A proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime

M. Lavrauw * L. Storme G. Van de Voorde *

Abstract

In this paper, we show that a small minimal k-blocking set in $\mathrm{PG}(n, q^3)$, $q = p^h$, $h \geq 1$, p prime, $p \geq 7$, intersecting every $(n-k)$-space in $1 \pmod q$ points, is linear. As a corollary, this result shows that all small minimal k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime, $p \geq 7$, are $\mathbb{F}_p$-linear, proving the linearity conjecture (see [9]) in the case $\mathrm{PG}(n, p^3)$, p prime, $p \geq 7$.

1 Introduction and preliminaries

Throughout this paper, $q = p^h$, p prime, $h \geq 1$, and $\mathrm{PG}(n, q)$ denotes the n-dimensional projective space over the finite field $\mathbb{F}_q$ of order q. A *k-blocking set* B in $\mathrm{PG}(n, q)$ is a set of points such that any $(n-k)$-dimensional subspace intersects B. A k-blocking set B is called *trivial* when a k-dimensional subspace is contained in B. If an $(n-k)$-dimensional space contains exactly one point of a k-blocking set B in $\mathrm{PG}(n, q)$, it is called a *tangent $(n-k)$-space* to B. A k-blocking set B is called *minimal* when no proper subset of B is a k-blocking set. A k-blocking set B is called *small* when $|B| < 3(q^k + 1)/2$.

Linear blocking sets were first introduced by Lunardon [5] and can be defined in several equivalent ways.

In this paper, we follow the approach described in [3]. In order to define a linear k-blocking set in this way, we introduce the notion of a Desarguesian spread. Suppose $q = q_0^t$, with $t \geq 1$. By "field reduction", the points of $\mathrm{PG}(n, q)$ correspond to $(t-1)$-dimensional subspaces of $\mathrm{PG}((n+1)t-1, q_0)$, since a point of $\mathrm{PG}(n, q)$ is a 1-dimensional vector space over $\mathbb{F}_q$, and so a t-dimensional vector space over $\mathbb{F}_{q_0}$. In this way, we obtain a partition $\mathcal{D}$ of the point set of $\mathrm{PG}((n+1)t-1, q_0)$ by $(t-1)$-dimensional subspaces. In general, a partition of the point set of a projective space by subspaces of a given dimension d is called a *spread*, or a *d-spread* if we want to specify the dimension. The spread obtained by field reduction is called a *Desarguesian spread*. Note that the Desarguesian spread satisfies the property that each subspace spanned by spread elements is partitioned by spread elements.

Let $\mathcal{D}$ be the Desarguesian $(t-1)$-spread of $\mathrm{PG}((n+1)t-1, q_0)$. If U is a subset of $\mathrm{PG}((n+1)t-1, q_0)$, then we define $\mathcal{B}(U) := \{R \in \mathcal{D} || U \cap R \neq \emptyset\}$, and we identify the elements of $\mathcal{B}(U)$ with the corresponding points of $\mathrm{PG}(n, q_0^t)$. If U is a subspace of $\mathrm{PG}((n+1)t-1, q_0)$, then we call $\mathcal{B}(U)$ a *linear set* or an *$\mathbb{F}_{q_0}$-linear*

*This author's research was supported by the Fund for Scientific Research - Flanders (FWO)

set if we want to specify the underlying field. Note that through every point in $\mathcal{B}(U)$, there is a subspace U' such that $\mathcal{B}(U') = \mathcal{B}(U)$ since the elementwise stabiliser of the Desarguesian spread $\mathcal{D}$ acts transitively on the points of a spread element of $\mathcal{D}$. If U intersects the elements of $\mathcal{D}$ in at most a point, i.e. $|\mathcal{B}(U)|$ is maximal, then we say that U is *scattered* with respect to $\mathcal{D}$; in this case $\mathcal{B}(U)$ is called a *scattered linear set*. We denote the element of $\mathcal{D}$ corresponding to a point P of $\mathrm{PG}(n, q_0^t)$ by $\mathcal{S}(P)$. If U is a subset of $\mathrm{PG}(n, q)$, then we define $\mathcal{S}(U) := \{\mathcal{S}(P) || P \in U\}$. Analogously to the correspondence between the points of $\mathrm{PG}(n, q_0^t)$, and the elements $\mathcal{D}$, we obtain the correspondence between the lines of $\mathrm{PG}(n, q)$ and the $(2t-1)$-dimensional subspaces of $\mathrm{PG}((n+1)t-1, q_0)$ spanned by two elements of $\mathcal{D}$, and in general, we obtain the correspondence between the $(n-k)$-spaces of $\mathrm{PG}(n, q)$ and the $((n-k+1)t-1)$-dimensional subspaces of $\mathrm{PG}((n+1)t-1, q_0)$ spanned by $n-k+1$ elements of $\mathcal{D}$. With this in mind, it is clear that any tk-dimensional subspace U of $\mathrm{PG}(t(n+1)-1, q_0)$ defines a k-blocking set $\mathcal{B}(U)$ in $\mathrm{PG}(n, q)$. A (k-)blocking set constructed in this way is called a *linear (k-)blocking set*, or an $\mathbb{F}_{q_0}$*-linear (k-)blocking set* if we want to specify the underlying field.

By far the most challenging problem concerning blocking sets is the so-called *linearity conjecture*. Since 1998, it has been conjectured by many mathematicians working in the field. The conjecture was explicitly stated in the literature by Sziklai in [9].

(LC) *All small minimal k-blocking sets in* $\mathrm{PG}(n, q)$ *are linear.*

Various instances of the conjecture have been proved; for an overview we refer to [9]. In this paper, we prove the following main theorem:

Theorem 1. *A small minimal k-blocking set in* $\mathrm{PG}(n, q^3)$*, $q = p^h$, p prime, $h \geq 1$, $p \geq 7$, intersecting every $(n-k)$-space in* $1 \pmod q$ *points is linear.*

This theorem was proven independently in [1] and [2]. As a corollary, we prove the linearity conjecture for small minimal k-blocking sets in $\mathrm{PG}(n, p^3)$, $p \geq 7$.

Corollary 2. *A small minimal 1-blocking set in* $\mathrm{PG}(n, p^3)$*, p prime, $p \geq 7$, is* $\mathbb{F}_p$*-linear.*

1.1 Known characterisation results

In this section we mention a few results, that we will rely on in the sequel of this paper. First of all, observe that a subspace intersects a linear set of $\mathrm{PG}(n, p^h)$ in $1 \pmod p$ or zero points. The following result of Szőnyi and Weiner shows that this property holds for all small minimal blocking sets.

Result 3. [10, Theorem 2.7] *If B is a small minimal k-blocking set of* $\mathrm{PG}(n, q)$*, $p > 2$, then every subspace intersects B in* $1 \pmod p$ *or zero points.*

Result 3 answers the linearity conjecture in the affirmative for $\mathrm{PG}(n, p)$. For $\mathrm{PG}(n, p^2)$, the linearity conjecture was proved by Weiner (see [11]). For 1-blocking sets in $\mathrm{PG}(n, q^3)$, we have the following theorem of Polverino ($n = 2$) and Storme and Weiner ($n \geq 3$).

Result 4. [7, 8] *A minimal 1-blocking set in* $\mathrm{PG}(n, q^3)$*, $q = p^h$, $h \geq 1$, p prime, $p \geq 7$, $n \geq 2$, of size at most $q^3 + q^2 + q + 1$, is linear.*

Remark 5. *From the results of [7], we also get that if a non-trivial minimal 1-blocking set B of size at most q^3+q^2+q+1 does not contain a $(q\sqrt{q}+1)$-secant, every point of B which lies on at least one $(q+1)$-secant to B, lies on at least q^2 $(q+1)$-secants to B.*

In Theorem 10, we show that Result 4 implies the linearity conjecture for small minimal 1-blocking sets in $\mathrm{PG}(n,q^3)$, $p \geq 7$, that intersect every hyperplane in $1 \pmod q$ points.

The following result by Szőnyi and Weiner gives a sufficient condition for a blocking set to be minimal.

Result 6. [10, Lemma 3.1] *Let B be a k-blocking set of $\mathrm{PG}(n,q)$, and suppose that $|B| \leq 2q^k$. If each $(n-k)$-dimensional subspace of $\mathrm{PG}(n,q)$ intersects B in $1 \pmod p$ points, then B is minimal.*

1.2 The intersection of a subline and an $\mathbb{F}_q$-linear set

The possibilities for an $\mathbb{F}_q$-linear set of $\mathrm{PG}(1,q^3)$, other than the empty set, a point, and the set $\mathrm{PG}(1,q^3)$ itself are the following: a subline $\mathrm{PG}(1,q)$ of $\mathrm{PG}(1,q^3)$, corresponding to a line of $\mathrm{PG}(5,q)$ not contained in an element of $\mathcal{D}$; a set of q^2+1 points of $\mathrm{PG}(1,q^3)$, corresponding to a plane of $\mathrm{PG}(5,q)$ that intersects an element of $\mathcal{D}$ in a line; a set of q^2+q+1 points of $\mathrm{PG}(1,q^3)$, corresponding to a plane of $\mathrm{PG}(5,q)$ that is scattered w.r.t. $\mathcal{D}$.

The following results describe the possibilities for the intersection of a subline with an $\mathbb{F}_q$-linear set in $\mathrm{PG}(1,q^3)$, and will play an important role in this paper.

Result 7. [4] *A subline isomorphic to $\mathrm{PG}(1,q)$ intersects an $\mathbb{F}_q$-linear set of $\mathrm{PG}(1,q^3)$ in $0,1,2,3,$ or $q+1$ points.*

Result 8. [6, Lemma 4.4, 4.5, 4.6] *Let q be a square. A subline $\mathrm{PG}(1,q)$ and a Baer subline $\mathrm{PG}(1,q\sqrt{q})$ of $\mathrm{PG}(1,q^3)$ share at most a subline $\mathrm{PG}(1,\sqrt{q})$. A Baer subline $\mathrm{PG}(1,q\sqrt{q})$ and an $\mathbb{F}_q$-linear set of q^2+1 or q^2+q+1 points in $\mathrm{PG}(1,q^3)$ share at most $q+\sqrt{q}+1$ points.*

2 Some bounds and the case $k=1$

The Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ denotes the number of $(k-1)$-subspaces in $\mathrm{PG}(n-1,q)$, i.e.,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Lemma 9. *If B is a subset of $\mathrm{PG}(n,q^3)$, $q \geq 7$, intersecting every $(n-k)$-space, $k \geq 1$, in $1 \pmod q$ points, and π is an $(n-k+s)$-space, $s \leq k$, then either*

$$|B \cap \pi| < q^{3s}+q^{3s-1}+q^{3s-2}+3q^{3s-3}$$

or

$$|B \cap \pi| > q^{3s+1}-q^{3s-1}-q^{3s-2}-3q^{3s-3}.$$

Proof. Let π be an $(n-k+s)$-space of $\mathrm{PG}(n,q^3)$, 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:

$$\sum_i x_i = \begin{bmatrix} n-k+s+1 \\ n-k+1 \end{bmatrix}_{q^3}, \quad (1)$$

$$\sum_i ix_i = |B_\pi| \begin{bmatrix} n-k+s \\ n-k \end{bmatrix}_{q^3}, \quad (2)$$

$$\sum i(i-1)x_i = |B_\pi|(|B_\pi|-1) \begin{bmatrix} n-k+s-1 \\ n-k-1 \end{bmatrix}_{q^3}. \quad (3)$$

Since we assume that every $(n-k)$-space intersects B in $1 \pmod q$ points, it follows that every $(n-k)$-space of π intersects B_π in $1 \pmod q$ points, and hence $\sum_i (i-1)(i-1-q)x_i \geq 0$. Using Equations (1), (2), and (3), this yields that

$$|B_\pi|(|B_\pi|-1)(q^{3n-3k}-1)(q^{3n-3k+3}-1)-(q+1)|B_\pi|(q^{3n-3k+3s}-1)(q^{3n-3k+3}-1)$$
$$+(q+1)(q^{3n-3k+3s+3}-1)(q^{3n-3k+3s}-1) \geq 0.$$

Putting $|B_\pi| = q^{3s}+q^{3s-1}+q^{3s-2}+3q^{3s-3}$ or $|B_\pi| = q^{3s+1}-q^{3s-1}-q^{3s-2}-3q^{3s-3}$ in this inequality, with $q \geq 7$, gives a contradiction. Hence, the statement follows. □

Theorem 10. *A small minimal* 1*-blocking set in* $\mathrm{PG}(n,q^3)$*,* $q=p^h$*,* p *prime,* $p \geq 7$*, intersecting every hyperplane in* $1 \pmod q$ *points, is linear.*

Proof. Lemma 9 implies that a small minimal 1-blocking set B in $\mathrm{PG}(n,q^3)$, intersecting every hyperplane in $1 \pmod q$ points, has at most q^3+q^2+q+3 points. Since every hyperplane intersects B in $1 \pmod q$ points, it is easy to see that $|B| \equiv 1 \pmod q$. This implies that $|B| \leq q^3+q^2+q+1$. Result 4 shows that B is linear. □

Corollary 11. *A small minimal* 1*-blocking set in* $\mathrm{PG}(n,p^3)$*,* p *prime,* $p \geq 7$*, is* $\mathbb{F}_p$*-linear.*

Proof. This follows from Result 3 and Theorem 10. □

For the remainder of this section, we use the following assumption:

(B) B is a small minimal k-blocking set in $\mathrm{PG}(n,q^3)$, $q=p^h$, p prime, $p \geq 7$, intersecting every $(n-k)$-space in $1 \pmod q$ points.

For convenience let us introduce the following terminology. A *full* line of B is a line which is contained in B. An $(n-k+s)$-space S, $s<k$, is called *large* if S contains more than $q^{3s+1}-q^{3s-1}-q^{3s-2}-3q^{3s-3}$ points of B, and S is called *small* if it contains less than $q^{3s}+q^{3s-1}+q^{3s-2}+3q^{3s-3}$ points of B.

Lemma 12. *Let* π *be an* $(n-k)$*-space of* $\mathrm{PG}(n,q^3)$*,* $k>1$*.*

(1) If $B \cap \pi$ *is a point, then there are at most* $q^{3k-5}+4q^{3k-6}-1$ *large* $(n-k+1)$*-spaces through* π*.*

(2) If π intersects B in $q\sqrt{q}+1$, q^2+1 or q^2+q+1 collinear points, then there are at most $q^{3k-5}+5q^{3k-6}-1$ large $(n-k+1)$-spaces through π.

(3) If π intersects B in $q+1$ collinear points, then there are at most $3q^{3k-6}-q^{3k-7}-1$ large $(n-k+1)$-spaces through π.

Proof. Suppose there are y large $(n-k+1)$-spaces through π. Then the number of points in B is at least

$$y(q^4-q^2-q-3-|B\cap\pi|)+((q^{3k}-1)/(q^3-1)-y)x+|B\cap\pi|, \ (*)$$

where x depends on the intersection $B\cap\pi$.

(1) In this case, $x=q^3$ and $|B\cap\pi|=1$. If $y=q^{3k-5}+4q^{3k-6}$, then $(*)$ is larger than $q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$, a contradiction.

(2) In this case, $x=q^3$ and $|B\cap\pi|\leq q^2+q+1$. If $y=q^{3k-5}+5q^{3k-6}$, then $(*)$ is larger than $q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$, a contradiction.

(3) By Result 4, we know that an $(n-k+1)$-space π' through π intersects B in at least q^3+q^2+1 points, since a $(q+1)$-secant in π' implies that the intersection of π' with B is non-trivial and not a Baer subplane, hence $x=q^3+q^2-q$, and $|B\cap\pi|=q+1$. If $3q^{3k-6}-q^{3k-7}$, then $(*)$ is larger than $q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$, a contradiction. □

Lemma 13. *Let L be a line such that $1<|B\cap L|<q^3+1$. For all $i\in\{1,\ldots,n-k\}$, there exists an i-space π_i on L such that $B\cap\pi_i=B\cap L$.*

Proof. It follows from Result 3 that every subspace on L intersects $B\setminus L$ in zero or at least p points. We proceed by induction on the dimension i. The statement obviously holds for $i=1$. Suppose there exists an i-space π_i on 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 on L, then the number of points of B is at least

$$|B\cap L|+p(q^{3(n-i)-3}+q^{3(n-i)-6}+\ldots+q^3+1),$$

but, by Lemma 9, $|B|\leq q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$. If $i\leq n-k-1$ and $p\geq 7$, this is a contradiction. We may conclude that there exists an i-space π_i on L such that $B\cap L=B\cap\pi_i$, $\forall i\in\{1,\ldots,n-k\}$. □

Theorem 14. *A line L intersects B in a linear set.*

Proof. Note that it is enough to show that L is contained in a subspace of $\mathrm{PG}(n,q^3)$ intersecting B in a linear set. If $k=1$, then B is linear by Theorem 10, and the statement follows. Let $k>1$, let L be a line, not contained in B, intersecting B in at least two points. It follows from Lemma 13 that there exists an $(n-k)$-space π_L such that $B\cap L=B\cap\pi_L$. If each of the $(q^{3k}-1)/(q^3-1)$ $(n-k+1)$-spaces through π_L were large, then the number of points in B would be at least

$$\frac{q^{3k}-1}{q^3-1}(q^4-q^2-q-3-q^3)+q^3>q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3},$$

a contradiction. Hence, there is a small $(n-k+1)$-space π through L, so $B\cap\pi$ is a small 1-blocking set which is linear by Theorem 10. This concludes the proof. □

3 The proof of Theorem 1

In the proof of the main theorem, we distinguish two cases. In both cases, we need the following lemmas.

We continue with the following assumption:

(B) B is a small minimal k-blocking set in $\mathrm{PG}(n, q^3)$, $q = p^h$, p prime, $p \geq 7$, intersecting every $(n-k)$-space in 1 (mod q) points;

and we consider the following properties:

(H_1) $\forall s < k$: every small minimal s-blocking set that does not contain a $(q\sqrt{q}+1)$-secant and intersects every $(n-s)$-space in 1 (mod q) points, is $\mathbb{F}_q$-linear;

(H_2) $\forall s < k$: every small minimal s-blocking set that contains a $(q\sqrt{q}+1)$-secant and intersects every $(n-s)$-space in 1 (mod q) points, is $\mathbb{F}_{q\sqrt{q}}$-linear.

Lemma 15. *If (H_1) or (H_2), and S is a small $(n-k+s)$-space, $0 < s < k$, then $B \cap S$ is a small minimal linear s-blocking set in S, and hence $|B \cap S| \leq (q^{3s+1}-1)/(q-1)$.*

Proof. Clearly, $B \cap S$ is an s-blocking set in S. By (B), $B \cap S$ intersects every $(n-k)$-space in 1 (mod q) points, and it follows from Result 6 that $B \cap S$ is minimal. Now apply (H_1) or (H_2). □

Lemma 16. *Suppose (H_1) or (H_2). Let $k > 2$ and let π_{n-2} be an $(n-2)$-space such that $B \cap \pi_{n-2}$ is a non-trivial small linear $(k-2)$-blocking set, then there are at least $q^3 - q + 6$ small hyperplanes through π_{n-2}.*

Proof. Applying Lemma 15 with $s = k-2$, it follows that $B \cap \pi_{n-2}$ contains at most $(q^{3k-5}-1)/(q-1)$ points. On the other hand, from Lemmas 9 and 15 with $s = k-1$, we know that a hyperplane intersects B in at most $(q^{3k-2}-1)/(q-1)$ points or in more than $q^{3k-2} - q^{3k-4} - q^{3k-5} - 3q^{3k-6}$ points. In the first case, a hyperplane H intersects B in at least $q^{3k-3} + 1 + (q^{3k-3}+q)/(q+1)$ points, using a result of Szőnyi and Weiner [10, Corollary 3.7] for the $(k-1)$-blocking set $H \cap B$. If there are at least $q-4$ large hyperplanes, then the number of points in B is at least

$$(q-4)(q^{3k-2} - q^{3k-4} - q^{3k-5} - 3q^{3k-6} - \frac{q^{3k-5}-1}{q-1})+$$

$$(q^3-q+5)(q^{3k-3} + 1 + \frac{q^{3k-3}+q}{q+1} - \frac{q^{3k-5}-1}{q-1}) + \frac{q^{3k-5}-1}{q-1},$$

which is larger than $q^{3k} + q^{3k-1} + q^{3k-2} + 3q^{3k-3}$ if $q \geq 7$, a contradiction. Hence, there are at most $q-5$ large hyperplanes through π_{n-2}. □

Lemma 17. *Suppose (H_1) or (H_2). Let $k > 2$ and let L be a secant line to B, not contained in B. Let N be a line of $\mathrm{PG}(n, q^3)$ skew to L. For all $i \in \{1, \dots, k-2\}$, there exists an $(n-k+i)$-space π_i through L, skew to N, such that $\pi_i \cap B$ is a small minimal i-blocking set of π_i.*

Proof. Lemma 13 shows that there is an $(n-k)$-space π_{n-k} through L, such that $B \cap L = B \cap \pi_{n-k}$; so we certainly find an $(n-k-2)$-space π_{n-k-2} through L, skew to N, such that $B \cap L = B \cap \pi_{n-k-2}$. Since the number of $(n-k-1)$-spaces through π_{n-k-2} that do not meet N, exceeds the number of points that can lie in B, there is an $(n-k-1)$-space π_{n-k-1} through π_{n-k-2} such that $B \cap L = B \cap \pi_{n-k-1}$. If an $(n-k)$-space through π_{n-k-1} contains an extra element of B, it contains at least q^2 extra elements of B, since a line containing 2 points of B contains at least $q+1$ points of B. This implies that there is an $(n-k)$-space π_{n-k} through π_{n-k-1} with no extra points of B, and skew to N.

We proceed by induction on the dimension i. Lemma 12 (2) and (3) show that there are at least $(q^{3k}-1)/(q^3-1) - q^{3k-5} - 5q^{3k-6} + 1 > q^3 + 1$ small $(n-k+1)$-spaces through π_{n-k} which proves the statement for $i = 1$.

Suppose that there exists an $(n-k+t)$-space π_{n-k+t} through L, skew to N, such that $B \cap \pi_{n-k+t}$ is a small minimal t-blocking set of π_{n-k+t}. An $(n-k+t+1)$-space through π_{n-k+t} contains at most $(q^{3t+4}-1)/(q-1)$ or more than $q^{3t+4} - q^{3t+2} - q^{3t+1} - 3q^{3t}$ points of B (see Lemmas 9 and 15).

Suppose all $(q^{3k-3t}-1)/(q^3-1) - q^3 - 1$ $(n-k+t+1)$-spaces through π_{n-k+t}, skew to N, contain more than $q^{3t+4} - q^{3t+2} - q^{3t+1} - 3q^{3t}$ points of B. Then the number of points in B is larger than $q^{3k} + q^{3k-1} + q^{3k-2} + 3q^{3k-3}$ if $t \leq k-3$, a contradiction.

We may conclude that there exists an $(n-k+i)$-space π_i on L such that $B \cap \pi_i$ is a small minimal i-blocking set, skew to N, $\forall i \in \{1, \ldots, k-2\}$. □

3.1 Case 1: there are no $(q\sqrt{q}+1)$-secants

In this subsection, we will use induction on k to prove that small minimal k-blocking sets in $\mathrm{PG}(n, q^3)$, intersecting every $(n-k)$-space in $1 \pmod q$ points and not containing a $(q\sqrt{q}+1)$-secant, are $\mathbb{F}_q$-linear. The induction basis is Theorem 10. Now we continue with the assumption that (H_1) holds, i.e.,

(H_1) $\forall s < k$: every small minimal s-blocking set that does not contain a $(q\sqrt{q}+1)$-secant and intersects every $(n-s)$-space in $1 \pmod q$ points, is $\mathbb{F}_q$-linear;

and that

(B_1) B is a small minimal k-blocking set in $\mathrm{PG}(n, q^3)$, $q = p^h$, p prime, $p \geq 7$, intersecting every $(n-k)$-space in $1 \pmod q$ points, not containing a $(q\sqrt{q}+1)$-secant.

Lemma 18. *If B is non-trivial, 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 $(q+1)$-secant through P in H_i, $i = 1, \ldots, q^{3k-3} - 2q^{3k-4}$.*

Proof. Since B is non-trivial, there is at least one line N with $1 < |N \cap B| < q^3 + 1$. Lemma 13 shows that there is an $(n-k)$-space π_N through N such that $B \cap N = B \cap \pi_N$. It follows from Lemma 12 and Theorem 14 that there is at least one $(n-k+1)$-space H through π_N such that $H \cap B$ is a small minimal linear 1-blocking set of H. In this non-trivial small minimal linear 1-blocking set, there are $(q+1)$-secants (see Remark 5). Let M be one of those $(q+1)$-secants of B. Again using Lemma 13, we find an $(n-k)$-space π_M through M such that $B \cap M = B \cap \pi_M$.

Lemma 12 (3) shows that through π_M, there are at least $\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7} + 1$ small $(n-k+1)$-spaces. Let P be a point of M. Since in each of these intersections, P lies on at least $q^2 - 1$ other $(q+1)$-secants, a point P of M lies in total on at least $(q^2-1)(\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7} + 1)$ other $(q+1)$-secants. Since each of the $\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7} + 1$ small $(n-k+1)$-spaces contains at least $q^3 + q^2 - q$ points of B not on M, and $|B| < q^{3k} + q^{3k-1} + q^{3k-2} + 3q^{3k-3}$ (see Lemma 9), there are less than $2q^{3k-2} + 6q^{3k-3}$ points of B left in the large $(n-k+1)$-spaces. Hence, P lies on less than $2q^{3k-5} + 6q^{3k-6}$ full lines.

Since B is minimal, P lies on a tangent $(n-k)$-space π. There are at most $q^{3k-5} + 4q^{3k-6} - 1$ large $(n-k+1)$-spaces through π (Lemma 12 (1)). Moreover, since at least $\frac{q^{3k}-1}{q^3-1} - (q^{3k-5} + 4q^{3k-6} - 1) - (2q^{3k-5} + 6q^{3k-6})$ $(n-k+1)$-spaces through π contain at least $q^3 + q^2$ points of B, and at most $2q^{3k-5} + 6q^{3k-6}$ of the small $(n-k+1)$-spaces through π contain exactly $q^3 + 1$ points of B, there are at most $2q^{3k-2} + 23q^{3k-3}$ points of B left. Hence, P lies on at most $2q^{3k-3} + 23q^{3k-4}$ $(q+1)$-secants of the large $(n-k+1)$-spaces through π. This implies that there are at least $(q^2-1)(\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7} + 1) - (2q^{3k-3} + 23q^{3k-4})$ distinct $(q+1)$-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 $q^2 + q + 1$ $(q+1)$-secants through P, this implies that there are at least $q^{3k-3} - 2q^{3k-4}$ $(n-k+1)$-spaces H_i through π such that P lies on a $(q+1)$-secant in H_i. □

Lemma 19. *Let π be an $(n-k)$-dimensional tangent space of B at the point 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 3-space π_i through $x \in \mathcal{S}(P)$, $\mathcal{B}(x) \cap \pi_i = \{x\}$ $(i = 1, 2)$ and $\mathcal{B}(\pi_i)$ not contained in a line of $\mathrm{PG}(n, q^3)$. Then $\mathcal{B}(\langle \pi_1, \pi_2 \rangle) \subseteq B$.*

Proof. Since $\langle \mathcal{B}(\pi_i) \rangle$ is not contained in a line of $\mathrm{PG}(n, q^3)$, there is at most one element Q of $\mathcal{B}(\pi_i)$ such that $\langle \mathcal{S}(P), Q \rangle$ intersects π_i in a plane. If there is such a plane, then we denote its point set by μ_i, otherwise we put $\mu_i = \emptyset$.

Let M be a line through x in $\pi_1 \setminus \mu_1$, let $s \neq x$ be a point of $\pi_2 \setminus \mu_2$, and note that $\mathcal{B}(s) \cap \pi_2 = \{s\}$.

We claim that there is a line T through s in π_2 and an $(n-2)$-space π_M through $\langle \mathcal{B}(M) \rangle$ such that there are at least 4 points $t_i \in T, t_i \notin \mu_2$, such that $\langle \pi_M, \mathcal{B}(t_i) \rangle$ is small and hence has a linear intersection with B, with $B \cap \pi_M = M$ if $k = 2$ and $B \cap \pi_M$ is a small minimal $(k-2)$-blocking set if $k > 2$.

If $k = 2$, the existence of π_M follows from Lemma 13, and we know from Lemma 12 (1) that there are at most $q + 3$ large hyperplanes through π_M. Denote the set of points of $\mathcal{B}(\pi_2)$, contained in one of those hyperplanes by F. Hence, if Q is a point of $\mathcal{B}(\pi_2) \setminus F$, $\langle Q, \pi_M \rangle$ is a small hyperplane.

Let T_1 be a line through s in $\pi_2 \setminus \mu_2$ and not through x, and suppose that $\mathcal{B}(T_1)$ contains at least $q - 3$ points of F.

Let T_2 be a line in $\pi_2 \setminus \mu_2$, through s, not in $\langle x, T_1 \rangle$, not through x. There are at most $q + 3 - (q - 3)$ reguli through x of $\mathcal{S}(F)$, not in $\langle x, T_1 \rangle$, and if $\mu \neq \emptyset$ one element of $\mathcal{B}(\mu_2)$ is contained in $\mathcal{B}(T_2)$. Since it is possible that $\mathcal{B}(s)$ is an element of F, this gives in total at most 8 points of $\mathcal{B}(T_2)$ that are contained in F. This implies, if $q > 11$, that at least 5 of the hyperplanes $\{\langle \pi_M, \mathcal{B}(t) \rangle || t \in T_2\}$ are small.

If $q = 11$, it is possible that $\mathcal{B}(T_2)$ contains at least 8 points of F. If T_3 is a line in $\pi_2 \setminus \mu_2$, through s, $\langle x, T_1 \rangle$, $\langle x, T_2 \rangle$ and not through x, then there are at least 5 points t of T_3 such that $\langle \pi_M, \mathcal{B}(t)\rangle$ is a small hyperplane.

If $q = 7$ and if $\mathcal{B}(s) \in \mathcal{B}(F)$, it is possible that $\mathcal{B}(T_2)$, $\mathcal{B}(T_3)$, and $\mathcal{B}(T_4)$, with T_i a line through s in $\pi_2 \setminus \mu_2$, not in $\langle x, T_j\rangle$, $j < i$, not through x, contain 4 points of F. A fifth line T_5 through s in $\pi_2 \setminus \mu_2$, not in $\langle x, T_j\rangle$, $j < i$, not through x, contains at least 5 points t such that $\langle \pi_M, \mathcal{B}(t)\rangle$ is a small hyperplane.

If $k > 2$, let T be a line through s in $\pi_2 \setminus \mu_2$, not through x. It follows from Lemma 17 that there is an $(n-2)$-space π_M through $\langle \mathcal{B}(M)\rangle$ such that $B \cap \pi_M$ is a small minimal $(k-2)$-blocking set of $\mathrm{PG}(n, q^3)$, skew to $\mathcal{B}(T)$. Lemma 16 shows that at most $q - 5$ of the hyperplanes through π_M are large. This implies that at least 5 of the hyperplanes $\{\langle \pi_M, \mathcal{B}(t)\rangle || t \in \mathcal{B}(T)\}$ are small. This proves our claim.

Since $B \cap \langle \mathcal{B}(t_i), \pi_M\rangle$ is linear, also the intersection of $\langle \mathcal{B}(t_i), \mathcal{B}(M)\rangle$ with B is linear, i.e., there exist subspaces τ_i, $\tau_i \cap \mathcal{S}(P) = \{x\}$, such that $\mathcal{B}(\tau_i) = \langle \mathcal{B}(t_i), \mathcal{B}(M)\rangle \cap B$. Since $\tau_i \cap \langle \mathcal{B}(M)\rangle$ and M are both transversals through x to the same regulus $\mathcal{B}(M)$, they coincide, hence $M \subseteq \tau_i$. The same holds for $\tau_i \cap \langle \mathcal{B}(t_i), \mathcal{S}(P)\rangle$, implying $t_i \in \tau_i$. We conclude that $\mathcal{B}(\langle M, t_i\rangle) \subseteq \mathcal{B}(\tau_i) \subseteq B$.

We show that $\mathcal{B}(\langle M, T\rangle) \subseteq B$. Let L' be a line of $\langle M, T\rangle$, not intersecting M. The line L' intersects the planes $\langle M, t_i\rangle$ in points p_i such that $\mathcal{B}(p_i) \in B$. Since $\mathcal{B}(L')$ is a subline intersecting B in at least 4 points, Result 7 shows that $\mathcal{B}(L') \subset B$. Since every point of the space $\langle M, T\rangle$ lies on such a line L', $\mathcal{B}(\langle M, T\rangle) \subseteq B$.

Hence, $\mathcal{B}(\langle M, s\rangle) \subseteq B$ for all lines M through x, M in $\pi_1 \setminus \mu_1$, and all points $s \neq x \in \pi_2 \setminus \mu_2$, so $\mathcal{B}(\langle \pi_1, \pi_2\rangle \setminus (\langle \mu_1, \pi_2\rangle \cup \langle \mu_2, \pi_1\rangle)) \subseteq B$. Since every point of $\langle \mu_1, \pi_2\rangle \cup \langle \mu_2, \pi_1\rangle$ lies on a line N with $q-1$ points of $\langle \pi_1, \pi_2\rangle \setminus (\langle \mu_1, \pi_2\rangle \cup \langle \mu_2, \pi_1\rangle)$, Result 7 shows that $\mathcal{B}(N) \subset B$. We conclude that $\mathcal{B}(\langle \pi_1, \pi_2\rangle) \subseteq B$. □

Theorem 20. *The set B is $\mathbb{F}_q$-linear.*

Proof. If B is a k-space, then B is $\mathbb{F}_q$-linear. If B is a non-trivial small minimal k-blocking set, Lemma 18 shows that there exists a point P of B, a tangent $(n-k)$-space π at the point P and at least $q^{3k-3} - 2q^{3k-4}$ $(n-k+1)$-spaces H_i through π for which $B \cap H_i$ is small and linear, where P lies on at least one $(q+1)$-secant of $B \cap H_i$, $i = 1, \ldots, s$, $s \geq q^{3k-3} - 2q^{3k-4}$. Let $B \cap H_i = \mathcal{B}(\pi_i), i = 1, \ldots, s$, with π_i a 3-dimensional space.

Lemma 19 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 $\mathrm{PG}(n, q^3)$. 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 18 that $z \leq 2q^{3k-4} + (q^{3k-3}-1)/(q^3-1)$. There are at least $(q^{3k-3} - 2q^{3k-4} - 1)/q^3$ 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 $5q^2 - 49$ of the spaces K_i, then $z \geq (5q^2 - 49)(q^{3k-3} - 2q^{3k-4} - 1)/q^3$, a contradiction if $q \geq 7$. Let $\langle H_1, H_2\rangle$ be an $(n-k+2)$-space containing less than $5q^2 - 49$ 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 $5q^{3i-4} - 49q^{3i-6}$ of the spaces K_i such that $\mathcal{B}(\langle \pi_1, \ldots, \pi_i\rangle) \subseteq B$.

There are at least $\frac{q^{3k-3}-2q^{3k-4}-(q^{3i}-1)/(q^3-1)}{q^{3i}}$ different $(n-k+i+1)$-spaces $\langle H_1, H_2, \ldots, H_i, H\rangle$, $H \not\subseteq \langle H_1, H_2, \ldots, H_i\rangle$. If all of these contain at least

$5q^{3i-1} - 49q^{3i-3}$ of the spaces K_i, then

$$z \geq \begin{array}{l}(5q^{3i-1} - 49q^{3i-3} - 5q^{3i-4} + 49q^{3i-6})\frac{q^{3k-3}-2q^{3k-4}-(q^{3i}-1)/(q^3-1)}{q^{3i}} \\ +5q^{3i-4} - 49q^{3i-6},\end{array}$$

a contradiction if $q \geq 7$. Let $\langle H_1, \dots, H_{i+1}\rangle$ be an $(n-k+i+1)$-space containing less than $5q^{3i-1} - 49q^{3i-3}$ spaces K_i. We still need to prove that $\mathcal{B}(\langle \pi_1, \dots, \pi_{i+1}\rangle) \subseteq B$. Since $\mathcal{B}(\langle \pi_{i+1}, \pi\rangle) \subseteq B$, with π a 3-space in $\langle \pi_1, \dots, \pi_i\rangle$ for which $\mathcal{B}(\pi)$ is not contained in one of the spaces K_i, there are at most $5q^{3i-4} - 49q^{3i-6}$ distinct 6-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 $(5q^{3i-4} - 49q^{3i-6})(q^6 + q^5 + q^4)$ points t for which $\mathcal{B}(t)$ is not necessarily contained in B. Let u be a point of such a space $\langle \pi_{i+1}, \mu\rangle$. Suppose that each of the $(q^{3i+3}-1)/(q-1)$ lines through u in $\langle \pi_1, \dots, \pi_{i+1}\rangle$ contains at least $q-2$ of the points t for which $\mathcal{B}(t)$ is not in B. Then there are at least $(q-3)(q^{3i+3}-1)/(q-1) + 1 > (5q^{3i-4} - 49q^{3i-6})(q^6 + q^5 + q^4)$ such points t, if $q \geq 7$, a contradiction. Hence, there is a line N through t for which for at least 4 points $v \in N$, $\mathcal{B}(v) \in B$. Result 7 yields that $\mathcal{B}(t) \in B$. This implies that $\mathcal{B}(\langle \pi_1, \dots, \pi_{i+1}\rangle) \subseteq B$.

Hence, the space $\langle H_1, H_2, \dots, H_k\rangle$, which spans the space $\mathrm{PG}(n, q^3)$, is such that $\mathcal{B}(\langle \pi_1, \dots, \pi_k\rangle) \subseteq B$. But $\mathcal{B}(\langle \pi_1, \dots, \pi_k\rangle)$ corresponds to a linear k-blocking set B' in $\mathrm{PG}(n, q^3)$. Since B is minimal, $B = B'$. □

Corollary 21. *A small minimal k-blocking set in $\mathrm{PG}(n, p^3)$, p prime, $p \geq 7$, is $\mathbb{F}_p$-linear.*

Proof. This follows from Result 3 and Theorem 20. □

3.2 Case 2: there are $(q\sqrt{q}+1)$-secants to B

In this subsection, we will use induction on k to prove that small minimal k-blocking sets in $\mathrm{PG}(n, q^3)$, containing a $(q\sqrt{q}+1)$-secant and intersecting every $(n-k)$-space in 1 (mod q) points, are $\mathbb{F}_{q\sqrt{q}}$-linear. The induction basis is Theorem 10. We continue with the assumption that (H_2) holds, i.e.,

(H_2) $\forall s < k$: every small minimal s-blocking set that contains a $(q\sqrt{q}+1)$-secant and intersects every $(n-s)$-space in 1 (mod q) points, is $\mathbb{F}_{q\sqrt{q}}$-linear.

and that

(B_2) B is small minimal k-blocking set in $\mathrm{PG}(n, q^3)$, containing a $(q\sqrt{q}+1)$-secant and intersecting every $(n-k)$-space in 1 (mod q) points.

In this case, $\mathcal{S}$ maps $\mathrm{PG}(n, q^3)$ onto $\mathrm{PG}(2n+1, q\sqrt{q})$ and the Desarguesian spread consists of lines.

Lemma 22. *If B is non-trivial, there exist a point $P \in B$, a tangent $(n-k)$-space π at P and small $(n-k+1)$-spaces H_i through π, such that there is a $(q\sqrt{q}+1)$-secant through P in H_i, $i = 1, \dots, q^{3k-3} - q^{3k-4} - 2\sqrt{q}q^{3k-5}$.*

Proof. There is a $(q\sqrt{q}+1)$-secant M. Lemma 13 shows that there is an $(n-k)$-space π_M through M such that $B \cap M = B \cap \pi_M$.

Lemma 12 (3) shows that there are at least $\frac{q^{3k}-1}{q^3-1} - q^{3k-5} - 5q^{3k-6} + 1$ small $(n-k+1)$-spaces through π_M. Moreover, the intersections of these small

$(n-k+1)$-spaces with B are Baer subplanes $\mathrm{PG}(2,q\sqrt{q})$, since there is a $(q\sqrt{q}+1)$-secant M. Let P be a point of $M\cap B$.

Since in any of these intersections, P lies on $q\sqrt{q}$ other $(q\sqrt{q}+1)$-secants, a point P of $M\cap B$ lies in total on at least $q\sqrt{q}(\frac{q^{3k}-1}{q^3-1}-q^{3k-5}-5q^{3k-6}+1)$ other $(q\sqrt{q}+1)$-secants. Since any of the $\frac{q^{3k}-1}{q^3-1}-q^{3k-5}-5q^{3k-6}+1$ small $(n-k+1)$-spaces through π_M contains q^3 points of B not in π_M, and $|B|<q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$ (see Lemma 9), there are less than $q^{3k-1}+4q^{3k-2}$ points of B left in the other $(n-k+1)$-spaces through π_M. Hence, P lies on less than $q^{3k-4}+4q^{3k-5}$ full lines.

Since B is minimal, there is a tangent $(n-k)$-space π through P. There are at most $q^{3k-5}+4q^{3k-6}-1$ large $(n-k+1)$-spaces through π (Lemma 12 (1)). Moreover, since at least $\frac{q^{3k}-1}{q^3-1}-(q^{3k-5}+4q^{3k-6}-1)-(q^{3k-4}+4q^{3k-5})$ small $(n-k+1)$-spaces through π contain $q^3+q\sqrt{q}+1$ points of B, and at most $q^{3k-4}+4q^{3k-5}$ of the small $(n-k+1)$-spaces through π contain exactly q^3+1 points of B, there are at most $q^{3k-1}-q^{3k-2}\sqrt{q}+4q^{3k-2}$ points of B left. Hence, P lies on at most $(q^{3k-1}-q^{3k-2}\sqrt{q}+4q^{3k-2})/(q\sqrt{q}+1)$ different $(q\sqrt{q}+1)$-secants of the large $(n-k+1)$-spaces through π. This implies that there are at least $q\sqrt{q}(\frac{q^{3k}-1}{q^3-1}-q^{3k-5}-5q^{3k-6}+1)-(q^{3k-1}-q^{3k-2}\sqrt{q}+4q^{3k-2})/(q\sqrt{q}+1)$ different $(q\sqrt{q}+1)$-secants left through P in small $(n-k+1)$-spaces through π. Since in a small $(n-k+1)$-space through π, there lie $q\sqrt{q}+1$ different $(q\sqrt{q}+1)$-secants through P, this implies that there are certainly at least $q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}$ small $(n-k+1)$-spaces H_i through π such that P lies on a $(q\sqrt{q}+1)$-secant in H_i. □

Lemma 23. *Let π be an $(n-k)$-dimensional tangent space of B at the point 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 plane π_i through $x\in\mathcal{S}(P)$, $\mathcal{B}(x)\cap\pi_i=\{x\}$ $(i=1,2)$ and $\mathcal{B}(\pi_i)$ not contained in a line of* $\mathrm{PG}(n,q^3)$. *Then $\mathcal{B}(\langle\pi_1,\pi_2\rangle)\subseteq B$.*

Proof. Let M be a line through x in π_1, let $s\neq x$ be a point of π_2.

We claim that there is a line T through s, not through x, in π_2 and an $(n-2)$-space π_M through $\langle\mathcal{B}(M)\rangle$ such that there are at least $q\sqrt{q}-q-2$ points $t_i\in T$, such that $\langle\pi_M,\mathcal{B}(t_i)\rangle$ is small and hence has a linear intersection with B, with $B\cap\pi_M=M$ if $k=2$ and $B\cap\pi_M$ is a small minimal $(k-2)$-blocking set if $k>2$. From Lemma 12 (1), we know that there are at most $q+3$ large hyperplanes through π_M if $k=2$, and at most $q-5$ if $k>2$ (see Lemma 16).

Let T be a line through s in π_2, not through x. The existence of π_M follows from Lemma 13 if $k=2$, and Lemma 17 if $k>2$. Since $\mathcal{B}(T)$ contains $q\sqrt{q}+1$ spread elements, there are at least $q\sqrt{q}-q-2$ points $t_i\in T$ such that $\langle\pi_M,\mathcal{B}(t_i)\rangle$ is small. This proves our claim.

Since $B\cap\langle\mathcal{B}(t_i),\pi_M\rangle$ is linear, also the intersection of $\langle\mathcal{B}(t_i),\mathcal{B}(M)\rangle$ with B is linear, i.e., there exist subspaces τ_i, $\tau_i\cap\mathcal{S}(P)=\{x\}$, such that $\mathcal{B}(\tau_i)=\langle\mathcal{B}(t_i),\mathcal{B}(M)\rangle\cap B$. Since $\tau_i\cap\langle\mathcal{B}(M)\rangle$ and M are both transversals through x to the same regulus $\mathcal{B}(M)$, they coincide, hence $M\subseteq\tau_i$. The same holds for $\tau_i\cap\langle\mathcal{B}(t_i),\mathcal{S}(P)\rangle$, implying $t_i\in\tau_i$. We conclude that $\mathcal{B}(\langle M,t_i\rangle)\subseteq\mathcal{B}(\tau_i)\subseteq B$.

We show that $\mathcal{B}(\langle M,T\rangle)\subseteq B$. Let L' be a line of $\langle M,T\rangle$, not intersecting M. The line L' intersects the planes $\langle M,t_i\rangle$ in points p_i such that $\mathcal{B}(p_i)\subseteq B$. Since $\mathcal{B}(L')$ is a subline intersecting B in at least $q\sqrt{q}-q-2$ points, Result 8 shows that $\mathcal{B}(L') \subseteq B$. Since every point of the space $\langle M, T\rangle$ lies on such a line L', $\mathcal{B}(\langle M, T\rangle) \subseteq B$.

Hence, $\mathcal{B}(\langle M, s\rangle) \subseteq B$ for all lines M through x in π_2, and all points $s \neq x \in \pi_2$. We conclude that $\mathcal{B}(\langle \pi_1, \pi_2\rangle) \subseteq B$. □

Theorem 24. *The set B is $\mathbb{F}_{q\sqrt{q}}$-linear.*

Proof. Lemma 22 shows that there exists a point P of B, a tangent $(n-k)$-space π at the point P and at least $q^{3k-3} - q^{3k-4} - 2\sqrt{q}q^{3k-5}$ distinct $(n-k+1)$-spaces H_i through π for which $B \cap H_i$ is a Baer subplane, $i = 1, \ldots, s$, $s \geq q^{3k-3} - q^{3k-4} - 2\sqrt{q}q^{3k-5}$. Let $B \cap H_i = \mathcal{B}(\pi_i), i = 1, \ldots, s$, with π_i a plane.

Lemma 23 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 $\mathrm{PG}(n, q^3)$. 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, $j = 1, \ldots, z$. There are at least $(q^{3k-3} - q^{3k-4} - 2\sqrt{q}q^{3k-5} - 1)/q^3$ 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 $2q^2$ of the spaces K_i, then $z \geq 2q^2(q^{3k-3} - q^{3k-4} - 2\sqrt{q}q^{3k-5} - 1)/q^3$, a contradiction if $q \geq 49$. Let $\langle H_1, H_2\rangle$ be an $(n-k+2)$-space containing less than $2q^2$ 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 $2q^{3i-4}$ of the spaces K_i, such that $\mathcal{B}(\langle \pi_1, \ldots, \pi_i\rangle) \subseteq B$.

There are at least $\frac{q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}-(q^{3i}-1)/(q^3-1)}{q^{3i}}$ different $(n-k+i+1)$-spaces $\langle H_1, H_2, \ldots, H_i, H\rangle$, $H \not\subseteq \langle H_1, H_2, \ldots, H_i\rangle$.

If all of these contain at least $2q^{3i-1}$ of the spaces K_i, then

$$z \geq (2q^{3i-1} - 2q^{3i-4})\frac{q^{3k-3} - q^{3k-4} - 2\sqrt{q}q^{3k-5} - (q^{3i} - 1)/(q^3 - 1)}{q^{3i}} + 2q^{3i-4},$$

a contradiction if $q \geq 49$. Let $\langle H_1, \ldots, H_{i+1}\rangle$ be an $(n-k+i+1)$-space containing less than $2q^{3i-1}$ spaces K_i. We still need to prove that $\mathcal{B}(\pi_1, \ldots, \pi_{i+1}) \subseteq B$.

Since $\mathcal{B}(\langle \pi_{i+1}, \pi\rangle) \subseteq B$, with π a plane 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 $2q^{3i-4}$ 4-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 $2q^{3i-4}(q^6 + q^4\sqrt{q})$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B. Let Q be a point of such a space $\langle \pi_{i+1}, \mu\rangle$.

There are $((q\sqrt{q})^{2i+2} - 1)/(q\sqrt{q} - 1)$ lines through Q in $\langle \pi_1, \ldots, \pi_{i+1}\rangle \cong \mathrm{PG}(2i+2, q\sqrt{q})$, and there are at most $2q^{3i-4}(q^6 + q^4\sqrt{q})$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B. Suppose all lines through Q in $\langle \pi_1, \ldots, \pi_{i+1}\rangle \cong \mathrm{PG}(2i+2, q\sqrt{q})$ contain at least $q\sqrt{q} - q - \sqrt{q}$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B, then there are at least $(q\sqrt{q}-q-\sqrt{q}-1)((q\sqrt{q})^{2i+2}-1)/(q\sqrt{q}-1) + 1 > 2q^{3i-4}(q^6 + q^4\sqrt{q})$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B, a contradiction.

Hence, there is a line N through Q in $\langle \pi_1, \ldots, \pi_{i+1}\rangle$ with at most $q\sqrt{q} - q - \sqrt{q} - 1$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily contained in B, hence, for at least $q + \sqrt{q} + 2$ points $R \in N$, $\mathcal{B}(R) \in B$. Result 8 yields that $\mathcal{B}(Q) \in B$. This implies that $\mathcal{B}(\langle \pi_1, \ldots, \pi_{i+1}\rangle) \subseteq B$.

Hence, the space $\mathcal{B}(\langle H_1, H_2, \ldots, H_k\rangle)$ is such that $\mathcal{B}(\langle \pi_1, \ldots, \pi_k\rangle) \subseteq B$. But $\mathcal{B}(\langle \pi_1, \ldots, \pi_k\rangle)$ corresponds to a linear k-blocking set B' in $\mathrm{PG}(n, q^3)$. Since B is minimal, $B = B'$. □

References

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

[2] N.V. Harrach and K. Metsch. Small point sets of $\mathrm{PG}(n, q^3)$ intersecting each k-subspace in 1 mod q points. *Des. Codes Cryptogr.* **56** (2010), 235–248.

[3] M. Lavrauw. Scattered spaces with respect to spreads, and eggs in finite projective spaces. PhD Dissertation, Eindhoven University of Technology, Eindhoven, 2001. viii+115 pp.

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

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

[6] K. Metsch and L. Storme. Partial t-spreads in $\mathrm{PG}(2t+1, q)$. *Des. Codes Cryptogr.* **18** (1999), 199–216.

[7] O. Polverino and L. Storme. Small minimal blocking sets in $\mathrm{PG}(2, q^3)$. *European J. Combin.* **23** (2002), no. 1, 83–92.

[8] L. Storme and Zs. Weiner. On 1-blocking sets in $\mathrm{PG}(n, q)$, $n \geq 3$. *Des. Codes Cryptogr.* **21** (2000), no. 1-3, 235–251.

[9] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory, Ser. A* **115** (2008), no. 7, 1167–1182.

[10] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory, Ser. A* **95** (2001), no. 1, 88–101.

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