Polynomials in Finite Geometries

S. Ball

Summary A method of using polynomials to describe objects in finite geometries is outlined and the problems where this method has led to a solution are surveyed. These problems concern nuclei, affine blocking sets, maximal arcs and unitals. In the case of nuclei these methods give lower bounds on the number of nuclei to a set of points in $\mathrm{PG}(n, q)$, usually dependent on some binomial coefficient not vanishing modulo the characteristic of the field. These lower bounds on nuclei lead directly to lower bounds on affine blocking sets with respect to lines. A short description of how linear polynomials can be used to construct maximal arcs in certain translation planes is included. A proof of the non-existence of maximal arcs in $\mathrm{PG}(2, q)$ when q is odd is outlined and some bounds are given as to when a (k, n)-arc can be extended to a maximal arc in $\mathrm{PG}(2, q)$. These methods can also be applied to unitals embedded in $\mathrm{PG}(2, q)$. One implication of this is that when q is the square of a prime a non-classical unital has a limited amount of Baer sublines amongst its secants.

1 Introduction

The effectiveness of polynomials as a means of studying problems in finite geometries has become increasingly evident in the 1990's, although the first examples seem to date back to R. Jamison [38] in 1977 and A. E. Brouwer and A. Schrijver [19] in 1978. Indeed in [22] A. A. Bruen and J. C. Fisher described the "Jamison method" as the following: reformulate the problem in terms of points of an affine space and associate suitable polynomials defined over the corresponding finite field; calculate. This is the approach employed in [19] too; in fact the main difference between [38] and [19] is that Jamison viewed the points of an affine space as elements of a finite field. In effect, this has the advantage of reducing the number of variables in the polynomials and allowing one to use simple arguments concerning the degree or the coefficients of a polynomial. Earlier survey papers covering polynomial applications to finite geometries include [11], [12] and [53] and in some ways the present paper is an update of those, although there is much material in those articles that is not covered here.

In general, we are interested in solving problems of the form: Given a set of subspaces (usually points) in a Desarguesian space with restricted intersections with larger subspaces (usually lines), what can we say about the size of the set and can we characterise the extremal cases ? Historically this stems from the famous proof of B. Segre [49] that any set of $q + 1$ points in the Desarguesian plane of odd order q having at most two points on a line is a conic.

Section 2 considers polynomials whose zeros correspond to subspaces of Desarguesian affine and projective spaces. This leads us to define polynomials, given an arbitrary set of points $\mathcal{S}$, whose properties reflect the properties of $\mathcal{S}$. These polynomials are fundamental to many of the proofs of the results covered in this paper.

Section 3 updates results concerning nuclei. It is not a complete survey; indeed emphasis is given to those results for which the polynomials in Section 2 have been the most useful. The intriguing conjecture from [16] is included. Following on directly from the bounds in Section 3, lower bounds on the size of affine blocking sets are detailed. I include a general definition for blocking sets in affine and projective spaces in the hope that this will be adopted. Since the early 1990's there have appeared conflicting definitions by various authors, which has led to some confusion. I have not surveyed recent developments in projective blocking sets, there being too much material for the scope of this paper. However a survey from 1997 can be found in [37, Chapter 13]. The recent constructions by G. Lunardon [40] and by P. Polito and O. Polverino [47] concerning linear blocking sets are the most notable developments since then.

Section 5 leaves surveying aside and gives details of how one can view translation planes with polynomials using the construction of André [1] and Bruck and Bose [20], in the hope of proving algebraic results previously only possible in Desarguesian planes. Returning to the surveying, Section 6 contains recent results and constructions concerning maximal arcs, including a sketch of the non-existence proof for Desarguesian planes. A construction of some maximal arcs in translation planes using polynomials is also included.

Finally Section 7 considers unitals embedded in a Desarguesian plane. The classification of such objects appears to be a very hard problem; some characterisations can be obtained from polynomial arguments.

Where possible I have put definitions in their relevant sections in such a way that each section is self-standing. However, the construction in Section 6 is dependent on Section 5 and Section 4 is closely related to Section 3.

2 Definitions and useful polynomials

Let π_n denote a projective space of dimension n and $\mathrm{PG}(n,q)$ the Desarguesian space of order q. Let $\mathcal{A}_n$ denote an affine space of dimension n and $\mathrm{AG}(n,q)$ the Desarguesian space of order q. Throughout, $\theta_n = (q^{n+1}-1)/(q-1)$, the number of points of π_n, and $q = p^h$ for some prime p.

2.1 Affine spaces

The elements of $\mathrm{GF}(q^n)$, where $q = p^h$ for some prime p, can be viewed as the points of $\mathrm{AG}(n,q)$. The points lying on a hyperplane are given by the zeros of equations

$$\mathrm{Tr}_{q^n \to q}(ax) + b = 0,$$

where b is an element of $\mathrm{GF}(q)$ and $\mathrm{Tr}_{q^n \to q}(x) = x^{q^{n-1}} + x^{q^{n-2}} + ... + x^q + x$ is the trace function from $\mathrm{GF}(q^n)$ to $\mathrm{GF}(q)$. To see this, note that the polynomial should have degree q^{n-1}. Every hyperplane in $\mathrm{AG}(n, q)$ is a translate of a hyperplane through the origin; this translate can be seen as an $(n-1)$-dimensional subspace over $\mathrm{GF}(q)$, and the corresponding polynomial is therefore $\mathrm{GF}(q)$-linear and so of the form

$$H(x) := \sum_{j=0}^{n-1} a_j x^{q^j} + b.$$

R. Jamison provided a proof of this [38, Lemma A, p. 259] which he credited to O. Ore, who wrote two expositions on polynomials of the form (1) [44, 45]. These polynomials are called linearized polynomials, see [39, Chapter 3, Section 4]. The polynomial

$$a_{n-1} H^q - a_{n-1}^{q+1}(x^{q^n} - x) - a_{n-2}^q H$$

has degree at most q^{n-2} and since all the points of the hyperplane are zeros it is identically zero. Equating coefficients of x^{q^i} for $0 \leq i \leq n-2$ implies the trace function form above.

A suitable linear combination of k hyperplane polynomials will give an equation of the form

$$\sum_{j=0}^{n-k-1} \alpha_j x^{q^j} + \beta = 0, \tag{1}$$

whose zeros correspond to a subspace of dimension $n - k - 1$ that is the intersection of the corresponding k hyperplanes. In particular, lines are given by the sets of zeros of polynomials of the form

$$x^q - \alpha x + \beta = 0,$$

and for a line joining a point x and a point y (viewed as elements of $\mathrm{GF}(q^n)$) we have $\alpha = (x - y)^{q-1}$. The non-zero $(q-1)$-th powers are θ_{n-1}-th roots of unity in $\mathrm{GF}(q^n)$, so there is a one-to-one correspondence between the θ_{n-1}-th roots of unity in $\mathrm{GF}(q^n)$ and the θ_{n-1} directions of lines in $\mathrm{AG}(n, q)$.

Given a set of points $\mathcal{S}$, a subset of $\mathrm{AG}(n, q)$, viewed as elements of $\mathrm{GF}(q^n)$ and not containing the zero element, define the *locator polynomial* (Jamison would call this the *root polynomial* and were $\mathcal{S}$ to be a subspace the *Ore polynomial*) of $\mathcal{S}$ to be

$$S(x) := \prod_{s \in \mathcal{S}} (1 - sx) = \sum_{j=0}^{|\mathcal{S}|} (-1)^j \sigma_j x^j,$$

where σ_j is the j-th symmetric function of the set $\mathcal{S}$. Strictly speaking this is the locator polynomial for the set $\{1/s \mid s \in \mathcal{S}\}$ since these are the zeros of $S(x)$, but we choose to define it this way simply so that the coefficient of $(-1)^j x^j$ in $S(x)$ is the j-th symmetric function.

Define the *direction polynomial* of a set $\mathcal{S}$ to be

$$F(u,x) := \prod_{s\in\mathcal{S}}(1-(1-sx)^{q-1}u) = \sum_{j=0}^{|\mathcal{S}|}(-1)^j\chi_j(x)u^j,$$

where $\chi_j(x)$ is the j-th symmetric function of the set $\{(1-sx)^{q-1} \mid s\in\mathcal{S}\}$, a polynomial in x of degree at most $k(q-1)$. If $F(u,x_0)$ is viewed as a polynomial in u, its zeros are θ_{n-1}-th roots of unity and moreover $(1-s_1x_0)^{q-1} = (1-s_2x_0)^{q-1}$ if and only if $(1/x_0-s_1)^{q-1} = (1/x_0-s_2)^{q-1}$ if and only if $1/x_0$, s_1 and s_2 are collinear.

2.2 Projective spaces

The $(q-1)$-th powers of the elements of $\mathrm{GF}(q^{n+1})$ can be viewed as the directions of the lines through the origin in $\mathrm{AG}(n+1,q)$ and hence the points of $\mathrm{PG}(n,q)$. The hyperplanes through the origin are given by zeros of equations of the form

$$\mathrm{Tr}_{q^{n+1}\to q}(AX) = 0 = AX\sum_{i=0}^{n} A^{q^i-1}X^{q^i-1},$$

and by writing $x = X^{q-1}$ and $a = A^{q-1}$ the hyperplanes of $\mathrm{PG}(n,q)$ are given by the zeros of equations of the form

$$\sum_{i=0}^{n} a^{(q^i-1)/(q-1)}x^{(q^i-1)/(q-1)} = 0.$$

As in the affine case, taking a suitable linear combination of k hyperplane polynomials, one can obtain an equation of the form

$$\sum_{j=0}^{n-k-1}\alpha_j x^{\theta_j} + \beta = 0$$

whose zeros correspond to the points of a subspace of dimension $n-k-1$, that is the intersection of the corresponding k hyperplanes. In particular lines are given by the sets of zeros of equations of the form

$$x^{q+1} - \alpha x + \beta = 0,$$

where there exist relations between α and β depending on the dimension, and for a line joining a point x and a point y (viewed as $(q-1)$-th power of $\mathrm{GF}(q^{n+1})$) we have

$$\alpha = (x^{q+1}-y^{q+1})/(x-y).$$

Given a set $\mathcal{S}$ we define the locator polynomial $S(x)$ as for the affine spaces but define the direction polynomial slightly differently as

$$F(u,x) := \prod_{s\in\mathcal{S}}(1 - sx(1-sx)^{q-1}u) = \sum_{j=0}^{|\mathcal{S}|}(-1)^j\Delta_j(x)u^j,$$

where $\Delta_j(x)$ is the j-th symmetric function of the set $\{sx(1-sx)^{q-1} \mid s \in \mathcal{S}\}$, a polynomial in x of degree at most jq. The linear factors of $F(u,x_0)$ have zeros of the form $u_0^{-1} = sx_0(1-sx_0)^{q-1}$ which satisfies

$$1 + u + u^{q+1} + u^{q^2+q+1} + \ldots + u^{\theta_{n-1}} = 0 \tag{2}$$

for $u = u_0^{-1}$. Moreover $s_1x_0(1-s_1x_0)^{q-1} = s_2x_0(1-s_2x_0)^{q-1}$ if and only if $1 + s_1x_0(1-s_1x_0)^{q-1} = 1 + s_2x_0(1-s_2x_0)^{q-1}$ if and only if

$$\frac{1/x_0^{q+1} - s_1^{q+1}}{1/x_0 - s_1} = \frac{1/x_0^{q+1} - s_2^{q+1}}{1/x_0 - s_2}$$

if and only if $1/x_0$, s_1 and s_2 are collinear. Therefore there is a one-to-one correspondence between the θ_{n-1} zeros of (2) and the directions of the lines through $1/x_0$.

3 Nuclei

A point P in π_n is a *t-fold nucleus* of a set of points $\mathcal{S}$ if $P \notin \mathcal{S}$ and on every line through P there are at least t points of $\mathcal{S}$. A 1-fold nucleus is called a *nucleus*. The original definition of nucleus stems from a $(q+1)$-arc in $\mathrm{PG}(2,2^h)$ which has one such nucleus.

3.1 Nuclei in affine planes

The following theorem is a consequence of results proved for q even by Bruen and Thas [23] and for q odd by Segre and Korchmáros [50].

Result 3.1 *Let $\mathcal{S}$ be a set of $q+1$ points of $\mathrm{AG}(2,q)$. The set of nuclei of $\mathcal{S}$ cannot contain a conic.*

Motivated by this the question of how many nuclei a $(q+1)$-set can have was posed. In the Desarguesian case this was answered by Blokhuis and Wilbrink [18] who gave a simple proof using polynomials which contains many of the basic ideas used to prove much of what is contained in this article. For that reason the proof is included, by way of an example of how the polynomials work.

Theorem 3.2 *Let $\mathcal{S}$ be a set of $q+1$ points in $\mathrm{AG}(2,q)$. The set of nuclei of $\mathcal{S}$ has size at most $q-1$.*

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

$$F(u,x) := \prod_{s\in\mathcal{S}}(1-(1-sx)^{q-1}u) = \sum_{j=0}^{q+1}(-1)^j\chi_j(x)u^j,$$

and an x_0 such that $1/x_0$ is a nucleus of $\mathcal{S}$. By definition, there is exactly one point of $\mathcal{S}$ on each line through $1/x_0$ and so

$$F(u,x_0) = 1-u^{q+1}$$

for all such x_0. Comparing the coefficient of u in the two above equations implies $\chi_1(x_0)=0$ and since $\chi_1(x)$ has degree at most $q-1$ it is identically zero if there exist more than $q-1$ nuclei. However

$$F(u,0) = (1-u)^{q+1} = 1-u-u^q+u^{q+1}$$

and in particular $\chi_1(0)=1$, and hence $\chi_1(x)$ cannot be identically zero.

In $\mathrm{AG}(2,q)$ the only known examples of $(q+1)$-sets having exactly $q-1$ nuclei are a set consisting of a line together with a point, and a sporadic example in $\mathrm{AG}(2,5)$ where the 10 points of a Desargues configuration can be partitioned into a set of size 6 and 4 nuclei. This leads to the following conjecture [16].

Conjecture 3.3 *In* $\mathrm{AG}(2,q)$ *these are the only* $(q+1)$*-sets having exactly* $q-1$ *nuclei.*

Partial results towards this conjecture appear in [16]. The following lemma of Segre and Korchmáros may well prove to be a powerful tool in settling the above conjecture.

Lemma 3.4 *Let* $\mathcal{S}$ *be a set of* $q+1$ *points in* $\mathrm{PG}(2,q)$*. For any three non-collinear nuclei* N_1*,* N_2 *and* N_3*, the points of* $\mathcal{S}$ *on the three lines* N_iN_j *are collinear.*

3.2 Generalised and non-planar nuclei

Following on from Theorem 3.2, various generalisations were proven. All of these are contained in Result 3.5, which appears in [4].

Result 3.5 *Suppose there exists a hyperplane* $\mathcal{H}$ *containing exactly* i *points of* $\mathcal{S}$*, a set of* $t\theta_{n-1}+k-1$ *points in* $PG(n,q)$*. The number of* t*-fold nuclei in* $AG(n,q)=PG(n,q)\setminus\mathcal{H}$ *is at most* $(k+r)(q-1)$ *provided that the binomial coefficient*

$$\binom{t\theta_{n-1}+k-i-1}{k+r} \not\equiv 0 \pmod p,$$

for some $r\geq 0$.

The case $t = 1$ and $i = r = 0$ and $n = 2$ comes from [13], and general t from [14], and for general n and i is due to Sziklai [52]. In all cases the essence of the proof follows Theorem 3.2.

Let us consider the case $t = k = 1$. Result 3.5 implies that a set $\mathcal{S}$ of size θ_{n-1} in $\mathrm{AG}(n, q)$ has at most $q - 1$ nuclei. However, in the case where $\mathcal{S}$ intersects every hyperplane of $\mathrm{PG}(n, q)$, Blokhuis and Mazzocca [17] proved the following.

Result 3.6 *If $\mathcal{S}$ intersects every hyperplane then the number of nuclei is at most $q^{n-1} - q^{n-2}$; moreover sets exist that attain the bound.*

Consider such a set $\mathcal{S}$ of size θ_{n-1} and with $q^{n-1} - q^{n-2}$ nuclei. Result 3.5 implies that $\mathcal{S}$ has at most $(r + 1)(q - 1)$ nuclei provided that the binomial coefficient

$$\binom{\theta_{n-1} - i}{r + 1} \neq 0 \pmod p.$$

In the extremal case when $r = q^{n-2} - 1$ we have that $q^{n-2} | \theta_{n-1} - i$ or we would have been able to find a smaller r for which the binomial coefficient was non-zero. It follows then that $i = \theta_{n-3} \pmod{q^{n-2}}$ or in words that every hyperplane meets $\mathcal{S}$ in $\theta_{n-3} \pmod{q^{n-2}}$ points. As a consequence of [17, Proposition 14] we have that the classification of θ_{n-1}-sets in $\mathrm{PG}(n, q)$ $(n > 2)$ with $q^{n-1} - q^{n-2}$ nuclei is equivalent to the case of $(q + 1)$-sets in $\mathrm{PG}(2, q)$ having $q - 1$ nuclei, that is Conjecture 3.3.

3.3 Extension of the nucleus definition

In [52], and for $n = 2$ earlier in [30], a point P in π_n is called a $(\leq t)$-fold nucleus of a set $\mathcal{S}$ of size *less* than $t\theta_{n-1}$ if $P \notin \mathcal{S}$ and on every line through P there are at *most* t points of $\mathcal{S}$. The following result appears in [30] for $r = 1$ and $n = 2$, and in [52] for general n.

Result 3.7 *Suppose there exists a hyperplane $\mathcal{H}$ containing exactly i points of $\mathcal{S}$, a set of $t\theta_{n-1} - k$ points in $PG(n, q)$. The number of $(\leq t)$-fold nuclei in $AG(n, q) = PG(n, q) \setminus \mathcal{H}$ is at most $(k + r)(q - 1)$ provided that the binomial coefficient*

$$\binom{-t\theta_{n-1} + k + i}{k + r} \neq 0 \pmod p,$$

for some $r > 0$.

4 Affine blocking sets

A set $\mathcal{S}$ is a *t-fold blocking set with respect to s-dimensional subspaces* if every s-dimensional subspace contains at least t points of $\mathcal{S}$. Some confusion in the definition and notation surrounding blocking sets has arisen in the 1990's and some clarification is required. Historically the term blocking set arises from a "blocking coalition" in game theory. Originally it signified a 1-fold blocking set of lines in the planar (projective) case; hence the term blocking set held no ambiguity.

However, conflicting definitions have appeared in for example [2], [21], [36], [40], [47] which is far from ideal. I propose to use the above definition along with calling a 1-fold blocking set with respect to s-dimensional subspaces a *blocking set with respect to s-dimensional subspaces*, and a t-fold blocking set with respect to 1-dimensional subspaces a *t-fold blocking set*. This is consistent with earlier definitions from [14] and [52].

A *(k,r)-arc* in π_2 or $\mathcal{A}_2$ is a set of k points having at most r points on a line. A $(k,2)$-arc is called a *k-arc*. In $\mathcal{A}_2$ the complement of a (k,r)-arc is a $(q-r)$-fold blocking set with q^2-k points and in π_2 the complement is a $(q+1-r)$-fold blocking set with $q^2+q+1-k$ points.

4.1 Line blocking sets

Consider a set $\mathcal{S}$ of $t\theta_{n-1}+k-1$ points of $\mathrm{AG}(n,q)$. For $\mathcal{S}$ to be a t-fold blocking set is equivalent to saying that every point of $\mathrm{AG}(n,q)\setminus\mathcal{S}$ is a t-fold nucleus. Since $\mathcal{S}$ is contained in $\mathrm{AG}(n,q)$ we can set $i=0$ and apply Result 3.5. The following appears in [4].

Theorem 4.1 *Let $\mathcal{S}$ be a t-fold blocking set of $AG(n,q)$ and let $e(t)$ be maximal such that $p^{e(t)}$ divides t. Then the set $\mathcal{S}$ has at least $(t+1)q^{n-1}-p^{e(t)}$ points.*

Proof Put $k=q^{n-1}-t\theta_{n-2}-p^{e(t)}$ in Result 3.5 and write $t=\gamma p^{e(t)}$ such that p does not divide γ. Consider the binomial coefficient

$$\binom{t\theta_{n-1}+k-1}{k}=\binom{t\theta_{n-1}+k-1}{t\theta_{n-1}-1}=\binom{tq^{n-1}+q(q^{n-2}-1)+q-p^{e(t)}-1}{tq^{n-1}+tq^{n-2}+....+tq+t-1}.$$

A simple application of Lucas' Theorem implies that this binomial coefficient is non-zero (modulo p) 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 (modulo p), and it is non-zero (modulo p) since $\gamma\neq 0 \pmod p$. Hence $\mathcal{S}$ cannot be a t-fold blocking set when $k=q^{n-1}-t\theta_{n-2}-p^{e(t)}$ since $\mathcal{S}$ has at most $k(q-1)$ t-fold nuclei and

$$\begin{aligned} &t\theta_{n-1}+k-1+k(q-1)\\ &=t\theta_{n-1}+kq-1\\ &=(q^{n-1}-t\theta_{n-2}-p^{e(t)})q+t\theta_{n-1}-1\\ &=q^n+t-p^{e(t)}q-1<q^n.\end{aligned}$$

This theorem brings together several bounds: for general t and q and $n = 2$, Bruen [21]; for $(t, q) = 1$ and $n = 2$, Blokhuis [14]; and for $(t, q) = 1$ and $n > 2$, Sziklai [52]. The bound is sharp in the planar case $n = 2$ in some cases. The following infinite families are good examples.

1. (Mason [41]) 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 $e(t) = m$.

2. (Denniston [28]) 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 $e(t) = m$.

3. (Barlotti [10]) 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 $e(t) = 0$.

4.2 Hyperplane blocking sets

J. Doyen[29] conjectured that an affine blocking set in $\mathrm{AG}(2, q)$ has at least $2q - 1$ points. This was proven by Jamison [38] and independently by Brouwer and Schrijver [19]. Generalising these methods, Bruen [21] proved the following.

Result 4.2 *Let $\mathcal{S}$ be a t-fold blocking set with respect to hyperplanes of $AG(n, q)$. Then $\mathcal{S}$ has at least $(n + t - 1)(q - 1) + 1$ points.*

In the case $n = 2$ this is a weak version of Result 4.1 and in most cases when $n > 2$ this bound can also be improved. For small t there is the following which is from [5].

Result 4.3 *For $t < q$ a t-fold blocking set with respect to hyperplanes in $AG(n, q)$ has at least $(t + n - 1)(q - 1) + k$ points provided there exists a j such that $k - 1 \leq j < t$ and the binomial coefficient*

$$\binom{k-n-t}{j} \neq 0 \pmod{p}.$$

5 Non-Desarguesian planes

Owing to their lack of regularity, polynomials seem hard to use for tackling problems in non-Desarguesian planes. To my knowledge there are no examples where they have been used. This section outlines a model for translation planes of order q^2 by way of an example of how polynomials might be used. Section 6 considers how such a model can be used to construct maximal arcs.

5.1 Spreads of $\mathrm{PG}(3,q)$

A *1-spread* of $\mathrm{PG}(3,q)$ is a collection of q^2+1 lines that partitions the space. Consider the model for $\mathrm{PG}(3,q)$ described in Section 2. As points we have the (q^3+q^2+q+1)-th roots of unity (or alternatively the non-zero $(q-1)$-th powers) in $\mathrm{GF}(q^4)$. Hyperplanes (planes) are given by the zeros of equations of the form

$$a^{q^2+q+1}x^{q^2+q+1}+a^{q+1}x^{q+1}+ax+1=0,$$

where a is also a (q^3+q^2+q+1)-th root of unity. Lines are given by the zeros of polynomials of the form

$$L_{\alpha\beta}(x):=x^{q+1}-\alpha x+\beta,$$

where α and β satisfy certain condition which we shall calculate. All the points of $\mathrm{PG}(3,q)$ satisfy $x^{q^3+q^2+q+1}-1=0$ and so

$$L^{q^2}_{\alpha\beta}x^{q+1}-(x^{q^3+q^2+q+1}-1)+\alpha^{q^2}xL^{q}_{\alpha\beta}-(\beta^{q^2}-\alpha^{q^2+q})L_{\alpha\beta}$$

$$=(\alpha^{q^2}\beta^{q}+\alpha\beta^{q^2}-\alpha^{q^2+q+1})x-(\beta^{q^2+1}-\alpha^{q^2+q}\beta-1)$$

is identically zero since it is a polynomial of degree at most 1 and has $q+1$ distinct zeros corresponding to the points on the line $L_{\alpha\beta}$. By manipulating the coefficients of the right-hand side we have that $L_{\alpha\beta}$ is a line of $\mathrm{PG}(3,q)$ precisely when

$$\beta^{q^3+q^2+q+1}=1 \quad \text{and} \quad \alpha^{q+1}=\beta^{q}-\beta^{q^2+q+1}. \tag{3}$$

If $\beta^{q^2+1}=1$ then $\alpha=0$ and if $\beta^{q^2+1}\neq 1$ then there are $q+1$ possibilities for α. This gives $(q^3+q)(q+1)+q^2+1=(q^2+1)(q^2+q+1)$ lines, so these restrictions are sufficient as well as necessary.

5.2 Translation planes

Given a 1-spread of $\mathrm{PG}(3,q)$ one can construct a translation plane of order q^2 via the construction of André [1] and Bruck and Bose [20]. Consider a hyperplane Σ of $\mathrm{PG}(4,q)$ and let $\mathcal{S}$ be a 1-spread of Σ. The following incidence structure is a translation plane $\pi(\mathcal{S})$ of order q^2.

Let points of $\mathrm{PG}(4,q)\setminus\Sigma$ be points of $\pi(\mathcal{S})$ together with the q^2+1 spread elements of $\mathcal{S}$. The lines of $\pi(\mathcal{S})$ are the planes of $\mathrm{PG}(4,q)$ meeting Σ in an (spread) element of $\mathcal{S}$, together with a line l_∞ consisting of points that are elements of $\mathcal{S}$. The incidence relation of $\pi(\mathcal{S})$ is induced by incidence in $\mathrm{PG}(4,q)$.

Given a spread $\mathcal{S}$ let (α_i,β_i) for $i=1,\dots,q^2+1$ be such that the zeros of the polynomials $x^{q+1}-\alpha_i x+\beta_i$ correspond to the lines of $\mathcal{S}$, those zeros coming from the non-zero $(q-1)$-th powers in $\mathrm{GF}(q^4)$. We put $x=X^{q-1}$ and multiply through by X to recover the polynomial whose zeros correspond to a plane of $\mathrm{AG}(4,q)$. This plane together with its translations give the lines of $\pi(\mathcal{S})$; that is, the plane and its translations are given by the zeros in $\mathrm{GF}(q^4)$ of equations of the form

$$X^{q^2} - \alpha_i X^q + \beta_i X + \gamma = 0$$

together with a point P_i on l_∞ corresponding to the spread element given by the pair (α_i, β_i). One can verify that γ satisfies the equation $\gamma^{q^2} - \alpha_i^{q^2}\gamma^q - \beta_i^{-1}\gamma = 0$, and the q^2 solutions for γ together with l_∞ give the q^2+1 lines through the point P_i.

5.3 Symplectic spreads

For every point λ of $\mathrm{PG}(3,q)$, viewed as a (q^3+q^2+q+1)-th root of unity in $\mathrm{GF}(q^4)$, let

$$\omega_\lambda(x) := (-\lambda^{q^2})^{q^2+q+1}x^{q^2+q+1} + (-\lambda^{q^2})^{q+1}x^{q+1} + (-\lambda^{q^2})x + 1$$

be a polynomial over $\mathrm{GF}(q^4)$ whose zeros correspond to the points of a hyperplane. It is easy to verify that

$$\omega_\lambda(\epsilon)\lambda^{q+1} = \omega_\epsilon(\lambda)\epsilon^{q+1} \quad \text{and} \quad \omega_\lambda(\lambda) = 0$$

and it follows from this that ω defines a symplectic polarity on $\mathrm{PG}(3,q)$, see Dembowski [27, pp. ??]. The planes $\omega_\lambda(x)$ and $\omega_\epsilon(x)$ intersect in the line given by the zeros of the equation

$$x^{q+1} + \epsilon\lambda\frac{(\lambda^{q+1}-\epsilon^{q+1})^q}{\lambda-\epsilon}x + \frac{\epsilon\lambda^{q+1}-\epsilon^{q+1}\lambda}{\epsilon-\lambda} = 0.$$

The line joining the points λ and ϵ is given by the zeros of the polynomial $x^{q+1} - \alpha x + \beta = 0$ where

$$\alpha = \frac{\lambda^{q+1}-\epsilon^{q+1}}{\lambda-\epsilon} \quad \text{and} \quad \beta = \frac{\lambda^{q+1}\epsilon - \epsilon^{q+1}\lambda}{\lambda-\epsilon}.$$

The two lines coincide whenever $\alpha^q\beta = -\alpha$ and the lines for which this condition hold are the totally isotropic lines, again see Dembowski [27, pp. 41].

A *symplectic 1-spread* is a spread whose elements are totally isotropic and a translation plane arising from a symplectic 1-spread is called a *symplectic translation plane*.

6 Maximal arcs

Recall that a (k,r)-arc in π_2 is a set $\mathcal{K}$ of k points with at most r points on a line. A line through a point $P \in \mathcal{K}$ has at most $r-1$ other points of $\mathcal{K}$

and therefore $k \leq (r-1)(q+1)+1 = rq-q+r$. If equality occurs then $\mathcal{K}$ is called a *maximal arc*. It follows that each line has either 0 or r points of a maximal arc. The *degree* of a maximal arc is r and the dual of the external lines to a maximal arc in π_2 is a maximal arc of degree q/r in the plane dual to π_2.

6.1 Constructions for q even

In PG$(2,q)$, q even, R. H. F. Denniston constructed maximal arcs for all r dividing q [28]. Following this, J. A. Thas [55] constructed maximal arcs in certain symplectic translation planes from ovoids in PG$(3,q)$, see [43] for a survey on ovoids in PG$(3,q)$. In [31], [32] and [33] N. Hamilton proved that the construction of Thas works in derived dual translation planes. N. Hamilton and C. Quinn [35] constructed maximal arcs from m-systems of polar spaces incorporating both the constructions by J. A. Thas [55, 56]. For details on m-systems and partial m-systems see [51].

6.2 A construction of maximal arcs using polynomials

Theorem 6.1 *For q even, the distinct zeros of the polynomial*

$$M(x) := Tr_{q^2 \to 2}(x^{q^2+1}) = x^{q^2+1} + x^{2(q^2+1)} + x^{4(q^2+1)} + ... + x^{(q^2/2)(q^2+1)}$$

in GF(q^4) form a maximal arc of degree $q^2/2$ in the translation plane of order q^2 arising from a symplectic 1-spread via the construction of André [1] and Bruck and Bose [20].

Proof Firstly let us prove that $M(x)$ has the correct number of distinct zeros in GF(q^4).

$$M(x)^2 + M(x) = x^{q^4+q^2} + x^{q^2+1} = x^{q^2}(x + x^{q^4})$$

and hence $M(x)/x^{q^2}$ divides $x+x^{q^4}$ and is therefore fully reducible into distinct linear factors over GF(q^4). Thus it has exactly $(q^2/2)(q^2+1)-q^2$ distinct zeros.

Secondly we have to prove that the distinct zeros of $M(x)$ have at most $q^2/2$ points on any line. This is sufficient by a simple counting argument; we do not need to prove equality. Any line of a translation plane of order q^2 is given by the zeros of polynomials of the form

$$L_{\alpha\beta\gamma}(x) := x^{q^2} - \alpha x^q + \beta x + \gamma.$$

We continue by reducing the polynomial $M(x)$ modulo $L_{\alpha\beta\gamma}(x)$. The characteristic is 2.

$$M(x) = Tr_{q^2 \to 2}(x(\alpha x^q + \beta x + \gamma)) \pmod{L_{\alpha\beta\gamma}}$$

$$= \sum_{i=0}^{h-1} \alpha^{2^i q} x^{2^i q}(\alpha^{2^i} x^{2^i q} + \beta^{2^i} x^{2^i} + \gamma^{2^i}) + \beta^{q^2/2}(\alpha x^q + \beta x + \gamma) + \alpha^{q/2} x^{q^2/2+q/2}$$

$$+ \quad \text{terms of degree at most } q^2/2 \pmod{L_{\alpha\beta\gamma}}$$
$$= (\alpha^{q^2/2}\beta^{q/2} + \alpha^{q/2})x^{q^2/2+q/2} + \quad \text{terms of degree at most } q^2/2 \pmod{L_{\alpha\beta\gamma}}.$$

Hence we have that for translation planes at most $q^2/2 + q/2$ of the distinct zeros of $M(x)$ lie on a line. Moreover if the corresponding spread is symplectic, $(\alpha^{q^2/2}\beta^{q/2} + \alpha^{q/2}) = (\alpha^q\beta + \alpha)^{q/2} = 0$, at most $q^2/2$ of the distinct zeros of $M(x)$ lie on a line. We have to check that this polynomial is not identically zero; this would imply that the the zeros of $M(x)$ contain all of the points on the line $L_{\alpha\beta\gamma}(x)$. However, the constant term in this reduction is

$$\gamma(\alpha^{q+1} + \beta^q)^{q/2} = \gamma\beta^{q/2(q^2+q+1)}$$

by (3) and the coefficient of x is

$$\gamma + \beta^{q^2/2+1} + \beta\alpha^{q^2/2+q/2} = \gamma + \beta^{q/2(q^2+q+1)},$$

again by (3). If both these are zero then $\alpha = \beta = \gamma = 0$ which is ridiculous.

This construction can be extended insofar as for each subfield $\mathrm{GF}(2^r)$ of $\mathrm{GF}(q^2)$ the distinct zeros of $\mathrm{Tr}_{q^2\to 2^r}(x^{q^2+1})$ form a maximal arc of degree $q^2/2^r$ in the translation plane of order q^2 arising from a symplectic 1-spread. The proof is similar but involves slightly more calculations. N. Hamilton [34] pointed out that this construction yields the maximal arcs constructed by J. A. Thas [56].

6.3 Non-existence for q odd

The non-existence of maximal arcs in Desarguesian planes was a conjecture dating back to the 1960's. Cossu [26] proved the initial case $(r, q) = (3, 9)$ and J. A. Thas [57] proved non-existence for $(r, q) = (3, 3^h)$. The conjecture was proven initially in [6], but a shorter proof is given in [7].

Let us consider a sketch of the proof. For $\mathcal{S}$ a maximal $(rq - q + r, r)$-arc in $\mathrm{AG}(2, q)$, we consider $\mathcal{S}$ as elements of $\mathrm{GF}(q^2)$ as in Section 2. The polynomial $F(u, x)$ defined there will then have the property

$$F(u, x_0) = (1 - u^{q+1})^{r-1}$$

whenever $1/x_0$ is an element of $\mathcal{S}$. This follows since every line through a point of the maximal arc has exactly $r - 1$ other points of $\mathcal{S}$ on it. The coefficient in $F(u, x)$ of u^r is $\chi_r(x)$, a polynomial of degree at most $r(q - 1)$ by definition. This polynomial is divisible by the locator polynomial $S(x)$ since $\chi_r(x_0) = 0$ for all $1/x_0 \in \mathcal{S}$. However, $\chi_r(0) = \binom{rq-q+r}{r} = 1$, so clearly χ_r cannot be identically zero. After some calculations one can show that not only S divides χ_r but S^{p-1} divides χ_r as well. This then implies that χ_r has more zeros than its degree whenever $p > 2$ and is therefore identically zero, a contradiction which implies that maximal arcs do not exist in Desarguesian planes.

The only non-existence results for non-Desarguesian planes come from the exhaustive computer searches of T. Penttila and G. Royle [46] who searched all planes of order 9, and A. Blokhuis, N. Hamilton and H. Wilbrink [15] who showed that Thas' constructions [55, 56] do not extend to odd order planes.

6.4 Incompleteness results

The method used in [6] and [7] can be extended to show that large (k, r) arcs in $\mathrm{PG}(2, q)$ can be extended to maximal arcs whenever (necessarily) r divides q. In the case q is odd this simply extends the non-existence to smaller arcs. More precisely we have the following, which appears in [8].

Result 6.2 *Let $\mathcal{S}$ be a $(rq - q + r - \varepsilon, r)$-arc in $PG(2, q)$ where r divides q.*

1. *(q even.) For $\varepsilon < r/2$ and $q/r > 2$ or $\varepsilon < .381r$ and $q/r = 2$, $\mathcal{S}$ can be extended uniquely to some maximal arc containing $rq - q + r$ points.*

2. *(q odd.) If $q/r > 3$ then $\varepsilon > r/2$ and if $q/r = 3$ then $\varepsilon > .476r$.*

In what is essentially also a polynomial proof, although involving some basic properties of algebraic curves, Szőnyi [54] proved the following.

Result 6.3 *Let $\mathcal{S}$ be a $(pq - q + p - \varepsilon, p)$-arc in $PG(2, q)$. Then for q odd $\varepsilon > q^{1/4}/2$.*

7 Unitals

A *unital* in π_2 of square order q is a set $\mathcal{U}$ of $q\sqrt{q}+1$ points, such that each line meets it in either 1 or $\sqrt{q}+1$ points. A line is a *tangent* or a *secant* of $\mathcal{U}$ if it contains 1 or $\sqrt{q}+1$ points of $\mathcal{U}$ respectively. A point P of $\mathcal{U}$ lies on one tangent and q secants, while a point Q not on $\mathcal{U}$ lies on $\sqrt{q}+1$ tangents and $q - \sqrt{q}$ secants. It follows that $\mathcal{U}$ has $q\sqrt{q}+1$ tangents and $q^2 - q\sqrt{q} + q$ secants, and that the set of tangents of $\mathcal{U}$ form a dual unital in the dual plane.

7.1 Unitals in PG$(2, q)$

An example of a unital in $\mathrm{PG}(2, q)$ is given by the set of absolute points of a unitary polarity (see Hirschfeld [37, pp. 36–37]). This is called a *classical unital* (or *Hermitian curve*), and any classical unital is the image under an element of $P\Gamma L(3, q)$ of the set of points (x_0, x_1, x_2) satisfying the equation

$$x_0^{\sqrt{q}+1} + x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} = 0.$$

In 1976, F. Buekenhout [24] proved the existence of unitals in every translation plane π of square order q with kernel containing $\mathrm{GF}(\sqrt{q})$. In particular, he noted that his construction gave a family of non-classical unitals in $\mathrm{PG}(2, q)$

for $\sqrt{q} > 2$ even and not a square. R. Metz [42], in 1979, extended this observation to the case of $\sqrt{q}$ even and square, and $\sqrt{q}$ odd; hence, for any prime power $\sqrt{q} > 2$, there exist non-classical unitals in $\mathrm{PG}(2,q)$. A *Buekenhout–Metz unital* in π is a unital which arises by the construction due to Buekenhout [24, Section 4., Remark (4)]. Since the classical unital in $\mathrm{PG}(2,q)$ can be constructed in this way, it is included in the class of Buekenhout–Metz unitals.

The following characterisation of Buekenhout-Metz unitals comes from [25, 48].

Result 7.1 *Let $\mathcal{U}$ be a unital in $PG(2,q)$, where q is square. Then $\mathcal{U}$ is a Buekenhout–Metz unital if and only if there exists a point T of $\mathcal{U}$ such that the points of $\mathcal{U}$ on each of the q secants to $\mathcal{U}$ through T form a Baer subline.*

There are many other characterisations of Buekenhout-Metz and classical unitals in $\mathrm{PG}(2,q)$. However, the classification appears to be a very hard problem and still somewhat out of reach. It may well be that all unitals embeddable in $\mathrm{PG}(2,q)$ are Buekenhout–Metz unitals. The following result again uses the application of the polynomials in Section 2 and appears in [9].

Result 7.2 *Let $\mathcal{U}$ be a unital in $PG(2,q)$, where $q = p^2$ and p is a prime. Then $\mathcal{U}$ is a classical unital if and only if it admits at least $(q-2)\sqrt{q}$ Baer sublines among its secants.*

7.2 Partial unitals

A *partial unital* is a $(k, \sqrt{q}+1)$-arc $\mathcal{X}$ such that each point of $\mathcal{X}$ lies on a tangent. It would be useful to know (and we are a long way from knowing) how large a partial unital can be, such that it is not part of a unital, i.e. cannot be extended to a unital. The current bound which appears in [3] and applies only to $\mathrm{PG}(2,q)$ again uses the polynomials from Section 2.

Result 7.3 *A partial unital $\mathcal{X}$ in $PG(2,q)$ with*

$$q\sqrt{q} + 1 - \sqrt{q} < |\mathcal{X}| < q\sqrt{q} + 1$$

can be extended to a unital.

There is no evidence that this is the right lower bound however. Indeed, the only construction that I know for a partial unital that cannot be extended to a unital is the following. Let $\mathcal{U}$ be a unital and P a point not in the unital. If we remove a point of $\mathcal{U}$ on each of the lines through P and add the point P, the remaining $q\sqrt{q} - q + 1$ points form a partial unital and one can verify that this cannot be extended to a larger partial unital.

Acknowledgements

I thank Aart Blokhuis, Nick Hamilton, Dieter Jungnickel, Michel Lavrauw and Tamas Szőnyi for their helpful comments during the preparation of this paper.

References

[1] J. André, Über nicht-Desarguessche Ebenen mit transitiver Translationgruppe, *Mathematische Zeitschrift*, **60** (1954), 156–186.

[2] S. Ball, Multiple blocking sets and arcs in finite planes, *Journal of the London Mathematical Society*, **54** (1996), 581–593.

[3] S. Ball, Partial unitals and related structures in Desarguesian planes, *Designs, Codes and Cryptography*, **15** (1998), 231–236.

[4] S. Ball, On nuclei and blocking sets in Desarguesian spaces, *Journal of Combinatorial Theory, Series A*, to appear.

[5] S. Ball, On intersection sets in Desarguesian affine spaces, preprint.

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

[7] S. Ball & A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proceedings of the American Mathematical Society*, **126** (1998), 3377–3380.

[8] S. Ball & A. Blokhuis, On the incompleteness of (k, n)-arcs in Desarguesian planes of order q where n divides q, *Geometriae Dedicata*, to appear.

[9] S. Ball, A. Blokhuis & C. M. O'Keefe, Unitals with many Baer sublines, *Designs, Codes and Cryptography*, to appear.

[10] A. Barlotti, *Some topics in finite geometrical structures*, Institute of Statistics, University of California, mimeo series 439 (1965).

[11] A. Blokhuis, Extremal problems in finite geometries, *Bolyai Society Mathematical Studies*, **3** (1991), 111–135.

[12] A. Blokhuis, Polynomials in finite geometries and combinatorics, in *Surveys in Combinatorics* (eds. K. Walker), *London Mathematical Society Lecture Note Series*, 187, Cambridge University Press, Cambridge (1993), pp. 35–52.

[13] A. Blokhuis, On nuclei and affine blocking sets, *Journal of Combinatorial Theory, Series A*, **67** (1994), 273–275.

[14] A. Blokhuis, On multiple nuclei and a conjecture of Lunelli-Sce, *Bulletin of the Belgian Mathematical Society*, **3** (1994), 349–353.

[15] A. Blokhuis, N. Hamilton & H. Wilbrink, The non-existence of Thas maximal arcs in translation planes of odd order, *European Journal of Combinatorics*, **19** (1998), 413–417.

[16] A. Blokhuis & F. Mazzocca, On maximal sets of nuclei in $\mathrm{PG}(2, q)$ and quasi-odd sets in $\mathrm{AG}(2, q)$, in *Advances in Finite Geometries and Designs* (eds. J. W. P. Hirschfeld, D. R. Hughes & J. A. Thas), Oxford University Press, Oxford New York Tokyo (1991), pp. 27–34.

[17] A. Blokhuis & F. Mazzocca, Special point sets in $\mathrm{PG}(n, q)$ and the structure of sets with the maximal number of nuclei, *Journal of Geometry*, **41** (1991), 33–41.

[18] A. Blokhuis & H. A. Wilbrink, A characterization of exterior lines of certain sets of points in $\mathrm{PG}(2, q)$, *Geometriae Dedicata*, **23** (1987), 253–254.

[19] A. E. Brouwer & A. Schrijver, The blocking number of an affine space, *Journal of Combinatorial Theory, Series A*, **24** (1978), 251–253.

[20] R. H. Bruck & R. C. Bose, Linear representations of projective planes in projective spaces, *Journal of Algebra*, **1** (1966), 117–172.

[21] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *Journal of Combinatorial Theory, Series A*, **60** (1992), 19–33.

[22] A. A. Bruen & J. C. Fisher, The Jamison method in Galois geometries, *Designs, Codes and Cryptography*, **1** (1991), 199–205.

[23] A. A. Bruen & J. A. Thas, Flocks, chains and configurations in finite geometries, *Atti della Accademia dei Lincei*, **59** (1975), 744–748.

[24] F. Buekenhout, Existence of unitals in finite translation planes of order q^2 with a kernel of order q, *Geometriae Dedicata*, **5** (1976), 189–194.

[25] L. R. A. Casse, C. M. O'Keefe & T. Penttila, Characterizations of Buekenhout–Metz Unitals, *Geometriae Dedicata*, **59** (1996), 29–42.

[26] A. Cossu, Su alcune proprietà dei $\{k; n\}$-archi di un piano proiettivo sopra un corpo finito, *Rendiconti di Matematica e delle sue Applicazioni*, **20** (1961), 271-277.

[27] P. Dembowski, *Finite Geometries*, Springer, Berlin (1968).

[28] R. H. F. Denniston, Some maximal arcs in finite projective planes, *Journal of Combinatorial Theory*, **6** (1969), 317–319.

[29] J. Doyen, Lecture at Oberwolfach, 1976.

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

[31] N. Hamilton, Some maximal arcs in derived dual Hall planes, *European Journal of Combinatorics*, **15** (1994), 525–532.

[32] N. Hamilton, Some inherited maximal arcs in derived dual translation planes, *Geometriae Dedicata*, **55** (1995), 165–173.

[33] N. Hamilton, Some maximal arcs in Hall planes, *Journal of Geometry*, **52** (1995), 101–107.

[34] N. Hamilton, Personal communication, 1998.

[35] N. Hamilton & C. Quinn, m-systems of polar spaces and maximal arcs in projective planes, *Bulletin of the Belgian Mathematical Society*, submitted.

[36] U. Heim, Proper blocking sets in projective spaces, *Discrete Mathematics*, **174** (1994), 167–176.

[37] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second edition, Oxford University Press, New York (1998).

[38] R. Jamison, Covering finite fields with cosets of subspaces, *Journal of Combinatorial Theory, Series A*, **22** (1977), 253–266.

[39] R. Lidl & H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge (1986).

[40] G. Lunardon, Linear k-blocking sets, *Combinatorica*, submitted.

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

[42] R. Metz, On a class of unitals, *Geometriae Dedicata*, **8** (1979), 125–126.

[43] C. M. O'Keefe, Ovoids of $\mathrm{PG}(3, q)$: a survey, *Discrete Mathematics*, **151** (1996), 175-188.

[44] O. Ore, On a special class of polynomials, *Transactions of the American Mathematical Society*, **35** (1933), 559–584.

[45] O. Ore, Contributions to the theory of finite fields, *Transactions of the American Mathematical Society*, **36** (1934), 243–274.

[46] T. Penttila & G. Royle, Sets of type (m, n) in the affine and projective planes of order nine, *Designs, Codes and Cryptography*, **6** (1995), 229–245.

[47] P. Polito & O. Polverino, Small blocking sets, *Combinatorica*, **18** (1998), 133–137.

[48] C. Quinn & L. R. A. Casse, Concerning a characterisation of Buekenhout-Metz unitals, *Journal of Geometry*, **52** (1995), 159–167.

[49] B. Segre, Ovals in a finite projective plane, *Canadian Journal of Mathematics*, **7** (1955), 414–416.

[50] B. Segre & G. Korchmáros, Una proprietà degli insiemi di punti di un piano di Galois caratterizzante quelli formati dei punti delle singole rette esterne ad una conica, *Atti della Accademia dei Lincei*, **62** (1977), 613–619.

[51] E. E. Shult & J. A. Thas, m-systems and partial m-systems of polar spaces, *Designs, Codes and Cryptography*, **8** (1996), 229–238.

[52] P. Sziklai, Nuclei of point sets in PG(n, q), *Discrete Mathematics*, **174** (1997), 323–327.

[53] T. Szőnyi, Some applications of algebraic curves in finite geometry and combinatorics, in *Surveys in Combinatorics* (ed. R. A. Bailey), *London Mathematical Society Lecture Note Series*, 241, Cambridge University Press, Cambridge (1997), pp. 197–236.

[54] T. Szőnyi, On the embeddability of (k, p)-arcs, *Designs, Codes and Cryptography*, submitted.

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

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

[57] 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, *Journal of Combinatorial Theory, Series A*, **19** (1975), 228–232.

Discrete Wiskunde
Technical University of Eindhoven
Den Dolech 2
5600 MB Eindhoven
The Netherlands
`simeon@win.tue.nl`