Directions in $AG(2, p^2)$

András Gács*  László Lovász  Tamás Szőnyi

Dedicated to Gábor Korchmáros on his 60th birthday.

Abstract

In this paper we prove that if $q$ is the square of a prime and $U$ is a set of $q$ points determining at least $\frac{q^2+3}{2}$ directions, then either $U$ is affinely equivalent to the graph of the function $x^{\frac{q+1}{2}}$ or it determines at least $\frac{q^2+p}{2}+1$ directions. This is sharp, the example is due to Polverino, Szőnyi and Weiner [10]. Our method combines the lacunary polynomial and the double power sum approach.

Keywords: affine planes, directions, blocking sets of Rédei type

MSC 2000: 51E21

1. Introduction

Throughout this paper $U = \{(a_i, b_i) : i = 1, \ldots, q\}$ will denote a $q$-element point set in $AG(2, q)$, the Desarguesian affine plane of order $q$. We write

$$D = \left\{ \frac{b_i - b_j}{a_i - a_j} \mid i \neq j \right\}$$

and call elements of this set the directions determined by $U$. This is a subset of $GF(q) \cup \{\infty\}$ and consists of slopes of lines joining two points of $U$. Finally, let $N = |D|$, the number of determined directions.

The problem of determining the possible values of $N$ and characterizing the corresponding point sets has received a lot of attention in recent years. For motivation and the history of the problem we refer to [3] and [4]. Here we summarize some known results.

*The authors were supported by Magyary and Bolyai grants, TÉT grants E16/04 and SI-2/2007, OTKA grants F043772, T043758, T049662, T067867.
Result 1.1 (Rédei [11]; Blokhuis, Ball, Brouwer, Storme, Szőnyi [4] and Ball [1]). Let \( q = p^h \) and let \( s = p^e \) be maximal with the property that any line containing at least two points of \( U \) meets \( U \) in a multiple of \( s \) points. Then one of the following holds:

(i) \( s = 1 \) and \( \frac{q+3}{2} \leq N \leq q+1 \);
(ii) \( \text{GF}(s) \) is a subfield of \( \text{GF}(q) \) and \( 1 + q/s \leq N \leq (q-1)/(s-1) \);
(iii) \( s = q \) and \( N = 1 \).

Moreover, if \( s > 2 \), then \( U \) can be regarded as a coset of a vector space over \( \text{GF}(s) \).

This result solves the problem entirely for the case \( N < \frac{q+3}{2} \). It was first proved in [4] with some exceptions for the characteristic 2 and 3 cases. Recently S. Ball [1] found an easier proof which also handles the missing cases.

For the case \( N \geq \frac{q+3}{2} \), there have been results only when \( q \) is a prime:

Result 1.2. (i) (Lovász and Schrijver [9]) If \( q \) is a prime, then the only sets determining \( \frac{q+3}{2} \) directions are the affine equivalents of the graph of the function \( x^{q+1} \).

(ii) (Gács [7]) If \( q \) is prime and \( N > \frac{q+3}{2} \), then \( N \geq \left\lfloor 2 \frac{q-1}{3} + 1 \right\rfloor \).

Note that for the case \( q \) is a prime Result 1.1 gives that \( N \) is at least \( \frac{q+3}{2} \), unless \( N = 1 \) (that is \( U \) is a line). This was already observed by Rédei and Megyesi, see [11]. The graph of \( x^{q+1} \) determines \( \frac{q+3}{2} \) directions for any odd prime power \( q \), showing that the bound in Result 1.1(i) is sharp.

In this paper we consider the next case, that is, when \( q \) is the square of a prime. We prove an analogous result to the two statements of Result 1.2:

Theorem 1.3. Suppose that \( q = p^2 \), where \( p \) is prime and \( U \) is a set of \( q \) points in \( \text{AG}(2,q) \) determining at least \( \frac{q+3}{2} \) directions. Then either \( U \) is affinely equivalent to the graph of \( x^{q+1} \), or the number of directions is at least \( \frac{q+2}{2} + 1 \).

The bound is sharp: Polverino, Szőnyi and Weiner [10] constructed an example determining \( \frac{q+\sqrt{q}}{2} + 1 \) directions when \( q \) is a square. We conjecture that for any square prime power, this should be the next possible value for \( N \), that is, \( \frac{q+3}{2} < N < \frac{q+\sqrt{q}}{2} + 1 \) cannot happen for \( q \) square.

We continue with some preliminary remarks on polynomials over finite fields and Lucas’ theorem. For proofs, see [8].

When \( U \) does not determine all directions, that is, when \( N < q+1 \), one can find a suitable transformation (not affecting \( N \)) to achieve that \( U = \{(x, f(x)) \mid x \in \text{GF}(q)\} \) for some function \( f \). After this we have another form for \( D \); namely,
it is easy to see that \( D \) consists of those \( c \in \mathbb{GF}(q) \) for which \( f(x) - cx \) is not bijective.

Over the finite field \( \mathbb{GF}(q) \) any function can be written as a polynomial of degree at most \( q - 1 \). This is called the reduced form of \( f \). For any \( f(x) = c_{q-1}x^{q-1} + \cdots + c_1x + c_0 \), we have \( \sum_{x \in \mathbb{GF}(q)} f(x) = -c_{q-1} \). Such an \( f \) is called a permutation polynomial if it is bijective as a function. For such polynomials we have \( \sum_{x \in \mathbb{GF}(q)} f(x) = 0 \) for any \( 1 \leq k \leq q - 2 \); this is equivalent to saying that in the reduced form of \( f(x)^k \) the coefficient of \( x^{q-1} \) is zero.

Lucas’ theorem tells how binomial coefficients behave modulo a prime \( p \). Let the \( p \)-adic expansion of \( n \) and \( k \) be 
\[
n = \sum_{i=1}^{r} n_i p^{i-1} \quad \text{and} \quad k = \sum_{i=1}^{r} k_i p^{i-1},
\]
respectively. Then \( \binom{n}{k} \equiv \binom{n_1}{k_1} \cdots \binom{n_r}{k_r} \) modulo \( p \).

Finally, we show how the direction problem is connected to blocking sets in \( \mathbb{PG}(2, q) \). A blocking set \( B \) in the projective plane \( \mathbb{PG}(2, q) \) is a set of points meeting every line. A blocking set \( B \) is called non-trivial if it contains no line, and minimal if it does not properly contain a blocking set.

If \( U \) is a set of \( q \) points in \( \mathbb{AG}(2, q) \) and \( D \) is the set of determined directions, then embedding \( \mathbb{AG}(2, q) \) into \( \mathbb{PG}(2, q) \) and adding to \( U \) the infinite points corresponding to elements in \( D \), we get a blocking set \( B \) of the projective plane. It contains a line if and only if either \( U \) is an affine line or \( U \) determines every direction. Then \( B \) has the property that there is a line (the line at infinity) missing exactly \( q \) points of \( B \). It is easy to see that this property characterizes minimal blocking sets arising from the above construction; they are called blocking sets of Rédei type.

In the next section we deal with blocking sets in general. After some easy observations we will end up in a result about Rédei type blocking sets (Proposition 2.4), which will be used in the proof of Theorem 1.3.

We will consider \( \mathbb{PG}(2, q) \) as \( \mathbb{AG}(2, q) \) extended by the line at infinity, \( l_{\infty} \). The infinite point of lines with slope \( c \) will be denoted by \( (c) \), the infinite point of the vertical lines will be denoted by \( (\infty) \).

### 2. Blocking sets

Suppose that \( B \) is a blocking set in \( \mathbb{PG}(2, q) \) with \( |B| < 2q - 1 \) and \( (\infty) \notin B \). Write \( U = B \setminus l_{\infty} = \{(a_i, b_i) \mid i = 1, \ldots, k\} \) and let \( D = B \cap l_{\infty} = \{(y_i) \mid i = 1, \ldots, N\} \). The Rédei polynomial of \( U \) is defined as

\[
H(X, Y) = \prod_{i=1}^{k} (X + a_iY + b_i).
\]
We will often use the Rédei polynomial of $B$ also, which is

$$H^*(X, Y) = \prod_{i=1}^{N} (Y + y_i)H(X, Y).$$

Finally, the homogeneous Rédei polynomial of $B$ is defined as

$$R(X, Y, Z) = \prod_{i=1}^{N} (Y + y_i Z) \prod_{i=1}^{k} (X + a_i Y + b_i Z).$$

Note that $R$ is the homogenization of $H^*$.

The partial derivatives of $R$ with respect to $X$, $Y$ and $Z$ will be denoted by $R'_X$, $R'_Y$ and $R'_Z$, respectively.

**Lemma 2.1.** (i) There exist polynomials $f_1$ and $f_2$ of degree at most $|B| - q$ such that

$$H^*(X, Y) = (X^q - X)f_1(X, Y) + (Y^q - Y)f_2(X, Y);$$

(ii) there exist homogeneous polynomials $f, g, h$ of degree $|B| - q$ such that

$$R(X, Y, Z) = X^q f + Y^q g + Z^q h;$$

(iii) $X f + Y g + Z h = 0$ for the polynomials found in (ii);

(iv) for any $(x, y, z) \in \text{GF}(q)^3 \setminus (0, 0, 0)$, we have

$$f(x, y, z) = -R'_X(x, y, z),$$

$$g(x, y, z) = -R'_Y(x, y, z),$$

$$h(x, y, z) = -R'_Z(x, y, z),$$

for the polynomials found in (ii).

**Proof.** (i) is well-known, see Blokhuis [2]. For the homogenization of $H^*$ it gives that it is of the form $R = X^q f_1^* + Y^q f_2^* - Z^{q-1} (X f_1^* + Y f_2^*)$. Hence the polynomials $f = f_1^*, g = f_2^*$ and $h = -\frac{1}{Z} (X f_1^* + Y f_2^*)$ will be appropriate for (ii) and (iii), provided that we can prove that $Z \mid X f_1^* + Y f_2^*$. Consider the terms of $R$ not containing $Z$. These are $Y^N \prod_{i}(X + a_i Y)$. Since $(\infty) \notin B$, each element of $\text{GF}(q)$ occurs at least once as an $a_i$. Hence the terms we are looking for can be written as $X^M Y^N (X^{q-1} - Y^{q-1}) s(X, Y)$ $(M, N \geq 1)$. They all come from $X^q f_1^* + Y^q f_2^*$, so we have to find out the terms containing $X^q$ and $Y^q$, which are $X^q X^{M-1} Y^N s(X, Y)$ and $-Y^q X^{M} Y^{N-1} s(X, Y)$. Hence the terms in $X f_1^* + Y f_2^*$ not containing $Z$ are $X X^{M-1} Y^N s(X, Y) - Y X^{M} Y^{N-1} s(X, Y) = 0$.

Now (iv) easily follows from (iii) and the derivative of (ii).
The following lemma gives an easy consequence of Lemma 2.1.

**Lemma 2.2.** Suppose that the line \( l : aX + bY + cZ = 0 \) is a 1-secant to \( B \). Then the unique intersection point of \( l \) and \( B \) is \((f(a, b, c), g(a, b, c), h(a, b, c))\).

**Proof.** The point \((f(a, b, c), g(a, b, c), h(a, b, c))\) is on the line in question because of Lemma 2.1(iii). At this stage it is more convenient not to distinguish between the affine and infinite points of \( B \), so write \( B = \{(u_i, v_i, w_i) \mid i = 1, \ldots, k + N\} \), hence \( R(X, Y, Z) = \prod_{i=1}^{k+N} (u_iX + v_iY + w_iZ) \). Differentiate \( R \) with respect to \( X \) to find \( R'_X(X, Y, Z) = \sum_i u_i \prod_{j \neq i} (u_jX + v_jY + w_jZ) \). If we substitute \( X = a, Y = b \) and \( Z = c \), then all products in the sum will be zero, except for the case when \((u_i, v_i, w_i)\) is the intersection point, hence \( R'_X(a, b, c) = u_i \prod_{j \neq i} (u_ja + v_jb + w_jc) \) (for this \( i \)). Similarly we have \( R'_Y(a, b, c) = v_i \prod_{j \neq i} (u_ja + v_jb + w_jc) \) and \( R'_Z(a, b, c) = w_i \prod_{j \neq i} (u_ja + v_jb + w_jc) \). Since the line \( aX + bY + cZ = 0 \) is a 1-secant to \( B \), this product is non-zero. By Lemma 2.1(iv), we are done. \( \square \)

Note that when the line \( aX + bY + cZ = 0 \) meets \( B \) in more than one point, then \( f(a, b, c) = g(a, b, c) = h(a, b, c) = 0 \).

Now we suppose that \( B \) is of Rédéi type. Hence we have \( k = q \) and \( D = \{(y_i) \mid i = 1, \ldots, N\} \) is the set of determined directions of the affine set \( U = \{(a_i, b_i) \mid i = 1, \ldots, q\} \).

Note that in this case we have \( f(X, Y, Z) = \prod_{i=1}^{N} (Y + y_iZ) \) in Lemma 2.1.

**Definition 2.3.** The index \( I \) of \( B \) is defined so that the \( X \)-degree of the polynomial \( Y^qg + Z^qh \) is \( q - I \).

From Lemma 2.1(iii) we see that \( q - I \) is also the \( X \)-degree of \( g \) and \( h \) (unless one of them is 1 and the other is 0). Note that considering \( H \) as a polynomial in \( X \) (with coefficient polynomials in \( Y \)), \( X^{q-I} \) is the first term after \( X^q \) with non-vanishing coefficient polynomial.

**Proposition 2.4.** (i) If the infinite point \((y)\) does not belong to \( B \) (that is, \((y)\) is not a determined direction), then the affine part of \( B \) is equivalent to \( \{(c \cdot g(t, y, -1), t) \mid t \in GF(q)\} \), where \( c \neq 0 \) depends on \( y \);

(ii) If \( q - N > N + I - q \), then by a suitable linear transformation we can suppose that the affine part of \( B \) is the graph of a polynomial of degree \( q - I \).

**Proof.** If \((y)\) is not determined, then all affine lines through it are 1-secants, hence by calculating the intersections of \( B \) and these lines, we can determine the \( q \) affine points.
The lines in question have equation \( tX_0 + yX_1 - X_2 = 0 \), so by Lemma 2.1, we find that the affine part of \( B \) is

\[
\{(f(t, y, -1), g(t, y, -1), h(t, y, -1)) \mid t \in \text{GF}(q)\}.
\]

We know that \( f(t, y, -1) = \prod(y - y_i) \), and from Lemma 2.1(iii) we have

\[
yg(t, y, -1) - h(t, y, -1) = -\prod(y - y_i)t.
\]

Note that \( c := \prod(y - y_i) \) is a constant, hence after the transformation \( X_2' = X_2 - yX_1 \) we find the form claimed in (i).

By the definition of \( I \), after (i) we only need that there is a suitable non-determined direction \( y \), for which the degree of \( g(X, y, -1) \) is the same as the \( X \)-degree of \( g \). We have \( q - N \) choices for \( y \). The coefficient of \( X^{q-1} \) in \( g(X, Y, Z) \) is a homogeneous polynomial \( g_0(Y, Z) \) of degree \( |B| - q - (q - I) = N + I - q \). If this is smaller than \( q - N \), then from the fact that \( g_0 \) is not identically zero, we should have an appropriate \( y \).

**Remark 2.5.** Similar ideas and some of the results were used by Sziklai to prove results about small blocking sets, see [12].

### 3. Results about directions for general \( q \)

In the spirit of the introduction, from now on \( U = \{(x, f(x)) \mid x \in \text{GF}(q)\} \)

\[
D = \left\{ \frac{f(x) - f(y)}{x - y} \mid x \neq y \right\} = \{c \in \text{GF}(q) \mid f(x) - cx \text{ is not a perm. pol.}\},
\]

and \( N(f) = |D| \). Here \( f(x) = c_nx^n + \cdots + c_0 \) with \( \deg(f) = n \leq q - 1 \). In this section we introduce two more parameters depending on \( f \) and relate them to \( N(f) \).

By the remarks at the end of the introduction, \( U \cup D \) is a blocking set of Rédéi type. In this case the Rédéi polynomial is

\[
H(X, Y) = \prod_{t \in \text{GF}(q)} (X + tY + f(t)).
\]

Expanding \( H \) in powers of \( X \), we have

\[
H(X, Y) = X^q + h_1(Y)X^{q-1} + \cdots + h_q(Y).
\]  \(\text{(1)}\)

Write \( h_i(Y) = \sum_j \sigma_{i-j,j}Y^j \). Note that \( h_i \) is the \( i \)-th elementary symmetric polynomial of the multiset \( \{Yt + f(t) \mid t \in \text{GF}(q)\} \). It is easy to see that \( \sigma_{0,i} \), that is, the coefficient of \( Y^i \) in \( h_i \), is the \( i \)-th elementary symmetric polynomial of the set \( \text{GF}(q) \). This is zero for \( 1 \leq i \leq q - 2 \), so for these \( i \)'s, \( \deg(h_i) \leq i - 1 \).
In general for \((a, b) \neq (0, 0)\) we have the following for \(\sigma_{a, b}\) (the coefficient of \(Y^a\) in \(h_{a+b}\), that is, the coefficient of \(X^{q-a-b} Y^a\) in \(H(X, Y)\)):

\[
\sigma_{a, b} = \sum_{t_1, \ldots, t_a, u_1, \ldots, u_b} t_1 \cdots t_a \cdot f(u_1) \cdots f(u_b),
\]

where the sum is over all choices of \(t_1, \ldots, t_a, u_1, \ldots, u_b\) all different. For \(a = b = 0\), we have \(\sigma_{0,0} = 1\).

The use of \(H(X, Y)\) is that it translates intersection properties of \(U\) to algebraic ones. This was used in all proofs mentioned in the Introduction and in Section 2.

**Lemma 3.1.** Fixing \(Y = y_0\) and considering \(H(X, y_0)\) as a polynomial in \(X\), the multiplicities of its roots are the same as a multiset as the intersection sizes of lines through the infinite point \((-y_0)\) with \(U\).

**Proof.** See Rédei [11].

We introduce another series of polynomials:

\[
g_k(c) := \sum_{t \in \text{GF}(q)} (f(t) + ct)^k = \sum_{i=0}^{k} \binom{k}{i} \pi_{i, k-1} c^i, \tag{2}
\]

where \(\pi_{a, b} = \sum_{t \in \text{GF}(q)} t^a f(t)^b\). Define \(\pi_{0,0}\) to be 1. Note that the \(g_k\)'s are the power sums of the multiset \(\{f(t) + ct \mid t \in \text{GF}(q)\}\).

The two parameters (depending on the reduced polynomial \(f\)) to be introduced are the following.

**Definition 3.2.** The first index \(I_1(f)\) of \(f\) is defined to be the smallest positive integer \(k\) for which the polynomial \(h_k\) defined by (1) is not identically zero.

The second index \(I_2(f)\) of \(f\) is defined to be the smallest positive integer \(k\) for which the polynomial \(g_k\) defined by (2) is not identically zero.

Note that \(I_1(f)\) coincides with the index (of the blocking set) defined in the previous section. The reason for not using the same notation is that we want to stress that \(I\) is a parameter of the blocking set \(B\), while \(I_1\) (and \(I_2\)) are parameters of the affine part \(U\) of the blocking set.

The proofs in [1] and in [4] make use of lacunary polynomials arising from \(H(X, Y)\), this means the consideration of the parameter \(I_1(f)\). On the other hand, [7] and [9] use double power sums in the proof, this is the consideration of the parameter \(I_2(f)\).

In this paper we use both parameters, it seems that this might be the way of attacking the \(N \geq \frac{q+3}{2}\) case. Next we relate \(I_1, I_2\) and \(N\) to each other. Most of
these observations are at least implicitly stated in one of the above mentioned papers. The first part was also observed by Evans, Greene and Niederreiter [6].

Lemma 3.3. (i) If \( I_1(f) \geq \frac{q+1}{2} \), then \( N(f) \leq \frac{q-1}{p-1} \);

(ii) if \( N(f) > 1 \), then \( q + 1 - N(f) \leq I_1(f) \leq I_2(f) \), with \( I_1(f) = I_2(f) \) if and only if \( p \) does not divide \( I_1(f) \).

Proof. For (i) we refer to [4]. This is the first easy step of the proof which was already found by Rédei [11].

The fact that \( I_1(f) \leq I_2(f) \) and the characterization of the case of equality is a consequence of the Newton formulas relating power sums and elementary symmetric polynomials.

For \( q+1-N(f) \leq I_1(f) \) note that fixing any \( -y \notin D \) we have \( H(X, y) = X^q - X \), hence for these \( y \)'s we have \( h_1(y) = \cdots = h_{q-2}(y) = 0 \). For \( h_1, \ldots, h_{q-N(f)} \) these are more roots than their degrees, so these \( h_i \)'s are identically zero. \( \square \)

Corollary 3.4. Suppose \( q \) is odd. If \( \frac{q+1}{2} \leq N(f) \leq \frac{q+1}{2} \), then \( I_1(f) = I_2(f) \).

Proof. From Lemma 3.3 we deduce \( \frac{q-p}{2} + 1 \leq I_1(f) \leq \frac{q-1}{2} \), so \( I_1 \) cannot be divisible by \( p \). The same lemma gives \( I_1 = I_2 \). \( \square \)

Lemma 3.5. Suppose \( N(f) < 3q/4 \) and \( I_1(f) \leq \frac{q-1}{2} \). Then one can make a linear transformation for the graph of \( f \) to find the graph of another polynomial \( f_1 \) with \( \deg(f_1) = q - I_1(f_1) = q - I_1(f) \).

Proof. This is a consequence of Proposition 2.4(ii). The conditions are easily seen to be satisfied, so after transformation, we can find the desired \( f_1 \). Since this is in fact a transformation of the blocking set that fixes the Rédei line, \( N(f_1) = N(f) \) and by the original definition of \( I \), we see that \( I_1(f) = I_1(f_1) \). \( \square \)

The following lemma gives a relation between the above defined \( \sigma_{k,l} \)'s and \( \pi_{k,l} \)'s. It can be considered as a generalization of the Newton-Girard formulas relating elementary symmetric polynomials to power sums.

Lemma 3.6. Fix two positive integers \( k \) and \( l \). The following formula holds:

\[
\sum_{r=0}^{k} \sum_{s=0}^{l} w(r, s) \pi_{r,s} \sigma_{k-r,l-s} = 0 ,
\]
where the function \( w(r, s) \) is defined as follows: fix two field-elements \( a \) and \( b \), then \( w(0, 0) := ak + bl \); while for \( (r, s) \neq (0, 0) \)

\[
w(r, s) := (-1)^{r+s} \left( \binom{r + s - 1}{s} a + \binom{r + s - 1}{r} b \right).
\]

(That is, we get a formula for every choice of \( a \) and \( b \).)

**Proof.** It is easy to see that after multiplication on the left hand side we have monomials of the form \( t^r f(t)^s t_1 \cdots t_{k-r} f(u_1) \cdots f(u_{l-s}) \), where \( t, t_1, \ldots, u_{l-s} \) are different field elements and \( 0 \leq r \leq k, 0 \leq s \leq l \).

If \( r \) and \( s \) are both positive, then we can get such a term from three summands: \( \pi_{r,s} \sigma_{k-r,l-s}, \pi_{r-1,s} \sigma_{k+1-r,l-s} \) and \( \pi_{r,s-1} \sigma_{k-r,l+1-s} \). Hence the coefficient of such a monomial is \( w(r, s) + w(r, s - 1) + w(r - 1, s) = 0 \).

If \( r = 0, s > 1 \), then there are two summands giving the monomial in question: \( \pi_{0,s} \sigma_{k,l-s} \) and \( \pi_{0,s-1} \sigma_{k,l+1-s} \), so the coefficient of such a monomial is \( w(0, s) + w(0, s - 1) = 0 \). The \( s = 0, r > 1 \) case is similar.

The \( \{r, s\} = \{0\} \) and \( \{r, s\} = \{0, 1\} \) cases are the same, so what is left is to show that monomials of the form \( t_1 \cdots t_k f(u_1) \cdots f(u_k) \) also have zero coefficient. There are three summands giving them: \( \pi_{0,0} \sigma_{k,l} \) (one time), \( \pi_{1,0} \sigma_{k-1,l} \) (\( k \) times) and \( \pi_{0,1} \sigma_{k,l-1} \) (\( l \) times). Hence the coefficient in question is \( w(0, 0) + lw(0, 1) + kw(1, 0) = 0 \). \( \square \)

We will use two corollaries of this lemma. The first one was noticed by Chou [5].

**Corollary 3.7.**

(i) \( \deg(f) \leq q - I_1(f) \);

(ii) in the reduced form of \( f^2 \) the only non-zero terms of degree higher than \( q + 1 - I_1(f) \) can be those of degree divisible by \( p \).

**Proof.**

(i) By the definition of \( I_1 \), we know that \( \sigma_{k,l} = 0 \) for every \( 0 < k + l < I_1(f) \). We use the formula of Lemma 3.6 with \( l = 1, a = 0 \) and \( b = 1 \). It gives \((-1)^{k+1} k \pi_{k,1} = 0 \) for all \( k \leq I_1(f) - 2 \), which means that the coefficients of \( x^{q-1}, x^{q-2}, \ldots, x^{q-I_1(f)+1} \) are zero in \( f \).

(ii) Similarly to (i), we now use the formula with \( l = 2, a = 0, b = 1 \) to find \((-1)^{k+2} k^{k+1} \pi_{k,2} = 0 \) for all \( k \leq I_1(f) - 3 \). This gives that in the reduced form of \( f^2x^k \), the coefficient of \( x^{q-1} \) is zero, unless \( p \mid k + 1 \); this is exactly what we wanted. \( \square \)

In the next theorem, we summarize what we have so far.
Theorem 3.8. Suppose $U$ is a set of $q$ points in $AG(2, q)$ determining $N \leq \frac{q + p}{2}$ directions, where $q$ is a proper power of the odd prime $p$. Then either $N \leq \frac{q + 1}{2}$ and we know all such examples from the classification [1, 4], or $U$ is affinely equivalent to the graph of a polynomial $f$ with $I_1(f) = I_2(f) = \frac{q - 1}{2}$ and $\deg(f) = \frac{q + 1}{2}$.

Proof. The previous lemmas together yield that after transformation, $U$ is the graph of a polynomial $f(x) = x^n + \cdots + c_2x^2 + c_1x + c_0$ with

$$\frac{q - p}{2} + 1 \leq I_1(f) = I_2(f) = q + 1 - n \leq \frac{q + 1}{2}.$$ 

All we need is that $n = \frac{q + 1}{2}$.

Write $n = \frac{q - 1}{2} + r$ with $1 \leq r \leq \frac{p - 1}{2}$. Consider the reduced form of $f^p$. The term $x^n$ will give $x^{(q - 1)/2 + rp}$ (after reduction). It follows that

$$\sum x^{(q - 1)/2 - rp} f(x)^p \neq 0.$$ 

Since $((q - 1)/2 - rp + p) \neq 0$ by Lucas’ theorem, this gives that $g((q - 1)/2 - (r - 1)p) \neq 0$ identically, hence by the definition of $I_2$, we have $(q - 1)/2 - (r - 1)p \geq I_2 > (q - p)/2$. This is only possible for $r = 1$. \hfill $\square$

The above theorem implies in particular, that to prove Theorem 1.3 or even its generalization to an arbitrary odd prime power $q$ (which is not a prime), one can suppose that the set $U$ is the graph of a polynomial of degree $\frac{q + 1}{2}$.

4. Proof of Theorem 1.3

From now on suppose $q = p^2$ for a prime $p$. For $p = 2$ and $p = 3$ there is nothing to prove, so suppose $p \geq 5$. By Theorem 3.8 let $f(x) = x^{\frac{q + 1}{2}} + \cdots + c_0$ be a polynomial with $\frac{q + 3}{2} \leq N(f) \leq \frac{q + p}{2}$ and $I_1 = I_2 = \frac{q - 1}{2}$. We make a transformation to achieve $c_2 = c_1 = c_0 = 0$. It is not difficult to see that this does not affect $I_1$ or $I_2$. We have to prove that $f$ is equivalent to $x^{\frac{q + 1}{2}}$. The proof will be carried out in several steps.

Claim 1. Consider the intervals

$$A_i = \left(\frac{q - 1}{2} - (i + 1)p, \frac{q - 1}{2} - ip\right)$$ 

for $i = 0, 1, \ldots, \frac{p - 3}{2}$.

The only possible indices $j \in A_i$ with $c_j \neq 0$ are

$$\frac{q - 1}{2} - ip, \frac{q - 1}{2} - ip - 1, \ldots, \frac{q - 1}{2} - ip - (i - 1)$$ 

(for $i = 0$ this means that for all $j \in (\frac{q - 1}{2} - p, \frac{q - 1}{2})$, $c_j = 0$).
Proof. We use Corollary 3.7(ii). Here \( q + 1 - I_1 = \frac{q+3}{2} \).

Using that in \( f^2 \) the coefficients of \( x^{q-1}, \ldots, x^{q-p+1} \) are zero, we find that \( c_{2q-3} = \cdots = c_{(q-1)/2-p+1} = 0 \). Then using the fact that in \( f^2 \) there is no \( x^{q-p-1}, \ldots, x^{q-2p+1} \), we find that \( c_{(q-1)/2-p-1} = \cdots = c_{(q-1)/2-2p+1} = 0 \). Again we cannot cancel \( c_{(q-1)/2-2p} \), but also \( c_{(q-1)/2-2p-1} \). The reason for the latter is that in \( f^2 \) the terms \( x^{\frac{q+1}{2} - q} x^{\frac{q-1}{2} - q} \) and \( (x^{\frac{q-1}{2}-p})^2 \) give terms of the same degree, so they might cancel each other.

In general we use induction on \( i \). Suppose we have proved the statement for \( 0, \ldots, i-1 \) but \( c_{(q-1)/2-ip-j} \neq 0 \) for a \( j \geq i \). Considering \( f^2 \) again, we find a term of degree \( q - ip - j \). This is a contradiction unless we can have this term from the product of two terms of the form \( (q-1)/2 - i_1p - j_1 \) and \( (q-1)/2 - i_2p - j_2 \) for some \( i_1, i_2 \leq i - 1 \) and \( j_1 \leq i_1 - 1, j_2 \leq i_2 - 1 \) (by the induction hypothesis). An easy calculation shows that this is not possible. \( \square \)

Note that what we have proved implies in particular that all terms below \( \frac{q+1}{2} \) have degree between 0 and \( \frac{q-1}{2} \) modulo \( p \).

Claim 2. If \( f(x) \neq x^{\frac{q+1}{2}} \), then \( f(x) = x^{\frac{q+1}{2}} + c_{(q-1)/2-ip-j} x^{(q-1)/2-jp} + \cdots \) with \( c_{(q-1)/2-ip-j} \neq 0 \). (That is, the first term after \( \frac{q+1}{2} \) with nonzero coefficient has to be congruent to \( \frac{q+1}{2} \) modulo \( p \).)

Proof. Let \( f(x) = x^{\frac{q+1}{2}} + c_3 x^s + \cdots \). Then in the reduced form of \( f(x)^2 \) the coefficient of the term \( x^{(q+1)/2+s} \) is not zero, hence by Corollary 3.7(ii), \( \frac{q+1}{2} + s \) is divisible by \( p \). \( \square \)

Claim 3. If \( f(x) \neq x^{\frac{q+1}{2}} \), then \( f(x) = x^{\frac{q+1}{2}} + c_{(q-1)/2-p} x^{(q-1)/2-p} + \cdots \) with \( c_{(q-1)/2-p} \neq 0 \) (hence \( j = 1 \) in Claim 2) and \( c_{(q-1)/2-p} + c_{(q-1)/2-ip-j} = 0 \).

Proof. By the remark after Claim 1, one can show that after reduction \( f(x)^p = x^{(q-1)/2+p} + c_{(q-1)/2-ip-j} x^{(q-1)/2-j} + \cdots \). Multiplying \( f \) and the reduced form of \( f^p \) we find that in the reduced form of \( f^{p+1} \) there are two big terms, namely \( c_{(q-1)/2-ip-j} x^{q-j} \) and \( c_{(q-1)/2-ip-j} x^{q-1-(j-1)p} \). These can cancel each other if \( j = 1 \) and \( c_{(q-1)/2-ip-j} + c_{(q-1)/2-ip-j} = 0 \), in all other cases \( f^{p+1} \) has a non-zero term of degree \( q - j \). But this cannot happen, since this would mean that \( g_{p+j} \) is not zero identically (note that \( (p+1) \) is not zero for \( j \geq 1 \)). \( \square \)

Claim 4. \( f(x) = x^{\frac{q+1}{2}} \).
Proof. Suppose $f(x) \neq x^{\frac{q+1}{2}}$. We summarize what we have from the previous three claims:

\[
\begin{align*}
    f(x) &= x \cdot (q+1) + c_{q-1} \cdot (q-1) / 2 - p \cdot x^{(q-1) / 2} + \cdots ; \\
    f(x)^p &= x \cdot (q+1) + p \cdot \cdot \cdot - p \cdot x^{(q-1) / 2} + \cdots ; \\
    0 &= c_{(q-1) / 2-p} + c_{(q-1) / 2-p}.
\end{align*}
\]

(3)

Now consider $x^2 \left( x^{p-1}f(x) - f(x)^p \right)^2$. This polynomial is the linear combination of polynomials of the form $x^k f(x)^l$ with $\binom{k+l}{k} \neq 0$, hence by the definition of $I_2$, after reduction it cannot have a term of degree $q-1$ (unless $2p + 2 \geq I_1$). It is easy to see that this gives $c_{(q-1) / 2-p} = 0$, which together with (3) implies $c_{(q-1) / 2-p} = 0$, a contradiction.

So the proof is finished except for the case $2p + 2 \geq I_1 = \frac{q-1}{2}$; this can only happen for $p = 5$. This case can be ruled out by computer. □

References


András Gács  
DEPARTMENT OF COMPUTER SCIENCE, Eötvös Loránd University, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary  
e-mail: gacs@cs.elte.hu

László Lovász  
DEPARTMENT OF COMPUTER SCIENCE, Eötvös Loránd University, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary  
e-mail: lovasz@cs.elte.hu

Tamás Szőnyi  
DEPARTMENT OF COMPUTER SCIENCE, Eötvös Loránd University, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary  

COMPUTER AND AUTOMATION RESEARCH INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES, H-1111 Budapest, Lágymányosi u. 11, Hungary  
e-mail: szonyi@cs.elte.hu, szonyi@sztaki.hu