1 Lacunary Polynomials over Finite Fields.

1.1 Introduction

In 1970 Rédei published his treatise *Lückenhafte Polynome über endlichen Körpern* [34], soon followed by the English translation *Lacunary Polynomials over Finite Fields*, the title of this chapter.

One of the important applications of his theory is to give information about the following two equivalent problems:

I: Directions: For $f : \mathbb{F}_q \to \mathbb{F}_q$, or $f \in \mathbb{F}_q[X]$ define the set of directions (slopes of secants of the graph):

$$(D_q(f) =)D(f) := \left\{ \frac{f(x) - f(y)}{x - y} \,|\, x \neq y \in \mathbb{F}_q \right\}.$$

What can be said about this set, in particular about its size.

II: Permutation polynomials: For $f \in \mathbb{F}_q[X]$ let

$$P(f) := \{m \in \mathbb{F}_q \,|\, f(X) + mX \text{ is a permutation polynomial}\}.$$

What can be said about this set.

The two problems are equivalent, since $P(f)$ and $D(f)$ partition $\mathbb{F}_q$. If $(f(x) - f(y))/(x - y) = m$ then $f(x) + mx = f(y) + my$, so m is a direction determined by f precisely when $f(X) + mX$ is *not* a permutation polynomial (on $\mathbb{F}_q$).

Soon after the publication of Rédei's book various people realized the importance of his results for problems in finite geometry, in particular blocking sets. To employ the strength of the theory it was necessary to generalize the questions and the results about lacunary polynomials. In this survey we will collect these problems and results. The introductory sections introducing lacunary polynomials and their connection with the direction problem heavily lean on the corresponding sections in [5].

1.2 Lacunary polynomials

Let K be a (finite) field. A polynomial $f \in K[x]$ is called *fully reducible* if K is a splitting field for f, that is, if f factors completely into linear factors in $K[X]$. Following Rédei we denote by f° the degree of f, and by $f^{\circ\circ}$ the second degree, the degree of the polynomial we obtain by removing the leading term. If $f^{\circ\circ} < f^\circ - 1$ then f is called *lacunary* and the difference $f^\circ - f^{\circ\circ}$ is called the *gap*. We want to survey what is known about lacunary polynomials (with a large gap) that are fully reducible. In many applications however the gap is not between the degree and the second degree.

Let us start by giving some important examples of polynomials with small second degree. For $d \,|\, q - 1$ the field $K = \mathbb{F}_q$ contains the d-th roots of unity, so the polynomial

$X^d - a^d$ is fully reducible. In many applications the degree $f^\circ = q$, and we have the examples $f(X) = X^q + c = (X + c)^q$, $f(X) = X^q - X = \prod_{a \in \mathbb{F}_q}(X - a)$, $f(X) = X^q \pm X^{(q+1)/2} = X^{(q+1)/2}(X^{(q-1)/2} \pm 1)$ and $f(X) = X^q \pm 2X^{(q+1)/2} + X = X(X^{(q-1)/2} \pm 1)^2$.

Proofs of results will not be given, but we make an exception for the following first and typical result because it shows the power of some simple observations. Throughout the paper we will tacitly assume that p is a prime, and q a prime power.

Theorem 1.1. Let $f(X) = X^p + g(X)$, with $g^\circ = f^{\circ\circ} < p$, be fully reducible in $\mathbb{F}_p[X]$, p prime. Then either g is constant, or $g = -X$ or g° (and hence $f^{\circ\circ}$) is at least $(p+1)/2$.

Proof. Let $s(X)$ be the zeros polynomial of f, that is the polynomial with the same set of zeros as f, but each with multiplicity one. So $s = \gcd(f, X^p - X)$. It follows that

$$s \mid f - (X^p - X) = X + g.$$

We may write $f = s \cdot r$, where r is the fully reducible polynomial that has the zeroes of f with multiplicity one less. Hence r divides the derivative $f' = g'$. So we conclude that

$$f = s \cdot r \mid (X + g)g'.$$

If the right hand side is zero, then either $g = -X$, corresponding to the fully reducible polynomial $f(X) = X^q - X$, or $g' = 0$ which (since $g^\circ < p$) implies $g(X) = c$ for some $c \in K$ and $f(X) = X^p + c = (X + c)^p$. If the right hand side is nonzero, then, being divisible by f, it has degree at least p, so $g^\circ + g^\circ - 1 \geq p$ which gives $g^\circ \geq (p+1)/2$. □

In the next section we will see how this result can be applied to obtain information about the number of directions determined by a function, but let us mention here first Rédei's original theorem in the general case (if q is prime then $e = 0$ and we have the previous theorem):

Theorem 1.2. Let $f(X) = X^q + g(X)$, be fully reducible in $\mathbb{F}_q[X^{p^e}] \backslash \mathbb{F}_q[X^{p^{e+1}}]$, $p^e < q = p^h$. Then

$$g^\circ \geq p^e \left\lceil \frac{q/p^e + 1}{p^e + 1} \right\rceil.$$

1.3 Directions and the Rédei polynomial

Let A be the Desarguesian affine plane of order q, $AG(2, q)$. Points of A will be denoted by pairs (a, b), $a, b \in GF(q)$. We consider A as part of the projective plane $\Pi = PG(2, q)$ with homogeneous point coordinates $(a : b : c)$ and line coordinates $[u : v : w]$. So the point $(a : b : c)$ is incident with the line $[u : v : w]$ precisely when $au + bv + cw = 0$. The equation of the line $[u : v : w]$ is then $uX + vY + wZ = 0$ and dually we say that the equation of the point $(a : b : c)$ is $aU + bV + cW = 0$. The line at infinity is $[0 : 0 : 1]$ with equation $Z = 0$. The affine point (a, b) corresponds to the projective point $(a : b : 1)$.

Let $u = (u_1, u_2)$ and $v = (v_1, v_2)$ be two affine points. We say that the pair u, v determines the direction m if the line joining them has slope m, or equivalently, if $(u_2 -$

$v_2)/(u_1 - v_1) = m$. The lines with slope m are all parallel and meet at the point on the line at infinity which we sometimes denote by (m), so $(m) = (1 : m : 0)$ if $m \neq \infty$ and $(\infty) = (0 : 1 : 0)$. The line $Y = mX + n$ with slope $m \neq \infty$ has line coordinates $[m : -1 : n]$, the coordinates of the vertical line $X = c$ are $[1 : 0 : -c]$.

In this section we shall see how fully reducible lacunary polynomials show up in the direction problem. Let R be a set of q points in A, and let D_R be the set of directions determined by the pairs of points in R.

The reason we take R to have size q is two-fold. Firstly, in Rédei's formulation of the problem R is the graph of a function f and $D_R = D_f$. Secondly, any set with more than q points determines all directions, by the pigeon hole principle: there are exactly q lines in every parallel class, so if $|R| > q$, then there is a line with at least two points of R in each parallel class. For results concerning the case $|R| < q$, see [36].

With an affine set R we associate its *Rédei Polynomial*,

$$r_R(U, V, W) = \prod_{(a,b)\in R} (aU + bV + W).$$

We are interested in the intersection of R with the lines having slope m, and these lines have coordinates $[m : -1 : n]$, so we fix $V = -1$ and obtain a polynomial in two variables

$$H(U, W) = r_R(U, -1, W) = \prod_{(a,b)\in R} (aU - b + W).$$

The connection between sets which do not determine all directions and lacunary polynomials comes from the following observation.

Write

$$H(U, W) = \sum_{j=0}^{q} h_j(U) W^{q-j}.$$

The polynomial h_j has degree at most j. Let $U = m$, and consider the polynomial in one variable

$$H_m(W) := H(m, W) = \sum_{j=0}^{q} h_j(m) W^{q-j} = \prod_{(a,b)\in R} (am - b + W).$$

If the direction m is *not* determined by the set R, then R has exactly one point on each line with slope m, and $am - b$ assumes all values in the field exactly once, and therefore $H_m(W) = W^q - W$. In particular $h_j(m) = 0$ for $j = 1, 2, \ldots, q-2$ and for $j = q$. Since h_j is a polynomial of degree at most j and vanishes for $q + 1 - N$ values m, where N is the number of directions determined by R, we get that h_j vanishes identically for $j = 1, 2, \ldots, q - N$.

If the direction m is determined by R, then $H_m(W)$ is a fully reducible lacunary polynomial of degree q, and second degree at most $N - 1$ so our bounds from the previous section will give us information on N.

Together with some geometrical observations this results in the following theorem (compare [34, Satz 24] or [11, Theorem 1]).

Theorem 1.3. Let R be a set of q points in $AG(2,q)$, and let N be the number of directions determined by pairs from R. Then either $N = 1$, or $N \geq (q+3)/2$, or $2+(q-1)/(p^e+1) \leq N \leq (q-1)/(p^e-1)$ for some e, $1 \leq e \leq \lfloor n/2 \rfloor$.

1.4 Sets of points determining few directions

The third case in Rédei's direction theorem, $2 + (q-1)/(p^e+1) \leq N \leq (q-1)/(p^e-1)$ for some e satisfying $1 \leq e \leq \lfloor n/2 \rfloor$, is not sharp but let us start by mentioning examples of functions determining few directions.

Example 1. The function $f(X) = X^{(q+1)/2}$, where q is odd, determines $(q+3)/2$ directions.

Example 2. The function $f(X) = X^s$, where $s = p^e$ is the order of a subfield of $\mathbb{F}_q$, determines $(q-1)/(s-1)$ directions.

Example 3. The function $f(X) = \mathbf{T}_{q\to s}(X)$, the trace from $\mathbb{F}_q$ to the subfield $\mathbb{F}_s$, determines $1 + q/s$ directions.

Example 4. If $f(X) \in \mathbb{F}_q[X^s]$, where s is the order of a subfield of $\mathbb{F}_q$ and is chosen maximal with this property, in other words, f is $\mathbb{F}_s$-linear (apart from the constant term) but not linear over a larger subfield, then $1 + q/s \leq N \leq (q-1)/(s-1)$.

Motivated by the form of the examples the following final theorem was obtained (in a number of steps) by Ball, Blokhuis, Brouwer, Storme and Szőnyi: Initial results are in [11], then the classification was all but obtained in [10], and completed in [2].

Theorem 1.4. If, for $f : \mathbb{F}_q \to \mathbb{F}_q$, with $f(0) = 0$, the number $N > 1$ of directions determined by f is less than $(q+3)/2$, then for a subfield $\mathbb{F}_s$ of $\mathbb{F}_q$

$$\frac{q}{s} + 1 \leq N \leq \frac{q-1}{s-1},$$

and if $s > 2$ then f is $\mathbb{F}_s$-linear.

To prove this result several lemmas about fully reducible lacunary polynomials are needed, that are of independent interest. The first is already in Rédei's book and can be proved in the same way as Theorem 1.1.

Lemma 1.5. Let $s = p^e$ be a power of p with $1 \leq s < q$ and suppose that

$$X^{q/s} + g(X) \in \mathbb{F}_q[X] \setminus \mathbb{F}_q[X^p]$$

is fully reducible over $\mathbb{F}_q$. Then either $s = 1$ and $g(X) = -X$ or $g^\circ \geq (\frac{q}{s}+1)/(s+1)$.

Lemma 1.6. Let s be a power of p with $1 \leq s < q$ and suppose that

$$X^{q/s} + g(X) \in \mathbb{F}_q[X] \setminus \mathbb{F}_q[X^p]$$

is fully reducible over $\mathbb{F}_q$. If $s > 2$, $g^\circ = q/s^2$ and $2(g')^\circ < g^\circ$ then

$$f \in \langle 1, X, X^s, X^{s^2}, \ldots, X^{q/s} \rangle_{\mathbb{F}_q}.$$

The directions theorem completely characterizes the case that the number of directions is *small*, that is less than $(q+3)/2$. In the case that $q = p$ is prime, $N < (p+3)/2$ implies $N = 1$, and the characterisation of $N = (p+3)/2$ directions was given by Lovász and Schrijver [26].

Theorem 1.7. If $f \in \mathbb{F}_p[X]$ determines $(p+3)/2$ directions, then $f(X) = X^{(p+1)/2}$ up to affine equivalence.

Much more can be said in this case, the following surprising theorem by András Gács [21] shows that there is a huge gap in the spectrum of possible number of directions:

Theorem 1.8. If the number of directions determined by $f \in \mathbb{F}_p[X]$ is more than $(p+3)/2$, then it is at least $\left\lceil \frac{2}{3}(p-1) \right\rceil + 1$.

This bound is almost tight, there are examples that determine $\frac{2}{3}(p-1)+2$ directions if $p = 1 \bmod 3$. Further progress was made using Gács' approach in [6] and some constructions can be found [24].

For results concerning the case $q = p^2$, see [22]. For results on functions $f : \mathbb{F}_q^k \to \mathbb{F}_q$, with $k \geq 2$, that determine few directions, see [3], and for results on functions $f, g : \mathbb{F}_q \to \mathbb{F}_q$, where $P(f,g) = \{(r,s) \in \mathbb{F}_q^2 \mid X + rf(X) + sg(X) \text{ is a permutation polynomial}\}$ is large, see [7].

1.5 Lacunary Polynomials and Blocking Sets

Let R be a subset of $A = AG(2,q)$ of size q and consider the set $B = R \cup D_R$, so the set R together with the directions it determines. Every line of the (projective) plane $\Pi = PG(2,q)$ intersects B. Indeed, if the intersection of an affine line l with the line at infinity is not in D_R, then l and its parallels all intersect R in exactly one point.

Sets with this property are called *blocking sets* and here we are interested in very small ones. Since through any point in $PG(2,q)$ there are $q+1$ lines, a blocking set must have at least $q+1$ points, and it is easy to see that equality can only obtained if these points all are on a line. Blocking sets containing a line are called *trivial*. We will tacitly assume that all blocking sets under consideration are *minimal*, so they do not contain a proper subset that is also a blocking set. For blocking sets of non-Desarguesian planes and for further reading on blocking sets see [9], [14], [16], [17], [18], [20] and [23] and for more recent articles concerning the linearity conjecture (Conjecture 1.11) see [25], [28], [29], [30], [35] and [37].

Let us consider the Rédei polynomial of a blocking set B of $PG(2,q)$. Suppose $|B| = q+k+1$, let $(1:0:0) \in B$, and assume that the line with equation $Z = 0$, that is $[0:0:1]$ is a tangent. The non-horizontal lines $[1:u:v]$ are then blocked by the affine points of B so the polynomial

$$F(V,W) = \prod_{(a:b:1)\in B} (a + bV + W)$$

of degree $q+k$ vanishes for all $v, w \in \mathbb{F}_q$. Therefore we can write

$$F(V,W) = (V^q - V)G(V,W) + (W^q - W)H(V,W)$$

where G and H are of total degree k in the variables V and W. Let F_0 denote the part of F that is homogeneous of degree $q+k$, and let G_0 and H_0 be the parts of G and H that are homogeneous of total degree k. Restricting to the terms of total degree $q+k$ we get the homogeneous equation

$$F_0 = V^q G_0 + W^q H_0,$$

with

$$F_0(V,W) = \prod_{(a:b:1)\in B} (bV + W).$$

Write $F_0(1,W) = f(W)$ and define g and h analogously, then we get the one-variable equation

$$f(W) = g(W) + W^q h(W)$$

where f is a fully reducible polynomial in $\mathbb{F}_q[W]$. So we are in a situation that is quite similar to that of Rédei's lacunary polynomial theorem, and in fact we can conclude more or less the same.

Theorem 1.9. Let $f \in \mathbb{F}_q[X]$ be fully reducible, and suppose that $f(X) = X^q g(X) + h(X)$, where g and h have no common factor. Let k be the maximum of the degrees of g and h. Then $k = 0$, or $k = 1$ and $f(X) = a(X^q - X)$ for some $a \in \mathbb{F}_q^*$, or q is prime and $k \geq (q+1)/2$, or q is a square and $k \geq \sqrt{q}$, or $q = p^{2e+1}$ for some prime p and $k \geq p^{e+1}$.

This bound is sharp in the case that q is a square, and if $q = p^{2e+1}$ we obtain the bound $|B| \geq q + p^{e+1} + 1$, which is only sharp in the case $e = 1$.

The most important consequence of this theorem is the following theorem.

Theorem 1.10. A non-trivial blocking set in $PG(2,p)$ has at least $\frac{3}{2}(p+1)$ points. If equality holds then every point of it is on precisely $\frac{1}{2}(p-1)$ tangents.

This bound was conjectured in [19] and proved in [8].

The proof of the lemma on lacunary polynomials follows Rédei's line given in the introduction, and leads to the following divisibility

$$f | (Xg + h)(h'g - g'h).$$

It would be very nice (and probably not infeasible) to characterize the case of equality here if p is prime, that is find all f, g and h with f of degree $q+(q+1)/2$, g and h of degree at most $(q+1)/2$ and $f \hat{=} (Xg+h)(h'g-g'h)$. This will be the subject of the next section.

To finish this section we mention the linearity conjecture from [35].

Conjecture 1.11. If B is a blocking set in $PG(2,p^n)$ of less than $3(p^n+1)/2$ points then there exists an n-dimensional subspace U of $PG(3n-1,p)$ with the property that every point of B, when viewed as an $n-1$-dimensional subspace of $PG(3n-1,p)$ has non-trivial intersection with U.

1.6 Lacunary Polynomials and Blocking Sets in Planes of Prime Order

We have seen that the blocking set problem leads one to search for polynomials $f(X)$, $g(X)$, $h(X)$, where f factors completely into linear factors and g and h have degree at most $\frac{1}{2}(p+1)$ such that $f = X^p g + h$.

More precisely: we find such an f given a blocking set S of size $\frac{3}{2}(p+1)$, a point $P \in S$, and a tangent L passing through P. An e-fold linear factor of f corresponds to a line on P distinct from L meeting S in $e+1$ points.

The equation has several infinite families of solutions, and some sporadic ones, not all of them necessarily corresponding to blocking sets. We give all solutions for $p < 41$.

a) (For odd p, say $p = 2r+1$.) Take $f(X) = X\prod(X-a)^3$ where the product is over the nonzero squares a. Then f satisfies $f(X) = X(X^r-1)^3 = X^p g + h$ with $g(X) = X^r - 3$, $h(X) = 3X^{r+1} - X$. This would correspond to line intersections (with frequencies written as exponents) 1^r, 2^2, 4^r. For $p = 7$ this is the function for the blocking set $\{(1:0:0),(0:1:0),(0:0:1)\} \cup \{(a:b:1) \mid a,b \in \{1,2,4\}\}$.

b) (For $p = 4t+1$.) Take $f(X) = X\prod(X-a)\prod(X-b)^4$ where the product is over the nonzero squares a and fourth powers b. Here $f(X) = X(X^{2t}-1)(X^t-1)^4 = X^p g + h$ with $g(X) = X^{2t} - 4X^t + 5$ and $h(X) = -5X^{2t+1} + 4X^{t+1} - X$. This would correspond to line intersections 1^{2t}, 2^{t+2}, 6^t.

c) (For $p = 4t+1$.) Take $f(X) = X^{t+1}\prod(X-a)\prod(X-b)^2$ where the product is over the nonzero squares a and fourth powers b. Here $f(X) = X^{t+1}(X^{2t}-1)(X^t-1)^2 = X^p g + h$ with $g(X) = X^t - 2$ and $h(X) = 2X^{2t+1} - X^{t+1}$. This would correspond to line intersections 1^{2t}, 2^t, 4^t $(t+2)^2$. For $p = 13$ this is a function for the blocking set $\{(1:0:0),(0:1:0),(0:0:1)\} \cup \{(1:a:0),(0:1:a),(a:0:1) \mid a^3 = -1\} \cup \{(b:c:1) \mid b^3 = c^3 = 1\}$.

d) (For $p = 13$.) Take $f(X) = X\prod(X-a)^4\prod(X-\frac{1}{2}a)$ where the product is over the a with $a^3 = 1$. Here $f(X) = X(X^3-1)^4(X^3-\frac{1}{8}) = X^p g + h$ with $g(X) = X^3 + 4$ and $h(X) = 5X^7 - 5X^4 - 5X$. This corresponds to line intersections 1^6, 2^4, 5^4, and indeed occurs.

These lacunary polynomials are just weighted subsets of the projective line, and in particular $PGL(2,p)$ acts. For example, $X \mapsto 1/X$ sends $X^p g + h$ to $X^p \tilde{h} + \tilde{g}$ where $\tilde{k}(X) = X^{(p+1)/2} k(X^{-1})$.

For completeness we describe the lacunary polynomials that correspond to the Rédei type blocking set:

e) Take $f(X) = X^p - X^{(p+1)/2} = X^{(p+1)/2}\prod(X-a)$ where the product is over the nonzero squares a.

f) Take $f(X) = X^p - 2X^{(p+1)/2} + X = X\prod(X-a)^2$ where the product is over the nonzero squares a.

As a consequence of this we have the following theorem from [12].

Theorem 1.12. Let B be a non-trivial blocking set in $PG(2,p)$ of size $\frac{3}{2}(p+1)$, where p is a prime less than 41. Then B is of Rédei type (and hence the example characterized by Lovász and Schrijver) or $p \in \{7, 13\}$ and there is a unique other example in both cases.

We conjecture that the restriction $p < 41$ is unnecessary.

1.7 Lacunary Polynomials and Multiple Blocking Sets

A t-fold blocking set is a collection of points such that every line contains at least t of them. As was the case for ordinary blocking sets, the theory of lacunary polynomials can be applied here as well.

The following result appears in [13] improving on [15].

Theorem 1.13. Let B be a t-fold blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, of size $t(q+1)+c$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$.

1. If $q = p^{2d+1}$ and $t < q/2 - c_p\, q^{2/3}/2$, then $c \geq c_p\, q^{2/3}$, unless $t = 1$ in which case B, with $|B| < q + 1 + c_p\, q^{2/3}$, contains a line.

2. If $4 < q$ is a square, $t < q^{1/4}/2$ and $c < c_p\, q^{2/3}$, then $c \geq t\sqrt{q}$ and B contains the union of t disjoint Baer subplanes, except for $t = 1$ in which case B contains a line or a Baer subplane.

3. If $q = p^2$, p prime, and $t < q^{1/4}/2$ and $c < p\left\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}} \right\rceil$, then $c \geq t\sqrt{q}$ and B contains the union of t disjoint Baer subplanes, except for $t = 1$ in which case B contains a line or a Baer subplane.

For more precise results in the case $t = 2$, see [4] for $t = 3$, see [1], for $q = p^3$, see [31], [32] and [33], for $q = p^{6n+3}$, see [13], and for $q = p^{6n}$, see [33] and [13].

The proof of Theorem 1.13 starts with the main theorem of [15] on fully reducible lacunary polynomials.

Theorem 1.14. Let $f \in \mathbb{F}_q[X]$, $q = p^n$, p prime, be fully reducible, $f(X) = X^q g(X) + h(X)$, where $(g,h) = 1$. Let $k = \max(g^\circ, h^\circ) < q$. Let e be maximal such that f is a p^e-th power. Then we have one of the following:

1. $e = n$ and $k = 0$;

2. $e \geq 2n/3$ and $k \geq p^e$;

3. $2n/3 > e > n/2$ and $k \geq p^{n-e/2} - (3/2)p^{n-e}$;

4. $e = n/2$ and $k = p^e$ and $f(X) = a\mathbf{T}(bX + c) + d$ or $f(X) = a\mathbf{Norm}(bX + c) + d$ for suitable constants a, b, c, d. Here $\mathbf{T}$ and $\mathbf{Norm}$ respectively denote the trace and norm function from $\mathbb{F}_q$ to $\mathbb{F}_{\sqrt{q}}$;

5. $e = n/2$ and $k \geq p^e \left\lceil \frac{1}{4} + \sqrt{(p^e+1)/2} \right\rceil$;

6. $n/2 > e > n/3$ and $k \geq p^{n/2+e/2} - p^{n-e} - p^e/2$, or if $3e = n + 1$ and $p \leq 3$, then $k \geq p^e(p^e + 1)/2$;

7. $n/3 \geq e > 0$ and $k \geq p^e \lceil (p^{n-e} + 1)/(p^e + 1) \rceil$;

8. $e = 0$ and $k \geq (q + 1)/2$;

9. $e = 0$, $k = 1$ and $f(X) = a(X^q - X)$.

References

[1] S. Ball, On the size of a triple blocking set in $PG(2, q)$, *European J. Combin.*, **5** (1996) 427–435.

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

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

[4] S. Ball and A. Blokhuis, On the size of a double blocking set in $PG(2, q)$, *Finite Fields Appl.*, **2** (1996) 125–137.

[5] S. Ball and A. Blokhuis, Polynomials in Finite Geometry, in: quaderni di matematica: *Methods of Discrete Mathematics* **5**, editors Stefan Löwe, Francesco Mazzocca, Nicola Melone and Udo Ott, Seconda Università degli Studi di Napoli, (1999) 71–101.

[6] S. Ball and A. Gács, On the graph of a function over a prime field whose small powers have bounded degree, *European J. Combin.*, **30** (2009) 1575–1584.

[7] 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.

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

[9] A. Blokhuis, Blocking sets in Desarguesian Planes, in: *Paul Erdős is Eighty* **2**, editors D. Miklós, V.T. Sós, T. Szőnyi, Bolyai Soc. Math. Studies, (1996) 133–155.

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

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

[12] A. Blokhuis, A. E. Brouwer and H.A. Wilbrink, Blocking sets in $PG(2,p)$ for small p, and partial spreads in $PG(3,7)$, *Adv. Geom.*, special issue, (2003) 245–253.

[13] A. Blokhuis, L. Lovász, L. Storme and T. Szőnyi, On multiple blocking sets in Galois planes, *Adv. Geom.*, **7** (2007) 39–53.

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

[15] A. Blokhuis, L. Storme and T. Szőnyi, Lacunary polynomials, multiple blocking sets and Baer subplanes, *J. London Math. Soc.*, **60** (1999) 321-332.

[16] A. A. Bruen, Blocking sets in finite projective planes, *SIAM J. Appl. Math.*, **21** (1971) 380–392.

[17] A. A. Bruen and R. Silverman, Arcs and Blocking Sets II, *European J. Combin.*, **8** (1987) 351–356.

[18] A.A. Bruen and J.A. Thas, Blocking Sets, *Geom. Ded.*, **6** (1977) 193–203.

[19] J. Di Paola, On minimum blocking coalitions in small projective plane games, *SIAM J. Appl. Math.*, **17** (1969) 378–392.

[20] A. Gács, A remark on blocking sets of almost Rédei type, *J. Geom.* **60** (1997) 65–73.

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

[22] A. Gács, L. Lovász and T. Szőnyi, Directions in $AG(2,p^2)$, *Innov. Incidence Geom.*, **6/7** (2007/8) 189–201.

[23] A. Gács, P. Sziklai and T. Szőnyi, Two remarks on blocking sets and nuclei in planes of prime order, *Des. Codes Cryptogr.*, **10** (1997) 29–39.

[24] N. V. Harrach and C. Mengyán, Minimal blocking sets in $PG(2,q)$ arising from a generalized construction of Megyesi, *Innov. Incidence Geom.*, **6/7** (2007/08) 211–226.

[25] M. Lavrauw, L. Storme and G. Van de Voorde, A proof of the linearity conjecture for k-blocking sets in $PG(n,p^3)$, p prime, *J. Combin. Theory Ser. A*, **118** (2011) 808–818.

[26] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Sci. Math. Hungar.*, **16** (1983) 449–454.

[27] L. Lovász and T. Szőnyi, Multiple blocking sets and algebraic curves. Abstract from *Finite Geometry and Combinatorics* (Third International Conference at Deinze (Belgium), May 18-24, 1997).

[28] G. Lunardon, Normal spreads, *Geom. Dedicata*, **75** (1999) 245–261.

[29] G. Lunardon and O. Polverino, Blocking sets of size $q^t + q^{t-1} + 1$, *J. Combin. Theory Ser. A*, **90** (2000) 148–158.

[30] P. Polito and O. Polverino, Linear blocking sets in $PG(2, q^4)$, *Australas. J. Combin.*, **26** (2002) 41–48.

[31] O. Polverino, Small minimal blocking sets and complete k-arcs in $PG(2, p^3)$, *Discrete Math.*, **208/209** (1999) 469–476.

[32] O. Polverino, Small blocking sets in $PG(2, p^3)$, *Des. Codes Cryptogr.*, **20** (2000) 319–324.

[33] O. Polverino and L. Storme, Minimal blocking sets in $PG(2, q^3)$, *European J. Combin.*, **23** (2002) 83–92.

[34] L. Rédei, *Lückenhafte Polynome über endlichen Körpern. Birkhäuser Verlag, Basel (1970)* (English translation Lacunary polynomials over finite fields, North Holland, 1973)

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

[36] 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.

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