Polynomials in Finite Geometry

Aart Blokhuis and Simeon Ball

23 May 1999

Abstract

These are the notes for the summer course on Polynomials in Finite Geometry, Braunschweig, May 23 - 29, 1999.

1 Introduction

In 1978 it was conjectured by van Lint and MacWilliams [24], that for q odd, the only q-subset X of $GF(q^2)$, containing 0 and 1, and with the property that $x-y$ is a square for all pairs $x, y \in X$, is the set $GF(q)$. They noted that for q prime this is a consequence of a theorem of Rédei on the number of directions determined by a function defined over a finite field. This theorem [26, p.237, Satz 24'] is one of the applications of his theory of lacunary polynomials. The same theorem on the number of directions was used by Bruen [15], and later by Brouwer and myself [8], to improve the lower bounds for *blocking sets* in desarguesian projective planes, and it became clear that much more could be said about these objects, but in order to do that one should understand completely, and improve, Rédei's results. This took and will take a long time however, but I believe it is possible.

In 1975, Bruen and Thas proved the following result [17]:

Let C be a conic in $PG(2,q)$, q even, and let B be a set of $q+1$ points such that the line joining any two misses C. Then B is an exterior line of the C.

In [27] Segre and Korchmáros proved the same result for odd q. Both results were generalized using the concept of a *nucleus*. If B is a set of $q+1$ points in $PG(2,q)$ then a point $P \notin B$ is called a nucleus of B if every line through P contains exactly one point of B. It was shown in [12] that unless B is a line, the number of nuclei is at most $q-1$. The proof and also the concept of nucleus was later generalized in all possible directions, connecting the problem with affine blocking sets, and even maximal arcs.

A (k,n)-arc (in $PG(2,q)$) is a set A of k points, such that each line intersects A in at most n points. An upper bound for the size k is $k \leq 1+(q+1)(n-1)$ and in the case of equality we call A a *maximal arc*. It was a very old conjecture that maximal arcs do not exist if q is odd, and we will give the complete proof of this conjecture (at least for the desarguesian plane).

2 Lacunary polynomials

Let K be a (commutative) field. A polynomial $f \in K[X]$ is said to be *fully reducible* if K is a splitting field for f, or in other words, if f factors completely into linear factors in $K[X]$. Let f° and $f^{\circ\circ}$ denote respectively the degree and the second degree of f. The second degree of f is the degree of the polynomial we obtain if we remove the leading term. The problem we (and Rédei) are interested in is what can be said about the pair $(f^\circ, f^{\circ\circ})$ if f is fully reducible. If $f^{\circ\circ} < f^\circ - 1$ we say that f is *lacunary*, and we call the pair $(f^\circ, f^{\circ\circ})$ the lacunarity type. If $K = \mathbf{C}$ (or any other algebraically closed field), then all lacunarity types are possible, since all polynomials in $\mathbf{C}[X]$ are fully reducible. The case $K = \mathbf{R}$ is only slightly more interesting. In this case $f^\circ - f^{\circ\circ} \leq 2$ or $f(X) = cX^{f^\circ}$. We leave the investigation of this problem for the possible extensions of $\mathbf{Q}$ to the interested reader, and go immediately to the case that really interests us: $K = GF(q)$, the finite field with q elements. So $q = p^h$ for some prime p, and some integer $h0$.

Let us first give some examples of polynomials with small second degree. If $d \,|\, q-1$, then $K = GF(q)$ contains the d-th roots of unity, so the polynomial

$$f(X) = X^d - a^d$$

is fully reducible for all $a \in K$. We will be particularly interested in the case $f^\circ = q$, and using the above with $d = q-1$ and $d = (q-1)/2$ we get the important examples

$$f(X) = X^q - X = X(X^{q-1} - 1) = \prod_{a \in K} (X - a),$$

$$f(X) = X^q \pm X^{(q+1)/2} = X^{(q+1)/2}(X^{(q-1)/2} \pm 1)$$

and finally

$$f(X) = X^q \pm 2X^{(q+1)/2} + X = X(X^{(q-1)/2} \pm 1)^2.$$

Obviously q must be odd in the last two cases.

As a warm up we prove the following result

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 prime. Then either g is constant, or $g = -X$ or g° (and hence $f^{\circ\circ}$) is at least $(p+1)/2$.*

Before proving this we first recall some basic properties of polynomials. Let $f(X) \in K[X]$, with $\mathrm{char}(K) = p$. If

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n,$$

then the (formal) derivative of f is given by

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

So $f' = 0$ implies that $f(X) \in K[X^p]$ (and conversely). If a is a (possibly more than) k-fold root of f (that is $(x-a)^k$ divides f), then a is a $(k-1)$-fold root of f', and even a k-fold root if p divides k (everything is a k-fold root of the zero polynomial for all k). Note that in our case, $f = X^p + g$, we have $f' = g'$.

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 $s = (f, X^p - X)$, where we use $(,)$ to denote the greatest common divisor. In particular $s \mid f - (X^p - X) = X + g$.
We may write $f = s.r$ for some fully reducible polynomial r and r divides the derivative $f' = g'$. So we conclude that

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

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 (if $g^\circ < p$) 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 $g^\circ \geq (p+1)/2$.

□

As we see from the examples the result is sharp. In fact the proof also gives us enough information about the case that $g^\circ = (p+1)/2$ to classify the examples. In order to avoid trivialities assume $p > 3$. Since $s \mid X + g$ and $r \mid g'$, and $s^\circ + r^\circ = (X + g)^\circ + (g')^\circ$ we must have $s = c_1(X + g)$ and $r = c_2 g'$ for certain constants c_1 and c_2. As a result we get the following differential equation:

$$f(X) = X^p + g = c(X + g)g'.$$

Let $g = \sum g_i X^i$, so $\alpha := g_{(p+1)/2} \neq 0$. If we replace the variable X by $X + a$ for a suitable $a \in K$ then f changes to $f(X + a) = X^p + a + g(X + a)$ which has the same lacunarity type, but has no term $X^{(p-1)/2}$. So we may put $g_{(p-1)/2} = 0$ without loss of generality. Let $k < (p-1)/2$ be the largest index for which $\beta = g_k \neq 0$. If $k \neq 1$ then equating the coefficient of $x^{k+(p-1)/2}$ gives

$$c(\frac{p+1}{2} + k)\alpha\beta = 0,$$

a contradiction. So $k = 1$ and

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

Comparing the coefficient of $x^{(p-1)/2}$ gives $\gamma = 0$, so that

$$g + X = \alpha X^{(p+1)/2}, \quad g' = \frac{1}{2}\alpha X^{(p-1)/2} + \beta.$$

Since both are fully reducible polynomials it now readily follows that we have one of the examples given before.
Most of the analysis so far can be carried out if we replace p be a prime power q. The conclusion from $g' = 0$ is now that $g \in K[X^p]$

Theorem 2.2 *Let $f(X) = X^q + g(X)$ be fully reducible in $K[X]$, $K = GF(q)$. Then either $g \in K[X^p]$, or $g = -X$ or g° (and hence $f^{\circ\circ}$) is at least $(q+1)/2$.*

The analysis of the case $g^\circ = (q+1)/2$ in this case is much more involved, in fact it basically takes up the first 200 pages of Rédei's book [26]. For the applications in finite geometry however it turns out that a closer investigation of the case $g \in K[X^p]$ is much more important.

Again we start with the original theorem (and proof) by Rédei.

Theorem 2.3 *Let $f(X) = X^q + g(X)$ be fully reducible in $K[X^{p^e}] \setminus K[X^{p^{e+1}}]$, $K = GF(q)$, $p^e < q$. Then*

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

Proof Write $f = f_1^{p^e}$, with $f_1 = X^{q/p^e} + g_1$ and $f_1' = g_1' \neq 0$. We write as before $f_1 = s_1.r_1$ with s_1 the zeroes polynomial of f_1 (and of f). As before $s_1 \mid X + g$ and $r_1 \mid g_1'$. Hence

$$f_1 \mid (X + g)g_1'$$

and comparing degrees (the right hand side cannot be zero in this case) we get

$$q/p^e \leq p^e g_1^\circ + g_1^\circ - 1,$$

from which the result follows.

□

3 Directions

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 be concerned with the following problem. Let R be a set of q points in A. How many directions are determined by the pairs of points in R?

The q in this problem is there for two reasons. In Rédei's original formulation of the problem R is the graph of a function f, so the directions determined by R are exactly the difference quotients of the function f. Second, 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.

With a point set S in Π we associate it's *Rédei Polynomial*:

$$r_S(U, V, W) = \prod_{(a:b:c)\in S} (aU + bV + cW).$$

Strictly speaking r_S is not a polynomial, since it is only defined up to a scalar multiple. Note that r_S is just the product of the equations of the points in S, and that $r_S(u, v, w) = 0$ precisely when the line $[u : v : w]$ intersects S.

For our affine set R we obtain the 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

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

This polynomial (with different names for and order of the variables) is called the Rédei polynomial of the (affine) set R in [9].

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

Write

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

So h_j is a polynomial of 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 $j = 1, 2, \ldots, q-2, q$. Since h_j is a polynomial of degree at most j and vanishes for $q + 1 - N$ values of 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 [26, Satz 24] or [9, Theorem 1])

Theorem 3.1 *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, $1 \leq e \leq [n/2]$.*

4 Blocking Sets

In the previous section we saw some intervals for the possible number of directions that an affine set of size q in $AG(2, q)$ can determine. We will now give some examples to show that these results are quite reasonable. The examples will be of the form $R = R_f = \{(a, f(a)) \,|\, a \in GF(q)\}$.

Example 4.1 *Let $f(X) = X^{(q+1)/2}$. Note that $f(x) = \pm x$ depending on whether x is a square or not. The $(q+3)/2$ directions determined by the graph of f are (± 1) and (m) for m in the set*

$$\{\frac{1+z}{1-z} \,:\, z \textit{not a square}\}.$$

The examples with fewer than $(q+3)/2$ directions all are of a very special form. In the next two examples we assume $q = q_1^d$, so $GF(q_1)$ is a subfield of $GF(q)$ (and $(q_1 - 1) \,|\, (q-1)$). The affine plane $AG(2, q)$ carries in a natural way the structure of a $2d$ dimensional affine space over $GF(q_1)$. All our examples appear as d-dimensional subspaces. Later we will see that this is true for essentially all examples.

Example 4.2 *Let $f(X) = X^{q_1}$, Since*

$$\frac{x^{q_1} - y^{q_1}}{x - y} = (x - y)^{q_1 - 1},$$

the directions determined by the graph of f are given by the $(q-1)/(q_1-1)$ different (q_1-1)-st powers in $GF(q)^*$.

Example 4.3 *Let $f(X) = X + X^{q_1} + X^{{q_1}^2} + \ldots + X^{q/q_1} = \mathrm{Tr}_{q \to q_1}(X)$. The trace function is $GF(q_1)$-linear, so the directions are given by the set*

$$\{\frac{\mathrm{Tr}(z)}{z} \ : \ z \in GF(q)\}$$

and since every nonzero value occurs exactly $q_1 - 1$ times, while 0 occurs q/q_1 times we see that the number of directions equals

$$1 + \frac{(q - q/q_1)}{q_1 - 1} = \frac{q}{q_1} + 1.$$

Now we will concentrate on another important property. If we consider the set $B = R \cup D(R)$, so the set R together with the directions determined by R then we notice that every line of the (projective) plane intersects B. Indeed, if the intersection of a 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 we are especially 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 will be called *trivial*. Any set containing a blocking set is itself a blocking set, and 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. Equivalently, for every point in the blocking set there is a line meeting the blocking set in that point only.
Bruen [15] gave the general lower bound $q + \sqrt{q} + 1$ for the size of a non-trivial blocking set in any (so not necessarily desarguesian) plane of order q, and this result is best possible if q is a square. In case of equality the blocking set must consist of the points of a Baer subplane. Several improvements of this bound in the case that q is not a square (and the plane is desarguesian) were obtained using a mixture of combinatorial and geometrical arguments, together with Rédei's theorem [13, 8] but the real improvements came from generalizations of Rédei's lemma on lacunary polynomials.

So let us consider the Rédei polynomial of a blocking set B (in $PG(2, q)$):

$$r_B = \prod_{(a:b:c) \in B} (aU + bV + cW)$$

Since B intersects all lines $r_B(u,v,w) = 0$ for all $u,v,w \in GF(q)$. This implies that r_B is in the ideal generated by the three polynomials $U^q - U$, $V^q - V$ and $W^q - W$. We may write, with $r_i = r_i(U,V,W)$ a polynomial of degree $\leq |B| - q$

$$r_B = r_1(U^q - U) + r_2(V^q - V) + r_3(W^q - W)$$

To make the subsequent analysis easier to follow we reduce the situation to a one-variable problem as follows: Write $|B| = q + k + 1$, 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 points $(a,b) = (a:b:1)$ of B so the polynomial

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

of degree $q + k$ vanishes for all $v, w \in GF(q)$. Let us 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

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

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 $GF(q)[W]$. 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 4.4 *Let $f \in GF(q)[X]$ 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 $a \in GF(q)^*$, 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 $k \geq p^{e+1}$.*

Proof We only consider the case q prime. The general case is only slightly more involved. So again we write $f = s.r$ where s is the zeros polynomial of

f and r is the rest. As before we get $s|Xg+h$ and for r we may combine the divisibility relations $r|f' = x^q g' + h'$ and $r|f = x^q g + h$ to get

$$r|h'g - g'h.$$

Together this yields

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

Now if $Xg+h=0$ then $k=1$, since $(g,h)=1$ and f has the desired form. If $h'g-g'h=0$ and $(g,h)=1$ then g and h are constant, so $k=0$. Finally if neither of them are 0, then comparing the degrees we get

$$q+k \leq k+1+2k-2,$$

which gives the desired conclusion.

□

As a direct consequence of this we get that a non-trivial blocking set in a plane of prime order p has at least $\frac{3}{2}(p+1)$ points, a bound conjectured in [23] and proved in [5].

For Desarguesian planes of non-prime order we recover Bruen's result in the case that q is a square, and if $q=p^{2e+1}$ we obtain the bound $|B| \geq q+p^{e+1}+1$; a result that is only sharp in the case $e=1$.

In the next section we will see how a more careful analysis of the Rédei polynomial leads to sharper bounds and more insight into the structure of small blocking sets.

5 Small blocking sets

In the previous section we saw that a non-trivial blocking set in a plane of prime order q has at least $\frac{3}{2}(q+1)$ points. For non prime q we also saw smaller examples coming from a subfield $GF(q_1)$ having $q+q/q_1+1$ and $q+(q-1)/(q_1-1)$ points respectively. Let us call a blocking set *small* if it has less than $\frac{3}{2}(q+1)$ points. The examples of small blocking sets we have seen all were of Rédei type, and all have the property that each line intersects them in 1 mod q_1 points, where q_1 is the order of a subfield of $GF(q)$. For a long time I was convinced that small blocking sets were necessarily of Rédei type, but a nice geometrical construction by Polito and Polverino [21, 25, 6] showed that for $q=p^n$ with $n \geq 4$ this is no longer true. Another conjecture, namely that a small (minimal) blocking set is intersected by all lines in 1 mod p points turned out to be true however. Here we will copy the nice proof by Támas Szőnyi [28].

As before we take $|B| = q+k+1 (< 2q)$, $(1:0:0) \in B$, the line $Z=0$ a tangent. Moreover we assume that the line $Y=0$ is a tangent. The polynomial

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

of degree $q+k$ vanishes for all $v, w \in GF(q)$. So

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

where G and H are of total degree (at most) k in the variables V and W. For fixed $W = w \in GF(q)$ the polynomial $F(V,w)$ equals

$$(V^q - V)G(V,w) = \prod_{(a,b)\in B} (a + bV + w).$$

It follows that for $(v,w) \in GF(q) \times GF(q)$, $G(v,w) = 0$ if and only if the line with equation $X + vY + w = 0$ intersects the affine part of B in at least two points. We may repeat this reasoning for $V = v$, so we obtain

Lemma 5.1 *For $v, w \in GF(q)$, $G(v,w) = 0$ if and only if $H(v,w) = 0$.*

Now any common factor of G and H is a factor of F, and hence is a product of linear factors of the form $a + bV + W$, for some $(a,b) \in B$. But such a factor would imply that every line containing the point (a,b) contains at least two points of B, contradicting the assumption that B is minimal. So we proved

Lemma 5.2 *The polynomials G and H do not have a common factor.*

The previous two lemmas 5.1 and 5.2 can be used to show that all the components of H have identically zero partial derivative with respect to W if the blocking set is small. Before doing this, recall a lower bound on the number of GF(q)-rational points of some components of H, see Blokhuis, Pellikaan, Szőnyi [10]

Lemma 5.3 *(1) The sum of the intersection multiplicities $I(P, H \cap v_P)$ over all GF(q)-rational points of H is exactly qk, where v_P denotes the vertical line through P. If h divides H, then the corresponding sum for h is precisely $q \deg(h)$. (2) Let $h(V,W)$ be a divisor of $H(V,W)$ and suppose that it has neither multiple components nor components with zero partial derivative with respect to W. Then the number of GF(q)-rational points of h is at least*

$$qs - s(s-1),$$

where s denotes the total degree of h.

Proof For any fixed $V = v$ the polynomial $H(v,W)$ is the product of linear factors over GF(q), hence the same is true for every divisor of H. So the number of points, counted with the intersection multiplicity of H and the vertical line at that point, is exactly qs. To get the number of points without this multiplicity we have to subtract the number of affine intersections of h and h'_W (see [10]). Bézout's theorem then gives the result.

□

Note that for any component h of H the total degree of h is the same as its degree in W.

Theorem 5.4 *If $k < (q+1)/2$ and $h(V,W)$ is an irreducible polynomial that divides $f(V,W)$, then $h'_W = 0$.*

Proof Suppose to the contrary that h is a component with nonzero partial derivative. Denote its degree by s. By Lemma 5.3 the number of GF(q)-rational points on h is at least $qs - s(s-1)$. Since these points are also on G, Bézout's theorem gives

$$qs - s(s-1) \leq sk,$$

since by Lemma 5.2, G and h cannot have a common component. This immediately implies $q + 1 \leq k + s$ and from $s \leq k$ it follows that $k \geq (q+1)/2$, a contradiction.

□

Theorem 5.5 *If B is a blocking set of size less than $3(q+1)/2$, then each line intersects it in 1 modulo p points.*

Proof Since all the components of H contain only terms of exponent (in W) divisible by p, for any fixed $V = v$ the polynomial $H(v,W)$ itself is the p-th power of a polynomial. This means that at each point (v,w) the line $V = v$ intersects $H(V,W)$ with multiplicity divisible by p, so the line $[1 : v : w]$ with equation $X + vY + wZ = 0$ intersects B in 1 modulo p points.

□

6 Further results and recent developments

We have seen how comparatively easy arguments using lacunary polynomials severely restricted the possible number of directions determined by a set of q points in $AG(2,q)$. In [7] the analysis is carried out further, but the details are to tedious to be incorporated in a course like this. The final theorem however almost characterizes the q-sets determining less that $(q+3)/2$ directions:

Theorem 6.1 *Let $R \subset AG(2,p^n)$ be a point set of size $q = p^n$ containing the origin, let D be the set of directions determined by R, and put $N := |D|$. Let e (with $0 \leq e \leq n$) be the largest integer such that each line with slope in D meets U in a multiple of p^e points. Then we have one of the following:*

(i) *$e = 0$ and $(q+3)/2 \leq N \leq q+1$,*

(ii) *$e = 1$, $p = 2$, and $(q+5)/3 \leq N \leq q-1$,*

(iii) *$p^e 2$, $e \mid n$, and $q/p^e + 1 \leq N \leq (q-1)/(p^e - 1)$,*

(iv) *$e = n$ and $N = 1$.*

Moreover, if $p^e > 3$ or ($p^e = 3$ and $N = q/3 + 1$), then R is $GF(p^e)$-linear, and all possibilities for N can be determined explicitly (in principle).

We saw Szőnyi's proof [28] that small blocking sets are intersected by each line in 1 mod p points, in fact his result is much more specific, giving bounds for the possible sizes of small blocking sets:

Theorem 6.2 *Let B be a minimal blocking set in $PG(2, q)$, $q = p^n$. Suppose that $|B| < 3(q + 1)/2$. Then*

$$q + 1 + \frac{q}{p^e + 2} \leq |B| \leq \frac{qp^e + 1 - \sqrt{(qp^e + 1)^2 - 4q^2p^e}}{2},$$

for some integer e, $1 \leq e$. The right hand side asymptotically equals

$$q + \frac{q}{p^e} + 2\frac{q}{p^{2e}} + 5\frac{q}{p^{3e}} + ... \leq q + 9q/(4p^e)$$

Moreover, every line intersects B in 1 mod p^e points provided that $p^e \geq 9$.

An *s-fold blocking set* is a collection of points with the property that every line contains at least s of them. Just as was the case for ordinary blocking sets, the theory of lacunary polynomials can be applied to multiple blocking sets. At present the most general result is the following

Theorem 6.3 *Let B be an s-fold blocking set in $PG(2, q)$ of size $s(q + 1) + c$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p3$.*

1. *If $q = p^{2d+1}$ and $s < q/2 - c_p q^{2/3}/2$ then $c \geq c_p q^{2/3}$.*
2. *If $4 < q$ is a square, $s < q^{1/4}/2$ and $c < c_p q^{2/3}$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*
3. *If $q = p^2$ and $s < q^{1/4}/2$ and $c < p\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}} \rceil$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*

This result relies on an improvement of the fundamental lemma for lacunary polynomials, which we discussed earlier. The most important special case is the following result.

Let $f = X^{\sqrt{q}}g + h \in \mathbf{F}_q[X]$, q square, be fully reducible with $(g, h) = 1$, $f' \neq 0$ and $t = \max(g^\circ, h^\circ)$. Then either $f(X) = a\,\mathrm{Tr}(bX + c) + d$ or $f(X) = a\,\mathrm{Norm}(bX + c) + d$ for suitable constants a, b, c, d or $t \geq \frac{1}{4} + \sqrt{\frac{\sqrt{q}+1}{2}}$.

The most attractive open problem in this area is the question whether a double blocking set in $PG(2, p)$, where p is prime must have at least $3p$ points (known to be true only for $p = 2, 3, 5$ and 7).

7 The direction polynomial

In the previous sections we have seen how the Rédei polynomial of a set allows the application of the theory of lacunary polynomials over $GF(q)$ to problems about blocking sets, and sets of points determining few directions, and how this helps to obtain information on the size or structure of these sets. In this section and the subsequent ones we shall consider the points of $AG(2,q)$ as elements of $GF(q^2)$ and look at polynomials in $GF(q^2)[X]$. In particular we will associate to an affine point set a 'direction polynomial' that encodes how many points of the set are seen in each direction.

Every line in $AG(2,q)$ is a translate of a line through the origin, that can be viewed as a one-dimensional subspace over $GF(q)$. If we consider identify the points of $AG(2,q)$ with the elements of $GF(q^2)$, then for every point $x^{q^2} = x$ and the points lying in a 1-dimensional $GF(q)$-subspace are zeros of equations

$$\mathrm{Tr}_{q^2 \to q}(aX) = a^q X^q + aX = 0$$

for some a. The translates of these subspaces are the zeros of equations of the form

$$\mathrm{Tr}_{q^2 \to q}(aX) + b = a^q X^q + aX + b = 0,$$

where b is an element of $\mathrm{GF}(q)$. In practise we divide by a^q (and replace $a^{-(q-1)}$ by a and ba^{-q} by b); this tells us that the lines of $AG(2,q)$ have equations

$$X^q + aX + b = 0$$

where a is a non-zero $(q-1)$-st power and $ba^q = b^q$. For a, a non-zero $(q-1)$-st power in $GF(q^2)$, we have $a^{q+1} = (\alpha^{q-1})^{q+1} = \alpha^{q^2-1} = 1$. Hence a is also a $(q+1)$-st root of unity in $GF(q^2)$. Now two lines are parallel (they do no meet) if and only if they have the same a. Indeed the equations $X^q + aX + b = 0$ and $X^q + aX + c = 0$ have no common zero for $b \neq c$ and the corresponding lines have no point in common. Hence the $q+1$ parallel classes of $AG(2,q)$ can be identified with the $q+1$-st roots of unity in $GF(q^2)$.

Let us calculate a and b for two points (elements of $GF(q^2)$), say x and y. Then there exist a and b such that

$$x^q + ax + b = 0 \quad \text{and} \quad y^q + ay + b = 0.$$

This gives $a = -(x^q - y^q)/(x-y) = -(x-y)^{q-1}$ and $b = (yx^q - xy^q)/(x-y)$.

Moreover we see now that points x, y and z are collinear precisely when $(x-y)^{q-1} = (x-z)^{q-1}$. Consider a set of points $\mathcal{S}$. Define the *direction polynomial* $F_{\mathcal{S}} = F(U,X)$, a polynomial in two variables, by

$$F(U,X) := \prod_{s \in \mathcal{S}} (1 + (1 - sX)^{q-1} U).$$

Each linear factor of F is of the form $(1+(1-sX)^{q-1}U)$ for some $s \in \mathcal{S}$. Now $(1-sX)^{q-1} = X^{q-1}(1/X-s)^{q-1}$. If we put $X = x \in GF(q^2)$ then two linear factors are the same if and only if $(1/x-s_0)^{q-1} = (1/x-s_1)^{q-1}$ if and only if $1/x$, s_0 and s_1 are collinear.

8 Quasi-odd sets

We begin with a quirky example of how the direction polynomial can give remarkably simple proofs to some problems. Let $\mathcal{S}$ be a set of points in $PG(2,q)$ or $AG(2,q)$, q even. $\mathcal{S}$ is called *odd* (*even*) is every line intersects $\mathcal{S}$ in an odd (even) number of points. In $AG(2,q)$ there are no odd sets if q is even. However there exist sets with the property that every line intersects it in an odd number of points or misses the set completely. We call such a set *quasi-odd*. The following are examples of quasi-odd sets.

1. $PG(2,2)$ in $AG(2,8)$;
2. $PG(2,\sqrt{q})$ minus a hyperoval in $AG(2,q)$;
3. $PG(n,2)$ embedded as a linear space in $AG(2,2^{n+1})$ (this example, containing the first one as a special case is due to M. J. de Resmini).

In all the above we see that the size of the quasi-odd set is $q-1$. This is in fact maximum size of a quasi-odd set.

Theorem 8.1 *Let $\mathcal{S}$ be a quasi-odd set in $AG(2,q)$, q even. Then $|\mathcal{S}| \leq q-1$.*

Proof Identify $AG(2,q)$ with $GF(q^2)$, as in the previous section, and consider the coefficient of U in the direction polynomial $F(U,X)$.

$$\chi_1 = \sum_{s\in\mathcal{S}} (1-sX)^{q-1}.$$

Suppose $\mathcal{S}$ is not empty. Consider the lines through some fixed $s \in \mathcal{S}$. Besides s they contain an even number of points from the set $\mathcal{S}$; so adding these numbers gives that $|\mathcal{S}|$ is odd. It follows that χ_1 is not identically zero since

$$\chi_1(0) = |\mathcal{S}| \pmod 2 = 1.$$

We saw that for $x \in GF(q^2)^*$ the value of $(1-sx)^{q-1}$ depends only on the direction of the line joining $1/x$ and s. If $1/x \in \mathcal{S}$ every direction will occur an even number of times, so $\chi_1(x) = 0$. $\chi_1(X)$ is a polynomial of degree at most $q-1$ and since it is not identically zero can have at most $q-1$ zeros. It follows that $|\mathcal{S}| \leq q-1$.

□

9 Nuclei

Recall that a (k,n)-*arc* in $PG(2,q)$ or $AG(2,q)$ is a set of k points with at most n points on a line. A $(k,2)$-arc is called a k-arc. A $(q+1)$-arc $\mathcal{K}$ has $q+1$ tangents which for q even meet in a point P. The point P is called the nucleus of $\mathcal{K}$.

Following Mazzocca we extend this definition to all point sets of size at least $q+1$. A point $P \notin \mathcal{K}$ is a *nucleus* of $\mathcal{K}$ if each line through P contains at least one point of $\mathcal{K}$. Note that if $|\mathcal{K}| = q+1$ then each line through P contains exactly one point of $\mathcal{K}$.

We are interested in finding sets of points with a large number of nuclei. Let us consider first the case $|\mathcal{K}| = q+1$. How many nuclei can $\mathcal{K}$ have ? In $PG(2,q)$ this is not an interesting problem; if we take for $\mathcal{K}$ a line, every point in $PG(2,q) \setminus \mathcal{K}$ is a nucleus. However, if we exclude this trivial case, then there will be a line missing $\mathcal{K}$, and we may consider $\mathcal{K}$ as a set of points in $AG(2,q)$. The possible number of nuclei is greatly reduced in this case as we shall see.

Example 9.1 *Consider $\mathcal{K}$ as an affine line l together with a point $Q \notin l$. The $q-1$ points of $AG(2,q)$ that lie on the line through Q and parallel to l are all nuclei of $\mathcal{K}$.*

We shall see that the number $q-1$ is in fact best possible, first proven by myself and H. Wilbrink [12], but let us first see another example of a set of $q+1$ points with $q-1$ nuclei.

Example 9.2 *Let $q = 5$ and consider 10 points of a Desargues configuration. These split into a set of six points and four nuclei.*

Theorem 9.3 *Let $\mathcal{K}$ be a set of $q+k$ points in* $\mathrm{AG}(2,q)$. *The set $\mathcal{K}$ has at most $k(q-1)$ nuclei.*

Proof Consider the direction polynomial of such a set $\mathcal{K}$

$$F(U,X) := \prod_{s \in \mathcal{K}} (1 + (1-sX)^{q-1}U).$$

We view $F(U,X)$ as a polynomial in U whose coefficients are polynomials in X in the following way and write

$$F(U,X) = \sum_{j=0}^{q+k} \chi_j(X) U^j,$$

where $\chi_j(X)$ has degree at most $j(q-1)$. Let $1/x$ be a nucleus of $\mathcal{K}$. By definition, there is at least one point of $\mathcal{K}$ on each line through $1/x$. Hence each

linear factor of $1 - U^{q+1}$ occurs as a linear factor of $F(U, x)$. Therefore

$$F(U, x) = (1 - U^{q+1}) \sum_{j=0}^{k-1} \chi_j(x) U^j$$

for all such x. Comparing the coefficient of U in the two above equations implies $\chi_k(x) = 0$ and since χ_k has degree at most $k(q-1)$ it is identically zero if there exist more than $k(q-1)$ nuclei. However

$$F(U, 0) = (1 + U)^{q+k} = (1 + U)^k + U^q(1 + U)^k$$

and in particular $\chi_k(0) = 1$. Hence χ_k cannot be identically zero. Thus there are at most $k(q-1)$ nuclei.

□

In AG$(2, q)$ the only known examples of $(q+1)$-sets having exactly $q-1$ nuclei are Example 9.1 and the sporadic Example 9.2. In fact Example 9.1 can be generalized by taking for B a set of q collinear points, together with k points on k different parallels. This set has $k(q-1)$ nuclei, namely the remaining points on these parallels.

10 t-fold nuclei and t-fold affine blocking sets

A set $\mathcal{S}$ is a t-fold blocking set if every line meets $\mathcal{S}$ in at least t points. A 1-fold blocking set is called a blocking set. We have already seen (multiple) blocking sets in $PG(2, q)$ but here we shall be interested in t-fold blocking sets in $AG(2, q)$. Again we shall be looking for good lower bounds, however now we shall be using t-fold nuclei, which are a generalization of the nuclei we saw in the previous section. A point $P \notin \mathcal{S}$ is called a *t-fold nucleus* if every line through P meets the set $\mathcal{S}$ in at least t points. In order for $\mathcal{S}$ to have a t-fold nucleus the set $\mathcal{S}$ has to have at least $t(q+1)$ points. The following theorem gives an upper bound on the number of t-fold nuclei of a set. The proof follows [4].

Theorem 10.1 *The number of t-fold nuclei of a set $\mathcal{S}$ of $t(q+1)+k-1$ points in $AG(2, q)$ is at most $k(q-1)$, provided that $\binom{t(q+1)+k-1}{k} \neq 0 \pmod{p}$.*

Proof We restrict to the case $k < q$, since otherwise the bound is obvious. Consider $\mathcal{S}$ as a subset of $GF(q^2)$ as before and consider again the direction polynomial

$$F(U, X) := \prod_{s \in \mathcal{S}} (1 + (1 - sX)^{q-1} U).$$

Consider a t-fold nucleus x of $\mathcal{S}$. This means, that every line through x contains at least t points of $\mathcal{S}$. Hence the multiset

$$\{(1 - sx)^{q-1} \mid s \in \mathcal{S}\}$$

contains every $(q+1)$-st root of unity at least t times. This implies that the polynomial $F(U,x)$ is divisible by

$$(1-U^{q+1})^t$$

whenever x is a t-fold nucleus of $\mathcal{S}$. Again we write $F(U,X)$ as a polynomial in U with coefficients polynomials in X.

$$F(U,X) = \sum_{j=0}^{t(q+1)+k-1} \chi_j(X)U^j,$$

where $\chi_j(X)$ has degree at most $j(q-1)$. Now for x a t-fold nucleus of $\mathcal{S}$

$$F(U,x) = (1-U^{q+1})^t \sum_{j=0}^{k-1} \chi_j(x)U^j$$

and as before we see that $\chi_k(x) = 0$. The degree of χ_k is at most $k(q-1)$ and $\chi_k(0)$ is equal to the coefficient of U^k in

$$F(U,0) = (1+U)^{t(q+1)+k-1}.$$

So we see that if

$$\binom{t(q+1)+k-1}{k} \neq 0 \pmod{p},$$

then χ_k is not identically zero and there can be at most $k(q-1)$ t -fold nuclei. □

Now we wish to examine this binomial coefficient and for this we will need Lucas' Theorem. The proof of the following comes from [26].

Theorem 10.2 *For a and b integers, with p-adic expansions, $a = a_0 + a_1p + a_2p^2 + \ldots$ and $b = b_0 + b_1p + b_2p^2 + \ldots + b_np^n$*

$$\binom{a}{b} = \binom{a_0}{b_0}\binom{a_1}{b_1}\ldots\binom{a_n}{b_n} \pmod{p}.$$

Proof In the polynomial ring $GF(p)[X]$ the following holds

$$(1+X)^a = \prod_{i=0}^{\infty}(1+X)^{a_ip^i} = \prod_{i=0}^{\infty}(1+X^{p^i})^{a_i}.$$

In other words

$$\sum_{b=0}^{\infty}\binom{a}{b}X^b = \prod_{i=0}^{\infty}\sum_{k_i=0}^{p-1}\binom{a_i}{k_i}X^{k_ip^i} = \sum_{k_0,k_1,\ldots=0}^{p-1}\binom{a_0}{k_0}\binom{a_1}{k_1}\ldots X^{k_0+k_1p+k_2p^2+\ldots}$$

and the theorem follows from comparison of coefficients.

□

Recall that a t-fold blocking set is a set $\mathcal{S}$ meeting every line at least t times. For such a set every other point is a t-fold nucleus. By applying Lucas' Theorem (Theorem 10.2) to Theorem 10.1 we get the following theorem. This proof comes from [1].

Theorem 10.3 *Let $\mathcal{S}$ be a t-fold blocking set of $AG(2,q)$ and let $e(t)$ be maximal such that $p^{e(t)} \mid t$. Then the set $\mathcal{S}$ has at least $(t+1)q - p^{e(t)}$ points.*

Proof Put $k = q - t - p^{e(t)}$ and write $t = \gamma p^{e(t)}$ such that $p \not| \gamma$. Consider the binomial coefficient

$$\binom{t(q+1)+k-1}{k} = \binom{t(q+1)+k-1}{t(q+1)-1} = \binom{tq+q-p^{e(t)}-1}{tq+t-1}.$$

A simple application of Lucas' Theorem implies that this binomial coefficient is non-zero precisely when

$$\binom{q-p^{e(t)}-1}{\gamma p^{e(t)}-1} = \binom{q-2p^{e(t)}+p^{e(t)}-1}{(\gamma-1)p^{e(t)}+p^{e(t)}-1} = \binom{q/p^{e(t)}-2}{\gamma-1} \pmod{p}$$

is non-zero, and it is non-zero since $\gamma \neq 0 \bmod p$. Hence $\mathcal{S}$ cannot be a t-fold blocking set when $k = q-t-p^{e(t)}$ since $\mathcal{S}$ has at most $k(q-1)$ t-fold nuclei and

$$t(q+1)+k-1+k(q-1) = (q-t-p^{e(t)})q+t(q+1)-1 = q^2+t-p^{e(t)}q-1 < q^2.$$

□

The lower bound $2q-1$ for a blocking set in $AG(2,q)$ was proved first by Jamison [20] and independently Brouwer and Schrijver [13]. Bruen [14] obtained the lower bound $(t+1)q - t$ for a t-fold blocking set.

The following examples all attain the lower bound in Theorem 10.3.

1. (Denniston [19]) The affine complements of the maximal arcs constructed by Denniston are $(q-2^m)$-fold blocking sets in $\mathrm{AG}(2,q)$, $q = 2^h$ for some h, of size $(q-2^m+1)q - 2^m = (t+1)q - 2^{e(t)}$ where $t = q - 2^m$ and hence $e(t) = m$.

2. The external points to a conic together with all but one points of the conic form a $(q+1)/2$-fold blocking set in $\mathrm{PG}(2,q)$ whenever q is odd. Moreover this set contains a line and by deletion we can form a $(q-1)/2$-fold blocking set of size $q(q+1)/2 + q - (q+1) = (t+1)q - 1$ in $\mathrm{AG}(2,q)$ where $t = (q-1)/2$ and hence $e(t) = 0$.

3. (Mason [22]) The affine complements of Mason's $((q-p^m)(q-1), q-p^m)$-arcs are p^m-fold blocking sets in $\mathrm{AG}(2,q)$, $q = p^h$ for some h, of size $p^m q - p^m + q = (t+1)q - p^m$ where $t = p^m$ and hence $e(t) = m$.

11 Maximal arcs

Recall that a (k,n)-arc is a set of k points, at most n on each line. For any (k,n)-arc in a projective plane of order q, $k \leq 1+(q+1)(n-1) = qn-q+n$ with equality if and only if every line intersects the arc in 0 or n points. Arcs realizing the upper bound are called *maximal arcs*. Equality in the bound implies that $n \mid q$ or $n = q+1$. If $1 < n < q$, then the maximal arc is called non-trivial. The only known examples of non-trivial maximal arcs in $PG(2,q)$ are the hyperovals ($n = 2$), for $n > 2$ the Denniston arcs [19] and an infinite family constructed by Thas [29, 31]. These exist for all pairs $(n,q) = (2^a, 2^b)$, $0 < a < b$. It is conjectured in [30] that for odd q maximal arcs do not exist. In that paper this was proved for $(n,q) = (3,3^h)$. The special case $(n,q) = (3,9)$ was settled earlier by Cossu [18]. A complete proof was given in [2]. The proof given in this section comes from [3].

We shall consider point sets in the affine plane $AG(2,q)$ instead of $PG(2,q)$. This is no restriction; there is always a line disjoint from a non-trivial maximal arc. As before we shall consider the points of $AG(2,q)$ as elements of $GF(q^2)$.

Let $\mathcal{B}$ be a non-trivial $(nq-q+n,n)$-arc in $AG(2,q) \simeq GF(q^2)$, $q = p^h$. For simplicity we assume $0 \notin \mathcal{B}$. Let $\mathcal{B}^{[-1]} = \{1/b \mid b \in \mathcal{B}\}$. Define $B(X)$ to be the polynomial

$$B(X) := \prod_{b\in\mathcal{B}}(1-bX) = \sum_{k=0}^{\infty}(-1)^k\sigma_k X^k$$

where σ_k denotes the k-th elementary symmetric function of the set $\mathcal{B}$, in particular $\sigma_k = 0$ for $k > |\mathcal{B}|$. As before we have the direction polynomial $F = F_{\mathcal{B}}$ in two variables and its coefficients χ_k in one variable defined by

$$F(U,X) := \prod_{b\in\mathcal{B}}(1+(1-bX)^{q-1}U) = \sum_{k=0}^{\infty}\chi_k U^k.$$

Here χ_k is the k-th elementary symmetric function of the set of polynomials $\{(1-bX)^{q-1} \mid b \in \mathcal{B}\}$, a polynomial of degree at most $k(q-1)$ in X. Again, χ_k is the zero polynomial for $k > |\mathcal{B}|$. For $x \in GF(q^2)\setminus\mathcal{B}^{[-1]}$ it follows that $F(U,x)$ is an n-th power. Indeed, for $x = 0$ this is clear, and if $x \neq 0$ then $1/x$ is a point not contained in the arc, so that every line through $1/x$ contains a number of points of $\mathcal{B}$ that is either 0 or n. In the multiset $\{(1/x-b)^{q-1} \mid b \in \mathcal{B}\}$, every element occurs therefore with multiplicity n, so that in $F(U,x)$ every factor occurs exactly n times.

For $x \in \mathcal{B}^{[-1]}$ we get that $F(U,x) = (1-U^{q+1})^{n-1}$, for in this case every line passing through the point $1/x$ contains exactly $n-1$ other points of $\mathcal{B}$, so that the multiset $\{(1/x-b)^{q-1}\}$ consists of every $(q+1)$-st root of unity repeated $n-1$ times, together with the element 0. This gives

$$F(U,x) = \prod_{b\in\mathcal{B}}(1+(1/x-b)^{q-1}x^{q-1}U) = (1-x^{q^2-1}U^{q+1})^{n-1} = (1-U^{q+1})^{n-1}.$$

From the shape of F in both cases it can be seen that for all $x \in GF(q^2)$, $\chi_k(x) = 0$, $0 < k < n$, and since the degree of χ_k is at most $k(q-1) < q^2$, these functions are in fact identically zero. The first coefficient of F that is not necessarily identically zero therefore is χ_n. Let $Z = X - X^{q^2}$. Since in both cases, i.e. for all $x \in GF(q^2)$, χ_k vanishes unless $n|k$ or $(q+1)|k$ it follows that $Z|\chi_k$. If $n \nmid k$ then χ_k still vanishes for $x \in GF(q^2) \setminus \mathcal{B}^{[-1]}$, and since $B \mid \chi_n$ we get the divisibility relation $(X - X^{q^2}) \mid \chi_n\chi_k$. Hence we can write

$$F(U,X) = 1 + \sum_{i=1}^{q-q/n+1} \chi_{in}U^{in} + \sum_{i=1}^{n-1} \chi_{i(q+1)}U^{i(q+1)} \pmod{Z}$$

and

$$BF(U,X) = B + B \sum_{i=1}^{q-q/n+1} (-1)^i \chi_{in}U^{in} \pmod{Z}.$$

Since $\chi_n(0) = \binom{|\mathcal{B}|}{n} = \binom{nq-q+n}{n} = 1$, by Lucas' theorem, it is not identically zero. On the other hand the coefficient of U^n in $(1-U^{q+1})^{n-1}$ is zero, so $\chi_n(x) = 0$ for $x \in \mathcal{B}^{[-1]}$, in other words, B divides χ_n. The polynomial χ_{q+1} will be of some use as well, so it is worth noting that $\chi_{q+1}(x) = 1$ for all $x \in \mathcal{B}^{[-1]}$ and $\chi_{q+1}(x) = 0$ for all $x \in GF(q^2) \setminus \mathcal{B}^{[-1]}$.

The main objective of the proof is to show $(B\chi_n)' \equiv 0$ which will lead swiftly to a contradiction for $p \neq 2$. Throughout f' will represent the derivative of a function f with respect to X and f_X will denote the partial derivative with respect to X.

By computing the derivative of $B(X)$ and expanding the denominator as an infinite sum we get

$$B'(X) = \sum_{b\in\mathcal{B}} \frac{-b}{1-bX} B(X) = -\left(\sum_{b\in\mathcal{B}} \sum_{i=0}^{\infty} b^{i+1}X^i\right) B(X).$$

Note that all $b \in \mathcal{B}^{[-1]}$ are elements of $GF(q^2)$ hence $b^{q^2} = b$ and it follows that

$$(X - X^{q^2}) \left(\sum_{b\in\mathcal{B}} \sum_{i=0}^{\infty} b^{i+1}X^i\right) = \sum_{b\in\mathcal{B}} \sum_{i=0}^{q^2-1} b^iX^i = \sum_{b\in\mathcal{B}} (1-bX)^{q^2-1}.$$

The polynomial $-\sum_{b\in\mathcal{B}}(1-bX)^{q^2-1}$ is equal to 1 for all $x \in \mathcal{B}^{[-1]}$ since there are $nq-q+n$ terms in the sum, one of which will be zero the others of which will be 1. For all other elements of $GF(q^2)$ it will be zero, since every term in the sum will be 1. Now χ_{q+1} takes the same values and both are of degree q^2-1. Hence it follows that they are the same. i.e. $\chi_{q+1} = -\sum_{b\in\mathcal{B}}(1-bX)^{q^2-1}$. So we get the important relation

$$ZB' = \chi_{q+1}B.$$

Differentiating this, multiplying by B and noting that $B\chi_{q+1} = 0 \pmod{Z}$ we get another useful relation

$$BB' = B^2\chi'_{q+1} \pmod{Z}.$$

Differentiating $F(U, X)$ with respect to X it follows that

$$F_X(U, X) = \left(\sum_{b \in \mathcal{B}} \frac{b(1 - bX)^{q-2}U}{1 + (1 - bX)^{q-1}U} \right) F(U, X) = \sum_{k=0}^{|\mathcal{B}|} \chi'_k U^k.$$

The terms in the denominator are of the form $(1 + (1 - bX)^{q-1}U)$ and for all $X = x \in GF(q^2)$ this is a factor of $(1 - U^{q+1})$. Hence multiplying the above by $(1 - U^{q+1})$ and putting $X = x \in GF(q^2)$ we see the bracket becomes a polynomial in U and that

$$F(U, x) | (1 - U^{q+1}) F_X(U, x).$$

Define the quotient of this division to be $R_x(U)$ and by computation we see

$$R_x(U) = \chi'_n(x)U^n + \hat{R}_x(U)U^{2n} + \chi'_{q+1}(x)U^{q+1}$$

where $\hat{R}_x(U)$ is an n-th power (considered as a function of U). Abusing notation we define the polynomial $R(U, X)$ in two variables with the property that for $x \in GF(q^2)$ $R(U, x) = R_x(U)$. Then we have that

$$FR = (1 - U^{q+1})F_X \pmod{Z},$$

and by multiplying by B that

$$\left(\sum_{i=0}^{q-q/n+1} B\chi_{in}U^{in} \right) R = (1 - U^{q+1})BF_X \pmod{Z}.$$

By equating the coefficient of U^{q+1+n} we see that

$$\chi'_{q+1}B\chi_n = \chi'_{q+1+n}B - B\chi'_n.$$

Note that since $B|\chi_n$ we can use the relation $B^2\chi'_{q+1} = BB' \pmod{Z}$ and rearranging terms gives

$$B\chi'_{q+1+n} = (B\chi_n)' \pmod{Z}.$$

Equating successively the coefficient of $U^{i(q+1)+n}$ for $1 < i < (n - 1)$ gives

$$B\chi'_{i(q+1)+n} = B\chi'_{(i-1)(q+1)+n} = (B\chi_n)' \pmod{Z}.$$

Since $|B| = nq - q + n$ it follows that $\chi_{(n-1)(q+1)+n} \equiv 0$ and so when we look at the coefficient of $U^{(n-1)(q+1)+n}$ we find that

$$(B\chi_n)' \equiv 0 \pmod{Z}.$$

Since $B\chi_n$ has degree at most $(nq - q + n) + n(q - 1) < q^2$ it follows that $(B\chi_n)' = 0$ identically, and hence $B\chi_n$ is a p-th power. Since B does not have multiple factors, this implies that $B^{p-1}|\chi_n$ which gives a contradiction for $p \neq 2$, since the degree of χ_n is at most $n(q-1)$ and it is not identically zero.

Theorem 11.1 *For $1 < n < q$ and q odd, there do not exist maximal arcs in $AG(2, q)$.*

References

[1] S. Ball, On nuclei and blocking sets in Desarguesian spaces, *J. Combin. Theory Ser. A*, **85**, (1999), 232–237.

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

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

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

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

[6] A. Blokhuis, Blocking sets in projective and affine planes, *Notes for the intensive course in Ghent*, April 14–24, 1998.

[7] 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, accepted for publication in *J. Combin. Theory Ser. A*.

[8] A. Blokhuis and A.E. Brouwer, Blocking sets in Desarguesian Projective Planes, *Bull. London Math. Soc.*, **18**, (1986), 132–134.

[9] A. Blokhuis and 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.

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

[11] A. Blokhuis, L. Storme and T. Szőnyi, Lacunary Polynomials, Multiple Blocking Sets and Baer Subplanes, submitted to *J. London Math. Soc.*

[12] A. Blokhuis and H.A. Wilbrink, A characterization of exterior lines of certain sets of points in $PG(2,q)$, *Geom. Dedicata*, **23**, (1987), 253–254.

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

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

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

[16] A.A. Bruen and R. Silverman, Arcs and blocking sets II, *Europ. J. Combin.*, **8**, (1987), 351–356.

[17] A.A. Bruen and J.A. Thas, Flocks, Chains and Configurations in Finite Geometries, *Atti del Acc. Naz. dei Lincei*, **LIX** no **6**, (1975), 744–748.

[18] A. Cossu, Su alcune proprietà dei $\{k;n\}$-archi di un piano proiettivo sopra un corpo finito, *Rend. Mat. e Appl.*, **20**, (1961), 271–277.

[19] R. H. F. Denniston, Some maximal arcs in finite projective planes *J. Combin. Theory Ser. A*, **6**, (1969), 317–319.

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

[21] G. Lunardon, Normal spreads, *Forum Mathematicorum*, submitted (1997).

[22] J. R. M. Mason, A class of $((p^n-p^m)(p^n-1),p^n-p^m)$-arcs in $\mathrm{PG}(2,p^n)$ *Geom. Dedicata*, **15**, (1984), 355–361.

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

[24] J.H. van Lint and F.J. MacWilliams, Generalized Quadratic Residue Codes, *IEEE Transactions on Information Theory*, IT **24**, (1978), 730–737.

[25] P. Polito and O. Polverino, On small blocking sets, *Combinatorica*, **18**, (1997), 133–137.

[26] L. Rédei, Lückenhafte Polynome über endlichen Körper, Birkhäuser Verlag, Basel und Stuttgart, 1970.

[27] B. Segre and G. Korchmáros, Una proprietà degli insiemi di punti, ecc, *Acc. Naz. dei Lincei, Rend. Sc. fis. Mat. nat.*, **LXII**, (1977).

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

[29] J. A. Thas, Construction of maximal arcs and partial geometries, *Geom. Dedicata*, **3**, (1974), 61–64.

[30] J. A. Thas, Some results concerning $\{(q+1)(n-1); n\}-$arcs and $\{(q+1)(n-1)+1; n\}-$arcs in finite projective planes of order q, *J. Combin. Theory Ser. A*, **19**, (1975), 228–232.

[31] J. A. Thas, Construction of maximal arcs and dual ovals in translation planes, *Europ. J. Combinatorics*, **1**, (1980), 189–192.