A $t \pmod p$ result on weighted multiple $(n-k)$-blocking sets in PG(n,q)

Sandy Ferret Leo Storme* Péter Sziklai†
Zsuzsa Weiner

Abstract

In this article, we prove a $t \pmod p$ result for minimal weighted t-fold $(n-k)$-blocking sets in PG(n,q), $q = p^h$, p prime, $h \geq 1$, $n \geq 2$. Such a theorem plays a crucial role in characterizing minimal weighted t-fold $(n-k)$-blocking sets. Our result is based on generalizations of earlier theorems on blocking sets in PG$(2,q)$ to weighted blocking sets of higher dimensions.

Keywords: weighted multiple blocking sets, $t \pmod p$ result

MSC 2000: 05B25, 51E20, 51E21

1. Introduction

Throughout this paper, PG(n,q) and AG(n,q) will respectively denote the n-dimensional projective and affine space over the Galois field GF(q), where $q = p^h$, p prime, $h \geq 1$.

A *t-fold* $(n-k)$*-blocking set* B of PG(n,q), with $0 < k < n$, is a set of points of PG(n,q) intersecting every k-dimensional subspace of PG(n,q) in at least t points.

*The second author thanks the Fund for Scientific Research Flanders-Belgium for a research grant.

†The third and the fourth author were partially sponsored by OTKA F043772, T043758, T049662, T067867, Magyary Z. grants, and the FWO Research Network WO.003.01N: Fundamental Methods and Techniques in Mathematics. They are also grateful for the hospitality of Ghent University, where this research was done.

ACADEMIA PRESS
UNIVERSITEIT GENT

A point P of B is called *essential* if there is a k-dimensional subspace through P intersecting B in exactly t points. A t-fold blocking set B is called *minimal* if all of its points are essential. A 1-fold $(n-k)$-blocking set is also called an $(n-k)$*-blocking set*. A t-fold 1-blocking set in $\mathrm{PG}(2,q)$ is also called a t*-fold blocking set*, or a t*-fold planar blocking set*. A 1-fold blocking set in $\mathrm{PG}(2,q)$ is simply called a *blocking set* in $\mathrm{PG}(2,q)$.

These latter t-fold planar blocking sets have been studied in great detail. General bounds can be found in Ball [1], and are mentioned in the following table. In this table, and in the following tables, p is a prime, and $c_2 = c_3 = 2^{-1/3}$, where $c_p = 1$ if $p > 3$. In the first table, the first two columns give the conditions on q and t, while the third column gives the lower bound on $k = |B| - t(q+1)$.

q	conditions	$k = \|B\| - t(q+1)$
q	no line in B	$\geq \sqrt{tq} + 1 - t$
$p > 3$	$1 < t < p/2$	$\geq (p+1)/2$
$p > 3$	$t > p/2$	$\geq p - t$

The following table contains what was proved for minimal t-fold blocking sets of $\mathrm{PG}(2,q)$ in [3]. The last two columns give the structure of B, plus an implied lower bound on the value k.

q	$t,\ k = \|B\| - t(q+1)$	implies k	B
p^{2d+1}	$t = 1,\ k < c_p q^{2/3}$		line
p^{2d+1}	$1 < t < q/2 - c_p q^{2/3}/2$	$\geq c_p q^{2/3}$	
$p^{2d} > 4$	$t = 1,\ k < c_p q^{2/3}$		line or Baer subplane
$p^{2d} > 4$	$1 < t < c_p q^{1/6},\ k < c_p q^{2/3}$	$\geq t\sqrt{q}$	union of t disjoint Baer subplanes
p^2	$t = 1,\ k < p\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}} \rceil$		line or Baer subplane
p^2	$1 < t < q^{1/4}/2,\ k < p\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}} \rceil$	$\geq t\sqrt{q}$	union of t disjoint Baer subplanes

The next two tables summarize the results of [2] for minimal t-fold blocking sets of $\mathrm{PG}(2,q)$. The third and fourth column give the implied lower bounds on k, the information on the structure of B, plus some extra remarks.

ACADEMIA PRESS
UNIVERSITEIT GENT

q	$t,\ k = \lvert B\rvert - t(q+1)$, other conditions	implies k	remark
p^{6m}	$2 \le t < p^{3m/2}/4,\ k < p^{4m}\sqrt{p}/2$ no Baer subplane in B	$\ge tp^{4m} - 4t^2p^{2m}$	
p^{6m+1}	$2 \le t < p^{3m/2+1/4}/4$, $k < p^{4m+1} - 2p^{2m+1}$	$\ge \max\big(tp^{4m} - 4t^2p^{2m-1}$, $p^{4m+1} - p^{4m} - p^{2m+1}/2\big)$	$m \ge 1$
p^{6m+2}	$2 \le t < p^3/(4(p+1))$ if $m = 1$ $2 \le t < p^{(3m+1)/2}/4$ if $m > 1$ $k < p^{4m+2}/2$ no Baer subplane in B	$\ge tp^{4m+1} - 4t^2p^{2m}$	$m \ge 1$ $p \ge 5$
p^{6m+3}	$2 \le t < p^{(6m+3)/4}/4$, $k < p^{4m+2}\sqrt{p}/2$	$\ge tp^{4m+2} - 4t^2p^{2m+1}$	$p \ge 23\ \ (m = 0)$ $p \ge 3\ \ \ (m = 1)$
p^{6m+4}	$2 \le t < p^{(3m+2)/2}/4$, $k < p^{4m+3} - 2p^{2m+2}$ no Baer subplane in B	$\ge \max\big(tp^{4m+2} - 4t^2p^{2m}$, $p^{4m+3} - p^{4m+2} - p^{2m+2}/2\big)$	$m \ge 1$
p^{6m+5}	$k < p^{4m+4}/2$, $2 \le t < p^{3m/2+5/4}/4$ for $m > 0$ $2 \le t \le (p-3)/4$ for $m = 0$	$\ge \max\big(tp^{4m+3} - 4t^2p^{2m+1}$, $p^{4m+7/2} - p^{4m+3} - p^{2m+2}/2\big)$	$p \ge 5$

q	$t,\ k = \lvert B\rvert - t(q+1)$, other conditions	B
p^{6m}	$2 \le t < p^{3m/2}/4, k < \min\big(p^{4m}\sqrt{p}/2$, $2p^{4m} + (t-2)p^{3m} - 16p^{2m}\big)$	$t-1$ disjoint Baer subplanes union a t-th minimal blocking set
p^{6m+2}	$m \ge 1,\ 2 \le t < p^{3m/2+1/2}/4,\ k < \min\big(p^{4m+2}/2$, $2p^{4m+1} + (t-2)p^{3m+1} - 16p^{2m}\big)$	union of t disjoint Baer subplanes
p^{6m+4}	$2 \le t < p^{(3m+2)/2}/4$, $k < \min\big(p^{4m+3} - 2p^{2m+2}, (t-2)p^{3m+2} +$ $\max(2p^{4m+2} - 16p^{2m}, p^{4m+3} - p^{4m+2} - p^{2m+2}/2)\big)$	union of t disjoint Baer subplanes

For a t-fold blocking set B, a "$t \pmod{p}$ result" states that every line intersects B in $t \pmod{p}$ points. In the theory of t-fold planar blocking sets, $t \pmod{p}$ results for *small* minimal t-fold planar blocking sets play an important role.

Definition 1.1. A blocking set of $\mathrm{PG}(2,q)$ is called *small* when it has less than $3(q+1)/2$ points.

If $q = p^h$, p prime, $h \geq 1$, the *exponent* e of the minimal blocking set B of $\mathrm{PG}(2,q)$ is the maximal integer e such that every line intersects B in $1 \pmod{p^e}$ points.

Theorem 1.2 (Szőnyi [10], Sziklai [9]). *Let B be a small minimal 1-fold blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$. Then B intersects every line in $1 \pmod{p}$ points, so for the exponent e of B we have $1 \leq e \leq h$. In fact this exponent is a divisor of h.*

The Linearity Conjecture (see Sziklai [9]) states that a small minimal blocking set is always a $\mathrm{GF}(p^e)$-linear blocking set, i.e. $\mathrm{GF}(p^e)$ is a subfield of $\mathrm{GF}(q)$ and the blocking set is a projected image of a suitable subgeometry $\mathrm{PG}(h/e, p^e)$.

Let's see how these notions were generalized for higher dimensions and for t-fold blocking sets.

Definition 1.3. A 1-fold $(n-k)$-blocking set of $\mathrm{PG}(n,q)$ is called *small* when it has less than $3(q^{n-k}+1)/2$ points.

If $q = p^h$, p prime, $h \geq 1$, the *exponent* e of a minimal 1-fold $(n-k)$-blocking set B in $\mathrm{PG}(n,q)$ is the maximal integer e such that every k-dimensional space intersects B in $1 \pmod{p^e}$ points.

Szőnyi and Weiner [11] proved a $1 \pmod{p}$ result for small minimal 1-fold $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$.

Theorem 1.4 (Szőnyi and Weiner [11]). *A minimal 1-fold $(n-k)$-blocking set in $\mathrm{PG}(n,q)$, $q = p^h$, $p > 2$ prime, $h \geq 1$, of size less than $\frac{3}{2}(q^{n-k}+1)$ intersects every subspace in zero points or in $1 \pmod{p}$ points.*

The $1 \pmod{p}$ result in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$, was extended by Blokhuis *et al.* to a $t \pmod{p}$ result on *small* minimal t-fold blocking sets in $\mathrm{PG}(2,q)$.

Definition 1.5. A t-fold blocking set of $\mathrm{PG}(2,q)$ is called *small* when it has less than $tq + (q+3)/2$ points.

If $q = p^h$, p prime, $h \geq 1$, the *exponent* e of the minimal t-fold blocking set B in $\mathrm{PG}(2,q)$ is the maximal integer e such that every line intersects B in $t \pmod{p^e}$ points.

ACADEMIA PRESS
UNIVERSITEIT GENT

Theorem 1.6 (Blokhuis *et al.* [2]). *Let B be a small minimal t-fold blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$, then B intersects every line in $t \pmod p$ points.*

For a multiset B in $\mathrm{PG}(n,q)$, we call the *multiplicity* of a point of B also the *weight* of that point. A point of B is called *simple* if it has weight one. A *multiple* point of B has weight larger than one. A *weighted t-fold $(n-k)$-blocking set* B of $\mathrm{PG}(n,q)$, with $0 < k < n$, is a multiset of points of $\mathrm{PG}(n,q)$ intersecting every k-dimensional subspace of $\mathrm{PG}(n,q)$ in at least t points, counted with weights.

A point P of a weighted t-fold $(n-k)$-blocking set B is called *essential* if there is a k-dimensional subspace through P intersecting B in t points, counted with weights. A weighted t-fold $(n-k)$-blocking set B is called *minimal* if all of its points are essential.

The General Linearity Conjecture for t-fold blocking sets (see Sziklai [9]) states that (if t is small enough then) a small minimal t-fold $(n-k)$-blocking set in $\mathrm{PG}(n,q)$ is always the (not necessarily disjoint) union of $\mathrm{GF}(p^{e_i})$-linear (possibly multiple) $(n-k)$-blocking sets, i.e. for each of the $(n-k)$-blocking sets $\mathrm{GF}(p^{e_i})$ is a subfield of $\mathrm{GF}(q)$ and it is a projected image of a suitable subgeometry $\mathrm{PG}(m_i, p^{e_i})$.

The goal of this article is to prove a $t \pmod p$ result on weighted minimal t-fold $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$, $n \geq 2$.

Once such a $t \pmod p$ result has been proved, characterization results can be obtained. We illustrate this in [5] by characterizing minimal t-fold $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$, q square.

We prove in the following section a $t \pmod p$ result on weighted minimal t-fold blocking sets in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$. This result is then used to obtain a $t \pmod p$ result on weighted minimal t-fold $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$, $n > 2$. Here the idea is based on the generalization of [11].

As a supplementary result, we also prove that small minimal weighted t-fold blocking sets in $\mathrm{PG}(2,q)$, containing a line ℓ, are the sum of this line ℓ and a minimal $(t-1)$-fold blocking set. This implies that, when characterizing small t-fold blocking sets in $\mathrm{PG}(2,q)$, it is possible to assume that they do not contain any lines.

2. A $t \pmod p$ result

Let B be a *minimal* weighted t-fold blocking set in $\mathrm{PG}(2,q)$, with $|B| = tq+t+k$, where $t + k < q$.

ACADEMIA PRESS
UNIVERSITEIT GENT

Assume that the line l_∞ is an m-secant to B. Consider PG$(2,q)$ as the affine plane AG$(2,q)$ with l_∞ as the line at infinity. Assume that $B \cap l_\infty = D = \{(\infty),\ldots,(\infty),(y_1),\ldots,(y_{m-s})\}$, where (∞) is a point of weight s of B $(1 \leq s \leq t)$, where some of the other points of D might be multiple points of B, and that $U = B \setminus D = \{(a_i,b_i) : i = 1,\ldots,tq+t+k-m\}$, where U is a multiset when B has affine multiple points.

We first define the Rédei polynomial associated to the t-fold blocking set B. The last equation in the following definition follows from the fact that this Rédei polynomial is t times zero everywhere in GF$(q) \times$ GF(q) [4].

Definition 2.1 (The Rédei polynomial of the set B).

$$\begin{aligned} H(X,Y) &= \prod_{j=1}^{m-s}(Y-y_j)\prod_{i=1}^{tq+t+k-m}(X+a_iY-b_i) \\ &= \prod_{j=1}^{m-s}(Y-y_j)\sum_{i=0}^{tq+t+k-m}X^{tq+t+k-m-i}h_i(Y) \qquad (1) \\ &= (X^q-X)^t f_0(X,Y)+(X^q-X)^{t-1}(Y^q-Y)f_1(X,Y) \\ &\qquad +\cdots+(Y^q-Y)^t f_t(X,Y)\,, \qquad (2) \end{aligned}$$

where $\deg(h_i) \leq i$, $i = 0,\ldots,tq+t+k-m$, and $\deg(f_i) \leq k+t-s$, $i = 0,\ldots,t$.

It is well-known that this polynomial encodes the intersection properties of B with lines: e.g. a line with equation $Y = mX+b$ intersects B in r points if and only if the point (b,m) in the *dual* plane has multiplicity r on the curve $H(X,Y)$ (i.e. r linear factors of H go through (b,m)).

Choose a point (b,m), $b \notin \{b_j \mid (0,b_j) \in U\}$, $m \neq y_j$. Consider $H(X,m) = (X^q-X)^t f_0(X,m)$. By the properties of the Rédei polynomial, the line $Y = mX+b$ intersects U in more than t points if and only if $X = b$ is a root of $H(X,m)$ with multiplicity $\geq t+1$ if and only if (b,m) is a point of the algebraic curve $f_0(X,Y)$. Considering $H(b,Y) = (Y^q-Y)^t f_t(b,Y)$ instead, we get that the line $Y = mX+b$ intersects U in more than t points if and only if (b,m) is a point of the algebraic curve $f_t(X,Y)$.

Therefore, these two algebraic curves f_0 and f_t have almost the same set of GF(q)-rational points.

If $m = y_j$ or $b \in \{b_j \mid (0,b_j) \in U\}$, and the line $Y = mX+b$ intersects U in more than t points, then $f_0(b,m) = f_t(b,m) = 0$ holds again. As $H(X,m)$ (or $H(b,Y)$) is identically zero in this case, $f_0(b,m) = 0$ or $f_t(b,m) = 0$ does not imply that $Y = mX+b$ intersects U in more than t points.

Later on in this section, we will assume that there is no line contained in B. As the following theorems will show, this is no restriction when $2t+k < q+2$.

Theorem 2.2. *Let B be a minimal weighted t-fold blocking set of $\mathsf{PG}(2,q)$, with $|B| = tq + t + k$, where $2t + k < q + 2$, containing a line ℓ. Then B is the sum of the line ℓ and the minimal weighted $(t-1)$-fold blocking set B^*, obtained from B by reducing the weight of every point P of ℓ by one.*

Proof. Since $\ell \subseteq B$, $|\ell \cap B| \geq q + 1$.

If $|\ell \cap B| \geq q + t$, then after reducing the weight of every point of ℓ by one, a new weighted set B^* is obtained which still intersects every line in at least $t - 1$ points. Since B is a minimal weighted t-fold blocking set, also B^* is a minimal weighted $(t-1)$-fold blocking set.

Assume now that $q + 1 \leq |B \cap \ell| < q + t$. Reduce again the weight of every point on ℓ by one, and add a minimal number of simple points $P_1, \ldots, P_r$ of ℓ back, until a weighted $(t-1)$-fold blocking set B^* is obtained, hence $|B^* \cap \ell| = t - 1$. We need to add at most $r \leq t - 1$ points to achieve this, hence $|B^*| \leq tq + t + k - (q + 1) + t - 1 = (t-1)q + 2(t-1) + k$. A particular feature of a point P_i, $i = 1, \ldots, r$, is that the line ℓ is the only $(t-1)$-secant to B^* passing through P_i.

Finally, we show that through P_i, there pass at least two $(t-1)$-secants, hence the above case cannot occur. Now we choose our coordinate system in such a way that $(\infty) \in B$, P_i is an affine point (a, b), and $\ell_\infty \cap \ell \notin B^*$ and (∞) has multiplicity s. Suppose that $|\ell_\infty \cap B^*| = m$ and write up the Rédei polynomial. Since B^* is a $(t-1)$-fold blocking set, using a suitable indexing we get that

$$\begin{aligned} H^*(X,Y) &= \prod_{j=1}^{m-s} (Y - y_j) \prod_{i=q+2}^{tq+t+k+r-m} (X + a_i Y - b_i) \\ &= (X^q - X)^{t-1} f_0^*(X,Y) + (X^q - X)^{t-2}(Y^q - Y) f_1^*(X,Y) \\ &\qquad + \cdots + (Y^q - Y)^{t-1} f_{t-1}^*(X,Y), \end{aligned} \tag{3}$$

where $\deg(f_i^*) \leq |B^*| - q(t-1) - s \leq 2(t-1) + k - s$, $i = 0, \ldots, t-1$.

The argument before this theorem shows that if a line $Y = mX + b$ intersects B^* in more than $(t-1)$ points, then (b, m) is a point of the curve f_0^*. Each line except ℓ through the point $P_i = (a, b)$ intersects B^* in at least t points. These lines are points of the line $X + aY - b$ in the dual plane. Hence $X + aY - b$ intersects f_0^* in at least $q - 1$ points (we do not see the vertical line here). Since $\deg f_0^* < q - 1$, Bézout's theorem implies that the line $X + aY - b$ is a component of f_0^*. Suppose that ℓ is the line $\ell = Y + m'X + b'$. Then $f_0^*(b', m') = 0$ and since $\ell \cap \ell_\infty \notin B^*$, ℓ intersects B^* in at least t points. This is a contradiction, hence $q + 1 \leq |B \cap \ell| < q + t$ does not occur. $\square$

As the next example shows, the above theorem is sharp.

Example 2.3. Let S be the set of points lying on the lines of a dual hyperoval in $\mathrm{PG}(2,q)$, q even. Then S is a $(\frac{q}{2}+1)$-fold blocking set of size $(\frac{q}{2}+1)q+(\frac{q}{2}+1)$ (each point in S has multiplicity one). Note that now $t=\frac{q}{2}+1$, $k=0$ and $2t+k=q+2$. If we delete a line of S, then the resulting point set is not a $\frac{q}{2}$-fold blocking set.

Remark 2.4. Theorem 2.2 has some straightforward applications.

(1) It first of all shows that when characterizing minimal weighted t-fold blocking sets of size $tq+t+k$, where $2t+k<q+2$, in $\mathrm{PG}(2,q)$, it is possible to assume that they do not contain any lines.

(2) Moreover, also when proving the $t \pmod p$ result for a minimal weighted t-fold blocking set B, $|B|=tq+t+k$, where $2t+k<q+2$, it is possible to assume that there are no lines contained in B. If there is a line ℓ contained in B, then Theorem 2.2 implies that you can reduce the weight of every point of ℓ by one in order to obtain a new minimal weighted $(t-1)$-fold blocking set B^*. Proving the $t \pmod p$ result for B is now reduced to proving the $(t-1) \pmod p$ result for B^*.

(3) Now we are also able to characterize weighted minimal t-fold blocking sets of size $tq+t$, with $2t<q+2$, and to exclude the existence of weighted minimal t-fold blocking sets of size $tq+t+1$, with $2t+1<q+2$.

Theorem 2.5. *A weighted t-fold blocking set B in $\mathrm{PG}(2,q)$, of size $|B|=tq+t$, where $2t<q+2$, is a sum of t lines.*

There does not exist a weighted minimal t-fold blocking set B in $\mathrm{PG}(2,q)$ of size $|B|=tq+t+1$, $2t+1<q+2$.

Proof. Suppose that $tq+t\le|B|\le tq+t+1$. Then counting the incidences of the points of B with the lines through a point R not in B, we have that through R all the lines are t-secants if $|B|=tq+t$ and there is exactly one $(t+1)$-secant and q t-secants through R if $|B|=tq+t+1$.

Now count the incidences of the points of B with the lines through a point $R'\in B$. Assume first of all that $|B|=t(q+1)$. Then we get in total $wt(R')+(q+1)(t-wt(R'))$ incidences if we assume that R' only lies on t-secants to B. Since $|B|=t(q+1)$, we obtain that $t(q+1)=t(q+1)-qwt(R')$, hence $wt(R')=0$, but then $R'\notin B$. So we get that R' lies on at least one line ℓ completely contained in B when $|B|=tq+t$.

Secondly, assume that $|B|=t(q+1)+1$, let $R'\in B$, and assume that R' does not lie on a line ℓ completely contained in B, then R' only lies on t- and $(t+1)$-secants to B. If we would assume that R' only lies on t-secants to B, then counting the incidences of the lines through R' with the points of B, we obtain $wt(R')+(q+1)(t-wt(R'))$ incidences. So, there still remain $t(q+1)+1-$

$wt(R')-t(q+1)+(q+1)wt(R') = 1+qwt(R')$ incidences of the lines through R' with the points of B. Since we assume that R' does not lie on a line completely contained in B, these lines can share at most one extra point with B. There are $q+1$ lines through R' and there remain $1+qwt(R')$ incidences. This implies that $wt(R') = 1$ and that R' lies on $q+1$ $(t+1)$-secants, when $|B| = tq+t+1$. This latter case means that B is not minimal. Hence we can assume that each point of B lies on at least one line completely contained in B.

Now the t points of any t-secant (which must exist) and Theorem 2.2 show that B contains the sum of t lines, which is a t-fold blocking set already, of size $tq+t$. $\square$

Remark 2.6. One can observe now that a weighted t-fold blocking set in $\mathrm{PG}(2,q)$, of size $tq+t$, where $2t < q+2$, intersects every line in $t \pmod p$ points; also that through any point of it there pass at least $q+1-t$ t-secants.

Lemma 2.7. *The polynomial $\prod_{j=1}^{t-s}(Y-y_j)$ divides $f_0(X,Y)$ if $k+t<q$.*

Proof. By (1),

$$H(X,Y) = \sum_{i=0}^{tq+k}\left(h_i(Y)\cdot\prod_{j=1}^{t-s}(Y-y_j)\right)X^{tq+k-i}.$$

So every coefficient polynomial of a term X^{tq+k-i} is divisible by $\prod_{j=1}^{t-s}(Y-y_j)$. By (2), the high degree part

$$\prod_{j=1}^{t-s}(Y-y_j)\cdot X^{tq+k}+\cdots+h_k(Y)\cdot\prod_{j=1}^{t-s}(Y-y_j)\cdot X^{tq}$$

must be equal to $X^{tq}f_0(X,Y)$, when one compares the X-degrees of the two expressions (1) and (2) for $H(X,Y)$. So $\prod_{j=1}^{t-s}(Y-y_j)$ divides $f_0(X,Y)$. $\square$

If $X=0$ intersects U in the, possible weighted, points $(0,b_j)$, $j=1,\ldots,z$, then a similar argument shows that $\prod_{j=1}^{z}(X-b_j)$ divides $f_t(X,Y)$, where the product is taken over the values b_j, according to their weights.

Theorem 2.8. *Let B be a minimal weighted t-fold blocking set of $\mathrm{PG}(2,q)$, with $|B| = tq+t+k < (t+1)q$. Then every point of B lies on at least $q+1-k-t$ different t-secants.*

Proof. Let $P=(a,b)\in U$ and suppose that $(\infty)\in B$, $|l_\infty\cap B| = t$. Assume that P lies on more than $k+t$ different lines sharing at least $t+1$ points with B. Then more than k of those lines intersect l_∞ in a point not belonging to B.

Each of these latter lines defines a point of $f_0(X,Y)/\prod_{j=1}^{t-s}(Y-y_j)$. More precisely, they define intersection points, in the dual plane, of the algebraic curve $f_0(X,Y)/\prod_{j=1}^{t-s}(Y-y_j)=0$ with the line $X+aY-b=0$. The polynomial $f_0(X,Y)/\prod_{j=1}^{t-s}(Y-y_j)$ has at most degree k, so by Bézout's theorem, the linear term $X+aY-b$ is a factor of $f_0(X,Y)/\prod_{j=1}^{t-s}(Y-y_j)$.

Consider a line through P with slope $m\neq y_j$, $m\neq\infty$, so that we can use the arguments above.

Evaluating $H(X,Y)$ at $Y=m$, we get

$$H(X,m)=\prod_{j=1}^{t-s}(m-y_j)\prod_{i=1}^{tq+k}(X+a_im-b_i)=(X^q-X)^t f_0(X,m).$$

The fact that $X+aY-b$ is a linear factor of f_0 means geometrically that the lines through P with slope $m\neq y_j$, $m\neq\infty$, intersect U in at least $t+1$ points.

We have shown that every line joining P to a point of $l_\infty\setminus B$ is a $\geq(t+1)$-secant. But l_∞ is an arbitrary t-secant, so for any t-secant l incident with P we just need to find a t-secant incident with a point of $l\setminus B$. A point $Q\notin B$ is incident with at least $q+1-k>t$ different t-secants, and so at least one of them meets l in a point not in B. □

Corollary 2.9. *Let B be a weighted t-fold blocking set of* $\mathrm{PG}(2,q)$*, with $|B|=tq+t+k<(t+1)q$. Assume that P is an essential point of B. Then there are at least $q+1-k-t$ different t-secants through P.*

Proof. Delete the non-essential points of B one-by-one until a minimal t-fold blocking set B' is obtained. By Theorem 2.8, there will be at least $q+1-(|B'|-tq)$ different t-secants of B' through P. Now if we add back the points of $B\setminus B'$, then through P, we will see at least $q+1-(|B'|-tq)-|B\setminus B'|$ t-secants to B. □

We will now adapt the results of [2, 8] to the case when there are multiple points. In this section, from now on, we suppose that $|B|<tq+(q+3)/2$. The cases of $|B|=t(q+1)$ and $|B|=t(q+1)+1$, with $|B|<tq+(q+3)/2$, are all discussed in Theorem 2.5, except for the case $|B|=t(q+1)$ with $t=q/2+1$ for q even.

The weighted t-fold blocking sets B in $\mathrm{PG}(2,q)$, q even, of size $t(q+1)$ with $t=q/2+1$, have been classified in [6] and [7]. They are either a sum of $t=q/2+1$ lines or equal to the $(q/2+1)$-fold blocking set of Example 2.3. So we can consider all the t-fold blocking sets of sizes $t(q+1)$ and $t(q+1)+1$, with $|B|<tq+(q+3)/2$, to be classified. So from now on, we assume that $tq+(q+3)/2>|B|=tq+t+k\geq tq+t+2$.

Note that since $k \geq 2$, we still have $2t + k < q + 2$ so that Theorem 2.2 is valid. Hence, we also can assume that B does not contain any line.

Furthermore, we choose our coordinate system so that ℓ_∞ is a t-secant and the point (∞) in B has multiplicity s, where $1 \leq s \leq t$.

The following lemma can be proved in the same way as [2, Lemma 3.2]. Let B be a minimal weighted t-fold blocking set of size $tq + t + k$, where $t + k < (q + 3)/2$ and $k \geq 2$. Recall the definition of the Rédei polynomial from the beginning of this section.

Lemma 2.10. *If a line $Y = mX + b$ intersects $B \cap U$ in more than t points, then $f_0(b, m) = \cdots = f_t(b, m) = 0$.*

The following lemma is similar to [2, Lemma 3.3].

Lemma 2.11. *The algebraic curve $f_0(X, Y) = 0$ does not have linear components depending on the variable X.*

Proof. Such a linear component depending on X should have the form $X + aY - b = 0$. The proof of Theorem 2.8 then shows that the point $P = (a, b)$ is a non-essential point of B; which contradicts the minimality of B. □

Lemma 2.12. *If B is minimal, then the polynomials $f_0, \ldots, f_t$ cannot have a common divisor different from $Y - y_j$.*

Proof. Such a polynomial would divide $H(X, Y)$; so would be linear. This can only be of the form $Y - y_j$. □

We now come to the main theorem of this section: the proof of the $t \pmod p$ result.

Theorem 2.13. *Let B be a minimal weighted t-fold blocking set in $\mathsf{PG}(2, q)$, $q = p^h$, p prime, $h \geq 1$, with $|B| = tq + t + k$, $t + k < (q + 3)/2$, $k \geq 2$. Then every line intersects B in $t \pmod p$ points.*

Proof. By Remark 2.4, it is possible to assume that B does not contain any lines. We will assume that the line at infinity intersects B in t points. In this way, we can use the beginning of the proof of [2, Theorem 3.1].

So let $h(X, Y)$ be an absolutely irreducible component of the polynomial $f_0(X, Y)/\prod_{j=1}^{t-s}(Y - y_j)$ of degree larger than one. The arguments of the proof of [2, Theorem 3.1] imply that $h'_X \equiv 0$.

If $Y = m \neq y_i$, we obtain $H(X, m) = (X^q - X)^t f_0(X, m)$, having $t \pmod p$ solutions since $f_0(X, m)$ is a p-th power. So every line $Y = mX + b$, not containing a point of B at infinity, intersects B in $t \pmod p$ points.

For every line ℓ of which we are not yet sure that it intersects B in $t \pmod p$ points, it is possible to find a new line at infinity intersecting B in t points and intersecting ℓ in a point not belonging to B. Repeating the previous arguments now shows that also ℓ intersects B in $t \pmod p$ points. □

The next corollary follows from Theorem 2.8 and Remark 2.6.

Corollary 2.14. *Let B be a weighted t-fold blocking set in* $\mathsf{PG}(2,q)$*, $q = p^h$, p prime, $h \geq 1$, with $|B| = tq + t + k$, $t + k < (q+3)/2$, $2t < q + 2$. Assume that all the points of B on the line ℓ are essential. Then ℓ intersects B in $t \pmod p$ points.* □

When each line intersects B in $t \pmod q$ points, then the characterization of B is immediate.

Proposition 2.15. *Let B be a minimal weighted t-fold blocking set in* $\mathsf{PG}(2,q)$ *of size $tq + t + k$, where $t + k < (q+3)/2$, $k \geq 2$. Assume that each line intersects B in $t \pmod q$ points. Then B is a sum of t (not necessarily different) lines.*

Proof. Let ℓ be a line of $\mathsf{PG}(2,q)$ not contained in B. Let $P \in \ell \setminus B$. Since all the lines, different from ℓ, through P contain at least t points of B, ℓ contains at most $t + k$ points of B.

Every point R of B lies on at least one line containing more than t points of B, so on a line ℓ containing at least $t + q$ points of B. Since $t + k < t + q$, the preceding paragraph implies that ℓ is contained in B. By Theorem 2.2, B is the sum of this line ℓ and a $(t-1)$-fold blocking set B^* intersecting every line in $(t-1) \pmod q$ points. Repeating the above argument shows that B is a sum of t lines. □

3. A lower bound on the size of B

We now determine a lower bound on the size of a minimal weighted t-fold blocking set B in $\mathsf{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$.

We again assume that B does not contain any lines, for it is trivially possible to construct a minimal weighted t-fold blocking set in $\mathsf{PG}(2,q)$ by taking a sum B of t lines. Then $|B| = t(q+1)$.

Theorem 3.1. *Let B be a minimal weighted t-fold blocking set in* $\mathsf{PG}(2,q)$*, $q = p^h$, p prime, $h \geq 1$, with $|B| = tq + t + k$, $t + k < (q+3)/2$, containing no lines.*

Assume that $h(X,Y)$ is a component of f_0, which can be written as $h(X,Y) = g(X^{p^e}, Y)$ with $g'_X \not\equiv 0$. Then $k \geq \frac{q+p^e}{p^e+1} - t + 1$.

ACADEMIA PRESS
UNIVERSITEIT GENT

Proof. This can be proved in the same way as [2, Prop. 3.6]. □

4. A $t \pmod p$ result in higher dimensions

Theorem 4.1. *A minimal weighted t-fold 1-blocking set B in $\mathsf{PG}(n,q)$, $q=p^h$, p prime, $h \geq 1$, of size $|B| = tq+t+k$, $t+k \leq (q-1)/2$, intersects every hyperplane in $t \pmod p$ points.*

Proof. The proof goes by induction on n. For $n=2$, see Theorem 2.13 and Remark 2.6. Assume now that the theorem is true for $n-1$ dimensions, we are going to prove it for n dimensions. We will adapt the ideas of [11].

Part 1. We embed $\Pi_n = \mathsf{PG}(n,q)$ into $\Pi_{2n-2} = \mathsf{PG}(2n-2,q)$. Let H be a hyperplane of Π_n.

By the induction hypothesis, we can assume that B is not contained in H. Assume therefore that $B \cap H$ is a weighted α-fold blocking set in H with respect to hyperplanes of H and of cardinality $\alpha(q+1)+\beta$, where $0 \leq \alpha < t$.

Consider an $(n-2)$-dimensional subspace L in H sharing α points with B. A counting argument shows that we can find an $(n-1)$-dimensional subspace $H^* \neq H$ of Π_n, through L, containing exactly t points P_i, $i=1,\ldots,t$, of B.

We construct in Π_{2n-2} the cone $\mathcal{C}$ with vertex P, where P is an $(n-3)$-dimensional space skew to Π_n, and base $B \cup \{Q\}$, with Q a point of $H^* \setminus H$, $Q \notin B$.

By [11, Remark 2.1], there exists a regular $(n-2)$-spread W of the hyperplane $\langle H^*, P\rangle$ of Π_{2n-2} so that it contains $\langle P, Q\rangle$ and L. Let π^W denote the projective plane defined by the $(n-2)$-spread W and let $\mathcal{C}'$ denote the image of $\mathcal{C}$ in π^W.

Part 2. We first discuss the structure of $\mathcal{C}'$ on the line at infinity of π^W.

The points of the cone with vertex P and base B in $\langle P, H^*\rangle$ are the points of t, not necessarily different, $(n-2)$-dimensional spaces $\langle P, P_i\rangle$, $i=1,\ldots,t$. The space $\langle P, Q\rangle$ belongs to the $(n-2)$-spread W and is given weight t in the weighted set $\mathcal{C}'$. The other elements of W are skew to $\langle P, Q\rangle$ and share at most one point with each of the spaces $\langle P, P_i\rangle$, $i=1,\ldots,t$. If an element of $W \setminus \{\langle P, Q\rangle\}$ contains γ points of the spaces $\langle P, P_i\rangle$, $i=1,\ldots,t$, then we give this element weight γ in $\mathcal{C}'$.

Hence the size of $\mathcal{C}'$ is $|B|q^{n-2}+t$.

Part 3. We prove that the set $\mathcal{C}'$ is a t-fold blocking set in π^W. The ideal point corresponding to the spread element $\langle P, Q\rangle$ has multiplicity t and so the lines in π^W through this point are blocked at least t times by $\mathcal{C}'$. Now take an arbitrary line ℓ' of π^W not through this ideal point. The $(n-1)$-dimensional subspace ℓ of Π_{2n-2} corresponding to this line is skew to P. The projection ℓ^* of ℓ from P to Π_n is an $(n-1)$-dimensional subspace in Π_n and so it contains at least t points of B. If S is in $\ell^* \cap B$ then $\langle P, S\rangle \subset \mathcal{C}'$, hence the intersection point of ℓ and $\langle P, S\rangle$ is a point of $\mathcal{C}'$. Therefore ℓ contains at least t points of $\mathcal{C}'$.

So, for $|B| = tq+t+k$, $t+k \leq (q-1)/2$, we have $|\mathcal{C}'| = tq^{n-1}+(t+k)q^{n-2}+t = tq^{n-1}+k'+t$ in $\pi^W = \mathrm{PG}(2, q^{n-1})$, with $t+k' < (q^{n-1}+3)/2$.

Note that in π^W, the subspace H corresponds to a line h. In the rest of the proof we will show that the points of $h \cap \mathcal{C}'$ are all essential to $\mathcal{C}'$. By Corollary 2.14, this will imply that h shares $t \pmod p$ points with $\mathcal{C}'$, and equivalently, that H shares $t \pmod p$ points with B.

Part 4. The ideal point L' of π^W corresponding to L is essential to $\mathcal{C}'$. To see this, note that we can find a second $(n-1)$-dimensional subspace through L, not lying in $\langle H^*, P\rangle$, containing t points of B. Hence the corresponding line in π^W will be a t-secant through L', which proves that the point L' is essential for $\mathcal{C}'$.

Finally we show that the points of $h \setminus L'$ are all essential to $\mathcal{C}'$.

Part 5. First we show that through each point R_i of $(H \setminus L) \cap B$ there is an $(n-1)$-space H_{R_i} of Π_n containing t points of B but not containing Q. Let $H^*_{R_i}$ be an $(n-1)$-space of Π_n through R_i containing t points of B and containing Q as well.

We show that there is an $(n-3)$-dimensional subspace Π_{n-3} in $H^*_{R_i}$ skew to B, such that $\langle \Pi_{n-3}, R_i\rangle \neq \langle \Pi_{n-3}, Q\rangle$ and such that $\langle \Pi_{n-3}, R_i\rangle$ only contains the point R_i of B. To obtain this, project the points of $(B \cap H^*_{R_i}) \setminus \{R_i\}$ from R_i to an $(n-2)$-space T of $H^*_{R_i}$ through Q. Since $|(B \cap H^*_{R_i}) \setminus \{R_i\}| \leq t-1$, the projection will contain at most $t-1 < q$ different points, hence we can choose an $(n-3)$-space M in T not containing Q nor any of the projections of the points of $(B \cap H^*_{R_i}) \setminus \{R_i\}$. So $\langle M, R_i\rangle$ intersects $B \cup \{Q\}$ in R_i only, hence for Π_{n-3} we can choose any of the $(n-3)$-spaces of $\langle M, R_i\rangle$ that are skew to R_i.

We now project B from Π_{n-3} onto a plane π of Π_n. We obtain a weighted t-fold blocking set B^* in π, of size $|B^*| = tq+t+k, t+k \leq (q-1)/2$, where R_i is projected onto a point R_i^* having the same weight as R_i and where $H^*_{R_i}$ is projected onto a t-secant through R_i. Hence R_i is an essential point of B^* and

ACADEMIA PRESS
UNIVERSITEIT GENT

so, by Corollary 2.9, we can choose a t-secant ℓ through R_i^*, but not through Q. Then the $(n-1)$-space $H_{R_i} = \langle \Pi_{n-3}, \ell \rangle$ contains t points of B but does not contain Q.

Part 6. Finally we show that the point R_i' in π^W (corresponding to R_i) is essential to $\mathcal{C}'$. A particular property of an $(n-2)$-spread in $\langle H^*, P\rangle = \mathrm{PG}(2n-3, q)$ is that every hyperplane of $\langle H^*, P\rangle$ contains exactly one element of the $(n-2)$-spread. The hyperplane $\langle H_{R_i}, P\rangle$ of Π_{2n-2} intersects $\langle H^*, P\rangle$ in a $(2n-4)$-dimensional subspace, so it contains one element w of W. The point $Q \notin H_{R_i}$, hence $w \neq \langle P, Q\rangle$. We show that $\langle w, R_i\rangle$ corresponds to a t-secant in π^W. As in Part 4, projecting the points of $\langle w, R_i\rangle$ from P to H_{R_i}, we get a one-to-one correspondence between the points of $H_{R_i} \cap B$ and $\langle w, R_i\rangle$, which proves that R_i' is essential to $\mathcal{C}'$. □

Theorem 4.2. *Let B be a minimal weighted t-fold $(n-k)$-blocking set of $\mathrm{PG}(n, q)$, $q = p^h$, p prime, $h \geq 1$, of size $|B| = tq^{n-k} + t + k'$, with $t + k' \leq (q^{n-k} - 1)/2$. Then B intersects every k-dimensional subspace in $t \pmod p$ points.*

Proof. This proof is similar to the proof of [11, Theorem 2.7]. We include it since it makes clear where the upper bound on the size of B comes from.

Case $k = n-1$ is proved in Theorem 4.1. Now let $k < n-1$. Embed $\mathrm{PG}(n, q)$ in $\mathrm{PG}(n, q^{n-k})$ as a subgeometry. Consider $\mathrm{PG}(n, q^{n-k})$ as an $(n+1)(n-k)$-dimensional vector space V over $\mathrm{GF}(q)$. A hyperplane of $\mathrm{PG}(n, q^{n-k})$ is an $n(n-k)$-dimensional vector space and $\mathrm{PG}(n, q)$ is an $(n+1)$-dimensional vector space in V. Hence, a hyperplane of $\mathrm{PG}(n, q^{n-k})$ contains at least a k-dimensional subspace of $\mathrm{PG}(n, q)$. Therefore, B is a t-fold blocking set with respect to the hyperplanes of $\mathrm{PG}(n, q^{n-k})$.

Then B is a minimal t-fold blocking set with respect to the hyperplanes of $\mathrm{PG}(n, q^{n-k})$. Namely, consider a point P of B. Since B was minimal as a t-fold $(n-k)$-blocking set in $\mathrm{PG}(n, q)$, there exists a k-dimensional subspace K of $\mathrm{PG}(n, q)$ through P that intersects B in exactly t points. Any hyperplane of $\mathrm{PG}(n, q^{n-k})$ through K that intersects $\mathrm{PG}(n, q)$ exactly in K proves that P is essential for B as t-fold blocking set with respect to the hyperplanes of $\mathrm{PG}(n, q^{n-k})$.

To prove the $t \pmod p$ result, every k-dimensional space K of $\mathrm{PG}(n, q)$ can be extended to a hyperplane of $\mathrm{PG}(n, q^{n-k})$ intersecting $\mathrm{PG}(n, q)$ in precisely this k-dimensional space K. Since $|B| = tq^{n-k} + t + k'$, with $t + k' \leq (q^{n-k} - 1)/2$, it is possible to apply Theorem 4.1. This hyperplane shares $t \pmod p$ points with B, so B shares $t \pmod p$ points with K. □

ACADEMIA PRESS
UNIVERSITEIT GENT

Lemma 4.3. *Let B be a minimal weighted t-fold 1-blocking set of* $\mathrm{PG}(n,q)$*, $q = p^h$, p prime, $h \geq 1$, of size $|B| = tq + t + k'$, with $t + k' \leq (q-1)/2$.*

By Theorem 4.1, each hyperplane intersects B in $t \pmod{p^e}$ points for some $e \geq 1$, with e the maximal integer for which this is true. Then for $0 \leq s \leq n-1$ and every s-dimensional subspace Π_s, $|B \cap \Pi_s| \in \{0, 1, \ldots, t\} \pmod{p^e}$.

Proof. Note that we can assume $t < p^e - 1$, otherwise the statement is obvious. Consider Π_s with $0 \leq s \leq n-2$, and suppose to the contrary that $|B \cap \Pi_s| \in \{t+1, \ldots, p^e - 1\} \pmod{p^e}$. Then each hyperplane through Π_s contains at least $t+1$ further points from $B \setminus \Pi_s$.

There are $|\mathrm{PG}(n-1-s,q)|$ hyperplanes through Π_s, so the number of incidences of the points of $B \setminus \Pi_s$ with the hyperplanes through Π_s is at least $(t+1)(q^{n-s}-1)/(q-1)$. As every point of $B \setminus \Pi_s$ takes part in $(q^{n-s-1}-1)/(q-1)$ incidences, we have $|B| \geq |B \setminus \Pi_s| \geq (t+1)(q^{n-s}-1)/(q^{n-s-1}-1) \geq (t+1)q$, which is false. □

Theorem 4.4. *Let B be a minimal weighted t-fold $(n-k)$-blocking set of* $\mathrm{PG}(n,q)$*, $q = p^h$, p prime, $h \geq 1$, of size $|B| = tq^{n-k} + t + k'$, with $t + k' \leq (q^{n-k} - 1)/2$.*

Let $e \geq 1$ be the largest integer such that each k-dimensional subspace intersects B in $t \pmod{p^e}$ points. Then, for $0 \leq s \leq k$ and every s-dimensional subspace Π_s, we have $|B \cap \Pi_s| \in \{0, 1, \ldots, t\} \pmod{p^e}$.

Proof. As in the proof of Theorem 4.2, embed $\mathrm{PG}(n,q)$ in $\mathrm{PG}(n,q^{n-k})$ as a subgeometry and note again that B is a minimal t-fold blocking set with respect to hyperplanes of $\mathrm{PG}(n,q^{n-k})$. Now apply Lemma 4.3. □

We note that all the known small minimal weighted t-fold $(n-k)$-blocking sets are unions of (not necessarily disjoint) linear $(n-k)$-blocking sets (if $t \leq p^e$, then linear 1-fold $(n-k)$-blocking sets), satisfying the General Linearity Conjecture for small minimal t-fold blocking sets. As these examples suggest, we think that for $0 \leq s \leq k-1$, $|B \cap \Pi_s| \equiv 0 \pmod{p^e}$ can only occur if $B \cap \Pi_s$ is in fact empty (some assumption for t might be needed). For $t = 1$, this was proved in [11].

5. Intervals on the sizes of minimal t-fold $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$

First we prove a lower bound on the size of a minimal weighted t-fold 1-blocking set.

Theorem 5.1. *Let B be a minimal weighted t-fold 1-blocking set in $\mathsf{PG}(n,q)$, $q=p^h$, p prime, $h\geq 1$. Assume that $|B|=tq+t+k$, where $t+k\leq (q-1)/2$. Let e be the largest integer for which each hyperplane intersects B in $t \pmod{p^e}$ points. Then*

$$|B|\geq tq+\frac{q^{n-1}+p^e}{q^{n-2}(p^e+1)}-\frac{t}{q^{n-2}}\,.$$

For simplicity we note that this bound implies the slightly weaker bound

$$|B|\geq tq+\frac{q}{p^e+1}-1\,.$$

Proof. By the maximality of e, there exists a hyperplane H such that $|B\cap H|\not\equiv t \pmod{p^{e+1}}$. Embed $\mathsf{PG}(n,q)$ into $\mathsf{PG}(2n-2,q)$ and as in the proof of Theorem 4.1, construct the cone $\mathcal{C}$. In the corresponding plane π^W, $\mathcal{C}'$ is a weighted t-fold blocking set of size $|\mathcal{C}'|=|B|q^{n-2}+t$. The blocking set $\mathcal{C}'$ is not necessarily minimal, but due to our construction, the subspace H corresponds to a line h of π^W so that all the points of $h\cap\mathcal{C}'$ are essential to $\mathcal{C}'$. If there are non-essential points in $\mathcal{C}'$, delete them one-by-one until a minimal t-fold blocking set B' of π^W is obtained. By Theorem 4.1, B' intersects each line of π^W in $t \pmod{p^{e^*}}$ points for some $e^*\leq e$. Since the lower bound in Theorem 3.1 is decreasing in e, $|\mathcal{C}'|\geq|B'|\geq tq^{n-1}+\frac{q^{n-1}+p^e}{p^e+1}+1$ holds, from which the bound on $|B|$ follows. $\square$

Theorem 5.1 immediately yields a lower bound on the size of minimal t-fold $(n-k)$-blocking sets in $\mathsf{PG}(n,q)$. As in the proof of Theorem 4.2, embed $\mathsf{PG}(n,q)$ in $\mathsf{PG}(n,q^{n-k})$ as a subgeometry and note again that B is a t-fold blocking set with respect to hyperplanes of $\mathsf{PG}(n,q^{n-k})$.

Corollary 5.2. *Let B be a minimal weighted t-fold $(n-k)$-blocking set in $\mathsf{PG}(n,q)$, $q=p^h$, p prime, $h\geq 1$. Assume that $|B|=tq^{n-k}+t+k'$, where $t+k'\leq (q^{n-k}-1)/2$. Let e be the largest integer for which each k-space intersects B in $t \pmod{p^e}$ points. Then*

$$|B|\geq tq^{n-k}+\frac{q^{n-k}}{p^e+1}-1\,. \qquad \square$$

Warning. From now on, we consider point sets *without* weights.

Theorem 5.3. *Let B be a minimal t-fold $(n-k)$-blocking set in $\mathsf{PG}(n,q)$, $n\geq 2$, $|B|=tq^{n-k}+t+k'$, with $t+k'\leq(q^{n-k}-1)/2$. Assume that $q=p^h$, p prime, $h\geq 1$, and that B intersects every k-dimensional space in $t \pmod{E}$ points, with $E=p^e$. If $2t<E$, then*

$$tq^{n-k}+\frac{q^{n-k}}{p^e+1}-1\leq|B|\leq tq^{n-k}+\frac{2tq^{n-k}}{E}\,.$$

Proof. Let τ_{t+iE} be the number of k-dimensional spaces intersecting B in $t+iE$ points. We count the number of k-dimensional spaces, the number of incident pairs (R,π), with $R \in B$ and with π a k-dimensional space through R, and the number of triples (R,R',π), with R and R' distinct points of B and π a k-dimensional space passing through R and R'.

Then the following formulas are valid.

$$\sum_{i\geq 0} \tau_{t+iE} = \frac{(q^{n+1}-1)(q^n-1)}{(q^{k+1}-1)(q^k-1)} \cdot C\,,$$
$$\sum_{i\geq 0} (t+iE)\tau_{t+iE} = |B| \left(\frac{q^n-1}{q^k-1}\right) \cdot C\,,$$
$$\sum_{i\geq 0} (t+iE)(t+iE-1)\tau_{t+iE} = |B|(|B|-1) \cdot C\,,$$

where
$$C = \frac{(q^{n-1}-1)\cdots(q^{n+1-k}-1)}{(q^{k-1}-1)\cdots(q-1)}\,.$$

Then $\sum_{i\geq 0} i(i-1)E^2\tau_{t+iE} \geq 0$ implies that

$$|B|(|B|-1) - (2t-1)|B|\left(\frac{q^n-1}{q^k-1}\right) + t^2\left(\frac{(q^{n+1}-1)(q^n-1)}{(q^{k+1}-1)(q^k-1)}\right)$$
$$- |B|E\left(\frac{q^n-1}{q^k-1}\right) + tE\left(\frac{(q^{n+1}-1)(q^n-1)}{(q^{k+1}-1)(q^k-1)}\right) \geq 0\,.$$

Under the condition $2t < E$, this implies that

$$|B| \leq tq^{n-k} + \frac{2tq^{n-k}}{E} \quad \text{or} \quad |B| \geq Eq^{n-k} + t\,.$$

The lower bound on the size of B was proved earlier. $\square$

The preceding proof also leads to the following corollary.

Corollary 5.4. *Let B be a minimal t-fold $(n-k)$-blocking set in* $\mathsf{PG}(n,q)$*. Assume that $q = p^h$, p prime, $h \geq 1$, and that B intersects every k-dimensional space in $t \pmod{E}$ points, with $E = p^e$. If $\max\{2t, 4\} < E$, then*

$$|B| \leq tq^{n-k} + \frac{2tq^{n-k}}{E} \quad \text{or} \quad |B| \geq Eq^{n-k} + t\,. \qquad \square$$

6. A characterization result which follows from the $t \pmod p$ result

In [5], the preceding $t \pmod p$ results are used to characterize minimal t-fold $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$, q square, of small cardinality.

Theorem 6.1. *Let B be a minimal t-fold $(n-k)$-blocking set in $\mathrm{PG}(n,q)$, q square, of size at most $|B| \le tq^{n-k} + 2tq^{n-k-1}\sqrt{q} < tq^{n-k} + q^{n-k-1/3}$. Then B is a union of t pairwise disjoint cones $\langle \pi_{m_i}, \mathrm{PG}(2(n-k-m_i-1), \sqrt{q})\rangle$, $-1 \le m_i \le n-k-1$, with vertex an m_i-dimensional space π_{m_i} and base $\mathrm{PG}(2(n-k-m_i-1), \sqrt{q})$, $i = 1, \ldots, t$.*

If $t \ge 2$, then $k > n/2$ if B contains at least one $(n-k)$-dimensional space $\mathrm{PG}(n-k,q)$ and $k \ge n/2$ in the other cases. □

Acknowledgments. We thank Tamás Szőnyi for his valuable comments and suggestions concerning the first drafts of this paper. We are also grateful to the anonymous referees of an earlier version of this paper, whose many pieces of advice were helpful when preparing the current version.

References

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

[2] **A. Blokhuis**, **L. Lovász**, **L. Storme** and **T. Szőnyi**, On multiple blocking sets in Galois planes, *Adv. Geom.* **7** (2007), 39–53.

[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* **60** (1992), 19–33.

[5] **S. Ferret**, **L. Storme**, **P. Sziklai** and **Zs. Weiner**, A characterization of multiple $(n-k)$-blocking sets in projective spaces of square order, submitted.

[6] **R. Hill** and **H. Ward**, A geometric approach to classifying Griesmer codes, *Des. Codes Cryptogr.* **44** (2007), 169–196.

[7] **I. Landjev** and **L. Storme**, On weighted $\{\delta(q+1), \delta; 2, q\}$-minihypers, unpublished manuscript.

[8] **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.

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

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

[11] **T. Szőnyi** and **Zs. Weiner**, Small blocking sets in higher dimensions, *J. Combin. Theory Ser. A* **95** (2001), 88–101.

Sandy Ferret

Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281-S22, 9000 Ghent, Belgium

e-mail: saferret@cage.ugent.be

website: http://cage.ugent.be/~saferret

Leo Storme

Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281-S22, 9000 Ghent, Belgium

e-mail: ls@cage.ugent.be

website: http://cage.ugent.be/~ls

Péter Sziklai

Eötvös University Budapest, Dept. of Computer Science, Pázmány P. s. 1/c, Budapest, Hungary, H-1117

e-mail: sziklai@cs.elte.hu

website: http://www.cs.elte.hu/~sziklai/

Zsuzsa Weiner

Eötvös University Budapest, Dept. of Computer Science, Pázmány P. s. 1/c, Budapest, Hungary, H-1117

e-mail: weiner@cs.elte.hu