The number of directions determined by less than q points

Szabolcs L. Fancsali, Peter Sziklai and Marcella Takáts*

February 28, 2012

Abstract

In this article we prove a theorem about the number of directions determined by less then q affine points, similar to the result of Blokhuis et. al. [3] on the number of directions determined by q affine points.

1 Introduction

In this article, p is a prime and $q = p^h$, where $h \geq 1$. $\mathsf{GF}(q)$ denotes the finite field with q elements, and $\mathbb{F}$ can denote an arbitrary field (or maybe a Euclidean ring). $\mathsf{PG}(d, q)$ denotes the projective geometry of dimension d over the finite field $\mathsf{GF}(q)$. $\mathsf{AG}(d, q)$ denotes the affine geometry of dimension d over $\mathsf{GF}(q)$ that corresponds to the co-ordinate space $\mathsf{GF}(q)^d$ of rank d over $\mathsf{GF}(q)$.

For the affine and projective planes $\mathsf{AG}(2, q) \subset \mathsf{PG}(2, q)$, we imagine the line $\ell_\infty = \mathsf{PG}(2, q) \setminus \mathsf{AG}(2, q)$ at infinity as the set $\ell_\infty \cong \mathsf{GF}(q) \cup \{\infty\}$. So the *non-vertical directions* are field-elements (numbers) and the *vertical direction* is ∞.

The original problem of direction sets was the following. Let $f : \mathsf{GF}(q) \to \mathsf{GF}(q)$ be a function and let $\mathcal{U} = \{(x, f(x)) \mid x \in \mathsf{GF}(q)\} \subseteq \mathsf{AG}(2, q)$ be the graph of the function f. The question is, how many *directions* can be *determined* by the graph of f.

*The authors were partially supported by the following grants: OTKA K 81310 and OTKA CNK 77780, ERC, Bolyai and TÁMOP 4.2.1./B-09/KMR-2010-0003

Definition (Direction set)**.** If $\mathcal{U}$ denotes an arbitrary set of points in the affine plane $\mathsf{AG}(2,q)$ then we say that the set

$$\mathcal{D} = \left\{ \frac{b-d}{a-c} \;\middle|\; (a,b),(c,d) \in \mathcal{U}, (a,b) \neq (c,d) \right\}$$

is the *set of directions determined by* $\mathcal{U}$. We define $\frac{a}{0}$ as ∞ if $a \neq 0$, thus $\mathcal{D} \subseteq \mathsf{GF}(q) \cup \{\infty\}$. If $\mathcal{U}$ is the graph of a function, then it simply means that $|\mathcal{U}| = q$ and $\infty \notin \mathcal{D}$.

In [1], Simeon Ball proved a stronger version of the structure theorem of Aart Blokhuis, Simeon Ball, Andries Brouwer, Leo Storme and Tamás Szőnyi, published in [3]. To recall their result we need some definitions.

Definition. Let $\mathcal{U}$ be a set of points of $\mathsf{AG}(2,q)$. If $y \in \ell_\infty$ is an arbitrary direction, then let $s(y)$ denote the greatest power of p such that each line ℓ of direction y meets $\mathcal{U}$ in zero modulo $s(y)$ points. In other words,

$$s(y) = \gcd\left(\left\{ |\ell \cap \mathcal{U}| \;\middle|\; \ell \cap \ell_\infty = \{y\} \right\} \cup \left\{ p^h \right\} \right).$$

Let s be the greatest power of p such that each line ℓ of direction in $\mathcal{D}$ meets $\mathcal{U}$ in zero modulo s points. In other words,

$$s = \gcd_{y \in \mathcal{D}} s(y) = \min_{y \in \mathcal{D}} s(y).$$

Note that $s(y)$ and thus also s might be equal to 1. Note that $s(y) = 1$ for each non-determined direction $y \notin \mathcal{D}$.

Remark 1. Suppose that $s \geq p$. Then for *each* line $\ell \subset \mathsf{PG}(2,q)$:

either	$(\mathcal{U} \cup \mathcal{D}) \cap \ell \;= \emptyset;$
or	$\lvert(\mathcal{U} \cup \mathcal{D}) \cap \ell\rvert \equiv 1 \pmod{s}.$

Moreover, $|\mathcal{U}| \equiv 0 \pmod{s}$.

(If $s = 1$ then $0 \equiv 1 \pmod{s}$, so in this case these remarks above would be meaningless.)

Proof. Fix a direction $y \in \mathcal{D}$. Each affine line with slope y meets $\mathcal{U}$ in zero modulo s points, so $|\mathcal{U}| \equiv 0 \pmod{s}$.
An affine line $L \subset \mathsf{AG}(2,q)$ with slope $y \in \mathcal{D}$ meets $\mathcal{U}$ in $0 \pmod{s}$ points, so the *projective* line $\ell = L \cup \{y\}$ meets $\mathcal{U} \cup \mathcal{D}$ in $1 \pmod{s}$ points.
An affine line $L \subset \mathsf{AG}(2,q)$ with slope $y \notin \mathcal{D}$ meets $\mathcal{U}$ in at most one point, so the *projective* line $\ell = L \cup \{y\}$ meets $\mathcal{U} \cup \mathcal{D}$ in either zero or one point.

Let $P \in \mathcal{U}$ and let $L \subset \mathsf{AG}(2,q)$ an affine line with slope $y \in \mathcal{D}$, such that $P \in L$. Then the *projective* line $\ell = L \cup \{y\}$ meets $\mathcal{U}$ in 0 (mod s) points, and thus, ℓ meets $\mathcal{D} \cup \mathcal{U} \setminus \{P\}$ also in 0 (mod s) points. Thus, considering all the lines through P (with slope in $\mathcal{D}$), we get $|\mathcal{U} \cup \mathcal{D}| \equiv 1 \pmod{s}$. Since $\mathcal{U}$ has 0 (mod s) points, $|\mathcal{D}| \equiv 1 \pmod{s}$. So we get that $\mathcal{U} \cup \mathcal{D}$ meets also the ideal line in 1 (mod s) points. ■

Remark 2 (Blocking set of Rédei type)**.** If $|\mathcal{U}| = q$ then each of the q affine lines with slope $y \notin \mathcal{D}$ meets $\mathcal{U}$ in exactly one point, so $\mathcal{B} = \mathcal{U} \cup \mathcal{D}$ is a blocking set meeting each projective line in 1 (mod s) points. Moreover, if $\infty \notin \mathcal{D}$ then $\mathcal{U}$ is the graph of a function, and in this case the blocking set $\mathcal{B}$ above is called *of Rédei type*.

Theorem 3 (Blokhuis, Ball, Brouwer, Storme and Szőnyi; and Ball)**.** [3] and [1, Theorem 1.1] *Let $|\mathcal{U}| = q$ and $\infty \notin \mathcal{D}$. Using the notation s defined above, one of the following holds:*

either	$s = 1$	*and*	$\frac{q+3}{2} \le \lvert\mathcal{D}\rvert \le q$;
or	$\mathsf{GF}(s)$ *is a subfield of* $\mathsf{GF}(q)$	*and*	$\frac{q}{s} + 1 \le \lvert\mathcal{D}\rvert \le \frac{q-1}{s-1}$;
or	$s = q$	*and*	$\lvert\mathcal{D}\rvert = 1$.

Moreover, if $s > 2$ then $\mathcal{U}$ is a $\mathsf{GF}(s)$-linear affine set (of rank $\log_s q$). ■

Definition (Affine linear set)**.** A $\mathsf{GF}(s)$*-linear affine set* is the $\mathsf{GF}(s)$-linear span of some vectors in $\mathsf{AG}(n,q) \cong \mathsf{GF}(s^{\log_s q})^n \cong \mathsf{GF}(s)^{n \log_s q}$ (or possibly a translate of such a span). The *rank* of the affine linear set is the rank of this span over $\mathsf{GF}(s)$.

What about the directions determined by an affine set $\mathcal{U} \subseteq \mathsf{AG}(2,q)$ of cardinality *not* q? Using the pigeon hole principle, one can easily prove that if $|\mathcal{U}| > q$ then it determines all the $q+1$ directions. So we can restrict our research to affine sets of *less than* q points.

Examining the case $q = p$ prime, Tamás Szőnyi [7] and later (independently) also Aart Blokhuis [2] have proved the following result.

Theorem 4 (Szőnyi; Blokhuis)**.** [7, Theorem 5.2] *Let $q = p$ prime and suppose that $1 < |\mathcal{U}| \le p$. Also suppose that $\infty \notin \mathcal{D}$. Then*

either			$\frac{\lvert\mathcal{U}\rvert+3}{2} \le \lvert\mathcal{D}\rvert \le p$;
or	$\mathcal{U}$ *is collinear*	*and*	$\lvert\mathcal{D}\rvert = 1$.

Moreover, these bounds are sharp. ■

In this article we try to generalize this result to the $q = p^h$ prime *power* case by proving an analogue of **Theorem 3** for the case $|\mathcal{U}| \leq q$. Before we examine the number of directions determined by less than q affine points in the plane, we ascend from the plane in the next section and examine the connection between linear sets and direction sets in arbitrary dimensions. The further sections will return to the plane.

2 Linear sets as direction sets

The affine space $\mathsf{AG}(n,q)$ and its ideal hyperplane $\Pi_\infty \cong \mathsf{PG}(n-1,q)$ of directions together constitute a projective space $\mathsf{PG}(n,q)$. We say that the point $P \in \Pi_\infty$ is a direction determined by the affine set $\mathcal{U} \subset \mathsf{AG}(n,q)$ if there exists at least one line through P that meets $\mathcal{U}$ in at least two points.

Definition (Projective linear set)**.** Suppose that $\mathsf{GF}(s)$ is a subfield of $\mathsf{GF}(q)$. A *projective* $\mathsf{GF}(s)$*-linear set* $\mathcal{B}$ of rank $d+1$ is a projected image of the canonical subgeometry $\mathsf{PG}(d,s) \subset \mathsf{PG}(d,q)$ from a center disjoint to this subgeometry. The projection can yield multiple points.

Proposition 5. *Suppose that* $\mathcal{U}$ *is an affine* $\mathsf{GF}(s)$*-linear set of rank* $d+1$ *in* $\mathsf{AG}(n,q)$ *such that* $\mathsf{AG}(n,q)$ *is the smallest dimensional affine subspace that contains* $\mathcal{U}$*. Let* $\mathcal{D}$ *denote the set of directions determined by* $\mathcal{U}$*. The set* $\mathcal{U} \cup \mathcal{D}$ *is a projective* $\mathsf{GF}(s)$*-linear set of rank* $d+1$ *in* $\mathsf{PG}(n,q)$ *and all the multiple points are in* $\mathcal{D}$*.*

Proof. Without loss of generality, we can suppose that $\mathcal{U}$ contains the origin and suppose that $\mathcal{U}$ is the set of $\mathsf{GF}(s)$-linear combinations of the vectors $\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_d$. We can coordinatize $\mathsf{AG}(n,q)$ such that $\mathbf{a}_{d-n+1}, \ldots, \mathbf{a}_d$ is the standard basis of $\mathsf{GF}(q)^n \cong \mathsf{AG}(n,q)$.
Embed $\mathsf{GF}(q)^n \cong \mathsf{AG}(n,q)$ into $\mathsf{GF}(q)^{d+1} \cong \mathsf{AG}(d+1,q)$ such that $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{d-n}, \mathbf{a}_{d-n+1}, \ldots, \mathbf{a}_d$ is the standard basis. Let π denote the projection of $\mathsf{AG}(d+1,q)$ onto $\mathsf{AG}(n,q)$ such that $\pi(\mathbf{z}_i) = \mathbf{a}_i$ for each $i = 0, \ldots, d-n$ and $\pi(\mathbf{a}_j) = \mathbf{a}_j$ for each $j > d-n$. Then $\mathcal{U}$ is the image of the canonical subgeometry $\mathsf{AG}(d+1,s)$ by π.
Extend π to the ideal hyperplane. The extended $\bar{\pi}$ is a collineation so the image of a determined direction is a determined direction, and vice versa, let A and B two arbitrary distinct points in $\ell \cap \mathcal{U}$ and let P be the direction determined by $\pi^{-1}(A)$ and $\pi^{-1}(B)$. Then the direction of ℓ is $\bar{\pi}(P)$. ■

Corollary 6. *If* $\mathcal{D}$ *is the set of directions determined by an affine* $\mathsf{GF}(s)$*-linear set, then* $\mathcal{D}$ *is a projective* $\mathsf{GF}(s)$*-linear set.* ■

Remark 7. In [4, Proposition 2.2], Olga Polverino proved that if $\mathcal{D}$ is a projective $\mathsf{GF}(s)$-linear set then $|\mathcal{D}| \equiv 1 \pmod{s}$. ■

The proposition above says that the set of directions determined by an affine linear set is a projective linear set. The converse of this proposition is also true; each projective linear set is a direction set:

Theorem 8. *Embed* $\mathsf{PG}(n,q)$ *into* $\mathsf{PG}(n+1,q)$ *as the ideal hyperplane and let* $\mathsf{AG}(n+1,q) = \mathsf{PG}(n+1,q) \setminus \mathsf{PG}(n,q)$ *denote the affine part.* For each *projective* $\mathsf{GF}(s)$*-linear set* $\mathcal{D}$ *of rank* $d+1$ *in* $\mathsf{PG}(n,q)$*, there exists an* affine $\mathsf{GF}(q)$*-linear set* $\mathcal{U}$ *of rank* $d+1$ *in* $\mathsf{AG}(n+1,q)$ *such that the set of directions determined by* $\mathcal{U}$ *is* $\mathcal{D}$*.*

Proof. $\mathcal{D} \subset \mathsf{PG}(n,q)$ is the image of the canonical subgeometry $\mathsf{PG}(d,s) \subset \mathsf{PG}(d,q)$ by the projection $\pi : \mathsf{PG}(d,q) \to \mathsf{PG}(n,q)$ where the center C of π is disjoint to this subgeometry. Embed $\mathsf{PG}(d,q)$ into $\mathsf{PG}(d+1,q)$ as the ideal hyperplane and extend π to $\bar{\pi} : \mathsf{PG}(d+1,q) \to \mathsf{PG}(n+1,q)$ such that its center remains C. That is, the center is in the ideal hyperplane. Consider the canonical subgeometry $\mathsf{PG}(d+1,s) \subset \mathsf{PG}(d+1,q)$ and its image by $\bar{\pi}$.

$$\begin{array}{ccccc} \mathsf{PG}(d+1,s) & \xrightarrow{\subset} & \mathsf{PG}(d+1,q) & \xrightarrow{\bar{\pi}} & \mathsf{PG}(n+1,q) \\ \downarrow & & \downarrow & & \downarrow \\ \mathsf{PG}(d,s) & \xrightarrow{\subset} & \mathsf{PG}(d,q) & \xrightarrow{\pi} & \mathsf{PG}(n,q) \end{array}$$

The 'ideal part' of this canonical subgeometry $\mathsf{PG}(d,s)$ is the original canonical subgeometry $\mathsf{PG}(d,s)$ of $\mathsf{PG}(d,q)$ and the projection $\bar{\pi}$ project this onto $\mathcal{D}$. Since the center is totally contained in the ideal hyperplane, $\bar{\pi}$ maps the affine part of the canonical subgeometry $\mathsf{PG}(d+1,s)$ one-to-one.
The directions determined by the affine part of $\mathsf{PG}(d+1,s)$ are the points of $\mathsf{PG}(d,s)$ in the ideal hyperplane of $\mathsf{AG}(d+1,q)$. Since the extended $\bar{\pi}$ preserves collinearity, the set of directions determined by the projected image of the affine part is $\mathcal{D}$. ■

3 The Rédei polynomial of less than q points

Let $\mathcal{U}$ be a set of less than q affine points in $\mathsf{AG}(2,q)$ and let $\mathcal{D}$ denote the set of directions determined by $\mathcal{U}$. Let $n = |\mathcal{U}|$ and let $R(X,Y)$ be the inhomogeneous affine Rédei polynomial of the affine set $\mathcal{U}$, that is,

$$R(X,Y) = \prod_{(a,b)\in\mathcal{U}} (X - aY + b) = X^n + \sum_{i=0}^{n-1} \sigma_{n-i}(Y) X^i$$

where the abbreviation $\sigma_k(Y)$ means the k-th elementary symmetric polynomial of the set $\{b - aY \mid (a, b) \in \mathcal{U}\}$ of linear polynomials.

Proposition 9. *If $y \in \mathcal{D}$ then $R(X, y) \in \mathsf{GF}(q)[X^{s(y)}] \setminus \mathsf{GF}(q)[X^{p \cdot s(y)}]$.*
If $y \notin \mathcal{D}$ then $R(X, y) \mid X^q - X$.

Proof. Assume $y \in \mathcal{D}$. Then the equation $R(X, y) = 0$ has root x with multiplicity m if there is a line with slope y meeting $\mathcal{U}$ in exactly m points. The value of x determines this line. So each x is either not a root of $R(X, y)$ or a root with multiplicity a multiple of $s(y)$; and $p \cdot s(y)$ does not have this property. Since R is totally reducible, it is the product of its root factors.
If $y \notin \mathcal{D}$ then a line with direction y cannot meet $\mathcal{U}$ in more than one point, so an x cannot be a multiple root of $R(X, y)$. ■

Notation. Let $\mathbb{F}$ be the polynomial ring $\mathsf{GF}(q)[Y]$ and consider $R(X, Y)$ as the element of the univariate polynomial ring $\mathbb{F}[X]$. Divide $X^q - X$ by $R(X, Y)$ as a univariate polynomial over $\mathbb{F}$ and let Q denote the quotient and let $H + X$ be the negative of the remainder.

$$\begin{aligned} Q(X, Y) &= (X^q - X) \quad \text{div } R(X, Y) \qquad \text{over} \quad \mathbb{F} \\ -X - H(X, Y) &\equiv (X^q - X) \quad \text{mod } R(X, Y) \qquad \text{over} \quad \mathbb{F} \end{aligned}$$

So

$$R(X, Y)Q(X, Y) = X^q + H(X, Y) = X^q + \sum_{i=0}^{q-1} h_{q-i}(Y)X^i$$

where $\deg_X H < \deg_X R$. Let σ^* denote the coefficients of Q,

$$Q(X, Y) = X^{q-n} + \sum_{i=0}^{q-n-1} \sigma^*_{q-n-i}(Y)X^i$$

and so

$$h_j(Y) = \sum_{i=0}^{j} \sigma_i(Y)\sigma^*_{j-i}(Y).$$

We know that $\deg h_i \le i$, $\deg \sigma_i \le i$ and $\deg \sigma^*_i \le i$. Note that the $\sigma^*(Y)$ polynomials are not necessarily elementary symmetric polynomials of linear polynomials and if $y \in \mathcal{D}$ then $Q(X, y)$ is not necessarily totally reducible.

Remark 10. Since $\deg_X H < \deg_X R$, we have $h_i = 0$ for $1 \le i \le q - n$. By definition, $\sigma_0 = \sigma^*_0 = 1$. The equation $h_1 = 0$ implies $\sigma^*_1 = -\sigma_1$, this fact and the equation $h_2 = 0$ implies $\sigma^*_2 = -\sigma_2 + \sigma_1^2$ and so on, the $q - n$ equations $h_i = 0$ uniquely define all the coefficients σ^*_i.

Proposition 11. *If $y \in \mathcal{D}$ then $Q(X,y), H(X,y) \in \mathsf{GF}(q)[X^{s(y)}]$ and if $\deg R \leq \deg Q$ then $Q(X,y) \in \mathsf{GF}(q)[X^{s(y)}] \setminus \mathsf{GF}(q)[X^{p \cdot s(y)}]$.*
If $y \notin \mathcal{D}$ then $R(X,y)Q(X,y) = X^q + H(X,y) = X^q - X$. In this case $Q(X,y)$ is also a totally reducible polynomial.

Proof. If $y \in \mathcal{D}$ then

$$R(X,y) = X^n + \sum_{i=0}^{n-1} \sigma_{n-i}(y) X^i \in \mathsf{GF}(q)[X^{s(y)}] \setminus \mathsf{GF}(q)[X^{p \cdot s(y)}].$$

So $s(y) \mid n$ and $\sigma_i(y) \neq 0 \Rightarrow s(y) \mid n-i \Rightarrow s(y) \mid i$. The defining equation of σ_i^* contains the sum of products of some σ_j where the sum of indices (counted with multiplicities) is i. Since $\sigma_j(y) \neq 0$ only if $s(y) \mid j$, also $\sigma_i^*(y) \neq 0$ only if $s(y) \mid i$.
If $\deg R \leq \deg Q$ then we can consider R as $(X^q - X)$ div Q and the reminder is the same H.
Since both $R(X,y)$ and $Q(X,y)$ are in $\mathsf{GF}(q)[X^{s(y)}]$, $H(X,y) \in \mathsf{GF}(q)[X^{s(y)}]$.
If $y \notin \mathcal{D}$ then $R(X,y) \mid (X^q - X)$ in $\mathsf{GF}(q)[X]$ so $Q(X,y)$ is also totally reducible. ■

Remark 12. Note that $H(X,y)$ can be an element of $\mathsf{GF}(q)[X^{p \cdot s(y)}]$. If $H(X,y) \equiv a$ is a constant polynomial, then $R(X,y)Q(X,y) = X^q + a = X^q + a^q = (X+a)^q$. This means that $R(X,y) = (X+a)^n$ and thus, there exists exactly one line (corresponding to $X = -a$) of direction y that contains $\mathcal{U}$, and so $\mathcal{D} = \{y\}$.

Definition. If $|\mathcal{D}| \geq 2$ (i.e. $H(X,y)$ is not a constant polynomial) then for each $y \in \mathcal{D}$, let $t(y)$ denote the maximal power of p such that $H(X,y) = f_y(X)^{t(y)}$ for some $f_y(X) \notin \mathsf{GF}(q)[X^p]$.

$$H(X,y) \in \mathsf{GF}(q)[X^{t(y)}] \setminus \mathsf{GF}(q)[X^{t(y)p}].$$

In this case $t(y) < q$ since $t(y) \leq \deg_X H < q$. Let t be the greatest common divisor of the numbers $t(y)$, that is,

$$t = \gcd_{y \in \mathcal{D}} t(y) = \min_{y \in \mathcal{D}} t(y).$$

If $H(X,y) \equiv a$ (i.e. $\mathcal{D} = \{y\}$) then we define $t = t(y) = q$.

Remark 13. If there exists at least one determined direction $y \in \mathcal{D}$ such that $H(X,y)$ is not constant then $t < q$. From **Proposition 11** we have $s(y) \leq t(y)$ for all $y \in \mathcal{D}$, so $s \leq t$. ■

Proposition 14. *Using the notation above,*

$$R(X,Y)Q(X,Y) = X^q + H(X,Y) \in \mathrm{Span}_{\mathbb{F}}\langle 1, X, X^t, X^{2t}, X^{3t}, \ldots, X^q\rangle.$$

Proof. If $|\mathcal{D}| = \{y\}$ then $H(X,y) \equiv a$ and $H(X,z) = -X$ for $z \neq y$.
Suppose that $|\mathcal{D}| \geq 2$. If $y \notin \mathcal{D}$ then $X^q + H(X,y) = X^q - X$ and if $y \in \mathcal{D}$ then $X^q + H(X,y) \in \mathsf{GF}(q)[X^{t(y)}] \setminus \mathsf{GF}(q)[X^{t(y)p}]$.
Thus, in both cases, if $i \neq 1$ and $i \nmid t$, then $h_{q-i}(Y)$ has q roots and its degree is less than q. ■

4 Bounds on the number of directions

Although, in the original problem, the vertical direction ∞ was not determined, from now on, without loss of generality we suppose that ∞ is a determined direction (if not, we apply an affine collineation). We continue to suppose that there is at least one non-determined direction.

Lemma 15. *If $\infty \in \mathcal{D} \subsetneqq \ell_\infty$ then $|\mathcal{D}| \geq \deg_X H(X,Y) + 1$.*

Proof. If $y \notin \mathcal{D}$ then $R(X,y) \mid X^q - X$, thus $H(X,y) = -X$ and thus $\forall i \neq q-1$: $h_i(y) = 0$.
If $y \in \mathcal{D}$ then $R(X,y) \nmid X^q - X$, hence $\exists i \neq q-1$: $h_i(y) \neq 0$ and thus $h_i \not\equiv 0$.
Let i be the smallest index such that $h_i \not\equiv 0$ and so $i = q - \deg_X H$. Since $h_i \not\equiv 0$ has at least $(q+1) - |\mathcal{D}| = q - (|\mathcal{D}| - 1)$ roots, $\deg_Y h_i \geq q - |\mathcal{D}| + 1$.

$$\text{Now } q \geq \deg X^{q-i}h_i(Y) = q - i + \deg_Y h_i \geq 2q - |\mathcal{D}| + 1 - i.$$

Hence $|\mathcal{D}| \geq q + 1 - i = \deg_X H + 1$. ■

Lemma 16. *Let $\kappa(y)$ denote the number of the roots of $X^q + H(X,y)$ in $\mathsf{GF}(q)$, counted with multiplicity. If $X^q + H(X,y) \neq X^q - X$ and if $H(X,y)$ is not a constant polynomial, then*

$$\frac{\kappa(y) - 1}{t(y) + 1} + 1 = \frac{\kappa(y) + t(y)}{t(y) + 1} \leq t(y) \cdot \deg f_y(X) = \deg_X H \leq \deg H$$

Proof. Fix $y \in \mathcal{D}$ and utilize that $X^q + H(X,y) \in \mathsf{GF}(q)[X^{t(y)}]$, thus

$$\Big(X^{q/t(y)} + f_y(X)\Big)^{t(y)} = X^q + H(X,y) = \Big(a(X) \cdot b(X) \cdot c(X)\Big)^{t(y)}$$

where the totally reducible $a(X)$ contains all the roots (in $\mathsf{GF}(q)$) without multiplicity, the totally reducible $b(X)$ contains the further roots (in $\mathsf{GF}(q)$),

and $c(X)$ has no root in $\mathsf{GF}(q)$. (Note that $t(y) < q$ so $X^{q/t(y)} \in \mathsf{GF}(q)[X^p]$.)

$$\left.\begin{array}{l} a(X) \mid (X^q - X) \\ a(X) \mid \left(X^q + f_y(X)^{t(y)}\right) \end{array}\right\} \Longrightarrow \begin{array}{r} a(X) \mid \left(f_y(X)^{t(y)} + X\right) \\ b(X) \mid \partial_X \left(X^{q/t(y)} + f_y(X)\right) = \partial_X f_y(X) \\ a(X)b(X) \mid \left(f_y(X)^{t(y)} + X\right) \partial_X f_y(X) \end{array}$$

And so, $\deg(a(X)b(X)) \leq t(y) \cdot \deg f_y + \deg f_y - 1 = (t(y)+1) \cdot \deg f_y - 1$, since $\partial_X f_y(X) \neq 0$ and $f_y(X)^{t(y)} = H(X,y) \neq -X$. We get

$$\frac{\kappa(y) + t(y)}{t(y)+1} = t(y) \frac{\deg(a(X)b(X)) + 1}{t(y)+1} \leq t(y) \cdot \deg f_y(X)$$

using $\kappa(y) = t(y) \cdot \deg(a(X)b(X))$. ■

Using these lemmas above we can prove a theorem similar to **Theorem 3** but it is weaker in our case.

Theorem 17. *Let $\mathcal{U} \subset \mathsf{AG}(2,q)$ be an arbitrary set of points and let $\mathcal{D}$ denote the directions determined by $\mathcal{U}$. We use the notation s and t defined above geometrically and algebraically, respectively. Suppose that $\infty \in \mathcal{D}$. One of the following holds:*

either	$1 = s \leq t < q$	*and*	$\dfrac{\lvert\mathcal{U}\rvert - 1}{t+1} + 2 \leq \lvert\mathcal{D}\rvert \leq q+1;$
or	$1 < s \leq t < q$	*and*	$\dfrac{\lvert\mathcal{U}\rvert - 1}{t+1} + 2 \leq \lvert\mathcal{D}\rvert \leq \dfrac{\lvert\mathcal{U}\rvert - 1}{s-1};$
or	$1 \leq s \leq t = q$	*and*	$\mathcal{D} = \{\infty\}.$

Proof. The third case is trivial ($t = q$ means $|\mathcal{D}| = 1$, by the definition of t). Let P be a point of $\mathcal{U}$ and consider the lines connecting P and the ideal points of $\mathcal{D}$. Since each such line meets $\mathcal{U}$ and has a direction determined by $\mathcal{U}$, it is incident with $\mathcal{U}$ in a multiple of s points. If $s > 1$ then counting the points of $\mathcal{U}$ on these lines we get the upper bound.
If $t < q$ then we can choose a direction $y \in \mathcal{D}$ such that the conditions of **Lemma 16** hold. Using **Lemma 15** and **Lemma 16**, we get

$$|\mathcal{D}| \geq \deg_X H(X,Y) + 1 \geq \frac{\kappa(y) - 1}{t(y)+1} + 1 + 1.$$

The number of roots of $R(X,y)Q(X,y)$ is at least the number of roots of $R(X,y)$ which equals to $|\mathcal{U}|$. Thus $\kappa(y) \geq |\mathcal{U}|$. And thus

$$\frac{\kappa(y) - 1}{t(y)+1} \geq \frac{|\mathcal{U}| - 1}{t+1}.$$

■

An affine collineation converts Szőnyi's and Blokhuis' **Theorem 4** to the special case of our **Theorem 17**, since t is equal to either 1 or p in the case $q = p$ prime.

In the case $q > p$, the main problem of **Theorem 17** is, that the definition of t is non-geometrical. Unfortunately, $t = s$ does not hold in general. For example, let $\mathcal{U}$ be a $\mathsf{GF}(p)$-linear set minus one point. In this case $s = 1$, but $t = p$. In the rest of this article, we try to describe this problem.

5 Maximal affine sets

One can easily show that a *proper* subset of the affine set $\mathcal{U}$ can determine the same directions. (For example, let $\mathcal{U}$ be an affine subplane over the subfield $\mathsf{GF}(s)$. Arbitrary $s + 1$ points of $\mathcal{U}$ determine the same directions.)

Definition (Maximal affine set)**.** We say that $\mathcal{U} \subseteq \mathsf{AG}(2, q)$ is a *maximal* affine set that determines the set $\mathcal{D} \subseteq \ell_\infty \cong \mathsf{PG}(1, q)$ of directions if each affine set that contains $\mathcal{U}$ as a *proper* subset determines *more than* $|\mathcal{D}|$ directions.

Tamás Szőnyi proved a 'completing theorem' (stability result) in [6], which was slightly generalized in [5] as follows.

Theorem 18 (Szőnyi; Sziklai)**.** [5, Theorem 3.1] *Let $\mathcal{D}$ denote the set of directions determined by the affine set $\mathcal{U} \subset \mathsf{AG}(2, q)$ containing $q - \varepsilon$ points, where $\varepsilon < \alpha\sqrt{q}$ and $|\mathcal{D}| < (q + 1)(1 - \alpha)$, $1/2 < \alpha < 1$. Then $\mathcal{U}$ can be extended to a set $\mathcal{U}'$ with $|\mathcal{U}'| = q$ such that $\mathcal{U}'$ determines the same directions.* ■

Szőnyi's stability theorem above also stimulates us to restrict ourselves to examine the *maximal* affine sets only. (An affine set of q points that does not determine all directions is *automatically* maximal.)

If we examine polynomials in one variable instead of Rédei polynomials, we can get similar 'stability' results. Such polynomials occur when we examine $R(X, y)$, $Q(X, y)$ and $H(X, y)$, or R, Q and H over $\mathsf{GF}(q)(Y)$. The second author conjectured that if 'almost all' roots of a polynomial $g \in \mathsf{GF}(q)[X]$ have muliplicity a power of p then the quotient X^q div g extends g to a polynomial in $\mathsf{GF}(q)[X^p]$. We can prove more.

Notation. Let $p = \operatorname{char} \mathbb{F} \neq 0$ be the characteristic of the *arbitrary* field $\mathbb{F}$. Let $s = p^e$ and $q = p^h$ two arbitrary powers of p such that $e \leq h$ (i.e. $s \mid q$ but q is not necessarily a power of s).

Theorem 19. *Let $g, f \in \mathbb{F}[X]$ be polynomials such that $g \cdot f \in \mathbb{F}[X^s]$. If $0 \leq \deg f \leq s-1$ then $X^q \mod g$ extends g to a polynomial in $\mathbb{F}[X^s]$.*

Proof. We know that $\deg(gf) = ks$ ($k \in \mathbb{N}$). Let $r = X^q \mod (fg)$ denote the remainder, that is, $X^q = (gf)h + r$ where $\deg r \leq \deg(fg) - 1$.
Now we show that $h \in \mathbb{F}[X^s]$. Suppose to the contrary that $h \notin \mathbb{F}[X^s]$, i.e. the polynomial h has at least one monomial $\bar{a} \notin \mathbb{F}[X^s]$. Let $\bar{a}$ denote such a monomial of *maximal degree*. Let $\bar{b}$ denote the leading term of fg. Since $gf \in \mathbb{F}[X^s]$, also $\bar{b} \in \mathbb{F}[X^s]$, and since $\bar{b}$ is the leading term, $\deg \bar{b} = \deg(fg)$. The product $\bar{a}\bar{b}$ is a monomial of the polynomial $(fg)h$, and since $\deg \bar{b} > \deg r$, then $\bar{a}\bar{b}$ is also a monomial of the polynomial $(f \cdot g \cdot h + r)$. The monomial $\bar{a}\bar{b}$ is not in $\mathbb{F}[X^s]$, because $\bar{a} \notin \mathbb{F}[X^s]$ and $\bar{b} \in \mathbb{F}[X^s]$. But $f \cdot g \cdot h + r = X^q \in \mathbb{F}[X^s]$, which is a contradiction.
Hence $r \in \mathbb{F}[X^s]$, and so $s \mid \deg r$, and thus, if the closed interval $[\deg g, \deg(gf) - 1]$ does not contain any integer that is a multiple of s then $\deg r$ is less than $\deg g$.
If we know that $\deg r < \deg g$ then from the equation $X^q = (gf)h + r$ we get $X^q = g(fh) + r$ hence $r = X^q \mod g$ and $X^q \operatorname{div} g = f \cdot h$, where f is a polynomial such that $fg \in \mathbb{F}[X^s]$ and also $h \in \mathbb{F}[X^s]$.
So it is enough to show that the closed interval $[\deg g, \deg(gf) - 1]$ does not contain any integer that is a multiple of s. Using $\deg(fg) = ks$, the closed interval $[\deg g, \deg(gf) - 1] = [ks - \deg f, ks - 1]$ and if $0 \leq \deg f \leq s - 1$ then it does not contain any integer which is the multiple of s. ■

This theorem above suggests that if the product $R(X, y)Q(X, y)$ is an element of $\mathsf{GF}(q)[Y][X^{p \cdot s(y)}]$ while $R(X, y) \in \mathsf{GF}(q)[Y][X^{s(y)}] \setminus \mathsf{GF}(q)[Y][X^{p \cdot s(y)}]$, then a 'completing result' might be in the background. If $\mathcal{U}$ is a maximal affine set then it cannot be completed, so we conjecture the following.

Conjecture 20. *If $\mathcal{U}$ is a* maximal *affine set that determines the set $\mathcal{D}$ of directions then $t(y) = s(y)$ for all $y \in \mathcal{D}$ where $t(y) > 2$.*

Note that there can be maximal affine sets which are not linear.

Example (Non-linear maximal affine set)**.** Let $\mathcal{U} \subset \mathsf{AG}(2, q)$ be a set, $|\mathcal{U}| = q$, $s = 1$, $q \geq |\mathcal{D}| \geq \dfrac{q+3}{2}$. In this case $\mathcal{U}$ cannot be linear because then s would be at least p. But $\mathcal{U}$ must be maximal since $q + 1$ points in $\mathsf{AG}(2, q)$ would determine all directions. Embed $\mathsf{AG}(2, q)$ into $\mathsf{AG}(2, q^m)$ as a subgeometry. Then $\mathcal{U} \subset \mathsf{AG}(2, q^m)$ is a maximal non-linear affine set of less than q^m points.

But if $s > 2$, we conjecture that the maximal set is linear.

Conjecture 21. *If $\mathcal{U}$ is a* maximal *affine set that determines the set $\mathcal{D}$ of directions and $t = s > 2$ then $\mathcal{U}$ is an affine $\mathsf{GF}(s)$-linear set.*

Although we conjecture that the maximal affine sets with $s = t > 2$ are linear sets, the converse is not true.

Example (Non-maximal affine linear set)**.** Let $\mathsf{AG}(2, s^i)$ be a canonical subgeometry of $\mathsf{AG}(2, q = s^{i \cdot j})$ and let $\mathcal{U}$ be an affine $\mathsf{GF}(s)$-linear set in the subgeometry $\mathsf{AG}(2, s^i)$ that contains more than s^i points. Then $\mathcal{U}$ determines the same direction set that is determined by the subgeometry $\mathsf{AG}(2, s^i)$.

References

[1] S. Ball The number of directions determined by a function over a finite field. *J. Combin. Theory Ser. A* **104**(2): 341–350, 2003.

[2] A. Blokhuis Personal communication.

[3] 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): 187–196, 1999.

[4] O. Polverino Linear sets in finite projective spaces. *Discrete Math.* **310**(22): 3096–3107, 2010.

[5] P. Sziklai On subsets of $\mathsf{GF}(q^2)$ with dth power differences. *Discrete Math.* **208/209**: 547–555, 1999. Combinatorics (Assisi, 1996).

[6] T. Szőnyi On the number of directions determined by a set of points in an affine Galois plane. *J. Combin. Theory Ser. A* **74**(1): 141–146, 1996.

[7] T. Szőnyi Around Rédei's theorem *Discrete Math.* **208/209**: 557–575, 1999. Combinatorics (Assisi, 1996).