The classification of maximal arcs in small Desarguesian planes

Simeon Ball
Queen Mary,
University of London,
London, E1 4NS,
United Kingdom

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

17 January 2001

Abstract

There are three types of maximal arcs in the planes of order 16, the hyperovals of degree 2, the dual hyperovals of degree 8 and the maximal arcs of degree 4. The hyperovals and dual hyperovals of the Desarguesian projective plane $PG(2, q)$ have been classified for $q \leq 32$. This article completes the classification of maximal arcs in $PG(2, 16)$. The initial calculations are valid for all maximal arcs of degree r in $PG(2, q)$. In the case $r = q/4$ (dually $r = 4$) further computations are possible. By means of a precursor we classify the hyperovals in $PG(2, 8)$ using these calculations and then classify, with the aid of a computer, the maximal arcs of degree 4 in $PG(2, 16)$; they are all Denniston maximal arcs.

1. Introduction

A $(k, r)-$*arc* in a projective plane is a set of k points, at most r on every line. If the order of the plane is q, then $k \leq 1 + (q + 1)(r - 1) = rq - q + r$ with equality if and only if every line intersects the arc in 0 or r points. Arcs realizing the upper bound are called *maximal arcs* and r is called the *degree* of the maximal arc. Equality in the bound implies that r divides q or $r = q + 1$. If $1 < r < q$, then the maximal arc is called non-trivial. The only known examples of non-trivial maximal arcs in Desarguesian projective planes, are the hyperovals ($r = 2$), the dual hyperovals ($r = q/2$), the Denniston arcs [4] and an infinite family constructed by J. A. Thas [9]. The Denniston arcs exist for all q even and r dividing q. The family constructed in [9], which are not Denniston arcs, are maximal arcs of degree q in $PG(2, q^2)$ and arise from a Tits ovoid in $PG(3, q)$, where q is even and not a square. The maximal arcs constructed by Thas in [10] are Denniston in $PG(2, q)$ [6]. For odd q maximal arcs in $PG(2, q)$ do not exist [1]. For $q = 2, 4$ and 8 the hyperovals are a conic plus nucleus. The hyperovals (and hence dual hyperovals) have been classified in $PG(2, 16)$ by M. Hall Jr. [5] and without the aid of a computer by T. Penttila and C. M. O'Keefe [7] and the hyperovals in $PG(2, 32)$ have been classified by T. Penttila and G. Royle [8] with the aid of a computer. The full collineation stabilisers of the Denniston and Thas maximal arcs are calculated in [6].

The method which is used here is similar to that used in [2]. However, even more relevant were those calculations which appeared in [3] which was never published.

2. Maximal arcs in $AG(2,q)$ as subsets of $GF(q^2)$

We shall consider sets of points in the affine plane $AG(2,q)$ instead of $PG(2,q)$ and assume throughout that q is even. The points of $AG(2,q)$ can be identified with the elements of $GF(q^2)$ in a suitable way, so that all sets of points can be considered as subsets of this field. 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 $\mathcal{B}$ be a non-trivial $(rq-q+r,r)$-arc in $AG(2,q) \simeq GF(q^2)$. Define $B(X)$ to be the polynomial

$$B(X) := \prod_{b\in\mathcal{B}}(1+bX) = \sum_{k=0}^{rq-q+r} \sigma_k X^k$$

where σ_k denotes the k-th elementary symmetric function of the set $\mathcal{B}$. Define the polynomials F in two variables and $\hat{\sigma}_k$ in one variable by

$$F(T,X) := \prod_{b\in\mathcal{B}}(1+(1+bX)^{q-1}T) = \sum_{k=0}^{rq-q+r} \hat{\sigma}_k(X)T^k$$

where $\hat{\sigma}_k$ is the k-th elementary symmetric function of the set of polynomials

$$\{(1+bX)^{q-1} \mid b \in \mathcal{B}\},$$

a polynomial of degree at most $k(q-1)$ in X. Let $1/x \in GF(q^2) \setminus \mathcal{B}$ be a point not contained in the arc. Every line through $1/x$ contains a number of points of $\mathcal{B}$ that is either 0 or r. In the multiset $\{(1/x+b)^{q-1} \,|\, b \in \mathcal{B}\}$, every element occurs therefore with multiplicity r, so that in $F(T,x)$ every factor occurs exactly r times.
For $1/x \in \mathcal{B}$ we get that $F(T,x) = (1+T^{q+1})^{r-1}$, since every line passing through the point $1/x$ contains exactly $r-1$ other points of $\mathcal{B}$, so that the multiset $\{(1/x+b)^{q-1}\}$ consists of every $(q+1)$-st root of unity repeated $r-1$ times, together with the element 0. This gives

$$F(T,x) = \prod_{b\in\mathcal{B}}(1+(1/x+b)^{q-1}x^{q-1}T) = (1+x^{q^2-1}T^{q+1})^{r-1} = (1+T^{q+1})^{r-1}.$$

The coefficient of T^k of F in both cases implies that for all $x \in GF(q^2)$, $\hat{\sigma}_k(x) = 0$, whenever k is not divisible by r and $0 < k < q$. The degree of $\hat{\sigma}_k$ is at most $k(q-1) < q^2$ and hence these polynomials are identically zero. The first coefficient of F that is not necessarily identically zero is $\hat{\sigma}_r$ and this polynomial is divisible by $B(X)$ since every zero of B is a zero of $\hat{\sigma}_r$.

3. Some calculations and two sets of equations

It is difficult to calculate $\hat{\sigma}_k$, however it is possible to calculate

$$B\hat{\sigma}_k = \sum(1+b_1X)^q \dots (1+b_kX)^q(1+b_{k+1}X)\dots(1+b_{rq-q+r}X),$$

where the sum is taken over all $(k, |\mathcal{B}|-k)$ partitions of $\mathcal{B}$. The coefficient of X^n is

$$\sum_{i=0}^{\lfloor \frac{n}{q} \rfloor} \binom{|\mathcal{B}|-n+iq-i}{k-i} \epsilon_{i,n}$$

where for $n \geq iq$

$$\epsilon_{i,n} = \sum (b_1 \dots b_i)^q b_{i+1} \dots b_{n-iq+i}$$

and the sum is taken over all relevant partitions of $\mathcal{B}$ and $\epsilon_{i,n} = 0$ for $n < iq$. To determine the binomial coefficient for each $\epsilon_{i,n}$ note that for each term in the summation we can choose $k - i$ elements of $\mathcal{B}$ that do not appear in either the $(b_1 \dots b_i)^q$ part or the $b_{i+1} \dots b_{n-iq+i}$ part. We can simplify the binomial coefficient by applying Lucas' theorem. The identities $\hat{\sigma}_k \equiv 0$ for $0 < k < r$ yield the equations

$$\sum_{i=0}^{\lfloor \frac{n}{q} \rfloor} \binom{-n-i}{k-i} \epsilon_{i,n} = 0.$$

To solve these equations we use the following binomial identities

$$\binom{-n-i}{k-i} = (-1)^{k-i} \binom{n+k-1}{k-i} \quad \text{and} \quad \sum_{i=0}^{k} \binom{n+k-1}{k-i} \binom{-n}{i} = \binom{k-1}{k} = 0.$$

The solution for $n \geq kq$ (which can be verified by direct substitution) is

$$\epsilon_{k,n} = \binom{-n}{k} \epsilon_{0,n} = \binom{-n}{k} \sigma_n.$$

The equations for $n < kq$ imply

$$\sum_{i=0}^{n_1} \binom{-n-i}{k-i} \binom{-n}{i} \sigma_n = \binom{-n}{k} \sum_{i=0}^{n_1} \binom{k}{i} \sigma_n = \binom{k-1}{n_1} \binom{-n_0}{k} \sigma_n = 0 \tag{1}$$

where $n = n_1 q + n_0$ and $0 < k < r$. The identities $\hat{\sigma}_{r+k} \equiv 0$ for $0 < k < r$ yield the equations

$$\sum_{i=0}^{\lfloor \frac{n}{q} \rfloor} \binom{r-n-i}{r+k-i} \epsilon_{i,n} = 0$$

which we solve in the same way. The solution for $n \geq rq + kq$ is

$$\epsilon_{r+k,n} = \binom{-n}{k} \epsilon_{r,n}$$

and for $rq \leq n < rq + kq$

$$\binom{k-1}{n_1 - r} \binom{-n_0}{k} \epsilon_{r,n} = 0. \tag{2}$$

4. The effect of a translation on the symmetric functions

Let $\mathcal{B}^{(\lambda)} := \{b+\lambda \mid b \in \mathcal{B}\}$ and let $\sigma_k^{(\lambda)}$ be the k-th symmetric function of $\mathcal{B}^{(\lambda)}$. The relationship between the symmetric functions $\sigma_k^{(\lambda)}$ and the symmetric functions σ_k is

$$\sigma_k^{(\lambda)} = \sum (b_1+\lambda)(b_2+\lambda)\dots(b_k+\lambda) = \sum_{i=0}^{k} \sigma_i \lambda^{k-i} \binom{|\mathcal{B}|-i}{k-i}.$$

The equations (1) for $n<q$ and $k=-n \pmod r$ imply $\sigma_n = 0$ unless $n = 0 \pmod r$. We can calculate that

$$\sigma_r^{(\lambda)} = \sigma_r + \lambda^r \text{ and } \sigma_{2r}^{(\lambda)} = \sigma_{2r}$$

and combining these that

$$\sigma_{2r}^{(\lambda)} + (\sigma_r^{(\lambda)})^2 = \lambda^{2r} + \sigma_r^2 + \sigma_{2r}.$$

Hence for any maximal arc there is a unique translation

$$\lambda = (\sigma_r^2 + \sigma_{2r})^{q^2/2r}$$

which translates the maximal arc to a maximal arc in which $\sigma_r^2 + \sigma_{2r} = 0$. Moreover for every maximal arc we find with $\sigma_{2r} = \sigma_r^2$ there will be q^2 maximal arcs by translation.

5. The main divisibility and another set of equations

In this section we shall use the previously mentioned divisibility that $B(X)$ divides $\hat{\sigma}_r$ to calculate another set of equations. Let $Q(X)$ denote the quotient such that $BQ = \hat{\sigma}_r$ and note that $Q^\circ \le r(q-1)-(rq-q+r) = q-2r$. As in the last section we can calculate that

$$B\hat{\sigma}_r = \sum_{n<rq} \binom{r-n}{r} \sigma_n X^n + \sum_{n \ge rq} \epsilon_{r,n} X^n = 1 + \sigma_{2r}X^{2r} + \dots$$

and directly from $B^2Q = B\hat{\sigma}_r$ we see that

$$Q = 1 + (\sigma_r^2 + \sigma_{2r})X^{2r} + \dots.$$

It is at this point that we must make the restriction on r. Note first however that for $r=q/2$ the degree of Q is zero and hence $Q \equiv 1$. However we are interested in the case $r = q/4$ and the degree of Q is at most $q/2$ and hence $Q = 1 + (\sigma_r^2 + \sigma_{2r})X^{2r}$. Moreover we assume that we have translated the maximal arc so that $\sigma_r^2 + \sigma_{2r} = 0$ and hence that $Q \equiv 1$. It is now a simple task to equate the coefficients from $B^2 = B\hat{\sigma}_r$ and conclude that for $n < rq$

$$\binom{q/4-n}{q/4} \sigma_n = \sigma_{n/2}^2 \tag{3}$$

and for $n \ge rq$ that $\epsilon_{r,n} = \sigma_{n/2}^2$ which the equations (2) imply that for $n < rq + kq$ and $0<k<r$ that

$$\binom{k-1}{n_1-r}\binom{-n_0}{k}\sigma_{n/2}^2 = 0 \tag{4}$$

where $n = n_1 q + n_0$.

6. The Newton identities

The Newton identities can be deduced by differentiating

$$B(X) = \prod_{b \in \mathcal{B}} (1 + bX) = \sum_{k=0}^{rq-q+r} \sigma_k X^k$$

with respect to X.

$$B'(X) = \left(\sum_{b \in \mathcal{B}} \frac{b}{1 + bX} \right) B(X) = \sum_{k=0}^{rq-q+r} k \sigma_k X^{k-1}$$

and multiplying both sides by X and expanding $(1 + bX)^{(-1)}$ in characteristic 2

$$\left(\sum_{k=0}^{rq-q+r} \sigma_k X^k \right) \left(\sum_{b \in \mathcal{B}} \sum_{j=1}^{\infty} b^j X^j \right) = \sum_{k=0}^{rq-q+r} k \sigma_k X^k.$$

Let $\pi_k = \sum_{b \in \mathcal{B}} b^k$ and define the n-th Newton identity to be the coefficient of X^n

$$n \sigma_n = \sum_{j=1}^{n} \pi_j \sigma_{n-j}.$$

Something similar holds when the characteristic is not 2. All the symmetric functions are elements of $GF(q^2)$, hence we also have the relations

$$\pi_{2k} = \sum_{b \in \mathcal{B}} b^{2k} = \left(\sum_{b \in \mathcal{B}} b^k \right)^2 = \pi_k^2$$

and

$$\pi_{k+q^2-1} = \sum_{b \in \mathcal{B}} b^{k+q^2-1} = \sum_{b \in \mathcal{B}} b^k = \pi_k$$

for $k > 0$.

7. The case $r = 4$ and $q = 8$

In this section we shall be classifying the $(10, 2)$-arcs (hyperovals) in $PG(2, 8)$. It is hoped that the reader will become familiar with the methods and the $q = 16$ case in the next section will be easier to follow.

The possibly non-zero symmetric functions after applying equations (1) are

$$\sigma_0 = 1,\ \sigma_2,\ \sigma_4,\ \sigma_6,\ \sigma_8,\ \sigma_9 \text{ and } \sigma_{10}.$$

The equations (3) imply

$$\sigma_4 = \sigma_2^2 \text{ and } \sigma_8 = \sigma_2^4.$$

The polynomial $B(X)$ has 9 or 10 distinct zeros in $GF(64)$. The symmetric function σ_9 is non-zero otherwise $B(X)$ would be the square of another polynomial and all its zeros would occur with even multiplicity. We now compute π_k in terms of the σ_j's where $j \leq k$ using the k-th Newton identity for each k in turn. The initial Newton identities imply that the initial non-zero π_k's are the following.

$$\begin{aligned}
\pi_9 &= \sigma_9 \\
\pi_{11} &= \sigma_2\sigma_9 \\
\pi_{15} &= \sigma_9(\sigma_6 + \sigma_2^3) \\
\pi_{19} &= \sigma_9(\sigma_6\sigma_2^2 + \sigma_{10}) \\
\pi_{21} &= \sigma_9\sigma_6^2 \\
\pi_{23} &= \sigma_9(\sigma_6^2\sigma_2 + \sigma_2^7 + \sigma_{10}\sigma_2^2) \\
\pi_{25} &= \sigma_9(\sigma_6^2\sigma_2^2 + \sigma_2^8) \\
\pi_{27} &= \sigma_9(\sigma_9^2 + \sigma_6\sigma_2^6 + \sigma_6^3) \\
\pi_{29} &= \sigma_9(\sigma_9^2\sigma_2 + \sigma_2^{10} + \sigma_{10}^2)
\end{aligned}$$

Now we make repeated use of the fact that $\pi_{2k} = \pi_k^2$ and $\pi_{q^2-1+k} = \pi_k$.

$\pi_9^8 = \pi_9$ implies that $\sigma_9 \in GF(8)$.

$\pi_{19} = \pi_{13}^{16} = 0$ and $\sigma_9 \neq 0$ imply that $\sigma_{10} = \sigma_6\sigma_2^2$.

$\pi_{25} = \pi_{11}^8$ implies that $\sigma_2^2\sigma_6^2\sigma_9 = 0$ which implies that $\sigma_2 = 0$ or $\sigma_6 = 0$ and in both cases that $\sigma_{10} = 0$.

If $\sigma_2 \neq 0$ then since $(2, q^2-1) = 1$ we can scale the elements of $\mathcal{B}$ by a suitable scalar in such a way that $\sigma_2 = 1$ and for each maximal arc we find there will be $(q^2-1)q^2$ distinct maximal arcs since we can multiply by a non-zero elements of $GF(q^2)$ and translate by an element of $GF(q^2)$. $\pi_{23}^4 = \pi_{29}$ implies $\sigma_9^4\sigma_2^{28} = \sigma_9\sigma_2^{10} + \sigma_9^3\sigma_2$ and since $\sigma_2 = 1$ and $\sigma_9 \neq 0$ that $\sigma_9^3 = 1 + \sigma_9^2$. This equation has at most 3 solutions and in this case we get a total of at most $3q^2(q^2-1)$ maximal arcs.

If $\sigma_2 = 0$ then $B(X) = 1 + \sigma_6X^6 + \sigma_9X^9$ and each zero of B is a zero of

$$X^9B^8 + \sigma_9^6B^2 + X^3B = \sigma_9^6 + \sigma_6^8 + \sigma_9\sigma_6^2X^3 + \sigma_6^3\sigma_9^5X^6 + X^9 \pmod{X^{64} + X}.$$

The right-hand side has degree 9 and hence the same zeros as $B(X)$ and must be a constant multiple of $B(X)$. This implies that $\sigma_6 = 0$ and $\sigma_9^7 = 1$. Hence in this case we have at most $7q^2$ maximal arcs.

The total number of maximal arcs of degree 2 (hyperovals) in $AG(2,8)$ is therefore at most

$$3q^2(q^2-1) + 7q^2 = q^2(3q^2+4) = 2^8.7^2.$$

The collineation group of the regular hyperoval in $PG(2,q)$ is of size $eq(q^2-1)$ where $q = 2^e$. Hence the number of regular hyperovals in $PG(2,q)$ is

$$\frac{|P\Gamma L(3,q)|}{eq(q^2-1)} = q^2(q^3-1).$$

There are $q(q-1)/2$ external lines to a hyperoval and so there are

$$\frac{q^2(q^3-1)q(q-1)}{2(q^2+q+1)} = q^3(q-1)^2/2$$

regular hyperovals in $AG(2,q)$. In $AG(2,8)$ there are $2^8.7^2$ regular hyperovals and these are indeed all the hyperovals in $AG(2,8)$.

8. The case $r = 4$ and $q = 16$

Throughout the rest of the article we shall only be concerned with the case $q = 16$, that of a $(52, 4)$-arc. We shall make further restrictions on the symmetric functions of $\mathcal{B}$ and then check which of the polynomials $B(X)$ have 51 or 52 distinct zeros in $GF(256)$. Note that if $0 \in \mathcal{B}$ then B will have only 51 distinct zeros and that $x \neq 0$ is a zero of B if and only if $1/x \in \mathcal{B}$. The possibly non-zero symmetric functions σ_i after applying the equations (1) and (4) are those where

$$i \in \{0, 4, 8, 12, 16, 19, 20, 24, 32, 34, 36, 38, 40, 42, 44, 48, 49, 50, 51, 52\}.$$

By definition $\sigma_0 = 1$. The equations (3) imply

$$\sigma_8 = \sigma_4^2,\ \ \sigma_{16} = \sigma_4^4,\ \ \sigma_{24} = \sigma_{12}^2,\ \ \sigma_{38} = \sigma_{19}^2,\ \ \sigma_{40} = \sigma_{20}^2 \text{ and } \sigma_{48} = \sigma_{12}^4$$

which leaves us with the task of determining relationships between the symmetric functions σ_i where

$$i \in \{4, 12, 19, 20, 34, 36, 42, 44, 49, 50, 51, 52\}.$$

The k-th Newton identity allows us to compute the π_k's in terms of σ_j's where $j \leq k$ and one can compute them by hand (although it helps to use a computer package). The tables list restrictions on the coefficients of B. The right-hand column gives the relation that is used to deduce the restriction on the σ_k where the relevant π_k is calculated in terms of σ_j's using the Newton identities.

Before we have to consider different cases we have from earlier calculations that

$$\sigma_{34}^2 = \epsilon_{4,68} = \sum (b_1 \dots b_4)^{16} b_5 \dots b_8 = \epsilon_{4,68}^{16}$$

and hence $\sigma_{34} \in GF(16)$.

We now consider four cases separately. Case I ($\sigma_4 \neq 0$ and $\sigma_{19} \neq 0$), Case II ($\sigma_{19} = 0$ and $\sigma_4 \neq 0$), Case III ($\sigma_4 = 0$ and $\sigma_{19} \neq 0$) and Case IV ($\sigma_4 = \sigma_{19} = 0$).

8.1. Case I

Here we assume that $\sigma_{19} \neq 0$ and $\sigma_4 \neq 0$. Since $\sigma_4 \neq 0$ and $(4, q^2 - 1) = 1$ we can scale the elements of $\mathcal{B}$ by a suitable scalar in such a way that $\sigma_4 = 1$ and for each maximal arc we find there will be $(q^2 - 1)q^2$ different maximal arcs since we can multiply by a non-zero element of $GF(q^2)$ and translate by an element of $GF(q^2)$.

$\sigma_4 = 1$	by assumption
σ_{12} satisfies $\sigma_{12}^5 + \sigma_{12}^3 + \sigma_{12} \in GF(16)$	$\pi_{119}^{16} = \pi_{119}$ and $\pi_{103}^8 = \pi_{59} = 0$ $\pi_{119} = \pi_{119} + \pi_{103} + \sigma_{12}\pi_{99}$
σ_{19}	
$\sigma_{20} = \sigma_{12}$	$\pi_{39}^8 = \pi_{57} = 0$
$\sigma_{34} \in GF(16)$	$\sigma_{34}^2 = \epsilon_{4,68}$
$\sigma_{36} = \sigma_{12}\sigma_{19}\sigma_{34}^8 + \sigma_{12}\sigma_{19}^{136} + \sigma_{19}^2 + \sigma_{12}^{128}\sigma_{19}^{136} + \sigma_{19}\sigma_{34}^8$ $+\sigma_{19}^{136} + \sigma_{19}^{160}\sigma_{34}^2 + \sigma_{19}^{130} + \sigma_{12}^2 + \sigma_{12}^{128}\sigma_{34}$	$\pi_{99}^8 = \pi_{27} = 0$
$\sigma_{42} = \sigma_{12}^2\sigma_{34} + \sigma_{19}^{15}\sigma_{12}^2 + \sigma_{19}^2 + \sigma_{19}^{15}\sigma_{12} + \sigma_{34} + \sigma_{19}^{15}$ $+\sigma_{19}^{63}\sigma_{34}^4 + \sigma_{19}^3$	$\pi_{77} = \pi_{53}^{64}$
$\sigma_{44} = 0$	$\pi_{101}^8 = \pi_{43} = 0$
$\sigma_{49} = \sigma_{19}^{16}$	$\pi_{49} = \pi_{19}^{16}$
$\sigma_{50} = \sigma_{19}^2\sigma_{12} + \sigma_{42}$	$\pi_{69}^4 = \pi_{21} = 0$
$\sigma_{51} \in GF(16)$	$\pi_{51}^{16} = \pi_{51}$
$\sigma_{52} = 0$	$\pi_{71}^4 = \pi_{29} = 0$

The restrictions on the symmetric functions in Case I

Therefore for Case I the polynomial $B(X)$ is of the form

$$1 + X^4 + X^8 + \sigma_{12}X^{12} + X^{16} + \sigma_{19}X^{19} + \sigma_{12}X^{20} + \sigma_{12}^2X^{24} + X^{32} + \sigma_{34}X^{34} + \sigma_{36}X^{36} + \sigma_{19}^2X^{38} + \sigma_{12}^2X^{40} + \sigma_{42}X^{42} + \sigma_{12}^4X^{48} + \sigma_{19}^{16}X^{49} + \sigma_{50}X^{50} + \sigma_{51}X^{51}$$

where σ_{36}, σ_{42} and σ_{50} are all determined by σ_{12}, σ_{19}, σ_{34} and σ_{51}. Moreover σ_{34} and $\sigma_{51} \in GF(16)$ and $\sigma_{12}^5 + \sigma_{12}^3 + \sigma_{12} \in GF(16)$. The mathematical package GAP was used to determine that 835 of these 5.2^{20} polynomials have 51 distinct zeros in $GF(256)$.

8.2. Case II

In this section we assume that $\sigma_{19} = 0$ and $\sigma_4 \neq 0$ and as in Case I we multiply the elements of $\mathcal{B}$ by a non-zero scalar and set $\sigma_4 = 1$. The odd degree coefficients of B cannot be all zero else B is a square and it would not have distinct zeros. Hence we may assume that $\sigma_{51} \neq 0$.

In Case II the polynomial $B(X)$ is of the form

$$1 + X^4 + X^8 + \sigma_{12}X^{12} + X^{16} + \sigma_{12}X^{20} + \sigma_{12}^2X^{24} + X^{32} + \sigma_{34}X^{34} + (\sigma_{12}^2 + \sigma_{12}^2\sigma_{34})X^{36} + \sigma_{12}^2X^{40} + \sigma_{34}\sigma_{12}X^{42} + \sigma_{12}^4X^{48} + \sigma_{34}\sigma_{12}X^{50} + \sigma_{51}X^{51}$$

and GAP was used to determine that 14 of these 2^9 polynomials have 51 distinct zeros in $GF(256)$.

$\sigma_4 = 1$	by assumption
σ_{12} satisfies $\sigma_{12}^2 + \sigma_{12} + 1 = 0$	$\pi_{79}^4 = \pi_{61} = 0$
$\sigma_{19} = 0$	by assumption
$\sigma_{20} = \sigma_{12}$	$\pi_{71}^4 = \pi_{29} = 0$
$\sigma_{34} \in GF(16)$	$\sigma_{34}^2 = \epsilon_{4,68}$
$\sigma_{36} = \sigma_{12}^2(1 + \sigma_{34})$	$\pi_{131}^2 = \pi_7 = 0$
$\sigma_{42} = \sigma_{34}\sigma_{12}$	$\pi_{109} = \pi_{91}^4 = 0$
$\sigma_{44} = 0$	$\pi_{139}^2 = \pi_{23} = 0$
$\sigma_{49} = 0$	$\pi_{49} = \pi_{19}^{16}$
$\sigma_{50} = \sigma_{34}\sigma_{12}$	$\pi_{101}^8 = \pi_{43} = 0$
$\sigma_{51} \in GF(16)^*$	$\pi_{51}^{16} = \pi_{51}$
$\sigma_{52} = 0$	$\pi_{103}^8 = \pi_{59} = 0$

The restrictions on the symmetric functions in Case II

8.3. Case III

Here we assume that $\sigma_4 = 0$ and $\sigma_{19} \neq 0$. Since $\sigma_{19} \neq 0$ and $(19, q^2 - 1) = 1$ we can scale the elements of $\mathcal{B}$ by a suitable scalar in such a way that $\sigma_{19} = 1$.

$\sigma_4 = 0$	by assumption
σ_{12} satisfies $\sigma_{12}^6 = \sigma_{12}$	$\pi_{83}^4 = \pi_{77}$ implies $\sigma_{34}^4 = \sigma_{34}\sigma_{12}^2$ and $\sigma_{34} \in GF(16)$
$\sigma_{19} = 1$	by assumption
$\sigma_{20} = 0$	$\pi_{39}^8 = \pi_{57} = 0$
$\sigma_{34} \in GF(16)$	$\sigma_{34}^2 = \epsilon_{4,68}$
$\sigma_{36} = \sigma_{34}^8 + \sigma_{34}\sigma_{12}^3 + \sigma_{12}^4 + \sigma_{34}$	$\pi_{91} = \pi_{107}^8$
$\sigma_{42} = \sigma_{12}\sigma_{34}^2$	$\pi_{99}^8 = \pi_{27} = 0$
$\sigma_{44} = 0$	$\pi_{101}^8 = \pi_{43} = 0$
$\sigma_{49} = 1$	$\pi_{49} = \pi_{19}^{16}$
$\sigma_{50} = \sigma_{12}$	$\pi_{69}^4 = \pi_{21} = 0$
$\sigma_{51} = \sigma_{34}^9 + \sigma_{34}\sigma_{12}^{128} + \sigma_{12}^4 + \sigma_{34}$	$\pi_{121} = \pi_{47}^8 = 0$
$\sigma_{52} = 0$	$\pi_{71}^4 = \pi_{29} = 0$

The restrictions on the symmetric functions in Case III

There are 3.2^5 polynomials $B(X)$ of the form

$$1+\sigma_{12}x^{12}+x^{19}+\sigma_{12}^2X^{24}+\sigma_{34}X^{34}+(\sigma_{34}^8+\sigma_{12}^3\sigma_{34}+\sigma_{12}^4+\sigma_{34})X^{36}+X^{38}+\sigma_{34}^2\sigma_{12}X^{42}+$$

$$\sigma_{12}^4X^{48}+X^{49}+\sigma_{12}X^{50}+(\sigma_{34}^9+\sigma_{34}\sigma_{12}^3+\sigma_{12}^4+\sigma_{34})X^{51}$$

and GAP was used to determine that 5 of them have 51 distinct zeros in $GF(256)$.

8.4. Case IV

Here we assume that $\sigma_4=0$ and $\sigma_{19}=0$. The equation $\pi_{103}^8=\pi_{59}=0$ implies that $\sigma_{34}\sigma_{12}=0$ and we have to consider the case $\sigma_{34}\neq 0$ (and hence $\sigma_{12}=0$) (Case IV-A) and the case $\sigma_{34}=0$ (Case IV-B) separately. Note also that in this case we do not do any scaling and so each solution will give us q^2 maximal arcs by translation and no more.

$\sigma_4=0$	by assumption
$\sigma_{12}=0$	by assumption
$\sigma_{19}=0$	by assumption
$\sigma_{20}=0$	$\pi_{71}^4=\pi_{29}=0$
$\sigma_{34}\in GF(16)^*$	$\sigma_{34}^2=\epsilon_{4,68}$ and non-zero by asssumption
$\sigma_{36}=0$	$\pi_{87}^4=\pi_{93}$
$\sigma_{42}=0$	$\pi_{93}^4=\pi_{117}$
$\sigma_{44}=0$	$\pi_{139}^2=\pi_{23}=0$
$\sigma_{49}=0$	$\pi_{49}=\pi_{19}^{16}$
$\sigma_{50}=0$	$\pi_{101}^8=\pi_{43}=0$
$\sigma_{51}\in GF(q)$	$\pi_{51}^{16}=\pi_{51}$
$\sigma_{52}=0$	$\pi_{103}^8=\pi_{59}=0$

The restrictions on the symmetric functions in Case IV-A

There are 2^8 polynomials of the form

$$1+\sigma_{34}X^{34}+\sigma_{51}X^{51}$$

and GAP calculates that there are 30 which have 51 distinct zeros in $GF(256)$.

In Case IV-B, if $\sigma_{42}=0$ we have to use the relation $\pi_{159}^2=\pi_{63}$ in conjunction with the other references in the table to prove that all the symmetric functions are zero with the exception of σ_{51} and one can see this corresponds to the solution given by the table in this case. In general we have the following restrictions.

$\sigma_4 = 0$	by assumption
$\sigma_{12} = \sigma_{42}^{129}\sigma_{51}^4$	$\pi_{117} = \pi_{93}^4$
$\sigma_{19} = 0$	by assumption
$\sigma_{20} = 0$	$\pi_{71}^4 = \pi_{29} = 0$
$\sigma_{34} = 0$	by assumption
$\sigma_{36} = \sigma_{42}^{64}\sigma_{51}^3 + \sigma_{51}^2\sigma_{42}^{132}$	$\pi_{87}^4 = \pi_{93}$
σ_{42}	
$\sigma_{44} = 0$	$\pi_{139}^2 = \pi_{23} = 0$
$\sigma_{49} = 0$	$\pi_{49} = \pi_{19}^{16}$
$\sigma_{50} = 0$	$\pi_{101}^8 = \pi_{43} = 0$
σ_{51} where $\sigma_{51}^5 = 1$	$\pi_{51}^{16} = \pi_{51}$ and $\pi_{153}^2 = \pi_{51}$
$\sigma_{52} = 0$	$\pi_{103}^8 = \pi_{59} = 0$

The restrictions on the symmetric functions in Case IV-B

The polynomial $B(X)$ is of the form

$$1 + \sigma_{42}^{129}\sigma_{51}^4 X^{12} + \sigma_{42}^3\sigma_{51}^3 X^{24} + (\sigma_{42}^{64}\sigma_{51}^3 + \sigma_{42}^{132}\sigma_{51}^2)X^{36} + \sigma_{42}X^{42} + \sigma_{42}^6\sigma_{51}X^{48} + \sigma_{51}X^{51}$$

and note that all the non-zero terms are of degree that is a multiple of 3. We have done no scaling so every maximal arc will give exactly q^2 maximal arcs by translation and GAP computes that 600 of these 5.2^8 polynomials have 51 distinct zeros over $GF(256)$.

8.5. The classification of $(52, 4)$-arcs in $PG(2, 16)$

The polynomials in Case I give at most $835q^2(q^2-1)$, in Case II at most $14q^2(q^2-1)$, in Case III at most $5q^2(q^2-1)$ and in Case IV at most $(30+600)q^2$, maximal arcs of degree 4 in $AG(2, 16)$. Hence there are at most

$$q^2(854(q^2-1) + 630) = 2^{13}.3.5^2.7.13$$

$(52, 4)$-arcs in $AG(2, 16)$.

There are two types of maximal arcs in $PG(2, 16)$ both of which are Denniston and they have collineation stablisers of size 68 and 408. The total number of Denniston $(52, 4)$-arcs in $PG(2, 16)$ is therefore

$$|P\Gamma L(3, 16)|(\frac{1}{68} + \frac{1}{408}) = 2^{11}.3^2.5^2.7^2.13.$$

There are 52 external lines to a $(52, 4)$-arc in $PG(2, 16)$ and so the number of Denniston $(52, 4)$-arcs in $AG(2, 16)$ is $2^{11}.3^2.5^2.7^2.13.52/273 = 2^{13}.3.5^2.7.13$.

References

[1] S. Ball and A. Blokhuis, An easier proof of the maximal arcs conjecture, *Proc. Amer. Math. Soc.*, **126**, (1998), 3377–3380.

[2] S. Ball, A. Blokhuis and F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica*, **17**, (1997), 31–47.

[3] A. Blokhuis and F. Mazzocca, There is no $(105, 5)$-arc in $PG(2, 25)$, unpublished notes.

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

[5] M. Hall Jr., Ovals in the Desarguesian plane of order 16, *Ann. Mat. Pura. Appl.*, **102**, (1975), 159–176.

[6] N. Hamilton and T. Penttila, Groups of maximal arcs, *J. Combin. Theory Ser. A*, submitted.

[7] C. M. O'Keefe and T. Penttila, Hyperovals in $PG(2, 16)$, *Europ. J. Combinatorics*, **12**, (1991), 51–59.

[8] T. Penttila and G. Royle, Classification of hyperovals in $PG(2, 32)$, *J. Geom.*, **50**, (1994), 151–158.

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

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