ON THE SIZE OF THE SMALLEST NON-CLASSICAL BLOCKING SET OF RÉDEI TYPE IN $PG(2,p)$

András Gács
Institute of Mathematics
Hungarian Academy of Sciences
H-1053, Budapest, Reáltanoda u. 13-15. Hungary
gacs@cs.elte.hu

Abstract. We prove that the number of directions determined by a set of p points in $AG(2,p)$, p prime, can not be between $\frac{p+3}{2}$ and $\frac{p-1}{2}+\frac{1}{3}\sqrt{p}$. This is equivalent to saying that besides the projective triangle, every blocking set of Rédei type in $PG(2,p)$ has size at least $3\frac{p-1}{2}+\frac{1}{3}\sqrt{p}$.

1. Introduction

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

Definition 1.1 We say that U determines the direction $m\in GF(q)\cup\{\infty\}$ if $m=\frac{b_i-b_j}{a_i-a_j}$ for suitable $i\neq j$, and denote by D the set of determined directions. Finally, let $N=|D|$, the number of determined directions.

The problem of determining the possible values of N and characterizing the corresponding point sets is important for at least two reasons. The first is that it has applications to the theory of permutation polynomials, see [1]. The second reason is its connection with blocking sets.

A *blocking set* in a projective plane is a point set meeting every line, but containing no line. A way to construct a blocking set in $PG(2,q)$ is to take a q-element point set U in $AG(2,q)$ and add all infinite points corresponding to the directions it determines. In this way we get a blocking set of size $q+N$ with the property that there is a line (namely the line at infinity) meeting the blocking set in all but q points. Blocking sets arising this way are called of *Rédei type*. For more information, we refer to [2].

After results of Rédei ([3]) and Lovász and Schrijver ([4]), recently the problem of determining the possible values of N and characterizing the corresponding point sets has been almost completely solved by Ball, Blokhuis, Brouwer, Storme and Szőnyi ([5]) for the case when the number of determined directions is less than $\frac{q+3}{2}$, that is essentially all Rédei type blocking sets of size less than $q+\frac{q+3}{2}$ have been classified.

For $q=p$ prime, there is no example in this case:

Theorem 1.2 (Lovász-Schrijver [4]) If a point set in $AG(2,p)$ is not a line, then it determines at least $\frac{p+3}{2}$ directions with equality if and only if it is affinely equivalent to the graph of the polynomial $f(x) = x^{\frac{p+1}{2}}$. ∎

In [1] we considered the next possible value for N and proved the following:

Theorem 1.3 For $p > 11$ a set of p points in $AG(2,p)$, p prime, can not determine $\frac{p+5}{2}$ directions. ∎

We also formulated a conjecture, which is still open:

Conjecture 1.4 Let U be a set of p points in $AG(2,p)$, p prime. One of the following holds:
(i) U is a line determining one direction;
(ii) U is affinely equivalent to the graph of $x^{\frac{p+1}{2}}$ determining $\frac{p+3}{2}$ directions;
(iii) U determines at least $\frac{2p+2}{3}$ directions. ($\frac{2p+4}{3}$ for $3|p-1$.) ∎

This would be sharp, Megyesi constructed an example with $N = \frac{2p+4}{3}$ whenever $3|p-1$, see [1].

In this paper we prove the following:

Theorem 1.5 Let U be a set of p points in $AG(2,p)$, p prime. One of the following holds:
(i) U is a line determining one direction;
(ii) U is affinely equivalent to the graph of $x^{\frac{p+1}{2}}$ determining $\frac{p+3}{2}$ directions;
(iii) U determines at least $\frac{p-1}{2} + \frac{1}{3}\sqrt{p}$ directions.

With the blocking set terminology, the results and conjecture above say that besides the unique example of size $p + \frac{p+3}{2}$, blocking sets of Rédei type have size considerably larger than $3\frac{p+1}{2}$. The unique blocking set of Rédei type of (minimum) size $p + \frac{p+3}{2}$ is called the *projective triangle*. For a direct construction in $PG(2,p)$ see [1].

For the size of an arbitrary blocking set in $PG(2,p)$ the generalization of 1.2 holds:

Theorem 1.6 (Blokhuis [6]) In $PG(2,p)$ a blocking set has size at least $p + \frac{p+3}{2}$. ∎

Here the characterization of the case of equality is still missing. In fact besides a sporadic example of size 12 in $PG(2,7)$, the only known blocking set of size $p + \frac{p+3}{2}$ is the projective triangle, all known examples have size considerably larger than $p + \frac{p+3}{2}$.

In Section 2 we reduce the proof of Theorem 1.5 to a result about double power sums of polynomials over $GF(p)$, which is proved in Section 3.

2. Connection of directions to double power sums of polynomials

A polynomial is called a *permutation polynomial* if it is bijective as a function over the field. The following propositions show the connection between our problem and permutation polynomials.

Proposition 2.1 If a set does not determine all directions, then after a suitable affine transformation (which does not affect the number of directions), it can be taken as the graph of a polynomial.

Proof Since every function is a polynomial over a finite field, the only thing we need is that ∞ is not a determined direction, this can be achieved. ∎

We say that *a polynomial determines a direction* if its graph determines it.
The use of considering polynomials can be seen through the following statement:

Proposition 2.2 If the set in question is the graph of the polynomial $f(x)$, then the direction c is determined if and only if $f(x) - cx$ is not a permutation polynomial.

Proof The direction c is determined if and only if $c = \frac{f(x_1)-f(x_2)}{x_1-x_2}$ for suitable $x_1 \neq x_2$, which is equivalent to saying that $f(x_1) - cx_1 = f(x_2) - cx_2$, that is $f(x) - cx$ takes a value twice, so it can not be a permutation. ∎

This proposition will be used in conjunction with the following statement:

Proposition 2.3 (i) If $f(x) = c_{p-1}x^{p-1} + ... + c_0$, then $\sum_{x \in GF(p)} f(x) = -c_{p-1}$.
(ii) If $f(x)$ is a permutation polynomial, then for all $1 \leq k \leq p-2$, $f(x)^k$ has degree at most $p-2$ when reduced modulo $(x^p - x)$.

Proof (i)$\sum_x f(x) = \sum_x \sum_{i=0}^{p-1} c_i x^i = \sum_{i=0}^{p-1} c_i \sum_x x^i = -c_{p-1}$.
(ii)If $f(x)$ is bijective, then $\sum_{x \in GF(p)} f(x)^k = \sum_{x \in GF(p)} x^k = 0$ for $1 \leq k \leq p-2$. This together with (i) completes the proof. ∎

Let f be an arbitrary polynomial over $GF(p)$. The *double power of order* (k, l) *of* f is the polynomial $x^k f(x)^l$. Here k and l are non-negative integers, $l > 0$; for $k = 0$, x^0 is defined to be 1.

The double power sum of order (k, l) of f is defined to be

$$\Sigma_{k,l} = \sum_{x \in GF(p)} x^k f(x)^l.$$

Note that according to 2.3, $\Sigma_{k,l}$ is (-1) times the coefficient of x^{p-1} in $x^k f(x)^l$, after reduction modulo $x^p - x$.

Finally, we define the *index* of f to be

$$I(f) = \min\{k + l : \Sigma_{k,l} \neq 0\}.$$

The following lemma and theorem can both be found (implicitly) in [4]:

Lemma 2.4 Let f be a polynomial over $GF(p)$ and denote by $N(f)$ the number of directions it determines. Then $N(f) + I(f) \geq p + 1$ holds.

Proof For $k = 1, ..., p-2$ let $g_k(c) = \sum_{x \in GF(p)} (f(x) + cx)^k = \sum_{i=0}^{k} \binom{k}{i} \Sigma_{i,k-i} c^i$. Note that $\deg(g_k) \leq k - 1$, since the coefficient of c^k in $g_k(c)$ is $\sum_{x \in GF(p)} x^k = 0$.

Whenever $-c$ is not a determined direction, $f(x) + cx$ is bijective, so $g_k(c) = \sum_{u \in GF(p)} u^k = 0$. This means, that $g_1, ..., g_{p-N(f)}$ are polynomials with more roots than their degrees, so they are identically zero. Considering their coefficients, we have $\Sigma_{k,l} = 0$ for all $k + l \leq p - N(f)$, so we are done. ∎

Theorem 2.5 If f has degree at least 2, then $I(f) \leq \frac{p-1}{2}$ with equality iff f is affinely equivalent to $x^{\frac{p+1}{2}}$ or x^2.

We are going to give the proof in the next section.

Now 1.5 follows from the following, which will also be proved in Section 3:

Theorem 2.6 Let f be a non-zero polynomial over $GF(p)$, $p > 2$ prime. One of the following holds:
(i) f is a constant, $I(f) = p$;
(ii) f is linear, $I(f) = p - 1$;
(iii) f is of degree 2, $I(f) = \frac{p-1}{2}$;
(iv) f is affinely equivalent to $x^{\frac{p+1}{2}}$, $I(f) = \frac{p-1}{2}$;
(v) $I(f) \leq \frac{p+3}{2} - [\frac{1}{3}\sqrt{p}]$;
(vi) The graph of f is contained in the union of two lines.

Note that (iv) is part of (vi), but we believe that (vi) is just a technical condition, which could be eliminated, see Section 4.

This result swiftly implies Theorem 1.5:

Proof of Theorem 1.5 According to 2.1, we can suppose, that U is the graph of a polynomial f, where $N(f) = N$ by definition. Apply 2.6.

If $n \leq 1$, then U is a line, this is case (i).

If 2.6 (v) holds, then 2.4 implies (iii).

If f is of degree 2, then it is easy to see that $N(f) = p$.

Finally, suppose that (vi) holds, that is U is contained in the union of two lines. A theorem of T. Szőnyi ([7]) states, that in this case $N = p + 1 - \frac{p-1}{d}$ for a suitable $d|p-1$. If $d \leq 2$, then 1.2 implies (ii). For $d \geq 3$, we have $N \geq p + 1 - \frac{p-1}{3}$, so again (iii) holds. ∎

3. Proof of Theorem 2.6

First we prove some properties of $I(f)$, where $f(x) = c_n x^n + ... + c_0$ is a (reduced) polynomial of degree n with $2 \leq n \leq p-1$.

Proposition 3.1 Suppose f and g are affinely equivalent, that is $f(x) = ag(bx+c)+dx+e$, where $a, b, c, d, e \in GF(p)$, $a \neq 0$, $b \neq 0$. Then $I(f) = I(g)$.

Proof Denote by $\Sigma^f_{k,l}$ and $\Sigma^g_{k,l}$ the double power sums of f and g, respectively. It is enough to prove that $\Sigma^f_{k,l} = 0$ for all $k+l \leq I(g)$, for the cases $f(x) = ag(x)$, $f(x) = g(bx)$, $f(x) = g(x+1)$, $f(x) = g(x) + x$ and $f(x) = g(x) + 1$.

First let $f(x) = ag(x)$. Then $\Sigma^f_{k,l} = a^l \Sigma^g_{k,l}$, so they are zero in the same time.

If $f(x) = g(bx)$, then $\Sigma^f_{k,l} = \sum_{x \in GF(p)} x^k g(bx)^l = \sum_{y \in GF(p)} (\frac{y}{b})^k f(y)^l = (\frac{1}{b})^k \Sigma^g_{k,l}$, so they are zero in the same time.

Next suppose $f(x) = g(x+1)$ and $k+l < I(g)$. Then $\Sigma^f_{k,l} = \sum_{y \in GF(p)} (y-1)^k g(y)^l = \sum_{i=0}^k \binom{k}{i} (-1)^i \Sigma^g_{k-i,l} = 0$.

Next let $f(x) = g(x) + x$ and $k + l < I(g)$. Then $\Sigma^f_{k,l} = \sum_{x \in GF(p)} x^k (g(x) + x)^l = \sum_{i=0}^l \binom{l}{i} \Sigma^g_{k+l-i,i} = 0$.

Finally, if $f(x) = g(x) + 1$ and $k + l < I(g)$, then $\Sigma^f_{k,l} = \sum_{x \in GF(p)} x^k (g(x) + 1)^l = \sum_{i=0}^l \binom{l}{i} \Sigma^g_{k,i} = 0$. ∎

Now we prove a couple of bounds on $I(f)$, depending on n.

Proposition 3.2 $I(f) \leq p - n$.

Proof 2.3 implies that $\Sigma_{p-1-n,1} = -c_n \neq 0$. ∎

Proposition 3.3 If $4 \leq n \leq \frac{p-1}{2}$, then $I(f) \leq \frac{p-1}{3}$ for $n \neq \frac{p+1}{3}$ and $I(f) \leq \frac{p+1}{3}$ for $n = \frac{p+1}{3}$.

Proof Write $p - 1 = an + b$ with $b \leq n - 1$. Since $f(x)^a x^b$ has degree $p - 1$, it is enough to prove that $a + b \leq \frac{p+1}{3}$ or $a + b \leq \frac{p-1}{3}$ according as $n = \frac{p+1}{3}$ or not. For $p \leq 23$, a case by case analysis shows that the claim is true, so we can suppose $p \geq 29$.

$a + b \leq \frac{p-n}{n} + n - 1$, so we need $p/n + n \leq \frac{p+5}{3}$. Multiplying with n, we see that the following quadratic inequality has to be satisfied: $n^2 - \frac{p+5}{3} n + p \leq 0$. With an easy calculation one sees that this is true for $p \geq 28$ and $4 \leq n \leq \frac{p-7}{3}$.

For $\frac{p-6}{3} \leq n \leq \frac{p-1}{3}$ and $p \geq 28$, we have $a = 3$, $b \leq 5$, so $a + b \leq 8 \leq \frac{p-1}{3}$.

For $n \geq \frac{p+1}{3}$, we have $a = 2$, $b \leq \frac{p-5}{3}$ with equality if and only if $n = \frac{p+1}{3}$. ∎

Note that for $n = 2$ and $p > 2$, we have $I(f) = \frac{p-1}{2}$, for $n = 3$ and $p \geq 5$, $I(f) = \frac{p-1}{3}$ or $\frac{p+1}{3}$ (according as $3|p-1$ or $3|p+1$).

Proposition 3.4 Suppose $n = \frac{p+1}{2}$. Then f is affinely equivalent to $x^{\frac{p+1}{2}}$ with $I(f) = \frac{p-1}{2}$, or $I(f) \leq \frac{p+1}{4}$.

Proof After affine transformation suppose $f(x) = x^{\frac{p+1}{2}} + g(x)$ with $s = \deg g \leq \frac{p-3}{2}$, $x^2 | g(x)$. For $s = 0$, we have $f(x) = x^{\frac{p+1}{2}}$. The calculation of $I(f)$ is easy in this case.

Suppose $s \geq 2$, write $\frac{p-3}{2} = as + b$ and consider $f(x)^{a+1}x^b = g(x)^{a+1}x^b + (a+1)g(x)^a x^{\frac{p+1}{2}+b} + ...$ We claim that the only term giving x^{p-1} after reduction is $g(x)^a x^{\frac{p+1}{2}+b}$. Take a typical term, $r(x) = g(x)^{a+1-k}x^{k\frac{p+1}{2}+b}$. For k even, $r(x) = g(x)^{a+1-k}x^{b+k}$ modulo $(x^p - x)$, which has degree $(a+1-k)s+b+k = \frac{p-3}{2}+s-(s-1)k < p-1$. For k odd, we have $r(x) = g(x)^{a+1-k}x^{\frac{p-1}{2}+k+b}$ modulo $(x^p - x)$, which has degree $(a+1-k)s + \frac{p-1}{2} + k + b = p - 1 - (s-1)(k-1) < p-1$ for $k \neq 1$ (k odd).

Now $a + b \leq 1/s(\frac{p-3}{2} - (s-1)) + s - 1 = \frac{p-1}{2s} + s - 2$. This is at most $\frac{p+1}{4}$ for $2 \leq s \leq \frac{p+1}{4}$. For $s \geq \frac{p+2}{4}$, $a + b \leq \frac{p+1}{4}$ obviously. ∎

Proof of 2.5 Suppose $I(f) \geq \frac{p-1}{2}$. According to 3.2, $n \leq \frac{p+1}{2}$. If $p \geq 7$, then $\frac{p+3}{2} < \frac{p-1}{2}$, so using 3.3 and the sentence after it, $n = \frac{p+1}{2}$, or $n = 2$. For $n = 2$, f is affinely equivalent to x^2. For $n = \frac{p+1}{2}$, 3.4 completes the proof. The case $p \leq 5$ is easy. ∎

We need two more lemmas before the proof of 2.6.

Lemma 3.5 Suppose f and g are polynomials of degree $\frac{p+1}{2} + r$ and $\frac{p+1}{2} + s$, respectively, where r and s are non-negative integers. Then there exist polynomials F and G with $\deg(F) \leq s$, $\deg(G) \leq r$ and satisfying $\deg(Ff + Gg) \leq \frac{p-1}{2}$.

Proof Write $f(x) = a_n x^n + ... + a_0$ and $g(x) = b_m x^m + ... + b_0$ with $n = \frac{p+1}{2} + r$ and $m = \frac{p+1}{2} + s$. We use induction on $r + s$. For $r = s = 0$, one can take $F(x) = b_{\frac{p+1}{2}}$ and $G(x) = -a_{\frac{p+1}{2}}$.

In general, w.l.o.g, suppose $r \leq s$ and let $g_1(x) = g(x) - \frac{b_m}{a_n}x^{s-r}f(x)$. Clearly $m' := \deg(g_1) \leq m - 1$. If $m' \leq \frac{p-1}{2}$, then we are done by taking $F(x) = -\frac{b_m}{a_n}x^{s-r}$ and $G(x) = 1$, otherwise by induction, we have two polynomials F_1 and G_1 with $\deg(F_1) \leq m' - \frac{p+1}{2}$, $deg(G_1) \leq r$ and $\deg(F_1 f + G_1 g_1) \leq \frac{p-1}{2}$. But $F_1(x)f(x) + G_1(x)g_1(x) = (F_1(x) - \frac{b_m}{a_n}x^{s-r}G_1(x))f(x) + G_1(x)g(x)$, so we can take $F(x) = F_1(x) - \frac{b_m}{a_n}x^{s-r}G_1(x)$ and $G(x) = G_1(x)$. ∎

Lemma 3.6 Suppose Φ is a subspace of the vectorspace of polynomials over $GF(p)$. Then $\dim(\Phi) = |\{\deg(f) : f \in \Phi\}|$.

Proof Let $\Phi_1 \subset \Phi$ contain one polynomial from Φ of each degree. It is easy to see that Φ_1 is a linearly independent system (here we do not think about a polynomial as a function, so for instance $x^p - x$ is not the same as the zero polynomial), it is sufficient to show, that $< \Phi_1 >= \Phi$. Suppose to the contrary and let $f \in \Phi \setminus < \Phi_1 >$ of minimum degree. Choose $f_1 \in \Phi_1$ with $\deg(f_1) = \deg(f)$. There is a c for which $f - cf_1$ has degree smaller, so it is in $< \Phi_1 >$. But this implies $f \in \Phi_1$, a contradiction. ∎

Proof of Theorem 2.6 The calculation of $I(f)$ is easy for $\deg(f) \leq 2$, so we can assume $\deg(f) \geq 3$. Suppose $I(f) > \frac{p+3}{2} - \frac{1}{3}\sqrt{p}$. What we need is that we are in case (vi), that is tha graph of f is contained in the union of two lines. Note, that according to 2.5, we can assume $p \geq 37$, since otherwise $I(f) \geq \frac{p-1}{2}$ holds.

Write $t = [\frac{1}{3}\sqrt{p}]$. Recall that by the definition of $I(f)$ and by 2.3, $x^k f(x)^l$ has reduced degree at most $p-2$ for all $k+l \leq \frac{p+1}{2} - t$ (or equivalently, $\Sigma_{k,l} = 0$ for these (k,l) pairs). Using 3.2 and 3.3, we can suppose that $\deg(f) = \frac{p+1}{2} + r$ with $1 \leq r \leq t-2$. From now on f^i will denote the i-th power of f after reduction modulo $x^p - x$. After suitable affine transformation, we can suppose that $\deg(f) < \deg(f^2)$ and also that f has at most one root. Note that $\Sigma_{0,i} = \Sigma_{1,i} = ... = 0$ implies $\deg(f^i) \leq \frac{p-5}{2} + t + i$ for $i < \frac{p+1}{2} - t$.

Write $\deg(g) = \frac{p+1}{2} + s$. As we already mentioned, we have $r \leq t-2$ and $s \leq t-1$. Applying 3.5, we find the following equation:

$$F(x)f(x) + G(x)f^2(x) = H(x), \tag{1}$$

where $deg(F) \leq t-1$, $\deg(G) \leq t-2$ and $\deg(H) \leq \frac{p-1}{2}$. Supposing that this is the equation with $\deg(F)$ minimal, we have $(F,G) = 1$.

Claim 1 $deg(H) \leq 2t$ and $H \neq 0$.

Proof Let $h = \deg(H)$ and first suppose $h \geq \frac{p+3}{2} - t$. Then, according to (1), $x^{p-1-2h}H^2(x)$ is the linear combination of double powers of f, all of them have the form $x^k f(x)^l$ with $k + l \leq 2t + p - 1 - 2h \leq 2t + p - 1 - 2(\frac{p+3}{2} - t) = 4t - 4 \leq \frac{p+1}{2} - t$. But this is a contradiction, since $x^{p-1-2h}H^2(x)$ has degree $p-1$.

Next suppose $2t < h < \frac{p+3}{2} - t$. Then $r + h \leq \frac{p-3}{2}$, so we can consider $f(x)H(x)x^{\frac{p-3}{2}-r-h}$. It has degree $p-1$ and is the linear combination of double powers of f of the form $x^k f(x)^l$ with $k+l \leq 1+t+\frac{p-3}{2}-r-h \leq 1+t+\frac{p-3}{2}-1-(2t+1) = \frac{p-3}{2}-t$, a contradiction.

Finally note, that $H = 0$ would imply that $f(x)(F(x) + G(x)f(x))$ is a multiple of $x^p - x$, which is impossible, since f has at most one root and $\deg(F + Gf) < p - 1$. ∎

Claim 2 For $2 \leq i \leq t$ there exist polynomials $A(x)$ and $B(x)$ (depending on i) with $\deg(A), \deg(B) \leq 2it$, $(A,G) = 1$ and such that

$$A(x)f(x) + G^{i-1}(x)f^i(x) = B(x). \tag{2}$$

Proof We use induction on i, for $i = 2$ we have $A(x) = F(x)$ and $B(x) = H(x)$. In general suppose (2) holds for i. Multiplying with $G(x)f(x)$ we have

$$A(x)G(x)f^2(x) + G^i(x)f^{i+1}(x) = B(x)G(x)f(x). \tag{3}$$

Now (1) implies $G(x)f^2(x) = H(x) - F(x)f(x)$. Putting this into (3) and after a little counting we have

$$-(B(x)G(x) + A(x)F(x))f(x) + G^i(x)f^{i+1}(x) = -H(x)A(x),$$

and this is what we need for $i+1$: $\deg(-BG-AF) \le 2it+t < 2(i+1)t$, $\deg(-HA) \le 2t+2it = 2(i+1)t$ and $(BG+AF, G) = (AF, G) = 1$. ∎

Note that the previous claim shows in particular, that $\deg(f^i) > \frac{p+1}{2}$.

Now let $\Phi = \{Af + Bf^t : \deg(A), \deg(B) \le 2t^2\}$ and $\Psi = \{\phi \in \Phi : \deg(\phi) \le \frac{p-1}{2}\}$, these are subspaces of the vectorspace of polynomials over $GF(p)$. Let $\psi_0(x) = A_0(x)f(x) + B_0(x)f^t(x)$ be a non-zero element of Ψ with $\deg(A_0)$ minimal. According to 3.5, $\deg(A_0) \le 2t-3$, $\deg(B_0) \le t-2$.

Claim 3 $\deg(\psi_0) \le \frac{p-1}{2} - 2t^2$.

Proof Let $u = \deg(\psi_0)$ and first suppose $\frac{p+1}{2} - 2t^2 \le u \le \frac{p+1}{2} - t$. Then we can consider $f(x)\psi_0(x)x^{\frac{p-3}{2}-r-u}$, which is a polynomial of degree $p-1$ and is a linear combination of double powers of f of the form $x^k f(x)^l$ with $k+l \le 1+2t-2+\frac{p-3}{2}-r-u \le 1+2t-2+\frac{p-3}{2}-1-(\frac{p+1}{2}-2t^2) = 2t^2+2t-4 \le \frac{p+1}{2}-t$, a contradiciton.

Next suppose $\frac{p+3}{2} - t \le u \le \frac{p-1}{2}$. Then $\psi_0^2(x)x^{p-1-2u}$ gives the contradiction. ∎

Claim 4 The system $\{f(x), xf(x), ..., x^{2t^2}f(x), f^t(x), xf^t(x), ..., x^{2t^2}f^t(x)\}$ is linearly independent, so $dim(\Phi) = 4t^2+2$.

Proof A zero linear combination is equivalent with an equiation of the form $A(x)f(x) + B(x)f^t(x) = 0$, where $\deg(A), \deg(B) \le 2t^2$. But this would imply $f(x)(A(x) + B(x)f^t(x)) = 0$ (as a function), which means, that $x^p - x$ divides $f(x)(A(x) + B(x)f(x))$. Since f has at most one root and $\deg(A+Bf) < p-1$, this is only possible for $A(x) = B(x) = 0$. ∎

Claim 5 $\Psi = \{C(x)\psi_0(x) : \deg(C) \le c\}$, for a c.

Proof Write $d = \deg(A_0)$, $e = \deg(B_0)$ and, w.l.o.g., suppose $d \ge e$. Let $c = 2t^2 - d$.

There are $2t^2 - d + 1$ different degrees in the set $\{C(x)\psi_0(x) : \deg(C) \le c\}$, so according to 3.6 and the previous claim, we only have to find $4t^2 + 2 - (2t^2 - d + 1) = 2t^2 + d + 1$ different degrees bigger than $\frac{p-1}{2}$ in Φ.

Let $\Phi' = < f(x), xf(x), ..., x^{d-1}f(x), f^t(x), xf^t(x), ..., x^{e-1}f^t(x) >$.

It is easy to see that its elements have $d+e$ different degrees, all between $\frac{p+1}{2}$ and $d - 1 + \deg(f) = e - 1 + \deg(f^t)$.

The set $\{x^e f^t(x), ..., x^{2t^2}f^t(x)\}$ gives the rest of the desired degrees. ∎

Claim 6 $G(x)$ is a constant.

Proof Apply Claim 2 with $i = t$. $\deg(A), \deg(G^{t-1}) \le 2t^2$, $\deg(B) \le 2t^2 \le \frac{p-1}{2}$, so by Claim 5, B is divisible by ϕ. Since $(A, G) = 1$, this is only possible, if G^{t-1} is a constant multiple of B_0. Considering the degrees, this is only possible, if G is a constant. ∎

Now we consider two cases according to the degree of F.

Case 1 $\deg(F) \leq 1$.

Then $(ax+b)f(x) + f^2(x) = H(x)$ with $a \neq 0$, since we had $\deg(f) < \deg(f^2)$. Write $g(x) = f(x) + a/2x + b/2$ and $H_1(x) = H(x) + 1/4(ax+b)^2$. Then $g^2(x) = f^2(x) + (ax+b)f(x) + 1/4(ax+b)^2 = H_1(x)$ (here g^2 is the square of g after reduction modulo $x^p - x$).

All values of H_1 are square elements, so it cannot be linear. If it is a constant or of degree 2, then the graph of g (and hence of f) is contained in the union of two lines.

If $deg(H_1) \geq 3$, then, since we also have $\deg(H_1) \leq 2t$, for $d := \deg(g^{2(t-1)})$ we have $3t - 3 \leq d \leq 2t^2 - 2t \leq \frac{p-1}{2} - t$.

Now $\deg(g) + \deg(g^{2t-2}) \leq \frac{p-1}{2} + t + \frac{p-1}{2} - t = p - 1$, so $\deg(g^{2t-1}) = \deg(g) + \deg(g^{2t-2}) \geq \frac{p+1}{2} + d \geq \frac{p+1}{2} + 3t - 3$, which is a contradiction, since we saw that $\deg(f^i) \leq \frac{p-3}{2} + t + i$.

Case 2 $k := \deg(F) \geq 2$.

After linear transformation, we can suppose that $\deg(H) > k$.

We consider two subcases according to the degree of H.

Subcase 1 $k < \deg(H) < 2k$.

By induction on i, one can easily prove that in equation (2) of Claim 2, we have $\deg(A) = (i-1)k$ and $\deg(B) = \deg(H) + (i-2)k$, implying $deg(f^i) = \deg(f) + k(i-1) \geq \frac{p+1}{2} + 2(i-1)$. For $i = t$ this is a contradiction.

Subcase 2 $\deg(H) \geq 2k$.

Recall that we also have $\deg(H) \leq 2t$. It is easy to see that if $\deg(f) = \frac{p+1}{2} + r$, then $\deg(f^2) = \frac{p+1}{2} + r + k$.

Consider $U(x) = H^{t-1}(x)$ and write $u = \deg(U)$. We have $2k(t-1) \leq u \leq 2t(t-1) \leq \frac{p-1}{2} - 2t \leq \frac{p-1}{2} - r - k - 1$.

$f(x)^2 U(x) x^{\frac{p-1}{2} - u - r - k - 1}$ is a polynomial of degree $p-1$ and is the linear combination of double powers of f of the form $x^a f(x)^b$ with $a + b \leq 2 + (t-1)(k+1) + \frac{p-1}{2} - k - r - u - 1 \leq 2 + (t-1)(k+1) + \frac{p-1}{2} - k - 1 - 2k(t-1) - 1 = \frac{p-3}{2} - (k-1)t \leq \frac{p-3}{2} - t$, a contradiction. ∎

4 Final Remarks

With a bit more careful counting, $\frac{1}{3}$ can be replaced with any $c < \frac{1}{2}$ constant for sufficiently large p both in 2.5 and 2.6.

With the terminology of blocking sets, 2.6 can be formulated in the following way:

Theorem 4.1 A blocking set of Rédei type in $PG(2,p)$, p prime, is the projective triangle (of size $p + \frac{p+3}{2}$) or has size at least $p + \frac{p+3}{2} + \frac{1}{3}\sqrt{p}$. ∎

For an arbitrary square prime power q, Szőnyi, Polverino and Weiner [8] constructed blocking sets of Rédei type of size $q + \frac{q+3}{2} + \frac{1}{2}\sqrt{q}$.

Finally, we formulate two conjectures motivated by this text. In both of them f is a polynomial over $GF(p)$, p prime, of degree at least 4. The first one would imply that condition (vi) is not necessary in the statement of 2.6.

Conjecture 4.2 If the graph of f is contained in the union of two lines, then its degree is $\frac{p+1}{2}$ or at least $\frac{p+1}{2} + \frac{1}{3}\sqrt{p}$.

Our last conjecture would imply 1.4.

Conjecture 4.3 If f is not affinely equivalent to $x^{\frac{p+1}{2}}$, then $I(f) \leq \frac{p-1}{3}$ or $\frac{p+1}{3}$ (according as $3|p-1$ or $3|p+1$).

Acknowledgements. The author acknowledges the financial support of OTKA Grants F-016302, T-019367.

5. References

[1] A. Gács: On the Number of Directions Determined by a Point Set in $AG(2,p)$ (to appear in Disc. Maths.).
[2] A. Blokhuis, A. E. Brouwer, T. Szőnyi: The number of directions determined by a function f on a finite field, *J. Comb. Theory, Ser. A.* **70** (1995), 349–353.
[3] L. Rédei: Lückenhafte Polynome über endlichen Körpern, *Birkhäuser Verlag, Basel* (1970) (English translation: Lacunary polynomials over finite fields, *North Holland, Amsterdam* (1973)).
[4] L. Lovász, A. Schrijver: Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981) 449-454.
[5] S. Ball, A. Blokhuis, A. Brouwer, L. Storme, T. Szőnyi: On the number of directions determined by a polynomial, *manuscript.*
[6] A. Blokhuis: On the size of a blocking set in $PG(2,p)$, *Combinatorica* **14** (1994), 111-114.
[7] T. Szőnyi: Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica*, **19** (1991), 91-100.
[8] O. Polverino, T. Szőnyi and Zs. Weiner: Blocking sets in $PG(2,q^{2t})$, submitted to *Acta Math. Szeged.*