On the linearity of higher-dimensional blocking sets

G. Van de Voorde*

Submitted: Jun 16, 2010; Accepted: Nov 29, 2010; Published: Dec 10, 2010
Mathematics Subject Classification: 51E21

Abstract

A small minimal k-blocking set B in $\mathrm{PG}(n,q)$, $q=p^t$, p prime, is a set of less than $3(q^k+1)/2$ points in $\mathrm{PG}(n,q)$, such that every $(n-k)$-dimensional space contains at least one point of B and such that no proper subset of B satisfies this property. The *linearity conjecture* states that all small minimal k-blocking sets in $\mathrm{PG}(n,q)$ are linear over a subfield $\mathbb{F}_{p^e}$ of $\mathbb{F}_q$. Apart from a few cases, this conjecture is still open. In this paper, we show that to prove the linearity conjecture for k-blocking sets in $\mathrm{PG}(n,p^t)$, with exponent e and $p^e \geq 7$, it is sufficient to prove it for one value of n that is at least $2k$. Furthermore, we show that the linearity of small minimal blocking sets in $\mathrm{PG}(2,q)$ implies the linearity of small minimal k-blocking sets in $\mathrm{PG}(n,p^t)$, with exponent e, with $p^e \geq t/e+11$.

Keywords: blocking set, linear set, linearity conjecture

1 Introduction and preliminaries

If V is a vectorspace, then we denote the corresponding projective space by $\mathrm{PG}(V)$. If V has dimension n over the finite field $\mathbb{F}_q$, with q elements, $q=p^t$, p prime, then we also write V as $\mathrm{V}(n,q)$ and $\mathrm{PG}(V)$ as $\mathrm{PG}(n-1,q)$. A k-dimensional space will be called a k-space.

A *k-blocking set* in $\mathrm{PG}(n,q)$ is a set B of points such that every $(n-k)$-space of $\mathrm{PG}(n,q)$ contains at least one point of B. A k-blocking set B is called *small* if $|B|<3(q^k+1)/2$ and *minimal* if no proper subset of B is a k-blocking set. The points of a k-space of $\mathrm{PG}(n,q)$ form a k-blocking set, and every k-blocking set containing a k-space is called *trivial*. Every small minimal k-blocking set B in $\mathrm{PG}(n,p^t)$, p prime, has an *exponent* e, defined to be the largest integer for which every $(n-k)$-space intersects B in 1 mod p^e points. The fact that every small minimal k-blocking set has an exponent $e \geq 1$ follows from a result of Szőnyi and Weiner and will be explained in Section 2. A minimal k-blocking set B in $\mathrm{PG}(n,q)$ is of *Rédei-type* if there exists a hyperplane containing $|B|-q^k$ points of B; this

*The author is supported by the Fund for Scientific Research Flanders (FWO – Vlaanderen).

is the maximum number possible if B is small and spans $\mathrm{PG}(n, q)$. For a long time, all constructed small minimal k-blocking sets were of Rédei-type, and it was conjectured that all small minimal k-blocking sets must be of Rédei-type. In 1998, Polito and Polverino [9] used a construction of Lunardon [8] to construct small minimal *linear* blocking sets that were not of Rédei-type, disproving this conjecture. Soon people conjectured that all small minimal k-blocking sets in $\mathrm{PG}(n, q)$ must be linear. In 2008, the 'Linearity conjecture' was for the first time formally stated in the literature, by Sziklai [15].

A point set S in $\mathrm{PG}(V)$, where V is an $(n+1)$-dimensional vector space over $\mathbb{F}_{p^t}$, is called *linear* if there exists a subset U of V that forms an $\mathbb{F}_{p_0}$-vector space for some $\mathbb{F}_{p_0} \subset \mathbb{F}_{p^t}$, such that $S = \mathcal{B}(U)$, where

$$\mathcal{B}(U) := \{\langle u \rangle_{\mathbb{F}_{p^t}} \ : \ u \in U \setminus \{0\}\}.$$

If we want to specify the subfield we call S an $\mathbb{F}_{p_0}$*-linear set* (of $\mathrm{PG}(n, p^t)$).

We have a one-to-one correspondence between the points of $\mathrm{PG}(n, p_0^h)$ and the elements of a Desarguesian $(h-1)$-spread $\mathcal{D}$ of $\mathrm{PG}(h(n+1)-1, p_0)$. This gives us a different view on linear sets; namely, an $\mathbb{F}_{p_0}$-linear set is a set S of points of $\mathrm{PG}(n, p_0^h)$ for which there exists a subspace π in $\mathrm{PG}(h(n+1)-1, p_0)$ such that the points of S correspond to the elements of $\mathcal{D}$ that have a non-empty intersection with π. We identify the elements of $\mathcal{D}$ with the points of $\mathrm{PG}(n, p_0^h)$, so we can view $\mathcal{B}(\pi)$ as a subset of $\mathcal{D}$, i.e.

$$\mathcal{B}(\pi) = \{S \in \mathcal{D} | S \cap \pi \neq \emptyset\}.$$

If we want to denote the element of $\mathcal{D}$ corresponding to the point P of $\mathrm{PG}(n, p_0^h)$, we write $\mathcal{S}(P)$, analogously, we denote the set of elements of $\mathcal{D}$ corresponding to a subspace H of $\mathrm{PG}(n, p_0^h)$, by $\mathcal{S}(H)$. For more information on this approach to linear sets, we refer to [7].

To avoid confusion, subspaces of $\mathrm{PG}(n, p_0^h)$ will be denoted by capital letters, while subspaces of $\mathrm{PG}(h(n+1)-1, p_0)$ will be denoted by lower-case letters.

Remark 1. The following well-known property will be used throughout this paper: if $\mathcal{B}(\pi)$ is an $\mathbb{F}_{p_0}$-linear set in $\mathrm{PG}(n, p_0^h)$, where π is a d-dimensional subspace of $\mathrm{PG}(h(n+1)-1, p_0)$, then for every point x in $\mathrm{PG}(h(n+1)-1, p_0)$, contained in an element of $\mathcal{B}(\pi)$, there is a d-dimensional space π', through x, such that $\mathcal{B}(\pi) = \mathcal{B}(\pi')$. This is a direct consequence of the fact that the elementwise stabilisor of $\mathcal{D}$ in $\mathrm{P\Gamma L}(h(n+1), p_0)$ acts transitively on the points of one element of $\mathcal{D}$.

To our knowledge, the Linearity conjecture for k-blocking sets B in $\mathrm{PG}(n, p^t)$, p prime, is still open, except in the following cases:

- $t = 1$ (for $n = 2$, see [1]; for $n > 2$, this is a corollary of Theorem 1 (i));
- $t = 2$ (for $n = 2$, see [13]; for $k = 1$, see [12]; for $k \geq 1$, see [3] and [16]);
- $t = 3$ (for $n = 2$, see [10]; for $k = 1$, see [12]; for $k \geq 1$, see [6] and independently [4],[5]);

- B is of Rédei-type (for $n = 2$, see [2]; for $n > 2$, see [11]);
- B spans an tk-dimenional space (see [14, Theorem 3.14]).

It should be noted that in $\mathrm{PG}(2, p^t)$, for $t = 1, 2, 3$, all small minimal blocking sets are of Rédei-type. Storme and Weiner show in [12] that small minimal 1-blocking sets in $\mathrm{PG}(n, p^t)$, $t = 2, 3$, are of Rédei-type too. The proofs rely on the fact that for $t = 2, 3$, small minimal blocking sets in $\mathrm{PG}(2, p^t)$ are listed. The special case $k = 1$ in Main Theorem 1 of this paper shows that using the (assumed) linearity of planar small minimal blocking sets, it is possible to prove the linearity of small minimal 1-blocking sets in $\mathrm{PG}(n, p^t)$, which reproofs the mentioned statements of Storme and Weiner in the cases $t = 2, 3$.

The techniques developed in [6] to show the linearity of k-blocking sets in $\mathrm{PG}(n, p^3)$, using the linearity of 1-blocking sets in $\mathrm{PG}(n, p^3)$, can be modified to apply for general t. This will be Main Theorem 2 of this paper. In particular, this theorem reproofs the results of [16], [6], [4], [5].

In this paper, we prove the following main theorems. Recall that the exponent e of a small minimal k-blocking set is the largest integer such that every $(n-k)$-space meets in 1 mod p^e points. Theorem 1 (i) will assure that the exponent of a small minimal blocking set is at least 1.

Main Theorem 1. *If for a certain pair (k, n^*) with $n^* \geq 2k$, all small minimal k-blocking sets in $\mathrm{PG}(n^*, p^t)$ are linear, then for all $n > k$, all small minimal k-blocking sets with exponent e in $\mathrm{PG}(n, p^t)$, p prime, $p^e \geq 7$, are linear.*

In particular, this shows that if the linearity conjecture holds in the plane, it holds for all small minimal 1-blocking sets with exponent e in $\mathrm{PG}(n, p^t)$, $p^e \geq 7$.

Main Theorem 2. *If all small minimal 1-blocking sets in $\mathrm{PG}(n, p^t)$ are linear, then all small minimal k-blocking sets with exponent e in $\mathrm{PG}(n, p^t)$, $n > k$, $p^e \geq t/e + 11$, are linear.*

Combining the two main theorems yields the following corollary.

Corollary 1. *If the linearity conjecture holds in the plane, it holds for all small minimal k-blocking sets with exponent e in $\mathrm{PG}(n, p^t)$, $n > k$, p prime, $p^e \geq t/e + 11$.*

2 Previous results

In this section, we list a few results on the linearity of small minimal k-blocking sets and on the size of small k-blocking sets that will be used throughout this paper. The first of the following theorems of Szőnyi and Weiner has the linearity of small minimal k-blocking sets in projective spaces over prime fields as a corollary.

Theorem 1. *Let B be a k-blocking set in $\mathrm{PG}(n, q)$, $q = p^t$, p prime.*

(i) [14, Theorem 2.7] *If B is small and minimal, then B intersects every subspace of* $\mathrm{PG}(n,q)$ *in* 1 *mod* p *or zero points.*

(ii) [14, Lemma 3.1] *If $|B| \leq 2q^k$ and every $(n-k)$-space intersects B in 1 mod p points, then B is minimal.*

(iii) [14, Corollary 3.2] *If B is small and minimal, then the projection of B from a point $Q \notin B$ onto a hyperplane H skew to Q is a small minimal k-blocking set in H.*

(iv) [14, Corollary 3.7] *The size of a non-trivial k-blocking set in* $\mathrm{PG}(n,p^t)$*, p prime, with exponent e, is at least $p^{tk}+1+p^e\lceil \frac{p^{tk}/p^e+1}{p^e+1}\rceil$.*

Part (iv) of the previous theorem gives a lower bound on the size of a k-blocking set. In this paper, we will work with the following, weaker, lower bound.

Corollary 2. *The size of a non-trivial k-blocking set in* $\mathrm{PG}(n,p^t)$*, p prime, with exponent e, is at least $p^{tk}+p^{tk-e}-p^{tk-2e}$.*

If a blocking set B in $\mathrm{PG}(2,q)$ is $\mathbb{F}_{p_0}$-linear, then every line intersects B in an $\mathbb{F}_{p_0}$-linear set. If B is small, many of these $\mathbb{F}_{p_0}$-linear sets are $\mathbb{F}_{p_0}$-sublines (i.e. $\mathbb{F}_{p_0}$-linear sets of rank 2). The following theorem of Sziklai shows that for *all* small minimal blocking sets, this property holds.

Theorem 2. *(i)* [15, Proposition 4.17 (2)] *If B is a small minimal blocking set in* $\mathrm{PG}(2,q)$*, with $|B|=q+\kappa$, then the number of (p_0+1)-secants to B through a point P of B lying on a (p_0+1)-secant to B, is at least*

$$q/p_0 - 3(\kappa-1)/p_0 + 2.$$

(ii) [15, Theorem 4.16] *Let B be a small minimal blocking set with exponent e in* $\mathrm{PG}(2,q)$*. If for a certain line L, $|L\cap B| = p^e+1$, then $\mathbb{F}_{p^e}$ is a subfield of $\mathbb{F}_q$ and $L\cap B$ is $\mathbb{F}_{p^e}$-linear.*

The next theorem, by Lavrauw and Van de Voorde, determines the intersection of an $\mathbb{F}_p$-subline with an $\mathbb{F}_p$-linear set; all possibilities for the size of the intersection that are obtained in this statement, can occur (see [7]). The bound on the characteristic of the field appearing in Main Theorem 2 arises from this theorem.

Theorem 3. [7, Theorem 8] *An $\mathbb{F}_{p_0}$-linear set of rank k in* $\mathrm{PG}(n,p^t)$ *and an $\mathbb{F}_{p_0}$-subline (i.e. an $\mathbb{F}_{p_0}$-linear set of rank 2), intersect in $0,1,2,\ldots,k$ or p_0+1 points.*

The following lemma is a straightforward extension of [6, Lemma 7], where the authors proved it for $h=3$.

Lemma 1. *If B is a subset of* $\mathrm{PG}(n,p_0^h)$*, $p_0 \geq 7$, intersecting every $(n-k)$-space, $k\geq 1$, in $1 \mod p_0$ points, and Π is an $(n-k+s)$-space, $s<k$, then either*

$$|B\cap\Pi| < p_0^{hs}+p_0^{hs-1}+p_0^{hs-2}+3p_0^{hs-3}$$

or

$$|B\cap\Pi| > p_0^{hs+1}-p_0^{hs-1}-p_0^{hs-2}-3p_0^{hs-3}.$$

Furthermore, $|B| < p_0^{hk}+p_0^{hk-1}+p_0^{hk-2}+3p_0^{hk-3}$.

Proof. Let Π be an $(n-k+s)$-space of $\mathrm{PG}(n,p_0^h)$, $s\le k$, and put $B_\Pi := B\cap\Pi$. Let x_i denote the number of $(n-k)$-spaces of Π intersecting B_Π in i points. Counting the number of $(n-k)$-spaces, the number of incident pairs (P,Σ) with $P\in B_\Pi, P\in\Sigma,\Sigma$ an $(n-k)$-space, and the number of triples (P_1,P_2,Σ), with $P_1,P_2\in B_\Pi$, $P_1\neq P_2$, $P_1,P_2\in\Sigma$, Σ an $(n-k)$-space yields:

$$\sum_i x_i = \begin{bmatrix} n-k+s+1 \\ n-k+1 \end{bmatrix}_{p_0^h}, \tag{1}$$

$$\sum_i ix_i = |B_\Pi| \begin{bmatrix} n-k+s \\ n-k \end{bmatrix}_{p_0^h}, \tag{2}$$

$$\sum i(i-1)x_i = |B_\Pi|(|B_\Pi|-1) \begin{bmatrix} n-k+s-1 \\ n-k-1 \end{bmatrix}_{p_0^h}. \tag{3}$$

Since we assume that every $(n-k)$-space intersects B in $1 \mod p_0$ points, it follows that every $(n-k)$-space of Π intersect B_Π in $1 \mod p_0$ points, and hence $\sum_i(i-1)(i-1-p_0)x_i\ge 0$. Using Equations (1), (2), and (3), this yields that

$$|B_\Pi|(|B_\Pi|-1)(p_0^{hn-hk+h}-1)(p_0^{hn-hk}-1)-(p_0+1)|B_\Pi|(p_0^{hn-hk+hs}-1)(p_0^{hn-hk+h}-1)$$
$$+(p_0+1)(p_0^{hn-hk+hs+h}-1)(p_0^{hn-hk+hs}-1)\ge 0.$$

Putting $|B_\Pi| = p_0^{hs}+p_0^{hs-1}+p_0^{hs-2}+3p_0^{hs-3}$ in this inequality, with $p_0\ge 7$, gives a contradiction; putting $|B_\Pi| = p_0^{hs+1}-p_0^{hs-1}-p_0^{hs-2}-3p_0^{hs-3}$ in this inequality, with $p_0\ge 7$, gives a contradiction if $s<k$. For $s=k$, it is sufficient to note that when $|B|$ is the size of a k-space, the inequality holds, to deduce that $|B| < p_0^{hk}+p_0^{hk-1}+p_0^{hk-2}+3p_0^{hk-3}$. The statement follows. □

Let B be a subset of $\mathrm{PG}(n,p_0^h)$, $p_0\ge 7$, intersecting every $(n-k)$-space, $k\ge 1$, in $1 \mod p_0$ points. From now on, we call an $(n-k+s)$-space *small* if it meets B in less than $p_0^{hs}+p_0^{hs-1}+p_0^{hs-2}+3p_0^{hs-3}$ points, and *large* if it meets B in more than $p_0^{hs+1}-p_0^{hs-1}-p_0^{hs-2}-3p_0^{hs-3}$ points, and it follows from the previous lemma that each $(n-k+s)$-space is either small or large.

The following Lemma and its corollaries show that if all $(n-k)$-spaces meet a k-blocking set B in 1 mod p_0 points, then every subspace that intersects B, intersects it in 1 mod p_0 points.

Lemma 2. *Let B be a small minimal k-blocking set in $\mathrm{PG}(n,p_0^h)$ and let L be a line such that $1<|B\cap L|<p_0^h+1$. For all $i\in\{1,\ldots,n-k\}$ there exists an i-space π_i through L such that $B\cap\pi_i = B\cap L$.*

Proof. It follows from Theorem 1 that every subspace through L intersects $B \setminus L$ in zero or at least p points, where $p_0 = p^e$, p prime. We proceed by induction on the dimension i. The statement obviously holds for $i = 1$. Suppose there exists an i-space Π_i through L such that $\Pi_i \cap B = L \cap B$, with $i \leq n-k-1$. If there is no $(i+1)$-space intersecting B only in points of L, then the number of points of B is at least

$$|B \cap L| + p(p_0^{h(n-i-1)} + p_0^{h(n-i-2)} + \ldots + p_0^h + 1),$$

but by Lemma 1 $|B| \leq p_0^{hk} + p_0^{hk-1} + p_0^{hk-2} + p_0^{hk-3}$. If $i < n-k$ this is a contradiction. We may conclude that there exists an i-space Π_i through L such that $B \cap L = B \cap \Pi_i$, $\forall i \in \{1, \ldots, n-k\}$. □

Using Lemma 2, the following corollaries follow easily.

Corollary 3. (see also [14, Corollary 3.11]) *Every line meets a small minimal k-blocking set in $\mathrm{PG}(n, p^t)$, p prime, with exponent e in 1 mod p^e or zero points.*

Proof. Suppose the line L meets the small minimal k-blocking set in x points, where $1 \leq x \leq p^t$. By Lemma 2, the line L is contained in an $(n-k)$-space π such that $B \cap \pi = B \cap L$. Since every $(n-k)$-space meets the k-blocking set B with exponent e in 1 mod p^e points, the corollary follows. □

By considering all lines through a certain point of B in some subspace, we get the following corollary.

Corollary 4. (see also [14, Corollary 3.11]) *Every subspace meets a small minimal k-blocking set in $\mathrm{PG}(n, p^t)$, p prime, with exponent e in 1 mod p^e or zero points.*

3 On the (p_0+1)-secants to a small minimal k-blocking set

In this section, we show that Theorem 2 on planar blocking sets can be extended to a similar result on k-blocking sets in $\mathrm{PG}(n, q)$.

Lemma 3. *Let B be a small minimal k-blocking set with exponent e in $\mathrm{PG}(n, p_0^h)$, $p_0 := p^e \geq 7$, p prime, $\mathbf{n \geq 2k+1}$. The number of points, not in B, that do not lie on a secant line to B is at least*

$$(p_0^{h(n+1)} - 1)/(p_0^h + 1) - (p_0^{2hk-2} + 2p_0^{2hk-3})(p_0^h + 1) - p_0^{hk} - p_0^{hk-1} - p_0^{hk-2} - 3p_0^{hk-3},$$

and this number is larger than the number of points in $\mathrm{PG}(n-1, p_0^h)$.

Proof. By Corollary 3, the number of secant lines to B is at most $\frac{|B|(|B|-1)}{(p_0+1)p_0}$. By Lemma 1, the number of points in B is at most $p_0^{hk} + p_0^{hk-1} + p_0^{hk-2} + 3p_0^{hk-3}$, hence the number of secant lines is at most $p_0^{2hk-2} + 2p_0^{2hk-3}$. This means that the number of points on at least one secant line is at most $(p_0^{2hk-2}+2p_0^{2hk-3})(p_0^h+1)$. It follows that the number of points in $\mathrm{PG}(n,p_0^h)$, not in B, not on a secant to B is at least $(p_0^{h(n+1)}-1)/(p_0^h+1)-(p_0^{2hk-2}+2p_0^{2hk-3})(p_0^h+1)-p_0^{hk}-p_0^{hk-1}-p_0^{hk-2}-3p_0^{hk-3}$. Since we assume that $n\geq 2k+1$ and $p_0\geq 7$, the last part of the statement follows. □

We first extend Theorem 2 (i) to 1-blocking sets in $\mathrm{PG}(n,q)$.

Lemma 4. *A point of a small minimal* 1*-blocking set B with exponent e in* $\mathrm{PG}(n,p_0^h)$*, $p_0:=p^e\geq 7$, p prime, lying on a (p_0+1)-secant, lies on at least $p_0^{h-1}-4p_0^{h-2}+1$ (p_0+1)-secants.*

Proof. We proceed by induction on the dimension n. If $n=2$, by Theorem 2, the number of (p_0+1)-secants through P is at least $q/p_0-3(\kappa-1)/p_0+2$, where $|B|=q+\kappa$. By Lemma 1, κ is at most $p_0^{h-1}+p_0^{h-2}+3p_0^{h-3}$, which means that the number of (p_0+1)-secants is at least $p_0^{h-1}-4p_0^{h-2}+1$. This proves the statement for $n=2$.

Now assume $n\geq 3$. From Lemma 3 (observe that, since $n\geq 3$ and $k=1$, $n\geq 2k+1$), we know that there is a point Q, not lying on a secant line to B. Project B from the point Q onto a hyperplane through P and not through Q. It is clear that the number of (p_0+1)-secants through P to the projection of B is the number of (p_0+1)-secants through P to B. By the induction hypothesis, this number is at least $p_0^{h-1}-4p_0^{h-2}+1$. □

Lemma 5. *Let Π be an $(n-k)$-space of* $\mathrm{PG}(n,p_0^h)$*, $k>1$, $p_0\geq 7$. If Π intersects a small minimal k-blocking set B with exponent e in* $\mathrm{PG}(n,p_0^h)$*, $p_0:=p^e\geq 7$, p prime in p_0+1 points, then there are at most $3p_0^{hk-h-3}$ large $(n-k+1)$-spaces through Π.*

Proof. Suppose there are y large $(n-k+1)$-spaces through Π. A small $(n-k+1)$-space through Π meets B clearly in a small 1-blocking set, which is in this case, non-trivial and hence, by Theorem 2, has at least $p_0^h+p_0^{h-1}-p_0^{h-2}$ points.

Then the number of points in B is at least

$$y(p_0^{h+1}-p_0^{h-1}-p_0^{h-2}-3p_0^{h-3}-p_0-1)+$$
$$((p_0^{hk}-1)/(p_0^h-1)-y)(p_0^h+p_0^{h-1}-p_0^{h-2}-p_0-1)+p_0+1\ (*)$$

which is at most $p_0^{hk}+p_0^{hk-1}+p_0^{hk-2}+3p_0^{hk-3}$. This yields $y\leq 3p_0^{hk-h-3}$. □

Theorem 4. *A point of a small minimal k-blocking set B with exponent e in* $\mathrm{PG}(n,p_0^h)$*, $p_0:=p^e\geq 7$, p prime, $k>1$, lying on a (p_0+1)-secant, lies on at least $((p_0^{hk}-1)/(p_0^h-1)-3p_0^{hk-h-3})(p_0^{h-1}-4p_0^{h-2})+1$ (p_0+1)-secants.*

Proof. Let P be a point on a (p_0+1)-secant L. By Lemma 2, there is an $(n-k)$-space Π through L such that $B\cap\Pi=B\cap L$. Let Σ be a small $(n-k+1)$-space. It is clear that the space Σ meets B in a small 1-blocking set B'. Every $(n-k)$-space contained in Σ meets B' in 1 mod p_0 points. By Theorem 1 (ii), B' is a small minimal 1-blocking set in Σ. For every small $(n-k+1)$-space Σ_i through π, P is a point in Σ_i, lying on a (p_0+1)-secant in Σ_i, and hence, by Lemma 4, P lies on at least $p_0^{h-1}-4p_0^{h-2}+1$ (p_0+1)-secants to B in Σ_i. From Lemma 5, we get that the number of small $(n-k+1)$-spaces Σ_i through Π is at least $(p_0^{hk}-1)/(p_0^h-1)-3p_0^{hk-h-3}$, hence, the number of (p_0+1)-secants to B through P is at least $((p_0^{hk}-1)/(p_0^h-1)-3p_0^{hk-h-3})(p_0^{h-1}-4p_0^{h-2})+1$. □

We will now show that Theorem 2 (ii) can be extended to k-blocking sets in $\mathrm{PG}(n,q)$. We start with the case $k=1$.

Lemma 6. *Let B be a small minimal 1-blocking set with exponent e in $\mathrm{PG}(n,q)$, $q=p^t$. If for a certain line L, $|L\cap B|=p^e+1$, then $\mathbb{F}_{p^e}$ is a subfield of $\mathbb{F}_q$ and $L\cap B$ is $\mathbb{F}_{p^e}$-linear.*

Proof. We proceed by induction on n. For $n=2$, the statement follows from Theorem 2 (ii), hence, let $n>2$. Let L be a line, meeting B in p^e+1 points and let H be a hyperplane through L. A plane through L containing a point of B, not on L, contains at least p^{2e} points of B, not on L by Theorem 1 (i). If all q^{n-2} planes through L, not in H, contain an extra point of B, then $|B|\geq p^{2e}q^{n-2}$, which is larger than $p^h+p^{h-1}+p^{h-2}+3p^{h-3}$, a contradiction by Lemma 1. Let Q be a point on a plane π through L, not in H such that π meets B only in points of L. The projection of B onto H is a small minimal 1-blocking set B' in H (see Theorem 1 (iii)), for which L is a (p^e+1)-secant. The intersection $B'\cap L$ is by the induction hypothesis an $\mathbb{F}_{p^e}$-linear set. Since $B\cap L=B'\cap L$, the statement follows. □

Finally, we extend Theorem 2 (ii) to a theorem on k-blocking sets in $\mathrm{PG}(n,q)$.

Theorem 5. *Let B be a small minimal k-blocking set with exponent e in $\mathrm{PG}(n,q)$, $q=p^t$. If for a certain line L, $|L\cap B|=p^e+1$, $p^e\geq 7$, then $\mathbb{F}_{p^e}$ is a subfield of $\mathbb{F}_q$ and $L\cap B$ is $\mathbb{F}_{p^e}$-linear.*

Proof. Let L be a p^e+1-secant to B. By Lemma 5, there is at least one small $(n-k+1)$-space Π through L. Since $\Pi\cap B$ is a small 1-blocking set to B, and every $(n-k)$-space, contained in Π meets B in 1 mod p^e points, by Theorem 1 (ii), B is minimal. By Lemma 6, $L\cap B$ is an $\mathbb{F}_{p^e}$-linear set. □

4 The proof of Main Theorem 1

In this section, we will prove Main Theorem 1, that, roughly speaking, states that if we can prove the linearity for k-blocking sets in $\mathrm{PG}(n,q)$ for a certain value of n, then it is true for all n. It is clear from the definition of a k-blocking set that we can only consider k-blocking sets in $\mathrm{PG}(n,q)$ where $1\leq k\leq n-1$, and whenever we use the notation k-blocking set in $\mathrm{PG}(n,q)$, we assume that the above condition is satisfied.

> From now on, if we want to state that for the pair (k,n^*), all small minimal k-blocking sets in $\mathrm{PG}(n^*,q)$ are linear, we say that the condition (H_{k,n^*}) holds.

To prove Main Theorem 1, we need to show that if (H_{k,n^*}) holds, then $(H_{k,n})$ holds for all $n\geq k+1$. The following observation shows that we only have to deal with the case $n\geq n^*$.

Lemma 7. *If (H_{k,n^*}) holds, then $(H_{k,n})$ holds for all n with $k+1\leq n\leq n^*$.*

Proof. A small minimal k-blocking set B in $\mathrm{PG}(n,q)$, with $k+1 \le n \le n^*$, can be embedded in $\mathrm{PG}(n^*,q)$, in which it clearly is a small minimal k-blocking set. Since (H_{k,n^*}) holds, B is linear, hence, $(H_{k,n})$ holds. □

The main idea for the proof of Main Theorem 1 is to prove that all the (p_0+1)-secants through a particular point P of a k-blocking set B span a hk-dimensional space μ over $\mathbb{F}_{p_0}$, and to prove that the linear blocking set defined by μ is exactly the k-blocking set B.

Lemma 8. *Assume $(H_{k,n-1})$ and $n-1 \ge 2k$, and let B denote a small minimal k-blocking set with exponent e in $\mathrm{PG}(n,p^t)$, p prime, $p^e \ge 7$, $t \ge 2$. Let Π be a plane in $\mathrm{PG}(n,p^t)$.*

(i) There is a 3-space Σ through Π meeting B only in points of Π and containing a point Q not lying on a secant line to B **if $\mathbf{k > 2}$**.

(ii) The intersection $\Pi \cap B$, is a linear set **if $\mathbf{k > 2}$**.

Proof. Let Π be a plane of $\mathrm{PG}(n,p^t)$, $p_0 := p^e \ge 7$. By Lemma 3, there are at least

$$s := (p_0^{h(n+1)}-1)/(p_0^h+1) - (p_0^{2hk-2}+2p_0^{2hk-3})(p_0^h+1) - p_0^{hk} - p_0^{hk-1} - p_0^{hk-2} - 3p_0^{hk-3},$$

points $Q \notin \{B\}$ not lying on a secant line to B. This means that there are at least $r := (s-(p_0^{2h}+p_0^h+1))/p_0^{3h}$ 3-spaces through Π that contain a point that does not lie on a secant line to B and is not contained in B nor in Π. If all r 3-spaces contain a point Q of B that is not contained in Π, then the number of points in B is at least r. It is easy to check that this is a contradiction if $n-1 \ge 2k$, $p^e \ge 7$, and $k > 2$.

Hence, there is a 3-space Σ through Π meeting B only in points of Π and containing a point Q not lying only on a secant line to B. The projection of B from Q onto a hyperplane containing Π is a small minimal k-blocking set $\bar{B}$ in $\mathrm{PG}(n-1,q)$ (see Theorem 1(iii)), which is, by $(H_{k,n-1})$, a linear set. Now $\Pi \cap \bar{B} = \Pi \cap B$, since the space $\langle Q, \pi \rangle$ meets B only in points of Π, and hence, the set $\Pi \cap B$ is linear. □

Corollary 5. *Assume $(H_{k,n-1})$, $k > 2$, $(n-1) \ge 2k$ and let B denote a small minimal k-blocking set with exponent e in $\mathrm{PG}(n,p^t)$, p prime, $p^e \ge 7$, $t \ge 2$. The intersection of a line with B is an $\mathbb{F}_{p^e}$-linear set.*

Remark 2. The linear set $\mathcal{B}(\mu)$ does not determine the subspace μ in a unique way; by Remark 1, we can choose μ through a fixed point $S(P)$, with $P \in \mathcal{B}(\mu)$. Note that there may exist different spaces μ and μ', *through the same point of* $\mathrm{PG}(h(n+1)-1,p)$, such that $\mathcal{B}(\mu) = \mathcal{B}(\mu')$. If μ is a line, however, if we fix a point x of an element of $\mathcal{B}(\mu)$, then there is a unique line μ' through x such that $\mathcal{B}(\mu) = \mathcal{B}(\mu')$ since, in this case, μ' is the unique transversal line through x to the regulus $\mathcal{B}(\mu)$. This observation is crucial for the proof of the following lemma.

Lemma 9. *Assume $(H_{k,n-1})$, $n-1 \ge 2k$, and let B be a small minimal k-blocking set with exponent e in $\mathrm{PG}(n,p^t)$, p prime, $p_0 := p^e \ge 7$. Denote the (p_0+1)-secants through a point P of B that lies on at least one (p_0+1)-secant, by $L_1, \ldots, L_s$. Let x be a point of $\mathcal{S}(P)$ and let ℓ_i be the line through x such that $\mathcal{B}(\ell_i) = L_i \cap B$. The following statements hold:*

(i) The space $\langle \ell_1, \ldots, \ell_s\rangle$ has dimension hk.

(ii) $\mathcal{B}(\langle \ell_i, \ell_j\rangle) \subseteq B$ for $1 \leq i \neq j \leq s$.

Proof. (i) Let P be a point of B lying on a (p_0+1)-secant, and let H be a hyperplane through P. By Lemma 6, there is a point Q, not in B and not in H, not lying on a secant line to B. The projection of B from Q onto H is a small minimal k-blocking set $\bar{B}$ in $H \cong \mathrm{PG}(n-1,q)$ (Theorem 1 (iii)). By $(H_{k,n-1})$, $\bar{B}$ is a linear set. Every line meets B in 1 mod p_0 or 0 points, which implies that every line in H meets $\bar{B}$ in 1 mod p_0 or 0 points, hence, $\bar{B}$ is $\mathbb{F}_{p_0}$-linear. Take a fixed point x in $\mathcal{S}(P)$. Since $\bar{B}$ is an $\mathbb{F}_{p_0}$-linear set, there is an hk-dimensional space μ in $\mathrm{PG}(h(n+1)-1,p_0)$, through x, such that $\mathcal{B}(\mu)=\bar{B}$.

From Lemma 4, we get that the number of (p_0+1)-secants through P to B is at least $z := ((p_0^{hk}-1)/(p_0^h-1)-3p_0^{hk-h-3})(p_0^{h-1}-4p_0^{h-2})+1$, denote them by $L_1,\ldots,L_s$ and let $\ell_1,\ldots,\ell_s$ be the lines through x such that $\mathcal{B}(\ell_i)=B\cap L_i$. These lines exist by Theorem 5. Note that, by Remark 2, $\mathcal{B}(\ell_i)$ determines the line ℓ_i through x in a unique way, and that $\ell_i \neq \ell_j$ for all $i \neq j$.

We will prove that the projection of ℓ_i from $\mathcal{S}(Q)$ onto $\langle \mathcal{S}(H)\rangle$ in $\mathrm{PG}(h(n+1)-1,p_0)$ is contained in μ. Since L_1 is projected onto a (p_0+1)-secant M to $\bar{B}$ through P, there is a line m through x in $\mathrm{PG}(h(n+1)-1,p_0)$ such that $\mathcal{B}(m)=M\cap\bar{B}$. Now $\bar{B}=\mathcal{B}(\mu)$, and $|\bar{B}\cap M|=p_0+1$, hence, there is a line m' through x in μ such that $\mathcal{B}(m')=\bar{B}\cap M$. Since m is the unique transversal line through x to $M\cap\bar{B}$ (see Remark 2), $m=m'$, and m is contained in μ.

This implies that the space $W := \langle \ell_1,\ldots,\ell_s\rangle$ is contained in $\langle \mathcal{S}(Q),\mu\rangle$, hence, W has dimension at most $hk+h$. Suppose that W has dimension at least $hk+1$, then it intersects the $(h-1)$-dimensional space $\mathcal{S}(Q)$ in at least a point. But this holds for all $\mathcal{S}(Q)$ corresponding to points, not in B, such that Q does not lie on a secant line to B. This number is at least

$$(p_0^{h(n+1)}-1)/(p_0^h+1)-(p_0^{2hk-2}+2p_0^{2hk-3})(p_0^h+1)-p_0^{hk}-p_0^{hk-1}-p_0^{hk-2}-3p_0^{hk-3}$$

by Lemma 3, which is larger than the number of points in W, since W is at most $(hk+h)$-dimensional, a contradiction.

From Theorem 4, we get that W contains at least

$$(((p_0^{hk}-1)/(p_0^h-1)-3p_0^{hk-h-3})(p_0^{h-1}-4p_0^{h-2})+1)p_0+1$$

points, which is larger than $(p_0^{hk}-1)/(p_0-1)$ if $p_0 \geq 7$, hence, W is at least hk-dimensional. Since we have already shown that W is at most hk-dimensional, the statement follows.

(ii) W.l.o.g. we choose $i=1, j=2$. Let m be a line in $\langle \ell_1,\ell_2\rangle$, not through $\ell_1\cap\ell_2$. Let M be the line of $\mathrm{PG}(n,q^t)$ containing $\mathcal{B}(m)$ and let H be a hyperplane of $\mathrm{PG}(n,q^t)$ containing the plane $\langle L_1,L_2\rangle$. We claim that there exists a point Q, not in H, such that the planes $\langle Q,L_1\rangle$, $\langle Q,L_2\rangle$ and $\langle Q,M\rangle$ only contain points of B that are in H.

If $k>2$, this follows from Lemma 8(i). Now assume that $1\leq k\leq 2$. There are q^{n-2} planes through M, not in in H. Since M is at least a (p_0+1)-secant (Theorem 1 (i)), it holds that if a plane Π through M contains a point of B, that is not contained in M, then, Π contains at least p_0^2 points of B, not in M (again by Theorem 1(i)). Since $|B| \leq q^k + q^{k-1} + q^{k-2} + 3q^{k-3}$ (Lemma 1), and $n-1 \geq 2k$, there is at least one plane Π through M, not contained in H that contains only points of B that are contained in M. Now, there is one of the q^2 points in Π, say Q, that is not contained in M for which the planes $\langle Q, L_i \rangle$, $i = 1, 2$ only contain points of B on the line L_i, $i = 1, 2$, since otherwise, the number of points in B would be at least $p_0^2 q^2$, a contradiction since $k \leq 2$ and $|B| \leq q^k + q^{k-1} + q^{k-2} + 3q^{k-3}$ by Lemma 1. This proves our claim.

The projection of B from Q onto H is a small minimal k-blocking set $\bar{B}$ in $\mathrm{PG}(n, q)$ (Theorem 1 (iii)). By $(H_{k,n-1})$, $\bar{B}$ is a linear set, hence, it meets $\langle L_1, L_2 \rangle$ in a linear set. This means that there is a space π through x such that $\langle L_1, L_2 \rangle \cap B = \mathcal{B}(\pi)$. Note that, since $\langle Q, L_1 \rangle$ and $\langle Q, L_2 \rangle$ only contain points of B that are contained in H, the lines L_1 and L_2 are (p_0+1)-secants to $\bar{B}$.

Hence, the space π contains ℓ_i since $\mathcal{B}(\pi) \cap L_i = \mathcal{B}(\ell_i)$ and ℓ_i is the unique transversal line to the regulus $B \cap L_i$, $i = 1, 2$. Hence, $\mathcal{B}(\langle \ell_1, \ell_2 \rangle) \subset \bar{B}$, so $\mathcal{B}(m) \subset \bar{B}$. The plane $\langle Q, M \rangle$ only contains points of B that are on M, so $M \cap B = M \cap \bar{B}$, hence, $\mathcal{B}(m) \subset B$. Since every point of $\langle \ell_1, \ell_2 \rangle$, not on ℓ_1, ℓ_2, lies on a line m meeting ℓ_1 and ℓ_2 in different points, $\mathcal{B}(\langle \ell_1, \ell_2 \rangle) \subseteq B$. □

Proof of Main Theorem 1.

Let B be a small minimal k-blocking set with exponent e in $\mathrm{PG}(n, p^t)$, p prime, $p_0 = p^e \geq 7$ and assume that $(H_{k,n-1})$ holds with $n-1 \geq 2k$. Let P be a point of B, lying on a (p_0+1)-secant. By Theorem 4, there are at least $((p_0^{hk}-1)/(p_0^h-1) - 3p_0^{hk-h-3})(p_0^{h-1} - 4p_0^{h-2}) + 1$ (p_0+1)-secants $L_1 \ldots, L_s$ through P, and by Lemma 9, the corresponding lines $\ell_1, \ldots, \ell_s$ in $\mathrm{PG}(h(n+1)-1, p_0)$, with $\mathcal{B}(\ell_i) = B \cap L_i$, ℓ_i through a fixed point x of $\mathcal{S}(P)$, span an hk-dimensional space W. Suppose that $\mathcal{B}(W) \not\subseteq B$, and let w be a point of W for which $\mathcal{B}(w) \notin B$. Since the number of points lying on one of the lines of the set $\{\ell_1, \ldots, \ell_s\}$, is at least $(((p_0^{hk}-1)/(p_0^h-1) - 3p_0^{hk-h-3})(p_0^{h-1} - 4p_0^{h-2}) + 1)p_0 + 1$, at least one of the $(p_0^{hk}-1)/(p_0-1)$ lines through w, say m, contains two points lying on one of the lines of the set $\{\ell_1, \ldots, \ell_s\}$. By Lemma 9 (b), $\mathcal{B}(m)$ is contained in B, a contradiction since $\mathcal{B}(w) \in \mathcal{B}(m)$, and $\mathcal{B}(w) \notin B$.

Hence, $\mathcal{B}(W) \subseteq B$, and since $\mathcal{B}(W)$ is a small minimal linear k-blocking set $\mathrm{PG}(n, p^t)$, contained in the minimal k-blocking set B, B equals the linear set $\mathcal{B}(W)$. Hence, we have shown that if $(H_{k,n-1})$ holds, with $n-1 \geq 2k$, then $(H_{k,n})$ holds, and repeating this argument shows that if (H_{k,n^*}) holds for some n^*, then $(H_{k,n})$ holds for all $n \geq n^*$. Since Lemma 7 shows the desired property for all n with $k+1 \leq n \leq n^*$, the statement follows. □

5 The proof of Main Theorem 2

In this section, we will prove Main Theorem 2, stating that, if all small minimal 1-blocking sets in $\mathrm{PG}(n, p_0^h)$ are linear, then all small minimal k-blocking sets in $\mathrm{PG}(n, p_0^h)$, are linear, provided a condition on p_0 and h holds.

We proved in Lemma 1 that a subspace meets the small minimal k-blocking set B in either in a 'small' number, or in a 'large' number of points. To simplify the terminology, we call a $(n-k+s)$-space Π, $s \leq k$, for which $|B \cap \Pi| < p_0^{hs} + p_0^{hs-1} + p_0^{hs-2} + 3p_0^{hs-3}$ points, a *small* $(n-k+s)$-space. An $(n-k+s)$-space which is not small is called *large*.

Lemma 10. *Let Π be an $(n-k)$-space of $\mathrm{PG}(n, p_0^h)$ and let B be a small minimal k-blocking set with exponent e in $\mathrm{PG}(n, p^t)$, p prime, $p_0 := p^e \geq 7$, $k > 1$.*

(i) If $B \cap \Pi$ is a point, then there are at most $p_0^{hk-h-2} + 4p_0^{hk-h-3} - 1$ large $(n-k+1)$-spaces through Π.

(ii) If Π intersects B in $p_0 + 1$ points, then there are at most $3p_0^{hk-h-3}$ large $(n-k+1)$-spaces through Π.

Proof. (i) A small $(n-k+1)$-space through Π meets B in at least $p_0^h + 1$ points. Suppose there are y large $(n-k+1)$-spaces through Π. Then the number of points in B is at least

$$y(p_0^{h+1} - p_0^{h-1} - p_0^{h-2} - 3p_0^{h-3} - 1) + ((p_0^{hk} - 1)/(p_0^h - 1) - y)p_0^h + 1$$

which is at most $p_0^{hk} + p_0^{hk-1} + p_0^{hk-2} + 3p_0^{hk-3}$. This yields $y \leq p_0^{hk-h-2} + 4p_0^{hk-h-3} - 1$.

(ii) Suppose there are y large $(n-k+1)$-spaces through Π. A small $(n-k+1)$-space through Π meets B in a linear 1-blocking set, which is in this case, non-trivial and hence, by Theorem 2, has at least $p_0^h + p_0^{h-1} - p_0^{h-2}$ points.

Then the number of points in B is at least

$$y(p_0^{h+1} - p_0^{h-1} - p_0^{h-2} - 3p_0^{h-3} - p_0 - 1) +$$

$$((p_0^{hk} - 1)/(p_0^h - 1) - y)(p_0^h + p_0^{h-1} - p_0^{h-2} - p_0 - 1) + p_0 + 1 \; (*)$$

which is at most $p_0^{hk} + p_0^{hk-1} + p_0^{hk-2} + 3p_0^{hk-3}$. This yields $y \leq 3p_0^{hk-h-3}$. □

Lemma 11. *If B is a non-trivial small minimal k-blocking set with exponent e in $\mathrm{PG}(n, p^t)$, p prime, $p_0 := p^e \geq 7$, $k > 1$, then there exist a point $P \in B$, a tangent $(n-k)$-space Π at the point P and small $(n-k+1)$-spaces H_i, through Π, such that there is a $(p_0 + 1)$-secant through P in H_i, $i = 1, \ldots, p_0^{hk-h} - 5p_0^{hk-h-1}$.*

Proof. Let L be a $(p_0 + 1)$-secant to B and let P be a point of $B \cap L$. Lemma 2 shows that there is an $(n-k)$-space Π_L such that $B \cap \Pi_L = B \cap L$. By Theorem 4, P lies on $((p_0^{hk} - 1)/(p_0^h - 1) - 3p_0^{hk-h-3})(p_0^{h-1} - 4p_0^{h-2}) + 1$ other $(p_0 + 1)$-secants. By Lemma 10 (ii), there are at least $(p_0^{hk} - 1)/(p_0^h - 1) - 3p_0^{hk-h-3}$ small hyperplanes through Π_L, which each contain at least $p_0^h + p_0^{h-1} - p_0^{h-2} - p_0 - 1$ points of B not on L. Since $|B| < p_0^{hk} + p_0^{hk-1} + p_0^{hk-2} + 3p_0^{hk-3}$ (see Lemma 2), there are less than $2p_0^{hk-1}$ points of B left in large $(n-k+1)$-spaces through Π_L. Hence, P lies on less than $2p_0^{hk-h-1}$ lines that are completely contained in B.

Since B is minimal, P lies on a tangent $(n-k)$-space Π to B. There are at most $p_0^{hk-h-2} + 4p_0^{hk-h-3} - 1$ large $(n-k+1)$-spaces through Π (Lemma 10 (i)). Moreover, since at least $\frac{p_0^{hk}-1}{p_0^h-1} - (p_0^{hk-h-2} + 4p_0^{hk-h-3} - 1) - (2p_0^{hk-h-1})$ $(n-k+1)$-spaces through Π

contain at least $p_0^h+p_0^{h-1}-p_0^{h-2}$ points of B, and at most $2p_0^{hk-h-1}$ of the small $(n-k+1)$-spaces through Π contain exactly p_0^h+1 points of B, there are at most p_0^{hk-2} points of B contained in large $(n-k+1)$-spaces through Π. Hence, P lies on at most p_0^{hk-3} (p_0+1)-secants of the large $(n-k+1)$-spaces through Π. This implies that there are at least $(((p_0^{hk}-1)/(p_0^h-1)-3p_0^{hk-h-3})(p_0^{h-1}-4p_0^{h-2})+1)-p_0^{hk-3}$ (p_0+1)-secants through P left in small $(n-k+1)$-spaces through Π. Since in a small $(n-k+1)$-space through Π, there can lie at most $(p_0^h-1)/(p_0-1)$ (p_0+1)-secants through P, this implies that there are at least $p_0^{hk-h}-5p_0^{hk-h-1}$ $(n-k+1)$-spaces H_i through Π such that P lies on a (p_0+1)-secant in H_i. □

We continue with the following hypothesis:

(H) A small minimal j-blocking set in $\mathrm{PG}(n,q)$, $1\le j<k$ is linear.

Lemma 12. *Let B be a non-trivial small minimal k-blocking set with exponent e in $\mathrm{PG}(n,p^t)$, p prime, $p_0:=p^e\ge 7$, $k>1$. If we assume (H), then the following statements hold.*

(i) A small $(n-k+s)$-dimensional space Π of $\mathrm{PG}(n,p^t)$, $s<k$, intersects B in a linear set and $|\Pi\cap B|\le(p_0^{hs+1}-1)/(p_0-1)$.

(ii) Let L be a (p_0+1)-secant to B and let S be a point of B, not on L. There exists a small $(n-2)$-space through L, skew to S.

(iii) A line intersects B in a linear set.

(iv) Let Π be a small $(n-2)$-space containing a (p_0+1)-secant to B. Then the number of large $(n-1)$-spaces through Π is at most $4p_0^{h-3}$.

Proof. (i) It is clear that an $(n-k+s)$-space Π meets B in a small s-blocking set B'. Every $(n-k)$-space contained in Π meets B' in 1 mod p_0 points, hence, by Theorem 1 (ii), B' is a small minimal s-blocking set in $\mathrm{PG}(n-k+s,p_0^h)$, which is, by the hypothesis (H), $\mathbb{F}_{p_0}$-linear. It follows that $|B'|\le(p_0^{hs+1}-1)/(p_0-1)$.

(ii) Lemma 2 shows that there is an $(n-k)$-space Π_{n-k} through L, such that $B\cap L=B\cap\Pi_{n-k}$. By Lemma 1, an $(n-k+1)$-space through Π_{n-k} contains at most $(p_0^{h+1}-1)/(p_0-1)$ or at least $p_0^{h+1}-p_0^{h-1}-p_0^{h-2}-3p_0^{h-3}$ points of B. If all $(n-k+1)$-spaces through Π_{n-k} (except possibly $\langle\Pi_{n-k},S\rangle$) would be large, the number of points in B would be at least $((p_0^{hk}-1)/(p_0^h-1)-1)(p_0^{h+1}-p_0^{h-1}-p_0^{h-2}-3p_0^{h-3}-p_0^h)$, which is larger than $p_0^{hk}+p_0^{hk-1}+p_0^{hk-2}+3p_0^{hk-3}$, a contradiction. Hence, there is a small $(n-k+1)$-space through Π_{n-k}.

Suppose, by induction, that there exists a small $(n-k+s)$-space Π_{n-k+s} through L, skew to S and suppose all $(p_0^{h(k-s)}-1)/(p_0^h-1)-1$ $(n-k+s)$-spaces through $\Pi_{n-k+s-1}$, different from $\langle\Pi_{n-k+s},S\rangle$ are large. Then the number of points in B is larger than $p_0^{hk}+p_0^{hk-1}+p_0^{hk-2}+3p_0^{hk-3}$ if $s\le k-2$, a contradiction. We conclude that there exists a small $(n-2)$-space through L, skew to S.

(iii) Let L be a line, with $0 < |L \cap B| < p^t + 1$, otherwise the statement trivially holds. The previous part of this lemma shows that L is contained in a small $(n-k+1)$-space, which has, by the first part of this lemma, a linear intersection with B. Hence, $B \cap L$ is a linear set.

(iv) A small $(n-1)$-space through Π meets B in at least $p_0^{hk-h} + p^{hk-h-1} - p^{hk-h-2}$ points (see Corollary 2) and a small $(n-2)$-space contains at most $(p_0^{hk-2h+1} - 1)/(p_0 - 1)$ points by the first part of this lemma. By Lemma 1, a large $(n-1)$-space through Π contains at least $p^{hk-h+1} - p^{hk-h-1} - p^{hk-h-2} - 3p^{hk-h-3}$ points of B. Suppose there are y large $(n-1)$-spaces through Π. Then the number of points in B is at least

$$y(p_0^{hk-h+1} - p_0^{hk-h-1} - p_0^{hk-h-2} - 3p_0^{hk-h-3} - (p_0^{hk-2h+1} - 1)/(p_0 - 1))+$$

$$(p_0^h + 1 - y)(p_0^{hk-h} + p^{hk-h-1} - p^{hk-h-2} - (p_0^{hk-h+1} - 1)/(p_0 - 1)) + (p_0^{hk-2h+1} - 1)/(p_0 - 1)$$

which is at most $p_0^{hk} + p_0^{hk-1} + p_0^{hk-2} + 3p_0^{hk-3}$. This yields $y \leq 4p_0^{h-3}$. □

Lemma 13. *Assume (H). Let B be a non-trivial small minimal k-blocking set with exponent e in $\mathrm{PG}(n, p^t)$, p prime, $p_0 := p^e \geq 7$ and let P be a point of B, and let Π be a tangent $(n-k)$-space to B through P. Let H_1 and H_2 be two $(n-k+1)$-spaces through Π for which $B \cap H_i = \mathcal{B}(\pi_i)$, for some h-space π_i through a point $x \in \mathcal{S}(P)$, such that P lies on a (p_0+1)-secant in H_i, $i = 1, 2$. Then $\mathcal{B}(\langle \pi_1, \pi_2 \rangle) \subset B$.*

Proof. Let L be a (p_0+1)-secant through P in H_1 and let ℓ be the line in π through x such that $\langle \mathcal{B}(\ell) \rangle = L$. Let s be a point of π_2. By Lemma 12 (ii), there is a small $(n-2)$-space Π_{n-2} through L, skew to $\mathcal{B}(s)$. There are at least $p_0^{h-1} - 4p_0^{h-2}$ (p_0+1)-secants through P, of which at least $p_0^{h-1} - 4p_0^{h-2} - (p_0^{h-1} - 1)/(p_0 - 1)$ span an $(n-1)$-space together with Π_{n-2}. By Lemma 12 (iv), there are at most $4p_0^{h-3}$ large spaces through Π_{n-2}, so at least $p_0^{h-1} - 4p_0^{h-2} - (p_0^{h-1} - 1)/(p_0 - 1) - 4p_0^{h-3}$ of the (p_0+1)-secants through P have a transversal line ℓ_k, for which $\mathcal{B}(\langle \ell, \ell_k \rangle) \subset B$. This gives in total at least $p_0^{h+1} - 6p_0^h$ points Q in $\langle \ell, \pi_2 \rangle$ for which $\mathcal{B}(Q) \subset B$, denote this pointset by G. This means that every point t of $\langle \ell, \pi_2 \rangle$ lies on a line m with at least $p_0 - 5$ points of G. Since $\langle \mathcal{B}(m) \rangle$ either is contained in B, or it meets B in a linear set of rank at most h (see Lemma 12 (iii)), and $p_0 - 5 > h$, again by Theorem 3, $\mathcal{B}(m) \subset B$ by Theorem 3, and hence, $\mathcal{B}(t) \subset B$.

Hence, for all (p_0+1)-secants $\mathcal{B}(\ell)$, with ℓ through x, in H_1, $\mathcal{B}(\langle \ell, \pi_2 \rangle) \subset B$. This shows that there are at least $(p_0^{h-1} - 4p_0^{h-2})p_0^{h+1} + (p_0^{h+1} - 1)/(p_0 - 1)$ points Q in the $2h$-space $\langle \pi_1, \pi_2 \rangle$ such that $\mathcal{B}(Q) \subset B$. Every point t of $\langle \pi_1, \pi_2 \rangle$ lies on a line m with at least $p_0 - 5$ points of G. Again, since $p_0 - 5 > h$, by Theorem 3, $\mathcal{B}(m) \subset B$ and hence, $\mathcal{B}(t) \subset B$. It follows that $\mathcal{B}(\langle \pi_1, \pi_2 \rangle) \subseteq B$.

□

Proof of Main Theorem 2. Let B be a non-trivial small minimal k-blocking set with exponent e in $\mathrm{PG}(n, p^t)$, p prime, $p_0 := p^e \geq 7$. We will show that, assuming that all small minimal 1-blocking sets with exponent e in $\mathrm{PG}(n, p^t)$, p prime, $p_0 := p^e \geq 7$, are $\mathbb{F}_{p_0}$-linear, B is $\mathbb{F}_{p_0}$-linear. By induction, we may assume (H) holds. If B is a k-space, then B is $\mathbb{F}_{p_0}$-linear. If B is a non-trivial small minimal k-blocking set, Lemma 11 shows that there exists a point P of B, a tangent $(n-k)$-space Π at the point P and at least $p_0^{hk-h} - 5p_0^{hk-h-1}$ $(n-k+1)$-spaces H_i through Π for which $B \cap H_i$ is small and linear, where P lies on at least one (p_0+1)-secant of $B \cap H_i$, $i = 1, \ldots, s$, $s \geq p_0^{hk-h} - 5p_0^{hk-h-1}$. Let $B \cap H_i = \mathcal{B}(\pi_i), i = 1, \ldots, s$, with π_i an h-dimensional space in $\mathrm{PG}(h(n+1)-1, p_0)$, where $x \in \pi_i$, with $x \in \mathcal{S}(P)$.

Lemma 13 shows that $\mathcal{B}(\langle \pi_i, \pi_j \rangle) \subseteq B$, $0 \leq i \neq j \leq s$.

If $k = 2$, the set $\mathcal{B}(\langle \pi_1, \pi_2 \rangle)$ corresponds to a linear 2-blocking set B' in $\mathrm{PG}(n, p_0^h)$. Since B is minimal, $B = B'$, and the Theorem is proven.

Let $k > 2$. Denote the $(n-k+1)$-spaces through Π, different from H_i, by $K_j, j = 1, \ldots, z$. It follows from Lemma 11 that $z \leq 5p_0^{hk-h-1} + (p_0^{hk-h} - 1)/(p_0 - 1) \leq 6p_0^{hk-h-1}$. There are at least $(p_0^{hk-h} - 5p_0^{hk-h-1} - 1)/p_0^h$ different $(n-k+2)$-spaces $\langle H_1, H_j \rangle$, $1 < j \leq s$. If all $(n-k+2)$-spaces $\langle H_1, H_j \rangle$, contain at least $10p_0^{h-1}$ of the spaces K_i, then $z \geq 10p_0^{h-1}(p_0^{hk-h} - 5p_0^{hk-h-1} - 1)/p_0^h > 6p_0^{hk-h-1}$, a contradiction if $p_0 > h + 10$. Let $\langle H_1, H_2 \rangle$ be an $(n-k+2)$-spaces containing less than $10p_0^{h-1}$ spaces K_i.

Suppose by induction that for any $1 < i < k$, there is an $(n-k+i)$-space $\langle H_1, H_2, \ldots, H_i \rangle$ containing at most $10p_0^{hi-h-1}$ of the spaces K_i such that $\mathcal{B}(\langle \pi_1, \ldots, \pi_i \rangle) \subseteq B$.

There are at least

$$\frac{p_0^{hk-h} - 6p_0^{hk-h-1} - (p_0^{hi} - 1)/(p_0^h - 1)}{p_0^h}$$

different $(n-k+i+1)$-spaces $\langle H_1, H_2, \ldots, H_i, H_r \rangle$, $H_r \not\subseteq \langle H_1, H_2, \ldots, H_i \rangle$. If all of these contain at least $10p_0^{hi-1}$ of the spaces K_i, then $z \geq 6p_0^{hk-h-1}$, a contradiction. Let $\langle H_1, \ldots, H_{i+1} \rangle$ be an $(n-k+i+1)$-space containing less than $10p_0^{hi-1}$ spaces K_i. We still need to prove that $\mathcal{B}(\langle \pi_1, \ldots, \pi_{i+1} \rangle) \subseteq B$. Since $\mathcal{B}(\langle \pi_{i+1}, \pi \rangle) \subseteq B$, with π an h-space in $\langle \pi_1, \ldots, \pi_i \rangle$ for which $\mathcal{B}(\pi)$ is not contained in one of the spaces K_i, there are at most $10p_0^{hi-h-1}$ $2h$-dimensional spaces $\langle \pi_{i+1}, \mu \rangle$ for which $\mathcal{B}(\langle \pi_{i+1}, \mu \rangle)$ is not necessarily contained in B, giving rise to at most $v := 10p_0^{hi-h-1}(p_0^{2h+1} - 1)/(p_0 - 1)$ points t for which $\mathcal{B}(t)$ is not necessarily contained in B. Let u be a point of such a space $\langle \pi_{i+1}, \mu \rangle$, and suppose that $\mathcal{B}(u) \notin B$. If each of the $(p_0^{hi+h} - 1)/(p_0 - 1)$ lines through u in $\langle \pi_1, \ldots, \pi_{i+1} \rangle$ contains at least 10 of the points t for which $\mathcal{B}(t)$ is not in B, then there are more than v such points t, a contradiction. Hence, there is a line n through u for which for at least $p_0 - 10$ points $v \in n$, $\mathcal{B}(v) \in B$. Every line L meets B in a linear set (see Lemma 12 (iii)), and if this linear set has rank at least $h+1$, then L is completely contained in B. This implies that $\langle \mathcal{B}(n) \rangle \cap B$ has rank at most h, and that the subline $\mathcal{B}(n)$ contains at least $p_0 - 10$ points of the linear set $\langle \mathcal{B}(n) \rangle \cap B$. Since $p_0 - 10 > h$, by Theorem 3, $\mathcal{B}(n)$ is contained in $\langle \mathcal{B}(n) \rangle \cap B$, so $\mathcal{B}(u) \subset B$, a contradiction.

This implies that $\mathcal{B}(\langle \pi_1, \ldots, \pi_{i+1} \rangle) \subseteq B$.

Since $\mathcal{B}(\langle \pi_1, \ldots, \pi_k \rangle) \subseteq B$, and $\mathcal{B}(\langle \pi_1, \ldots, \pi_k \rangle)$ corresponds to a linear k-blocking set B' in $\mathrm{PG}(n, p_0^h)$ contained in the minimal k-blocking set B, $B = B'$ and hence, B is $\mathbb{F}_{p_0}$-linear. □

Acknowledgment: This research was done while the author was visiting the discrete algebra and geometry group (DAM) at Eindhoven University of Technology, the Netherlands. The author thanks A. Blokhuis and all other members of this group for their hospitality during her stay.

References

[1] A. Blokhuis. On the size of a blocking set in PG$(2, p)$. *Combinatorica* **14 (1)** (1994), 111-114.

[2] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Combin. Theory Ser. A* **86 (1)** (1999), 187–196.

[3] M. Bokler. Minimal blocking sets in projective spaces of square order. *Des. Codes Cryptogr.* **24 (2)** (2001), 131–144.

[4] N. Harrach and K. Metsch. Small point sets of PG(n, q^3) intersecting each k-subspace in $1 \mod q$ points. Submitted to *Des. Codes Cryptogr.*

[5] N. Harrach, K. Metsch, T. Szőnyi, and Zs. Weiner. Small point sets of PG(n, p^{3h}) intersecting each line in 1 mod p^h points. *J. Geom.*, to appear.

[6] M. Lavrauw, L. Storme, and G. Van de Voorde. A proof for the linearity conjecture for k-blocking sets in PG(n, p^3), p prime. Submitted to *J. Combin. Theory, Ser. A.*

[7] M. Lavrauw and G. Van de Voorde. On linear sets on a projective line. *Des. Codes Cryptogr.* **56 (2-3)** (2010), 89–104,

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

[9] P. Polito and O. Polverino. On small blocking sets. *Combinatorica* **18 (1)** (1998), 133–137.

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

[11] L. Storme and P. Sziklai. Linear pointsets and Rédei type k -blocking sets in PG(n, q).*J. Algebraic Combin.* **14 (3)** (2001), 221–228.

[12] L. Storme and Zs. Weiner. On 1-blocking sets in PG(n, q), $n \geq 3$. *Des. Codes Cryptogr.* **21 (1–3)** (2000), 235–251.

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

[14] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory, Ser. A* **95 (1)** (2001), 88–101.

[15] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory, Ser. A*, **115 (7)** (2008), 1167–1182.

[16] Zs. Weiner. Small point sets of PG$(n, \sqrt{q})$ intersecting every k-space in 1 modulo $\sqrt{q}$ points. *Innov. Incidence Geom.* **1** (2005), 171–180.