# On small complete arcs in a finite plane

*Simeon Ball*

**Abstract**

Recent results on blocking sets are applied to the bisecants of a small complete arc, since these lines form a dual blocking set. It is shown that such blocking sets yield a lacunary polynomial of specific type. This leads to an improvement to the lower bound of the existence of a complete $k$-arc when the order of the plane is a square prime.

## 1. Introduction

Many attempts have been made to determine the size of the smallest complete arc in $PG(2,q)$. Most of the results can be found in [3, Chapter 9]. Define an $i$-secant to be a line that intersects a set of points in exactly $i$ points, and let $\tau_i$ denote the number of $i$-secants to such a set. If $K$ is a complete $k$-arc then the bisecants to $K$ form a blocking set with secant distribution $\tau_{k-1} = k$, $\tau_i = c_i$, $i = 1, ..., \lfloor \frac{k}{2} \rfloor$, where $c_i$ is equal to the number of points in $PG(2,q) \setminus K$ lying on exactly $i$ bisecants. By applying elementary results of blocking sets this implies that a complete $k$-arc must have at least $\sqrt{2q}$ points.

In [1] Blokhuis mentions that his result in [2] implies that for $PG(2,p)$, $p$ prime, a complete arc has at least $\sqrt{3p}$ points. He also claims that it should be possible to prove this bound for all $q$. This is because blocking sets arising from small complete arcs have properties inconsistent with those of a small blocking set. Such properties are used in the section on small blocking sets to prove that a small complete arc in $PG(2,q)$, $q = p^2$, $p$ prime, has at least $\sqrt{3q}$ points.

It has also been conjectured by de Resmini [1] that the smallest complete arc has size $\lfloor 3\sqrt{q} - 2 \rfloor$, if $q$ is even and $\lfloor 3\sqrt{q} - 3 \rfloor$, if $q$ is odd (and not too small). However, in general, complete arcs of size about $\frac{1}{2}q$ have been constructed [3] and, for certain values of $q$, complete arcs of size about $\frac{1}{4}q$ have been constructed [4].

## 2. Lacunary polynomials

A polynomial in $GF(q)[x]$ is called *fully reducible* if it factors completely into linear factors over $GF(q)$. If in the sequence of coefficients of a polynomial a long run of zeros occurs we call this polynomial *lacunary*. In [5] Rédei studied properties of lacunary polynomials that are fully reducible. The following theorem copied together with the proof from [1] is really just a slight generalization of Theorem 24′ in [5]. Throughout $q = p^h$, where $p$ is prime.

**Theorem 2.1** *Let $f \in GF(q)[x]$ be fully reducible, and suppose that $f(x) = x^q v(x) + w(x)$, where $v$ and $w$ have no common factor. Let $m < q$ be the maximum of the degrees of $v$ and $w$. Let $e$ be maximal such that $f$ (and hence $v$ and $w$) is a $p^e$-th power. Then one of the following holds:*

1. *$e = h$ and $m = 0$;*
2. *$e \geq h/2$ and $m \geq p^e$;*
3. *$e < h/2$ and $m \geq p^e\lceil (p^{h-e}+1)/(p^e+1)\rceil$;*
4. *$e = 0$, $m = 1$ and $f(x) = a(x^q - x)$.*

Note that in particular when $q$ is prime and $m > 1$, then $m \geq (q+1)/2$.

**Proof :** If $e \geq h/2$ then since $v$ and $w$ are $p^e$-th powers their degrees, and hence $m$, are greater than $p^e$ unless $m = 0$ and then Case 1 occurs. So assume $e < h/2$. Write $E = p^e$. Let $f(x) = f_1(x)^E$ and define $v_1$ and $w_1$ similarly. Then extracting $E$-th roots we get

$$f_1 = x^{q/E} v_1 + w_1.$$

Now write $f_1(x) = s(x)r(x)$ where $s(x)$ contains all different linear factors of $f_1$ exactly once, and $r(x)$ the rest. Since $s \mid x^q - x$ and $s \mid f = x^q v + w$ these imply

$$s \mid xv + w.$$

Since $r \mid f_1'$ and $r \mid f_1$ these imply $r \mid f_1' v_1 - v_1' f_1$ or

$$r \mid w_1' v_1 - v_1' w_1.$$

Note that $(v, w) = 1$ and $v_1$ and $w_1$ are not both $p$-th powers; so the right hand side does not vanish. Combining these two divisibility relations we get

$$f_1 (= rs) | (xv + w)(w_1' v_1 - v_1' w_1).$$

Now if $xv + w = 0$ then $m = 1$ since $(v, w) = 1$, and $f$ has the desired form. Otherwise the degree of the left hand side is at most equal to that of the right hand side. First consider the case that $\deg v = m = Em_1$. In this case

$$q/E + m_1 \leq 1 + Em_1 + 2m_1 - 2.$$

Hence

$$m_1 \geq \frac{q/E + 1}{E + 1}.$$

The other case ($\deg v < \deg w = m$) is similar and gives the same conclusion. □

## 3. Small complete arcs

The main purpose of this section is determine lower bounds for the existence of small complete arcs. This is done by using the theory of blocking sets since the bisecants to a complete arc form a dual blocking set. This blocking set is non-trivial since, if it contained a line, this would imply that $q + 1$ bisecants meet in a point, which is not possible. The bisecants meet in points of order $k - 1$, (the points of the arc), and of order at most $k/2$ otherwise. This observation leads to the first result. See Theorem 9.1.10 and Theorem 9.1.12 in [3] for similar results.

**Theorem 3.1** *A complete $k$-arc has at least $\lfloor \sqrt{2q} + 2 \rfloor$ points.*

**Proof :** The bisecants to a complete $k$-arc form a non-trivial blocking set and so

$$\frac{k(k-1)}{2} \geq q + \sqrt{q} + 1.$$

This implies that $k \geq \lfloor \sqrt{2q} + 2 \rfloor$. □

The following result is an improvement on this bound for prime planes by Blokhuis who used his theorem on blocking sets in [2] to prove Theorem 3.2.

**Theorem 3.2** *A complete $k$-arc in $PG(2, p)$ has more than $\sqrt{3p} + \frac{1}{2}$ points for $p$, prime.*

**Proof :** A non-trivial blocking set in $PG(2, p)$ has at least $\frac{3(p+1)}{2}$ points. Therefore

$$\frac{k(k-1)}{2} \geq \frac{3(p+1)}{2},$$

which implies that $k > \sqrt{3p} + \frac{1}{2}$. □

The previous theorem uses the theory of lacunary polynomials only to obtain the bound on the size of a blocking set. It does not use the extra properties that arise when the blocking set is formed from a $k$-arc. The following theorem implies the existence of a lacunary polynomial of a certain type. The first half of the proof follows that of [2]. When Theorem 2.1 is applied, properties arising from the $k$-arc are considered.

**Theorem 3.3** *Suppose there exists a complete $k$-arc with less than $\sqrt{3q} + \frac{1}{2}$ points in $PG(2, q)$, with $q = p^h$. Then there exists a lacunary polynomial, of degree $q + m = k(k-1)/2 - 1$, that must satisfy the conditions of case 3 of Theorem 2.1.*

**Proof :** Let $x = 0$ be a bisecant of the $k$-arc and (0,0,1) be a point where this bisecant meets no other bisecants. There exists such a point only when the dual blocking set is irreducible. If the dual blocking set is not irreducible remove bisecants until it is. Now proceed as in [2].

The points dual to the other bisecants are therefore contained in $AG(2, q)$ and let those points form the set $B = \{(a_i, b_i) | i = 1, ..., q + m\}$.

The set $B$ has at least one point on every non-horizontal line ( the horizontal lines being blocked by (1,0,0)). And so for every $u, t \in GF(q)$ the equation $x + uy + t = 0$ has a solution in $B$; that is, for some $i$, there is an $(a_i, b_i)$ such that $a_i + b_i u + t = 0$. It follows therefore that the polynomial

$$F(t, u) = \prod_{i=1}^{q+m} (t + a_i + ub_i)$$

vanishes for all $t, u \in GF(q)$.

This implies that $F$ is in the ideal generated by $(t^q - t)$ and $(u^q - u)$. So

$$F(t, u) = (t^q - t)G(t, u) + (u^q - u)H(t, u)$$

where $G$ and $H$ are of total degree $m$ in the variables $t$ and $u$. Let $F_0$, $G_0$ and $H_0$ denote the parts of $F$, $G$ and $H$, respectively, that are homogeneous of total degree $m$. Restricting to the terms of total degree $q + m$ implies

$$F_0 = t^q G_0 + H_0$$

where

$$F_0 = \prod_{i=1}^{q+m} (t + ub_i).$$

The variable $u$ does not play any further role since the equation is homogeneous, so put $u = 1$ and define $f(t) = F_0(t, 1)$, $g(t) = G_0(t, 1)$ and $h(t) = H_0(t, 1)$. So

$$f(t) = \prod_{i=1}^{q+m} (t + b_i) = t^q g(t) + h(t).$$

Now apply Theorem 2.1 to $f$. If $g$ and $h$ have a common factor, remove it; this possibly reduces $m$. Consider each of the four cases in turn.

*Case 1 of Theorem 2.1.* $f$ contains a $q$-th power; that is, it contains a factor of the form $(t-a)^q$. This implies that $B$ contains a line. But $B$ is a non-trivial blocking set; so this case cannot occur.

*Case 4 of Theorem 2.1.* Since the degree of $g$ is not less than the degree of $h$, this case also cannot occur.

*Case 2 of Theorem 2.1.* After factoring out $g$ and $h$, the polynomial $f$ is an $E$-th power and so all secants are of length 1, $1 + E$, $1 + 2E$, .... where $E = p^e$ and $e \geq h/2$. Since $B$ is formed from the bisecants to a $k$-arc, through each of its points there are two $(k-1)$-secants and no other secants with more than $k/2$ points. This implies, unless after removing bisecants to make it irreducible and factoring out, all secants through (1,0,0) are of length 1 except the two $(k-1)$-secants, that

$$1 + E \leq k/2,$$

since there are no secants longer than $k/2$ apart from the $(k-1)$-secants. The above inequality implies

$$k \geq 2 + 2E \geq 2 + 2\sqrt{q},$$

which is strictly bigger than $\sqrt{3q} + \frac{1}{2}$.

So, if after removing bisecants to make it irreducible and factoring out, all secants are of length 1 except the two $(k-1)$-secants, then $\deg f \leq 2(k-2) = 2k - 4$. But $\deg f = q + m \geq q + \sqrt{q}$ and so

$$k \geq \frac{q + \sqrt{q} + 4}{2},$$

which is bigger than $\sqrt{3q} + \frac{1}{2}$ for all $q$.

Hence $f$ must be in case 3 of Theorem 2.1. □

**Theorem 3.4** *A complete $k$-arc in $PG(2, q)$ has more than $\sqrt{3q} + \frac{1}{2}$ points for $q = p^2$, $p$ prime.*

**Proof :** If there exists a smaller complete $k$-arc in $PG(2,q)$ then Theorem 3.3 implies the existence of a polynomial $f$ satisfying case 3 of Theorem 2.1. But in case 3 of Theorem 2.1, $e < h/2 = 1$ and so $e = 0$ and hence $m \geq \frac{q+1}{2}$. This implies

$$\frac{k(k-1)}{2} \geq \frac{3(q+1)}{2}$$

and so $k > \sqrt{3q} + \frac{1}{2}$. □

## 4. Small planes

In $PG(2,3)$ Theorem 3.2 implies that the 4-arcs are the only complete arcs of the plane and this is indeed the case. In $PG(2,4)$ Theorem 3.4 only implies $k \geq 4$ but Lemma 9.2.1 (i) and (ii) from [3] imply that no complete 4-arc or 5-arc exist in $PG(2,4)$. In fact Lemma 9.2.1 (ii) states there exist no complete 5-arcs and hence in $PG(2,5)$ since Theorem 3.2 gives the bound $k \geq 5$, the only complete arcs in $PG(2,5)$ are the conics.

In $PG(2,7)$ Theorem 3.2 gives the bound $k \geq 6$ and complete 6-arcs do exist; so this bound is attained. In $PG(2,8)$ Theorem 3.1 gives the bound $k \geq 6$ and complete 6-arcs do exist; so this bound is attained. In $PG(2,9)$ Theorem 3.4 gives the bound $k \geq 6$ and again complete 6-arcs do exist.

In $PG(2,11)$ Theorem 3.2 gives the bound $k \geq 7$ and complete 7-arcs do exist and are all projectively equivalent to
$\{(0,0,1)(0,1,0)(1,0,0)(1,1,1)(2,3,1)(3,7,1)(8,10,1)\}$.

In $PG(2,13)$ Theorem 3.2 gives the bound $k \geq 7$. If $K$ is a complete $k$-arc whose points of index $i$ are given by the $c_i$, as in [3, Chapter 9], then this gives a blocking set with secant distribution $\tau_{k-1} = k$ and $\tau_i = c_i$ for $i = 1, ..., k/2$. If there exists a complete 7-arc then this implies the existence of a 21 point blocking set. This is necessarily irreducible since $3(p+1)/2 = 21$ and this is the smallest size of a blocking set in $PG(2,p)$. By considering the polynomial $s$ in the proof of Theorem 2.1 when applied to a 21 point blocking set in $PG(2,13)$ it is deduced that deg $s = 8$. This implies that there are 6 tangents through each point of the blocking set and hence there are 126=21.6 tangents in all. Lemma 9.1.1 of [3] implies that

$$\sum_{i=0}^{q+1} c_i = q^2 + q + 1 - k, \quad (1)$$

$$\sum_{i=1}^{q+1} i c_i = \frac{k(k-1)(q-1)}{2}, \quad (2)$$

$$\sum_{1=2}^{q+1} \frac{i(i-1)}{2} c_i = \frac{k(k-1)(k-2)(k-3)}{8}. \tag{3}$$

In the case $q = 13$ and $k = 7$ these equations give $c_1 = 129$. But $\tau_1 = 126$ which is a contradiction since these two values must be equal. Therefore $k \geq 8$ and indeed there exist two projectively distinct complete 8-arcs in $PG(2, 13)$ which are { (0,0,1) (0,1,0) (1,0,0) (1,1,1) (2,3,1) (3,2,1) (5,7,1) (7,5,1) } and { (0,0,1) (0,1,0) (1,0,0) (1,1,1) (2,3,1) (3,9,1) (4,5,1) (7,11,1) }.

## References

[1] A. Blokhuis, Blocking sets in Desarguesian planes, in: *Paul Erdős is Eighty*, Volume 2, (eds: D. Miklós, V.T. Sós and T. Szőnyi), Bolyai Soc. Math. Studies, to appear.

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

[3] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford (1979).

[4] G. Korchmáros, New examples of $k$-arcs in $PG(2, q)$, *Europ. J. Combin.*, **4**, (1983), 329–334.

[5] L. Rédei, *Lacunary polynomials over finite fields*, Birkhäuser Verlag, Basel, (1973).

Simeon Ball
*School of Mathematical and Physical Sciences,*
*University of Sussex,*
*Brighton BN1 9QH,*
*U.K.*