On multiple blocking sets in Galois planes

A. Blokhuis L. Lovász L. Storme T. Szőnyi

Abstract

This article continues the study of multiple blocking sets in $\mathrm{PG}(2,q)$. In [3], using lacunary polynomials, it was proven that t-fold blocking sets of $\mathrm{PG}(2,q)$, q square, $t < q^{1/4}/2$, of size smaller than $t(q+1)+c_q q^{2/3}$, with $c_q = 2^{-1/3}$ when q is a power of 2 or 3 and $c_q = 1$ otherwise, contain the union of t pairwise disjoint Baer subplanes when $t \geq 2$, or a line or a Baer subplane when $t = 1$. We now combine the method of lacunary polynomials with the use of algebraic curves to improve the known characterization results on multiple blocking sets and to prove a $t \pmod p$ result on small t-fold blocking sets of $\mathrm{PG}(2, q = p^n)$, p prime, $n \geq 1$.

1 Introduction

Throughout this paper, let $q = p^n$ where p is a prime. We use the standard notations $\mathrm{PG}(2,q)$ and $\mathrm{AG}(2,q)$ for the Desarguesian projective and affine plane of order q. A *t-fold blocking set B* in $\mathrm{PG}(2,q)$ is a set of points such that every line of $\mathrm{PG}(2,q)$ intersects B in at least t points.

A 1-fold blocking set is simply called a *blocking set*. A 1-fold blocking set is called *trivial* if it contains a line of $\mathrm{PG}(2,q)$. A t-fold blocking set is called *minimal* (or *irreducible*) when no proper subset of it still is a t-fold blocking set.

Presently, the following bounds on the cardinalities of t-fold blocking sets are known.

Theorem 1.1 *Let B be a t-fold blocking set in* $\mathrm{PG}(2,q)$, *$q = p^n$, p prime, of size $t(q+1)+c$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$.*

(0) (Ball [1]) *When $q = p > 3$ is a prime and $t < p/2$, then $|B| \geq (t+\frac{1}{2})(p+1)$.*

(1) *If n is odd and $t < q/2 - c_p q^{2/3}/2$, then $c \geq c_p q^{2/3}$, unless $t = 1$ in which case B contains a line, if $|B| < q + 1 + c_p q^{2/3}$.*

(2) *If q is a square, $t < q^{1/4}/2$ and $c < c_p q^{2/3}$, then $c \geq t\sqrt{q}$ and B contains the union of t pairwise disjoint Baer subplanes, except for $t = 1$ in which case B contains a line or a Baer subplane.*

(3) *If $q = p^2$, p prime, and $t < q^{1/4}/2$ and $c < p\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}} \rceil$, then $c \geq t\sqrt{q}$ and B contains the union of t pairwise disjoint Baer subplanes, except for $t = 1$ in which case B contains a line or a Baer subplane.*

These results were obtained by using the relation between lacunary polynomials and multiple blocking sets (Section 2).

We use algebraic curves to obtain further information on line intersections of blocking sets (Section 3). An earlier version of this technique was published as a conference abstract, see [6].

We now combine these two techniques to improve on Theorem 1.1. Our main results are Theorem 4.12, the bounds of Section 5 which state that if a t-fold blocking set in $\mathrm{PG}(2,q)$, q square, is not too large, then it consists of the union of a Baer subplane and a $(t-1)$-fold blocking set which are disjoint, and the $t \pmod p$ result of Section 3 (Theorem 3.1).

This latter $t \pmod p$ result was already proven by Szőnyi [13] for minimal 1-fold blocking sets in $\mathrm{PG}(2,q)$, $q = p^n$, p prime, with $|B| < 3(q+1)/2$.

Recently, Sziklai [12] improved this latter $1 \pmod p$ result. Namely, let B be a minimal blocking set in $\mathrm{PG}(2,q)$, $q = p^n$, p prime, with $|B| < 3(q+1)/2$, and let e be the maximal integer e for which a line intersects B in $1 \pmod{p^e}$ points. Then Sziklai [12] proved that e divides n, and proved that the lines intersecting B in exactly $1 + p^e$ points intersect B in a subline $\mathrm{PG}(1,p^e)$.

2 Blocking sets, lacunary polynomials and algebraic curves

We say that a polynomial in $\mathbb{F}_q[X]$ is *fully reducible* if it factors completely in linear factors over $\mathbb{F}_q$. If a large number of consecutive coefficients of a polynomial vanish, this polynomial is called *lacunary* [11].

To each point P of a blocking set, we will associate a fully reducible lacunary polynomial, called the *excess polynomial*, which encodes how the points of the blocking set are distributed over the lines through P. Let B be a t-fold blocking set in $\mathrm{PG}(2,q)$ of size $t(q+1)+c$, with $t+c < q$ and P a point of B. Let the line ℓ be a $(t+c_1)$-secant of B containing P and choose homogeneous coordinates $(X : Y : Z)$ in such a way that $P = (0:1:0) = (\infty)$, ℓ has equation $Z = 0$ and $B \cap \ell = \{(1 : -y_j : 0) || j = 1, \ldots, t+c_1-1\} \cup \{(0:1:0)\}$.

Let $\mathcal{A}$ be the affine plane $\mathrm{PG}(2,q) \setminus \ell$, provided with affine coordinates, such that $(x,y) = (x:y:1)$, and let

$$B \cap \mathcal{A} = \{(a_i, b_i) || i = 1, \ldots, tq + c_2\}$$

where $c_2 = c - c_1$. Let

$$F(U,V) = \prod_{j=1}^{t+c_1-1} (V + y_j) \prod_{i=1}^{tq+c_2} (U + a_i V + b_i),$$

be the *Rédei-polynomial* of the set. Since $F(U,V)$ vanishes at least t times for all $(u,v) \in \mathbb{F}_q^2$, it can be written as

$$F(U,V) = \sum_{i=0}^{t} F_i(U,V)(U^q - U)^{t-i}(V^q - V)^i,$$

where $\deg(F_i) \leq \deg(F) - qt$, see [3, 4]. Considering the homogeneous part of largest degree and substituting $V = 1$, we get

$$f(U) := \prod_{i=1}^{tq+c_2} (U + a_i) = \sum_{i=0}^{t} f_i(U) U^{q(t-i)},$$

where $f_i(U) = F_{i0}(U,1)$, and where F_{i0} is the homogeneous part of $F_i(U,V)$ of highest degree. Since B is a t-fold blocking set, f contains the factor $(U + y)$ at least $t-1$ times, for all $y \in \mathbb{F}_q$. So f is divisible by $(U^q - U)^{t-1}$. Dividing by $(U^q - U)^{t-1}$, we obtain the *excess polynomial*

$$\mathrm{ex}(U) = U^q f_0(U) + f_1(U) + (t-1)U f_0(U)$$

of P. In [3], it was proven that $\deg(f_1(U) + (t-1)U f_0(U)) \leq c$. This polynomial is determined up to projective linear transformations. Its geometric meaning is the following: whenever a line $X = y$ (through P) meets $B \cap \mathcal{A}$ in r points, then $U = -y$ is an $(r - t + 1)$-fold root of the excess polynomial (of P).

Definition 2.1 *Let* $\mathrm{ex}(U)$ *be the excess polynomial of* P. *Let* $q = p^n$, p *prime. Let* $d(U) = \gcd(f_0(U), f_1(U))$. *If* e *is the largest integer for which* $\mathrm{ex}(U)/d(U)$ *is a* p^e*-th power, then* e *is called the* exponent *of the point* P.

In [3], it is shown that the exponent is well defined. We recall the main theorem of [3] on fully reducible lacunary polynomials. The degree of a polynomial f is denoted by f°; following Rédei [11].

Theorem 2.2 *Let $f \in \mathbb{F}_q[X]$, $q = p^n$, p prime, be fully reducible, $f(X) = X^q h(X) + g(X)$, where $\gcd(g, h) = 1$. Let $k = \max(g^\circ, h^\circ) < q$. Let e be maximal such that f is a p^e-th power. Then we have one of the following cases:*

(1) $e = n$ *and* $k = 0$*;*

(2) $e \geq 2n/3$ *and* $k \geq p^e$*;*

(3) $2n/3 > e > n/2$ *and* $k \geq p^{n-e/2} - (3/2)p^{n-e}$*;*

(4) $e = n/2$ *and* $k = p^e$ *and* $f(X) = a\mathbf{T}(bX + c) + d$ *or* $f(X) = a\mathbf{N}(bX + c) + d$ *for suitable constants* a, b, c, d*. Here* $\mathbf{T}$ *and* $\mathbf{N}$ *denote the trace and norm function from* $\mathbb{F}_q$ *to* $\mathbb{F}_{\sqrt{q}}$*, respectively;*

(5) $e = n/2$ *and* $k \geq p^e \left\lceil \frac{1}{4} + \sqrt{(p^e + 1)/2} \right\rceil$*;*

(6) $n/2 > e > n/3$ *and* $k \geq p^{n/2+e/2} - p^{n-e} - p^e/2$*, or if* $3e = n + 1$ *and* $p \leq 3$*, then* $k \geq p^e(p^e + 1)/2$*;*

(7) $n/3 \geq e > 0$ *and* $k \geq p^e \lceil (p^{n-e} + 1)/(p^e + 1) \rceil$*;*

(8) $e = 0$ *and* $k \geq (q + 1)/2$*;*

(9) $e = 0$*,* $k = 1$ *and* $f(X) = a(X^q - X)$*.*

The next two lemmas about lacunary polynomials will be used in our proofs.

Lemma 2.3 *Let B be a minimal t-fold blocking set, $|B| = t(q + 1) + c$ and let P be a point of exponent $e > 0$ in B. Then there are at least $q - c$ lines through P intersecting B in exactly t points.*

Proof: Let P be the point $(0 : 1 : 0)$, choose the line at infinity as a t-secant and consider the excess polynomial $\mathrm{ex}(U) = U^q h(U) + g(U)$ introduced above. For simplicity, we wrote $h(U)$ for $f_0(U)$ and $g(U)$ for $f_1(U) + (t - 1)U f_0(U)$. As mentioned above, $h^\circ, g^\circ \leq c$. Let $d(U) = \gcd(h(U), g(U))$. Then $\mathrm{ex}(U)/d(U) = (U^{q/p^e} h_1(U) + g_1(U))^{p^e}$. The vertical lines that are not t-secants correspond to roots of $\mathrm{ex}(U)$. They are either roots of $d(U)$ or roots of $U^{q/p^e} h_1(U) + g_1(U)$. In the latter case, they are also roots of $U h_1(U)^{p^e} + g_1(U)^{p^e}$. Now $d^\circ + p^e h_1^\circ \leq c$, hence the number of lines that are not t-secants is at most $c + 1$. Therefore, the number of t-secants is at least $q - c$. $\square$

Lemma 2.4 *Let B be a minimal t-fold blocking set of* $\mathrm{PG}(2,q)$ *of size $tq+t+c$. Let P be a point of exponent e. Then*

(1) *P lies on at least $2+(q-c)/p^e$ different lines meeting B in at least p^e+t points;*

(2) *P lies on at least $(q-3c)/p^e+4$ distinct (p^e+t)-secants to B.*

Proof: In this argument, we assume that $d(U)=1$. The excess polynomial of P is a p^e-th power, say $\mathrm{ex}(U)=(e_1(U))^{p^e}$. Let $e_1(U)=U^{q/p^e}h_1(U)+g_1(U)$ with $g_1^\circ, h_1^\circ \le c/p^e$, see Definition 2.1 and the comments preceding it. Then $e_1'(U)$ divides $U^{q/p^e}h_1'(U)+g_1'(U)$, hence $\gcd(e_1(U),e_1'(U))$ divides $g_1(U)h_1'(U)-g_1'(U)h_1(U)$. This contains the contribution of multiple roots of e_1. The degree of $g_1(U)h_1'(U)-g_1'(U)h_1(U)$ is at most $2c/p^e-2$. So, e_1 has at least $(q-c)/p^e+2$ distinct roots. At most $2c/p^e-2$ of them can be multiple roots, hence $e_1(U)$ has at least $(q-3c)/p^e+4$ simple roots.

The assertions of the lemma come from the geometric reformulation of these facts for the excess polynomial. □

3 Multiple blocking sets and algebraic curves

The main result of this section is the following theorem.

Theorem 3.1 *Let B be a minimal t-fold blocking set in $\mathrm{PG}(2,q)$, $q=p^n$, p prime, $n\ge 1$, $|B|=tq+t+c$, $c+t<(q+3)/2$. Then every line intersects B in $t \pmod p$ points.*

In order to prove Theorem 3.1, let B be a t-fold blocking set with $|B|=tq+t+c, c+t<(q+3)/2$. We use the notations of the previous section and consider the Rédei polynomial where we assume that $\ell : Z=0$ is a t-secant to B, so $c_1=0$ and $c_2=c$, and

$$F(U,V) \;=\; \prod_{j=1}^{t-1}(V+y_j)\prod_{i=1}^{tq+c}(U+a_iV+b_i). \tag{1}$$

By the results of the previous section,

$$\begin{aligned} F(U,V) \;=\; & (U^q-U)^tF_0(U,V)+(U^q-U)^{t-1}(V^q-V)F_1(U,V)+\\ & \cdots+(V^q-V)^tF_t(U,V), \end{aligned} \tag{2}$$

where $\deg(F_i)\le c+t-1$.

Select the reference system in such a way that the line $X = 0$ intersects B in t points. If the line $X = 0$ intersects $B \cap \mathcal{A}$ in the points $(0, b_j)$, $j = 1, \ldots, t-1$, then $\prod_{j=1}^{t-1}(U + b_j)$ divides $F_t(U, V)$. Similarly, $\prod_{j=1}^{t-1}(V + y_j)$ divides $F_0(U, V)$. The algebraic curves $F_0(U, V)$ and $F_t(U, V)$ have a direct geometric meaning: the point (b, m), $b \neq -b_j, m \neq -y_j$, $j = 1, \ldots, t-1$, of $F_t(U, V)$ corresponds to a line $Y = -mX - b$ intersecting $B \cap \mathcal{A}$ in more than t points. Similarly, a point (b, m) of $F_0(U, V)$, with $-m \neq y_j$, corresponds to a line $Y = -mX - b$ intersecting $B \cap \mathcal{A}$ in more than t points. If $m = -y_j$ or $b = -b_j$ and the line $Y + mX + b = 0$ intersects $\mathcal{A}$ in more than t points, then $F_0(b, m) = F_t(b, m) = 0$. Because of the above divisibility, $F_0(b, m) = 0$ or $F_t(b, m) = 0$ do not imply that $Y + mX + b = 0$ intersects $\mathcal{A}$ in more than t points.

Therefore, F_0 and F_t have essentially the same set of $\mathbb{F}_q$-rational points. For $0 < j < t$, this is not clear for F_j. Our aim is to prove that, again except for the points on some lines, F_j also has the same set of $\mathbb{F}_q$-rational points. We prove this in a series of lemmas.

Lemma 3.2 *If the line $Y = -mX - b$ intersects $B \cap \mathcal{A}$ in more than t points, then $F_0(b, m) = \ldots = F_t(b, m) = 0$.*

Proof: This is clear for F_0 and F_t from the preceding calculations. Now we verify the assertion for $0 < j < t$.

Let $(U, V) = (U' + \lambda V', V')$ be a change of variables, for some $\lambda \in \mathbb{F}_q$, for which the line $X = -\lambda$ intersects B in t points. Then

$$F(U, V) = F(U' + \lambda V', V') = \prod(V' + y_j) \prod(U' + (a_i + \lambda)V' + b_i) =$$
$$(U'^q - U')^t F_0(U' + \lambda V', V') + \ldots + (V'^q - V')^t (F_t(.) + \ldots + \lambda^t F_0(.)).$$

Here $U^q - U = U'^q - U' + \lambda(V'^q - V')$ was used. Again, if $(X = -\lambda) \cap B = \{(-\lambda, c_j) || j = 1, \ldots, t-1\} \cup \{(\infty)\}$, then

$$\prod(U' + c_j) | (F_t + \ldots + \lambda^t F_0)(U' + \lambda V', V'),$$

and if the line $Y = -mX - b$ intersects $B \cap \mathcal{A}$ in more than t points, then the point $(b - \lambda m, m)$ is a point of $(F_t + \ldots + \lambda^t F_0)(U' + \lambda V', V')$.

If we choose $t + 1$ pairwise different values λ such that the lines $X = -\lambda$ intersect $B \cap \mathcal{A}$ in $t - 1$ points, then we simply get that $F_j(b, m) = 0$ for all j, since we have a homogeneous system of $t + 1$ linear equations, and the determinant is of Vandermonde type; whence the only solution is the trivial one. $\square$

Lemma 3.3 *The algebraic curve F_0 does not have linear components different from $V + y_j$, $j = 1, \ldots, t-1$.*

Proof: To prove this, observe that a linear component of F_0, dependent on U, should have the form $U + aV + b$. Geometrically, this means that through the point $P : (a, b)$, the lines with slope $m \neq -y_j$ intersect $B \cap \mathcal{A}$ in at least $t+1$ points. If $P \notin \mathcal{A}$, then $|B \cap \mathcal{A}| \geq (t+1)(q+1-t) + t^2$, a contradiction.

If $P \in \mathcal{A}$, then at least $q+1-t$ lines through P intersect B in more than t points. Comparing this with Lemma 2.3 gives a contradiction, so P cannot be an essential point. □

Lemma 3.4 *The polynomials $F_0, \ldots, F_t$ cannot have a common divisor, dependent on U.*

Proof: Indeed, such a polynomial would divide $F(U, V)$, hence it would contain a linear component. By the previous lemma, this is impossible. □

Remark 3.5 *Actually, $V + y_j$ cannot be a common divisor of $F_0, \ldots, F_t$ either. This would imply that through the point $(1 : -y_j : 0)$ there passed only one t-secant, namely the line at infinity. This is impossible by Lemma 2.3.*

Proof of Theorem 3.1. Now let $H(U, V)$ be an absolutely irreducible component of $F_0(U, V)/\prod_{j=1}^{t-1}(V + y_j)$, with $\deg(H) = s$. Note that from (1) and (2), $F_0(U, V)/\prod_{j=1}^{t-1}(V + y_j)$ is a polynomial of total degree c and of U-degree c. So all the absolutely irreducible components of this polynomial have terms in U.

There is an i such that H does not divide F_i. If $H'_U \not\equiv 0$, then H has at least

$$(q + 1 - t)s - s(s - 1)$$

$\mathbb{F}_q$-rational points, see [2, p. 145]. In this counting argument, we only considered the points (b, m) for which $m \neq -y_j$; explaining the factor $q+1-t$. This is motivated by the fact that these points all correspond to lines intersecting $\mathcal{A}$ in more than t points. By Lemma 3.2, these points all belong to F_i, and Bézout's theorem gives

$$(q + 1 - t)s - s(s - 1) \leq s(c + t - 1).$$

This gives the inequality

$$c + t + (t + s) \geq q + 3,$$

and as $s \leq c$, we immediately get

$$c + t \geq (q + 3)/2.$$

If $c+t<(q+3)/2$, then $H'_U \equiv 0$ for any component H, so all lines not through (∞) and not passing through one of the points $(1:-y_j:0)$ intersect B in $t \pmod p$ points. By replacing the line at infinity by an other line through (∞), it is possible to prove that all lines not through (∞) intersect B in $t \pmod p$ points. Since (∞) is an arbitrary point of B, all lines meet B in $t \pmod p$ points. This completes the proof of Theorem 3.1. □

Theorem 3.1 already gives the existence of an integer $e \geq 1$ such that all lines meet B in $t \pmod{p^e}$ points. We first wish to relate this e to the components of $F_0(U,V)$. One direction is clear: all the components of F_0 are of the form $H(U,V) = x(U^{p^e}, V)$. If we take the minimum of these values e where P varies over all the points of B, then all lines meet B in $t \pmod{p^e}$ points. The next propositions go in the opposite direction. The following argument is based on an argument from [13] or rather the improvement presented in [14].

Proposition 3.6 *Assume that $c+t<(q+3)/2$ and let $H(U,V)$ be an absolutely irreducible component of F_0, which can be written as $H(U,V) = x(U^{p^e},V)$ with $x'_U \not\equiv 0$. Then*

$$c \geq \frac{q+p^e}{p^e+1} - t + 1.$$

Proof: Let s denote the U-degree of the polynomial x. The total degree of x is at most sp^e. Use Bézout's theorem for the curves H and F_i, where H is not a component of F_i (Lemma 3.4). Since all the points of H on the lines different from $V=-y_j$, $j=1,\ldots,t-1$, are also points of F_i, the number of such points of H is at most $H^\circ F_i^\circ \leq sp^e(c+t-1)$.

Let

$$F(U,y) = \prod_{j=1}^{t-1}(y+y_j)\prod_{i=1}^{tq+c}(U+a_iy+b_i) = (U^q-U)^tF_0(U,y),$$

with $y \neq -y_j$, $j=1,\ldots,t-1$.

Then these $q+1-t$ lines $V=y$ give linear factors over $\mathbb{F}_q$ for $F_0(U,y)$. The factor x of F_0 has U-degree s, so the number of points of x on these lines, counted according to their intersection multiplicity with the vertical lines, is $(q+1-t)s$. We need to subtract the affine intersections of x and x'_U. By the improvement of [13, Lemma 5.1], see [14, pp. 267-268], this is at most $s(s-1)p^e$. So $x(U,V)$ has at least $(q+1-t)s - s(s-1)p^e$ points. This gives

$$(q-t+1)s - s(s-1)p^e \leq sp^e(c+t-1),$$

from which

$$c \geq \frac{q + p^e}{p^e + 1} - t + 1$$

follows using $sp^e \leq c$. $\square$

As in [7], we do the standard counting arguments to find an upper bound on $|B|$. Suppose that there are τ_i lines that intersect B in exactly i points. Then $\tau_i = 0$ for $i \not\equiv 0 \pmod{p^e}$. The equations are, with $E = p^e$,

$$\begin{aligned} \sum_{i \geq 0} \tau_{t+iE} &= q^2 + q + 1, & (3) \\ \sum_{i \geq 0} (t + iE)\tau_{t+iE} &= |B|(q + 1), & (4) \\ \sum_{i \geq 0} (t + iE)(t + iE - 1)\tau_{t+iE} &= |B|(|B| - 1). & (5) \end{aligned}$$

Now

$$\sum_{i \geq 0} iE^2(i - 1)\tau_{t+iE} \geq 0,$$

so

$$|B|^2 - |B|(1 + (q + 1)(2t - 1 + E)) + (q^2 + q + 1)(t^2 + tE) \geq 0,$$

which leads to

$$|B| \leq \frac{1 + (q + 1)(2t - 1 + E) - \sqrt{\Delta}}{2},$$

with $\Delta = (1 + (q + 1)(2t - 1 + E))^2 - 4(q^2 + q + 1)(t^2 + tE)$.

We have the following theorem as final conclusion of this section.

Theorem 3.7 *Associated to a minimal t-fold blocking set B in $\mathrm{PG}(2, q)$, $q = p^n$, p prime, there are $t + 1$ algebraic curves $F_0(U, V), F_1(U, V), \ldots, F_t(U, V)$ having almost the same set of $\mathbb{F}_q$-rational points. More precisely, if $\ell : Z = 0$ is a t-secant and $|B| = t(q + 1) + c$, then $\deg(F_0) = c + t - 1$ and F_0 contains the factor $\prod_{j=1}^{t-1}(V + y_j)$. After factoring out these linear components, an algebraic curve F_0^* of degree c is obtained.*

(1) *If $F_0^*(b, m) = 0$, $m \neq -y_j$, then the line with equation $Y = -mX - b$ intersects B in more than t points.*

(2) *If F_0^* intersects the line $U = b$ at the point (b, m), $m \neq -y_j$, with multiplicity r, then $Y = -mX - b$ intersects B in exactly $r + t$ points.*

(3) *If* $c + t < (q+3)/2$*, then all the components of* F_0^* *are of the form* $x(U^{p^e}, V)$*, for some* $e > 0$*. The same holds for the non-linear components of* F_j*,* $j = 1, \ldots, t$*. If* e_0 *is the minimum of these values* e *taken over all non-linear components of the algebraic curves* F_j*,* $j = 0, \ldots, t$*, then every line intersects* B *in* $t \pmod{p^{e_0}}$ *points.*

   This number e_0 *is called the* exponent *of the minimal* t*-fold blocking set* B*.*

(4) *If* $x(U^{p^e}, V)$ *is an absolutely irreducible component of* $F_0^*(U, V)$*, with* e *the maximal exponent for which this is true, then* $c \geq \frac{q+p^e}{p^e+1} - t + 1$*.*

4 A characterization result on t-fold blocking sets

In this section, we prove a characterization result on t-fold blocking sets which either completely characterizes or partially characterizes a t-fold blocking set. For the sake of simplicity, we only consider planes of order $q = p^{6m}$, but the arguments for other powers of the characteristic p are similar. Let B be a minimal t-fold blocking set of $\mathrm{PG}(2, p^{6m})$ of size $t(q+1) + c$. To simplify the computations, we suppose that $2 \leq t < q^{1/4}/4$, and $c < p^{4m}\sqrt{p}/2$. These restrictions on t and c will be used throughout this section.

To make the article as accessible as possible to the reader, avoiding detailed calculations, we will not discuss during the presentation of the arguments whether inequalities are valid for all characteristics p, or valid only if some lower bound on the characteristic p holds. The calculations have been done in detail to give the reader precise bounds on the cardinalities of t-fold blocking sets. These bounds are presented in Section 5.

Proposition 4.1 *A point of* B *has exponent* $4m$*,* $3m$ *or* $2m$*.*

Moreover, when $e = 3m$*, then this point defines a dual Baer subline of lines all containing at least* $p^{3m} + t$ *points of* B*.*

Proof: We have to check all the possibilities of Theorem 2.2. As an illustration, we show that neither $e > 4m$ nor $4m > e > 3m$ is possible. In the first case, we would have $c \geq p^e \geq p^{4m}p$, contradicting our upper bound on c. In the second case, $c \geq p^{6m-e/2} - \frac{3}{2}p^{6m-e}$ would follow. Here the first term is at least $p^{4m+1/2}$, the second term is much smaller, so we again have a contradiction. □

As indicated in Theorem 3.7 (3), there is another notion of "exponent" introduced in Section 3. From Theorem 3.7 (3), we know that the components of F_0^* are of the form $x(U^{p^e}, V)$, for some $e > 0$.

The importance of this number e is that it improves the result that every line ℓ intersects B in $t \pmod p$ points.

Proposition 4.2 *For any component $x(U^{p^e}, V)$ of $F_0^*(U, V)$, we have $e \geq 2m$. In particular, every line meets B in $t \pmod{p^{2m}}$ points.*

Proof: By Theorem 3.7 (4), we have the lower bound $c \geq \frac{q+p^e}{p^e+1} - t + 1$. If e was smaller than $2m$, then the right hand side would be larger than $p^{4m}\sqrt{p}/2$, a contradiction. The geometric assertion follows immediately from Theorem 3.7 (2). □

Lemma 4.3 *A Baer subplane not contained in B shares at most $M \leq c + t(\sqrt{q} + 1)$ points with B.*

Proof: The argument in [3, Lemma 4.4] can be copied. □

Definition 4.4 *A line containing at least $p^{4m} + t$ points of B will be called* very long*, while a line meeting B in at least $p^{3m} + t$ points will be called* long.

Lemma 4.5 *The dual Baer subline of long lines through a point of exponent $3m$ is unique.*

Proof: Two dual Baer sublines through the same point meet in at most two lines. If there would be two dual Baer sublines of long lines through the same point, then B would have at least $1 + 2\sqrt{q}\sqrt{q} + (t-1)(q+1) \geq (t+1)q$ points, which is a contradiction. □

Proposition 4.6 *If there is a Baer subplane S contained in B, then $B \setminus S$ is a minimal $(t-1)$-fold blocking set.*

Proof: This follows immediately from Proposition 4.2. □

Therefore, from now on, we can suppose that B does not contain a Baer subplane.

Definition 4.7 *If P is a point of the t-fold blocking set B of exponent $3m$ defining a dual Baer subline of long lines, and ℓ is one of the lines of this dual Baer subline, then we call P a* special point *of ℓ.*

Lemma 4.8 *If a line ℓ contains $2t+1$ special points, then there is a Baer subplane contained in B.*

Proof: This proof is essentially the first part of the proof of [3, Proposition 4.5]. Let $P_1, \dots, P_{2t+1} \in \ell$ be special points, and let B_i be the intersection of B and $\cup_{j=1}^{\sqrt{q}} \ell_j^i$, where ℓ_j^i and ℓ are the lines of the (unique) dual Baer subline of long lines through P_i. Then $|B_i| \geq \sqrt{q}(\sqrt{q}+t-1)$, $|B_i \cap B_j| \leq |B \cap S_{ij}|$, where S_{ij} is the affine Baer subplane determined by the dual Baer sublines, different from ℓ, through P_i and P_j. If $S_{ij} \not\subseteq B$, then by Lemma 4.3, $|B \cap S_{ij}| \leq c + t(\sqrt{q}+1)$. By inclusion-exclusion,

$$|B \setminus \ell| \geq (2t+1)\sqrt{q}(\sqrt{q}+t-1) - \binom{2t+1}{2} \max_{i \neq j} |B_i \cap B_j|.$$

Substituting the cardinalities

$$t(q+1) + c - |B \setminus \ell| \geq (2t+1)\sqrt{q}(\sqrt{q}+t-1) - (2t+1)t(c+t+t\sqrt{q})$$

follows. Considering the main terms, one gets $tq + c \geq 2tq - 2t^2c - 2t^3\sqrt{q}$. Using the fact that $2t^3\sqrt{q} \leq tq/8$, we obtain that $2t^2c + c \geq 7qt/8$. Finally, $2t^2c \leq tp^{11m/2}\sqrt{p}/4 \leq tq/4$ which implies that $tq/4 + c \geq 2t^2c + c \geq 7tq/8$ and so $c \geq 5qt/8$, a contradiction. □

Proposition 4.9 *There are at most $2t$ points of exponent $4m$.*

Proof: Suppose that there are at least $2t+1$ points of exponent $4m$. Choose $2t+1$ of them, $P_1, \dots, P_{2t+1}$. By the previous lemma, through a point P_i of exponent $4m$, there are at least $p^{2m} - \sqrt{p}$ and at most $p^{2m} + \sqrt{p}$ very long lines. At most $2t$ of them pass through an other point P_j, $j \neq i$. On the remaining very long lines through P_i, there are at least $p^{4m} + t - 2t(p^{2m} + \sqrt{p})$ points which are not on very long lines passing through P_j, $j \neq i$. Therefore the total number of points of B on very long lines is at least $(2t+1)(p^{2m} - \sqrt{p} - 2t)(p^{4m} + t - 2tp^{2m} - 2t\sqrt{p})$. This number is larger than $tp^{6m} + c + t$, a contradiction. □

Let x denote the number of points of B of exponent $3m$, and let y denote the number of points of exponent $4m$. The previous proposition says that $y \leq 2t$. Now we bound the number of points of exponent $3m$ if B does not contain a Baer subplane.

Lemma 4.10 *The number L of long lines is at most*

$$L \leq (x\sqrt{q} + 2tp^{2m} + |B|\frac{4c}{\sqrt{q} - p^{2m}})/(\sqrt{q}+t).$$

Proof: Count the number of incident (point of B, long line) pairs. Then

$$L(\sqrt{q}+t) \leq x\frac{q+c}{\sqrt{q}} + y(p^{2m}+\frac{c}{\sqrt{q}}) + (|B|-x-y)\frac{4c}{\sqrt{q}-p^{2m}}.$$

Namely, if we subtract $1+(t-1)(q+1)$ from $|B|$, we know the number $q+c$ of points of B lying "extra" on the lines through a point R of B. For a point R of exponent $3m$, every long line passing through this point R still needs $\sqrt{q}$ other points of B, so such a point lies on at most $(q+c)/\sqrt{q}$ long lines. For a point R of exponent $2m$, we know that it lies on at least $(p^{6m}-3c)/p^{2m}+4$ lines with exactly $p^{2m}+t$ points. So at least $p^{6m}-3c+4p^{2m}$ "extra" points of B are on these lines with exactly $p^{2m}+t$ points. Then at most $4c-4p^{2m}$ points of B remain which lie on lines through R with more than $p^{2m}+t$ points. We want to count the number of lines through R with at least $p^{3m}+t$ points of B; so there are at most $(4c-4p^{2m})/(p^{3m}-p^{2m}) < 4c/(\sqrt{q}-p^{2m})$ such lines through R.

If we do the reasoning for a point R of exponent $4m$, we extract the power p^{4m} from the excess polynomial (Section 2) $X^q h(X)+g(X) = X^q f_0(X) + +(f_1(X)+(t-1)Xf_0(X))$ after we have divided by $\gcd(g(X),h(X))$. Suppose that $d=\deg(\gcd(g(X),h(X)))$. Then we see that there are at most $(q+c-d)/p^{4m}$ lines through R which are very long. The linear factors arising from $\gcd(g(X),h(X))$ also can lead to long lines through R, so there are at most $(q+c-d)/p^{4m}+d/p^{3m} \leq p^{2m}+c/p^{3m}$ long lines through R. □

Lemma 4.11 $x \leq c$.

Proof: Count the number of pairs (point of exponent $3m$, line of its dual Baer subline of long lines). Then $x(\sqrt{q}+1) \leq 2tL$, by Lemma 4.8. Substituting the bound obtained in the previous lemma, we obtain that

$$x(\sqrt{q}+1)(\sqrt{q}+t) \leq 2tx\sqrt{q} + 4t^2p^{2m} + (tq+t+c)\frac{8ct}{\sqrt{q}-p^{2m}}.$$

Using that $8t^2 < \sqrt{q}/2$, and the bound $c < p^{4m}\sqrt{p}/2$, we get a contradiction after some computations, if $x > c$ is assumed. □

Theorem 4.12 *A minimal t-fold blocking set B in* $\mathrm{PG}(2,p^{6m})$, $2 \leq t < p^{3m/2}/4$, *with* $|B| < tp^{6m}+p^{4m}\sqrt{p}/2+t$, *not containing a Baer subplane, has size* $|B| \geq tp^{6m}+tp^{4m}-O(p^{2m})$.

Proof: Let $|B| = tq+t+c$. We count the number S of $(p^{2m}+t)$-secants by using the algebraic curve F_0^* associated to B, see Theorem 3.7, and by using Lemma 2.4. There are at least $tq-t$ points of B having exponent

$2m$. Through any such point, there are at least $(p^{6m}-3c)/p^{2m}$ different $(p^{2m}+t)$-secants, hence

$$S \geq \frac{(tq-t)(q-3c)}{p^{2m}(p^{2m}+t)}.$$

Through the t infinite points of B, there are at most $t(q+c)/p^{2m}$ such lines. If such a line does not pass through an infinite point of B, then it corresponds to a point of the algebraic curve F_0^*. In this latter case, a $(p^{2m}+t)$-secant can only correspond to a point on a component of F_0^* with $e=2m$. Let w be such a component. There can be at most $\deg(w)(q+1)/p^{2m}$ distinct points on this component. Summing this over all components w of F_0^*, we find $(q+1)c/p^{2m}$ as upper bound. So

$$(q+1)c/p^{2m}+t(q+c)/p^{2m} \geq S \geq \frac{(tq-t)(q-3c)}{p^{2m}(p^{2m}+t)}.$$

Studying this inequality, the lower bound on c follows. □

5 Detailed bounds

We now present bounds arising from detailed calculations of the preceding arguments. Let p be a prime.

5.1 General bounds

Theorem 5.1 (1) *If B is a minimal t-fold blocking set in* $\mathrm{PG}(2,p^{6m})$, *$m \geq 1$, $2 \leq t < p^{3m/2}/4$, with $|B| < tp^{6m}+p^{4m}\sqrt{p}/2+t$, not containing a Baer subplane, then*

$$|B| \geq tp^{6m}+tp^{4m}-4t^2p^{2m}+t.$$

Such a minimal t-fold blocking set only can have points of exponents $2m$, $3m$ and $4m$.

(2) *If B is a minimal t-fold blocking set in* $\mathrm{PG}(2,p^{6m+1})$, *$m \geq 1$, $2 \leq t < p^{3m/2+1/4}/4$, with $|B| < tp^{6m+1}+p^{4m+1}-2p^{2m+1}+t$, then*

$$|B| \geq tp^{6m+1}+t+\max(tp^{4m}-4t^2p^{2m-1}, p^{4m+1}-p^{4m}-p^{2m+1}/2).$$

Such a minimal t-fold blocking set only can have points of exponent $2m+1$.

(3) *If B is a minimal t-fold blocking set in* $\mathrm{PG}(2, p^{6m+2})$, *$m \geq 1$, $p \geq 5$, with $2 \leq t < p^3/(4(p+1))$ when $m = 1$ and with $2 \leq t < p^{(3m+1)/2}/4$ when $m > 1$, and with $|B| < tp^{6m+2} + p^{4m+2}/2 + t$, not containing a Baer subplane, then*

$$|B| \geq tp^{6m+2} + tp^{4m+1} - 4t^2p^{2m} + t.$$

Such a minimal t-fold blocking set only can have points of exponents $2m+1, 3m+1$ and $4m+1$.

(4) *If B is a minimal t-fold blocking set in* $\mathrm{PG}(2, p^{6m+3})$, *$m \geq 0$, $2 \leq t < p^{(6m+3)/4}/4$, $|B| < tp^{6m+3} + p^{4m+2}\sqrt{p}/2 + t$, where $p \geq 23$ for $m = 0$ and $p \geq 3$ for $m = 1$, then*

$$|B| \geq tp^{6m+3} + tp^{4m+2} - 4t^2p^{2m+1} + t.$$

Such a minimal t-fold blocking set only can have points of exponents $2m+1$ and $4m+2$.

(5) *If B is a minimal t-fold blocking set in* $\mathrm{PG}(2, p^{6m+4})$, *$m \geq 1$, with $2 \leq t < p^{(3m+2)/2}/4$, and with $|B| < tp^{6m+4} + p^{4m+3} - 2p^{2m+2} + t$, not containing a Baer subplane, then*

$$|B| \geq tp^{6m+4} + t + \max(tp^{4m+2} - 4t^2p^{2m}, p^{4m+3} - p^{4m+2} - p^{2m+2}/2).$$

Such a minimal t-fold blocking set only can have points of exponents $2m+2$ and $3m+2$.

(6) *If B is a minimal t-fold blocking set in* $\mathrm{PG}(2, p^{6m+5})$, *$m \geq 0$, $p \geq 5$, with $|B| < tp^{6m+5} + p^{4m+4}/2 + t$, with $2 \leq t < p^{3m/2+5/4}/4$ for $m > 0$ and $2 \leq t \leq (p-3)/4$ for $m = 0$, then*

$$|B| \geq tp^{6m+5} + t + \max(tp^{4m+3} - 4t^2p^{2m+1}, p^{4m+3}\sqrt{p} - p^{4m+3} - p^{2m+2}/2).$$

Such a minimal t-fold blocking set only can have points of exponents $2m+2$ and $4m+3$.

5.2 Complete classifications

We now present for $q = p^{6m}, p^{6m+2}$ and p^{6m+4}, the cases in which a complete description of the t-fold blocking sets is given.

Presently, the following complete characterizations of blocking sets are known.

Theorem 5.2 (Polverino, Polverino and Storme [7, 8, 9]) *The smallest minimal blocking sets in* $\mathrm{PG}(2, p^{3h})$*, p prime, $p \geq 7$, with exponent $e \geq h$, are:*

(1) *a line,*
(2) *a Baer subplane of cardinality $p^{3h} + p^{3h/2} + 1$, when p^h is a square,*
(3) *a set of cardinality $p^{3h} + p^{2h} + 1$, equivalent to*

$$\{(x, T(x), 1) || x \in \mathbb{F}_{p^{3h}}\} \cup \{(x, T(x), 0) || x \in \mathbb{F}_{p^{3h}} \setminus \{0\}\},$$

with T the trace function from $\mathbb{F}_{p^{3h}}$ to $\mathbb{F}_{p^h}$,
(4) *a set of cardinality $p^{3h} + p^{2h} + p^h + 1$, equivalent to*

$$\{(x, x^{p^h}, 1) || x \in \mathbb{F}_{p^{3h}}\} \cup \{(x, x^{p^h}, 0) || x \in \mathbb{F}_{p^{3h}} \setminus \{0\}\}.$$

Theorem 5.3 *Let B be a minimal t-fold blocking set in* $\mathrm{PG}(2, p^{6m})$*, p prime, $m \geq 1$, with $2 \leq t < p^{3m/2}/4$, of size $|B| < tp^{6m} + p^{4m}\sqrt{p}/2 + t$.*

If

$$|B| < tp^{6m} + 2p^{4m} + (t-2)p^{3m} - 16p^{2m} + t,$$

then B is the union of t pairwise disjoint Baer subplanes or the union of $t-1$ Baer subplanes and one minimal blocking set of size $p^{6m} + p^{4m}(+p^{2m}) + 1$, which all are pairwise disjoint.

Proof: We apply inductively the result of Theorem 5.1 (1) to prove that B is the union of $t-2$ Baer subplanes and a 2-fold blocking set of size $|B| < 2p^{6m} + 2p^{4m} - 16p^{2m} + 2$, which all are pairwise disjoint. From Theorem 5.1 (1), this remaining 2-fold blocking set is the union of a Baer subplane and an other blocking set which are pairwise disjoint. This latter blocking set is either a Baer subplane or a minimal blocking set of size $p^{6m} + p^{4m}(+p^{2m}) + 1$ since it has exponent $e \geq 2m$ (Theorem 5.2). $\square$

The question is whether there exist t-fold blocking sets which are the union of $t-1$ Baer subplanes and a minimal blocking set of size $p^{6m} + p^{4m}(+p^{2m}) + 1$ in $\mathrm{PG}(2, p^{6m})$, which are pairwise disjoint.

Polverino and Storme found a particular example of such a 2-fold blocking set.

Theorem 5.4 (Polverino and Storme [10]) *In* $\mathrm{PG}(2, p^{6m})$*, p odd, $m \geq 1$,* $p^m \equiv 5 \pmod 7$*, there exists a minimal 2-fold blocking set which is the union of a Baer subplane and a minimal blocking set of size $p^{6m} + p^{4m} + p^{2m} + 1$, which are pairwise disjoint.*

Similarly, parts (4) and (1) of Theorem 5.1 state lower bounds on the size of minimal t-fold blocking sets in $\mathrm{PG}(2, p^{6m+3})$, and on the size of minimal t-fold blocking sets in $\mathrm{PG}(2, p^{6m})$ not containing a Baer subplane. Also here, the question arises whether an example of a minimal t-fold blocking set exists whose size is of this order. Again, such an example of a 2-fold blocking set was found by Polverino and Storme.

Theorem 5.5 (Polverino and Storme [10]) *In* $\mathrm{PG}(2, p^{3h})$, $p^h \equiv 2 \pmod 7$, *there exists a minimal 2-fold blocking set which is the union of two disjoint minimal blocking sets of size* $p^{3h} + p^{2h} + p^h + 1$.

We end the article with a discussion of t-fold blocking sets in $\mathrm{PG}(2, p^{6m+2})$ and $\mathrm{PG}(2, p^{6m+4})$.

Theorem 5.6 *Let B be a minimal t-fold blocking set in* $\mathrm{PG}(2, p^{6m+2})$, *p prime, $m \geq 1$, with $2 \leq t < p^{3m/2+1/2}/4$, of size $|B| < tp^{6m+2} + p^{4m+2}/2 + t$.*

If

$$|B| < tp^{6m+2} + 2p^{4m+1} + (t-2)p^{3m+1} - 16p^{2m} + t,$$

then B is a union of t pairwise disjoint Baer subplanes.

Proof: Applying Theorem 5.1 (3) inductively, we obtain that B is a union of pairwise disjoint $t-1$ Baer subplanes and one other minimal blocking set of size smaller than $p^{6m+2} + 2p^{4m+1} - p^{3m+1} - 16p^{2m} + 1$.

This latter minimal blocking set must have exponent $e \geq 2m+1$. Moreover, by the recent results of Sziklai [12], this exponent must be a divisor of $6m+2$. Hence, $e \geq 3m+1$, and this implies that this latter blocking set also is a Baer subplane. $\square$

A similar argument gives the following theorem.

Theorem 5.7 *Let B be a minimal t-fold blocking set, $2 \leq t < p^{(3m+2)/2}/4$, in* $\mathrm{PG}(2, p^{6m+4})$, *$m \geq 1$, of size $|B| < tp^{6m+4} + p^{4m+3} - 2p^{2m+2} + t$.*

If

$$|B| < tp^{6m+4} + t + (t-2)p^{3m+2} + \max(2p^{4m+2} - 16p^{2m}, p^{4m+3} - p^{4m+2} - p^{2m+2}/2),$$

then B is the union of t pairwise disjoint Baer subplanes.

References

[1] S. Ball, Multiple blocking sets and arcs in finite planes, *J. London Math. Soc.* **54** (1996), 581–593.

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

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

[4] A.A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A* **24** (1992), 19–33.

[5] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields (Second Edition)*, Oxford: Oxford University Press 1998.

[6] L. Lovász and T. Szőnyi, Multiple blocking sets and algebraic curves. Abstract from *Finite Geometry and Combinatorics* (Third International Conference at Deinze (Belgium), May 18–24, 1997).

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

[8] O. Polverino, Small blocking sets in $PG(2, p^3)$, *Des. Codes Cryptogr.* **20** (2000), 319–324.

[9] O. Polverino and L. Storme, Minimal blocking sets in $PG(2, q^3)$, *Europ. J. Combinatorics* **23** (2002), 83–92.

[10] O. Polverino and L. Storme, Unpublished manuscript 2000.

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

[12] P. Sziklai, On small blocking sets and their linearity. (Preprint)

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

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

A. Blokhuis,
Eindhoven University of Technology,
Department of Mathematics and Computing Science
Den Dolech 2, 5600 MB Eindhoven, The Netherlands
(aartb@win.tue.nl)

L. Lovász,
Microsoft Research
One Microsoft Way, Redmond, WA 98052
(lovasz@microsoft.com) and
Eötvös Loránd University, Dept. of Computer Science,
Pázmány P. sétány 1/c, 1117 Budapest, Hungary
(lovasz@cs.elte.hu)

L. Storme,
Ghent University, Dept. of Pure Maths and Computer Algebra,
Krijgslaan 281 - S22, 9000 Gent, Belgium
(ls@cage.ugent.be, http://cage.ugent.be/∼ls)

T. Szőnyi,
Eötvös Loránd University, Dept. of Computer Science,
Pázmány P. sétány 1/c, 1117 Budapest, Hungary
(szonyi@cs.elte.hu), and
Computer and Automation Institute, Hungarian Academy of Sciences
Lágymányosi u. 11, 1111 Budapest, Hungary