



On the spectrum of non-Denniston maximal arcs in $PG(2, 2^h)$

Nicholas Hamilton^a, Rudolf Mathon^b

^aAdvanced Computational Modelling Centre, The University of Queensland, Brisbane 4072, Australia

^bDepartment of Computer Science, The University of Toronto, Ontario, Canada M5S3G4

Received 10 February 2003; accepted 22 July 2003

Abstract

In 1969, Denniston gave a construction of maximal arcs of degree n in Desarguesian projective planes of even order q , for all n dividing q . Recently, Mathon gave a construction method that generalized that of Denniston. In this paper we use that method to give maximal arcs that are not of Denniston type for all n dividing q , $4 < n < q/2$, q even. It is then shown that there are a large number of isomorphism classes of such maximal arcs when n is approximately \sqrt{q} .

© 2003 Elsevier Ltd. All rights reserved.

Keywords: Maximal arc; Projective plane

1. Introduction

A **maximal** $\{q(n-1) + n; n\}$ -arc in a projective plane of order q is a subset of $q(n-1) + n$ points such that every line meets the set in 0 or n points for some $2 \leq n \leq q$. For such a maximal arc n is called the **degree**. If \mathcal{K} is a maximal $\{q(n-1) + n; n\}$ -arc, the set of lines external to \mathcal{K} is a maximal $\{q(q-n+1)/n; q/n\}$ -arc in the dual plane called the **dual** of \mathcal{K} . It follows that a necessary condition for the existence of a maximal $\{q(n-1) + n; n\}$ -arc in a projective plane of order q is that n divides q . Ball, Blokhuis and Mazzocca have also shown that non-trivial maximal arcs do not exist in odd order Desarguesian projective planes [1].

In [8], Mathon gave a construction method for maximal arcs in Desarguesian projective planes that generalized a previously known construction of Denniston [3]. We begin by describing this construction method.

E-mail addresses: nick@maths.uq.edu.au (N. Hamilton), combin@cs.toronto.edu (R. Mathon).

Let Tr be the usual absolute trace map from the finite field $\text{GF}(q)$ onto $\text{GF}(2)$. We represent the points of the Desarguesian projective plane $\text{PG}(2, q)$ via homogeneous coordinates (a, b, c) over $\text{GF}(q)$, and lines similarly as triples $[u, v, w]$ over $\text{GF}(q)$, and incidence by the usual inner product $au + bv + cw = 0$. For $\alpha, \beta \in \text{GF}(q)$ such that the absolute trace $\text{Tr}(\alpha\beta) = 1$, and $\lambda \in \text{GF}(q)$, define $F_{\alpha,\beta,\lambda}$ to be the conic

$$F_{\alpha,\beta,\lambda} = \{(x, y, z) : \alpha x^2 + xy + \beta y^2 + \lambda z^2 = 0\}$$

and let \mathcal{F} be the union of all such conics. Note that all the conics in \mathcal{F} have the point $F_0 = (0, 0, 1)$ as their nucleus.

For given $\lambda \neq \lambda'$, define a composition

$$F_{\alpha,\beta,\lambda} \oplus F_{\alpha',\beta',\lambda'} = F_{\alpha \oplus \alpha', \beta \oplus \beta', \lambda + \lambda'}$$

where the operator \oplus is defined on $\text{GF}(q) \times \text{GF}(q)$ by

$$a \oplus b = \frac{\lambda a + \lambda' b}{\lambda + \lambda'}.$$

Given some subset \mathcal{C} of \mathcal{F} , we say \mathcal{C} is closed if for every $F_{\alpha,\beta,\lambda} \neq F_{\alpha',\beta',\lambda'} \in \mathcal{C}$, we have that $F_{\alpha \oplus \alpha', \beta \oplus \beta', \lambda + \lambda'} \in \mathcal{C}$. In [8], the following theorem is proved.

Theorem 1 ([8, Theorem 2.4]). *Let \mathcal{C} be a closed set of conics in $\text{PG}(2, q)$, q even. Then the union of the points of the conics of \mathcal{C} together with F_0 form the points of a degree $|\mathcal{C}| + 1$ maximal arc in $\text{PG}(2, q)$.*

In this paper several classes of examples of new maximal arcs were given using his method. See also [5] and [4] for further examples as well as results on the geometric structure and collineation stabilizers of the maximal arcs.

Suppose we choose $\alpha \in \text{GF}(q)$ such that $\text{Tr}(\alpha) = 1$, and let A be a subset of $\text{GF}(q)^*$ such that $A \cup \{0\}$ is closed under addition. Then the set of conics

$$\{F_{\alpha,1,\lambda} : \lambda \in A\}$$

together with the nucleus F_0 is the set of points of a degree $|A| + 1$ maximal arc in $\text{PG}(2, q)$. These maximal arcs were constructed by Denniston in [3].

To describe closed sets of conics we will use the following notation. Suppose we have a closed set of conics where A is the set of values that λ ranges over. Then there are functions $p : A \rightarrow \text{GF}(q)$ and $r : A \rightarrow \text{GF}(q)$ such that the closed set of conics is described by the equations

$$\{p(\lambda)x^2 + xy + r(\lambda)y^2 + \lambda z^2 = 0 : \lambda \in A\}. \tag{1}$$

The following constructions of closed sets of conics are known. All have $p(\lambda) = 1$ for every λ . Let b_0 be a fixed element of absolute trace 1 in the field coordinatising the projective plane.

- (a) Degree q in $\text{PG}(2, q^m)$, with $r(\lambda) = b_0 + b_1\lambda + b_2\lambda^3 + \dots + b_{m-1}\lambda^{2^{m-1}-1}$, $\lambda \in \text{GF}(q)^*$ and fixed $b_i \in \text{Ker}(\text{Tr}_{q^m \rightarrow q})$, $i \geq 1$, and $\text{Tr}_{q^m \rightarrow q}$ is the usual trace from $\text{GF}(q^m)$ to $\text{GF}(q)$ [5].
- (b) Degree 2^{m+1} in $\text{PG}(2, 2^{2m})$, with $r(\lambda) = b_0 + \lambda^{2^{m-1}-1}$, $\lambda \in \{x \in \text{GF}(2^{2m})^* : x^2 + x \in \text{GF}(2^m)\}$ [8].

- (c) Degree 2^{2m+2} in $\text{PG}(2, 2^{4m+2})$, with $r(\lambda) = b_0 + \lambda^3$, $\lambda \in \{x \in \text{GF}(2^{2m})^* : x^2 + x \in \text{GF}(2^m)\}$ [8].
- (d) Degree 8 in $\text{PG}(2, 2^{2m+1})$. Choose $\alpha \in \text{GF}(2^{2m+1})^*$ such that $\text{Tr}(1 + \alpha) = \text{Tr}\left(\frac{1}{1+\alpha}\right) = \text{Tr}\left(\frac{1}{1+\alpha+\alpha^2}\right) = 1$. Then take $(\lambda, r(\lambda)) \in \left\{(\alpha, 1), (\alpha^2, 1), (\alpha + \alpha^2, 1), (1, 1 + \alpha + \alpha^2), (1 + \alpha, 1 + \alpha), \left(1 + \alpha^2, \frac{1}{1+\alpha}\right), \left(1 + \alpha + \alpha^2, \frac{1}{1+\alpha+\alpha^2}\right)\right\}$ [4].
- (e) “Sporadics”. In [8], many examples of closed sets of conics were constructed in $\text{PG}(2, 32)$ and $\text{PG}(2, 64)$ by computer. In $\text{PG}(2, 32)$, three non-Denniston maximal arcs of degree 8 that arise from a closed set of conics were constructed, and a non-Denniston maximal arc of degree 16. The dual of the later maximal arc is in fact the Cherowitzo hyperoval. In $\text{PG}(2, 64)$, 31 non-Denniston maximal arcs of degree 8 that arise from closed sets of conics were constructed, and 90 non-Denniston maximal arcs of degree 16.

Given a closed set of conics the following two theorems can be used to construct more examples.

Theorem 2 ([5]). *Let \mathcal{G} be a closed set of conics in $\text{PG}(2, q)$. Then the equations of the conics of \mathcal{G} give a closed set of conics in $\text{PG}(2, q^m)$, for any $m \geq 1$, m odd.*

Lemma 3 ([5]). *Let \mathcal{G} be a closed set of conics giving rise to a degree $8 \leq n < q/2$ maximal arc \mathcal{K} in $\text{PG}(2, q)$ that is not of Denniston type. Then there exist maximal arcs of degree r that are not of type Denniston in $\text{PG}(2, q)$ for all $r \geq 8$, r dividing n .*

In [4], the following test for when a closed set of conics is not of type Denniston was given.

Lemma 4 ([4, Corollary 2.2]). *Let A be a subset of $\text{GF}(q)$ with functions $p, r : A \rightarrow \text{GF}(q)$ such that $\{p(\lambda)x^2 + xy + r(\lambda)y^2 + \lambda z^2 = 0 : \lambda \in A\}$ is the set of equations for a closed set of conics. Suppose that either $(p(\lambda) + p(\lambda'))/(\lambda + \lambda')$ or $(r(\lambda) + r(\lambda'))/(\lambda + \lambda')$ is a polynomial of degree d in λ and λ' , and that $1 < d < |A| - 1$. Then the closed set of conics gives rise to a maximal arc which is not of Denniston type.*

In the next section a new construction of closed sets of conics will be given using certain quadratic forms on projective spaces. The construction (together with the dual maximal arcs) will give maximal arcs not of Denniston type for all n dividing q , $4 < n < q/2$, q even. In the final section the isomorphism problem will be examined and it will be shown that the new construction gives large numbers of examples when the degree is approximately \sqrt{q} in $\text{PG}(2, q)$, q even.

2. A new construction of closed sets of conics

In this section we give a new construction of closed sets of conics. To do this we will need the following lemma.

Lemma 5. *Let $b_1, b_2 \in \text{GF}(2^h)$, $b_2 \neq 0$, then the function $Q : \text{GF}(2^h)^* \rightarrow \text{GF}(2)$ given by $Q(\lambda) = \text{Tr}(b_1\lambda + b_2\lambda^3)$ is a quadratic form on $\text{GF}(2^h)^*$ considered as a projective space $\text{PG}(h - 1, 2)$ of dimension $h - 1$ over $\text{GF}(2)$.*

Proof. To show that Q is a quadratic form on $\text{PG}(h - 1, 2)$ we first note that $Q(k\lambda) = kQ(\lambda) = k^2Q(\lambda)$ for every $\lambda \in \text{GF}(2^h)^*$ and $k \in \text{GF}(2)$. Further, if we define the form $B : \text{GF}(2^h)^* \times \text{GF}(2^h)^* \rightarrow \text{GF}(2)$ by $B(\lambda, \mu) = Q(\lambda + \mu) - Q(\lambda) - Q(\mu)$ then it is easy algebra to check that this is bilinear. The result follows. \square

Closed sets of conics, and so maximal arcs, may then be constructed as follows.

Theorem 6. *Choose $b_0, b_1, b_2 \in \text{GF}(2^h)$ with $b_2 \neq 0$ and $\text{Tr}(b_0) = 1$. Define the quadratic form $Q(\lambda) = \text{Tr}(b_1\lambda + b_2\lambda^3)$ on $\text{GF}(2^h)^*$ considered as a projective space $\text{PG}(h - 1, 2)$, and let A be a subspace of the associated quadric. Then the set*

$$\{x^2 + xy + (b_0 + b_1\lambda + b_2\lambda^3)y^2 + \lambda z^2 = 0 : \lambda \in A\} \tag{2}$$

is a closed set of conics giving rise to a maximal arc of degree $|A| + 1$.

Proof. We show the set is a closed set of conics. It must first be shown that each of the conics is in \mathcal{F} by observing that for each conic the trace of the product of the coefficients of x^2 and y^2 is one. Note that we have chosen A , so that $Q(\lambda) = \text{Tr}(b_1\lambda + b_2\lambda^3) = 0$ for every $\lambda \in A$. Hence for each $\lambda \in A$, $\text{Tr}(b_0 + b_1\lambda + b_2\lambda^3) = \text{Tr}(b_0) + \text{Tr}(b_1\lambda + b_2\lambda^3) = \text{Tr}(b_0) = 1$, and the trace condition for a closed set of conics is satisfied. Closure under addition is trivial to check. \square

To find out how large a degree such maximal arcs may have, the question that then arises is what is the type of the quadric. We solve this by counting the number of zeros of the quadratic form. Here we have been very lucky in that Carlitz [2] chose to evaluate the sums

$$S(b_1, b_2) = \sum_{x \in \text{GF}(2^h)} e^{\pi i \text{Tr}(b_1x + b_2x^3)} \tag{3}$$

for fixed $b_1, b_2 \in \text{GF}(2^h)$. The main result of Carlitz’s paper is to prove the following.

Theorem 7 ([2]). *In $\text{GF}(2^h)$, $h = 2m + 1$ for some integer m , $S(b_1, b_2)$ is either -2^{m+1} , 0 or 2^{m+1} . In $\text{GF}(2^h)$, $h = 2m$ for some integer m , $S(b_1, b_2)$ is either -2^{m+1} , -2^m , 0 , 2^m or 2^{m+1} . In both cases for h each value does occur for some b_1, b_2 . \square*

With Q as above, the terms in Eq. (3) in the sum are -1 if $Q(x) = 1$ and 1 if $Q(x) = 0$. Hence if t_0 is the number of elements of $\text{GF}(2^h)^*$ such that $Q(x) = 0$, and t_1 is the number such that $Q(x) = 1$, then we have that

$$t_0 + t_1 = 2^h - 1 \quad \text{and} \quad t_0 - t_1 = S(b_1, b_2) - 1,$$

and so $t_0 = 2^{h-1} + S(b_1, b_2)/2 - 1$ is the number of points of the quadric determined by Q in $\text{PG}(h - 1, 2)$.

Hence when $h = 2m + 1$, b_1, b_2 can be chosen to give quadrics in Lemma 5 of size $2^{2m} - 2^m - 1$, $2^{2m} - 1$ or $2^{2m} + 2^m - 1$. It is easily shown that the type of a quadric is determined by the number of points it contains. These three sizes correspond respectively to

- (a) $pQ^-(2m - 1, 2)$. The span of the points of a non-degenerate elliptic quadric $Q^-(2m - 1, 2)$ in some hyperplane $\text{PG}(2m - 1, 2)$ with a point p not contained in that hyperplane.

- (b) A (possibly degenerate) parabolic quadric.
- (c) $pQ^+(2m - 1, 2)$. The span of the points of a non-degenerate hyperbolic quadric $Q^+(2m - 1, 2)$ in some hyperplane $PG(2m - 1, 2)$ with a point p not contained in that hyperplane.

Similarly, when $h = 2m$, we get the cases

- (i) $lQ^-(2m - 3, 2)$. The span of the points of a non-degenerate elliptic quadric $Q^-(2m - 3, 2)$ in some subspace $PG(2m - 3, 2)$ with a line l not meeting that subspace.
- (ii) $Q^-(2m - 1, 2)$. A non-degenerate elliptic quadric.
- (iii) A degenerate parabolic quadric.
- (iv) $Q^+(2m - 1, 2)$. A non-degenerate hyperbolic quadric.
- (v) $lQ^+(2m - 3, 2)$. The span of the points of a non-degenerate hyperbolic quadric $Q^+(2m - 3, 2)$ in some subspace $PG(2m - 3, 2)$ with a line l not meeting that subspace.

Note that in (b) and (iii) above it is not possible from the numerology to determine the dimension of the radical of the quadric. However, in the following we will not be concerned with these two cases.

The cases that give the largest subspaces contained in the above quadrics are (c) and (v), which both contain maximal totally singular subspaces of dimension m . Such a subspace contains $2^{m+1} - 1$ points, and so by Theorem 6 give maximal arcs of degree 2^{m+1} . Hence we have the following theorem.

Theorem 8. *In $PG(2, q)$, $q = 2^{2m}$ or $q = 2^{2m+1}$, $m \geq 2$, there exist $b_0, b_1, b_2 \in GF(q)$, $b_2 \neq 0$, and $A \subset GF(q)$, such that the set*

$$\{x^2 + xy + (b_0 + b_1\lambda + b_2\lambda^3)y^2 + \lambda z^2 = 0 : \lambda \in A\} \tag{4}$$

is a closed set of conics giving rise to a maximal arc of degree 2^{m+1} .

Corollary 1. *In $PG(2, 2^h)$, $h \geq 4$, there exist maximal arcs of degree n that are not of Denniston type for all n dividing q with the possible exceptions of $n = 4$ or $n = q/4$.*

Proof. Suppose \mathcal{K} is a degree 2^{m+1} maximal arc arising from the theorem. Then for $\lambda \neq \lambda' \in A$ we have that

$$\frac{(b_0 + b_1\lambda + b_2\lambda^3) + (b_0 + b_1\lambda' + b_2\lambda'^3)}{\lambda + \lambda'} = b_1 + b_2(\lambda^2 + \lambda\lambda' + \lambda'^2).$$

Since $b_2 \neq 0$, this is a polynomial of degree 2, and since $m \geq 2$, $|A| \geq 7$. Applying Lemma 4 stated in the introduction shows that \mathcal{K} is not of Denniston type.

Considering A as the set of points of a projective space over $GF(2)$ we can take subspaces A' of A (in other words subsets A' of A such that $A' \cup \{0\}$ is closed under addition). It follows immediately that

$$\{x^2 + xy + (b_0 + b_1\lambda + b_2\lambda^3)y^2 + \lambda z^2 = 0 : \lambda \in A'\}$$

is a closed set of conics giving rise to a degree $|A'| + 1$ maximal arc \mathcal{K}' . Exactly the same polynomial argument applies to show that \mathcal{K}' is not of Denniston type as long as

$|A'| - 1 > 2$. Hence degree n maximal arcs are constructed for all n dividing q , with $8 \leq n \leq 2^{m+1}$.

Now $2^{m+1} > \sqrt{q}$, so these maximal arcs together with their duals give non-Denniston maximal arcs for all n dividing q in the range $8 \leq n \leq q/8$. Note that in [5, Corollary 2] it is shown that the dual of a non-Denniston maximal arc arising from a closed set of conics cannot be constructed from a closed set of conics. In particular, the duals are not of Denniston type.

Finally, a maximal arc of degree 2 that is of Denniston type is just a regular hyperoval. Hyperovals that are not regular are known for all $q = 2^h$, $h \geq 4$ (see [6, Chapter 8]). The degree $q/2$ maximal arcs that are the duals of these are also not of Denniston type. \square

3. Isomorphism of the new maximal arcs

In [8, Table 1], 31 degree 8 maximal arcs in $\text{PG}(2, 64)$ that are not of Denniston type and that arise from closed sets of conics are given. All of them can be understood as being maximal arcs of the type given in Theorem 8 and the corollary. However, of the 91 degree 16 non-Denniston maximal arcs in $\text{PG}(2, 64)$ given in the same paper, only two can be understood in this way. Of the classes of known examples (as listed in the introduction) it is clear that the current construction includes those of (c) as a subclass. Taking $m = 2$ in the class (a) gives maximal arcs which are each a subset of a maximal arc of the current construction. Otherwise, the current construction appears to give new maximal arcs.

We conclude by giving a lower bound on the number of maximal arcs arising from Theorem 8. First consider the case $q = 2^{2m+1}$. Choose b_0, b_1 and b_2 to give the quadric $pQ^+(2m-1, 2)$. Then A can be chosen to be any maximal totally singular subspace of the quadric. Now two conics have the same point set if and only if their quadratic equations are scalar multiples of each other. It follows that each choice of A gives rise to a distinct set of conics in the plane. In [5, Theorem 6] it is shown that if a maximal arc \mathcal{K} of degree $n < q/2$ arises from a closed set of conics, then there are no conics contained in the maximal arc apart from those of the closed set. It follows that distinct maximal totally singular subspaces in $pQ^+(2m-1, 2)$ give rise to distinct point sets in $\text{PG}(2, 2^{2m+1})$.

The number of maximal totally singular subspaces of $pQ^+(2m-1, 2)$ is the same as the number of maximal totally singular subspaces of the quadric $Q^+(2m-1, 2)$, which is well known to be $2(2+1)(2^2+1)\dots(2^{m-1}+1)$ (see [6, Theorem 5.23]). Hence for given b_0, b_1 and b_2 we have $N = 2(2+1)(2^2+1)\dots(2^{m-1}+1)$ distinct maximal arcs of degree 2^{m+1} in $\text{PG}(2, 2^{2m+1})$. The order of the collineation stabilizer of the plane $\text{PG}(2, 2^{2m+1})$ is $G = (2m+1)q^3(q^3-1)(q^2-1)$, $q = 2^{2m+1}$. The number of isomorphism classes of such maximal arcs must then be at least N/G .

Now $N > 2(2 \cdot 2^2 \cdot 2^3 \dots 2^{m-1}) = 2 \cdot 2^{1+2+3+\dots+m-1} = 2^{m(m-1)/2+1} = 2^{11/8}q^{m/4-3/8}$, and $G < q^9$. Hence $N/G > 2^{11/8}q^{m/4-9-3/8}$, and so for carefully chosen b_0, b_1 and b_2 there are at least $2q^{m/4-10}$ isomorphism classes of maximal arcs of degree $\sqrt{2q}$ in $\text{PG}(2, q)$, $q = 2^{2m+1}$, that are not of Denniston type. Similar calculations for when $q = 2^{2m}$ show that for given b_0, b_1 and b_2 , Theorem 8 gives at least $4q^{m/4-10}$ isomorphism classes of maximal arcs of degree \sqrt{q} in $\text{PG}(2, q)$, that are not of Denniston type. Hence we have the following theorem.

Theorem 9. *In $\text{PG}(2, q)$, $q = 2^{2m+1}$, the number of isomorphism classes of maximal arcs of degree $\sqrt{2q}$ that are not of Denniston type is bounded below by $2q^{m/4-10}$. In $\text{PG}(2, q)$, $q = 2^{2m}$, the number of isomorphism classes of maximal arcs of degree $2\sqrt{q}$ that are not of Denniston type is bounded below by $4q^{m/4-10}$.*

Suppose, as in the proof of [Corollary 1](#), instead of taking maximal totally singular subspaces of $pQ^+(2m-1, 2)$ and $lQ^+(2m-3, 2)$ we take smaller dimension subspaces to give our sets A to construct (smaller degree) maximal arcs. Then the number of subspaces of a given dimension in the quadrics is well known (see [[7](#), Theorem 22.5.1]) and similar calculations to the above are possible. However, the number of subspaces substantially reduces with the dimension of the subspaces. The above method then shows there are many (more than $\sim q^{m/4}$) maximal arcs of degree around \sqrt{q} using subspaces of quadrics. But for small degrees (i.e. near to 8) the number of subspaces is of roughly the same order as G and so we get little information on how many isomorphism classes there may be.

We conclude by noting that classes of larger degree maximal arcs arising from closed sets of conics may well exist. But the only example we know of with a non-Denniston maximal arc of degree 2^{m+2} in a $\text{PG}(2, 2^{2m+1})$ having $p(\lambda) = 1$ occurs in $\text{PG}(2, 512)$ for $r(\lambda) = 1 + \lambda^7$ with λ in the union of nine multiplicative cosets of $\text{GF}(8)^*$ given by $A = \{\alpha^{17 \cdot 2^j + 73 \cdot \alpha^i} \mid i = 0, \dots, 6, j = 0, \dots, 8\}$, where α is a fixed element of $\text{GF}(512)$ satisfying $\alpha^{130} + \alpha = 1$.

Acknowledgement

Rudolf Mathon was supported by NSERC grant OGP0008651.

References

- [1] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica* 17 (1997) 31–41.
- [2] L. Carlitz, Explicit evaluation of certain exponential sums, *Math. Scand.* 44 (1979) 5–16.
- [3] R.H.F. Denniston, Some maximal arcs in finite projective planes, *J. Combin. Theory* 6 (1969) 317–319.
- [4] N. Hamilton, Degree 8 maximal arcs in $\text{PG}(2, 2^h)$, h odd, *J. Combin. Theory Ser. A* 100 (2002) 265–276.
- [5] N. Hamilton, R. Mathon, More maximal arcs in Desarguesian projective planes and their geometric structure, *Adv. Geom.* 3 (2003) 251–261.
- [6] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1998.
- [7] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*, Oxford University Press, Oxford, 1991.
- [8] R. Mathon, New maximal arcs in Desarguesian planes, *J. Combin. Theory Ser. A* 97 (2002) 353–368.