On the incompleteness of (k, n)-arcs in Desarguesian planes of order q where n divides q

Simeon Ball *Aart Blokhuis*
Technische Universiteit Eindhoven,
Postbox 513, 5600 MB Eindhoven,
The Netherlands

simeon@win.tue.nl
aartb@win.tue.nl

Abstract

We investigate the completeness of an $(nq - q + n - \varepsilon, n)$-arc in the Desarguesian plane of order q where n divides q. It is shown that such arcs are incomplete for $0 < \varepsilon \leq n/2$ if $q/n > 3$. For $q = 2n$ they are incomplete for $0 < \varepsilon < .381n$ and for $q = 3n$ they are incomplete for $0 < \varepsilon < .476n$. For q odd it is known that such arcs do not exist for $\varepsilon = 0$ and hence we improve the upper bound on the maximum size of such a (k, n)-arc.

Mathematics Subject Classification numbers
05B25 51E15 51E21

Key words
Maximal arcs, arcs, finite Desarguesian planes.

1. Introduction

A $(k, n)-$*arc* in a projective plane is a set of k points, at most n on every line. A (k, n)-arc is called *complete* if it cannot be extended to a $(k + 1, n)$-arc. If the order of the plane is q, then $k \leq 1 + (q+1)(n-1) = qn - q + n$ 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 Desarguesian projective planes, are the hyperovals ($n = 2$), and, for $n > 2$ the Denniston arcs [4] and an infinite family constructed by Thas [8, 10]. The Denniston arcs exist for all pairs $(n, q) = (2^a, 2^b)$, $0 < a < b$.

Maximal arcs do not exist in Desarguesian planes of odd order, The case $(n, q) = (3, 9)$ was proved by Cossu [3] and Thas [9] proved the cases $(n, q) = (3, 3^h)$. A general proof first appeared in [1] although a more accessible version of the proof appears in [2] and [5]. The techniques used in [1, 2] depend strongly on the properties of certain polynomials over finite fields. We shall again be using such techniques.

In this paper we show that a $(nq-q+n-\varepsilon,n)$-arc in $PG(2,q)$, $n<q/3$ is incomplete for $0<\varepsilon\leq n/2$ and any such arc can therefore be completed to a maximal arc. For q odd this implies immediately that the maximal size of a (k,n)-arc, denoted $m_n(2,q)$ in other literature (see [6]), for $n|q$ is less than $nq-q+n/2$.

At this point we compare our result to the work of Szőnyi [7]. Although his work is still in progress it is interesting to note the different bounds achieved using different techniques. His algebraic geometric approach gives a bound on epsilon of $cq^{1/4}$. In other words, a $(nq-q+n-\varepsilon,n)$-arc is incomplete for $\varepsilon<cq^{1/4}$. It follows that for $n/2<cq^{1/4}$ his bound is better, since we would like ε as large as possible. However, reversing the inequality clearly implies the opposite.

2. Some counting and some conclusions

Let $\mathcal{B}$ be a $(nq-q+n-\varepsilon,n)$-arc in $PG(2,q)$ where $n/2>\varepsilon>0$. Counting the number of points of $\mathcal{B}$ on the lines passing through a point of $\mathcal{B}$ we immediately get that a line with at least one point of B in fact has at least $n-\varepsilon$ points. Using this, the standard counting arguments involving incident (point, line) pairs and (point, point, line) triples gives that there will be lines missing B (if l_i denotes the number of lines containing precisely i points, then we can compute $\sum l_i$, $\sum il_i$ and $\sum i(i-1)l_i$ and it turns out that $\sum(i-n)(i-(n-\varepsilon))l_i>0$, hence $l_0>0$), so we can, and will, consider our point set $\mathcal{B}$ in the affine plane $AG(2,q)$.

Define a *good* point to be a point not in $\mathcal{B}$ which lies on exactly q/n external lines. Let $\mathcal{G}$ be the set of good points. Let $\mathcal{H}$ be the set of points not in $\mathcal{B}$ which are not good, we shall call such points *bad*. Our aim is to show that bad points are on no external lines. First however we wish to get some kind of lower bound on the number of good points. Using this we then apply some polynomial techniques, which imply the incompleteness property.

Define s_i to be the number of lines containing $n-i$ points of $\mathcal{B}$, and let $s_i(P)$ be the number of lines through the point P containing $n-i$ points of $\mathcal{B}$. Let $\mathcal{S}$ be the set of lines containing some points of $\mathcal{B}$ but less than n points of $\mathcal{B}$. For every point $P\in\mathcal{B}$

$$\sum_{i=1}^{\varepsilon} is_i(P)=\varepsilon$$

and summing this over all points $P\in\mathcal{B}$ gives

$$\sum_{i=1}^{\varepsilon} i(n-i)s_i=\varepsilon(nq-q+n-\varepsilon)\geq(n-\varepsilon)\sum_{i=1}^{\varepsilon} is_i.$$

For all bad points $P\in\mathcal{H}$

$$\sum_{i=1}^{\varepsilon} is_i(P)\geq n+\varepsilon$$

with equality if and only if P is on exactly $q/n-1$ external lines. In fact if a point P is on (exactly) $q/n-l$ external lines then

$$\sum_{i=1}^{\varepsilon} is_i(P)=ln+\varepsilon.$$

It is clear that

$$\sum_{P\in\mathcal{H}}\sum_{i=1}^{\varepsilon} is_i(P)\geq|\mathcal{H}|(n+\varepsilon)$$

and we can manipulate the sum on the left as follows:

$$\sum_{P\in\mathcal{H}}\sum_{i=1}^{\varepsilon} is_i(P)=\sum_{l\in\mathcal{S}}(n-|l\cap\mathcal{B}|)(|l\cap\mathcal{H}|)$$

$$\leq\sum_{l\in\mathcal{S}}(n-|l\cap\mathcal{B}|)(q-n+\varepsilon)=(\sum_{i=1}^{\varepsilon} is_i)(q-n+\varepsilon).$$

Combining various inequalities we get

$$|\mathcal{H}|\leq(q-n+\varepsilon)(nq-q+n-\varepsilon)\varepsilon/(n-\varepsilon)(n+\varepsilon).$$

Now $|\mathcal{G}|+|\mathcal{H}|+|\mathcal{B}|=q^2$ and so

$$|\mathcal{G}|+|\mathcal{B}|\geq q^2-(q-n+\varepsilon)(nq-q+n-\varepsilon)\varepsilon/(n-\varepsilon)(n+\varepsilon).$$

In the initial stage we will require the number of good points together with the number of points in the arc to be more than $(n+\varepsilon)(q-1)$. This will occur when

$$q^2-(q-n+\varepsilon)(nq-q+n-\varepsilon)\varepsilon/(n-\varepsilon)(n+\varepsilon)>(n+\varepsilon)(q-1),$$

and ignoring some positive terms on the right-hand side and some negative terms on the left-hand side when

$$q^2-(q-n+\varepsilon)nq\varepsilon/(n-\varepsilon)(n+\varepsilon)>(n+\varepsilon)q.$$

Writing $\varepsilon=cn$ and $m=q/n$ this will hold for $0\leq c\leq c_m$, where c_m is the unique zero in the interval $(0,1)$ of the cubic $c^3/m-c^2-c-1/m+1$. For $m=2$ we get $c_m>.381$, for $m=3$ we get $c_m>.476$ and for $m\geq 4$ we have $c_m>1/2$.

3. A technical lemma

At several points in the rest of the paper we will make use of the following lemma; it will be referred to simply as the lemma. Here q, n and ε are as before.

Lemma 3.1 *Let $R\in\mathbf{F}_{q^2}[t,x]$, be of the form*

$$R(t,x)=\sum_{j=0}^{q+\varepsilon}\rho_j(x)t^j$$

with $\rho_0=1$, and ρ_j a polynomial of degree at most $j(q-1)$. Suppose $R(t,x_0)$ is fully reducible in $\mathbf{F}_{q^2}[t]$ for all $x_0\in\mathbf{F}_{q^2}$. Let $S\in\mathbf{F}_{q^2}$ be the set of points x_0 for which we have a factorization

$$R(t,x_0)=\sum_{i=0}^{q/n}\rho_{in}(x_0)t^{in}\sum_{j=0}^{\varepsilon}\rho_j(x_0)t^j,$$

Suppose for some $x_1\in\mathbf{F}_{q^2}$ we have the factorization

$$R(t,x_1)=\sum_{i=0}^{q/n-l}\gamma_{in}t^{in}\sum_{j=0}^{ln+\varepsilon}\delta_j t^j,$$

for some $l>0$, with $ln+\varepsilon<|S|/(q-1)$. Then $x_1\in S$.

Proof : For $x_0 \in S$ and $0 \leq j < n$ we have $\rho_{in+j}(x_0) = \rho_{in}(x_0)\rho_j(x_0)$ and $\rho_j(x_0) = 0$ for $\varepsilon < j < n$. Since ρ_{in+j} has degree at most $(in+j)(q-1)$ these equations hold identically for $in + j \leq ln + \varepsilon < |S|/(q-1)$. It follows that $\delta_j = 0$ for $in + \varepsilon < j < (i+1)n$, where $i = 0, 1, \ldots, l-1$, and we may write

$$\sum_{j=0}^{ln+\varepsilon} \delta_j t^j = \sum_{i=0}^{l} \Delta_i(t) t^{in},$$

where Δ_i has degree at most ε in t. Let $R_0 = \sum_{j=0}^{\varepsilon} \rho_j(x_1)t^j$. Then we can successively solve $\Delta_0 = R_0$, $\Delta_1 + \gamma_n \Delta_0 = R_0 \rho_n(x_1)$, $\ldots$, $\Delta_l + \gamma_n \Delta_{l-1} + \ldots + \gamma_{nl}\Delta_0 = R_0 \rho_{ln}(x_1)$ so we get that all Δ's are constant multiples (depending on x_1 of course) of R_0 and it follows that $x_1 \in S$.

4. Some useful polynomials and their consequences

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 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. Let $\mathcal{B}$, $\mathcal{G}$ and $\mathcal{H}$ be as they were in the last section but view them now as subsets of $GF(q^2)$.

Let $\mathcal{B}^{[-1]} = \{1/b \,|\, b \in \mathcal{B} \setminus \{0\}\}$ and define $\mathcal{G}^{[-1]}$ and $\mathcal{H}^{[-1]}$ similarly.

Define the polynomials F in two variables and σ_k in one variable by

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

where σ_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.

Define the formal inverse to F, when viewed as a polynomial in t to be

$$F^{-1}(t,x) := \sum_{k=0}^{\infty} \alpha_k t^k$$

such that $FF^{-1} \equiv 1$. It is clear that α_k is a polynomial in x. Moreover it is a sum of certain terms of the form $\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_m}$ where $\sum_{j=1}^{m} i_j = k$ and therefore has degree at most $k(q-1)$ in x.

For $x_0 \in \mathcal{B}^{[-1]}$ 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 at most $n-1$ other points of $\mathcal{B}$, so that the multiset $\{(1/x_0 - b)^{q-1}\}$ consists of every $(q+1)$-st root of unity repeated at most $n-1$ times, together with the element 0. The quotient of this divisibility has degree ε and since this is assumed to be less than n (in fact we need only less than q here) we have that the quotient is $\sum_{j=0}^{\varepsilon} \alpha_j(x_0)t^j$. Consider the equality

$$F(t,x_0)\left(\sum_{j=0}^{\varepsilon} \alpha_j(x_0)t^j\right) = (1-t^{q+1})^{n-1}.$$

The right-hand side has no non-constant term until $q+1$. If we look at the terms of degree greater than ε yet less than $q+1$ we find that

$$\alpha_j(x_0) = 0$$

for $\varepsilon < j < q+1$ whenever $x_0 \in \mathcal{B}^{[-1]}$.

For $x_0 \in \mathcal{G}^{[-1]} \cup \mathcal{H}^{[-1]}$ we get that $F(t, x_0) | (1 - t^{q+1})^n$, for in this case every line passing through the point $1/x_0$ contains at most n points of $\mathcal{B}$, so that the multiset $\{(1/x_0 - b)^{q-1} | b \in \mathcal{B}\}$ consists of various $(q+1)$-st root of unity repeated at most n times. Define the quotient of this divisibility to be $Q(t, x_0)$ where Q has degree $q+\varepsilon$ in t and

$$F(t, x_0) Q(t, x_0) = (1 - t^{q+1})^n = 1 - t^{nq+n}.$$

We can write down an expression for $Q(t, x_0)$, it is simply

$$Q(t, x_0) = \sum_{j=0}^{q+\varepsilon} \alpha_j t^j.$$

By definition $Q(t, x_0)$ splits into linear factors in t whose (inverse) roots correspond to the directions of lines through $1/x_0$ that have less than n points of $\mathcal{B}$, counted with multiplicity. For example, consider a line through $1/x_0$ that has direction γ yet contains no points of $\mathcal{B}$. It follows that $(1 - \gamma t)^n | Q(t, x_0)$. Moreover consider $x_0 \in \mathcal{G}^{[-1]}$. The corresponding point to $1/x_0$ lies on q/n external lines and hence

$$Q(t, x_0) = \left(\sum_{i=0}^{q/n} \alpha_{in} t^{in} \right) \left(\sum_{j=0}^{\varepsilon} \alpha_j t^j \right).$$

Note that this equation also holds for $x_0 \in \mathcal{B}^{[-1]}$ since for these points the first factor reduces to the constant term $\alpha_0 = 1$.

Consider $x_1 \in \mathcal{H}^{[-1]}$ such that $1/x_1$ corresponds to a point on exactly $q/n - 1$ external lines. It follows that

$$Q(t, x_1) = \left(\sum_{i=0}^{q/n-1} \gamma_{in} t^{in} \right) \left(\sum_{j=0}^{n+\varepsilon} \delta_j t^j \right)$$

for some γ_{in} and δ_j. We are now in the position to apply our lemma, with $l = 1$ and $R = Q$. We have $\mathcal{B}^{[-1]} \cup \mathcal{G}^{[-1]} \subset S$, so $|S| > (n+\varepsilon)(q-1)$, (here we assume that $\varepsilon < .381n$ if $q/n = 2$, that $\varepsilon < .476n$ if $q/n = 3$ and $\varepsilon < n/2$ if $q/n > 2$) and we conclude that $x_1 \in S$. This would imply however that $1/x_1$ corresponds to a point on q/n external lines since $Q(t, x_1)$ has q/n factors repeated n times. In other words, $1/x_1$ is a good point. Therefore, all elements of $\mathcal{H}$ lie on less than $q/n - 1$ external lines. In particular if $q/n = 2$ bad points are on no external lines. In the remaining part we will therefore take $q/n > 2$.

In the next section we go back to our counting argument from an earlier section with the added knowledge that $\mathcal{H}$ contains no points on exactly $q/n - 1$ external lines.

5. More counting and more polynomials

All points in $\mathcal{H}$ are on at most $q/n - 2$ external lines so we have now that for $P \in \mathcal{H}$

$$\sum_{i=1}^{\varepsilon} i s_i(P) \geq 2n + \varepsilon.$$

Continuing the same argument as before with this new bound implies

$$|\mathcal{G}| + |\mathcal{B}| \geq q^2 - \frac{(q-n+\varepsilon)(nq-q+n-\varepsilon)\varepsilon}{(n-\varepsilon)(2n+\varepsilon)} \geq 0.6q^2,$$

where we just use $\varepsilon \leq .476n$.

Consider again $x_0 \in \mathcal{G}^{[-1]} \cup \mathcal{B}^{[-1]}$. As before,

$$Q(t,x_0) = \left(\sum_{i=0}^{q/n} \alpha_{in} t^{in}\right)\left(\sum_{j=0}^{\varepsilon} \alpha_j t^j\right)$$

Consider $x_1 \in \mathcal{H}^{[-1]}$ such that $1/x_1$ corresponds to a point on exactly $q/n - l$ external lines, with $l < 0.6q/n$. It follows that

$$Q(t,x_1) = \left(\sum_{i=0}^{q/n-l} \gamma_{in} t^{in}\right)\left(\sum_{j=0}^{ln+\varepsilon} \delta_j t^j\right)$$

for some γ_{in} and δ_j. We may apply our technical lemma again and conclude as before that x_1 is in fact a good point. Now we have that all points in $\mathcal{H}$ are on less than $0.4q/n$ external lines. For $q/n = 3$ it pays to be a bit more precise in our bookkeeping, and in fact we get that in this case bad points are on no external lines. So from here on we assume $q/n > 3$. We return to our counting argument and conclude that for $P \in \mathcal{H}$

$$\sum_{i=1}^{\varepsilon} i s_i(P) \geq 0.6(q/n)n + \varepsilon = 0.6q + \varepsilon.$$

Continuing as before we get that $|\mathcal{H}| < 2nq$ and hence at least $q^2 - 2nq$ points are either good or in $\mathcal{B}$. Applying the lemma, now with $l = q/n - 3$ we get that all points in $\mathcal{H}$ are now on at most 2 external lines, and doing it once more on no external lines.

We have now proven that all points on external lines are good points and, since good points lie on exactly q/n external lines, the external lines form a dual maximal arc of degree q/n. The lines in the dual plane that are external to this dual maximal arc are simply the points $\mathcal{B} \cup \mathcal{H}$ in the original plane. The external lines to a maximal arc form a dual maximal arc and hence $\mathcal{B} \cup \mathcal{H}$ is a maximal arc. Note that this implies that the extension of $\mathcal{B}$ to a maximal arc is unique. We have, therefore, proved the following theorem:

Theorem 5.1 *Let $\mathcal{B}$ be a $(nq-q+n-\varepsilon, n)$-arc in $PG(2,q)$ where n divides q.*

1. *(q even.) For $\varepsilon < n/2$ and $q/n > 2$ or $\varepsilon < .381n$ and $q/n = 2$, $\mathcal{B}$ can be extended uniquely to some maximal arc containing $nq - q + n$ points.*
2. *(q odd.) If $q/n > 3$ then $\varepsilon > n/2$ and if $q/n = 3$ then $\varepsilon > .476n$.*

References

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

[2] S. Ball and A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.*, to appear.

[3] 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.

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

[5] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second Edition, Clarendon Press, Oxford (1997).

[6] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces, *Journal of Statistical Planning and Inference*, Proceedings of the Bose Memorial Conference (Colorado, June 7–11 1995).

[7] T. Szőnyi, On the embeddability of (k,p)-arcs, manuscript.

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

[9] 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.

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

[11] B. J. Wilson, Incompleteness of $(nq+n-q-2,n)$-arcs in finite projective planes of even order, *Math. Proc. Cambridge Philos. Soc.*, **91**, (1982), 1–8.