LACUNARY POLYNOMIALS, MULTIPLE BLOCKING SETS AND BAER SUBPLANES

A. BLOKHUIS, L. STORME AND T. SZŐNYI

ABSTRACT

New lower bounds are given for the size of a point set in a Desarguesian projective plane over a finite field that contains at least a prescribed number s of points on every line. These bounds are best possible when q is square and s is small compared with q. In this case the smallest set is shown to be the union of disjoint Baer subplanes. The results are based on new results on the structure of certain lacunary polynomials, which can be regarded as a generalization of Rédei's results in the case when the derivative of the polynomial vanishes.

1. *Introduction*

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 [**14**]. An *s-fold blocking set* B in $\mathrm{PG}(2, q)$ (or $\mathrm{AG}(2, q)$) is a set of points such that every line of $\mathrm{PG}(2, q)$ (or $\mathrm{AG}(2, q)$) intersects B in at least s points.

A 1-fold blocking set is simply called a *blocking set*. We say that a (1-fold) blocking set is *trivial* if it contains a line of $\mathrm{PG}(2, q)$. An s-fold blocking set is called *minimal* or *irreducible* when no proper subset of it is an s-fold blocking set. For $s = 2$ and 3 we also speak of a *double* blocking set and a *triple* blocking set.

A (k, n)-*arc* in a projective plane Π is a set of k points such that at most n of them are collinear (this n is unrelated to the n in $q = p^n$, and the k is independent of any k occurring in the rest of this paper). A k-arc is a $(k, 2)$-arc. Note that (k, n)-arcs and s-fold blocking sets with $n + s = q + 1$ are in fact each other's complement. Throughout this paper s will be small compared with q, so we will not make use of the (k, n)-arc terminology. For old and recent results on (k, n)-arcs the reader is referred to [**2**, **4**, **7**, **13–15**].

While there are many interesting results about blocking sets (that is $s = 1$ (see Blokhuis [**7**] for a survey)), not much is known for larger s, except for the special case of an s-fold blocking set B containing a line ℓ. In this case the set $B \setminus \ell$ is an $(s-1)$-fold blocking set in the affine plane $\mathrm{PG}(2, q) \setminus \ell = \mathrm{AG}(2, q)$. The results of Bruen [**10**, **11**] and Blokhuis [**7**] then give the following.

Let B be an s-fold blocking set in $\mathrm{PG}(2, q)$ that contains a line. If $(s-1, q) = 1$, then $|B| \geqslant q(s+1)$. If $(s-1, q) > 1$ and $s \leqslant (q/2) + 1$, then $|B| \geqslant sq + q - s + 2$, and finally if $(s-1, q) > 1$ and $s \geqslant (q/2) + 1$, then $|B| \geqslant s(q+1)$.

Bruen's result was a generalization of the case $s = 2$ that was known much earlier. This case follows from the results of Jamison [**16**] and Brouwer and Schrijver [**8**] on the blocking number of an affine plane.

In the case of s-fold blocking sets not containing a line much less is known. Using

Received 21 March 1997; revised 28 January 1998.

1991 *Mathematics Subject Classification* 05B25, 51E21.

The second author is a Senior Research Assistant of the National Fund for Scientific Research (Belgium). The third author gratefully acknowledges the financial support of NWO. This author's research was partly supported by OTKA Grants T-014302 and T-014105.

J. London Math. Soc. (2) 60 (1999) 321–332

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

purely combinatorial methods, Ball [**2**] showed that such an s-fold blocking set has at least $sq+\sqrt{sq}+1$ points. Using the technique of lacunary polynomials, Ball and Blokhuis [**3**] proved a much better bound for $s=2$. Let us mention the probably most interesting special case of their result.

If $4<q$ is a square, then $|B|\geqslant 2q+2\sqrt{q}+2$ for a 2-fold blocking set in PG$(2,q)$.

Gács and Szőnyi [**12**] have shown the following.

A 2-fold blocking set of size $2q+2\sqrt{q}+2$ in PG$(2,q)$, *q odd, $q\geqslant 169$, must be the union of two disjoint Baer subplanes.*

The corresponding bound for $s=3$ was proved by Ball [**1**]. For a more detailed account on the lower bounds, we refer to the original papers and also to [**2**]. For $s>3$ only one general result, due to Ball and Blokhuis [**2**], is known.

Let B be an s-fold blocking set in PG$(2,p)$, *$p>3$ prime. If $s<p/2$, then $|B|\geqslant (s+\frac{1}{2})(p+1)$, and if $s>p/2$, then $|B|\geqslant (s+1)p$.*

The important fact about this result is that for $s=1$, $(p-1)/2$, $(p+1)/2$, it is sharp. The examples are due for $s=1$ to Bruen [**9**] and for $s>1$ to Barlotti [**5**]. The aim of this paper is to extend the results of Ball and Blokhuis for $s>3$. We shall be interested in the case when q is not a prime. Our main result not just generalizes Ball and Blokhuis's result, but also the characterization result of Gács and Szőnyi (and more).

THEOREM 1.1. *Let B be an s-fold blocking set in* PG$(2,q)$ *of size $s(q+1)+c$. Let $c_2=c_3=2^{-1/3}$ and $c_p=1$ for $p>3$.*

(1) *If $q=p^{2d+1}$ and $s<q/2-c_p q^{2/3}/2$ then $c\geqslant c_p q^{2/3}$.*

(2) *If $4<q$ is a square, $s<q^{1/4}/2$ and $c<c_p q^{2/3}$, then $c\geqslant s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*

(3) *If $q=p^2$ and $s<q^{1/4}/2$ and $c<p[\frac{1}{4}+\sqrt{(p+1)/2}]$, then $c\geqslant s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*

The main result relies on an improvement of the fundamental lemma for lacunary polynomials, which we discuss in Section 3. The most important special case is the following result. Here, and in the rest of the paper, we use Rédei's notation f° for the degree of f; see [**18**].

Let $f=X^{\sqrt{q}}g+h\in\mathbf{F}_q[X]$, q square, be fully reducible with $(g,h)=1$, $f'\neq 0$ and $t=\max(g^\circ,h^\circ)$. Then either $f(X)=a\,\mathrm{Tr}(bX+c)+d$ or $f(X)=a\,\mathrm{Norm}(bX+c)+d$ for suitable constants a,b,c,d or $t\geqslant\frac{1}{4}+\sqrt{(\sqrt{q}+1)/2}$.

This result can be regarded as a generalization of Rédei's original theorems (or rather Blokhuis' generalization (see [**7**, Theorem 5])) for fully reducible lacunary polynomials of the form $f=X^q g+h$. With the notations and conditions of the above result Blokhuis' theorem says that either $t=1$ and $f(X)=a(X^q-X)$, or $t\geqslant(q+1)/2$.

Example 3.4 shows that our result is essentially sharp, so in the more general case we cannot hope for a lower bound that is linear in $\sqrt{q}$.

2. *Blocking sets and lacunary polynomials*

We say that a polynomial in $\mathbf{F}_q[X]$ is *fully reducible* if it factors completely into linear factors over $\mathbf{F}_q$. If a large number of consecutive coefficients of a polynomial vanish, this polynomial is called *lacunary* [**18**]. The key tools in the analysis are certain fully reducible lacunary polynomials associated with an s-fold blocking set B in PG$(2,q)$.

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

Let B be an s-fold blocking set in PG$(2,q)$ of size $s(q+1)+c$, with $s+c<q$. Let the line l be an $(s+c_1)$-secant of B and choose homogeneous coordinates $(X:Y:Z)$ in such a way that l has equation $Z=0$ and $B\cap l=\{(d_j,1,0)\|j=1,\dots,s+c_1-1\}\cup\{(1,0,0)\}$.

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

$$B\cap\mathscr{A}=\{(x_i,y_i)\|i=1,\dots,sq+c_2\}$$

where $c_2=c-c_1$.

The non-horizontal line $m_{uv}: X+u+vY=0$ contains at least s points of B, except possibly when $(d_j,1,0)\in m$, that is, when $v=-d_j$. In this case m_{uv} still contains at least $s-1$ points of B. Let

$$F(U,V)=\prod_{j=1}^{s+c_1-1}(V+d_j)\prod_{i=1}^{sq+c_2}(U+x_i+y_iV).$$

Then $F(U,V)$ vanishes at least s times for all $(u,v)\in\mathbf{F}_q^2$. By [**11**, Theorem 1.3], $F(U,V)$ belongs to the ideal defined by the polynomials $\Pi_i(U,V)=(U^q-U)^{s-i}(V^q-V)^i$, $i=0,\dots,s$, and so

$$F(U,V)=\sum_{i=0}^{s}F_i(U,V)\,\Pi_i(U,V)$$

for certain polynomials F_i. Also by the proof of [**11**, Theorem 1.3], it is possible to select the polynomials F_i in such a way that $F_i^\circ\leqslant F^\circ-qs$.

Consider in this equation the homogeneous part of total degree $s(q+1)+c-1$:

$$V^{s+c_1-1}\prod_{i=1}^{sq+c_2}(U+y_iV)=\sum_{i=0}^{s}F_{i0}(U,V)U^{(s-i)q}V^{iq},$$

where F_{i0} denotes the homogeneous part of F_i of total degree $c+s-1$. This immediately gives that V^{s+c_1-1} divides F_{00}. With $f_i(U)=F_{i0}(U,1)$, the expression can be simplified to

$$\prod_{i=1}^{sq+c_2}(U+y_i)=\sum_{i=0}^{s}f_i(U)U^{(s-i)q}. \tag{1}$$

Every horizontal line contains at least $s-1$ points (x_i,y_i) of $B\cap\mathscr{A}$, so $(U^q-U)^{s-1}$ divides the left-hand side of (1). If the quotient is denoted by $U^qg(U)+h(U)$, then $g(U)=f_0(U)$, that is, a polynomial of degree c_2, and $h(U)=f_1(U)+(s-1)Uf_0(U)$, so $h^\circ\leqslant c+s-1$.

Comparing the terms of degree less than q in

$$\sum_{i=0}^{s}f_i(U)U^{(s-i)q}=(U^qf_0(U)+f_1(U)+(s-1)Uf_0(U))(U^q-U)^{s-1},$$

we get

$$f_s(U)=U^{s-1}(f_1(U)+(s-1)Uf_0(U))(-1)^{s-1},$$

so

$$(f_1(U)+(s-1)Uf_0(U))^\circ\leqslant c.$$

Thus with the s-fold blocking set B there corresponds a lacunary polynomial $U^qg(U)+h(U)$.

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

REMARK 2.1. This polynomial is called the *excess polynomial* of B with respect to the point $(1,0,0)$ (and also with respect to the special choice of the line at infinity). This polynomial is determined up to projective linear transformations, but the lacunarity type is always at most c.

EXAMPLES 2.2. (1) Let

$$B = \{(1:-u^2:0) \| u \in \mathbf{F}_q\} \cup \{(0:1:-u^2) \| u \in \mathbf{F}_q\} \cup \{(-u^2:0:1) \| u \in \mathbf{F}_q\}$$

be the standard blocking set of size $3(q+1)/2$ in PG$(2,q)$, q odd.

With $l: Z = 0$ the line at infinity, and with $(x_i, y_i) = (0, -1/u^2)$, $u \neq 0$, and $(x_i, y_i) = (-u^2, 0)$, $u \in \mathbf{F}_q$, the affine points of B, if $I = \{1/u^2 \| u \in \mathbf{F}_q^*\}$, then

$$\prod (U + y_i) = U^{(q+1)/2} \prod_{w \in I} (U - w) = U^{(q+1)/2}(U^{(q-1)/2} - 1) = U^q - U^{(q+1)/2}.$$

Hence $g(U) = 1$ and $h(U) = -U^{(q+1)/2}$.

(2) Let $B = \{(x:y:z) \| (x,y,z) \in \mathbf{F}_{\sqrt{q}}^3 \setminus \{(0,0,0)\}\}$ be the standard Baer subplane in PG$(2,q)$, q square.

Let $l: Z = 0$ be the line at infinity; then the affine points of B are (x,y), $x, y, \in \mathbf{F}_{\sqrt{q}}$. Hence, the lacunary polynomial is

$$\prod_{y \in \mathbf{F}_{\sqrt{q}}} (U + y)^{\sqrt{q}} = (U^{\sqrt{q}} - U)^{\sqrt{q}} = U^q - U^{\sqrt{q}},$$

and so $g(U) = 1$ and $h(U) = -U^{\sqrt{q}}$.

(3) Let $q = q_1^e$, $e > 1$, and let f be the trace function of $\mathbf{F}_q$ to the subfield $\mathbf{F}_{q_1}$. Then the points $(x, f(x))$ constitute the affine points of a blocking set of Rédei type.

For this blocking set, the lacunary polynomial is

$$\prod_{x \in \mathbf{F}_q} (U + f(x)) = \prod_{y \in \mathbf{F}_{q_1}} (U + y)^{q/q_1} = (U^{q_1} - U)^{q/q_1} = U^q - U^{q/q_1}.$$

Hence $g(U) = 1$ and $h(U) = -U^{q/q_1}$.

(4) Let $B = \{(1:0:0), (0:1:0), (0:0:1), (1:1:1), (1:4:2), (1:2:4), (2:1:1), (1:2:1), (1:1:2), (4:1:1), (1:4:1), (1:1:4)\}$, the sporadic blocking set in PG$(2,7)$ [**17**].

With $l: Z = 0$, $\mathscr{A} \cap B = \{(0,0), (1,1), (4,2), (2,4), (2,1), (1,2), (4,4), (4,1), (1,4), (2,2)\}$. Hence

$$\prod (U + y_i) = U(U+1)^3(U+2)^3(U+4)^3 = U^7(U^3+3) + 3U^4 + U,$$

which shows that for the lacunary polynomial $U^7 g(U) + h(U)$ corresponding with this blocking set, $g(U) = U^3 + 3$ and $h(U) = 3U^4 + U$.

(5) As a last example we compute the lacunary polynomial corresponding with the 2-fold blocking set B in PG$(2,4)$ which is the complement of a unital $\mathscr{H}$. Let $l: Z = 0$ and let $\mathscr{H}: X_0^3 + X_1^3 + X_2^3 = 0$.

Then $B = \{(0:0:1), (0:1:0), (1:0:0), (1:1:1), (\omega:1:1), (\omega^2:1:1), (1:\omega:1), (\omega:\omega:1), (\omega^2:\omega:1), (1:\omega^2:1), (\omega:\omega^2:1), (\omega^2:\omega^2:1)\}$ and $\mathscr{A} \cap B = \{(0,0), (1,1), (\omega,1), (\omega^2,1), (1,\omega), (\omega,\omega), (\omega^2,\omega), (1,\omega^2), (\omega,\omega^2), (\omega^2,\omega^2)\}$. Thus

$$\prod (U + y_i) = U^{10} + U^7 + U^4 + U = (U^4 + U)(U^6 + 1).$$

Hence the lacunary polynomial is $U^4 g(U) + h(U)$ with $g(U) = U^2$ and $h(U) = 1$.

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

3. *An improved lemma on lacunary polynomials*

We recall from [**3**] the fundamental lemma on fully reducible lacunary polynomials.

LEMMA 3.1. *Let $f \in \mathbf{F}_q[X]$, $q = p^n$, p prime, be fully reducible, $f(X) = X^q g(X) + h(X)$, where g and h have no common factor. Let $k < q$ be the maximum of the degrees of g and h. Let e be maximal such that f (and hence g and h) is a p^eth power. Then we have one of the following:*

(1) *$e = n$ and $k = 0$;*
(2) *$n > e \geqslant n/2$ and $k \geqslant p^e$;*
(3) *$n/2 > e > 0$ and $k \geqslant p^e[(p^{n-e}+1)/(p^e+1)]$;*
(4) *$e = 0$ and $k \geqslant (q+1)/2$;*
(5) *$e = 0, k = 1$ and $f(X) = a(X^q - X)$.*

The aim of this section is to investigate the case $n/3 < e < 2n/3$. As a result we shall obtain the following improvement.

THEOREM 3.2. *Let $f \in \mathbf{F}_q[X]$, $q = p^n$, p prime, be fully reducible, $f(X) = X^q g(X) + h(X)$, where $(g, h) = 1$. Let $k = \max(g^\circ, h^\circ) < q$. Let e be maximal such that f is a p^eth power. Then we have one of the following:*

(1) *$e = n$ and $k = 0$;*
(2) *$e \geqslant 2n/3$ and $k \geqslant p^e$;*
(3) *$2n/3 > e > n/2$ and $k \geqslant p^{n-e/2} - \frac{3}{2}p^{n-e}$;*
(4) *$e = n/2$ and $k = p^e$ and $f(X) = a\mathrm{Tr}(bX+c)+d$ or $f(X) = a\mathrm{Norm}(bX+c)+d$ for suitable constants a, b, c, d. Here* Tr *and* Norm *respectively denote the trace and norm function from $\mathbf{F}_q$ to $\mathbf{F}_{\sqrt{q}}$;*
(5) *$e = n/2$ and $k \geqslant p^e[\frac{1}{4} + \sqrt{(p^e+1)/2}]$;*
(6) *$n/2 > e > n/3$ and $k \geqslant p^{(n+e)/2} - p^{n-e} - p^e/2$, or if $3e = n+1$ and $p \leqslant 3$, then $k \geqslant p^e(p^e+1)/2$;*
(7) *$n/3 \geqslant e > 0$ and $k \geqslant p^e[(p^{n-e}+1)/(p^e+1)]$;*
(8) *$e = 0$ and $k \geqslant (q+1)/2$;*
(9) *$e = 0$, $k = 1$ and $f(X) = a(X^q - X)$.*

Proof. Let $q = p^{e+d}$, where p is prime, $e + d = n$. For $e \notin (n/3, 2n/3)$ we get cases 1, 2, 7, 8 and 9 as a consequence of Lemma 3.1.

Let $n/3 < e$, $d < 2n/3$, $E = p^e$, and $D = p^d$, so that $ED = q$. Let $\mathscr{F}_t \subset \mathbf{F}_q[X]$ be the set of fully reducible polynomials f of the form

$$f(X) = X^D g(X) + h(X),$$

where $(g, h) = 1$, $f \notin \mathbf{F}_q[X^p]$, and $t = \max(g^\circ, h^\circ)$. Hence $f^E = X^q g^E + h^E$ will be of the form discussed in the theorem, with $k = Et$. We are interested in small values of t for which $\mathscr{F}_t$ is possibly non-empty. To avoid unnecessary complications we will assume that

$$t \leqslant \min(E, D/2).$$

For $a, b, c, d \in \mathbf{F}_q$, with $ad - bc \neq 0$, the polynomial

$$\tilde{f}(x) = (cX+d)^{D+t} f\left(\frac{aX+b}{cX+d}\right)$$

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

is in $\mathscr{F}_t$ if (and only if) f is. Indeed, with $g = \Sigma g_i x^i$ and $h = \Sigma h_i x^i$, the coefficient of x^{D+t} in $\tilde{f}$ becomes

$$a^D \sum g_i c^i a^{t-i} + c^D \sum h_i c^i a^{t-i}.$$

For the coefficient of x^t we get

$$b^D \sum g_i c^i a^{t-i} + d^D \sum h_i c^i a^{t-i}.$$

If both of these expressions vanish, then $a \neq 0$, since at least one of g_t and h_t is non-zero, and we get $g(c/a) = h(c/a) = 0$, contradicting the assumption that $(g, h) = 1$.

Being associated defines an equivalence relation on $\mathscr{F}_t$.

Let $f \in \mathscr{F}_t$. We may assume that $g^\circ < h^\circ = t$ by considering an associate polynomial if necessary (this amounts to moving one of the zeros of f to infinity).

The characterization of the case $t = 1$ turns out to be rather easy; in fact it can already explicitly be found in [**3**]. We include the proof here for completeness. In this case $f(x) = x^D + h_1 x + h_0$, and $f' = h_1 \neq 0$. In particular f has no multiple zeros, so $f \mid f^E - (x^q - x) = h_1^E x^E + x + h_0^E$. This already implies that $D \leqslant E$. Also $f \mid h_1^E f^{E/D} = h_1^E x^E + h_1^{E+E/D} X^{E/D} + h_1^E h_0^{E/D}$. Since $E/D < D$ the difference $x + h_0^E - h_1^{E+E/D} X^{E/D} - h_1^E h_0^{E/D}$ is identically zero. It follows that $D = E$, $h_1^{E+1} = 1$ and $f(x) = a^E \mathrm{Tr}(x/a + b)$ where a is any solution of $a^{E-1} = h_1$ and $\mathrm{Tr}(b) = 1$.

In the rest of the proof we will assume that $t > 1$. Let s be the polynomial with the same zeros as f, but all with multiplicity 1. Then we have $f = s \cdot r$, and $r \mid (f, f')$, so $r \mid (gh' - hg')$, and consequently $r^\circ < 2t - 1$. In fact, if $r^\circ > 0$, then f has a multiple zero, and moving this zero to infinity we may (and will) assume that $g^\circ \leqslant t - 2$, and therefore $r^\circ \leqslant h^\circ + g^\circ - 1 \leqslant 2t - 3$.

From $f \mid f^E = x^q g^E + h^E$ and $f \mid (x^q - x) r$ we get $f \mid r(xg^E + h^E)$.

Let $u := r(xg^E + h^E)/f$; also let $G = rg(x^q - x)/f$. Denote the rational function h/g by j. Then

$$G = r(x^{q-D} - x^{q-2D} j + x^{q-3D} j^2 - \ldots + j^{E-1}) - \frac{u}{g^{E-1}}.$$

Multiplying both sides of the equation $uf = r(xg^E + h^E)$ by G/r gives

$$gu(x^q - x) = (xg^E + h^E)\left(-\frac{u}{g^{E-1}} + r \sum_{n=1}^{E} x^{q-nD} (-j)^{n-1} \right).$$

Let

$$m := |\tilde{m}|, \quad \text{where } \tilde{m} = \frac{Et - t + r^\circ - g^\circ}{D - t}.$$

Note that $m \geqslant 1$, since $u^\circ \geqslant 0$.

Let $C = \min(D, E)$. We shall prove the following two inequalities.

(I) If $r^\circ > 0$ or ($E \neq D$ and $m > 1$), then $r^\circ + mt + 1 \geqslant C$.

(II) If $r^\circ = 0$ and ($E = D$ or $m = 1$), then $(2m - 1)(t - 1) + t = 2mt - 2m + 1 \geqslant C$.

To obtain these inequalities, consider the polynomial

$$g^m u x^q - (xg^E + h^E) r \sum_{n=1}^{m} x^{q-nD} g^{m-n} (-h)^{n-1}. \tag{2}$$

Its most important property is that it has degree less than q, since it is equal to

$$g^m u x + (xg^E + h^E)\left(-\frac{u}{g^{E-m}} + r \sum_{n=m+1}^{E} x^{q-nD} \frac{(-h)^{n-1}}{g^{n-m}} \right).$$

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

Indeed, the degree of $(xg^E+h^E)rx^{q-nD}(-h)^{n-1}/g^{n-m}$ is at most $Et+r^\circ+q-(m+1)D+tm-g^\circ < q$ (m was chosen in such a way that this would be satisfied), and the degree of h^Eu/g^{E-m} is at most $Et+r^\circ+Et-D-t<(2E+1)t-D<q$, since $t\leqslant D/2$.

Define the (C-)height $\mathrm{ht}(P)$ of a polynomial P to be the largest value mod C of the exponents occurring in P. Note that if P_1 and P_2 satisfy $\mathrm{ht}(P_1)+\mathrm{ht}(P_2)<C$ then $\mathrm{ht}(P_1P_2)=\mathrm{ht}(P_1)+\mathrm{ht}(P_2)$.

Consider $\mathrm{ht}(g^mu)$. This is of course the same as $\mathrm{ht}(g^mux^q)$. Since all terms in g^mux^q have degree $\geqslant q$, they must be cancelled in (2), by an expression from the second term. The height can therefore be obtained by considering the part in the second term of degree at least q.

Note that the height of the entire second term is $1+r^\circ+(m-1)t$, and this height only occurs in the part coming from $xg^Erx^{q-mD}(-h)^{m-1}$ and its degree

$$1+Eg^\circ+r^\circ+q-mD+(m-1)t$$

is smaller than q when $E>D$, so

$$\mathrm{ht}(g^mu)\leqslant 1+r^\circ+(m-1)t$$

and the inequality is strict when $E>D$.

Case 1: $r^\circ>0$ or ($E\neq D$ and $m>1$).

We show that in this case $\mathrm{ht}(g^mu)\geqslant r^\circ+(m-1)t$.

If $\mathrm{ht}(g^mux^q)\neq 1+r^\circ+(m-1)t$ then it is determined by the part of the second term coming from $h^Erx^{q-mD}(-h)^{m-1}$ with height $r^\circ+(m-1)t$. Indeed, the only way that the term of this height might vanish is that it is cancelled by something coming from $xq^Erx^{q-(m-1)D}g(-h)^{m-2}$.

If $r^\circ>0$ then we may take $g^\circ\leqslant t-2$ and it does not have the required height.

If $r^\circ=0$ (and hence $g^\circ=t-1$), then we compare the maximal degrees realizing the heights: for $h^Erx^{q-mD}(-h)^{m-1}$ we get degree

$$Et+r^\circ+q-mD+(m-1)t,$$

and for $xg^Erx^{q-(m-1)D}g(-h)^{m-2}$ we obtain

$$1+E(t-1)+r^\circ+q-(m-1)D+(t-1)+(m-2)t,$$

and these expressions are equal only if $E=D$.

Comparing the height of both sides of the equation

$$g^mu(x^Dg+h)=g^mr(xg^E+h^E),$$

we find, assuming that $r^\circ+mt+1<C$, that $(1+)r^\circ+(m-1)t+t=mg^\circ+r^\circ+1$, which implies that $(1+)mt=mg^\circ+1$, a contradiction, since $m>1$.

Thus the conclusion in this case is $r^\circ+mt+1\geqslant C$, and this implies that

$$t^2(E-2)+t(2D+C+1)-(C+2)D\geqslant 0.$$

Case 2: $r^\circ=0$ and ($E=D$ or $m=1$).

We shall prove that in this case $(2m-1)(t-1)+t\geqslant C$.

Assume that $(2m-1)(t-1)+t<C$. The main idea is to bound $\mathrm{ht}(u)$. We start by proving, using induction on i, that the height of the polynomial $g^{m-i}h^iu$ equals $(m-1)(t-1)+i$ ($0\leqslant i\leqslant m$) by considering the equation

$$g^{m-i-1}h^iu(x^Dg+h)=g^{m-i-1}h^ir(xg^E+h^E). \tag{3}$$

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

Indeed, for $i=0$, we get this from the estimate $\mathrm{ht}(g^m u) \leqslant 1+(m-1)t$ and equating the heights of both sides of the equation

$$g^m u(x^D g+h) = g^m r(xg^E+h^E).$$

The height of the left-hand side is $\mathrm{ht}(g^m u)+t$, and that of the right-hand side is $mg^\circ+1 = m(t-1)+1$. This gives $\mathrm{ht}(g^m u) = (m-1)(t-1)$, since $mt < C$.

The rest follows by induction in the following way. Consider (3) and rewrite it as

$$g^{m-i}h^i u x^D + g^{m-i-1}h^{i+1}u = g^{m-i-1}h^i r(xg^E+h^E).$$

The height of the right-hand side is exactly $1+(m-i-1)(t-1)+ti = (m-1)(t-1)+i+1$. This immediately gives $\mathrm{ht}(g^{m-i-1}h^{i+1}u) = (m-1)(t-1)+i+1$, since the height of the first term on the left-hand side is smaller.

We assumed that $(g,h)=1$; therefore there exist polynomials a and b, of degree at most $t-1$ and $t-2$ respectively, with $ag+bh=1$. Since $u = u(ag+bh)^m$, and all terms in the expansion of the right-hand side are of the form $ua^{m-i}b^i g^{m-i}h^i$, it follows that the height of u is at most $(2m-1)(t-1)$, with m as before, namely

$$m = \left\lfloor \frac{(E-2)t+1}{D-t} \right\rfloor.$$

If now $(2m-1)(t-1)+t < C$, then looking at the height on both sides of the identity

$$u(x^D g+h) = r(xg^E+h^E),$$

we get that the height of the left-hand side is at least $t = h^\circ$ and at most $\mathrm{ht}(u)+h^\circ \leqslant (2m-1)(t-1)+t < C$, and that of the right-hand side is 1 since r is a constant r_0; thus $t=1$, a contradiction.

We conclude that

$$(2m-1)(t-1)+t \geqslant C.$$

In fact we now see that the case $r^\circ = 0$ and $m=1$ does not occur for $p \geqslant 5$, for on the one hand we have $2t-1 \geqslant C$, but if $m=1$ then $(E-2)t+1 < 2(D-t)$ which implies that $(2D-1)/E > t \geqslant (C+1)/2$. As $C=E$ and $D < E^2$, this can only happen if $E^2 = Dp$ and $p \leqslant 3$.

Putting in the value $((E-2)t+1)/(D-t) \geqslant m$, with $E = D = \sqrt{q} = w$, this gives the inequality

$$t^2(2w-4)+t(5-w)-2+w-q \geqslant 0.$$

Now we can put together the bounds obtained in cases 1 and 2:

$$\begin{cases} D < E (< D^2) & t^2(E-2)+t(3D+1)-D^2-2D \geqslant 0; \\ E < D (< E^2) \text{ and if } E^2 = Dp, \text{ then } p \geqslant 5 & t^2(E-2)+t(2D+E+1)-q-2D \geqslant 0; \\ E^2 = Dp,\ p \leqslant 3 & t \geqslant (E+1)/2; \\ D = E = w & t^2(2w-4)+t(5-w)-(q-w+2) \geqslant 0; \\ D = E = w & t = 1. \end{cases}$$

If $D=E=w$ and $t>1$, the resulting bound is $t \geqslant \frac{1}{4}+\sqrt{(w+1)/2}$. For $D<E$, the bound is $t \geqslant (D-1/2)/\sqrt{2E-4}$, and for $E<D$, it is $t \geqslant \sqrt{D/2}$. This proves the theorem. □

COROLLARY 3.3. *If $n/3 < e$, $d < 2n/3$ with $t>1$ if $e=d$, then $k = Et \geqslant c_p q^{2/3}$. For $p>3$ we may take $c_p = 1$; for $p=2$ and 3 we may take $c_p = 2^{-1/3}$.*

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

EXAMPLE 3.4. The following example shows that the bound in the case $D = E = \sqrt{q}$ is sharp up to a constant factor. If $\sqrt{q}$ is a prime power of the form k^2+k-1 then the polynomial $X^{\sqrt{q}}-X^k$ is fully reducible (in $\mathbf{F}_q[X]$). It is generally believed (but not known unfortunately) that there are infinitely many such prime powers. Note also that $r^\circ > 0$ in the example, so we are in the first case of the proof, and thus the example also shows that the first part of the proof is essentially correct in the case $E = D = w$.

4. *Application to multiple blocking sets*

In this section the improved fundamental lemma on lacunary polynomials will be used to show that for planes of square order an s-fold blocking set (s is small with respect to q) has at least $sq+s\sqrt{q}+s$ points, and in the case of equality it is the union of s disjoint Baer subplanes. Actually, we prove slightly more (cf. Theorem 1.1): if the size of the s-fold blocking set is only slightly bigger than $sq+s\sqrt{q}+s$, then it contains the union of s disjoint Baer subplanes.

Some properties of Baer subplanes and sublines will be essential in the proof, so we try to collect these properties here. The field $\mathbf{F}_q \cup \{\infty\}$ can be identified with the projective line $\mathrm{PG}(1,q)$. It contains the Baer subline $\mathbf{F}_{\sqrt{q}} \cup \{\infty\}$. The other Baer sublines are images of this subline under the group $\mathrm{PGL}(2,q)$. The collection of all Baer sublines forms a 3-$(q+1, \sqrt{q}+1, 1)$ design (also known as a Möbius plane, or an inversive plane). Baer sublines not through the point ∞ are related to the norm function $N(x) = x^{\sqrt{q}+1}$ from $\mathbf{F}_q$ to $\mathbf{F}_{\sqrt{q}}$. With every such Baer subline correspond $b \in \mathbf{F}_q$ and $a \in \mathbf{F}^*_{\sqrt{q}}$, such that

$$l = \{x \in \mathbf{F}_q \| \mathrm{Norm}(x+b) = a\}.$$

The Baer sublines containing ∞ correspond with the trace function $\mathrm{Tr}(x) = x + x^{\sqrt{q}}$ in a similar way. (This can all be checked by direct calculations.)

The following properties of Baer sublines will also be used.

(1) Two Baer sublines intersect in at most two points.

(2) If one has two points and two dual Baer sublines through these points so that the line joining the two points belongs to both dual Baer sublines, then the intersection of the lines of these dual Baer sublines contains a Baer subplane.

Proof of Theorem 1.1. By the results of Blokhuis and Bruen mentioned in the introduction we can suppose that B does not contain a line. We will also assume that B is minimal.

Let $B \subset \mathrm{PG}(2,q)$ be a minimal s-fold blocking set of size $s(q+1)+c$, $c < (q+1)/2$. The excess polynomial of B (see Section 2), with respect to a point P of B and with respect to a line l intersecting B in exactly s points, will be a fully reducible polynomial of type $X^q g(X) + h(X)$ with $g^\circ, h^\circ \leqslant c$.

Now apply the improved fundamental lemma (see Theorem 3.2) for lacunary polynomials: case 1 cannot occur, since this means that $c = 0$; hence $|B| = s(q+1)$ and this would imply that $K = \mathrm{PG}(2,q) \setminus B$ is a maximal $((r-1)q+r,\ r = q+1-n)$-arc. Since $r > q/2$, $r \nmid q$ and so this is impossible [**14**]. Case 8 would imply that $c \geqslant (q+1)/2$; hence it is also impossible. Case 9 is never possible for excess polynomials, since $g^\circ = c \geqslant h^\circ$. In case 2 we immediately get $c \geqslant p^{\lceil 2n/3 \rceil}$. As we have remarked in Corollary 3.3, the improved bounds always give $c \geqslant c_p q^{2/3}$, so this excludes cases 3, 5 and 6. In case 7 the old bound gives $k \geqslant q^{2/3} - q^{1/3} + 1$. In the particular case $q = p^2$, which is case 3 in Theorem 1.1, we can only have case 5 or 4

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

in Theorem 3.2 and that implies the bounds in Theorem 1.1. Thus, in all these cases the improved fundamental lemma immediately implies the bound stated in Theorem 1.1.

In the rest of this section we therefore assume that for each point of B the excess polynomial has a divisor associated with the trace (or equivalently the norm) function (case 4 in Theorem 3.2). A line ℓ will be called *long* if it intersects B in at least $\sqrt{q}+s$ points. Geometrically, the above property of the excess polynomials means that *through each point of B there is a dual Baer subline consisting of long lines* (*).

Note that condition (*) was also a key element in the proof of the results of Ball and Blokhuis [**3**] and Ball [**1**] for $s = 2, 3$.

LEMMA 4.1. *The dual Baer subline of long lines through a point is unique.*

Proof. Two dual Baer sublines meet in at most two lines. Hence if there were two dual Baer sublines of long lines through P, then we would have at lest $2\sqrt{q}$ long lines through P. Thus $|B|$ would be at least

$$1+2\sqrt{q}(\sqrt{q}+s-1)+(q+1-2\sqrt{q})(s-1) = (q+1)(s-1)+2q+1 > (q+1)s+c. \quad \square$$

LEMMA 4.2. *The total number of long lines is at most*

$$\frac{(s(q+1)+c)(q+c)}{\sqrt{q}(\sqrt{q}+s)}.$$

Proof. Count the number of incident (point, long line) pairs. On the one hand, it is at least $(\#\text{long lines})(\sqrt{q}+s)$. On the other hand, through a point of B there are at most $(|B|-(q+1)(s-1)-1)/\sqrt{q}$ long lines, which immediately gives the assertion. $\square$

If P is a point of B and ℓ is a long line through P belonging to the dual Baer subline of long lines, then the point P will be called a *special point* of ℓ.

LEMMA 4.3. *If $s \leqslant (\sqrt{q}+1)/2$, then there is a long line with more than $2s$ special points on it.*

Proof. Suppose to the contrary that all long lines have at most $2s$ special points. Counting the (long line, special point of it) pairs gives

$$|B|(\sqrt{q}+1) \leqslant (\#\text{long lines})2s \leqslant \frac{|B|(q+c)2s}{\sqrt{q}(\sqrt{q}+s)},$$

by Lemma 4.2. Hence $(q+\sqrt{q})(\sqrt{q}+s) \leqslant (q+c)2s$, and this is a contradiction if $s \leqslant (\sqrt{q}+1)/2$ and $c < (q+1)/2$. $\square$

LEMMA 4.4. *Let S be a Baer subplane not contained in B and suppose that $|B \cap S| = M (< q+\sqrt{q}+1)$. Then $M \leqslant c+s(\sqrt{q}+1)$.*

Proof. Take a point $P \in S \backslash B$. The lines of S intersect B in at least M points in total. Each of the $q-\sqrt{q}$ tangent lines of S through P intersect B in at least s points. Hence $|B| = (q+1)s+c \geqslant (q-\sqrt{q})s+M$, from which the assertion immediately follows. $\square$

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

PROPOSITION 4.5. *If $c < q/(2s) - s\sqrt{q}$ and B satisfies condition (*), then there is a Baer subplane entirely contained in B.*

Proof. Let ℓ be a long line with at least $2s+1$ special points on it. List $2s+1$ of these special points: $P_1, \ldots, P_{2s+1}$. Denote by B_i the union of points (not on ℓ) on the lines of the dual Baer subline of long lines through P_i ($i = 1, \ldots, 2s+1$). Hence $B_i \subset B\backslash\ell$ and $|B_i| \geqslant \sqrt{q}(\sqrt{q}+s-1)$.

Since $\bigcup_{i=1}^{2s+1} B_i \subseteq B\backslash\ell$, it follows by inclusion/exclusion that

$$|B\backslash\ell| \geqslant (2s+1)\sqrt{q}(\sqrt{q}+s-1) - \binom{2s+1}{2} \max_{1\leqslant i<j\leqslant 2s+1} |B_i \cap B_j|.$$

Now the set $B_i \cap B_j$ is contained in a Baer subplane S_{ij} by property (2) of Baer sublines listed at the beginning of this section. We wish to prove that S_{ij} is contained in B. If not then $|B_i \cap B_j| \leqslant |B \cap S_{ij}| - 2 \leqslant c + s(\sqrt{q}+1) - 2$, by Lemma 4.4. The -2 term comes from the points P_i, P_j. Substituting this upper bound for the maximum in the previous displayed equation one gets

$$s(q+1) + c - \sqrt{q} - s \geqslant (2s+1)(\sqrt{q}(\sqrt{q}+s-1) - s(c + s(\sqrt{q}+1) - 2)).$$

If $1 \leqslant s \leqslant \sqrt{q}$, then $s\sqrt{q} - \sqrt{q} - s^2 + 2s > 0$, so these terms (and also the $\sqrt{q}$ term on the left-hand side) can be neglected and we obtain

$$sq + c \geqslant (2s+1)(q - sc - s^2\sqrt{q}).$$

With elementary computations we find that

$$c \geqslant q\frac{s+1}{2s^2+s+1} - s\sqrt{q}\frac{2s^2+s}{2s^2+s+1} > \frac{q}{2s} - s\sqrt{q},$$

which contradicts our assumption on c. □

In the statement of the previous lemma we tried to find a simple upper bound for c. The proof gives something slightly stronger, but even the stronger bound is not enough to use the full force of the improved fundamental lemma on lacunary polynomials.

PROPOSITION 4.6. *If $s < q^{1/4}/2$ and B is an s-fold blocking set of size $s(q+1)+c$ with $s\sqrt{q} \leqslant c < q/(2s) - s\sqrt{q}$ satisfying (*), then B contains the union of s disjoint Baer subplanes. In particular $c \geqslant s\sqrt{q}$.*

Proof. Let S be a Baer subplane contained in B (see Proposition 4.5). Consider the dual Baer subline of long lines for a point $P \in S$. Consider also the dual Baer subline at P consisting of the lines of S.

If these two were different then $|B| \geqslant 1 + (\sqrt{q}+1)(\sqrt{q}+s-1) + (\sqrt{q}-1)(\sqrt{q}) + (q+1-2\sqrt{q})(s-1)$. Here we used the fact that two dual Baer sublines intersect in at most two lines; see property (1) at the beginning of this section.

Simplifying the inequality gives $|B| \geqslant s(q+2) + q - s\sqrt{q} + \sqrt{q} - 1$, which is bigger than $s(q+1) + (q+1)/2$ already for $s \geqslant \sqrt{q}/2$.

Therefore the lines of S must be long lines and they form the dual Baer subline at P. Hence $B\backslash S$ is an $(s-1)$-fold blocking set, and repeating the procedure gives our proposition.

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press

Note that for s bigger than the bound in our proposition, $s\sqrt{q} \leqslant c < q/(2s) - s(\sqrt{q}+1)+1$ is a contradiction; hence in this case our proposition gives that s-fold blocking sets with $c < q/(2s) - s(\sqrt{q}+1)+1$ do not exist. □

This completes the proof of our main geometric theorem. Note that for small s, our bound on c is much larger than $s\sqrt{q}$. However, it can only be used for blocking sets satisfying condition (*). For example, it gives that a minimal blocking set satisfying (*) must be a Baer subplane if its size is smaller than $3q/2 - \sqrt{q}$. □

References

1. S. Ball, 'On the size of a triple blocking set in $PG(2,q)$', *European J. Combin.* 17 (1996) 427–435.
2. S. Ball, 'Multiple blocking set and arcs in finite planes', *J. London Math. Soc.* 54 (1996) 581–593.
3. S. Ball and A. Blokhuis, 'On the size of a double blocking set in $PG(2,q)$', *Finite Fields Appl.* 2 (1996) 125–137.
4. S. Ball, A. Blokhuis and F. Mazzocca, 'Maximal arcs in Desarguesian planes do not exist', *Combinatorica* 17 (1997) 31–41.
5. A. Barlotti, 'Su $\{k;n\}$-archi di un piano lineare finito', *Boll. Un. Mat. Ital.* 11 (1956) 553–556.
6. A. Blokhuis, 'On multiple nuclei and a conjecture of Lunelli and Sce', *Bull. Belg. Math. Soc.* 3 (1994) 349–353.
7. A. Blokhuis, 'Blocking sets in Desarguesian planes', *Paul Erdős is eighty – Vol. 2*, Bolyai Society Mathematical Studies 2 (ed. D. Miklós, V. T. Sós and T. Szőnyi, János Bolyai Mathematical Society, 1996) 133–155.
8. A. E. Brouwer and A. Schrijver, 'The blocking number of an affine space', *J. Combin. Theory Ser. A* 24 (1978) 251–253.
9. A. A. Bruen, 'Blocking sets in finite projective planes', *SIAM J. Appl. Math.* 21 (1971) 380–392.
10. A. A. Bruen, 'Arcs and multiple blocking sets', *Combinatorica Symp. Math.* 28 (1986) 15–29.
11. A. A. Bruen, 'Polynomial multiplicities over finite fields and intersection sets', *J. Combin. Theory Ser. A* 60 (1992) 19–33.
12. A. Gács and T. Szőnyi, 'Double blocking sets and Baer subplanes', unpublished manuscript, 1995.
13. R. Hill, 'Some problems concerning (k,n)-arcs in finite projective planes', *Rend. Sem. Mat. Brescia* 7 (1984) 367–383.
14. J. W. P. Hirschfeld, *Projective geometries over finite fields* (Clarendon Press, Oxford, 1979).
15. J. W. P. Hirschfeld and L. Storme, 'The packing problem in statistics, coding theory and finite projective spaces', *J. Statist. Plann. Inference* 72 (1998) 355–380.
16. R. E. Jamison, 'Covering finite fields with cosets of subspaces', *J. Combin. Theory Ser. A* 22 (1977) 253–266.
17. J. W. di Paola, 'On minimum blocking coalitions in small projective plane games', *SIAM J. Appl. Math.* 17 (1969) 378–392.
18. L. Rédei, *Lückenhafte Polynome über endlichen Körpern* (Birkhäuser, Basel, 1970).

A. Blokhuis
Technical University Eindhoven
PO Box 513
5600 MB Eindhoven
Netherlands

aartb@win.tue.nl

T. Szőnyi
Department of Computer Science
Eötvös Loránd University
Múzeum krt. 6–8
H-1088 Budapest
Hungary

szonyi@cs.elte.hu

L. Storme
University of Gent
FCW
Galglaan 2
9000 Gent
Belgium

ls@cage.rug.ac.be

https://doi.org/10.1112/S0024610799007875 Published online by Cambridge University Press