Journal of Combinatorial Theory, Series A 164 (2019) 109–124

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

The minimum size of a linear set

Jan De Beule [a], Geertrui Van de Voorde [b]

[a] *Vrije Universiteit Brussel, Department of Mathematics, Pleinlaan 2, B-1050 Brussel, Belgium*
[b] *University of Canterbury, School of Mathematics and Statistics, Private Bag 4800, 8140 Christchurch, New Zealand*

ARTICLE INFO

Article history:
Received 19 April 2018
Available online xxxx

Keywords:
Linear set
Linearised polynomial
Directions determined by a point set

ABSTRACT

In this paper, we first determine the minimum possible size of an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^n)$. We obtain this result by relating it to the number of directions determined by a linearized polynomial whose domain is restricted to a subspace. We then use this result to find a lower bound on the number of points in an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(2, q^n)$. In the case $k = n$, this confirms a conjecture by Sziklai in [9].

1. Introduction

Let $q = p^h$, p prime, $h \geq 1$. The finite field of order q will be denoted as $\mathbb{F}_q$. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function. The graph of f is the set of affine points $\{(x, f(x)) | x \in \mathbb{F}_q\}$. The following theorem expresses the state of the art on the number of directions determined by this affine point set.

Theorem 1.1 *([1]). Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function. Let N be the number of directions determined by f. Let $s = p^e$ be maximal such that any line with a direction determined*

E-mail addresses: jan@debeule.eu (J. De Beule), geertrui.vandevoorde@canterbury.ac.nz (G. Van de Voorde).

https://doi.org/10.1016/j.jcta.2018.12.008
0097-3165/

by f that is incident with a point of the graph of f is incident with a multiple of s points of the graph of f. Then one of the following holds:

(i) $s = 1$ *and* $\frac{q+3}{2} \leq N \leq q+1$;
(ii) $\mathbb{F}_s$ *is a subfield of* $\mathbb{F}_q$ *and* $\frac{q}{s} + 1 \leq N \leq \frac{q-1}{s-1}$;
(iii) $s = q$ *and* $N = 1$.

Moreover, if $s > 2$, then the graph of f is $\mathbb{F}_s$-linear.

Theorem 1.1 completed two unresolved cases from [2, Theorem 1.1]. Many generalizations of the questions studied in [2] have been investigated, and it is impossible to summarize them in a concise way in this introduction. One notable generalization is found in [4], where bounds on the number of directions determined by an affine set of points of size smaller than q are derived. This paper turns out to be very useful to study the following question.

Let $n > 1$ and let $V \subset \mathbb{F}_{q^n}$ be a set of size q^k, $k \geq 1$, that is also a k-dimensional vector space over $\mathbb{F}_q$. Let $f : V \to \mathbb{F}_{q^n}$ be a function that is $\mathbb{F}_q$ linear, i.e. $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ for all $x, y \in V$ and for all $\lambda, \mu \in \mathbb{F}_q$. Then what is the minimum number of directions determined by the *graph of f*, i.e. the set $\{(x, f(x)) | x \in V\} \subset \mathrm{AG}(2, q^n)$?

This question is motivated by the question to find a lower bound on the size of an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^n)$. The main result can be stated as follows.

Theorem 1.2. *An $\mathbb{F}_q$-linear set of rank $k \leq n$ in $\mathrm{PG}(1, q^n)$ which contains at least one point of weight one, contains at least $q^{k-1} + 1$ points.*

For linear sets of rank n in $\mathrm{PG}(1, q^n)$, Theorem 1.2 was shown in [3, Lemma 2.2].

In Section 2, the connection between linear sets in $\mathrm{PG}(1, q^n)$ and the direction problem is described. Section 3 is devoted to the proof of Theorem 1.2, and in Section 4 we will use Theorem 1.2 to derive a lower bound on the size of linear sets in $\mathrm{PG}(2, q^n)$ under certain assumptions.

2. Preliminaries

For any additive group V let $V^* := V \setminus \{0\}$.

2.1. Linear sets

Let $k \geq 1$ and $r \geq 2$. A point set in $\mathrm{PG}(r-1, q^n)$ is an $\mathbb{F}_q$-linear set of rank k if it equals a set L_U for some $\mathbb{F}_q$-vector subspace U of $\mathbb{F}_q^{rn}$ of dimension k, where

$$L_U = \{\langle u \rangle_{q^n} \mid u \in U^*\}.$$

In other words, L_U consists of the projective points defined by the vectors of U^*. Let $P = \langle v \rangle_{q^n}$ be a point of L_U, then the *weight* of the point P in L_U is defined as $wt(P) = \dim_q(\langle v \rangle_{q^n} \cap U)$.[1] Hence, whenever we talk about the weight of a point in a linear set, the underlying defining vector space U should be specified.

An equivalent point of view on linear sets and their weights is obtained using *field reduction*. The underlying vector space of the projective space $\mathrm{PG}(r-1, q^n)$ is $V(r, q^n)$; if we consider $V(r, q^n)$ as a vector space over $\mathbb{F}_q$, then it has dimension rn, so it defines a projective space $\mathrm{PG}(rn-1, q)$. In this way, every point P of $\mathrm{PG}(r-1, q^n)$ corresponds to a subspace of $\mathrm{PG}(rn-1, q)$ of dimension $(n-1)$ and it is not hard to see that this set of $(n-1)$-spaces forms a spread of $\mathrm{PG}(rn-1, q)$, which is called a *Desarguesian spread*. If U is a subset of $\mathrm{PG}(rn-1, q)$, and $\mathcal{S}$ a Desarguesian $(n-1)$-spread, then we define $\mathcal{B}(U) := \{R \in \mathcal{S} \mid U \cap R \neq \emptyset\}$. In this paper, we consider the Desarguesian spread $\mathcal{S}$ as fixed and we identify the elements of $\mathcal{B}(U)$ with their corresponding points of $\mathrm{PG}(r-1, q^n)$. An *$\mathbb{F}_q$-linear set T of rank k* in $\mathrm{PG}(r-1, q^n)$ is then a set of points such that $T = \mathcal{B}(\mu)$, where μ is an $(k-1)$-dimensional subspace of $\mathrm{PG}(rn-1, q)$. If μ is the $(k-1)$-space defined by the k-dimensional vectorspace U of $V(rn-1, q)$, then $\mathcal{B}(\mu) = L_U$. The *weight* of a point $P = \mathcal{B}(p)$ of the linear set $\mathcal{B}(\mu)$ can then equivalently be defined as $\dim(\mu \cap \mathcal{B}(p)) + 1$, i.e., one more than the projective dimension of the intersection of the spread element corresponding to the point P with the subspace μ defining the linear set $\mathcal{B}(\mu)$. We see that a point Q belongs to the linear set $\mathcal{B}(\mu)$ if and only if the weight of Q in $\mathcal{B}(\mu)$ is at least one. For more information about linear sets and field reduction, we refer to [5,8].

Remark 1. Suppose that we have a linear set $\mathcal{B}(\mu)$ that has only points of weight at least j for some $j > 1$ and contains a point $P = \mathcal{B}(\pi)$ of weight exactly j. We can pick a subspace ν of codimension $j-1$ in μ meeting $\mathcal{B}(\pi) \cap \mu$ in exactly a point. As all points have weight at least j and ν has codimension $j-1$ in μ, $\mathcal{B}(\mu) = \mathcal{B}(\nu)$ and P has weight 1 in $\mathcal{B}(\nu)$.

We see that every $\mathbb{F}_q$-linear set L_U can be written as an $\mathbb{F}_q$-linear set $L_{U'}$ that contains at least one point of weight one. In Theorem 3.7, we will restrict ourselves to linear sets having a point of weight one, which is, by the previous argument, not a heavy restriction. However, the study of linear sets L_U where all points have weight strictly larger than 1 is of interest as well (see Remark 13).

Remark 2. The only $\mathbb{F}_q$-linear set of rank $k > n$ in $\mathrm{PG}(1, q^n)$ is the set of all points of $\mathrm{PG}(1, q^n)$. For this reason, we restrict ourselves to $\mathbb{F}_q$-linear sets of rank $k \leq n$.

Lemma 2.1. *Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^n)$, $k \leq n$, not containing the point $\langle (0,1) \rangle_{q^n}$, then $L_U = \{\langle (x, f(x)) \rangle_{q^n} | x \in V^*\}$ for some vector subspace V of dimension k and some $\mathbb{F}_q$-linear map $f : V \to \mathbb{F}_{q^n}$.*

[1] Note that here $\langle v \rangle_{q^n}$ refers to an n-dimensional subspace of $\mathbb{F}_q^{rn}$ and not to a vector line of $\mathbb{F}_{q^n}^r$.

Proof. We have that $L_U = \{\langle u\rangle_{q^n} \mid u \in U^*\}$, where U is a subspace of dimension k of $\mathbb{F}_q^{2n}$. We consider $\mathbb{F}_q^{2n}$ as $\mathbb{F}_{q^n}^2$ and see that every element of U can be written as (α_i, β_i) for some α_i, β_i in $\mathbb{F}_{q^n}$, $i = 1, \ldots, q^k$. Put $\beta_i = f(\alpha_i)$. Suppose to the contrary that $\alpha_{i_0} = \alpha_{j_0}$ for some $i_0 \neq j_0$. The elements $(\alpha_{i_0}, f(\alpha_{i_0}))$ and $(\alpha_{j_0}, f(\alpha_{j_0}))$ are distinct elements of U, so if $\alpha_{i_0} = \alpha_{j_0}$, then $f(\alpha_{i_0}) \neq f(\alpha_{j_0})$. As U is a vector subspace, it follows that $(\alpha_{i_0}, f(\alpha_{i_0})) - (\alpha_{j_0}, f(\alpha_{j_0})) = (0, f(\alpha_{i_0}) - f(\alpha_{j_0}))$ is an element of U. But L_U is skew from the point $\langle(0,1)\rangle_{q^n}$, a contradiction. We conclude that $V = \{\alpha_i \mid 1 \leq i \leq q^k\}$ has size q^k.

Since U is an $\mathbb{F}_q$-subspace, we have that for all $1 \leq i \leq q^k$, and $\lambda, \mu \in \mathbb{F}_q$ that $\lambda(\alpha_i, f(\alpha_i)) + \mu(\alpha_j, f(\alpha_j)) = (\lambda\alpha_i + \mu\alpha_j, \lambda f(\alpha_i) + \mu f(\alpha_j))$ has to be a vector of U. Hence, both the set $V = \{\alpha_i \mid 1 \leq i \leq q^k\}$ as the map f are closed under $\mathbb{F}_q$-linear combinations. It follows that $V = \{\alpha_i \mid 1 \leq i \leq q^k\}$ is an $\mathbb{F}_q$-subspace of dimension k and that f is an $\mathbb{F}_q$-linear map. □

From now on, whenever we write $L_U = \{\langle(x, f(x))\rangle_{q^n} | x \in V^*\}$, we assume that U is the subspace $\{(x, f(x)) | x \in V\}$. In this way, the weight of a point in L_U is unambiguously defined.

2.2. Directions determined by a point set

The set of directions determined by an affine point set $\mathcal{A} = \{\langle(1, x_i, y_i)\rangle_{q^n} \mid 1 \leq i \leq |\mathcal{A}|\}$ in $\mathrm{PG}(2, q^n)$ is the set $\{\langle(0, x_i - x_j, y_i - y_j)\rangle_{q^n} \mid 1 \leq i \neq j \leq |\mathcal{A}|\}$. The *slope* of a direction $\langle(0,1,y)\rangle_{q^n}$ is y, while the slope of $\langle(0,0,1)\rangle_{q^n}$ is ∞. If $\mathcal{A}$ is an affine point set, we define $\mathcal{D}_\mathcal{A}$ to be the set of slopes of the directions determined by $\mathcal{A}$.

Lemma 2.2. *The number of points of $L = \{\langle(x, f(x))\rangle_{q^n} | x \in V^*\}$, where V is a vector subspace of $\mathbb{F}_{q^n}$ and $f : V \to \mathbb{F}_{q^n}$ is an $\mathbb{F}_q$-linear map, is equal to the number of directions determined by the affine point set $\mathcal{A} = \{\langle(1, x, f(x))\rangle_{q^n} \mid x \in V\}$.*

Proof. The number of points of $\{\langle(x, f(x))\rangle_{q^n} | x \in V^*\} = \{\langle(1, f(x)/x)\rangle_{q^n} | x \in V^*\}$ is clearly equal to the size of the set $W = \{f(x)/x | x \in V^*\}$. The points $\langle(1, x_1, f(x_1))\rangle_{q^n}$ and $\langle(1, x_2, f(x_2))\rangle_{q^n}$ determine the direction $\langle(0, x_1 - x_2, f(x_1) - f(x_2))\rangle_{q^n}$. Since f is $\mathbb{F}_q$-linear and V is a subspace, $\langle(0, x_1 - x_2, f(x_1) - f(x_2))\rangle_{q^n}$ is the direction $\langle(0, 1, f(x_3)/x_3)\rangle_{q^n}$, with $x_3 = x_1 - x_2$. This implies that every direction determined by $\mathcal{A}$ is an element of the set $\{\langle(0,1,w)\rangle_{q^n} \mid w \in W\}$. Vice versa, take a point $\langle(0,1,w_0)\rangle_{q^n}$, with $w_0 \in W$, then $w_0 = f(x_0)/x_0$ for some $x_0 \in V^*$. Then $\langle(1,0,0)\rangle_{q^n}$ and $\langle(1, x_0, f(x_0))\rangle_{q^n}$ are points of $\mathcal{A}$ that determine the direction $\langle(0,1,w_0)\rangle_{q^n}$. This proves that the number of directions determined by $\mathcal{A}$ is equal to the size of W. □

Remark 3. Note that the direction $\langle(0,0,1)\rangle_{q^n}$ with slope ∞ is not determined by $\mathcal{A} = \{\langle(1, x, f(x))\rangle_{q^n} | x \in V^*\}$.

2.3. The Rédei polynomial

Let $S = \{\langle(1, x_i, y_i)\rangle_{q^n} \mid 1 \leq i \leq |S|\}$ be a set of affine points in $\mathrm{PG}(2, q^n)$. Define the Rédei polynomial of S as follows:

$$R(X, Y) = \prod_{i=1}^{|S|}(X - x_i Y + y_i).$$

As usual (see e.g. [2,4]), we will consider the expansion of $R(X, Y)$ using elementary symmetric polynomials. Let $\sigma_i(Y)$ be the i-th elementary symmetric polynomial of the set $\{-x_i Y + y_i | 1 \leq i \leq |S|\}$, then

$$R(X, Y) = X^{|S|} + \sum_{i=1}^{|S|} \sigma_i(Y) X^{|S|-i}.$$

Note that $\deg \sigma_i(Y) \leq i$.

Let y be a slope. Then x is a root of $R(X, y) = 0$ with multiplicity m if and only if the line with equation $xX_0 - yX_1 + X_2 = 0$ contains exactly m points of S.

3. Linear sets of $\mathbf{PG}(1, q^n)$

Substituting the variable Y in $R(X, Y)$ by slopes will provide particular information on the shape of the Rédei polynomial. In the language of direction problems, the next Lemma deals with substitution of a determined slope.

Lemma 3.1. *Let $P = \langle(x_0, f(x_0))\rangle_{q^n}$ be a point of weight j in $L_U = \{\langle(x, f(x))\rangle_{q^n} \mid x \in V^*\}$, then $R(X, y_0)$ with $y_0 = f(x_0)/x_0$ is of the form*

$$R(X, y_0) = \prod_{i=1}^{q^{k-j}} (X - \alpha_i)^{q^j},$$

for distinct $\alpha_i \in \mathbb{F}_{q^n}$.

Proof. Let $P = \langle(x_0, f(x_0))\rangle_{q^n}$ be a point of weight j in $L_U = \{\langle(x, f(x)\rangle_{q^n} | x \in V^*\}$. By definition, P has weight j in L_U if there are q^j elements $\Lambda \in \mathbb{F}_{q^n}$ such that $(\Lambda x, \Lambda f(x))$ is contained in $U = \{(x, f(x)) | x \in V\}$. This implies that

$$f(\Lambda x_0) = \Lambda f(x_0) \tag{1}$$

has q^j solutions for Λ.

Let $x_1 \in V$. For any $\Lambda \in \mathbb{F}_{q^n}$, the point $\langle(1, x_1 + \Lambda x_0, f(x_1) + \Lambda f(x_0))\rangle_{q^n} \in \mathcal{A} \iff$ $f(x_1 + \Lambda x_0) = f(x_1) + \Lambda f(x_0)$ and $x_1 + \Lambda x_0 \in V$. The condition $x_1 + \Lambda x_0 \in V$ is equivalent

with $\Lambda x_0 \in V$, and so the condition $f(x_1 + \Lambda x_0) = f(x_1) + \Lambda f(x_0)$ is equivalent with $f(\Lambda x_0) = \Lambda f(x_0)$.

Hence, the number of points of $\mathcal{A}$ on the line through $\langle (1, x_1, f(x_1)) \rangle_{q^n}$ and $\langle (0, x_0, f(x_0)) \rangle_{q^n}$ equals precisely the number of solutions of Equation (1) (and $\Lambda = 0$ corresponds with the point $\langle (1, x_1, f(x_1)) \rangle_{q^n}$).

By definition, $R(X, y_0) = \prod_{x \in V}(X - xy_0 + f(x))$. Now $X - xy_0 + f(x) = X - x_1y_0 + f(x_1)$ if and only if the points $\langle (1, x, f(x)) \rangle_{q^n}$, $\langle (1, x_1, f(x_1)) \rangle_{q^n}$, and $\langle (0, 1, y_0) \rangle_{q^n}$ are collinear. Hence, the factor $(X - x_1y_0 + f(x_1))$ appears exactly q^j times in $R(X, y_0)$. □

Remark 4. We can also deduce Lemma 3.1 from a more geometrical point of view. Let $L_U = \mathcal{B}(\pi)$, where π is a $(k-1)$-space in $\mathrm{PG}(2n-1, q)$, embed $\mathrm{PG}(2n-1, q)$ as the subspace consisting of all points of the form $\langle (0, y, z) \rangle_q$ in $\mathrm{PG}(3n-1, q)$ and consider L_U as a subset of $\mathrm{PG}(2, q^n)$, contained in the line $X_0 = 0$ (at infinity). Let μ be the subspace spanned by the point $\langle (1, 0, 0) \rangle_q$ of $\mathrm{PG}(3n-1, q)$ and π. Then $\mathcal{B}(\mu) \backslash \mathcal{B}(\pi)$ consists of the q^k points of $\{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$. If $P = \langle (0, x_0, f(x_0)) \rangle_{q^n}$, $x_0 \in V^*$ is a point of weight j in $L_U = \mathcal{B}(\pi)$, this means the spread element S (of the Desarguesian $(n-1)$-spread $\mathcal{S}$) corresponding to P meets π, and hence also μ, in a $(j-1)$-dimensional space. Every line through P in $\mathrm{PG}(2, q^n)$ containing a point $\langle (1, x_0, f(x_0)) \rangle_{q^n}$ of $\{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$ corresponds to a $(2n-1)$-dimensional subspace of $\mathrm{PG}(3n-1, q)$, spanned by spread elements of $\mathcal{S}$, meeting μ in a subspace ν of dimension j. As π is a hyperplane of μ, and $P = \mathcal{B}(\pi \cap \nu)$ this means that the line $\mathcal{B}(\nu)$ contains exactly q^j points of $\{\langle (1, x, f(x)) \mid x \in V \rangle_{q^n}\}$. Hence every line on a point of weight j of L_U that contains a point of $\mathcal{A}$, contains exactly q^j points of $\mathcal{A}$. From the definition of the Rédei polynomial $R(X, Y)$, this is saying exactly that every root of $R(X, y_0)$ has multiplicity exactly q^j, if y_0 is a slope corresponding with a point of weight j of L_U, in other words, every factor of $R(X, y_0)$ has multiplicity q^j.

We are now ready to deduce the shape of the Rédei polynomial of the set $\mathcal{A} = \{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$.

Lemma 3.2. *If $\mathcal{A} = \{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$, where V is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^n}$ of dimension k and $f : V \to \mathbb{F}_{q^n}$ is an $\mathbb{F}_q$-linear map, then the Rédei polynomial of $\mathcal{A}$ is of the following shape:*

$$R(X, Y) = X^{q^k} + \sigma_{q^k - q^{k-1}}(Y) X^{q^{k-1}} + \sigma_{q^k - q^{k-2}}(Y) X^{q^{k-2}} + \ldots + \sigma_{q^k - 1}(Y) X \,. \quad (2)$$

Proof. First consider an element $y_0 \notin \mathcal{D}_{\mathcal{A}}$. Then the set $V_{y_0} = \{-xy_0 + f(x) | x \in V\}$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^n}$ of dimension k. Hence, by [6, Theorem 3.52],

$$R(X, y_0) = \prod_{\beta \in V_{y_0}} (X - \beta) = X^{q^k} + \alpha_1 X^{q^{k-1}} + \alpha_2 X^{q^{k-2}} + \ldots + \alpha_k X \,,$$

with $\alpha_i \in \mathbb{F}_{q^n}$. Then consider an element $y_1 \in \mathcal{D}_{\mathcal{A}}$. By Lemma 3.1, we know that if $\langle (1, y_1) \rangle_{q^n}$ is a point of weight j_1, then $R(X, y_1)$ contains q^{k-j_1} distinct factors, each

of degree q^{j_1}. As before, the set $V_{y_1} = \{-xy_1 + f(x) | x \in V\}$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^n}$, but the number of elements in V_{y_1} is q^{k-j_1}, and hence, the dimension of V_{y_1} is $k - j_1$. We now obtain that

$$R(X, y_1) = \prod_{\beta' \in V_{y_1}} (X - \beta')^{q^j} = (X^{q^{k-j_1}} + \alpha'_1 X^{q^{k-j_1-1}} + \alpha'_2 X^{q^{k-j_1-2}} + \ldots + \alpha'_{k-j_1-1} X)^{q^{j_1}}.$$

We conclude that for all $y \in \mathbb{F}_{q^n}$, $\sigma_i(y) = 0$ if $i \notin \{q^k - q^j | j = 0 \ldots k-1\}$. Since $\deg \sigma_i(Y) \leq i$, each of the polynomials $\sigma_i(Y), i \notin \{q^k - q^j | j = 0 \ldots k-1\}$ has more roots than its degree, and so is identically zero. Also note that since $\langle (1,0,0) \rangle_{q^n} \in \mathcal{A}$, $0 \in \{-x_i Y + y_i | 1 \leq i \leq |\mathcal{A}|\}$, hence $\sigma_{q^k}(Y)$ is identically zero. So $R(X,Y)$ has the shape of (2). □

Remark 5. A set of the form $\mathcal{A} = \{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$, where f is an $\mathbb{F}_q$-linear map and V is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^n}$, is called an *affine $\mathbb{F}_q$-linear set* in [4].

We see that if $R(X,Y)$ is the Rédei polynomial associated with $\{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$ then $R(X,Y)$ is an $\mathbb{F}_q$-linear map in the variable X, and for every $y \in \mathbb{F}_{q^n}$, the map $R(X, y)$ is a linearised polynomial.

The following arguments are based on [4]. We consider the polynomial $R(X,Y)$ as a univariate polynomial in X over the ring $\mathbb{F}_{q^n}[Y]$. Since $R(X,Y)$ is monic, division with remainder of $X^{q^n} - X$ by $R(X,Y)$ can be executed using the ordinary Euclidean division algorithm for polynomials over a field. Hence there exist polynomials $Q(X,Y), r(X,Y) \in \mathbb{F}_{q^n}[Y][X]$ such that

$$X^{q^n} - X = R(X,Y)Q(X,Y) + r(X,Y), \tag{3}$$

with $\deg_X r(X,Y) < \deg_X R(X,Y)$. Since $R(X,Y)$ is monic of degree q^k, we can write

$$Q(X,Y) = X^{q^n - q^k} + \sum_{i=1}^{q^n - q^k} \sigma_i^*(Y) X^{q^n - q^k - i}. \tag{4}$$

For convenience, we define $\sigma_0^*(Y) = 0$.

Lemma 3.3. *Consider the polynomials $Q(X,Y)$ and $r(X,Y)$ from Equation (3). Then $\deg Q(X,Y) \leq q^n$ and $\deg r(X,Y) \leq q^n$ (where $\deg Q(X,Y)$ means the total degree). Furthermore, in Equation (4), $\deg \sigma_i^*(Y) \leq i$.*

Proof. Before starting the Euclidean division with remainder algorithm, $Q(X,Y)$ is initialized as 0 and $r(X,Y)$ is initialized as $X^{q^n} - X$. So let

$$r(X,Y) = \sum_{i=0}^{q^n} \rho_i(Y) X^{q^n - i}. \tag{5}$$

Then initially, $\rho_0(Y) = 1$, $\rho_{q^n-1}(Y) = -1$, and $\rho_i(Y) = 0$ for $i \notin \{0, q^n - 1\}$, so initially $\deg \rho_i(Y) \leq i$ and $\deg r(X,Y) = \deg_X r(X,Y) = q^n$. As induction hypothesis, we assume that after execution of step $j-1 \geq 0$ in the Euclidean algorithm, $\deg r(X,Y) \leq q^n$, $\deg_X r(X,Y) \leq q^n - j$, and $\deg \sigma_i^*(Y) \leq i$ for all $i \leq j-1$.

During step j of the algorithm, (1) $\sigma_j^*(Y)$ is computed and (2) $r(X,Y)$ is changed.

(1) The polynomial $\sigma_j^*(Y)$ becomes the leading coefficient of $r(X,Y)$ if $\deg_X r(X,Y) = q^n - j$ (because $R(X,Y)$ is monic), and 0 otherwise. From the induction hypothesis, $\deg r(X,Y) \leq q^n$ and $\deg_X r(X,Y) \leq q^n - j$, so in both cases $\deg \sigma_j^*(Y) \leq j$.

(2) The remainder $r(X,Y)$ becomes $r(X,Y) - \sigma_j^*(Y) X^{q^n - q^k - j} R(X,Y)$. Since $\deg R(X,Y) = q^k$ and by the induction hypothesis, $\deg \sigma_j^*(Y) \leq j$ and $\deg r(X,Y) \leq q^n$, the total degree of $r(X,Y)$ remains bounded by q^n. Clearly, after executing step j, $\deg_X r(X,Y) \leq q^n - (j+1)$, so $\deg \rho_i(Y) \leq i$ for all admissible i.

By induction we can now conclude that after execution of the algorithm, $\deg r(X,Y) \leq q^n$, $\deg Q(X,Y) \leq q^n$, $\deg \sigma_i^*(Y) \leq i$, and $\deg \rho_i(Y) \leq i$, for all i. □

As in [4], define $H(X,Y) = -r(X,Y) - X$, then

$$X^{q^n} - X = R(X,Y)Q(X,Y) - H(X,Y) - X\,. \tag{6}$$

Corollary 3.4. *Consider the polynomial $H(X,Y)$ from Equation (6). Then $\deg_X H(X,Y) \leq q^k - 1$. Let*

$$H(X,Y) = \sum_{i=0}^{q^n} h_i(Y) X^{q^n - i}\,,$$

then $\deg h_i(Y) \leq i$.

Proof. This follows from $H(X,Y) = -r(X,Y) - X$ and $\deg r(X,Y) \leq q^n$ by Lemma 3.3. □

Remark 6. Since $\deg_X H(X,Y) \leq q^k - 1$, the polynomials $h_i(Y)$ are identically zero for $i \in \{0, \ldots, q^n - q^k + 1\}$. In [4], it is also mentioned how the coefficient polynomials $h_i(Y)$ can be computed from the polynomials $\sigma_i(Y)$ and $\sigma_i^*(Y)$.

The following lemma is essentially Lemma 15 from [4], where the authors prove a similar theorem assuming $\infty \in \mathcal{D}_{\mathcal{A}}$, whereas in our case $\infty \notin \mathcal{D}_{\mathcal{A}}$.

Lemma 3.5. *Let $R(X,Y)$ be the Rédei polynomial of the point set $\mathcal{A} = \{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$, and $H(X,Y)$ the polynomial defined in Equation (6). Then the number of points in $L_U = \{\langle (x, f(x) \rangle_{q^n} \mid x \in V^*\}$ is at least $\deg_X H(X,Y)$.*

Proof. By Lemma 2.2, the number of points in L_U is the number of directions determined by the point set $\mathcal{A} = \{\langle(1, x, f(x))\rangle_{q^n} \mid x \in V\}$, where f is an $\mathbb{F}_q$-linear map and V is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^n}$.

Recall that the slope $y \in \mathcal{D}_\mathcal{A}$ corresponds with the direction $\langle(0, 1, y)\rangle_{q^n}$, and that $\langle(0, 0, 1)\rangle_{q^n}$ is not a direction determined by $\mathcal{A}$. Assume now that $y \notin \mathcal{D}_\mathcal{A}$, then $R(X, y) \mid X^{q^n} - X$, hence $H(X, y) = -X$, from which it follows that $h_i(y) = 0$ for all $i \neq q^n - 1$.

Now assume that $y \in \mathcal{D}_\mathcal{A}$. Then $R(X, y) \nmid X^{q^n} - X$, so there exists an index $j \neq q^n - 1$ such that $h_j(y) \neq 0$, hence $h_j(Y)$ is not identically 0. Define i_0 to be the smallest index such that $h_{i_0}(Y)$ is not identically 0, then

$$i_0 = q^n - \deg_X H(X, Y). \tag{7}$$

The polynomial $h_{i_0}(Y)$ has at least $q^n - |\mathcal{D}_\mathcal{A}|$ roots, so

$$\deg h_{i_0}(Y) \geq q^n - |\mathcal{D}_\mathcal{A}|. \tag{8}$$

From Corollary 3.4, we have that $\deg h_{i_0} \leq i_0$, which implies that $q^n \geq \deg(X^{q^n - i_0} h_{i_0}(Y))$. By Equation (8),

$$\deg(X^{q^n - i_0} h_{i_0}(Y)) = q^n - i_0 + \deg h_{i_0}(Y) \geq 2q^n - |\mathcal{D}_\mathcal{A}| - i_0.$$

Combining the above two inequalities, we obtain that $q^n \geq 2q^n - |\mathcal{D}_\mathcal{A}| - i_0$ and we find by Equation (7) that $|\mathcal{D}_\mathcal{A}| \geq q^n - i_0 = \deg_X H(X, Y)$. □

Remark 7. From Lemma 3.5, we could have deduced that the number of points in L_U is at least $\deg_X H(X, Y) + 1$ (just like in [4]) instead of the slightly weaker lower bound $\deg_X H(X, Y)$ that we now have. However, in order to obtain this improvement, we would have needed to transform our point set so that ∞ is a determined slope. While it is perfectly possible to do so, we chose to avoid doing this as in the proof of Theorem 3.7, we will obtain the same lower bound $\deg_X H(X, Y) + 1$ anyhow.

We will need the following result, which easily follows from the geometric point of view on $\mathbb{F}_q$-linear sets.

Result 3.6. [8] The number of points in an $\mathbb{F}_q$-linear set is congruent to 1 mod q.

Theorem 3.7. *Let $L_U = \{\langle(x, f(x))\rangle_{q^n} \mid x \in V^*\}$, where V has dimension k, be an $\mathbb{F}_q$-linear set in $\mathrm{PG}(1, q^n)$ of rank k which contains at least one point of weight one, then the size of L_U is at least $q^{k-1} + 1$.*

Proof. With $R(X, Y)$ the Rédei-polynomial of $\mathcal{A} = \{\langle(1, x, f(x))\rangle_{q^n} \mid x \in V^*\}$, and $H(X, Y)$ defined as in (6), by Lemma 3.5, we know that the number of points in L_U is at least $\deg_X H(X, Y)$. Let $P = \langle(x_0, f(x_0))\rangle_{q^n}$ be a point of weight one in L_U. By

Lemma 3.1, $R(X, y_0)$ with $y_0 = f(x_0)/x_0$ splits in factors of degree q, and since $R(X, y_0)$ has degree q^k, there are q^{k-1} different factors, each of the form $(X - \alpha_i)^q$ for some $\alpha_i \in \mathbb{F}_{q^n}$, $i = 1, \ldots, q^{k-1}$. Since $X - \alpha_i$ divides $X^{q^n} - X$, it divides $H(X, y) - X$ as well. As we have found at least q^{k-1} different linear factors dividing $H(X, y) - X$, this implies that $\deg_X H(X, Y)$ is at least q^{k-1}. We conclude that the number of points in L_U is at least q^{k-1}, and hence, by Lemma 3.6, at least $q^{k-1} + 1$. □

In Theorem 3.7, we find that the number of points in an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^n)$, containing a point of weight one, is at least $q^{k-1} + 1$. In the following proposition, we see that we can always find an example of such an $\mathbb{F}_q$-linear set, and hence, that this lower bound is sharp.

Proposition 3.8. *Let $2 \leq k \leq n$. There exists an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^n)$ with $q^{k-1} + 1$ elements.*

Proof. As usual, consider the Desarguesian $(n-1)$-spread $\mathcal{S}$ in $\mathrm{PG}(2n-1, q)$. Take a $(k-2)$-space μ contained in a spread element S_1 of $\mathcal{S}$ and let π be a $(k-1)$-space meeting S_1 exactly in μ. Then $\mathcal{B}(\mu)$ has size $q^{k-1} + 1$. □

Remark 8. An example of a set $\mathcal{B}(\pi)$ from Proposition 3.8 can be obtained using coordinates as follows: take $\alpha_0 = 1, \alpha_1, \ldots, \alpha_{n-k}$ to be $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^n}$, let V be the sub space of $\mathbb{F}_{q^n}$ defined by $\mathrm{Tr}(\alpha_i x) = 0$, for $i = 1, \ldots, n-k$ and put $L_U = \{\langle (x, \mathrm{Tr}(x)) \rangle_{q^n} \mid x \in V^*\}$.

However, not every $\mathbb{F}_q$-linear set of size $q^{k-1} + 1$ arises as in Proposition 3.8. For example, in $\mathrm{PG}(1, q^4)$, it is possible to find two non-equivalent $\mathbb{F}_q$-linear sets of rank 4, each containing $q^3 + 1$ points (see Example B1 and C12 of [3]). The example of Proposition 3.8 arises as $\mathcal{B}(\pi)$, where π is a 3-space meeting one element of the Desarguesian 3-spread $\mathcal{S}$ of $\mathrm{PG}(7, q)$ in a plane, and q^3 other elements in a point. The other example arises as $\mathcal{B}(\pi)$ where π meets $q + 1$ elements of a regulus of $\mathcal{S}$ in a line and $q^3 - q$ others in a point.

Remark 9. In [3, Lemma 2.2], the authors prove that a linear set L_U of rank n in $\mathrm{PG}(1, q^n)$ containing at least one point of weight 1 has size at least $q^{n-1} + 1$, and they show that U is spanned by the vectors of U defining the points of weight one in L_U. Now consider a linear set L_U of rank k in $\mathrm{PG}(1, q^n)$ containing at least one point of weight one. By Theorem 3.7, L_U has at least $q^{k-1} + 1$ points. Using this result, it is easy to see that the proof of the second part of [3, Lemma 2.2] goes through for $k < n$, and we obtain that also in this case, U is spanned by the vectors defining the points of weight 1.

Looking at the proof of Theorem 3.7, one might think that for $\mathbb{F}_q$-linear sets of rank k with more than $q^{k-1} + 1$ points, the lower bound on $\deg_X H(X, Y)$ could be improved. This is not the case: we will show in Corollary 3.10 that $\deg_X H(X, Y)$ is independent of the choice of the $\mathbb{F}_q$-linear set of rank k (as long as it has a point of weight one).

For this, we need the *symbolic* product of linearised polynomials, which is defined as their composition and denoted by $\circ$. More precisely, let $F(x)$ and $G(x)$ be two $\mathbb{F}_q$-linearised polynomials, then

$$(F \circ G)(x) := F(G(x)) \mod x^{q^n} - x.$$

Unlike the ordinary product of two linearised polynomials, the composition of two linearised polynomials is again a linearised polynomial. A linearised polynomial $G(x)$ is called a (right) symbolic divisor of a linearised polynomial $F(x)$ if $F(x) = Q(x) \circ G(x)$ for some linearised polynomial $Q(x)$. With respect to symbolic (right) division, one can execute Euclid's algorithm (see [7]). So for any two linearised polynomials $F(x)$ and $G(x)$ with $\deg(G) \leq \deg(F)$, there are linearised polynomials $Q(x)$ and $H(x)$ with $\deg(H) < \deg(G)$, such that

$$F(x) = Q(x) \circ G(x) + H(x). \tag{9}$$

Proposition 3.9. *Let $\mathcal{A} = \{\langle (1, x, f(x)) \rangle_{q^n} \mid x \in V\}$, where f is an $\mathbb{F}_q$-linear map and V is a k-dimensional subspace of $\mathbb{F}_{q^n}$. Let R be the Rédei-polynomial of $\mathcal{A}$, and Q and H as in Equation (6). Then $\deg_X H(X, Y)$ is a power of q.*

Proof. Pick an element $y \in \mathbb{F}_{q^n}$ and write $R_y(X) = R(X, y)$. By Lemma 3.2, $R(X, y)$ is a linearised polynomial. Note that $X^{q^n} - X$ is a linearised polynomial as well. So we can symbolically divide $X^{q^n} - X$ by $R_y(X)$ and find (see Equation (9)):

$$X^{q^n} - X = \widetilde{Q}_y(X) \circ R_y(X) + \widetilde{H}_y(X) = \widetilde{Q}_y(X) \circ R_y(X) - H'_y(X) - X,$$

for some linearised polynomials $\widetilde{Q}_y(X)$ and $\widetilde{H}_y(X)$ where $\deg H' \leq \deg \widetilde{H} < \deg R_y$. Note that $H'_y(X) = -\widetilde{H}_y(X) - X$ is a linearised polynomial as well and that the polynomials $\widetilde{Q}_y$ and H'_y are dependent on the choice of y.

Write $\widetilde{Q}_y(X) = \sum_{i=0}^{n-k} \widetilde{Q}_{y,i} X^{q^i}$. Now

$$\begin{aligned} X^{q^n} - X &= \widetilde{Q}_y(X) \circ R_y(X) - H'_y(X) - X \\ &= \widetilde{Q}_y(R_y(X)) - H'_y(X) - X \\ &= \sum_{i=0}^{n-k} \widetilde{Q}_{y,i} (R_y(X))^{q^i} - H'_y(X) - X \\ &= R_y(X) \sum_{i=0}^{n-k} \widetilde{Q}_{y,i} (R_y(X))^{q^i - 1} - H'_y(X) - X \end{aligned}$$

We find that

$$X^{q^n} - X = R_y(X) \sum_{i=0}^{n-k} \widetilde{Q}_{y,i}(R_y(X))^{q^i-1} - H'_y(X) - X = R_y(X)Q'_y(X) - H'_y(X) - X$$

where we defined $Q'_y(X) = \sum_{i=0}^{n-k} \widetilde{Q}_{y,i}((R_y(X))^{q^i-1}$.

However, we know that, for a fixed y,

$$X^{q^n} - X = R_y(X)Q(X,y) - H(X,y) - X.$$

This implies that for every $y \in \mathbb{F}_{q^n}$,

$$X^{q^n} - X = R_y(X)Q(X,y) - H(X,y) - X = R_y(X)Q'_y(X) - H'_y(X) - X,$$

or

$$R_y(X)(Q(X,y) - Q'_y(X)) = H(X,y) - H'_y(X).$$

But, if the polynomials in this equation are non-zero polynomials, then the degree of the left hand side is at least $\deg_X R(X,Y)$ and the degree of the right hand side is less than $\deg_X R(X,Y)$ since H and H' have degrees less than $\deg_X R(X,Y)$. Hence, for all y,

$$Q(X,y) = Q'_y(X) \text{ and } H(X,y) = H'_y(X).$$

Since for all $y \in \mathbb{F}_{q^n}$, $H(X,y) = H'_y(X)$ is a linearised polynomial in the variable X, and $\deg H(X,Y) < q^n$ (see Corollary 3.4), we have that $H(X,y)$ is a linearised polynomial which means that $\deg_X H(X,Y) = q^i$ for some i. □

Corollary 3.10. *Let $L_U = \{\langle (x, f(x))\rangle_{q^n} \mid x \in V^*\}$ be an $\mathbb{F}_q$-linear set of rank k containing a point of weight 1. Let $\mathcal{A} = \{\langle (1, x, f(x))\rangle_{q^n} \mid x \in V\}$, let R be the Rédei polynomial of $\mathcal{A}$ and let Q and H be as in Equation (6). Then $\deg_X H(X,Y) = q^{k-1}$.*

Proof. By Proposition 3.9, $\deg_X H(X,Y)$ is a power of q. But $\deg_X H(X,Y) < \deg_X R(X,Y) = q^k$, which shows that $\deg_X H(X,Y) \leq q^{k-1}$. In the proof of Theorem 3.7, we have seen that $\deg_X H(X,Y)$ is at least q^{k-1}. Hence, $\deg_X H(X,Y) = q^{k-1}$. □

4. The size of an $\mathbb{F}_q$-linear (blocking) set in $\mathbf{PG}(2, q^n)$

In this section, we will extend the results found for linear sets on a line in Theorem 3.7, to linear sets in a plane. Note that the hypothesis in the next theorem implies that the linear set is not contained in a line.

Theorem 4.1. *Let L be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(2,q^n)$ such that there is at least one line of $\mathrm{PG}(2,q^n)$ meeting L in exactly $q+1$ points, then L contains at least $q^{k-1}+q^{k-2}+1$ points.*

Proof. As usual, let $\mathcal{S}$ be the Desarguesian $(n-1)$-spread in $\mathrm{PG}(3n-1,q)$. Recall that we identify a point of $\mathrm{PG}(2,q^n)$ with its corresponding element of $\mathcal{S}$.

Let $L=\mathcal{B}(\pi)$, where π is a $(k-1)$-dimensional subspace of $\mathrm{PG}(3n-1,q)$. Let p_1 and p_2 be points of π such that the line $T=\langle\mathcal{B}(p_1),\mathcal{B}(p_2)\rangle$ of $\mathrm{PG}(2,q^n)$ meets $\mathcal{B}(\pi)$ in $q+1$ points (these are then exactly the $q+1$ points of the form $\mathcal{B}(r)$ with r a point of the line p_1p_2 in $\mathrm{PG}(3n-1,q)$). Let $\widetilde{T}$ be the $(2n-1)$-space of $\mathrm{PG}(3n-1,q)$ corresponding to T, i.e., the subspace of $\mathrm{PG}(3n-1,q)$ spanned by the spread elements $\mathcal{B}(p_1)$ and $\mathcal{B}(p_2)$.

Consider a line M of $\mathrm{PG}(2,q^n)$ through the point $\mathcal{B}(p_2)$, but not containing the point $\mathcal{B}(p_1)$. Then M corresponds to a $(2n-1)$-dimensional subspace $\widetilde{M}$ of $\mathrm{PG}(3n-1,q)$ which is spanned by spread elements of $\mathcal{S}$. Project π from p_1 onto $\widetilde{M}$. Since $\mathcal{B}(p_1)$, the spread element through p_1, meets π in a point, the projection μ of the $(k-1)$-space π from p_1 onto $\widetilde{M}$ is $(k-2)$-dimensional. Let π' be the $(k-1)$-dimensional subspace of $\mathrm{PG}(3n-1,q)$ spanned by p_1 and μ. The $\mathbb{F}_q$-linear set $\mathcal{B}(\pi')$ clearly contains $q^{k-1}+|\mathcal{B}(\mu)|$ points. Now $\mathcal{B}(\mu)$ contains the point $\mathcal{B}(p_2)$. The intersection of the spread element through p_2 with μ is precisely the projection of the intersection of the $(2n-1)$-dimensional space $\widetilde{T}$ with π. We know that $\widetilde{T}$ meets $\pi=\langle p_1,\mu\rangle$ in the line p_1p_2 so it follows that the spread element through p_2 meets μ only in the point p_2. Hence, $\mathcal{B}(p_2)$ is a point of weight 1 in $\mathcal{B}(\mu)$ and by Theorem 3.7, $\mathcal{B}(\mu)$ has size at least $q^{k-2}+1$. Since $\mathcal{B}(\pi')$ contains $q^{k-1}+|\mathcal{B}(\mu)|$ points, this shows that $\mathcal{B}(\pi')$ has at least $q^{k-1}+q^{k-2}+1$ points.

Now consider a line N of $\mathrm{PG}(2,q^n)$ through $\mathcal{B}(p_1)$ and a point of $\mathcal{B}(\pi)$, different from $\mathcal{B}(p_1)$. The number of points of $\mathcal{B}(\pi)$ on N is the number of points of $\mathcal{B}(\pi\cap\widetilde{N})$, where $\widetilde{N}$ is the $(2n-1)$-dimensional subspace of $\mathrm{PG}(3n-1,q)$ corresponding to N. Let $\nu=\pi\cap\widetilde{N}$, and suppose that ν is r-dimensional, then $\mathcal{B}(p_1)$ is a point of weight 1 in $\mathcal{B}(\nu)$ and by Theorem 3.7, $\mathcal{B}(\nu)$ has at least $q^{r-1}+1$ points. Note that ν is r-dimensional, and hence, π' meets $\widetilde{N}$ in an r-dimensional space. By construction, this means that $\pi'\cap\widetilde{N}\cap\widetilde{M}$ is $(r-1)$-dimensional, and $\mathcal{B}(\pi'\cap\widetilde{N})$ has exactly q^r+1 points. Hence, for every line N through $\mathcal{B}(p_1)$, the number of points of $\mathcal{B}(\pi)\cap N$ is at least the number of points of $\mathcal{B}(\pi')\cap N$. We conclude that the number of points in $\mathcal{B}(\pi)$ is at least the number of points in $\mathcal{B}(\pi')$, which is at least $q^{k-1}+q^{k-2}+1$. □

Just as in Proposition 3.8, it is easy to see that the bound in Theorem 4.1 is sharp.

Proposition 4.2. *Let $3\leq k\leq n$. There exists an $\mathbb{F}_q$-linear set S of rank k in $\mathrm{PG}(2,q^n)$ with $q^{k-1}+q^{k-2}+1$ elements such that there is a line meeting S in exactly $q+1$ points.*

Proof. Let $\mathcal{S}$ be the Desarguesian $(n-1)$-spread in $\mathrm{PG}(3n-1,q)$. Let μ be a $(k-3)$-space of a spread element $\mathcal{B}(p)$ of $\mathcal{S}$. Consider a line N in $\mathrm{PG}(2,q^n)$ skew from $\mathcal{B}(p)$ and let $\widetilde{N}$ be the $(2n-1)$-dimensional subspace of $\mathrm{PG}(3n-1,q)$ corresponding to N. Let ℓ be a

line of $\widetilde{N}$, not contained in an element of $\mathcal{S}$. Then $\langle \mu, \ell \rangle$ is a $(k-1)$-dimensional subspace of $\mathrm{PG}(3n-1,q)$, so $\mathcal{B}(\langle \mu, \ell \rangle)$ is an $\mathbb{F}_q$-linear set of rank k. By construction, it spans $\mathrm{PG}(2,q^n)$, contains $q^{k-1}+q^{k-2}+1$ points and meets N in exactly $q+1$ points. □

4.1. Concluding remarks

One particular instance for which the question of finding the minimum size of a linear set is very relevant, is for linear sets of rank n in $\mathrm{PG}(2,q^n)$. In this case, the $\mathbb{F}_q$-linear set defines a minimal *blocking set*. A blocking set in $\mathrm{PG}(2,q^n)$ is a set B of points such that every line of $\mathrm{PG}(2,q^n)$ meets B in at least 1 point. If a blocking set in $\mathrm{PG}(2,q^n)$ does not contain a line, it is called *non-trivial* and if it contains less than $3(q^n+1)/2$ points, it is called *small*. It is conjectured (see [9, Conjecture 3.1]) that all *small* minimal blocking sets in $\mathrm{PG}(2,q^n)$ are $\mathbb{F}_p$-linear sets where q is a power of the prime p. In the same paper, the author conjectures the following:

Conjecture 4.3. *[9, p. 1170] Let p be a prime. If $\mathbb{F}_{p^e}$ is the "maximum field of linearity" then a non-trivial blocking set in $\mathrm{PG}(2,p^t)$, with $t=en$, has at least $(p^e)^n+(p^e)^{n-1}+1$ points.*

The notion "maximum field of linearity" is used by Sziklai to indicate the following: the maximum field of linearity of a blocking set in $\mathrm{PG}(2,p^t)$ is $\mathbb{F}_{p^e}$ if and only if every line meets the blocking set in 1 mod p^e points, but not every line meets in 1 mod p^{e+1} points. The fact that e is a divisor of t, and hence, that there is a subfield $\mathbb{F}_{p^e}$ of $\mathbb{F}_{p^t}$ follows from his work on blocking sets, but it does not necessarily hold for linear sets in general (see Remark 12).

Remark 10. In Theorem 4.1, we proved that an $\mathbb{F}_q$-linear set of rank k that contains a $(q+1)$-secant, contains at least $q^{k-1}+q^{k-2}+1$ points. It is clear if an $\mathbb{F}_q$-linear set contains a $(q+1)$-secant, then the maximum field of linearity is indeed $\mathbb{F}_q$. In [9, Corollary 5.2], the author also shows the converse for blocking sets with respect to k-spaces in $\mathrm{PG}(r-1,q^n)$: if the maximum field of linearity is $\mathbb{F}_{p^e}$, then there are (many) (p^e+1)-secants to the set. This observation shows that assuming that there is $(q+1)$-secant in the case of an $\mathbb{F}_q$-linear blocking set in $\mathrm{PG}(2,q^n)$, is equivalent to assuming that the maximum field of linearity is $\mathbb{F}_q$. So we see that if the linearity conjecture for blocking sets holds, then Theorem 4.1 proves Conjecture 4.3.

Remark 11. We know that every linear set L_U can be written as a linear set $L_{U'}$ that contains at least one point of weight 1. However, in Theorem 4.1, we cannot replace the condition "there is a $(q+1)$-secant" with the condition "containing a point of weight 1" which we used in Theorem 3.7. For example, a subplane $\mathrm{PG}(2,q^2)$ of $\mathrm{PG}(2,q^4)$ can be written as $\mathcal{B}(\mu)$ where μ is a 4-space in $\mathrm{PG}(11,q)$ that meets a certain 7-dimensional space spanned by elements of $\mathcal{S}$ in a 3-space π which intersects every element of $\mathcal{S}$ in a

line. We see that $\mathcal{B}(\mu)$ has $q^4+q^2+1 < q^4+q^3+1$ elements, and does contain q^4 points of weight one. Note that in this case, the maximum field of linearity is $\mathbb{F}_{q^2}$.

Remark 12. Note that, for general sets, from the condition "every line meets a set in 1 mod p^e points, but not every line meets in 1 mod p^{e+1} points" does not need to follow that e is a divisor of t, and hence, that $\mathbb{F}_{p^t}$ has a subfield $\mathbb{F}_{p^e}$. For an example of this behaviour, consider L to be a subline $\mathrm{PG}(1,q^3)$ in $\mathrm{PG}(1,q^9)$. By field reduction, L corresponds to a set T of q^3+1 elements of a Desarguesian 8-spread $\mathcal{S}$ in $\Pi=\mathrm{PG}(17,q)$ such that there is a 5-dimensional space μ of $\mathrm{PG}(17,q)$ meeting each element of T in a plane (the q^3+1 planes form a Desarguesian subspread of μ). Now let μ' be a hyperplane of μ, then $\mathcal{B}(\mu')$ consists of the q^3+1 elements of T; there is one element of T that meets μ' in a plane, and all other elements of T meet μ' in a line. Now embed Π in $\mathrm{PG}(26,q)$ and extend the Desarguesian spread $\mathcal{S}$ in Π to a Desarguesian 8-spread in $\mathrm{PG}(26,q)$. Take π to be a 5-space that meets Π in μ'. Then $\mathcal{B}(\pi)$ is an $\mathbb{F}_q$-linear set in $\mathrm{PG}(2,q^9)$ of rank 6 which has size $q^5+q^3+1 < q^5+q^4+1$. Moreover, a line through two points of $\mathcal{B}(\pi)$ meets $\mathcal{B}(\pi)$ in 1 mod q^2 points, and there are $(1+q^2)$-secants to this set. However, 2 is not a divisor of 9. Note that in this case, $\mathcal{B}(\mu')$ has only points of weight at least 2.

Remark 13. Remark 12 leads us to a crucial point for a possible extension of Theorem 4.1 to general dimension, without having to impose heavy conditions on the point set as in Theorem 4.4. Namely, it would be useful to deduce whether or not the following holds: if an $\mathbb{F}_q$-linear set L_U of rank k has only points of weight at least 2, is it then true that L_U is an $\mathbb{F}_{q^i}$-linear set for some $i>1$? It follows from [2] that this statement is true for $\mathbb{F}_q$-linear sets of rank n in $\mathrm{PG}(1,q^n)$.

If we impose the assumption that there is a hyperplane of $\mathrm{PG}(r-1,q^n)$ that meets the linear set in $\frac{q^{r-1}-1}{q-1}$ points that span this hyperplane, then it is clear that we can repeat the argument of Theorem 4.1 and, by induction, obtain the following Theorem:

Theorem 4.4. *Let L be an $\mathbb{F}_q$-linear set of rank k spanning $\mathrm{PG}(r-1,q^n)$ (hence $k\geq r$) such that there is at least one hyperplane Π of $\mathrm{PG}(r-1,q^n)$ meeting L in exactly $\frac{q^{r-1}-1}{q-1}$ points which span Π, then L contains at least $q^{k-1}+q^{k-2}+\ldots+q^{k-r+1}+1$ points.*

Of course, ideally, we would like to obtain a lower bound for $\mathbb{F}_q$-linear sets of rank k which span $\mathrm{PG}(r-1,q^n)$, where this condition is removed and replaced by a different condition.

Remark 14. In the case $r=3$, the imposed condition for Theorem 4.1 is that there is one line meeting the linear set in an $\mathbb{F}_q$-subline. It is not clear to the authors whether it is possible to have an $\mathbb{F}_q$-linear set L in $\mathrm{PG}(2,q^n)$ with the following properties: L does not admit a $(q+1)$-secant, every line that meets L, meets it in 1 mod q points and there is a line meeting L that does not meet in 1 mod q^2 points. As said before, it follows from

the work of [9, Corollary 5.2] for blocking sets that it is only possible for this situation to occur for $\mathbb{F}_q$-linear sets of rank $k < n$.

Acknowledgments

Jan De Beule acknowledges the Research Foundation Flanders (Belgium) (FWO) for a travel grant (grant number K202718N), and the Fund Professor Frans Wuytack of Ghent University for a research grant.

References

[1] S. Ball, The number of directions determined by a function over a finite field, J. Combin. Theory Ser. A 104 (2) (2003) 341–350.
[2] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, 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] G. Bonoli, O. Polverino, $\mathbb{F}_q$-linear blocking sets in PG$(2, q^4)$, Innov. Incidence Geom. 2 (2005) 35–56.
[4] Sz.L. Fancsali, P. Sziklai, M. Takáts, The number of directions determined by less than q points, J. Algebraic Combin. 37 (1) (2013) 27–37.
[5] M. Lavrauw, G. Van de Voorde, On linear sets on a projective line, Des. Codes Cryptogr. 56 (2–3) (2010) 89–104.
[6] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983, with a foreword by P.M. Cohn.
[7] O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc. 35 (3) (1933) 559–584.
[8] O. Polverino, Linear sets in finite projective spaces, Discrete Math. 310 (22) (2010) 3096–3107.
[9] P. Sziklai, On small blocking sets and their linearity, J. Combin. Theory Ser. A 115 (7) (2008) 1167–1182.