets of Rédei type.*

There are important particular cases of this construction. These are listed in the following theorem.

Theorem 2.1 (1) *Let f be the function $f(x) = x^{(q+1)/2}$. Then $|B| = 3(q+1)/2$. This example is called the* projective triangle.

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

(3) *Let $f(x) = x^{q'}$. Then $|B| = q + (q-1)/\gcd(q-1, q'-1)$. For $q' = \sqrt{q}$ this gives* Baer subplanes.

More details on Rédei's construction will be given in the next two sections, but can also be found in [13], [75], [39, Chapter 13].

2.2 Blocking sets arising from projecting in three dimensions

The next construction, due to Polverino, Szőnyi, Weiner [64], is for Galois planes of square order.

Construction 2.2 *Let B' be a blocking set in $\mathrm{PG}(3,q)$ with respect to lines. Embed $\mathrm{PG}(3,q)$ as a subgeometry in $\mathrm{PG}(3,q^2)$. Choose a point P not in $\mathrm{PG}(3,q)$ and project B' from this point onto a plane $\pi \cong \mathrm{PG}(2,q^2)$.*

Then the projection B'' will be a blocking set of cardinality $|B''| = |B'| + 1 - |r \cap B'|$, where r is the unique line of $\mathrm{PG}(3,q)$ passing through P.

Of course, it is not at all obvious that the projection of a minimal blocking set is also a minimal one, but it was shown in [64] that in some cases the minimality can be guaranteed.

Result 2.3 *Suppose that through any point of $B' \setminus r$ there is a tangent line of B', which does not intersect r. Then B'' is minimal.*

Result 2.4 *When $|B'| \leq 2q^2 - 1$, then B'' is automatically minimal.*

As a particular case, let B be a blocking set of $\mathrm{PG}(2,q)$, and let B' be the cone with base B and vertex $V' \in \mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$. The previous construction gives a blocking set B'' of $\mathrm{PG}(2,q^2)$. This particular case is called the *cone construction*.

In case of the cone construction the minimality of B'' is less difficult to control than in the general case. For example, if the line r does not pass through V', then any point of B' not contained in the plane $\langle r, V' \rangle$ is projected onto an essential point of B''.

2.3 Blocking sets arising from projecting in high dimensions

In this section we generalize the results of [64]. Our aim is to extend Construction 2.2 to higher dimensions. To do this, first we need to extend the idea of projecting from a point to projecting from a subspace.

Definition 2.5 *Let β be an m-dimensional and Q an $(n-m-1)$-dimensional subspace in* $\mathrm{PG}(n,q)$*, $\beta \cap Q = \emptyset$. Take a point S from* $\mathrm{PG}(n,q) \setminus Q$*. The $(n-m)$-dimensional subspace $\langle Q, S\rangle$ intersects β in a unique point S', that will be called* the projection of S from Q onto β.

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

Lemma 2.6 *Let M be an $(h+1)$-dimensional subgeometry of order q in* $\mathrm{PG}(h+1,q^h)$*. Assume that R is an $(h-1)$-dimensional subspace of M and let R^* be the unique $(h-1)$-dimensional subspace of* $\mathrm{PG}(h+1,q^h)$ *that contains R.*

(i) *There exists an $(h-2)$-dimensional subspace P in R^* such that P does not intersect the subgeometry M.*

(ii) *An $(h-1)$-dimensional subspace containing P, different from R^* intersects the subgeometry M in 0 or 1 point.*

(iii) *Project the subgeometry M from P onto a plane π ($\pi \cap P = \emptyset$) of $PG(h+1,q^h)$ to obtain M'. Then there is a one-to-one correspondence between the points of $M \setminus R$ and their projections. The subspace R projects onto the unique common point R' of R^* and π.*

(iv) *Let l be a line in π. Then the pre-image of $l \cap M'$ is a hyperplane (of the subgeometry M) containing R or a line (of M) skew to R, according as the point R' was on the line l or not.*

Proof. See Gács, Weiner [36]. ■

Now we are ready to generalize Construction 2.2.

Construction 2.7 *Let B' be a blocking set in* $\mathrm{PG}(h+1,q)$ *with respect to lines, that is, a set of points which intersects every line. 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* PG$(h+1,q)$ *and let* R^* *be the unique* $(h-1)$*-dimensional subspace of* 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* PG$(h+1,q)$*, (for the existence of such a subspace see Lemma 2.6 (i)), and project* B' *from this subspace onto a plane* π *of* PG$(h+1,q^h)$*, where* $\pi \cap P = \emptyset$ *.*

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

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

Proof. Since B' is a blocking set in PG$(h+1,q)$ with respect to lines, it follows from Lemma 2.6 *(iv)* that B'' is a planar blocking set. Using *(iii)* the size of B'' can be calculated. ■

Generalizing Construction 2.2 this way allows us to repeat most of the results of [64] almost literally.

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

Proposition 2.8 *The point* $R'' = R^* \cap \pi$ *is always an essential point of* B''*. Suppose that through a point* S' *of* $B' \setminus R$ *there is a tangent line which does not intersect* R*. Let* S'' *be the projection of* S' *onto* π*. Then* S'' *is an essential point of* B''*. If this condition holds for each point of* $B' \setminus R$*, then* B'' *is minimal.*

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

Now pick a point S' of $B' \setminus R$. Denote its projection by S'' ($\neq R''$). By assumption there is a tangent $t_{S'}$ of B' through S' which does not intersect R. Consider the line $t'' = \langle t_{S'}, P\rangle \cap \pi$. From Lemma 2.6 *(iv)* it follows that t'' is a tangent of B'' at S'', hence S'' is essential. ■

Theorem 2.9 *Let* B' *be a minimal blocking set of* PG$(h+1,q)$ *with respect to lines and suppose that* $|B'| \leq 2q^h - 1$*. Then the projection* B'' *of* B' *(see Construction 2.7) is a minimal blocking set.*

This theorem is a generalization of Result 2.4. In [64] the essential lemma for proving Result 2.4 was a 3-dimensional extension of the following result due to Blokhuis and Brouwer [15].

Result 2.10 (Blokhuis, Brouwer) *Let B be a blocking set in* $\mathrm{PG}(2,q)$, $|B| = 2q - s$ *and let P be an essential point of B. Then there are at least $s+1$ tangents through P.*

Now we extend this result to arbitrary dimensions.

Lemma 2.11 *Let K be a blocking set in* $\mathrm{PG}(h+1,q)$ *with respect to lines. If $|K| = 2q^h + q^{h-1} + \ldots + q - s$, then there are at least $s+1$ tangent lines through each essential point of K.*

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

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

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

Proof of Theorem 2.9: By Construction 2.7 we only have to show that B'' is minimal. Pick a point T'' of B''. When $\langle T'', P \rangle = R^*$, then T'' is essential by Proposition 2.8. Otherwise, by Lemma 2.6 *(iii)*, there is a unique point T', which projects onto T''. By the previous lemma there are at least $q^{h-1} + \ldots + q + 2$ tangents of B' at T', hence there is at least one that does not intersect the subspace R. Applying Proposition 2.8 the result follows immediately. ■

Next we generalize the cone construction mentioned in the previous subsection.

Construction 2.12 *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'. Remark that the cone B' is a blocking set in* $\mathrm{PG}(h+1,q)$ *with respect to lines, hence using Construction 2.7 we can construct the blocking set B'' of* $\mathrm{PG}(2,q^h)$.

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

Remark 2.13 When the size of B is less than $2q$, then $|B'| < 2q^h$ holds; hence by Proposition 2.9, B'' is a minimal blocking set.

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

Let B be a projective triangle of $\mathrm{PG}(2,q)$ and use Construction 2.12 to obtain the cone B' and the blocking set B''. The cone B' has size $\frac{3}{2}(q+1)q^{h-1} + \frac{q^{h-1}-1}{q-1}$, hence, by Remark 2.13, B'' is minimal. To calculate the size of B'' (see above) we have to determine $|R \cap B'|$. Since R is an $(h-1)$-dimensional subspace, the intersection of the vertex V' of the cone and R contains an $(h-4)$-dimensional subspace of the subgeometry $\mathrm{PG}(h+1,q)$.

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

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

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

Corollary 2.14 *There are minimal blocking sets in* $\mathrm{PG}(2, q^h)$ *of size* $\frac{3}{2}(q+1)q^{h-1}+1-q^{h-1}$, $\frac{3}{2}(q+1)q^{h-1}+1-\frac{1}{2}(q^{h-1}+q^{h-2})$, $\frac{3}{2}(q+1)q^{h-1}+1-2q^{h-2}$, $\frac{3}{2}(q+1)q^{h-1}+1-q^{h-2}$, $\frac{3}{2}(q+1)q^{h-1}+1-\frac{1}{2}(q^{h-2}+q^{h-3})$ *and* $\frac{3}{2}(q+1)q^{h-1}+1$.

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

Construction 2.15 *Suppose that* B' *is the cone obtained by Construction 2.12. Assume that* Q *is a point of the plane* $\mathrm{PG}(2, q)$ *in Construction 2.12. Let* R *be the subspace spanned by* Q *and* V'*, and again use Construction 2.7 to obtain the blocking set* B'' *of* $\mathrm{PG}(2, q^h)$*. This construction will be called the* generalized cone construction*.*

Proposition 2.16 *Let* B *be a minimal blocking set of* $\mathrm{PG}(2, q)$ *and assume that* Q *is a point of* $\mathrm{PG}(2, q)$*, such that through each point of* $B \setminus Q$ *there passes at least one tangent line of* B*, not passing through* Q*. Then the blocking set* B'' *obtained by the generalized cone construction is minimal.*

Proof. By Proposition 2.8, it is enough to show that through each point of $B' \setminus R$ there passes at least one tangent line skew to R.

Let S' be a point of $B' \setminus R$ and denote the projection of S' from V' onto $\mathrm{PG}(2, q)$ by S. According to our assumption there is a tangent line t_S of B that passes through S and that is skew to Q. Hence the hyperplane $\langle V', t_S \rangle$ of the subgeometry $\mathrm{PG}(h+1, q)$ intersects the cone B' in $\langle V', S \rangle$ and it intersects R in V', only. Therefore any line of the hyperplane $\langle V', t_S \rangle$ through S' not contained in $\langle V', S \rangle$ is a tangent line of B' skew to R. ■

Corollary 2.17 *Let* B *be a minimal blocking set of* $\mathrm{PG}(2, q)$ *and assume that* Q *is a point of* B*. Then the blocking set* B'' *obtained by the generalized cone construction is minimal.*

Proof. ¿From the previous proposition it follows that the points of $B'' \setminus Q$ are essential, since a tangent line of $B \setminus Q$ cannot pass through Q. Proposition 2.8 proves the essentiality of Q. ■

Later in Section 3 we will use Construction 2.12 and the generalized cone construction to obtain various examples of minimal blocking sets of $\mathrm{PG}(2, q^h)$. As before (see [64]), the advantage of this construction is that it is very easy to control the intersection numbers of B'' with respect to lines.

2.4 An alternative (algebraic) way of constructing blocking sets

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

Replacing the base of the cone B' by hyperovals in the generalized cone construction one can obtain $(q+t,t)$-arcs of type $(0,2,t)$, for more details see [36]. In [36], there is also an algebraic description for the arcs obtained. Let ℓ be a line of $\mathrm{PG}(2,q^h)$ that intersects the subplane $\mathrm{PG}(2,q)$ in a subline and passes through the point Q. Choose a coordinate system, such that ℓ is the line at infinity $[0,0,1]$ and Q is the point $(0,1,0)$. First we write up the coordinates of the affine part of the blocking set B'' obtained by the generalized cone construction. This was done in [36] when the base of the cone is a hyperoval. There the structure of the base was not used, so we can repeat that result for an arbitrary point set, hence for a blocking set, too.

Lemma 2.18 *Assume that $B'' \subset \mathrm{PG}(2,q^h)$ is a minimal blocking set obtained by the generalized cone construction from the minimal blocking set $B \subset \mathrm{PG}(2,q)$. Let ℓ be a line of $\mathrm{PG}(2,q^h)$ that is secant to B (hence intersects the subplane $\mathrm{PG}(2,q)$ in a subline) and passes through the point Q. Choose a coordinate system, such that $\ell = [0,0,1]$ and $Q = (0,1,0)$; hence the points of $B \setminus \ell$ can be written in the form $(x_k, y_k, 1)$. Then*

$$B'' \setminus \ell = \{(x_k, y_k + i, 1) : (x_k, y_k, 1) \in B \setminus \ell_\infty, i \in I\}, \tag{1}$$

where I is a direct complement of $\mathrm{GF}(q)$ in the additive group of $\mathrm{GF}(q^h)$. ■

Here direct complement means a vector subspace I (over $\mathrm{GF}(q)$) of $\mathrm{GF}(q^h)$, where $|I| = q^{h-1}$, $I \cap \mathrm{GF}(q) = \{0\}$. The next remark shows that in some cases, (1) determines the minimal blocking set B'' uniquely.

Remark 2.19 Assume that B is a minimal blocking set in $\mathrm{PG}(2,q)$. Choose a line ℓ of $\mathrm{PG}(2,q)$, so that ℓ is a secant line to B or if ℓ is tangent to B, then there exists another line tangent to B through $B \cap \ell$. Delete the points of $B \cap \ell$. Note that the unique way to extend $B \setminus \ell$ to a minimal blocking set is to add the points of ℓ to B, through that there passes at least one 0-secant of $B \setminus \ell$ (different from ℓ), that is we get back B.

The next construction shows that I in (1) can be replaced by an arbitrary direct complement of $\mathrm{GF}(q)$ in $(\mathrm{GF}(q^h), +)$.

Construction 2.20 *Let B be a minimal blocking set in $\mathrm{PG}(2, q)$ and let $\ell_\infty = [0, 0, 1]$ be the line at infinity. For sake of simplicity, suppose that ℓ_∞ is secant to B. Choose a coordinate system such that $(0, 1, 0) \in B$. Then the points of $B \setminus \ell$ can be written in the form $(x_k, y_k, 1)$. Assume that $h > 1$ is an integer and I is a direct complement of $\mathrm{GF}(q)$. Let B^* be the following subset of $\mathrm{AG}(2, q^h)$:*

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

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

Proof. As in Section 3.2 of [36] one can show that $\bar{B} \setminus \ell$ can be obtained by the generalized cone construction starting from the minimal blocking set B, choosing Q to be the point $(0, 1, 0)$ and at the end deleting the points that were projected onto ℓ. Since this can be copied literally from [36], it is left to the reader.

Let B'' be the blocking set above obtained by the generalized cone construction. By Corollary 2.17 B'' is minimal. Now Remark 2.19 yields that B'' and $\bar{B}$ coincide, hence the result follows. ■

The proof above and Lemma 2.18 have the following consequence.

Corollary 2.21 *The minimal blocking sets obtained by the generalized cone construction are exactly the minimal blocking sets constructed by Construction 2.20.* ■

3 The spectrum problem for minimal blocking sets

3.1 Small minimal blocking sets

Since in this section we concentrate on blocking sets in $\mathrm{PG}(2, q)$, let us just briefly mention combinatorial results about the size of the smallest minimal non-trivial blocking set. The main result is due to Bruen [23, 24], (and Pelikán, who only published a weaker result [57], but in an unpublished manuscript had the lower bound): *the smallest minimal blocking set, different from a line, has at least $q + \sqrt{q} + 1$ points. In case of equality, the blocking set is the point set of a Baer subplane.*

Slight improvements on this result for planes of non-square order are due to Bierbrauer [11], Drake [29], and Kitto [48].

A blocking set is called *small* if it has size less than $3(q + 1)/2$. Such minimal blocking sets are characterized in some cases.

Theorem 3.1 (1) *(Blokhuis, [12]) If $q = p$ prime, then there are no small minimal non-trivial blocking sets in* $\mathrm{PG}(2, p)$ *at all;*

(2) *(Szőnyi, [73]) If $q = p^2$, p prime, then small minimal non-trivial blocking sets in* $\mathrm{PG}(2, p^2)$ *are Baer subplanes;*

(3) *(Polverino, [61]) If $q = p^3$, p prime, $p \geq 7$, then small minimal non-trivial blocking sets in* $\mathrm{PG}(2, p^3)$ *have size $p^3 + p^2 + 1$ or $p^3 + p^2 + p + 1$ and they are of Rédei type.*

Note that in Case (3) the blocking sets are unique. They either come from the graph of the trace function or from the graph of x^p. This follows from Theorem 3.9. This case is generalized to planes of order q^3, see Polverino, Storme [63]. The bound in Theorem 3.1 (1) was conjectured by Di Paola [56], who studied the smallest non-trivial blocking sets in planes of small order. The lower bound in Theorem 3.1 (3) was conjectured by Bruen [24], and proved by Blokhuis [13].

In the general case, Szőnyi [73] proved that small minimal blocking sets intersect every line in 1 modulo p^e points for some $e \leq n/2$, confirming a conjecture of Blokhuis [13]. There are two approaches to studying small minimal blocking sets. Blokhuis [12], [13] used lacunary polynomials, which gave lower bounds on the size of blocking sets. The other approach is to use algebraic curves, which we shall see soon. Actually, when we have the 1 modulo p result, then the existence of e follows immediately. This result also implies that the possible sizes of small minimal blocking sets lie in certain, relatively short, intervals, a phenomenon discovered earlier by Rédei [65] for blocking sets of Rédei type. In [73], the following theorem was proved.

Theorem 3.2 (Theorems 5.6 and 5.12 in [73]) *Let B be a minimal non-trivial blocking set in* $\mathrm{PG}(2,q)$*, $q = p^n$. Suppose that $|B| < 3(q+1)/2$. Then*

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

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

Using the fact that lines intersect B in 1 modulo p^e points, Blokhuis and Polverino observed that the upper bound given in Theorem 3.2 can be improved by just counting arguments. The best intervals are due to Polverino [60]. Only the upper bound is stated here.

Theorem 3.3 *For a small minimal blocking set B in* $\mathrm{PG}(2,q)$*, $q = p^n$, there is an e such that every line meets B in 1 modulo p^e points, and*

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

where $\Delta = (1+(p^e+1)(q+1))^2 - 4(p^e+1)(q^2+q+1)$.

In her paper the lacunary polynomial approach was used for a lower bound, which requires that either $e = 1$, or $p^e \geq 9$. For the lacunary polynomial approach the reader is referred to Blokhuis [13], or [75]. Here we present a slight improvement on the size of the intervals, which implies that the 1 modulo p^e result remains true for the interval belonging to $p^e = 8$; so the only remaining case is $p^e = 4$ (some comments on this case will appear later in this section). Actually, it gives exactly the same lower bound as the one coming from the lacunary polynomial approach.

Let us first briefly recall the key steps of the proof of the 1 modulo p^e result from [73]. Let L be the line at infinity, $D := B \cap L$, and suppose that $\{(\infty)\} = D$ and that the line with equation $x = 0$ does not intersect $U := B \setminus L$. Give affine coordinates to the points of U; namely, let $U = \{(a_i, b_i) : i = 1, ..., q+k\}$. So $|B| = q + k + 1$. We will always suppose that $|B| \le 2q$, and that $k < q - 1$. Write up the *Rédei-polynomial* of U, that is,

$$H(X,Y) := \prod_i (X + a_iY - b_i) = X^{q+k} + h_1(Y)X^{q+k-1} + ... + h_{q+k}(Y). \quad (3)$$

Note that for all $j = 1, ..., q+k$: $\deg(h_j) \le j$. If $H(X,Y)$ is considered for a fixed $Y = y$ as a polynomial of X, then we write $H_y(X)$ (or just $H(X,y)$). Since $H(X,Y)$ vanishes for all $(x,y) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$, we can write it as

$$H(X,Y) = (X^q - X)f(X,Y) + (Y^q - Y)g(X,Y),$$

where $\deg(f), \deg(g) \le k$ as polynomials in two variables (see [12], [20]). If one fixes $Y = y$, then $H(X,y)$ is divisible by $(X^q - X)$ and for an $(x,y) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$: $f(x,y) = 0$ if and only if the line with equation $Y = yX + x$ intersects U in at least two points. To make this paper more or less self-contained, let us recall some results from [73].

Result 3.4 (1) (Theorem 4.6 in [73]) *If $k < (q+1)/2$ and $h(X,Y)$ is an irreducible polynomial dividing $f(X,Y)$, then $h'_X = 0$. This means that $h(X,Y) = u(X^{p^e}, Y)$ for some e.*

(2) (Corollary 4.8 in [73]) *If B is a minimal blocking set of size less than $3(q+1)/2$, then each line intersects it in 1 modulo p points.*

Now we recall some lemmas from [73], which will be improved in order to obtain the promised better lower bound for $|B|$.

Result 3.5 (Theorem 5.3 in [73]) *Assume that $k < (q+1)/2$ and let $h(X,Y) = u(X^{p^e}, Y)$ be an irreducible polynomial dividing $f(X,Y)$. Choose e in such a way that $u'_X \neq 0$. Then*

$$k \ge \frac{q}{p^e + 2}. \quad (4)$$

Result 3.6 (1) (Lemma 5.1 of [73]) *Let $h(X,Y) = u(X^{p^e}, Y)$ be an irreducible component of $f(X,Y)$. If the X-degree of u is denoted by t, then the total degree of u is at most tp^e, which is the total degree of h. The number of common points of $u(X,Y)$ and $u'_X(X,Y)$ is bounded from above by $2t^2p^e - t^2 - tp^e$.*

(2) (Lemma 5.2 of [73]) *The number of affine* GF(q)*-rational points of* $u(X,Y)$ *(which is the same as that of* $h(X,Y)$*) is at least* $qt - C$*, where* C *is the number of common points of* $u(X,Y)$ *and* $u'_X(X,Y)$*.*

In the actual statement of Lemma 5.2 in [73], the bound in (1) of Result 3.6 is substituted, but the proof gives the present formulation. This shows that if we improve on (1) of Result 3.6, then we can hope for a better lower bound. The key observation for the improvement is the following.

Claim 3.7 *When the intersection multiplicity of* u *and* u'_X *at* P *is* m*, then the intersection multiplicity of* $u(X^{p^e},Y)$ *and* $u'_X(X^{p^e},Y)$ *at a suitable* P^* *is at least* mp^e*.*

We will not use the fact that one of the curves is the derivative of the other. For example when $P = (0,0)$, then the point P^* is also $(0,0)$. This can be achieved by a suitable translation, as usual.

Sketch of the proof of the Claim: We will prove the claim for any two polynomials F, G instead of u and u'_X. The proof goes by induction with respect to the intersection multiplicity of F and G at $O = (0,0)$, which will be denoted by $I(P; F \cap G)$.

Recall first the algorithm, given by Scherk [67], to compute the intersection multiplicity at the origin. If F and G are two polynomials, not divisible by Y, then let $f(X) = F(X,0)$, $g(X) = G(X,0)$. The greatest common divisor of f and g is denoted by $d(X)$. Write $d(X) = a(X)f(X) + b(X)g(X)$, $f(X)/d(X) = c(X)$, $g(X)/d(X) = e(X)$. Then $I(O; F \cap G) = I(O; F^* \cap G^*)$, where $F^* = aG + bF$, $G^* = cG - eF$, since they generate the same ideal. Now G^* is divisible by Y, hence the intersection multiplicity can be reduced.

If we do the same procedure after substituting X^{p^e}, then we simply have to substitute X^{p^e} in place of X everywhere in the above algorithm. When $I(O; F^* \cap Y)$ is computed, then only the terms of F^* independent from Y are important. If we substitute X^{p^e} in this, then it will be a p^e-th power, hence the intersection multiplicity of this part will be multiplied by p^e. The same holds for the other part, because of the induction hypothesis. ■

Choose a component $h(X,Y) = u(X^{p^e},Y)$, $u'_X \neq 0$, where e is minimal. For this e, k is divisible by p^e. Since h was irreducible, u is automatically irreducible, Claim 3.7 gives that the number of common points of u

and u'_X multiplied by p^e is at most the number of common points of h and $u'_X(X^{p^e}, Y)$. Bézout's theorem gives that this is at most $\deg(h)(\deg(h) - p^e)$. This improves (1) of Result 3.6. Substituting this better bound in Result 3.6 (2), we get

$$qt - tp^e(t-1) \leq tkp^e,$$

from which $k \geq q/p^e - t + 1$ follows. On the other hand, $k/p^e \geq t$ is obvious. This gives $k \geq q/p^e - k/p^e + 1$, that is

$$k/p^e \geq \lceil \frac{q/p^e + 1}{p^e + 1} \rceil.$$

Here we used that k/p^e is an integer. It implies $k \geq p^e \lceil \frac{q/p^e+1}{p^e+1} \rceil$, which is the promised lower bound. If there is a line that meets B in 1 modulo p^e points, but not in 1 modulo p^{e+1} points, then there is a component $h(X, Y) = u(X^{p^i}, Y)$ for which $i \leq e$. Indeed, otherwise all lines would intersect B in 1 modulo p^{e+1} points. Comparing the lower bound for p^{e-1} and the upper bound for p^e one sees that it might happen that $i < e$, but only for $p^e = 4$. This simply means that when the size of the minimal blocking set is between $q+1+\frac{q+2}{3}$ and $\frac{1+5(q+1)-\sqrt{(1+5(q+1))^2-20(q^2+q+1)}}{2}$, then it can happen that every line intersects the blocking set in 1 modulo 4 points, but it is also possible that there are lines intersecting the blocking set in 3 modulo 4 points. (If someone believes that all small minimal blocking sets are linear, then this hypothetic interval would be empty, see Theorem 3.8 (1).) Note also that for $p^e = 2, 3$, the upper bound has to be replaced by $< 3(q+1)/2$.

Blocking sets of Rédei type show that the intervals for which e divides n are non-empty. A more general, very attractive construction, providing minimal blocking sets for $e|n$ again, was recently introduced by Lunardon [51], Polito and Polverino [58], see also [62]. The class of blocking sets arising from this construction is called the class of *linear blocking sets*. The construction comes from the representation of $\mathrm{PG}(2, q^t)$ in $\mathrm{PG}(3t-1, q)$ using the so-called normal (or geometric) spreads. Since there is a survey paper by Lunardon and Polverino [54] about linear blocking sets, we just mention a theorem that incorporates some consequences of this method on the spectrum of minimal blocking sets.

Theorem 3.8 *Consider the Galois plane* $\mathrm{PG}(2, q^t)$*.*

(1) (Polito, Polverino, [58]) *For the size of a linear blocking set B we have* $|B| \leq q^t + q^{t-1} + \ldots + q + 1$*;*

(2) (Lunardon, Polverino, [52]) *There are at least two non-isomorphic blocking sets of cardinality* $q^t + q^{t-1} + \ldots + q + 1$*, for* $t \geq 4$*;*

(3) (Lunardon, Polverino, [53]) *There are at least three non-isomorphic blocking sets of cardinality* $q^t + q^{t-1} + 1$*, for* $t \geq 4$*;*

(4) (Polito, Polverino, [58]) *There are non-Rédei type blocking sets of size* $q^t + q^{t-1} + \ldots + q^{t-r} + 1$*, if* $r \leq t - 2$*.*

(5) (Polito, Polverino, [59]) *Let B be a* $\mathrm{GF}(q)$*-linear blocking set in* $\mathrm{PG}(2, q^4)$*. If B is of Rédei type with at least two Rédei lines, then either B is a Baer subplane or B has* $q^4 + q^3 + 1$ *points,* $q + 1$ *Rédei lines and it is equivalent to the blocking set obtained from the graph of the trace function from* $GF(q^4)$ *to* $GF(q)$*. If B is of Rédei type with a unique Rédei line, then the possible sizes of B are* $q^4 + q^3 + 1$ *and* $q^4 + q^3 + q^2 + cq + 1$ *with* $c = -1, 0, 1$*. Finally, if B is not of Rédei type, then B has size* $q^4 + q^3 + q^2 + dq + 1$ *with* $d = 0, 1$*.*

For blocking sets of Rédei type we have an almost complete characterization. Aart Blokhuis et al. [14] proved the ultimate version of Rédei's theorem by showing that e must divide n and by characterizing all the examples. It essentially confirms the conjecture in [16]. Before stating the result we need a definition. Let K denote the field $\mathrm{GF}(q)$, $q = p^n$. Then K^2 may be mapped to $L = \mathrm{GF}(q^2)$ 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 (that is, $F = \mathrm{GF}(p^e)$, where e divides n), then K and hence also L is a vector space over F. A subset V of K^2 will be called *F-linear*, if it is mapped in this way to an F-subspace of L. It is easy to check that this property is well-defined, that is, it is independent of the choice of α and β defining the mapping.

Theorem 3.9 (Blokhuis, Ball, Brouwer, Storme, Szőnyi [14]) *Let* $U \subset K^2$ *be a point set of size q containing the origin, let D be the set of directions determined by U, and put* $N := |D|$*. Let e (with* $0 \leq e \leq n$*) be the largest integer such that each line with slope in D meets U in a multiple of* p^e *points. Then we have one of the following:*

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

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

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

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

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

Very recently, Simeon Ball [3] found a beautiful new proof of this result, which deals with the missing cases. This means that for $p^e = 2$ he proved the lower bound $q/2+1 \leq N$, and for $p^e = 3$ his method gives the GF(3)-linearity of the set U.

3.2 Blocking sets of size between $3(q+1)/2$ and $2q-1$

In this range there are mainly constructions, and some surprisingly tight bounds for Rédei type blocking sets. Let us begin with the constructions.

Using the Rédei construction, see Section 2.1, one can construct several blocking sets in this interval.

Theorem 3.10 (Megyesi) *Let* d *be a divisor of* $q-1$ *and let* H *be a multiplicative subgroup of size* d*. Consider the set* $U = \{(0,h) : h \notin H\} \cup \{(g,0) : g \in H\}$*. Then* U *determines exactly* $q+1-d$ *directions. Similarly, if* d *divides* q*, then using additive subgroups and two parallel lines (instead of the two axes) one can construct Rédei type blocking sets of size* $2q+1-d$*.*

Definition 3.11 *If* $d = (q-1)/2$*, then the Rédei type blocking set arising from Megyesi's construction is called the* projective triangle*, while for* $d = q/2$*, it is called the* projective triad *(we saw both of them in another form in Theorem 2.1, and it is easy to see that they are projectively equivalent).*

The projective triangles show that Blokhuis' bound (Theorem 3.1 (1)) is sharp when $q = p$ prime. The characterization of blocking sets of size $3(p+1)/2$ in PG$(2,p)$ is open. The Rédei type examples were first characterized as projective triangles by Lovász and Schrijver [50]. Blocking sets of size $3(p+1)/2$ which are not projective triangles seem to be very rare. In the plane of order 7, there is such a blocking set of size 12, coming from the embedding of an affine plane of order 3 in $\mathrm{PG}(2,7)$. For a more detailed description, see [13] or [35]. Recently, Blokhuis, Brouwer and Wilbrink [19] have found another example for $p = 13$. If $q \equiv 1 \pmod 3$, then the affine plane $\mathrm{AG}(2,3)$ can be embedded in $\mathrm{PG}(2,q)$ as the inflexions of a cubic curve, see Bichara, Korchmáros [10] or Vedder [79]. Consider the lines that are parallel in $\mathrm{AG}(2,3)$. They intersect each other in $\mathrm{PG}(2,13)$. This way we get 12 points, so together with the original 9 inflexions we have a set of 21 points. For $q = 13$, they form a blocking set. Note that for $q = 7$, they even form a double blocking set, that is, they intersect each line twice. Blokhuis, Brouwer and Wilbrink also did a computer search. For $p \leq 37$, they found that the only exceptions occur for $p = 7, 13$, in all the other cases a blocking set of size $3(p+1)/2$ must be a projective triangle. Besides this, the following partial result is known showing that a possible new example would be far away from being of Rédei type.

Theorem 3.12 (Blokhuis, Pellikaan, Szőnyi, Gács, Sziklai [18], [35], [33]) *Suppose B is a blocking set in $\mathrm{PG}(2,p)$ of size $\frac{3(p+1)}{2}$ which is neither a projective triangle nor one of the two sporadic examples described above. Then for any line l, $|B \setminus l| > p + \frac{p+45}{20}$.*

The Rédei type blocking sets coming from the previous construction are contained in the union of three lines. This class of blocking sets was first studied by Cameron [26]. It was proved in [70] that they always have size $2q + 1 - d$, where d divides either q or $q - 1$.

A different example, contained in the union of four lines, was constructed by Gács [32]. We shall give the affine part, the points at infinity come from the set of determined directions, see Rédei's construction.

Theorem 3.13 *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 N_i the number of directions determined by U_i. Then $N_1+N_2+N_3 = 3q + 1 - 2(q-1)/3$, and $N_i = 7q/9 + O(\sqrt{q})$.

Using Remark 2.13, if one starts with a minimal blocking set of size less than $2q$ in $\mathrm{PG}(2,q)$, several minimal blocking sets can be obtained, see

Corollary 2.14. It is not difficult to determine how many Rédei lines they can have. As an illustration we mention the following result, generalizing Corollary 2.9 of [64].

Proposition 3.14 *In* $\mathrm{PG}(2, q^h)$*,* $h \geq 2$*, there are minimal blocking sets of size* $(3(q+1)q^{h-1}/2)+1$*, which are not of Rédei type. There are minimal blocking sets of size* $(3(q+1)q^{h-1}/2)+1-q^{h-1}$*, which have exactly one or exactly two Rédei lines.*

At this point, it is worth mentioning that blocking sets with more than one Rédei line were characterized by Korchmáros and Mazzocca [49] and by Sherman [66]. For small minimal blocking sets the only ones with at least two Rédei lines are the examples mentioned in Theorem 2.1 (2), see also [53].

Looking at the examples given when $q = p$ is a prime, we see that one can obtain Rédei type blocking sets of size $3(p+1)/2$, and the next example coming from Megyesi's construction will have size at least $p + (2p+2)/3$. The following theorem almost reaches this bound.

Theorem 3.15 (Gács, [34]) *Let* B *be a Rédei type blocking set of* $\mathrm{PG}(2, p)$*, where* p *is prime. Then either* B *is the projective triangle or* $|B| \geq p + [2(p-1)/3] + 1$*.*

For general prime powers not much is known, except for the case $q = p^2$. In this case, using a lemma of Lovász and Szőnyi, Gács proved the following theorem.

Proposition 3.16 *Any blocking set in* $\mathrm{PG}(2, p^2)$ *of Rédei type of size* $3(p^2+1)/2$ *has to be equivalent to the projective triangle. If the Rédei type blocking set has more than this number of points, then it has at least* $1 + (3p^2+p)/2$ *points.*

First of all, it should be noted that this includes a characterization of the projective triangles, which does not seem to follow from Rédei's lacunary polynomial approach (and except for the cases $q = p$ and $q = p^2$, it is still open). In the prime case, the Lovász–Schrijver characterization result can be proved using Rédei's approach, see [75].

Note also that the bound in Proposition 3.16 is sharp: using Proposition 3.14 with $h = 2$, one gets a Rédei type blocking set of size $1 + (3p^2+p)/2$

in $\mathrm{PG}(2,p^2)$. Finally, we mention again that the cone construction can be used starting from any blocking set, not just the projective triangle. In particular, for planes of non-prime order one can obtain several examples of blocking sets, whose size is around $2q+1-d$, where d divides q or $q-1$. Some of them are of Rédei type, some are not.

Let us mention some open questions. The above results show that there is hope to prove gap theorems in this interval, too. It would be very interesting to have such results for arbitrary blocking sets, not just for blocking sets of Rédei type. One such result is known for almost Rédei type blocking sets. The proof of the next theorem can be more or less copied from [18].

Theorem 3.17 *Let B be a minimal blocking set in $\mathrm{PG}(2,p)$, p prime. Assume that $\frac{3}{2}(p+1) \le |B| < \frac{3}{2}(p+1) + \frac{1}{50}p + \frac{1}{10}$. If a line l contains at most $2p-|B|+1$ points of the blocking set B when $\frac{3}{2}(p+1) < |B|$, and at most $2p-|B|$ points when $\frac{3}{2}(p+1) = |B|$, then*

$$|l \cap B| \le |B| - p - (\frac{4}{5}p + 3 - \frac{|B|}{2}).$$

Proof. For $|B| = 3(p+1)/2$, this was proved in [18], so we can suppose that $|B| > 3(p+1)/2$.

Let $(\infty) \in B$, $N = |l \cap B|$. Assume to the contrary that $2p - |B| + 1 \ge N > |B| - p - (\frac{4}{5}p + 3 - \frac{|B|}{2})$. Let l be the line at infinity and write up the Rédei polynomial $H(X,Y)$ corresponding to $B \setminus l$. For this, let $B \setminus l = U = \{(a_i, b_i) : i = 1, \ldots, |B| - N\}$. Consider

$$\prod_{i=1}^{|B|-N} (X + a_i Y - b_i) = H(X,Y).$$

Since $\prod_{(m)\in B}(Y-m)H(X,Y)$ vanishes everywhere in $\mathrm{GF}(p)^2$, it can be written as $(X^p - X)u(X,Y) + (Y^p - Y)v(X,Y)$, hence

$$H(X,Y) = (X^p - X)f(X,Y) + \frac{Y^p - Y}{\prod_{(m)\in B}(Y-m)} v(X,Y).$$

The second term vanishes for any $Y = m$, where $(m) \notin B$, and the polynomial $f(X,m)$ factors into linear factors over $\mathrm{GF}(p)$ whenever $(m) \notin B$. This allows us to estimate the number of $\mathrm{GF}(p)$-rational points on the components of the curve $f(X,Y)$, see [18] or [69].

Take an absolutely irreducible component h of the curve f and denote the degree of h by s. The number of GF(p)-rational points of h is at least $(p+1-N)s - s(s-1)$.

When $s = 1$, h is a pencil of lines in the original plane. If the center H of the pencil h is in B, then H is a non-essential point of B, see [18], which contradicts the minimality of B. Hence there are at least $2(p+1-N)$ affine points of B, so $|B| \geq 2(p+1-N)+N$. It is a contradiction, since $N \leq 2p - |B| + 1$.

If $s = 2$, then h is a conic, hence it has exactly $p+1$ points. Using the lower bound on the number of the GF(p)-rational points of h from above and knowing that $|B| > \frac{3}{2}(p+1)$, we get a contradiction again.

Finally, when $s \geq 3$, then due to the Stöhr-Voloch bound (see [68], or [39, Chapter 2.11]), there are at most $2s(s-3) + 2s\frac{p+5}{5}$ GF(p)-rational points on h. Note that $s < (\frac{4}{5}p + 3 - \frac{|B|}{2})$. Comparing our upper and lower bounds on the number of GF(p)-rational points of h, we get that s cannot be bigger than 2, whence the result follows.

Note that this argument only has a meaning when $|B| - p - (\frac{4}{5}p + 3 - \frac{|B|}{2}) < 2p - |B| + 1$, from which we get the upper bound on the size of B. ■

3.3 Blocking sets of size greater than $2q-1$

In this range, there are only few constructions known. An attractive construction, due to Innamorati and Maturo [45] and Illés, Szőnyi, Wettl [43] gives minimal blocking sets of size k, where $2q-1 \leq k \leq 3q-5$. This construction will be used frequently for planes of small order. Since among the authors of [43], this was an idea of Illés, we shall call it the *IMI construction.*

Theorem 3.18 *In* PG$(2,q)$*,* $q \geq 4$*, there exists a minimal blocking set of size* k*, contained in the union of four lines, for every* k *with* $2q-1 \leq k \leq 3q-5$*. There are minimal blocking sets of size* $3q-4$ *and* $3q-3$*, too.*

Another quite general construction best works for $q \equiv 1 \pmod 4$. Let $\mathcal{P}_c$ be the parabola with equation $Y = X^2 + c$. The following result is easy to prove. Later we simply call it the *parabola construction.*

Theorem 3.19 ([72]) *Let* C *be an independent set in the Paley-graph* P_q*. Then* $\cup_{c \in C} \mathcal{P}_c$ *is a minimal blocking set of size* $|C|q+1$ *in* PG$(2,q)$*.*

Standard bounds for the size of an independent set in P_q, based on the character version of Weil's theorem, immediately give the existence of minimal blocking sets of size at least $cq \log q$. This was extended to $q \equiv 3 \pmod 4$ in [72].

Deep number theoretic results give slightly larger independent sets, see S. Graham, C. Ringrose [37].

A similar construction, giving not necessarily minimal blocking sets as unions of parabolas, is due to Abbott and Liu [1]. The probabilistic argument in Erdős, Silverman and Stein [30] shows that in some sense $cq \log q$ is the "typical size" of a minimal blocking set. For small values of q, such a phenomenon was observed by Cameron [26]. For blocking sets obtained as a union of conics, this was proved by Ughi [78], see also [71].

3.4 Large minimal blocking sets

The first result about large minimal blocking sets is due to Bruen and Thas [25]: a minimal blocking set has at most $q\sqrt{q}+1$ points. In case of equality the set has to be a unital, that means that there is a unique tangent at each point, and the non-tangent lines meet the set in $\sqrt{q}+1$ points. Unitals do exist in $\mathrm{PG}(2,q)$, q square; a Hermitian curve is always a unital. Recall that a Hermitian curve is defined by the equation $X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1} + X_3^{\sqrt{q}+1} = 0$.

Essentially nothing has been known for planes of non-square order, but recently it was shown by a simple combinatorial counting that a minimal blocking set can have at most $q\sqrt{q}+1-\sqrt{q}/8$ points; see [28].

For planes of square order $q \geq 49$, Blokhuis and Metsch [17] proved that there are no minimal blocking sets of size $q\sqrt{q}$. Their proof is combinatorial. For Galois planes (of even square order), they could lower the bound by one. For $q = 9$, Innamorati [44] proved that there is no minimal blocking set of size 27.

A variation of this result is the following. A set which meets every line in at most $\sqrt{q}+1$ points and has a tangent at each of its points is called a *partial unital*. Ball [2] proved that any partial unital whose size is larger than $q\sqrt{q}+1-\sqrt{q}$ can be embedded in a unital; therefore it cannot be a blocking set except when it is a unital. A different proof of this fact was given in [38].

The following non-existence result for large blocking sets was proved recently by Szőnyi and Weiner [76].

Theorem 3.20 *In* $\mathrm{PG}(2,q)$*, q square, there is no minimal blocking set of size* $q\sqrt{q}+1-\varepsilon$*, where* $1 \le \varepsilon \le \frac{1}{3}q^{1/6}$.

Unfortunately, the bound in this theorem does not give good results for planes of small order, hence in the next section we have to apply ad hoc arguments.

Regarding constructions, not much is known. The following construction is easy to prove (see [28]), but it was not noted explicitly earlier (it seems). It can also be regarded as a natural extension of Buekenhout's construction for unitals. Also related is a construction idea of Brouwer and Wilbrink [21].

Theorem 3.21 *In* $\mathrm{PG}(2,q^3)$*, there are minimal blocking sets of size* q^4+1.

Here is a sketch of the construction and the proof. Consider the well-known André, Bruck–Bose representation of the plane $\mathrm{PG}(2,q^3)$ (or a translation plane of order q^3 with kernel $\mathrm{GF}(q)$). It arises from a regular (or any) 2-spread of the hyperplane at infinity in $\mathrm{PG}(6,q)$. The affine lines of the plane are 3-dimensional subspaces containing the planes of the 2-spread. First we construct a set that blocks 3-dimensional subspaces. Take an ovoid O of a 3-space π, and a line ℓ disjoint to this subspace. Let B be a cone with vertex ℓ and base O. Then B is contained in a 5-dimensional subspace Π, and it blocks all the planes of this 5-dimensional subspace. Therefore, B meets every 3-space of $\mathrm{PG}(6,q)$. Now we put this cone in $\mathrm{PG}(6,q)$ in such a way that it yields a blocking set in the plane $\mathrm{PG}(2,q^3)$ defined by the given 2-spread. Choose π so that it meets each plane of the 2-spread in at most one point and let O meet the hyperplane at infinity in just one point X. Let σ be the plane of the 2-spread containing X. Let the line ℓ be contained in σ, $X \notin \ell$. Thus σ is contained entirely in B. Replace this plane by just one point at infinity, and consider the affine part of B. This way a set S of size q^4+1 is obtained in the plane $\mathrm{PG}(2,q^3)$, defined by the (regular) 2-spread. Since B intersects every 3-dimensional subspace, the set S is a blocking set of $\mathrm{PG}(2,q^3)$.

The only question is whether S is minimal or not. The line intersection numbers for S can easily be determined. First of all, any line through the infinite point in S (corresponding to σ) meets the affine part of S in either 0 or q^2 points. The other lines intersect the affine part of S in either 1 or $q+1$ points. All this follows from the fact that any plane of π meets O in either 1 or $q+1$ points. Hence through any affine point of S, there is a line meeting S in q^2+1 points, and hence there must also be tangents, since S contains q^4+1 points. ■

A similar construction works for planes of order q^h, and it gives the following result.

Theorem 3.22 *In* PG$(2, q^h)$, $h > 1$, *there are minimal blocking sets of size* $q^{h+1}+1$.

Using a slight variation of the above construction, even larger minimal blocking sets can be obtained. Modifying the position of O and ℓ with respect to the planes of the given 2-spread, one can get minimal blocking sets having q^4+q+1 points in PG$(2, q^3)$. For more details, see the manuscript of Cossidente, Gács, Siciliano, Szőnyi, Weiner [28].

For planes of square order, the situation is much better. In this case the following theorem was proved by Hirschfeld and Szőnyi [41].

Theorem 3.23 *For every* λ *with* $1/4 < \lambda \leq 1/2$, *there are constants* c_1 *and* c_2 *such that in* PG$(2, q)$, *q square, there are minimal blocking sets of size* k *with* $c_1 q^{1+\lambda} \leq k \leq c_2 q^{1+\lambda}$ *for* $q > q_0(\lambda)$.

Combining this with the general cone construction (see Section 2.3), for planes of fourth power order we get a similar result, but for $1/8 < \lambda \leq 1/2$. The process can be iterated: for planes of eighth power order one can get minimal blocking sets of size $q^{1+\lambda}$, where $1/16 < \lambda \leq 1/2$, and so on. As an illustration, the next theorem can be proved. It is stated for planes of order q^h, not only for planes of order q^2.

Proposition 3.24 *Let* B *be a unital of the plane* PG$(2, q)$, *q square. Embed* PG$(2, q)$ *into* PG$(h+1, q)$ *and choose an* $(h-2)$*-dimensional subspace* V' *according to Construction 2.12. As in that construction, let* B' *be the cone over* B *with vertex* V' *and let* B'' *be the projection of* B' *from* P. *Let* B^* *be a minimal blocking set contained in* B''.

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

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

Case 2. of this proposition shows how the generalized cone construction works for large blocking sets. According to Corollary 2.17, the subspace V' can always be chosen in such a way that B'' is a minimal blocking set. The size of B'' is $q^{h-1}(|B|-1)+1$. When $|B| \sim q^{1+\alpha}$, then $|B''| \sim (q^h)^{1+\alpha/h}$. For $h = 1$, this means that the exponents can roughly be halved, as remarked after Theorem 3.23. When $|B| \sim cq$, then $|B''| \sim cq^h$, so this does not give anything new about the spectrum.

3.5 Planes of small order

The general references for this section are [7], [8], [26], [45], [46], [25] and [43], but basically everything which is known is in Section 13.5 of the new edition of Hirschfeld's book [39], so we try to concentrate on the new facts, and give the references for those results.

$q = 3$. In PG(2, 3), the only minimal blocking sets are projective triangles (of size 6).

$q = 4$. The possible sizes for minimal blocking sets are $7, 8, 9$. Bruen's theorem says that a minimal blocking set of size 7 is a Baer subplane. Bruen and Thas proved that a minimal blocking set of size 9 is a unital, and for $8 = 2q$, the IMI construction works. For each cardinality, there is a unique example. For more details, see Berardi, Eugeni [7].

$q = 5$. By Blokhuis' result, the smallest blocking set has size 9. Already Jane di Paola [56] showed that there is a unique blocking set of size 9. The Bruen–Thas upper bound is 12, the IMI construction gives minimal blocking sets of size $10, 11, 12$. The examples are unique, except for 10, when there are seven different examples. For more details, see Berardi, Innamorati [8].

$q = 7$. The minimum size is 12 and there are two such blocking sets, one of them is the projective triangle. For the description of the other (non-Rédei) blocking set, see [13], or [35]. The IMI construction gives blocking sets of size $13, 14, 15, 16, 17, 18$. The Bruen–Thas upper bound is 19, and a minimal blocking set of this size can be obtained as the orbit of a subgroup of the Singer group. This example is unique, see Innamorati and Maturo [46].

$q = 8$. The minimum size is 13 (projective triad, see [47]). There is no minimal blocking set of size 14 (see Barát, Del Fra, Innamorati, Storme [5]), the IMI construction gives a minimal blocking set for each size between 15 and 21. Recently, Barát and Innamorati [4] constructed minimal blocking sets of size 22, 23, and 23 is the Bruen–Thas upper bound. The construction is very nice for 23, the blocking set consists of three disjoint Fano subplanes from a subplane partition of the plane minus a simplex, plus two vertices of the simplex. The existence of such a partition is guaranteed by a general result of Brown [22].

$q = 9$. The minimum size is again 13 (Baer subplane), there is no minimal blocking set of size 14 (this follows from [25], but also from the 1 modulo p result), and there are minimal blocking sets for each size from the interval $15, ..., 26$, see [43]. Minimal blocking sets of size 15 were classified by Pambianco and Storme [55]. They are the projective triangle and the dual of the 15 bisecants of a complete 6-arc. The latter one is not of Rédei type. The non-existence of a minimal blocking set of size 27 was proved by Innamorati [44], and for 28, we have the unitals.

$q = 11$. In Hirschfeld's book [39] (Theorem 13.28 (ii)), we see that there are minimal blocking sets of size $k = 18, 19$, and $21 \leq k \leq 30$. The first two examples are of Rédei type, and it is not too difficult to find a set of 11 points determining 9 directions, so there is a Rédei type blocking set of size 20. The other values come from the IMI construction. A random algorithm, see Cameron [26], found minimal blocking sets of size $22, \ldots, 29$. In 1000 trials, the frequencies were $16, 116, 284, 330, 197, 50, 6, 1$. This supports the impression that minimal blocking sets of size from the two ends of the spectrum are difficult to construct, while minimal blocking sets of size $cq \log q$ are abundant. The same phenomenon, concerning Erdős' problem, can be found in Béres, Illés [9] and Illés and Pisinger [42]. Let us briefly recall what the problem of Erdős is:

Does there exist an absolute constant c such that in any projective plane of order q, there is a blocking set intersecting every line in at most c points?

For the known results, the reader is referred to [42] or [27].

Let us close this survey with a list of known examples of minimal blocking sets of Rédei type in planes of small prime order. Columns correspond to the number of points on the Rédei line, rows to the order p of the plane, ! stands for a known example, $-$ for the known non-existence, while ? for the open cases.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	!	!	!																
3	!	-	!	!															
5	!	-	-	!	!	!													
7	!	-	-	-	!	!	!	!											
11	!	-	-	-	-	-	!	!	!	!	!	!							
13	!	-	-	-	-	-	-	!	-	!	!	!	!	!					
17	!	-	-	-	-	-	-	-	-	!	-	?	?	!	!	!	!	!	
19	!	-	-	-	-	-	-	-	-	-	!	-	?	!	!	-	!	!	!

Acknowledgement. The authors would like to express their warmest thanks to Prof. Leo Storme and Prof. Antonello Cossidente for their comments on an earlier version of this paper.

This research was partially supported by the Italian–Hungarian Intergovernmental Research Project *Finite geometry and its applications* (I–66/99).

The first and last author were also supported by OTKA Grant T–032455.

The second and third author were also supported by OTKA Grant F-030737 and FKFP Grant 0063/2001.

The second author was also supported by the Magyary scholarship from "Alapítvány a Magyar Felsőoktatásért és Kutatásért" and by OTKA Grant T-029255.

References

[1] H. L. Abbott and A. Liu, Property of $B(s)$ and projective planes, *Ars Combin.* **20** (1985), 217–220.

[2] S. Ball, Partial unitals and related structures in Desarguesian planes, *Designs, Codes and Cryptography*, **15** (1998), 231–236.

[3] S. Ball, personal communication.

[4] J. Barát and S. Innamorati, 23 is the largest size of a minimal blocking set in PG$(2,8)$, manuscript, 2001.

[5] J. Barát, A. Del Fra, S. Innamorati and L. Storme, Minimal blocking sets in PG$(2,8)$ and maximal partial spreads in PG$(3,8)$, *Design, Codes and Cryptography*, submitted.

[6] L. Berardi and F. Eugeni, Blocking sets e teoria dei giochi: origini e problematiche, *Atti Sem. Mat. Fis. Univ. Modena* **34** (1988), 165–196.

[7] L. Berardi and F. Eugeni, Blocking sets in the projective plane of order four, in: *Combinatorics '86* (eds.: A. Barlotti et al.), *Annals of Discrete Mathematics* **37** (1988), 43–50.

[8] L. Berardi and S. Innamorati, Irreducible blocking sets in the projective plane of order five, *Atti Sem. Mat. Fis. Univ. Modena* **38** (1990), 293–311.

[9] T. Béres and T. Illés, Computational investigation of the covering number of finite projective planes with small order (in Hungarian), *Alk. Mat. Lapok* **17** (1993/97), 397–411.

[10] A. Bichara and G. Korchmáros, n^2-sets in a projective plane which determine exactly $n^2 + n$ lines, *J. of Geometry* **15** (1980), 175–181.

[11] J. Bierbrauer, On minimal blocking sets, *Arch. Math.* **35** (1980), 394-400.

[12] A. Blokhuis, On the size of a blocking set in $\mathrm{PG}(2, p)$, *Combinatorica* **14** (1994), 273–276.

[13] 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.

[14] 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. Comb. Theory Ser. A* **86** (1999), 187–196.

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

[16] A. Blokhuis, A. E. Brouwer and T. Szőnyi, The number of directions determined by a function f on a finite field, *J. Comb. Theory Ser. A.* **70** (1995), 349–353.

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

[18] A. Blokhuis, R. Pellikaan and T. Szőnyi, Blocking sets of almost Rédei type, *J. Comb. Theory Ser. A* **78** (1997), 141–150.

[19] A. Blokhuis, A. E. Brouwer and H. A. Wilbrink, Blocking sets in $\mathrm{PG}(2, p)$ for small p, and partial spreads in $\mathrm{PG}(3, 7)$, manuscript, 2001–04–06.

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

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

[22] J. M. N. Brown, Partitioning the complement of a simplex in $\mathrm{PG}(e, q^{d+1})$ into copies of $\mathrm{PG}(d, q)$, *J. of Geometry* **33** (1988), 11–16.

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

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

[25] A. A. Bruen and J. A. Thas, Blocking sets, *Geom. Dedicata* **6** (1977), 193–203.

[26] P. J. Cameron, Four lectures on projective geometry, in: *Finite Geometry* (eds.: C.A. Baker, L.M. Batten), *Lecture Notes in Pure Appl. Math.* **103**, M. Dekker, New York, 1985, 27–65.

[27] J. A. Cornelissen, Ph. D. Thesis, DIKU.

[28] A. Cossidente, A. Gács, A. Siciliano, T. Szőnyi and Zs. Weiner, Large minimal blocking sets in Galois planes of non-prime order, in preparation.

[29] D. A. Drake, A bound for blocking sets in finite projective planes, in: *Contemporary Math.* **111** *"Finite Geometries and Combinatorial Designs"* (eds.: E. S. Kramer and S. S. Magliveras), Amer. Math. Soc. 1991, 93–97.

[30] P. Erdős, R. Silverman and A. Stein, Intersection properties of families of sets of nearly the same size, *Ars Combin.* **15** (1983), 247–259.

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

[32] A. Gács, On the number of directions determined by a point set in $\mathrm{AG}(2,p)$, *Discrete Math.* **208/9** (1999), 299–309.

[33] A. Gács, A remark on blocking sets of almost Rédei type, *J. of Geometry* **60** (1997), 65–73.

[34] A. Gács, On a generalization of Rédei's theorem, *Combinatorica*, submitted.

[35] A. Gács, P. Sziklai and T. Szőnyi, Two remarks on blocking sets and nuclei in planes of prime order, *Designs, Codes, Cryptography* **10** (1997), 29–39.

[36] A. Gács and Zs. Weiner, On $(q+t,t)$-arcs of type $(0,2,t)$, submitted to *Designs, Codes and Cryptography.*

[37] S. W. Graham and C. J. Ringrose, Lower bounds for the least quadratic nonresidues, in: *Analytic number theory*, (Allerton Park, IL, 1989), *Progr. in Math.* **85** Birkhäuser, 1990, 269–309.

[38] É. Hadnagy and T. Szőnyi, On the embedding of large (k,n)-arcs and partial unitals, *Ars Combinatoria*, to appear.

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

[40] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, in: *Finite Geometries* (A. Blokhuis, J.W.P. Hirschfeld, D. Jungnickel, J. A. Thas, eds.) Developments of Mathematics, Kluwer, 2001, 201-246.

[41] J. W. P. Hirschfeld and T. Szőnyi, Constructions of large arcs and blocking sets in finite planes, *European J. Comb.* **12** (1991), 499-511.

[42] T. Illés and D. Pisinger, Upper Bounds on the Covering Number of Galois-Planes with Small Order, *J. of Heuristics* **7** (2000), 59–76.

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

[44] S. Innamorati, The non-existence of certain large minimal blocking sets *Mitt. Math. Sem. Giessen* **235** (1998), 1–23.

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

[46] S. Innamorati and A. Maturo, The spectrum of minimal blocking sets, *Discrete Math.* **208/209** (1999), 339–347.

[47] S. Innamorati and F. Zuanni, Minimal blocking configurations, *J. of Geometry* **55** (1996), 86–98.

[48] C. Kitto, A bound for blocking sets of maximal type in finite projective planes, *Arch. Math.* **52** (1989), 203–208.

[49] G. Korchmáros and F. Mazzocca, Nuclei of point sets of size $q+1$ contained in the union of two lines in $\mathrm{PG}(2,q)$, *Combinatorica* **14** (1994), 63–69.

[50] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Sci. Math. Hungar.* **16** (1981), 449–454.

[51] G. Lunardon, Normal spreads, *Geom. Dedicata* **75** (1999), 245–261.

[52] G. Lunardon and O. Polverino, Blocking sets of size $q^t+q^{t-1}+1$, *J. Comb. Theory Ser. A* **90** (2000), 148–158.

[53] G. Lunardon and O. Polverino, Blocking sets and derivable partial spreads, *J. Algebraic Comb.* **14** (2001), 49–56.

[54] G. Lunardon and O. Polverino, Linear blocking sets: a survey, in: *Finite fields and applications* (ed.: D. Jungnickel), Springer, 2001, 356–362.

[55] F. Pambianco and L. Storme, Minimal blocking sets in $\mathrm{PG}(2,9)$ and maximal partial spreads in $\mathrm{PG}(3,9)$, preprint.

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

[57] J. Pelikán, Properties of incomplete balanced block designs, in: *Combinatorial Theory and its Applications*, (Balatonfüred, Hungary, 1969), *Colloq. Math. Soc. J. Bolyai* **4** North Holland, Amsterdam, 1970, 869–889.

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

[59] P. Polito and O. Polverino, Linear blocking sets in $\mathrm{PG}(2,q^4)$, to appear in *Australasian Journal Combinatorics.*

[60] O. Polverino, Small minimal blocking sets and complete k-arcs in $\mathrm{PG}(2,p^3)$, *Discrete Math.* **208/9** (1999), 469–476.

[61] O. Polverino, Small blocking sets in $\mathrm{PG}(2,p^3)$, *Designs, Codes and Cryptography* **20** (2000), 319–324.

[62] O. Polverino, *Blocking set nei piani proiettivi*, Ph. D. Thesis, Univ. Naples, 1998.

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

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

[65] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Akadémiai Kiadó and Birkhäuser Verlag, Budapest and Basel, 1970.

[66] B. J. Sherman, Minimal blocking sets in finite planes, *J. of Geometry* **43** (1992), 178–187.

[67] P. Scherk, On the intersection number of two plane curves, *J. of Geometry* **10** (1977), 57–68.

[68] K.-O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc. (3)* **52** (1986), 1–19.

[69] P. Sziklai and T. Szőnyi, Blocking sets and algebraic curves, *Rend. Circ. Mat. Palermo* **51** (1998), 71–86.

[70] T. Szőnyi, Combinatorial problems for abelian groups arising from geometry, *Per. Polytechnica* **19** (1991), 91–100.

[71] T. Szőnyi, Blocking sets in finite planes and spaces, *Ratio Math.* **5** (1992), 93–106.

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

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

[74] T. Szőnyi, Some applications of algebraic curves in finite geometry and combinatorics, in: *Surveys in Combinatorics* (R. A. Bailey, ed.), Cambridge Univ. Press, Cambridge, 1997, 198–236.

[75] T. Szőnyi, Around Rédei's theorem, *Discrete Math.* **208/9** (1999), 557–575.

[76] T. Szőnyi and Zs. Weiner, Large minimal blocking sets, manuscript, 2002.

[77] J. A. Thas, Projective geometry over a finite field, Chapter in: *Handbook of Incidence Geometry* (F. Buekenhout, ed.), North-Holland, Amsterdam, 1995.

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

[79] K. Vedder, Affine subplanes of projective planes, in: *Finite Geometries and designs*, (Isle of Thorns, 1980), vol. **49** of *London Math. Soc. Lecture Notes Series*, Cambridge Univ. Press, 1981, 359–364.

[80] Zs. Weiner, *Blocking sets* (in Hungarian), Diploma Thesis, Eötvös University, Budapest, 1998.

Author's addresses:

András Gács, Tamás Szőnyi, Zsuzsa Weiner
Department of Computer Science, Eötvös Loránd University,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY

e-mail: gacs@cs.elte.hu, szonyi@cs.elte.hu, weiner@cs.elte.hu

Tamás Szőnyi,
Alfréd Rényi Mathematical Institute of the Hungarian Academy of Sciences
H-1053 Budapest, Reáltanoda u. 13–15, HUNGARY

e-mail: szonyi@renyi.hu