AN EASIER PROOF OF THE MAXIMAL ARCS CONJECTURE

SIMEON BALL AND AART BLOKHUIS

(Communicated by Jeffry N. Kahn)

ABSTRACT. It was a long-standing conjecture in finite geometry that a Desarguesian plane of odd order contains no maximal arcs. A rather inaccessible and long proof was given recently by the authors in collaboration with Mazza. In this paper a new observation leads to a greatly simplified proof of the conjecture.

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 \(k \leq 1 + (q + 1)(n - 1) = qn - q + n\), 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 [3] 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 [2]. A complete proof was given in [1], however the methods used there are difficult to follow and the arguments are quite long.

A new observation, concerning a divisibility relation between a function \(F\) and its partial derivative \(F_x\), led to the discovery of a greatly simplified proof which should be accessible to a wider audience.

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 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.

2. Some useful polynomials

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

\[ B(x) := \prod_{b \in B} (1 - bx) = \sum_{k=0}^{\infty} (-1)^k \sigma_k x^k, \]

where \( \sigma_k \) denotes the \( k \)-th elementary symmetric function of the set \( B \); in particular, \( \sigma_k = 0 \) for \( k > |B| \). Define the polynomials \( F \) in two variables and \( \hat{\sigma}_k \) in one variable by

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

where \( \hat{\sigma}_k \) is the \( k \)-th elementary symmetric function of the set of polynomials \( \{(1 - bx)^{q-1} | b \in B\} \), a polynomial of degree at most \( k(q - 1) \) in \( x \). Again, \( \hat{\sigma}_k \) is the zero polynomial for \( k > |B| \). For \( x_0 \in GF(q^2) \setminus B^{[-1]} \) 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 \( B \) that is either 0 or \( n \). In the multiset \( \{(1/x_0 - b)^{q-1} | b \in B\} \), every element occurs therefore with multiplicity \( n \), so that in \( F(t, x_0) \) every factor occurs exactly \( n \) times. For \( x_0 \in B^{[-1]} \) 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 exactly \( n - 1 \) other points of \( B \), 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

\[ F(t, x_0) = \prod_{b \in B} (1 - (1/x_0 - b)^{q-1})^{-1} \]
By computing the derivative of $B(x)$ and expanding the denominator as an infinite sum we get

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

Note that all $b \in B^{[-1]}$ are elements of $GF(q^2)$. Hence $b^{i+1} = b$, and it follows that

$$(x - x^{q^2}) \left( \sum_{b \in B} \sum_{i=0}^{\infty} b^{i+1} x^i \right) = \sum_{b \in B} \sum_{i=0}^{q^2-1} b^i x^i = \sum_{b \in B} (1 - bx)^{q^2-1}.$$ 

The polynomial $- \sum_{b \in B} (1 - bx)^{q^2-1}$ is equal to 1 for all $x_0 \in B^{[-1]}$, since there are $nq - q + n$ terms in the sum, of which one will be zero and the others will be 1. For all other elements of $GF(q^2)$ it will be zero, since every term in the sum will be 1. Now $\hat{\sigma}_{q+1}$ takes the same values, and both are of degree $q^2 - 1$. Hence it follows that they are the same, i.e. $\hat{\sigma}_{q+1} = - \sum_{b \in B} (1 - bx)^{q^2-1}$. So we get the important relation

$$zB' = \hat{\sigma}_{q+1} B.$$ 

Differentiating this, multiplying by $B$ and noting that $B\hat{\sigma}_{q+1} = 0 \mod z$, we get another useful relation:

$$BB' = B^2 \hat{\sigma}_{q+1}' \mod z.$$ 

Differentiating $F(t, x)$ with respect to $x$, we get

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

The terms in the denominator are of the form $(1 - (1 - bx)^{q^2-1} t)$, and for all $x = x_0 \in GF(q^2)$ this is a factor of $(1 - tq^{q+1})$. Expanding the term in the bracket as a formal power series in $t$, multiplying by $(1 - tq^{q+1})$ and reducing mod $z$, we obtain a polynomial $R(t, x)$ of degree at most $q + 1$ in $t$ such that

$$FR = (1 - tq^{q+1}) F_x \mod z.$$ 

Comparing coefficients of powers of $t$ we can calculate that the polynomial $R(t, x)$ is of the form

$$R(t, x) = -\hat{\sigma}'_n(x) t^n + \hat{R}(t, x) t^{2n} + \hat{\sigma}'_{q+1 + 1} t^{q+1},$$

where $\hat{R}(t, x)$ is a polynomial containing only powers of $t$ with exponents divisible by $n$. Multiplying the equation by $B$ gives

$$\left( \sum_{i=0}^{q-q/n+1} (-1)^i B \hat{\sigma}_n t^n \right) R = (1 - tq^{q+1}) BF_x \mod z.$$ 

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

$$-\hat{\sigma}'_{q+1} B \hat{\sigma}_n = -\hat{\sigma}'_{q+1+n} B + B \hat{\sigma}'_n.$$ 

Note that since $B | \hat{\sigma}_n$ we can use the relation $B^2 \hat{\sigma}'_{q+1} = BB' \mod z$, and rearranging terms gives

$$B \hat{\sigma}'_{q+1+n} = (B \hat{\sigma}_n)' \mod z.$$ 

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

$$B \hat{\sigma}'_{i(q+1)+n} = B \hat{\sigma}'_{(i-1)(q+1)+n} = (B \hat{\sigma}_n)' \mod z.$$
Since $|B| = nq - q + n$, it follows that $\sigma_{(n-1)(q+1)+n} \equiv 0$, and so when we look at the coefficient of $t^{(n-1)(q+1)+n}$ we find that

$$(B\sigma_n)' \equiv 0 \pmod{z}.$$  

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

References

[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. MR 51:13851

Department of Mathematics, Vrije Universiteit Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands