THE POLYNOMIAL METHOD IN GALOIS GEOMETRIES *

Simeon Ball†
Universitat Politécnica de Catalunya

Abstract

The polynomial method refers to the application of polynomials to combinatorial problems. The method is particularly effective for Galois geometries and a number of problems and conjectures have been solved using the polynomial method. In many cases the polynomial approach is the only method which we know of that works. In this article, the various polynomial techniques that have been applied to Galois geometries are detailed and, to demonstrate how to apply these techniques, some of the problems referred to above are resolved.

1 Introduction

In this chapter we shall introduce the polynomial method that allows us to solve some problems in Galois geometries by considering properties of certain polynomials of $\mathbb{F}_q[X]$. In general the method is the following. Given an object O in a Galois geometry over $\mathbb{F}_q$ with a regular property, define a polynomial f with coefficients in $\mathbb{F}_q$, or some finite extension of $\mathbb{F}_q$, which translates the geometrical property of O into an algebraic property of f. Using this algebraic property of f we then try to deduce further algebraic properties which translate back into further geometrical properties of O.

This is best seen by way of an example. Consider a set $\mathcal{S}$ of points of $\mathrm{AG}(n,q)$ with the property that every hyperplane of $\mathrm{AG}(n,q)$ is incident with a point of $\mathcal{S}$. We wish to prove a lower bound on $\mathcal{S}$ and construct an example to show that this bound is best possible. A combinatorial counting argument gives a bound of roughly $q+\sqrt{q}$ for $n=2$, whereas by construction the best we can do is $2q-1$. For the construction one can take the points on the union of two intersecting lines.

*29 June 2009

†simeon@ma4.upc.edu. The author acknowledges the support of the project MTM2008-06620-C03-01 of the Spanish Ministry of Science and Education and the project 2005SGR00256 of the Catalan Research Council.

A hyperplane of $\mathrm{AG}(n,q)$ which does not contain the origin is defined by an equation

$$a_1X_1 + \ldots + a_nX_n + 1 = 0.$$

By assumption there is a point $s \in \mathcal{S}$ which is incident with this hyperplane or, in other words,

$$a_1s_1 + \ldots + a_ns_n + 1 = 0.$$

Let

$$f(X) = \prod_{s\in\mathcal{S}}(s_1X_1 + \ldots + s_nX_n + 1).$$

Assuming that the origin is an element of $\mathcal{S}$ this polynomial has degree $|\mathcal{S}| - 1$. It has the property that

$$f(a) = 0$$

for all $a \in \mathbb{F}_q^n$, provided that $a \neq 0$. Moreover, $f(0) = 1$.

We shall show in the next section that the degree of a polynomial with such properties is at least $n(q-1)$, which will imply that $|\mathcal{S}| \geq n(q-1)+1$. This bound was first proven by Jamison [36] and will be referred to as Jamison's theorem.

Note that the various sections are written in such a way that, apart from Section 3, they stand alone and can be read independently.

2 Combinatorial Nullstellensatz

Let $\mathbb{F}$ be a field, not necessarily finite. Let $f \in \mathbb{F}[X]$ be a polynomial with the property that $f(x) = 0$ for all $x \in \mathcal{S}_1$, where $\mathcal{S}_1$ is some finite subset of $\mathbb{F}$. If we define

$$g_1(X) = \prod_{s\in\mathcal{S}_1}(X - s)$$

then we can write $f = g_1h_1$, for some polynomial h_1 of degree $f^\circ - g_1^\circ$, where f° will denote the degree of a polynomial f.

The Combinatorial Nullstellensatz of Alon extends this observation to polynomials in more indeterminates. The proof is straightforward induction so we shall not include it here, those interested can find a proof in the article by Alon [1].

For $i = 1,\ldots,n$, let $\mathcal{S}_i$ be finite subsets of $\mathbb{F}$ and define

$$g_i(X_i) = \prod_{s\in\mathcal{S}_i}(X_i - s).$$

THEOREM 2.1. *If $f \in \mathbb{F}[X_1,\ldots,X_n]$ has the property that $f(s_1,\ldots,s_n) = 0$ for all $(s_1,\ldots,s_n) \in \mathcal{S}_1 \times \ldots \times \mathcal{S}_n$ then*

$$f = \sum_{i=1}^{n} g_ih_i,$$

for some polynomials h_i of degree at most $f^\circ - g_i^\circ$.

Let us return to the polynomial f from the previous section. The following theorem is essentially the proof of Jamison's theorem given by Brouwer and Schrijver in [27].

THEOREM 2.2. *If $f \in \mathbb{F}_q[X_1,\ldots,X_n]$ is a polynomial with the property that $f(s)=0$ for all $s \in \mathbb{F}_q^n$, $s \neq 0$ and $f(0)=1$, then $f^\circ \geq n(q-1)$.*

Proof. Let

$$g_i(X_i) = \prod_{s\in\mathbb{F}_q} (X_i - s) = X_i^q - X_i.$$

We can write

$$f = \sum g_i u_i + w$$

for some polynomials u_i in such a way that the polynomial $w = w(X_1,\ldots,X_n) \neq 0$ has degree at most $q-1$ in X_i and $f^\circ \geq w^\circ$.

For every i the polynomial $X_i w$ has the property that $(X_i w)(s_1,\ldots,s_n) = 0$ for all $(s_1,\ldots,s_n) \in \mathbb{F}_q^n$. However, for $j \neq i$ the degree in X_j of $X_i w$ is at most $q-1$. When we apply Theorem 2.1 to $X_i w$ the $g_j h_j$ terms are zero since the X_j^q term in g_j would give terms on the right-hand side that do not appear in $X_i w$. Hence

$$X_i w = g_i h_i,$$

for some polynomial h_i. Thus $g_i(X_i)$ divides $X_i w$ for all i. The g_i are polynomials in different indeterminates and so are pairwise coprime and therefore $\prod g_i(X_i)$ divides $(\prod X_i)w$. Thus the degree of w, and therefore the degree of f, is at least $\sum g_i^\circ - n = nq - n$. □

This can be easily extended to more general sets where $\mathbb{F}_q$ is replaced by arbitrary finite subsets of a field, see [15].

The consequences of Theorem 2.2 for the set of points $\mathcal{S}$ were already mentioned in the previous section. Namely we get Jamison's theorem, which is the following.

COROLLARY 2.3. *If $\mathcal{S}$ is a set of points of $AG(n,q)$ with the property that every hyperplane is incident with a point of $\mathcal{S}$ then*

$$|\mathcal{S}| \geq n(q-1)+1.$$

Proof. Since the degree of the polynomial f is bounded below by $n(q-1)$, the set of points $\mathcal{S}$ has size at least $n(q-1)+1$. □

This bound can be obtained by taking the set of points that is the union of n lines which span $\mathrm{AG}(n,q)$ and all concurrent with a point x.

3 Nullstellensätze for lower dimensional subspaces ?

In the previous section we proved that a set of points $\mathcal{S}$, with the property that every hyperplane of $\mathrm{AG}(n,q)$ is incident with a point of $\mathcal{S}$, has size at least $n(q-1)+1$. There are various generalisations which we may consider. If we replace the condition "one point" with "t points" then similar techniques to those mentioned before have been used to prove lower bounds on the size of the set, see [3]and [28], although it is doubtful in most cases that these bounds are attainable. We shall not consider them here.

Another possible generalisation would be to replace "hyperplane" with "k-dimensional subspace", where $k \leq n-2$. Here, we can combine a combinatorial counting approach, with

the theorem we obtained using the polynomial method in the previous section, to obtain a lower bound on the size of $\mathcal{S}$.

Suppose that $\mathcal{S}$ is a set of points with the property that every k-dimensional subspace of $\mathrm{AG}(n,q)$ is incident with a point of $\mathcal{S}$. Let ρ be a k-dimensional subspace incident with exactly one point x of $\mathcal{S}$. Let σ be a $(k+1)$-dimensional subspace containing ρ. The set $\mathcal{S} \cap \sigma$ has the property that every hyperplane of σ is incident with a point of $\mathcal{S} \cap \sigma$ and so by Jamison's theorem, which we proved in the previous section, it has size at least $(k+1)(q-1)+1$. There are $(q^{n-k}-1)/(q-1)$ subspaces σ containing ρ which all contain the point x but share no other point of $\mathcal{S}$. Thus

$$|\mathcal{S}| \geq (k+1)(q^{n-k}-1)+1.$$

This bound is, more or less, the best known bound. The polynomial method does not seem to allow us to improve on this, although that may be because we simply do not know how to apply it to this more general case.

The known constructions are somewhat crude. For example, let $\mathcal{S}$ be a set of points of $\mathrm{AG}(3,q)$ with the property that every line is incident with a point of $\mathcal{S}$. For q square, the smallest known example has size roughly $2q^2+2q\sqrt{q}$ and is constructed using a double blocking set of $\mathrm{PG}(2,q)$ at infinity and forming a cone with a vertex point of the affine space. However, the lower bound we obtained with $n=3$ and $k=1$ is $2q^2-1$, so we are some way short of the size of the set in the construction.

Let us see where a polynomial approach, similar to that used in the introduction leads to. Define

$$f(X_1,X_2,X_3) = \prod_{s \in \mathcal{S}} (s_1X_1 + s_2X_2 + s_3X_3 + 1).$$

We would like to translate the geometric property of $\mathcal{S}$, that every line is incident with a point of $\mathcal{S}$, into an algebraic property of f. An affine line is defined by two equations of the form

$$a_1X_1 + a_2X_2 + a_3X_3 + 1 = 0, \quad b_1X_1 + b_2X_2 + b_3X_3 = 0,$$

where a and b are linearly independent. By assumption, for every $a,b \in \mathbb{F}_q^3$, linearly independent, there is a point $s \in \mathcal{S}$ with the property that

$$a_1s_1 + a_2s_2 + a_3s_3 + 1 = 0, \quad b_1s_1 + b_2s_2 + b_3s_3 = 0.$$

Therefore

$$f(a_1+b_1X, a_2+b_2X, a_3+b_3X) = \prod_{s \in \mathcal{S}} (s_1a_1 + s_2a_2 + s_3a_3 + 1 + (s_1b_1 + s_2b_2 + s_3b_3)X) = 0$$

for all $a,b \in \mathbb{F}_q^3$ linearly independent, and $f(0) = 1$. It is not clear what lower bound can be proved for the degree of a polynomial with such properties but clearly any lower bound would give a lower bound for the size of $\mathcal{S}$.

There are a number of objects in higher dimensional spaces for which properties can be deduced using planar results but where a direct application of the polynomial method doesn't appear to offer more insight but probably should. The example mentioned above is just one example of these.

4 Lacunary polynomials

It was Rédei who first worked on lacunary polynomials over finite fields and wrote the book [40]. In Chapter VI, §36, he applies a theorem on lacunary polynomials to functions over a finite field which determine few directions. This may have been the first application of the polynomial method to a geometrical problem. Before considering the geometrical problem, let us prove a generalisation of one of Rédei's result on lacunary polynomials, which is due to Blokhuis [16].

Let (g,h) denote the greatest common divisor of polynomials g and h.

LEMMA 4.1. *Suppose that $f(X) = g(X)X^q + h(X)$ is a polynomial in $\mathbb{F}_q[X]$ which factorises completely into linear factors in $\mathbb{F}_q[X]$. If $\max(g^\circ, h^\circ) \le (q-1)/2$ then $f(X) = g(X)(X^q - X)$ or $f(X) = (g,h)e(X^p)$, where $q = p^h$.*

Proof. We can suppose that g and h have no common factors since removing them does not affect the hypothesis.

The factors of f are factors of $X^q - X$ and so factors of $f - (X^q - X)g = Xg + h$.

The factors of multiplicity $m \ge 2$ are factors of multiplicity at least $m-1$ of

$$f' = \frac{df}{dX} = g'X^q + h',$$

and so are factors of multiplicity at least $m-1$ of $f'g - g'f = h'g - g'h$.

Therefore f is a factor of $(Xg+h)(h'g-g'h)$. This polynomial has degree at most $(q+1)/2 + g^\circ + h^\circ - 1 \le q - 1 + g^\circ$, whereas $f^\circ = q + g^\circ$. Since f cannot be a factor of a non-zero polynomial of less degree than itself, it follows that $(Xg+h)(h'g-g'h) = 0$.

If $Xg + h = 0$ then $f(X) = g(X)(X^q - X)$.

If $h'g - g'h = 0$ then h divides h' (assuming $(g,h) = 1$) and so $h' = 0$ and $g' = 0$. Thus in this case g and h are in $\mathbb{F}_q[X^p]$ and the lemma is proved. □

This lemma was used by Blokhuis to prove his theorem on blocking sets in $\mathrm{PG}(2,p)$ which we shall see later. Note that the bound on g° and h° is tight for q odd since the polynomial $X^q - X^{(q+1)/2}$ factors into linear factors in $\mathbb{F}_q[X]$.

Consider the graph of a function ϕ over a finite field $\mathbb{F}_q$; in other words the set of q points $\{(x,\phi(x)) \mid x \in \mathbb{F}_q\}$ of $\mathrm{AG}(2,q)$. The set of directions determined by this set is

$$\mathcal{D}_\phi = \{\frac{\phi(y) - \phi(x)}{y - x} \mid y \ne x,\ x,y \in \mathbb{F}_q\}.$$

For a typical function ϕ, the set $\mathcal{D}_\phi$ will be the set of all elements of $\mathbb{F}_q$. However, there are functions for which $\mathcal{D}_\phi$ is not all $\mathbb{F}_q$. The linear functions determine only one direction of course. For a function ϕ, which is linear over a proper subfield $\mathbb{F}_s$ of $\mathbb{F}_q$, $\mathcal{D}_\phi$ satisfies

$$\frac{q}{s} + 1 \le |\mathcal{D}_\phi| \le \frac{q-1}{s-1},$$

and there are functions which attain both bounds. If q is odd then, for the function ϕ defined by the monomial $x^{(q+1)/2}$, the set $\mathcal{D}_\phi$ has $(q+3)/2$ elements. Thus, for every q (since $\mathbb{F}_2$ is a subfield of $\mathbb{F}_q$ when q is even), there is some function ϕ for which

$$|\mathcal{D}_\phi| \le \frac{q+3}{2}.$$

Rédei started the investigation which would eventually lead to proving that the functions ϕ that determine less than $(q+3)/2$ directions are linear over a subfield. Some improvements to Rédei's initial work are included in [20], the classification being all but obtained in [19], and finally obtained in [4]. It can be summarised in the following theorem.

THEOREM 4.2. *If, for some function ϕ from $\mathbb{F}_q$ to $\mathbb{F}_q$, the set $\mathcal{D}_\phi$ has less than $(q+3)/2$ elements, then there is a subfield $\mathbb{F}_s$ of $\mathbb{F}_q$ such that*

$$\frac{q}{s}+1 \leq |\mathcal{D}_\phi| \leq \frac{q-1}{s-1},$$

and ϕ is linear over $\mathbb{F}_s$.

We shall prove the classification in the prime case, as Rédei did in his book, and leave the interested reader to consult the references for the non-prime case. We shall in fact prove something stronger, that was first proved by Blokhuis in [16]. He proved that a set $\mathcal{S}$ of less than $(3p+1)/2$ points of $\mathrm{PG}(2,p)$, p prime, with the property that every line is incident with a point of $\mathcal{S}$, contains all the points of a line.

Consider a set of q points $\mathcal{S}$ of $\mathrm{AG}(2,q)$ and let

$$\mathcal{D} = \{\frac{s_2-t_2}{s_1-t_1} \mid s \neq t,\ s,t \in \mathcal{S}\},$$

be the set of directions determined by the points of $\mathcal{S}$. Let us assume that $\infty \in \mathcal{D}$. Note that if S is the graph of a function then $\infty \notin \mathcal{D}$. However, we can apply an affine transformation to $\mathcal{S}$ so that ∞ is an element of $\mathcal{D}$.

An element $-x \in \mathcal{D}$ if and only if there are elements $s,t \in \mathcal{S}$ with the property that $xs_1+s_2 = xt_1+t_2$. Therefore if $-x \notin \mathcal{D}$ the set $\{xs_1+s_2 \mid s \in \mathcal{S}\} = \mathbb{F}_q$.

Let $\mathcal{E} = (\mathbb{F}_q \cup \{\infty\}) \setminus \mathcal{D}$. We are interested in the case $|\mathcal{D}| \leq (q+1)/2$ or equivalently $|\mathcal{E}| \geq (q+1)/2$.

Let us generalise the situation to a set $\mathcal{S}$ of $q+k$ points where

$$\mathcal{E} = \{-x \in \mathbb{F}_q \mid \{xs_1+s_2 \mid s \in \mathcal{S}\} = \mathbb{F}_q\}$$

has size at least $(q+1)/2+k$. The parallel lines with direction m are defined by equations of the form $X_2 = mX_1+c$. The lines in this set of lines are all incident with a point of $\mathcal{S}$ if and only if $m \in \mathcal{E}$.

We shall prove that in the prime case $\mathcal{S}$ contains all the points of a line.

Firstly we introduce a polynomial f which translates the geometric property of $\mathcal{S}$ into an algebraic property of f. Let

$$f(X_1,X_2) = \prod_{s\in\mathcal{S}}(X_1+s_1X_2+s_2).$$

The polynomial f has the property that the polynomial $X_1^q - X_1$ is a factor of $f(X_1,x)$ if and only if $-x \in \mathcal{E}$.

The proof of Theorem 4.3 follows Blokhuis' approach in [16].

THEOREM 4.3. *Let p be a prime and let $f \in \mathbb{F}_p[X_1, X_2]$ be the product of $p+k$ linear polynomials in $\mathbb{F}_p[X_1, X_2]$. If there are at least $(p+1)/2+k \leq p-1$ elements $x \in \mathbb{F}_p$ with the property that $X_1^p - X_1$ is a factor of $f(X_1, x)$ then f has a factor*

$$X_1^p - X_1 - c(X_2+m)^{p-1} + c = \prod_{a_1 \in \mathbb{F}_p} (X_1 + a_1 X_2 + m a_1 + c),$$

for some $m, c \in \mathbb{F}_p$.

Proof. Define polynomials $h_j(X_2)$ of degree at most j by writing

$$f(X_1, X_2) = \sum_{j=0}^{p+k} h_j(X_2) X_1^{p+k-j}.$$

Let $\mathcal{E} = \{x \in \mathbb{F}_p \mid X_1^p - X_1 \text{ divides } f(X_1, x)\}$.

If $x \in \mathcal{E}$ then

$$f(X_1, x) = (X_1^p - X_1) g(X_1)$$

for some $g(X_1)$, dependent on x, of degree at most k. Therefore $h_{k+1}(x) = \ldots = h_{p-1}(x) = 0$. Since a non-zero polynomial h has at most h° roots, the polynomials $h_{k+1}(X_2) = \ldots = h_{|\mathcal{E}|-1}(X_2) = 0$.

Therefore

$$f(X_1, X_2) = \sum_{j=0}^{k} h_j(X_2) X_1^{p+k-j} + \sum_{j=|\mathcal{E}|}^{p+k} h_j(X_2) X_1^{p+k-j}.$$

If $y \notin \mathcal{E}$ then

$$f(X_1, y) = X^p g(X_1) + h(X_1),$$

where $\max(g^\circ, h^\circ) = k \leq (p-1)/2$ and $X_1^p - X_1$ is not a factor. By Lemma 4.1,

$$f(X_1, y) = g(X)(X^p + c)$$

where $c \in \mathbb{F}_p$. Note that here we use the fact that we are working over a prime field.

The polynomial $f(X_1, y)$ has a factor $X_1 + c$ of multiplicity p and so $f(X_1, X_2)$ has p factors $X_1 + a_1 X_2 + a_2$ for which $a_1 y + a_2 = c$. Defining $m = -y$ proves the theorem. □

Let us return to the set of points $\mathcal{S}$.

COROLLARY 4.4. *Let $\mathcal{S}$ be a set of points of $AG(2, p)$. If there are at least $|\mathcal{S}| - (p-1)/2$ and at most $p-1$ parallel classes for which the lines of these parallel classes are all incident with at least one point of $\mathcal{S}$ then $\mathcal{S}$ contains all the points of a line.*

Proof. Since there are at most $p-1$ parallel classes for which the lines of these parallel classes are all incident with at least one point of $\mathcal{S}$, we can assume that there is an m such that the parallel class of lines defined by equations $X_2 = mX_1 + c$ are not all incident with a point of $\mathcal{S}$.

Define

$$f(X_1, X_2) = \prod_{s \in \mathcal{S}} (X_1 + s_1 X_2 + s_2),$$

a product of $|\mathcal{S}| = p+k$ linear polynomials. By hypothesis there are at least $(p+1)/2+k$ elements $x \neq m$ with the property that $X_1^p - X_1$ is a factor of $f(X_1, x)$.

Applying Theorem 4.3, we can conclude that $\mathcal{S}$ contains all the points on the line $X_2 = mX_1 + c$, for some c. □

The corollary above implies Blokhuis' theorem on blocking sets in PG$(2, p)$.

COROLLARY 4.5. *Let $\mathcal{B}$ be a set of points in PG$(2, p)$ with the property that every line is incident with at least one point of $\mathcal{B}$. If $|\mathcal{B}| \leq (3p+1)/2$ then $\mathcal{B}$ contains all the points of a line.*

Proof. Suppose that $|\mathcal{B}| \leq (3p+1)/2$. Let l_∞ be a line which is incident with $n \geq 2$ points of $\mathcal{B}$. Let $\mathcal{S} = \mathcal{B} \setminus l_\infty$. Then $|\mathcal{S}| = |\mathcal{B}| - n$ and there are $p+1-n$ parallel classes for which the lines of these parallel classes are all incident with at least one point of $\mathcal{S}$. Since $p-1 \geq p+1-n \geq |\mathcal{S}| - (p-1)/2$ we can apply Corollary 4.4. Hence $\mathcal{B}$ contains all the points of an affine line. If it does not contain the point where this line meets l_∞ then it must contain a point on the p other lines through this point, which would imply $|B| \geq 2p$. □

We are, of course, also interested in the case $q = p^h$ non-prime. It is conjectured that a minimal blocking set in PG$(2, q)$ of size at most $(3q+1)/2$ is of a certain type but this will not be discussed here. It is known that every line is incident with 1 mod p points of a minimal blocking set of size at most $(3q+1)/2$, from the work of Szőnyi [46], see also [43].

There have been some results obtained using lacunary polynomials in several indeterminates, see for example [13], [31]. However, it seems that many of these can also be obtained using field extensions as we shall see in Section 6, so they will not be directly discussed here.

5 Vector spaces of polynomials and functions over $\mathbb{F}_q$

Let $\mathbb{K}$ be a field.

Let $\mathcal{E}$ be a non-empty subset of $\mathbb{K}^n$. The set $\mathcal{E}^{\mathbb{F}_q}$ of functions from $\mathcal{E}$ to $\mathbb{F}_q$ is a vector space over $\mathbb{F}_q$ of dimension $|\mathcal{E}|$. A basis for this vector space is

$$\{f_y \mid y \in \mathcal{E}\},$$

where $f_y(x) = 1$ if $y = x$ and $f_y(x) = 0$ if $y \neq x$.

The set $\mathbb{K}_d[X_1, \ldots, X_n]$ of polynomials of degree at most d with coefficients from $\mathbb{K}$ is a vector space over $\mathbb{F}_q$ of dimension $\binom{n+d}{d}$. It has a basis

$$\{X_1^{d_1} \cdots X_n^{d_n} \mid d_1 + \ldots + d_n \leq d\}.$$

The set $\mathbb{K}_{[d]}[X_1, \ldots, X_n]$ of polynomials of degree at most d in each variable, and with coefficients from $\mathbb{K}$, is a vector space over $\mathbb{F}_q$ of dimension $(d+1)^n$. It has a basis

$$\{X_1^{d_1} \cdots X_n^{d_n} \mid d_i \leq d\}.$$

LEMMA 5.1. *For every function $\phi \in (\mathbb{F}_q^n)^{\mathbb{F}_q}$ there is a unique polynomial $f \in (\mathbb{F}_q)_{[q-1]}[X_1, \ldots, X_n]$ with the property that $\phi(x) = f(x)$ for all $x \in \mathbb{F}_q^n$.*

Proof. By Alon's Nullstellensatz, Theorem 2.1, a polynomial $f(X_1,\ldots,X_n)$, with the property that $f(x)=0$ for all $x\in\mathbb{F}_q^n$, is an element of the ideal

$$I=\langle X_1^q-X_1,\ldots,X_n^q-X_n\rangle.$$

If f and g are polynomials in n variables whose evaluations define the same function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ then $f-g\in I$. If they are both of degree at most $q-1$ in each variable then $f=g$.

The vector space of functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ has dimension q^n and this set of polynomials in n variables of degree at most $q-1$ in each variable also has dimension q^n. Thus, each function $\phi\in(\mathbb{F}_q^n)^{\mathbb{F}_q}$ is uniquely represented by a polynomial f, of degree at most $q-1$ in each variable, where $\phi(x_1,\ldots,x_n)=f(x_1,\ldots,x_n)$. □

We shall now use this observation to obtain shorter proofs of Theorem 2.2. The following proof is due to Blokhuis, Brouwer and Szőnyi [21].

Proof. The polynomials $f_b(X_1,\ldots,X_n)=f(X_1-b_1,\ldots,X_n-b_n)$ have the property that $f_b(b)=1$ and $f_b(a)=0$ for $a\neq b$. Thus, their evaluations form a basis for the vector space $(\mathbb{F}_q^n)^{\mathbb{F}_q}$ and therefore a basis for the set of polynomials in n variables of degree at most $q-1$ in each variable. This set contains the monomial $X_1^{q-1}\cdots X_n^{q-1}$, so f has must have degree at least $n(q-1)$. □

The following proof, which was noted by Pepe [39], is similar to that of Bruen [29, Theorem 1.8, Proof 1] and Wilson [29, Theorem 1.8, Proof 3].

Proof. Let $f_0=f \bmod I$, where the degree of f_0 in each indeterminate is at most $q-1$. The function defined by evaluating f is the same as the function defined by evaluating the polynomial

$$g(X)=\prod_{i=1}^{n}(1-X_i^{q-1}),$$

which is the same as the function defined by evaluating f_0. However, the degree of f_0 in each indeterminate is at most $q-1$ and so $f_0=g$. Hence, the degree of f is at least $n(q-1)$. □

We will apply the following lemma to a distinct geometrical problem. In the following we are interested in the degree of the polynomial and not the degree in each variable.

LEMMA 5.2. *Let $\mathcal{E}$ be a subset of $\mathbb{F}_q^n$. If*

$$|\mathcal{E}|<\binom{d+n}{d}$$

then there is a non-zero polynomial f of degree at most d with the property that $f(x)=0$ for all $x\in\mathcal{E}$.

Proof. The dimension of the vector space of functions from $\mathcal{E}$ to $\mathbb{F}_q$ is $|\mathcal{E}|$. The dimension of the vector space of polynomials in n variables of degree at most d is $\binom{d+n}{d}$. Since $|E|<\binom{d+n}{d}$ there are distinct polynomials g and h which agree on $\mathcal{E}$. Let $f=g-h$. □

Suppose that a subset $\mathcal{E}$ of $AG(n,q)$ has the property that for any direction m, there is a line ℓ with direction m contained in $\mathcal{E}$. In other words, all the points of ℓ are points of $\mathcal{E}$. A set $\mathcal{E}$ with such a property is sometimes called a Besikovitch set and is related to the Kakeya problem which concerns the real space analogue. We wish to prove a lower bound for $|\mathcal{E}|$.

The following Lemma 5.3 and Theorem 5.4 are due to Dvir [32].

LEMMA 5.3. *Let $\mathcal{E}$ be a set of points of $AG(n,q)$ which contains a line in every direction. A non-zero polynomial f, which is zero at all elements of $\mathcal{E}$, has degree at least q.*

Proof. The geometrical property that $\mathcal{E}$ contains a line in every direction translates to the following algebraic property of f. Namely, for all $y \in \mathbb{F}_q^n$, $y \neq 0$, there is an x with the property that $f(x+\lambda y) = 0$ for all $\lambda \in \mathbb{F}_q$.

Suppose that $f^\circ = d \leq q-1$. Write

$$f(X+\lambda Y) = \sum_{i=1}^{d} g_i(X,Y)\lambda^i.$$

The polynomial g_d is non-zero, of degree d and depends only on Y, so we can write $g_d(X,Y) = g_d(Y)$.

Since $d \leq q-1$ and f vanishes for all $\lambda \in \mathbb{F}_q$, for each i, the coefficient of λ^i is zero. Specifically $g_d(y) = 0$. By Alon's Nullstellensatz, Theorem 2.1, $g_d \in \langle Y_1^q - Y_1, \ldots, Y_n^q - Y_n \rangle$. However, the polynomial g has degree $d \leq q-1$ and so $g_d = 0$, which is a contradiction. Therefore $f^\circ \geq q$. □

THEOREM 5.4. *A set of points $\mathcal{E}$ of $AG(n,q)$ which contains a line in every direction contains at least $\binom{n+q-1}{n}$ points.*

Proof. If not then by Lemma 5.2, there is a non-zero polynomial f of degree at most $q-1$ which is zero on $\mathcal{E}$, which contradicts Lemma 5.3. □

There are many questions which arise as a result of Dvir's Theorem, the most obvious being to ask how good the bound is. For $n = 2$, it is tight for q even and can be improved to $q(q+1)/2 + (q-1)/2$ for q odd. Blokhuis and Mazzocca [23] classified all sets which meet this bound for q odd. For $n = 3$, it is not clear if a lower bound of approximately $q^3/6$ is near to being the true value. For n large and q small, there are probably better bounds to be found.

There are some obvious generalisations to be considered. If we replace lines by k-dimensional subspaces, for example, or if we replace one line in every direction with t lines in every direction. For the moment, this has yet to be done.

The approach of Dvir should be applicable to more geometrical problems, as should the following idea, which was developed by Gács.

Consider again $\mathcal{S}$, the graph of a function ϕ from $\mathbb{F}_q$ to $\mathbb{F}_q$. The set $\mathcal{S}$ contains q points and is a subset of points of $\mathrm{AG}(2,q)$ (and therefore of $\mathbb{F}_q^2$). Applying Lemma 5.2, we have that there is a non-zero polynomial $f(X_1,X_2)$ of degree less than $\sqrt{2q}$ with the property that $f(x_1,x_2) = 0$ for all $x \in \mathcal{S}$. In other words, $\mathcal{S}$ lies on an algebraic curve of degree at most $\sqrt{2q}$.

Gács was interested in the case that the function ϕ is a map from $\mathbb{F}_p$ to $\mathbb{F}_p$, where p is a prime. By Corollary 4.4, if the number of directions $M(\phi)$, not determined by ϕ, is at least $(p+1)/2$ then ϕ is linear. Lovász and Schrijver [38] proved that if $M(\phi) = (p-1)/2$ then the graph of the function ϕ is affinely equivalent to the graph of the function $x \mapsto x^{(p+1)/2}$. Megyesi [40] provided examples of functions where $M(\phi) = (p-1)/d$, whenever $p = 1 \mod d$, using the multiplicative subgroup of $\mathbb{F}_p$ of index d. In Megyesi's examples the graph of the function is contained in the union of two lines and so in an algebraic plane curve of degree two. Gács wanted to prove that there were no examples of functions ϕ for which $(p-1)/3 < M(\phi) < (p-1)/2$, which he almost succeeded in doing. In [34], he proved the following.

THEOREM 5.5. *If $M(\phi) > (p+2)/3$ then the graph of ϕ is contained in the union of two lines.*

This allowed him to apply the following theorem of Szőnyi [44]. Note that the generalised examples of Megyesi mentioned in the following also have $M(\phi) = (p-1)/d$, for some d dividing $p-1$.

THEOREM 5.6. *If $M(\phi) \geq 2$ and the graph of ϕ is contained in the union of two lines then f is affinely equivalent to a generalised example of Megyesi.*

In [10], his approach, which we shall summarise below, led to the following theorem and conjecture. Let $\varepsilon = 0$ if $M(\phi)$ is even and $\varepsilon = 1$ if $M(\phi)$ is odd.

THEOREM 5.7. *If $M(\phi) > (p-1-2\varepsilon)/t + t - 3 + \varepsilon$ for some integer $t \geq 2$, then every line of $AG(2,p)$ is incident with at least $M(\phi) + 4 - t$ points of the graph of ϕ or at most $t-1$ points of the graph of ϕ.*

CONJECTURE 5.8. *If $M(\phi) > (p-1-2\varepsilon)/t + t - 3 + \varepsilon$ for some integer $t \geq 2$, then the graph of ϕ is contained in an algebraic curve of degree $t-1$.*

The Gács approach starts in the same way as that of Lovász and Schrijver [38]. If $-c$ is a direction not determined by ϕ then the map

$$x \mapsto \phi(x) + cx$$

is a permutation. By [37, Lemma 7.3], $-c$ is a zero of the polynomials

$$h_k(Y) = \sum_{x \in \mathbb{F}_p} (\phi(x) + xY)^k = \sum_{i+j=k} \sum_{x \in \mathbb{F}_p} \binom{k}{i} x^j \phi(x)^i Y^j,$$

for $p-2 \geq k \geq 1$. The degree of these polynomials h_k is at most $k-1$ and so for $1 \leq k \leq M(\phi) - 1$ the polynomials h_k are zero. Since $k < p$ the binomial coefficient $\binom{k}{i} \neq 0$ and so we conclude that

$$\sum_{x \in \mathbb{F}_p} x^j \phi(x)^i = 0,$$

for all $1 \leq i + j \leq M(\phi) - 1$.

For any polynomial $g(X) = \sum_{i=0}^{p-1} g_i X^i$, of degree at most $p-1$, the sum

$$\sum_{x \in \mathbb{F}_p} g(x) = -g_{p-1}.$$

Therefore the above implies that the polynomial that represents the function $\phi(x)^i$ has degree at most $p - M(\phi) + i - 1$ for $i = 1, \ldots, M(\phi) - 1$.

The dimension of a subspace of polynomials is equal to the number of distinct degrees of polynomials occuring in the subspace.

We wish to combine this fact with our observation that the polynomials

$$\sum_{i=1}^{M(\phi)-1} F_i \phi^i,$$

where $F_i^\circ \leq M(\phi) - i - 1$, are of degree at most $p-2$.

In [10], linear maps ψ from $\{(F_1, \ldots, F_s) \mid F_i^\circ \leq s - i\}$ to $\mathbb{F}_p[X]$, defined by

$$\psi(F_1, \ldots, F_s) = F_1\phi + \ldots + F_s\phi^s$$

are considered. If $s < M(\phi)/2$ then for all polynomials $g, h \in \mathrm{Im}(\psi)$ the product gh does not have degree $p-1$. Since it can be written as a sum of the type

$$\sum_{i=1}^{M(\phi)-1} G_i \phi^i,$$

where $G_i^\circ \leq M(\phi) - i - 1$, it has degree at most $p-2$.

Therefore, only half the degrees can occur amongst the polynomials in $\mathrm{Im}(\psi)$ and so its dimension is bounded by roughly $p/2$. This then gives a lower bound for the dimension of the kernel of ψ. For an element $(F_1, \ldots, F_s)$ in the kernel of ψ and x, not a zero of ϕ,

$$-F_1 = F_2\phi + \ldots + F_s\phi^{s-1}.$$

If the number of zeros of ϕ is limited then this equation is valid for sufficiently many elements that it is a polynomial identity. The condition that ϕ has few zeros is equivalent to saying that the line, defined by the second coordinate is zero, contains few points of the graph of ϕ. This line can be chosen arbitrarily so, under the assumption that some line is incident with a bounded number of points of the graph of ϕ, we can consider further iterative linear maps reducing s by one each time. Note that Conjecture 5.8 is true if and only if the map ψ has a non-trivial kernel when $s = t - 1$.

This approach should extend to other combinatorial objects. One could hope to obtain further properties for any object that can be parameterised by a function ϕ (which may be in several indeterminates) and whose combinatorial property implies that the powers of ϕ are represented by polynomials which do not have certain degrees.

6 Field extensions as vector spaces

The field $\mathbb{F}_{q^h}$ is a vector space of dimension h over $\mathbb{F}_q$. Since $\mathrm{PG}(n-1,q)$ and $\mathrm{AG}(n,q)$ are constructed from the n-dimensional vector space over $\mathbb{F}_q$, one can also construct them from $\mathbb{F}_{q^n}$, or more generally from

$$\prod_{i=1}^{k} \mathbb{F}_{q^{r_i}},$$

where $\sum_{i=1}^{k} r_i = n$ and $r_1 | r_2 | \ldots | r_k$. Note that the last condition implies that all the fields $\mathbb{F}_{q^{r_i}}$ are subfields of $\mathbb{F}_{q^{r_k}}$.

Up until now we have only considered the case $r_1 = \ldots = r_n = 1$. Let us consider the other extremal case $r_1 = n$.

The hyperplanes of the vector space $\mathbb{F}_{q^n}$ are defined by equations of the form $Tr(ax) = 0$, where a is a non-zero element of $\mathbb{F}_{q^n}$ and

$$Tr(X) = X + X^q + \ldots + X^{q^{n-1}}.$$

The k-dimensional subspaces are defined by equations of the form $f(x) = 0$, where

$$f(X) = X^{q^k} + b_{k-1}X^{q^{k-1}} + \ldots + b_1 X^q + b_0 X,$$

and the b_i satisfy relations, which are determined by the divisibility $f(X)$ divides $X^{q^n} - X$.

In the case of the 1-dimensional subspaces, $X^q - aX$ divides $X^{q^n} - X$ if and only if $a^{(q^n-1)/(q-1)} = 1$.

In $\mathrm{AG}(n,q)$ the lines are cosets of the one-dimensional subspaces of $\mathbb{F}_q^n$ and so are defined by equations of the form

$$x^q - ax = b.$$

The points are cosets of the zero dimensional subspace and so are simply the elements of $\mathbb{F}_{q^n}$. For the line joining the points x and y, $a = (x-y)^{q-1}$, which corresponds to the direction of the line. The point z is on this line if and only if $(x-z)^{q-1} = (x-y)^{q-1}$, so we can interpret this condition as a collinearity condition for three points x, y and z.

Let $\mathcal{S}$ be a subset of points of $\mathrm{AG}(n,q)$ in this model, so $\mathcal{S}$ is a subset of $\mathbb{F}_{q^n}$. Consider the polynomial

$$f(T,X) = \prod_{s \in \mathcal{S}} (T - (X-s)^{q-1}).$$

Two factors of $f(T,x)$ are the same if and only if there are two elements $s,t \in \mathcal{S}$, for which $(x-s)^{q-1} = (x-t)^{q-1}$; or in other words, if x, s and t are collinear. Thus, the polynomial f can be used for any set of points $\mathcal{S}$ of $\mathrm{AG}(n,q)$ which has some regular property with respect to lines. Note that the linear factors of $f(T,x)$ are factors of the polynomial $T^{(q^n-1)/(q-1)} - 1$.

Blokhuis [17] used this model with $n = 2$ to prove Theorem 6.1. An *external nucleus* to a set of points $\mathcal{S}$ is a point x with the property that every line incident with x is incident with at least one point of $\mathcal{S}$.

THEOREM 6.1. *A set $\mathcal{S}$ of $q+k$ points of $AG(2,q)$ has at most $k(q-1)$ external nuclei.*

Proof. We can assume that $k \leq q-1$ otherwise there is nothing to prove. For any external nucleus x, the polynomial $f(T,x)$ has every factor of $T^{q+1}-1$ amongst its linear factors. Therefore, there is a polynomial $g(T,x)$, of degree $k-1$, for which

$$f(T,x) = (T^{q+1}-1)g(T,x).$$

The coefficient of T^q in f is a polynomial $\sigma(X)$, which by definition is

$$(-1)^k \sum (X-s_1)^{q-1} \dots (X-s_k)^{q-1},$$

where the sum is taken over all k-subsets of $\mathcal{S}$. There are $\binom{|S|}{k} = \binom{q+k}{k}$ such subsets and so the leading term has degree $k(q-1)$ and coefficient $(-1)^k\binom{q+k}{k} = (-1)^k$.

For any external nucleus x we have seen that $\sigma(x) = 0$ and since σ is a polynomial of degree $k(q-1)$, there are at most $k(q-1)$ external nuclei. □

The bound in Theorem 6.1 is attainable by taking, for example, $\mathcal{S} = \ell \cup \{x_1, \dots, x_k\}$, where ℓ is a line and the points $x_1, \dots, x_k$ are points on distinct lines parallel to ℓ.

Blokhuis extended Theorem 6.1 to t-fold nuclei [18], where a *t-fold external nucleus* to a set of points $\mathcal{S}$ is a point x with the property that every line incident with x is incident with at least t points of $\mathcal{S}$.

Let us consider another application of the polynomial f. Suppose $\mathcal{S}$ is a set of points with the property that every line of $\mathrm{AG}(2,q)$ is incident with a multiple of r points, for some fixed r. It is trivial to prove that $|\mathcal{S}| \geq (r-1)q + r$ and that r divides q. We shall sketch a proof that the lower bound can be improved to $|\mathcal{S}| \geq (r-1)q + (p-1)r$, where $q = p^h$. This implies that, for q odd, there are no non-trivial sets of points with intersection number 0 or r (so-called *maximal arcs*), which was the main result of [9] and [7]. The result stated here is from [8], although the sketched proof is that used to prove the main result of [7].

THEOREM 6.2. *If $\mathcal{S}$ is a set of points of $AG(2,q)$ with the property that every line is incident with a multiple of r points of $\mathcal{S}$ then $|S| \geq (r-1)q + (p-1)r$.*

Proof. (sketch) Suppose that $|\mathcal{S}| = (r-1)q + kr$, where $k < p-1$.

The geometrical property translates to the following algebraic properties for the polynomial f. Namely, if $x \in \mathcal{S}$ then

$$f(T,x) = T(T^{q+1}-1)^{r-1} g(T)^r,$$

where g is a polynomial of degree at most $(k-1)r$. If $x \notin \mathcal{S}$ then $f(T,x)$ has factors repeated a multiple of r times and so is an r-th power. As in the proof of Theorem 6.1, we focus on one particular coefficient of f, in this case the coefficient $\sigma(X)$ of $T^{|S|-kr}$. As in the proof of Theorem 6.1, we can deduce that it has a leading term of degree $kr(q-1)$. If $x \in \mathcal{S}$ then the fact that $g(T)$ has degree at most $(k-1)r$ implies $\sigma(x) = 0$. Thus the polynomial

$$a(X) = \prod_{s \in \mathcal{S}} (X-s)$$

divides $\sigma(X)$. One then exploits the divisibility

$$f(T,x) \text{ divides } (T^{q+1}-1)\frac{\partial f}{\partial X}(T,x)$$

to prove that $a(X)^{p-1}$ divides $\sigma(X)$. This implies that $(p-1)|\mathcal{S}| \leq kr(q-1)$ which gives $k \geq p-1$. □

Let us consider how to use another representation of $\mathbb{F}_q^n$, specifically

$$\prod_{i=1}^{k} \mathbb{F}_{q^{r_i}},$$

where $r_1 = 1$ and $r_2 = n-1$.

The points of the affine space $\mathrm{AG}(n,q)$ are elements of

$$\mathbb{F}_q \times \mathbb{F}_{q^{n-1}}.$$

Suppose that $s = (s_1, s_2)$ and $t = (t_1, t_2)$ are points of $\mathrm{AG}(n,q)$. The direction of the line joining s and t is given by the projective point $\langle (s_1 - t_1, s_2 - t_2) \rangle$, which if $s_1 \neq t_1$ is the point $\langle (1,x) \rangle$ where

$$x = \frac{s_2 - t_2}{s_1 - t_1}.$$

We shall look at two related problems with this representation and use slightly differing polynomials. In the first problem we wish to obtain further geometrical properties for the higher dimensional analogue of the graph of a function which determines few directions and in the second problem we shall prove a stability result for such graphs.

Let ϕ be a function from $\mathbb{F}_q^{n-1}$ to $\mathbb{F}_q$. The graph of the function ϕ is the set of points

$$\{(\phi(s_2), s_2) \mid s_2 \in \mathbb{F}_{q^{n-1}}\}.$$

Let $M(\phi)$ be the number of directions not determined by ϕ. Let $\mathcal{S}$ be a set of q^{n-1} points of $\mathrm{AG}(n,q)$, affinely equivalent to the graph of ϕ, for which the number of points of $\mathcal{S}$ on the hyperplane defined by the first coordinate being zero, is not q^{n-2}. This condition implies that the directions not determined by the set of points $\mathcal{S}$ are not of the form $\langle (0,x) \rangle$ for any $x \in \mathbb{F}_{q^{n-1}}$.

Consider the polynomial

$$h(T,X) = \prod_{s \in \mathcal{S}} (T - (s_1 X - s_2)^{q-1}).$$

If $\langle (1,x) \rangle$ is a direction not determined by $\mathcal{S}$ then $s_1 x - s_2 \neq t_1 x - t_2$ and so $s_1 x - s_2$ are distinct values of $\mathbb{F}_{q^{n-1}}$. Therefore

$$h(T,x) = \prod_{\lambda \in \mathbb{F}_{q^{n-1}}} (T - \lambda^{q-1}) = T(T^{(q^{n-1}-1)/(q-1)} - 1)^{q-1}. \tag{1}$$

The polynomial h allows us to prove the following theorem from [6], which improves on a similar result in [14], where the representation $r_1 = \ldots = r_n = 1$ was used.

Let $q = p^h$, p prime.

THEOREM 6.3. *If, for some non-negative integer $e \leq (n-2)h - 1$, there are more than $p^e(q-1)$ directions not determined by a set $\mathcal{S}$ of q^{n-1} points of $AG(n,q)$ then every hyperplane is incident with a multiple of p^{e+1} points of $\mathcal{S}$.*

Proof. The coefficient of $T^{q^{n-1}-p^e}$ in $h(T,X)$ is a polynomial $\sigma(X)$ which, by definition, is

$$(-1)^{p^e}\sum(s_1X-s_2)^{q-1}\dots(t_1X-t_2)^{q-1},$$

where the sum is taken over all p^e-subsets of $\mathcal{S}$. The coefficient of $X^{p^e(q-1)}$ is

$$\sum s_1^{q-1}\dots t_1^{q-1}$$

where the sum is taken over all p^e-subsets of $\mathcal{S}$. Note that $s_1 \in \mathbb{F}_q$, so the terms in this sum are 1 for every p^e subset of $\mathcal{S}$ in which all the points in the subset have first-coordinate non-zero. Let N be the number of points in $\mathcal{S}$ with first coordinate zero. Then the coefficient of $X^{p^e(q-1)}$ in $\sigma(X)$ is $\binom{|\mathcal{S}|-N}{p^e} = \binom{-N}{p^e}$.

On the other hand, if $\langle(1,x)\rangle$ is a direction not determined by $\mathcal{S}$ then (1) implies that $\sigma_{p^e}(x) = 0$. By assumption, there are more than $p^e(q-1)$ directions not determined by $\mathcal{S}$ and the degree of σ is at most $p^e(q-1)$, so we conclude that it is identically zero. Therefore $N = 0$ modulo p^{e+1} and so the number of points of $\mathcal{S}$, on the hyperplane of points with first coordinate zero, is 0 mod p^{e+1}. Since this hyperplane was chosen arbitrarily, the theorem is proved. □

Theorem 6.3 has an immediate corollary for ovoids of the parabolic quadric $\mathrm{Q}(4,q)$. Indeed, using the Tits representation of $\mathrm{Q}(4,q)$ as $\mathrm{T}_2(O)$, where O is a conic, one obtains the following result, which first appeared in [5] and for $p = 2$ in [2].

COROLLARY 6.4. *An ovoid of $Q(4,q)$ and an elliptic quadric $Q^-(3,q)$ embedded in $Q(4,q)$ intersect in* 1 *modulo p points, where $q = p^h$.*

With some combinatorial counting this leads to the following theorem from [12].

THEOREM 6.5. *An ovoid of $Q(4,p)$, where p is prime, is an elliptic quadric.*

Corollary 6.4 can be improved in the q even case. The following is from [30].

THEOREM 6.6. *An ovoid of $Q(4,q)$ and an elliptic quadric $Q^-(3,q)$ embedded in $Q(4,q)$ intersect in* 1 *modulo* 4 *points, where $q = 2^h$.*

Theorem 6.3 implies that if $\mathcal{S}$ is a set of p^2 points in $\mathrm{AG}(3,p)$, which does not determine at least p directions, then every plane is incident with a multiple of p points of $\mathcal{S}$. The only examples which we are aware of which have this property are the cylinders, i.e. the points on the union of p parallel lines. This leads to the following conjecture, which is called the *strong cylinder conjecture*.

CONJECTURE 6.7. *If $\mathcal{S}$ is a set of p^2 points in $AG(3,p)$ with the property that every plane is incident with a multiple of p points of $\mathcal{S}$ then $\mathcal{S}$ is a cylinder.*

We shall use the same representation of $\mathrm{AG}(n,q)$ to prove a stability result for sets of points that do not determine all directions. Here we shall use a slightly different (although somewhat familiar) polynomial

$$e(X_1,X_2) = \prod_{s\in\mathcal{S}}(X_1+s_1X_2+s_2).$$

As for the polynomial $f(X_1,x)$, we conclude that if $\mathcal{S}$ is a set of q^{n-1} points and $\langle(1,-x)\rangle$ is a direction not determined by $\mathcal{S}$ then

$$e(X_1,x) = X_1^{q^{n-1}} - X_1.$$

Now consider a set $\mathcal{S}$ of $q^{n-1}-2$ points and suppose that $\mathcal{D}$ is the set of directions not determined by $\mathcal{S}$. We wish to show that if $\mathcal{D}$ is large enough then $\mathcal{S}$ can be extended to a set of q^{n-1} points which do not determine the directions $\mathcal{D}$. This type of result is called a stability theorem.

More precisely we prove the following, which was proved in [31] using the representation $r_1 = \ldots = r_n = 1$.

THEOREM 6.8. *A set of $q^{n-1}-2$ points of $AG(n,q)$, $q=p^h$ odd, which does not determine a set $\mathcal{D}$, of at least $p+2$ directions, can be extended to a set of q^{n-1} points not determining the set of directions $\mathcal{D}$.*

Proof. Writing $e(X_1,X_2)$ as a polynomial in X_1, we define polynomials $\sigma_j(X_2)$ of degree at most j by

$$e(X_1,X_2) = \sum_{j=0}^{|\mathcal{S}|} \sigma_j(X_2) X_1^{|\mathcal{S}|-j}.$$

The polynomial

$$\sigma_1(X_2) = \sum_{s\in\mathcal{S}} (s_1X_2 + s_2).$$

By making the translation $(s_1,s_2) \mapsto (s_1+\lambda_1, s_2+\lambda_2)$, where $\lambda_1 = (\sum_{s\in\mathcal{S}} s_1)/2$ and $\lambda_2 = (\sum_{s\in\mathcal{S}} s_2)/2$, then we can assume $\sigma_1(X_2) = 0$. Here we use the assumption q is odd.

Suppose that $\langle(1,-x)\rangle$ is a direction not determined by $\mathcal{S}$. Then, by the discussion preceding the theorem,

$$e(X_1,x)(X_1^2 - \sigma_2(x)) = X_1^{q^{n-1}} - X_1.$$

This implies that $\sigma_{2k}(x) = \sigma_2(x)^k$ for all $k < q^{n-1}/2$.

Let $\pi_k(X_2) = \sum_{s\in\mathcal{S}} (s_1X_2+s_2)^k$. The Newton identities relate the symmetric functions σ_k and the power sums π_k by the equations

$$k\sigma_k = \sum_{j=1}^{k} (-1)^{j-1} \pi_j \sigma_{k-j}.$$

Solving these equation recursively implies $\pi_{2k} = -2\sigma_2^k$. Thus, for $2k = p+1$, we have

$$(-2\sigma_2)(x)^{(p+1)/2} = \sum_{s\in\mathcal{S}} (s_1x+s_2)^{p+1} = c_{p+1}x^{p+1} + c_px^p + c_1x + c_0,$$

for some $c_i \in \mathbb{F}_{q^{n-1}}$.

Write $-2\sigma_2(X_2) = d_2X_2^2 + d_1X_2 + d_0$. We have shown that the polynomial

$$(d_2X_2^2 + d_1X_2 + d_0)^{(p+1)/2} - (c_{p+1}X_2^{p+1} + c_pX_2^p + c_1X_2 + c_0)$$

is zero for every direction not determined by $\mathcal{S}$. Since, by assumption, there are at least $p+2$ of these, this polynomial is zero. Thus, either $d_0 = d_1 = c_0 = c_1 = c_p = 0$ and $d_2^{(p+1)/2} = c_{p+1}$, or $d_2 = d_1 = c_{p+1} = c_p = c_1 = 0$ and $d_0^{(p+1)/2} = c_0$.

In the first case $\sigma_2(X_2) = d_2 X_2^2$. When $\langle (1,-x) \rangle$ is not a direction determined by $\mathcal{S}$

$$T^2 - \sigma_2(x) = (T - d_2^{1/2}x)(T + d_2^{1/2}x),$$

so d_2 is a square. We can then extend $\mathcal{S}$ with the points $(-d^{1/2},0)$ and $(d^{1/2},0)$ without determining any of the directions not determined by $\mathcal{S}$. The other case is similar. □

Again, using the Tits representation of $\mathrm{Q}(4,q)$ as $\mathrm{T}_2(O)$, where O is a conic, Theorem 6.8 has the following consequences for partial ovoids of $\mathrm{Q}(4,q)$.

COROLLARY 6.9. *A partial ovoid of $Q(4,q)$, q odd and not a prime, of size q^2-1 can be extended to an ovoid.*

Curiously, for $q = 5, 7$ and 11, there are examples of partial ovoids of size q^2-1 which cannot be extended to an ovoid.

7 Algebraic curves over finite fields

In this section, we shall give an example of how to apply bounds on the number of points on an algebraic curve defined over $\mathbb{F}_q$ to a geometrical problem of the type discussed before.

The following is from Szőnyi [45].

LEMMA 7.1. *Suppose $f \in \mathbb{F}_q[X_1,X_2]$ is a polynomial of degree d. If f has no linear factor in $\mathbb{F}_q[X_1,X_2]$ and $2 \le d \le \sqrt{q}/2$ then f has at most $d(q+1)/2$ zeros in $\mathbb{F}_q^2$.*

Proof. Let N be the number of zeros of f in $\mathbb{F}_q^2$.

If f is absolutely irreducible then Weil's theorem [35, Corollary 2.29] implies

$$N \le q+1+(d-1)(d-2)\sqrt{q} \le d(q+1)/2.$$

If not then f factorises into irreducible factors $f = f_1 \dots f_k$ over the algebraic closure of $\mathbb{F}_q$. Let N_i be the number of zeros of f_i in $\mathbb{F}_q[X_1,X_2]$ and let d_i be the degree of f_i.

If $f_i \in \mathbb{F}_q[X_1,X_2]$ then Weil's theorem implies $N_i \le d_i(q+1)/2$.

If $f_i \notin \mathbb{F}_q[X_1,X_2]$ then by [35, Lemma 2.24] $N_i \le d_i^2 < d_i(q+1)/2$. Thus,

$$N \le \sum_{i=1}^{k} N_i \le (\sum_{i=1}^{k} d_i)(q+1)/2 = d(q+1)/2.$$

□

Using Lemma 7.1, we shall prove the following stability result for the graphs of functions from $\mathbb{F}_q$ to $\mathbb{F}_q$. Again this is from Szőnyi [45]. Compare this to Theorem 6.8.

THEOREM 7.2. *A set of $q-k > q-\sqrt{q}/2$ points of $AG(2,q)$ which does not determine a set $\mathcal{D}$, of more than $(q+1)/2$ directions, can be extended to a set of q points not determining the set of directions $\mathcal{D}$.*

Proof. For any polynomial f of degree n one can construct a polynomial g of degree m with the property that $fg = X^{n+m} + h$, where the degree of h is at most $n-1$, by choosing the coefficient of X^{m-j} in g, for $j = 1,\ldots,m$, in such a way that the coefficient of X^{n+m-j} on the right-hand side is zero.

Apply this observation to the polynomial

$$f(X_1,X_2) = \prod_{s\in\mathcal{S}}(X_1 + s_1X_2 + s_2),$$

with $m = k$, by considering this polynomial as a polynomial in X_1 with coefficients that are polynomials in X_2. The polynomial $g(X_1,X_2)$ obtained has overall degree at most k, and

$$f(X_1,X_2)g(X_1,X_2) = X_1^q + h(X_1,X_2),$$

where the degree of h in X_1 is at most $q-k-1$.

If $-x \in \mathcal{D}$, a direction not determined by $\mathcal{S}$, then $f(X_1,x)$ divides $X_1^q - X_1$. The quotient of this division is of degree k and so is $g(X_1,x)$. Therefore, $g(X_1,x)$ is the product of distinct linear factors over $\mathbb{F}_q$ and has k zeros in $\mathbb{F}_q$. Hence, $g(X_1,X_2)$ has $kM \geq k(q+1)/2$ zeros, where M is the number of directions not determined by $\mathcal{S}$. By Lemma 7.1, $g(X_1,X_2)$ has a linear factor $X_1 + t_1X_2 + t_2$ in $\mathbb{F}_q[X_1,X_2]$.

The set $\mathcal{S} \cup \{(t_1,t_2)\}$ does not determine a direction $-x$, not determined by $\mathcal{S}$, since $X_1 + t_1x + t_2$ is a factor of $g(X_1,x)$, whose factors are different to the factors of $f(X_1,x)$. In other words, for all $s \in \mathcal{S}$, $t_1x + t_2 \neq s_1x + s_2$. Thus, $\mathcal{S}$ can be extended, and repeating the above, can be extended to a set of q points, which does not determine any of the directions in $\mathcal{D}$. □

Further applications of bounds on the number of points on algebraic curves over finite fields from both Weil's lemma, those deduced from Stöhr-Voloch [42], and the number of points in the intersection of two curves deduced from Bezout's theorem, can be found in articles such as [11], [33] and [24].

8 Resultant of polynomials in two variables

In [47] Szőnyi showed that a generalisation of the resultant of two polynomials could be applied to finite geometrical problems. This was further developed by Weiner [49] and together with Szőnyi in [48].

Suppose that f and g are polynomials of degree n and at most $n-1$ respectively. Let $b = \sum_{i=0}^{m-1} b_iX^i + X^m$ and $a = \sum_{i=0}^{m-1} a_iX^i$ be polynomials of degree m and at most $m-1$ respectively, with the property that

$$af + bg = 0.$$

Considering the coefficients of $X^{n-m-1},\ldots,X^{n+m-1}$ gives $2m$ linear equations which can be written in matrix form

$$(a_1,\ldots,a_{m-1},b_0,\ldots,b_{m-1})R_m = (g_0,\ldots,g_{2m-1}),$$

where the entries in the $2m \times 2m$ matrix R_m are the suitable coefficients of f and g.

Suppose that $h = (f,g)$ has degree $n-k$.

If $m \geq k+1$ then there are multiple solution to the above equation, choosing b to be a non-constant multiple of f/h and $a = -bg/h$. Hence, the system of linear equations has multiple solutions and therefore $\det R_m = 0$.

If $m = k$ then there is a unique solution to the above equation $b = \gamma f/h$ and $a = -bg/h$, where γ is chosen so that b is monic. Thus, $\det R_k \neq 0$.

Now suppose that $f = f(X_1, X_2)$ and $g = g(X_1, X_2)$ are polynomials in two variables. By writing the polynomials as polynomials in X_1, with coefficients which are polynomials in X_2, the determinant $\det R_m$ becomes a polynomial in X_2.

LEMMA 8.1. *Suppose that there is an element $x_2 \in \mathbb{F}_q$ for which*

$$\deg(f(X_1,x_2), g(X_1,x_2)) = n-k.$$

If there are n_h elements $y \in \mathbb{F}_q$ for which

$$\deg(f(X_1,y), g(X_1,y)) = n-(k-h)$$

then

$$\sum_{h=1}^{k-1} h n_h \leq \deg(\det R_k).$$

Proof. (sketch) The determinant of the matrix R_k is a polynomial in X_2 and $(\det R_k)(x_2) \neq 0$ by the above discussion. If, for $y \in \mathbb{F}_q$, the degree of $(f(X_1,y), g(X_1,y))$ is $n-(k-h)$ then it can be shown that y is a zero of $\det R_k$ (of multiplicity h). The discussion preceding the lemma implies that y is a zero of $\det R_k$, if $h \geq 1$. □

This lemma has been applied to a variety of problems, see for example [47] and [49]. The following is from [48].

THEOREM 8.2. *Let $\mathcal{S}$ be a set of points of $AG(2,q)$ and suppose $|\mathcal{S}| \neq q$. Let n_h be the number of directions d for which exactly h of the lines with direction d are incident with $\mathcal{S}$. If $n_k \neq 0$ then*

$$\sum_{h=k+1}^{q} h n_h \leq (|\mathcal{S}|-k)(q-k).$$

Proof. Let

$$f(X_1,X_2) = \prod_{(s_1,s_2)\in\mathcal{S}} (X_1 + s_1X_2 + s_2) = \sum_{j=0}^{|\mathcal{S}|} f_j(X_2) X_1^{|\mathcal{S}|-j},$$

where the degree of $f_j(X_2)$ is at most j.

Consider the matrix R_k for $f(X_1,X_2)$ and $g(X_1,X_2) = X_1^q - X_1$. One should check that the determinant $\det R_k$ is a polynomial in X_2 of degree at most $(|\mathcal{S}|-k)(q-k)$.

If there are exactly t lines with direction m which are incident with $\mathcal{S}$ then $\deg(f(X_1,m), X_1^q - X_1) = t$. Since $n_k \neq 0$ we have that $\det R_k \neq 0$. Applying Lemma 8.1, the theorem follows. □

This theorem has Metsch's conjecture as a corollary.

COROLLARY 8.3. *Let $\mathcal{S}$ be a point set of $PG(2,q)$. Let x be a point not in $\mathcal{S}$. If there are exactly r lines incident with x that are incident with $\mathcal{S}$, then the total number of lines incident with $\mathcal{S}$ is at most*

$$1 + rq + (|\mathcal{S}| - r)(q + 1 - r).$$

Note that when $|S| = 2q - 2$ and $r = q$ then the above implies that the total number of lines incident with $\mathcal{S}$ is at most $q^2 + q - 1$, which gives yet another proof of Jamison's theorem, Corollary 2.3, in the plane.

9 Open problems

In this section I have listed some problems which we would like to see resolved. Most are stated in the form that implies a conjecture. For example, "Prove that" implies that the statement is thought more likely to hold than the contrary.

Section 3.

1. Let $1 \leq k \leq n-2$ and let $\mathcal{S}$ be a set of points of $\mathrm{AG}(n,q)$ with the property that every k-dimensional subspace is incident with a point of $\mathcal{S}$. It should be possibly to prove that there are examples for which $|\mathcal{S}|/(k+1)q^{n-k} \to 0$ as $q \to \infty$. It would be interesting to know the order of magnitude of $|\mathcal{S}| - (k+1)q^{n-k}$. In the smallest case $n = 3$ and $k = 1$ we only have that $c < |\mathcal{S}| - 2q^2 < 2q^{\frac{3}{2}}$ for some constant c.

2. Let $\mathcal{S}$ be a set of points of $\mathrm{AG}(n,q)$ with the property that every hyperplane is incident with at least t points of $\mathcal{S}$. Prove a lower bound for $|\mathcal{S}|$ of about $(t+n-1)q-n$ for most t. See [3] for a proof in the case $t \leq q-1$.

Section 4.

1. The projective plane $\mathrm{PG}(2,q)$ consists of points and lines which are the one and two dimensional subspaces of $\mathbb{F}_q^3$. If $q = p^t$, where p is prime, then these subspaces are respectively rank t and rank $2t$ subspaces of $\mathbb{F}_p^{3t}$. Here, rank refers to vector space dimension. Let $\mathcal{U}$ be a rank $(t+1)$ subspace of $\mathbb{F}_p^{3t}$. The set of points of $\mathrm{PG}(2,q)$ whose corrsponding rank t subspace has a non-trivial intersection with $\mathcal{U}$ is denoted $B(\mathcal{U})$, the *bubble* of $\mathcal{U}$. Prove that if $\mathcal{S}$ is a set of less than $3(q+1)/2$ points of $\mathrm{PG}(2,q)$ with the property that every line is incident with a point of $\mathcal{S}$ then $\mathcal{S} = B(\mathcal{U})$, for some rank $(t+1)$ subspace $\mathcal{U}$ of $\mathbb{F}_p^{3t}$.

Section 5.

1. Prove a lower bound for the size of a set $\mathcal{E}$ of points of $\mathrm{AG}(n,q)$ with the property that for every direction (slope, gradient) d there are at least t lines of direction d contained in $\mathcal{E}$.

2. Let π be a hyperplane of $\mathrm{PG}(n,q)$ and consider the affine space $PG(n,q) \setminus \pi$. We say that two affine subspaces $U_1 \setminus \pi$ and $U_2 \setminus \pi$ have the same direction if $U_1 \cap \pi = U_2 \cap \pi$. For a fixed k, prove a lower bound for the size of a set $\mathcal{E}$ of points of $\mathrm{AG}(n,q)$ with the property that for every direction d, there is at least one k-dimensional subspace of direction d contained in $\mathcal{E}$.

3. Prove Conjecture 5.8.

4. Apply Gács' approach to other geometrical objects that can be defined by one or more polynomials $f \in \mathbb{F}_p[X_1,\ldots,X_n]$, whose geometrical property implies that the power sums
$$\sum_{x\in\mathbb{F}_p^n} f(x)^i = 0,$$
for some i's.

Section 6.

1. Prove that an ovoid of $Q(4,q)$ and an elliptic quadric $Q^-(3,q)$ embedded in $Q(4,q)$ intersect in 1 mod p^r points, for some $2 \le r < h/2$, where $q = p^h$ for some prime p.

2. Prove the cylinder conjecture, Conjecture 6.7. If not, prove a weaker form of this conjecture in which one assume that there are at least p directions not determined by $\mathcal{S}$.

3. Prove a version of Theorem 6.8 in which a larger set $\mathcal{D}$ implies more stability. For example, if $|\mathcal{D}| > p^2$ then the $q^{n-1}-2$ can be replaced by $q^{n-1}-f(q)$, for some function of q.

Section 7.

1. In [24] some stability is proven for sets of $q+k$ points in $AG(2,q)$. Comparing this with Theorem 6.8 and Theorem 7.2, one may be able to extend this stability to sets of points in higher dimensional spaces.

2. In [11] the Stöhr-Voloch bound is used to prove that a set of p points in $AG(3,p)$, which does not determine approximately $p^2/3$ line directions (see Problem 2. of Section 5 for the definition of a line direction) is contained in a plane. Prove that this can be extended to p^2/d, for a larger $d \in \mathbb{N}$, with few exceptions. It may be possible using Gács' approach from Section 5.

Section 8.

1. Applications of Lemma 8.1 have centered on the cases $g(X_1,X_2) = X_1^q - X_1$ and $g(X_1,X_2) = \frac{\partial f}{\partial X_1}$. There is a huge scope for further applications here, using other polynomials for g, introducing more indeterminates, or even more polynomials.

10 Acknowledgements and final comments

There are also many results obtained using Menelaus theorem, an approach introduced by Segre in [41]. This is not elaborated here but some examples are included in [22], [25], [26] and [50].

I would like to thank Andras Gács, Peter Sziklai and Zsuzsa Weiner for their suggestions and corrections to an earlier version of this manuscript.

References

[1] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.*, **8** (1999) 7–29.

[2] B. Bagchi and N. S. Narasimha Sastry, Even order inversive planes, generalized quadrangles and codes, *Geom. Dedicata*, **22** (1987) 137–147.

[3] S. Ball, On intersection sets in Desarguesian affine spaces, *European J. Combin.*, **21** (2000) 441–446.

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

[5] S. Ball, On ovoids of O(5,q), *Adv. Geom.*, **4** (2004) 1–7.

[6] S. Ball, On the graph of a function in many variables over a finite field, *Des. Codes Cryptogr.*, **47** (2008) 159–164.

[7] S. Ball and A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.*, **126** (1998) 3377–3380.

[8] S. Ball, A. Blokhuis, A. Gács, P. Sziklai and Zs. Weiner, On linear codes whose weights and length have a common divisor, *Adv. Math.*, **211** (2007) 94–104.

[9] S. Ball, A. Blokhuis and F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica*, **17** (1997) 31–41.

[10] S. Ball and A. Gács, On the graph of a function over a prime field whose small powers have bounded degree, *European J. Combin.*, to appear.

[11] S. Ball, A. Gács and P. Sziklai, On the number of directions determined by a pair of functions over a prime field, *J. Combin. Theory Ser. A*, **115** (2008) 505–516.

[12] S. Ball, P. Govaerts and L. Storme, On ovoids of parabolic quadrics, *Des. Codes Cryptogr.*, **38** (2006) 131–145.

[13] S. Ball and M. Lavrauw, How to use Rédei polynomials in higher dimensional spaces, *Le Matematiche (Catania)*, **59** (2004) 39–52 (2006).

[14] S. Ball and M. Lavrauw, On the graph of a function in two variables over a finite field, *J. Algebraic Combin.*, **23** (2006) 243–253.

[15] S. Ball and O. Serra, Punctured Combinatorial Nullstellensätze, *Combinatorica*, to appear.

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

[17] A. Blokhuis, On nuclei and affine blocking sets, *J. Combin. Theory Ser. A*, **67** (1994) 273–275.

[18] A. Blokhuis, On multiple nuclei and a conjecture of Lunelli and Sce, *Bull. Belg. Math. Soc.*, **3** (1994) 349–353.

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

[20] A. Blokhuis, A. E. Brouwer and T. Szőnyi, The number of directions determined by a function f on a finite field, *J. Combin. Theory Ser. A*, **70** (1995) 349–353.

[21] A. Blokhuis, A. E. Brouwer and T. Szőnyi, Covering all points except one, preprint.

[22] A. Blokhuis, A. A. Bruen and J. A. Thas, Arcs in $PG(n,q)$, MDS-codes and three fundamental problems of B. Segre - some extensions, *Geom. Dedicata*, **35** (1990) 1–11.

[23] A. Blokhuis and F. Mazzocca, The finite field Kakeya problem, in: *Building Bridges Between Mathematics and Computer Science*, Bolyai Society Mathematical Studies, **19** (2008).

[24] A. Blokhuis, R. Pellikaan and T. Szőnyi, Blocking sets of almost Rédei type, *J. Combin. Theory Ser. A*, **78** (1997) 141–150.

[25] A. Blokhuis, T. Szőnyi and Zs. Weiner, On sets without tangents in Galois planes of even order, *Des. Codes Cryptogr.*, **29** (2003) 91–98.

[26] A. Blokhuis, T. Szőnyi and H. A. Wilbrink, On sets of points in $\mathrm{PG}(2,q)$ without tangents, *Mitt. Math. Sem. Giessen*, **201** (1991) 39–44.

[27] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combin. Theory Ser. A*, **24** (1978) 251–253.

[28] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A*, **60** (1992) 19–33.

[29] A. A. Bruen, Applications of finite fields to combinatorics and finite geometries, *Acta Appl. Math.*, **93** (2006) 179–196.

[30] D. K. Butler, On the intersection of ovoids sharing a polarity, *Geom. Dedicata*, **135** (2008) 157–165.

[31] J. De Beule and A. Gács, Complete arcs on the parabolic quadric $\mathrm{Q}(4,q)$, *Finite Fields and Their Applications*, **14** (2008) 14-21.

[32] Z. Dvir, On the size of Kakeya sets in finite fields, *J. Amer. Math. Soc.*, to appear.

[33] S. Ferret, L. Storme, P. Sziklai and Zs. Weiner, A $t \pmod p$ result on weighted multiple $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$, *Innov. Incidence Geom.*, **6-7** (2009) 169-188.

[34] A. Gács, On a generalization of Rédei's theorem, *Combinatorica*, **23** (2003) 585–598.

[35] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, Second Edition, *Oxford Mathematical Monographs*, Clarendon Press, Oxford, 1998.

[36] R. Jamison, Covering finite fields with cosets of subspaces, *J. Combin. Theory Ser. A*, **22** (1977) 253–266.

[37] R. Lidl and H. Niederreiter, *Finite Fields*, Second Edition, Cambridge University Press, 1997.

[38] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981) 449–454.

[39] V. Pepe, personal communication.

[40] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser-Verlag, Basel, 1970. (English translation: *Lacunary Polynomials over finite fields*, North-Holland, Amsterdam, 1973.)

[41] B. Segre, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.* **39** (1955) 357-379.

[42] K-O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.*, **52** (1986) 1–19.

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

[44] T. Szőnyi, Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica*, **19** (1991) 197–212.

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

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

[47] T. Szőnyi, On the embedding of (k,p)-arcs in maximal arcs, *Des. Codes Cryptogr.*, **18** (1999) 235–246.

[48] T. Szőnyi and Zs. Weiner, On stability theorems in finite geometry, preprint.

[49] Zs. Weiner, On (k,p^e)-arcs in Galois planes of order p^h, *Finite Fields Appl.*, **10** (2004) 390–404.

[50] J. F. Voloch, Arcs in projective planes over prime fields, *J. Geom.*, **38** (1990) 198–200.