Lacunary Polynomials over Finite Fields

Course notes

Javier Herranz

Abstract

This is a summary of the course Lacunary Polynomials over Finite Fields, given by Simeon Ball, from the University of London, in March 5-8, 2002, at the Universitat Politècnica de Catalunya (Barcelona). Explanations of Dr. Ball have been complemented with some results of [3] and [4].

1 Introduction

The object of the talks was to give an introduction to lacunary polynomials over finite fields and show some applications to the problem of determining the number of slopes defined by the graph of a function on a finite field and to the size of minimum blocking sets in projective planes.

The notes are organised as follows. Section 2 is an introduction to lacunary polynomials, fully reducible polynomials with a gap between its degree and second degree, together with main results on the size of this gap. In Section 3, application of these results to obtain bounds on the number of slopes of the graph of a function defined on a finite field. Section 4 deals with an application to bound the size of a minimal blocking set in a projective plane. Finally, Section 5 includes some recent results on the above two problems together with open problems and conjectures.

2 Lacunary Polynomials

Definition 2.1. Let K be a (commutative) field. A polynomial $f \in K[X]$ is said to be *fully reducible* if f factors completely into linear factors over $K[X]$; in other words, K is a splitting field for f.

We denote by f° the degree of f, and by $f^{\circ\circ}$ its second degree, that is, the degree of $f(x) - c_{f^\circ} X^{f^\circ}$, were c_{f° is the leading coefficient of f.

Definition 2.2. We say a polynomial f is a *lacunary polynomial* if it is fully reducible and $f^{\circ\circ} < f^\circ - 1$.

For example, any polynomial in $\mathbb{C}[X]$ is fully reducible. In $\mathbb{R}[X]$, if a polynomial f is lacunary, then $f^\circ - f^{\circ\circ} \leq 2$ or $f(X) = cX^{f^\circ}$. We are interested in $K = GF(q)$, the finite field with q elements. So $q = p^h$ for some prime p and some integer h. Let us see some examples in this case.

Example 2.1. $f(X) = X^q - X = \prod_{a \in GF(q)} (X - a)$. In this case, $f^{\circ\circ} = 1$.

Example 2.2. If q is even, we can define the polynomial

$$Tr_{q \to 2}(X) := X + X^2 + X^4 + \ldots + X^{q/2},$$

which satisfies $Tr(X)$ divides $(X^q + X)$, since

$$(Tr(X)_{q \to 2})^2 + Tr(X)_{q \to 2} = X^q + X,$$

and thus the polynomial is fully reducible. Here $f^{\circ\circ} = f^{\circ}/2$.

Lacunary polynomials were introduced by Rédei in [11]. The main results in this section (basically Theorems 2.1 and 2.2) are due to him. Before stating the first theorem, let us consider a polynomial

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^i \in GF(q)[X].$$

If we define

$$f'(X) = \sum_{i=0}^{n} i a_i X^{i-1},$$

then we have

$$f' = 0 \iff f \in GF(q)[X^p].$$

Definition 2.3. We say that a is a *k-fold root* of f if $(X - a)^k | f(X)$.

If a is a k-fold root of f, then it is clear that a is a $(k-1)$-fold root of f'. Furthermore, if $p|k$, then a is also a k-fold root of f'; indeed, if $f(X) = (X - a)^k g(X)$, then

$$f'(X) = (X - a)^k g'(X) + g(X) k (X - a)^{k-1} = (X - a)^k g'(X),$$

because $k = 0$ in $GF(q)[X]$.

Theorem 2.1. *Let $f(X) = X^p + g(X)$, with $g^{\circ} = f^{\circ\circ} < p$, be fully reducible in $GF(p)[X]$, p a prime. Then either g is constant, or $g = -X$, or $g^{\circ} \geq (p+1)/2$.*

Proof. We note first that $f' = g'$. Let us now write $f(X) = r(X)s(X)$, where $s(X)$ contains all the linear factors of f exactly once. So $r(X)$ contains all the repeated factors of f. Now

$$\left.\begin{array}{c} s(X) | f - (X^p - X) \ = X + g \\ r(X) | f' \ = g' \end{array}\right\} \Longrightarrow \ f(X) = \ r(X)s(X) \mid (X + g)g' \qquad (1)$$

We consider 3 cases:

(a) If $g' = 0$, then $\left.\begin{array}{c} g \in K[X^p] \\ g^{\circ} < p \end{array}\right\} \Longrightarrow$ g is constant.

(b) If $g' \neq 0$ and $X + g \neq 0$ (i.e., $g \neq -X$), then comparison of degrees in the divisibility relation (1) gives:

$$p \leq g^{\circ} - 1 + g^{\circ} \implies g^{\circ} \geq \frac{p+1}{2}$$

(c) Finally, if $g' \neq 0$ and $X + g = 0$, then $g = -X$.

□

When $g^\circ = (p+1)/2$ holds, we can be more precise about the structure of f. The divisibility relation (1) is actually an equality (up to scalars), that is,

$$X^p + g = c(X+g)g',$$

where c is a scalar and $g(X) = \sum_{i=0}^{(p+1)/2} g_i X^i$ with $\alpha = g_{\frac{p+1}{2}} \neq 0$. If we replace X by $X+a$, then f changes to $f(X+a) = X^p + a + g(X+a)$, which has the same lacunarity type, but has coefficient of $X^{\frac{p-1}{2}}$ equal to zero if we choose $a = -2g_{\frac{p-1}{2}}/g_{\frac{p+1}{2}}$. So we can assume without loss of generality that $g_{\frac{p-1}{2}} = 0$.

We now have

$$X^p + \sum_{i=0}^{\frac{p+1}{2}} g_i X^i = c(X + \sum_{i=0}^{\frac{p+1}{2}} g_i X^i)(\sum_{i=0}^{\frac{p+1}{2}} i g_i X^{i-1})$$

Let $k < (p-1)/2$ be the largest index for which $\beta = g_k \neq 0$. Assume that $k > 1$; then equating the coefficients of $X^{k+\frac{p-1}{2}}$ we obtain: $0 = c(\alpha\beta)(k + \frac{p-1}{2})$. Since $c \neq 0$ and $\alpha \neq 0$ and $k < (p+1)/2$, then we would have $\beta = 0$, a contradiction. So $k = 1$ and

$$g(X) = \alpha X^{\frac{p+1}{2}} + \beta X + \gamma \ .$$

By comparing the coefficients of $X^{\frac{p-1}{2}}$ in the two sides of the equality $X^p + g = c(X+g)g'$ we obtain $\gamma = 0$. Hence, if $g^\circ = (p+1)/2$, then up to a linear transformation

$$f(X) = X^p + \alpha X^{\frac{p+1}{2}} + \beta X.$$

Theorem 2.2. *Let $f = X^q + g(X)$ be fully reducible in $GF(q)[X]$, where $q = p^h$, and let e be such that $f \in GF(q)[X^{p^e}] \setminus GF(q)[X^{p^{e+1}}]$. Then*
(i) $p^e = q$ and $f = (X+c)^q = X^q + c$, for some $c \in GF(q)$, or
(ii) $g = -X$ and $f = X^q - X$, or
(iii) $g^\circ \geq p^e \lceil \frac{q/p^e+1}{p^e+1} \rceil$.

Proof. Write $f = f_1^{p^e}$, so $f_1 = X^{q/p^e} + g_1$, with $g = g_1^{p^e}$. Again we write $f_1 = r(X)s(X)$, where s contains linear factors of f_1 exactly once, and r contains the repeated linear factors.

Note that, excluding the case in which $g = c$ is a constant and hence $e = h$ (giving (i)), we have $g_1' \neq 0$, because otherwise we would have $g \in GF(q)[X^{p^{e+1}}]$ and so $f \in GF(q)[X^{p^{e+1}}]$, which is not the case.

Now we have

$$\left.\begin{array}{c} s(X) | f - (X^q - X) \ = X + g \\ r(X) | f_1' = \ g_1' \neq 0 \end{array}\right\} \Longrightarrow \ f_1 | (X+g) g_1' \qquad (2)$$

Either $X + g = 0$, i.e. $g = -X$, giving (ii), or $f_1^\circ \leq g^\circ + g_1^\circ - 1$; the last case implies $q/p^e \leq g^\circ + g^\circ/p^e - 1$, and so

$$q/p^e + 1 \leq (\frac{p^e+1}{p^e}) g^\circ.$$

Since g°/p^e is an integer, we have that $\lceil \frac{q/p^e+1}{p^e+1} \rceil \leq g^\circ/p^e$ and finally

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

□

As in Theorem 2.1, if there is equality in Theorem 2.2 (iii) then the divisibility relation (4) becames an equality (up to scalaras), that is,

$$f_1 = X^{q/p^e} + g_1 = c(X+g)g_1' = c(X+g_1^{p^e})g_1',$$

for some scalar c. If we denote $t = p^e$ and replace g_1 by g, what can we say about the equation $X^{q/t} + g = (X+g^t)g'$? Let's look at the case $g' = 1$.

Lemma 2.1. If $X^{q/t} + g = X + g^t$ where $q = p^h$ and $t = p^e$, then $X^{q/t} + g = Tr_{q\to t}(X) = X + X^t + \ldots + X^{q/t}$ and $GF(t)$ is a subfield of $GF(q)$, i.e. $e|h$.

Proof. First note that $g^\circ = q/t^2$. Write $g = \sum_{i=0}^{q/t^2} g_i X^i$ and, equating coefficients, we obtain that $g_1 = 1$, $g_k = 0$, for $1 < k < t$, $g_t = 1$, and so on. That is, all non-zero coefficients are coefficients of terms of order t^i. However, $g_{q/t^2} = 1 \neq 0$, so there exists some positive integer i such that $q/t^2 = t^i$. Then, $q = t^{i+2} \;\Rightarrow\; p^h = p^{e(i+2)} \;\Rightarrow\; e|h$.

□

A general result in this direction is given in the following result whose proof can be found in Lemma 3.2 of [3].

Lemma 2.2. Let $X^{q/t} + g = (X+g^t)g'$, where $t = p^e > 1$. Then, either g' is constant, or

(1) for some $i > 0$, $g' \in GF(q)[X^{t^i}] \backslash GF(q)[X^{t^{i+1}}]$, and

(2) $\frac{q(t-1)}{t^{i+2}} \leq (g')^\circ \leq \frac{(t-1)(q-t^{i+1})}{t^{i+2}-t}$, and

(3) $g' = \eta\tau^{t-1}$, for some polynomials $\eta \in GF(q)[X^{t^{i+1}}]$ and $\tau \in GF(q)[X^{t^i}]$.

3 Number of Slopes of the Graph of a Function Defined on a Finite Field

Let f be a function $f : GF(q) \to GF(q)$. We want to find answers to the question: how few directions can be determined by a function f? Or in other words, how small can the set D be, where

$$D = \{\frac{f(x)-f(y)}{x-y} \mid x, y \in GF(q),\ x \neq y\}$$

Let us look at a couple of examples.

Example 3.1. If q is a square and $f(X) = X^{\sqrt{q}}$, then we have

$$\frac{f(x)-f(y)}{x-y} = \frac{x^{\sqrt{q}} - y^{\sqrt{q}}}{x-y} = \frac{(x-y)^{\sqrt{q}}}{x-y} = (x-y)^{\sqrt{q}-1},$$

and so $D = \{z^{\sqrt{q}-1} \mid z \in GF(q)^*\}$. Since $(z^{\sqrt{q}-1})^{\sqrt{q}+1} = z^{q-1} = 1$, we have that the elements in D are the solutions of the equation $X^{\sqrt{q}+1} = 1$ (roots of the unity), so we can conclude that $|D| = \sqrt{q}+1$.

Example 3.2. If q is even and $f(X) = Tr_{q\to 2}(X) = X + X^2 + X^4 + \ldots + X^{q/2}$, we have that $f(X)$ divides $X^q + X$, since $f^2 + f = X^q + X$ has $q/2$ different roots, and that $f(x) + f(y) = f(x+y)$. Then:

$$\frac{f(x)-f(y)}{x-y} = \frac{Tr_{q\to 2}(x+y)}{x+y}.$$

So we can write

$$D = \{\frac{Tr(z)}{z} \mid z \in GF(q)^*\} = \{0\} \cup \{\frac{Tr(z)}{z} \mid Tr(z) \neq 0\}.$$

But now, if we put $u = f(x) = Tr_{q\to 2}(x) = x + x^2 + x^4 + \ldots + x^{q/2}$, then $u^2 = x^2 + x^4 + \ldots + x^{q/2} + x^q = x^2 + x^4 + \ldots + x^{q/2} + x = u$. We have $u^2 = u$, and so $u \in GF(2) = \{0, 1\}$. Hence we can write

$$D = \{0\} \cup \{\frac{1}{z} \mid Tr(z) \neq 0\}.$$

Since the equation $Tr(z) = 0$ has $q/2$ different solutions, the number of elements z such that $Tr(z) \neq 0$ is also $q/2$, and so we have that $|D| = q/2 + 1$.

We want to find bounds for the value $N = |D|$, in the case of any function f.

Theorem 3.1. (Rédei) *Let f be a function $f : GF(q) \to GF(q)$ with $q = p^h$, and $U = \{(x, f(x)) \mid x \in GF(q)\}$. Let e be the largest integer such that each line (between two points of U) is incident with a multiple of p^e points of U. Then either*

1. *$e = 0$ and $(q + 3)/2 \leq N$;*
2. *$e > 0$ and*
$$p^e\lceil\frac{q/p^e + 1}{p^e + 1}\rceil + 1 \leq N \leq (q - 1)/(p^e - 1);$$
3. *f is linear, $e = h$ and $N = 1$.*

Proof. Consider the following polynomial in two variables:

$$R(X, Y) = \prod_{x\in GF(q)} (X + xY - f(x))$$

Let $c \in GF(q)$ and suppose that two of the linear factors in $R(X, c)$ are the same. That is, there exist $x, y \in GF(q)$ such that $x \neq y$ and $X + xc - f(x) = X + yc - f(y)$. Then $c = \frac{f(x)-f(y)}{x-y} \in D$.

On the other hand, if $c \notin D$, then all linear factors of $R(X, c)$ are different, and so $R(X, c) = X^q - X$. We now write

$$R(X, Y) = \sum_{j=0}^{q} h_j(Y)X^{q-j}$$

where h_j is a polynomial in Y of degree at most j (because the total degree of $R(X, Y)$ is q). In fact $h_j^\circ \leq j - 1$, for $1 \leq j \leq q - 2$, since the coefficient of Y^j in $h_j(Y)$ is the coefficient of X^{q-j} in

$$\prod_{x\in GF(q)} (X + xY) = X^q + XY^{q-1}.$$

Choose $c \notin D$. Then, $h_j(c) = 0$ for $1 \leq j \leq q - 1$. Since $h_j^\circ \leq j - 1$ for $1 \leq j \leq q - 2$ and there exist $q - N = |GF(q) \setminus D|$ different values of c such that $h_j(c) = 0$ we can conclude that $h_j \equiv 0$ when $j - 1 < q - N$. Hence,

$$R(X, Y) = X^q + h_{q-N+1}(Y)X^{N-1} + (\text{ lower order terms in } X).$$

Now choose $c \in D$. We have $R(X,c) = X^q + g(X)$, where $g^\circ \leq N-1$.

If $g(X) = -X$, then $R(X,c) = X^q - X \;\Rightarrow\; c \notin D$, a contradiction. So we have $g(X) \neq -X$. Put now $f(X) = R(X,c)$, and use Theorem 2.2. The required condition on the value e in Theorem 2.2 is implied by the geometric condition that is imposed on e in the current theorem. Statement (ii) of Theorem 2.2 does not hold, because $g(X) \neq -X$. Possibility (i) means that $R(X,c) = (X+\alpha)^q$. But $R(X,c) = \prod_{x \in GF(q)}(X + xc - f(x))$, so we conclude that $xc - f(x) = \alpha$, for all $x \in GF(q)$. Thus, $f(X) = cX - \alpha$ is a linear function, and it is easy to see that then $N = 1$, giving statement (3) of this theorem.

Possibility (iii) gives us

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

Note that, if $e = 0$, then we have $N - 1 \geq g^\circ \geq \frac{q+1}{2}$, and so $N \geq \frac{q+3}{2}$, giving us statement (1) of the theorem.

□

This theorem was subsequently improved to the following theorem in [3], with the exception of the cases $p^e = 2$ and 3. A proof of the following theorem which includes the cases $p^e = 2$ and 3 can be found in [1].

Theorem 3.2. [1] *Let f be a function $f : GF(q) \to GF(q)$ with $q = p^h$, and $U = \{(x, f(x)) \mid x \in GF(q)\}$. Let e be the largest integer such that each line (between two points of U) is incident with a multiple of p^e points of U. Then all the following statements hold;*

1. *$e = 0$ and $(q+3)/2 \leq N$;*
2. *$e > 0$, $e|h$ and $q/p^e + 1 \leq N \leq (q-1)/(p^e - 1)$;*
3. *f is linear, $e = h$ and $N = 1$.*

Moreover if $p^e > 2$ then the graph of f is $GF(p^e)$-linear.

Note that for many values c (those such that $c \notin D$), we have that $f(X) - cX$ is a permutation polynomial. That is, $f(X) - cX : GF(q) \to GF(q)$ is a permutation (bijective function) of the elements of $GF(q)$.

4 Blocking Sets

We start this section by explaining the basic notions of affine and projective planes. The *affine plane* over a finite field $GF(q)$ is defined as a set of points $\mathcal{P} = \{(x,y) \mid x, y \in GF(q)\}$, and a set of lines, which are defined as subsets of points that are solutions of linear equations. We denote these lines as

$$\ell_{c,d} := \{(x,y) \mid y = cx + d\}.$$

[1] Lecturer's note: It was my original intention to give a proof of the bounds in this theorem following the lacunary polynomial approach in [3]. However this turned out to be too time consuming. Fortunately I discovered a simpler proof using Hasse derivatives but only after the course had finished. This is the proof that appears in [1]. It should be possible to give a sketch that proof as well in any future course.

Furthermore, there are vertical lines $\ell_e := \{(e, y) \mid y \in GF(q)\}$. Each line contains q different points of $\mathcal{P}$. There are in all q^2 points and $q^2 + q$ lines. We denote this affine plane as $AG(2, q)$.

To complete this to the projective plane $PG(2, q)$ we must add points (c), where (c) is incident with all lines with direction c, i.e. $\ell_{c,d}$ for all $d \in GF(q)$. We must add also a point (∞) incident with all vertical lines ℓ_e, and the line $\ell_\infty = \{(c) \mid c \in GF(q)\} \cup \{(\infty)\}$. Now the number of points $|\mathcal{P}|$ is equal to the number of lines $|\mathcal{L}|$ which is equal to $q^2 + q + 1$, and each line contains $q + 1$ points. Moreover, the following properties are satisfied:

(P1) any two points are incident with a unique line,

(P2) any two lines are incident with a unique point,

(P3) there is a set of four points no three of which are collinear (in other words, there exists a *quadrangle*).

Any incident structure satisfying (P1), (P2) and (P3) is called a projective plane.

Definition 4.1. The *order* of a projective plane is the number of points on a line minus one. For example, the order of $PG(2, q)$ is q.

If q is a prime power, then as we have seen there exist projective planes of order q. It is not known whether there exist projective planes of non-prime power order.

Definition 4.2. A *blocking set* B in a projective plane Π is a set of points such that every line in Π is incident with some point in B.

Example 4.1. Let B be the set of points on a line. Then $|B| = q + 1$, and it is trivial to see that B is a blocking set.

Example 4.2. If D is the set of directions determined by a function f, as defined in Section 2, then

$$B = \{(x, f(x)) \mid x \in GF(q)\} \cup \{(c) \mid c \in D\}$$

is a blocking set of $q + N$ points. Indeed, if a line l of the affine plane $AG(2, q)$ is not incident with $B_1 = \{(x, f(x)) \mid x \in GF(q)\}$ then one of the $q - 1$ parallel lines to l must meet B_1 in at least two points and therefore its direction c is a point in B.

Definition 4.3. A *minimal blocking set* is a blocking set that contains no proper subset that is a blocking set.

Proposition 4.1. *Let B be a blocking set with $|B| = q + k$ such that B does not contain any line. Then every line is incident with at most k points of B.*

Proof. Assume that there exists a line ℓ incident with $k + 1$ points of B. Let P be a point of this line ℓ that is not in B (P exists because B does not contain any line). Now we know that there are $q + 1$ different lines incident with P, and that any of these lines must be also incident with a (different) point of B. So we have that line ℓ is incident with $k + 1$ different points of B, and each of the q other lines is incident with a different point of B. Therefore, $|B| \geq k + 1 + q$, a contradiction. □

Note that if there is a line ℓ such that $|\ell \cap B| = k$, then $|B| \geq q + k$.

Definition 4.4. If B is a minimal and non-trivial (it does not contain any line) blocking set of size $q+k$ such that there is a line incident with k points of B, then B is called a *Rédei blocking set*.

Any Rédei blocking set can be constructed from the graph of a function.

Example 4.3. Let q be odd and B the Rédei blocking set associated to the function $f(x) = x^{\frac{q+1}{2}}$, that is,

$$B = \{(x, x^{\frac{q+1}{2}}) \mid x \in GF(q)\} \cup \{(\pm 1)\} \cup \{(\frac{1+x}{1-x}) \mid x \text{ not an square}\}.$$

Then $|B| = q + 2 + (q-1)/2 = 3(q+1)/2$.

Example 4.4. $GF(q_1)$ a subfield of $GF(q)$. Define $B = \{(x, Tr_{q \to q_1}(x)) \mid x \in GF(q)\} \cup \{(c) \ / \ c \in D\}$.

Then $|B| = q + q/q_1 + 1$ (applying some techniques similar to those in Example 3.2). Note that if q is a square, taking $q_1 = \sqrt{q}$, we obtain $|B| = q + \sqrt{q} + 1$.

Theorem 4.1. (Bruen [5]) *If B is a blocking set, not containing a line, in a projective plane of order q, then $|B| \geq q + \sqrt{q} + 1$.*

Proof. If there is a line incident with more than $\sqrt{q}+1$ points of B, then Proposition 4.1 is enough. Otherwise, we can write $|B| = q + k + 1$ (we want to see $k \geq \sqrt{q}$), and let $\tau_i = |\{\text{lines incident with exactly } i \text{ points of } B\}|$. Then we have:

$$\sum_{i=0}^{k+1} \tau_i = q^2 + q + 1 \tag{3}$$

$$\sum_{i=0}^{k+1} (k+1-i)(i-1)\tau_i \geq 0 \tag{4}$$

Inequality 4 holds because all terms of the sum are greater or equal to 0 (note that $\tau_0 = 0$, by the definition of a blocking set).

Now we consider pairs (P, ℓ) such that $P \in B$ is incident with line ℓ, and count these pairs in two different ways, obtaining

$$|B|(q+1) = \sum_{i=0}^{k+1} i\tau_i \tag{5}$$

Finally, if we count in two different ways the number of triples (P, Q, ℓ) such that $P, Q \in B$, $P \neq Q$ and P, Q incident with line ℓ, we obtain

$$|B|(|B|-1) = \sum_{i=0}^{k+1} i(i-1)\tau_i \tag{6}$$

Then, combining equations (3), (4), (5) and (6), it is easy to deduce that $k \geq \sqrt{q}$.

□

Theorem 4.2. (Blokhuis [2]) *Let p be a prime and B a blocking set in $PG(2,p)$ not containing a line. Then $|B| \geq \frac{3(p+1)}{2}$.*

Proof. Let $|B| = p + k + 1$. We can assume that ℓ_∞ is a tangent of B and that the point of B incident with ℓ_∞ is the point (∞). Then $B \backslash \ell_\infty \subset AG(2, p)$ and $|B \backslash \ell_\infty| = p + k$. Now the p^2 lines defined by $Y = -yX - x$, where $x, y \in GF(p)$, are the p^2 lines not incident with (∞). We define

$$R(X, Y) = \prod_{(a,b) \in B \backslash \ell_\infty} (X + aY + b)$$

Now, for all $x, y \in GF(p)$, there exists a point $(a, b) \in B \backslash \ell_\infty$ such that the line $Y = -yX - x$ is incident with point (a, b). That is, $b = -ya - x$ and so $x + ay + b = 0$, which implies $R(x, y) = 0$. So $R(X, Y) \in GF(p)[X, Y]$ and $R(x, y) = 0$ for all $(x, y) \in GF(p)^2$. This implies that there exist $G, H \in GF(p)[X, Y]$ such that

$$R(X, Y) = (X^p - X)G(X, Y) + (Y^p - Y)H(X, Y).$$

Note that $G^\circ = k$ and $H^\circ \leq k$. Now we consider $\bar{R}(X, Y) = \prod(X + aY) = X^p \bar{G} + Y^p \bar{H}$, where $\bar{G}$, $\bar{H}$, $\bar{R}$ are the homogeneous parts of G, H, R of highest degree. If we put $Y = 1$, we obtain $\prod(X + a) = X^p g + h = f$, with $f(X) = \bar{R}(X, 1)$, $g = \bar{G}(X, 1)$ and $h = \bar{H}(X, 1)$. Note again that $g^\circ = k$ and $h^\circ \leq k$, and f is fully reducible over $GF(p)$.

We split up $f = rs$, where $s(X)$ contains all the linear factors of f exactly once, and $r(X)$ the repeated linear factors. Now s divides $X^p - X$ and f and so s divides $f - (X^p - X)g = Xg + h$. The polynomial r divides f and f' and hence divides $f'g - g'f = h'g - g'h$. Therefore

$$f \mid (Xg + h)(h'g - g'h).$$

Now $Xg \neq h$ since $g^\circ = k \geq h^\circ$.

If $h'g - g'h \neq 0$ then comparing degrees in this divisibility implies $p + k \leq k + 1 + 2k - 2$. Note that the coefficients of the term of degree $2k - 1$ in $h'g$ and $g'h$ are the same and so the degree of $h'g - g'h$ is at most $2k - 2$. Hence $k \geq (p + 1)/2$ and $|B| \geq 3(p + 1)/2$.

If $h'g - g'h = 0$ then $(gh^{p-1})' = 0$. Let m be the largest common factor of g and h, $(g, h) = m$ and write $g = mg_1$ and $h = mh_1$ so that $(g_1, h_1) = 1$. Then $(g_1 h_1^{p-1})' = 0$ and so $g_1 h_1^{p-1}$ is a p-th power and since h_1 and g_1 have no common factors they are p-th powers themselves. If g_1° or h_1° are not zero then they are at least p and we have that $k \geq p$ and $|B| \geq 2p + 1$. If not, then g_1 and h_1 are both constant and

$$f = m(X^p g_1 + h_1) = m(Xg_1 + h_1)^p.$$

Let $a = h_1/g_1 \in GF(p)$. Then $X + a$ occurs p times as a factor of f and by the definition of f this implies that the blocking set has p points incident with the line $X = a$. Hence either B contains this line or $|B| \geq 2p + 1$. □

5 Recent Results on the Number of Directions and Blocking Sets

Summing up the results that we have seen until now, any non-linear function $f : GF(q) \rightarrow GF(q)$, with q prime, determines at least $\frac{q+3}{2}$ directions. And

the bound is tight, since the function $f(X) = X^{\frac{q+1}{2}}$ determines exactly $\frac{q+3}{2}$ directions.

Theorem 5.1. (Lovász and Schrijver [7]) *Any function that determines $\frac{q+3}{2}$ directions, where q is prime, is affinely equivalent to $X^{\frac{q+1}{2}}$.*

Proof. (idea) We define, for a function f determining $\frac{q+3}{2}$ directions,

$$F(X,Y) = \prod_{x \in GF(q)} (X + xY - f(x))$$

Then, for $c \in D$, we have $R(X,c) = X^q + g(X)$, where $g^\circ = \frac{q+1}{2}$. But as a corollary of Theorem 2.1, we showed that any fully reducible lacunary polynomial of the form $X^q + g(X)$, with $g^\circ = \frac{q+1}{2}$, is equivalent, up to transformations $X \mapsto X + a$, to $X^q \pm 2X^{\frac{q+1}{2}} + 1$ or to $X^q \pm X^{\frac{q+1}{2}}$.

With some algebraic work we get that f is affinely equivalent to $X^{\frac{q+1}{2}}$.

□

Before returning to blocking sets, we state a "number theory" theorem:

Theorem 5.2. (Kneser's theorem[9]) *Let G be an Abelian group, and let A, B be finite non-empty subsets of G. Denote by $A+B = \{a+b \mid a \in A,\ b \in B\}$, and let $H = \{g \in G \mid g + A + B = A + B\}$.*

Then H is a subgroup of G, and if $|A + B| < |A| + |B|$, then $|A + B| = |A + H| + |B + H| - |H|$.

Now we consider $GF(q)^* = \{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{q-2}\}$, where ε is a primitive element of $GF(q)$. $GF(q)^*$ is an Abelian group (with multiplication).

Let U be a minimal blocking set contained in 3 non-concurrent lines. We can choose these lines to be the x-axis ℓ_x, the y-axis ℓ_y and ℓ_∞. If U does not contain a line, then the points $(0,0)$, (0) and (∞) belong to U. We define the following sets:

$$A = \{a \mid (0, \varepsilon^a) \notin U\} \qquad W_A = \{(0, \varepsilon^a) \mid a \in A\}$$

$$B = \{b \mid (\varepsilon^{-b}, 0) \notin U\} \qquad W_B = \{(\varepsilon^{-b}, 0) \mid b \in B\}$$

Then $W_A = \ell_y \backslash U$ and $W_B = \ell_x \backslash U$.

The direction of a line joining a point of W_A and a point of W_B is $\frac{\varepsilon^a}{\varepsilon^{-b}} = \varepsilon^{a+b}$, for some $a \in A$, $b \in B$. Hence if we have $c \in A + B$ the point (c) must be in the blocking set U. Now we define the sets:

$$W_C = \{(\varepsilon^g) \mid g \notin A + B\} \qquad C = \{c \mid (\varepsilon^c) \in W_C\}$$

Then by the minimality of U we have that $U = (\ell_\infty \cup \ell_x \cup \ell_y) \backslash (W_A \cup W_B \cup W_C)$ and $|U| = 3q - |A| - |B| - |C|$, where $|C| = |W_C| = |GF(q)^*| - |A + B| = q - 1 - |A + B|$, so $|U| = 2q + 1 - |A| - |B| + |A + B|$.

If $|A + B| \geq |A| + |B|$, then $|U| \geq 2q + 1$ (very large!).

Otherwise, replace A by $A + H$ and B by $B + H$, where H is defined as in Theorem 5.2 (then U possibly becomes smaller, but U is minimal). Then we have $|U| = 2q+1-|A+H|-|B+H|-|A+B|$ (remember that $A+B+H = A+B$). We can apply Theorem 5.2 and conclude that $|U| = 2q + 1 - |H|$, where H is a subgroup of $GF(q)^*$ (and so, $|H| = d$, for some $d|q-1$). This result was proved by Szőnyi:

Theorem 5.3. (Szőnyi [12]) *Every minimal blocking set U of size less than $2q+1$ contained in 3 non-concurrent lines satisfies $|U| = 2q+1-d$, for some $d|q-1$.*

Note that the above also constructs a minimal blocking set of size $2q+1-d$ contained in the union of three lines, for all $d|q-1$; take H to be a subgroup of $GF(q)^*$ and $A = B = H$, so that $C = GF(q)^* \setminus H$ and $|U| = 3 + 2(q-1-|H|) + |H|$.

Theorem 5.4. (Gács [6]) *If $f: GF(q) \to GF(q)$, with q prime, determines more than $\frac{q+3}{2}$ directions, then it determines at least $\lceil \frac{2(q-1)}{3} \rceil + 1$ directions.*

This bound is almost tight, there are examples for $q = 1 \mod 3$, of functions that determine $\frac{2q+1}{3} + 1$ directions.

Proof. (idea) It is complicated but the idea is to show that functions determining less than $\lceil \frac{2(q-1)}{3} \rceil + 1$ directions are affinely equivalent to a function f satisfying $f^2(X) = (aX+b)^2$, for some $a, b \in GF(q)$.

Then one sees that the graph $\{(x, f(x)) \mid x \in GF(q)\}$ is contained in the union of two lines $(f(x) - ax - b)(f(x) + ax + b) = 0$.

Then we can construct a blocking set by adding the determined directions on ℓ_∞. This blocking set is contained in the union of three lines and the result follows by applying Theorem 5.3.

□

Let us return to blocking sets. The following theorem summarizes some known bounds on the cardinality of blocking sets.

Theorem 5.5. *If B is a blocking set of $PG(2,q)$ not containing a line. Then one of the following statements hold:*
(i) q is prime and $|B| \geq \frac{3(q+1)}{2}$.
(ii) q is a square and $|B| \geq q + \sqrt{q} + 1$.
(iii) $q = p^{2d+1}$ and $|B| \geq q + \sqrt{pq} + 2$.

All examples we have seen where $|B| \leq \frac{3(q+1)}{2}$ have been of Rédei type, i.e. $|B| = q + k$, where there exists a line incident with k points of B. But there exist many other blocking sets of size less than $\frac{3(q+1)}{2}$. These come from the following construction proposed by Lunardon [8] and Polito and Polverino [10].

Let V be a vector space of dimension 3 over $GF(q)$. $PG(2,q)$ is the point-line incidence structure where: points are the subspaces of V of dimension 1, and lines are the subspaces of V of dimension 2. If $q = p^t$, for some prime p and some integer t, we have that V can be viewed as a vector space of dimension $3t$ over $GF(q)$.

Let $\mathcal{P}$ be the set of points of $PG(2,q)$. Then $P \in \mathcal{P}$ corresponds to a t-dimensional subspace $\bar{P}$ of this vector space, and $\forall P, Q \in \mathcal{P}$, we have $\bar{P} \cap \bar{Q} = \{\underline{O}\}$.

Lines of $PG(2,q)$ are $2t$-dimensional subspaces of V spanned by two points of $PG(2,q)$. Let U be a $(t+1)$-dimensional subspace, and define

$$B_U = \{P \in \mathcal{P} \ / \ \bar{P} \cap U \neq \{\underline{0}\}\}$$

Then B_U is a blocking set that satisfies:

$$|B_U| \leq \frac{p^{t+1}-1}{p-1} = p^t + p^{t-1} + \ldots + 1 = q + \frac{p^t - 1}{p-1} = q + \frac{q-1}{p-1}$$

It was shown by Polito and Polverino in [10] that if $t \geq 4$ it is possible to choose U so that B_U is not of Rédei type.

Conjecture 5.1. *All blocking sets of size less than* $\frac{3(q+1)}{2}$ *come from this construction of Polito, Polverino and Lunardon.*

Theorem 5.6. (Szőnyi [13]) *If a minimal blocking set* B *satisfies* $|B| < \frac{3(q+1)}{2}$ *and* $q = p^h$ *with* $p \geq 5$*, then every line is incident with* $1 \mod p$ *points of* B*.*

This is Theorem 5.5 in Section 5 of [4] and the proof can be found there.

References

[1] S. Ball, The number of directions determined by a function over a finite field, `http://www.maths.qmw.ac.uk/~simeon/listofpapers.html`

[2] A. Blokhuis, On the size of a blocking set in $PG(2,p)$, *Combinatorica*, **14** (1), (1994), 111–114.

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

[4] A. Blokhuis and S. Ball, Polynomials in finite geometry, *Methods of Discrete Mathematics*, Quaderni di mathematica, Napoli, **5**, 71–101 (1999).

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

[6] A. Gács, On a generalization of Rédei's theorem, *Combinatorica*, to appear.

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

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

[9] M. B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Springer-Verlag, 1996.

[10] P. Polito and O. Polverino, On small blocking sets, *Combinatorica*, **18**, (1998), 133–137.

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

[12] T. Szőnyi, Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica*, **19** (1991), 91–100.

[13] T. Szőnyi, Blocking Sets in Desarguesian Affine and Projective Planes, *Finite Fields Appl.*, **3**, (1997), 187–202.