COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA 17 (1) (1997) 31–41

MAXIMAL ARCS IN DESARGUESIAN PLANES OF ODD ORDER DO NOT EXIST

SIMEON BALL, AART BLOKHUIS and FRANCESCO MAZZOCCA*

Received January 29, 1996

For q an odd prime power, and $1<n<q$, the Desarguesian plane $PG(2,q)$ does not contain an $(nq-q+n,n)$-arc.

1. Introduction

A $(k,n)-$*arc* in a projective plane is a set of k points, at most n on every line. If the order of the plane is q, then $k \le 1+(q+1)(n-1) = qn-q+n$ 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 Desarguesian projective planes, are the hyperovals ($n=2$), and, for $n>2$ the Denniston arcs [2] and an infinite family constructed by Thas [5, 7]. These exist for all pairs $(n,q)=(2^a,2^b)$, $0<a<b$. It is conjectured in [6] 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 [1]. In a recent paper on sets of type (m,n) [3] this conjecture is labeled "most wanted" research problem. In this note we shall show that the conjecture is true in general.

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. The points of $AG(2,q)$ can be identified with the elements of $GF(q^2)$ in a suitable way, so that in fact all point sets can be considered as subsets of this field. Note

Mathematics Subject Classification (1991): 51 E 21, 51 A 30, 05 D 05, 05 B 25

* Supported by Italian M.U.R.S.T. (Research Group on *Strutture geometriche, combinatoria, loro applicazioni*) and G.N.S.A.G.A. of C.N.R.

that three points a, b, c are collinear, precisely when $(a-b)^{q-1} = (a-c)^{q-1}$. If the direction of the line joining a and b is identified with the number $(a-b)^{q-1}$, then a one-to-one correspondence between the $q+1$ directions (or parallel classes) and the different $(q+1)$-st roots of unity in $GF(q^2)$ is obtained.

We finish this introduction with a short discussion on Lucas' theorem and Hasse derivatives.

Lucas' theorem gives the value of binomial coefficients modulo a prime: Let $a = a_0 + a_1p + a_2p^2 + \dots$ and $b = b_0 + b_1p + b_2p^2 + \dots$ be the p-ary expansion of the numbers a and b, where b is a non-negative integer. Then

$$\binom{a}{b} = \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2}\dots \pmod p.$$

This can be proved by expanding $(1+x)^a$ and using $(1+x)^r = 1+x^r$ whenever r is a power of the characteristic p (cf. [4], Section 5).
In particular we have the following,

$$(-1)^i\binom{r-1}{i} = 1 \pmod p \quad \text{for} \quad r = p^e,\ 0 \le i < r,$$

and, more generally

$$(-1)^i\binom{r-j-1}{i} = \binom{i+j}{i} \pmod p \quad \text{for} \quad r = p^e,\ 0 \le i, j < r.$$

Hasse derivatives cope with the problem that over a field of characteristic p the p-th and higher ordinary derivatives of a polynomial vanish identically. The k-th Hasse derivative H_k (with respect to the variable x) is a linear operator on polynomials defined by $H_k(x^n) = \binom{n}{k}x^{n-k}$ if $k \le n$, and 0 otherwise. If f and g are two polynomials then

$$H_n(fg) = \sum_{k=0}^{n} H_k(f)H_{n-k}(g).$$

From this it can be seen that $(x-a)^k \mid f$ if and only if $H_i(f)(a) = 0$ for $i = 0, 1, \dots, k-1$.

2. Some useful polynomials

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 $\mathscr{B}$, in particular $\sigma_k = 0$ for $k > |\mathscr{B}|$. Define the polynomials F in two variables and $\hat{\sigma}_k$ in one variable by

$$F(t,x) := \prod_{b\in\mathscr{B}} (1-(1-bx)^{q-1}t) = \sum_{k=0}^{\infty} (-1)^k \hat{\sigma}_k t^k$$

where $\hat{\sigma}_k$ is the k-th elementary symmetric function of the set of polynomials $\{(1-bx)^{q-1} \mid b \in \mathscr{B}\}$, a polynomial of degree at most $k(q-1)$ in x. Again, $\hat{\sigma}_k$ is the zero polynomial for $k > |\mathscr{B}|$. For $x_0 \in GF(q^2) \setminus \mathscr{B}^{[-1]}$ it follows that $F(t, x_0)$ is an n-th power. Indeed, if $x_0 = 0$ this is clear, and if $x_0 \neq 0$ then $1/x_0$ is a point not contained in the arc, so that every line through $1/x_0$ contains a number of points of $\mathscr{B}$ that is either 0 or n. In the multiset $\{(1/x_0 - b)^{q-1} \mid b \in \mathscr{B}\}$, every element occurs therefore with multiplicity n, so that in $F(t, x_0)$ every factor occurs exactly n times.

For $x_0 \in \mathscr{B}^{[-1]}$ we get that $F(t, x_0) = (1-t^{q+1})^{n-1}$, for in this case every line passing through the point $1/x_0$ contains exactly $n-1$ other points of $\mathscr{B}$, so that the multiset $\{(1/x_0 - b)^{q-1}\}$ consists of every $(q+1)$-st root of unity repeated $n-1$ times, together with the element 0. This gives

$$F(t,x_0) = \prod_{b\in\mathscr{B}} (1-(1/x_0-b)^{q-1}x_0^{q-1}t) = (1-x_0^{q^2-1}t^{q+1})^{n-1} = (1-t^{q+1})^{n-1}.$$

From the shape of F in both cases it can be seen that for all $x_0 \in GF(q^2)$, $\hat{\sigma}_k(x_0) = 0$, $0 < k < n$, and since the degree of $\hat{\sigma}_k$ 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 $\hat{\sigma}_n$.

The main idea of the non-existence proof is to show that $\hat{\sigma}_n^2$ is a p-th power. Together with the fact that B divides $\hat{\sigma}_n$, and the observation that $\hat{\sigma}_n$ is not identically zero, this leads swiftly to a contradiction for $p \neq 2$.

Since $\hat{\sigma}_n(0) = \binom{|\mathscr{B}|}{n} = \binom{nq-q+n}{n} = 1$, by Lucas' theorem, it is not identically zero. On the other hand the coefficient of t^n in $(1-t^{q+1})^{n-1}$ is zero, so $\hat{\sigma}_n(x_0) = 0$ for $x_0 \in \mathscr{B}^{[-1]}$, in other words, B divides $\hat{\sigma}_n$. Let $Q = \hat{\sigma}_n / B$. Then Q is a polynomial of degree at most $n(q-1) - nq + q - n = q - 2n$.

Define the power sums corresponding to σ_k and $\hat{\sigma}_k$:

$$(1) \quad \pi_k = \sum_{b\in\mathscr{B}} b^k \quad \text{and} \quad \hat{\pi}_k = \sum_{b\in\mathscr{B}} (1-bx)^{k(q-1)} = \sum_{i=0}^{k(q-1)} (-1)^i \binom{k(q-1)}{i} \pi_i x^i.$$

For future use we collect the relevant divisibility relations.

Lemma 2.1. *The following polynomials are divisible by* $x - x^{q^2}$*:*

1. $\hat{\sigma}_k$, *unless* $n\,|\,k$ *or* $(q+1)\,|\,k$;
2. $\hat{\sigma}_n\hat{\sigma}_k$, *unless* $n\,|\,k$;
3. $\hat{\pi}_k$, *unless* $(q+1)\,|\,k$;
4. $\hat{\sigma}_n\hat{\pi}_k$ *for all* k.

Proof. Unless $n\,|\,k$ or $(q+1)\,|\,k$, $\hat{\sigma}_k$ vanishes for all $x \in GF(q^2)$, so it follows that in these cases $(x - x^{q^2})\,|\,\hat{\sigma}_k$. If $n \nmid k$ then $\hat{\sigma}_k$ still vanishes for $x_0 \in GF(q^2) \setminus \mathscr{B}^{[-1]}$, and since $B\,|\,\hat{\sigma}_n$ we get the divisibility relation $(x - x^{q^2})\,|\,\hat{\sigma}_n\hat{\sigma}_k$ in this case. For $x_0 \in GF(q^2) \setminus \mathscr{B}^{[-1]}$ it follows that $\hat{\pi}_k(x_0) = 0$, because every value is assumed 0 or n times, and $p\,|\,n$. If $(q+1) \nmid k$ and $x_0 \in \mathscr{B}^{[-1]}$ it follows that

$$\hat{\pi}_k(x_0) = 0 + \left(\sum_{\xi:\xi^{q+1}=1} \xi^k \right) (n-1) = 0.$$

Hence $(x - x^{q^2})\,|\,\hat{\pi}_k$ unless $(q+1)\,|\,k$ and $(x - x^{q^2})\,|\,\hat{\sigma}_n\hat{\pi}_k$ if $(q+1)\,|\,k$ since $B\,|\,\hat{\sigma}_n$. ∎

3. The Newton Identities and some consequences

The power sums π and the symmetric functions σ are related by the Newton identities $N(k)$:

$$k\sigma_k + \sum_{j=0}^{k-1} (-1)^{k-j} \sigma_j \pi_{k-j} = 0,$$

for all $k \geq 0$. These identities can be obtained by computing the derivative of $B(x)$ to get

$$B'(x) = \sum_{b \in \mathscr{B}} \frac{-b}{1-bx} B(x) = \sum_{k=1}^{\infty} (-1)^k k \sigma_k x^{k-1}.$$

and comparing the coefficient of x^k (resp. t^k) after substituting $(1-bx)^{-1} = \sum_{j=0}^{\infty} b^j x^j$.

The Newton identities $\hat{N}(k)$:

$$k\hat{\sigma}_k + \sum_{j=0}^{k-1} (-1)^{k-j} \hat{\sigma}_j \hat{\pi}_{k-j} = 0,$$

can be derived in a similar way, by computing the partial derivative with respect to t of $F(t,x)$.

For all $k \leq q$ the degrees of $\hat{\sigma}_k$ and $\hat{\pi}_k$ are less than q^2 so in view of the divisibility relations $\hat{\pi}_k$ is identically zero for $k \leq q$, and so is $\hat{\sigma}_k$, unless $n|k$. By considering the Newton Identity $\hat{N}(q+1)$ we find that

$$\hat{\sigma}_{q+1} = -\hat{\pi}_{q+1} = -\sum_{j=0}^{q^2-1} \pi_j x^j. \tag{2}$$

by (1). Note that since $\pi_0 = 0$ and $\pi_{k+q^2-1} = \pi_k$ for all $k > 0$, we get that

$$\hat{\pi}_{q+1} = (x - x^{q^2}) \sum_{k=0}^{\infty} \pi_{k+1} x^k.$$

Differentiating $F(t,x)$ with respect to x it follows that

$$F_x(t,x) = \left(\sum_{b \in \mathscr{B}} \frac{-b(1-bx)^{q-2} t}{1-(1-bx)^{q-1} t} \right) F(t,x) = \sum_{k=0}^{|\mathscr{B}|} (-1)^k \hat{\sigma}'_k t^k. \tag{3}$$

The expression in front of $F(t,x)$ may be expanded in a formal power series so that

$$F_x(t,x) = \left(-\sum_{b \in \mathscr{B}} \sum_{i=1}^{\infty} b(1-bx)^{iq-i-1} t^i \right) F(t,x).$$

Expanding the bracket using the Binomial theorem gives

$$F_x(t,x) = -\sum_{i=1}^{\infty} \left[\sum_{k=0}^{iq-i-1} (-1)^k \binom{iq-i-1}{k} \pi_{k+1} x^k \right] t^i \, F(t,x). \tag{4}$$

We already observed that $F(t,x)$ as a function of t is an n-th power modulo t^q, and the same is of course true for $F_x(t,x)$. It follows that the same is again true for

$$-\sum_{b \in \mathscr{B}} \sum_{i=1}^{\infty} b(1-bx)^{iq-i-1} t^i.$$

This gives $\binom{mq-m-1}{k-1} \pi_k = 0$ for $0 < m < q$, $n \nmid m$ and all k. Note that from $\hat{\pi}_m \equiv 0$ for $m < q$ it follows that

$$\binom{mq-m}{k} \pi_k = 0 \quad \text{for} \quad m < q \text{ and all } k. \tag{5}$$

From $\binom{mq-m}{k} = \binom{mq-m-1}{k} + \binom{mq-m-1}{k-1}$ follows the important equality

$$\binom{mq-m-1}{k}\pi_k = 0 \quad \text{for} \quad 0<m<q, \quad n\nmid m \quad \text{and all } k. \tag{6}$$

Equating the coefficient of t^n in (4) implies

$$\hat{\sigma}'_n = \sum_{k=0}^{nq-n-1} (-1)^k \binom{nq-n-1}{k} \pi_{k+1} x^k.$$

From $\hat{\pi}_1 = \sum_{j=0}^{q-1} \pi_j x^j \equiv 0$ it follows that $\pi_j = 0$ for $j < q$. This then implies that $\hat{\sigma}_n$ is a p-th power mod x^q. By considering the Newton identities relating the σ_k's and the π_k's it follows that $\sigma_j = 0$ for $j < q$ unless $p|j$ and hence B is a p-th power mod x^q. Therefore their quotient Q which has degree at most $q-2n$ is a p-th power, i.e. $Q'=0$.

From the proof of the Newton identities it follows that

$$B'(x - x^{q^2}) = -B\hat{\pi}_{q+1}.$$

Multiplying each side by Q and writing $B'Q=(BQ)'=\hat{\sigma}'_n$ this is seen to imply the important identity

$$\hat{\sigma}'_n(x - x^{q^2}) = -\hat{\sigma}_n\hat{\pi}_{q+1}. \tag{7}$$

Our main conclusion, namely that $\hat{\sigma}_n^2$ is a p-th power will follow from considering the Newton identity $\hat{N}(nq-q+2n-1)$ modulo $(x-x^{q^2})^2$. As it will turn out the only relevant $\hat{\pi}$-s involved in this identity will be the $\hat{\pi}_k$ with $k \equiv -1 \bmod n$ and most of these vanish identically. We start by showing that $\hat{\pi}_{an-1} \equiv 0$ for $a \le q - q/n$, and then $\hat{\pi}_{i(q+1)}$ and $\hat{\pi}_{i(q+1)+n}$ will be calculated in terms of Hasse derivatives for $i<n$. In this way in particular $\hat{\pi}_{(n-1)(q+1)}$ and $\hat{\pi}_{(n-1)(q+1)+n}$ are obtained (the last two $\hat{\pi}_{an-1}$'s).

4. Proof that $\hat{\pi}_{an-1} \equiv 0$ for $a \le q - q/n$

Recall that, by definition

$$\hat{\pi}_{an-1} = \sum_{b\in\mathcal{B}} (1-bx)^{(q-1)(an-1)} = \sum_{j=0}^{(an-1)(q-1)} \binom{anq-q-an+1}{j} (-1)^j \pi_j x^j$$

From this expansion, and Lucas' theorem, note that the only exponents j that occur on the left hand side are those with $j=0,1 \bmod n$. Therefore

$$\hat{\pi}_{an-1} = xG_0^n + G_1^n,$$

where G_0 and G_1 are polynomials of degree at most $aq-q/n-a$. We proceed to show that in fact $\hat{\pi}_{an-1} = (x-x^{q^2})G_0^n$. Recall that Lemma 2.1 implies $\hat{\pi}_{an-1}$ is divisible by $x-x^{q^2}$. Indeed, if it is not, then $(q+1)|an-1$, but this implies $a \geq q+1-q/n$. Hence

$$x - x^{q^2} \mid xG_0^n + G_1^n.$$

We now use a trick essentially due to Rédei ([4], Section 33) , and raise the right hand side to the q^2/n-th power, then simplify using the divisibility relation $x-x^{q^2} \mid G_i^{q^2} - G_i$ to obtain

$$x - x^{q^2} \mid x^{q^2/n}G_0 + G_1.$$

The polynomials G_0 and G_1 both have degree at most $aq-q/n-a \leq q^2-q^2/n-q/n-q+q/n$ so the right hand side has degree less than q^2 and therefore is identically zero. So $G_1 = -x^{q^2/n}G_0$ and we have proved that

$$\hat{\pi}_{an-1} = (x - x^{q^2})G_0^n$$

One may check, directly from the definition, that

$$G_1 = \sum_{j=0}^{aq-q/n-a} \binom{aqn - q - an + 1}{jn} \pi_{nj}^{1/n} x^j$$

Note that $\pi_{jn}^{1/n} = \pi_j$ and $\binom{aqn-q-an+1}{jn} = \binom{aq-q/n-a}{j}$ We now proceed to show that in fact $G_1 \equiv 0$. In other words, we want to show that for all j, $\binom{aq-q/n-a}{j} \neq 0$ implies that $\pi_j = 0$.

Define the (cyclic) shift operator s on k with $0 \leq k \leq q^2-1$ by $s(q^2-1) = q^2-1$ and $s(k) = pk \bmod q^2-1$ otherwise. So what s does is cycle the p-ary digits of k. Then it follows immediately from Lucas' theorem that $\binom{u}{v} = \binom{s(u)}{s(v)}$, (for $0 \leq u, v < q^2$). Moreover we have $\pi_{s(u)} = \pi_u^p$ and so $\pi_u = 0$ if and only if $\pi_{s(u)} = 0$. It follows that it is sufficient to prove that

$$\binom{s^{e-h}(aq - q/n - a)}{k} \pi_k = 0$$

for all $k(=s^{e-h}j)$. Here e and h come from $q=p^h$ and $n=p^e$, and the effect of s^{e-h} is essentially dividing by q/n modulo q^2-1. If we write $q-a=\alpha(q/n)+\beta$, with $0\leq\beta<q/n$, then $0<\alpha(<n)$, since $a\leq q-q/n$. Using this we get

$$s^{e-h}(aq-q/n-a)=(a-1)n+\alpha-1+\beta qn=mq-m-1,$$

where $m=\beta n+n-\alpha$. In particular $m<q$ and $m\neq 0 \bmod n$, so that the desired equality is exactly equation (6) from the previous section.

5. Calculation of $\hat{\pi}_{i(q+1)}$ and $\hat{\pi}_{i(q+1)+n}$ for $i<n$

Recall that H_k stands for the k-th Hasse derivative with respect to x. We will write $z=x-x^{q^2}$. Note that by the chain rule $H_k(f(1-x))=(-1)^kH_k(f)(1-x)$.

Lemma 5.1.

$$H_{i-1}\left(\frac{z^i}{x}\right)=1-x^{i(q^2-1)} \quad \textit{for } i\leq q^2.$$

Proof.

$$H_{i-1}\left(\frac{z^i}{x}\right)=H_{i-1}\left(\sum_{j=0}^{i}(-1)^j\binom{i}{j}x^{j(q^2-1)+i-1}\right)$$

$$=\sum_{j=0}^{i}(-1)^j\binom{i}{j}\binom{j(q^2-1)+i-1}{i-1}x^{j(q^2-1)}.$$

But if $0<j<i\leq q^2$, then $\binom{j(q^2-1)+i-1}{i-1}=\binom{i-j-1}{i-1}=0$. ∎

Substituting $1-x$ for x changes z into $-z$ and gives us $H_{i-1}\left(z^i/(1-x)\right)=(1-x)^{i(q^2-1)}-1$. Writing $z/(1-x)=\sum_{j=1}^{q^2-1}x^j$ we see that $H_{i-1}(z^{i-1}x^j)$ is the part of $(1-x)^{i(q^2-1)}-1$ that has exponent $\equiv j \bmod (q^2-1)$ (for $1\leq j\leq q^2-1$). Since $b^j=b^{j+q^2-1}$ for $b\in GF(q^2)$ it follows that

$$\sum_{b\in\mathcal{B}}\left((1-bx)^{i(q^2-1)}-1\right)=\sum_{j=1}^{q^2-1}\pi_jH_{i-1}\left(z^{i-1}x^j\right).$$

Lemma 5.2.

$$\hat{\pi}_{i(q+1)}=H_{i-1}\left(z^{i-1}\hat{\pi}_{q+1}\right).$$

Proof. Since $|\mathscr{B}| \equiv 0 \bmod p$ we may write $\hat{\pi}_{i(q+1)} = \sum_{b\in\mathscr{B}} \left((1-bx)^{i(q^2-1)} - 1\right)$ and the result now follows by using the identity above and the expansion (2) of $\hat{\pi}_{q+1}$. ∎

Lemma 5.3.

$$H_{i-1}\left(z^{i-1}x^{q^2-1+nj}\right) = x^{i(q^2-1)+nj} \quad \text{for } 0 < i \leq n.$$

Proof.

$$H_{i-1}\left(z^{i-1}x^a\right) = \sum_{m=0}^{i-1}(-1)^m\binom{i-1}{m}\binom{m(q^2-1)+i-1+a}{i-1}x^{m(q^2-1)+a}.$$

For $a = q^2-1+nj$ the second binomial coefficient equals $\binom{i-1-m-1}{i-1}$ and only the term with $m = i-1$ gives a non-zero contribution. ∎

Substituting again $1-x$ for x, yields

$$H_{i-1}\left(z^{i-1}(1-x)^{q^2-1+nj}\right) = (1-x)^{i(q^2-1)+nj}.$$

In the same way as before this gives

Lemma 5.4.

$$\hat{\pi}_{i(q+1)+n} = H_{i-1}\left(z^{i-1}\hat{\pi}_{q+1+n}\right).$$

For the special case $i=1$ this does not give anything. This case is settled by

Lemma 5.5.

$$\hat{\pi}_{q+1+n} = z\hat{\sigma}'_n.$$

Proof. Lemma 2.1 says that z divides $\hat{\pi}_{q+1+n}$ and modulo x^{q^2}

$$\hat{\pi}_{q+1+n} - x\hat{\sigma}'_n = \sum_{k=1}^{q^2-1}\left[\binom{n(q-1)-1}{k} + \binom{n(q-1)-1}{k-1}\right](-1)^k\pi_k x^k,$$

but $\binom{n(q-1)}{k}\pi_k = 0$ for all k (5). ∎

6. Proof of the theorem

Let z and H_k be as before. Note for $k<q^2$ and $k\leq m$ that $H_k(z^m)=\binom{m}{k}z^{m-k}$. We will be interested in expressions modulo z^2. In that case $H_k(z^k f)\equiv f+kzf'$ mod z^2 and if f is divisible by z, then $H_k(z^k f)\equiv (k+1)f$ mod z^2.

Consider the Newton identity $\hat{N}(|\mathscr{B}|+n-1)$ (note that $\hat{\sigma}_{|\mathscr{B}|+n-1}\equiv 0$),

$$\sum_{j=1}^{nq-q+2n-1} (-1)^{j-1}\hat{\pi}_j\hat{\sigma}_{(n-1)(q+1)+n-j} \equiv 0$$

Multiplying this equation by $\hat{\sigma}_n$ and considering the terms modulo z^2, the divisibility relations in Lemma 2.1, together with the fact that $\hat{\pi}_{an-1}\equiv 0$ for $a\leq q-q/n$ imply

$$\hat{\sigma}_n\hat{\pi}_{(n-1)(q+1)+n} - \hat{\sigma}_n^2\hat{\pi}_{(n-1)(q+1)} \equiv 0 \pmod{z^2}.$$

Using the results of the previous section it follows that $\hat{\pi}_{(n-1)(q+1)} = \hat{\pi}_{q+1} + (n-2)z\pi'_{q+1}$ mod z^2 and $\hat{\pi}_{(n-1)(q+1)+n}=(n-1)z\hat{\sigma}'_n$ mod z^2. Since $n\equiv 0$ mod p,

$$-z\hat{\sigma}'_n\hat{\sigma}_n - \hat{\pi}_{q+1}\hat{\sigma}_n^2 + 2z\hat{\pi}'_{q+1}\hat{\sigma}_n^2 \equiv 0 \pmod{z^2}.$$

The first two terms cancel since $z\hat{\sigma}'_n=-\hat{\pi}_{q+1}\hat{\sigma}_n$ (7). The third term can be reduced using the same expression and its derivative

$$\hat{\pi}'_{q+1}\sigma_n = -\hat{\pi}_{q+1}\hat{\sigma}'_n - \hat{\sigma}'_n \pmod{z}$$

to give $2z\hat{\sigma}'_n\hat{\sigma}_n$ mod z^2. Therefore

$$\left(\hat{\sigma}_n^2\right)' \equiv 0 \pmod{z}.$$

Since the degree of $\hat{\sigma}_n$ is at most $n(q-1)$ it follows that $\left(\hat{\sigma}_n^2\right)'\equiv 0$.

Now $\hat{\sigma}_n=BQ$, and Q is a p-th power, so $\left(B^2\right)'\equiv 0$. Hence B^2 is a p-th power. For $p\neq 2$ this implies that B is a p-th power which is a contradiction, since B has $qn-q+n$ distinct linear factors.

Acknowledgement. The authors wish to thank Andries Brouwer for carefully reading the manuscript and simplifying parts of the proof.

References

[1] 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.

[2] R. H. F. DENNISTON: Some maximal arcs in finite projective planes, *J. Combin. Theory*, **6** (1969), 317–319.

[3] T. PENTTILA AND G. F. ROYLE: Sets of Type (m, n) in the Affine and Projective Planes of Order Nine, *Designs, Codes and Cryptography*, **6** (1995), 229–245.

[4] L. RÉDEI: Lückenhafte Polynome über endlichen Körpern, Birkhäuser Verlag, Basel (1970) (English translation: Lacunary polynomials over finite fields, North Holland, Amsterdam, 1973).

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

[6] 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.

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

Simeon Ball

Techn. University Eindhoven,
P.O. Box 513, 5600 MB Eindhoven,
The Netherlands
simeon@win.tue.nl

Aart Blokhuis

Techn. University Eindhoven,
P.O. Box 513, 5600 MB Eindhoven,
The Netherlands
aartb@win.tue.nl

Francesco Mazzocca

Seconda Università degli Studi di Napoli,
Piazza Duomo, c/o Curia Vescovile,
81100 Caserta, Italy
mazzocca@napoli.infn.it