Special Issue (2003), S119–S139 **Advances in Geometry**

On Mathon's construction of maximal arcs in Desarguesian planes

Frank Fiedler, Ka Hin Leung and Qing Xiang

Dedicated to Adriano Barlotti on the occasion of his 80th birthday

Abstract. We study the problem of determining the largest d of a non-Denniston maximal arc of degree 2^d generated by a $\{p,1\}$-map in $\mathrm{PG}(2,2^m)$ via a recent construction of Mathon [9]. On one hand, we show that there are $\{p,1\}$-maps that generate non-Denniston maximal arcs of degree $2^{(m+1)/2}$, where $m \geqslant 5$ is odd. Together with Mathon's result [9] in the m even case, this shows that there are always $\{p,1\}$-maps generating non-Denniston maximal arcs of degree $2^{\lfloor (m+2)/2 \rfloor}$ in $\mathrm{PG}(2,2^m)$. On the other hand, we prove that the largest degree of a non-Denniston maximal arc in $\mathrm{PG}(2,2^m)$ constructed using a $\{p,1\}$-map is less than or equal to 2^{m-3}. We conjecture that this largest degree is actually $2^{\lfloor (m+2)/2 \rfloor}$ when $m > 9$.

Key words. Arc, linearized polynomial, maximal arc, quadratic form.

1 Introduction

Let $\mathrm{PG}(2,q)$ be the Desarguesian projective plane of order q, q a prime power. A set of k points in $\mathrm{PG}(2,q)$ is called a (k,n)-*arc* if no $n+1$ points of the set are collinear. The number n is usually called the *degree* of the arc.

Let $\mathscr{K}$ be a (k,n)-arc in $\mathrm{PG}(2,q)$, and let P be a point in $\mathscr{K}$. Then each of the $q+1$ lines through P contains at most $n-1$ points of $\mathscr{K}$. Therefore

$$k \leqslant 1 + (q+1)(n-1) = qn + n - q.$$

A (k,n)-arc is said to be *maximal* if $k = qn + n - q$. From the above argument, it is easily seen that any line of $\mathrm{PG}(2,q)$ that contains a point of a maximal arc $\mathscr{K}$ must contain exactly n points of that arc; that is

$$|L \cap \mathscr{K}| = 0 \text{ or } n$$

for every line L of $\mathrm{PG}(2,q)$. Therefore the degree n of a maximal $(qn+n-q,n)$-arc must divide q.

The study of arcs of degree greater than two was started by Barlotti [2]. For $q = 2^m$, Denniston [3] constructed maximal $(qn+n-q,n)$-arcs in $\mathrm{PG}(2,q)$ for every

n, $n \mid q$, $n < q$ (see also [6, p. 304]). Thas [10], [11] also gave two other constructions of maximal arcs of certain degrees in $\mathrm{PG}(2, 2^m)$, where m is even. For odd prime powers q, Ball, Blokhuis and Mazzocca [1] proved that maximal arcs of degree n do not exist in $\mathrm{PG}(2, q)$, when $n < q$. Recently Mathon [9] gave a new construction of maximal arcs in $\mathrm{PG}(2, 2^m)$ that generalizes the construction of Denniston. We give a brief account of his construction.

Let $\mathscr{C}$ be the set of all conics

$$F_{\alpha,\beta,\lambda} = \{(x, y, z) \in \mathrm{PG}(2, 2^m) \mid \alpha x^2 + xy + \beta y^2 + \lambda z^2 = 0\}$$

where $\alpha, \beta \in \mathbb{F}_{2^m}^*$ and $\alpha x^2 + x + \beta$ is irreducible over $\mathbb{F}_{2^m}$ (that is, $\mathrm{Tr}_{2^m/2}(\alpha\beta) = 1$, here $\mathrm{Tr}_{2^m/2}$ is the trace map from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$). For $\lambda, \lambda' \in \mathbb{F}_{2^m}$, $\lambda \neq \lambda'$ we define a composition

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

where

$$a \oplus a' = \frac{a\lambda + a'\lambda'}{\lambda + \lambda'} \quad \text{for any } a, a' \in \mathbb{F}_{2^m}.$$

A subset $\mathscr{F}$ of $\mathscr{C}$ is said to be *closed* under the composition $\oplus$ if for any $F_1, F_2 \in \mathscr{F}$ with $F_1 \neq F_2$ we have $F_1 \oplus F_2 \in \mathscr{F}$. In [9] Mathon proved that the set of points of all conics in a closed set of conics together with the common nucleus $F_0 = F_{\alpha,\beta,0} = (0, 0, 1)$ forms a maximal arc in $\mathrm{PG}(2, 2^m)$. When all conics in a closed set of conics come from a single pencil of conics, Mathon's construction gives rise to Denniston maximal arcs. In general, Mathon showed that closed sets of conics can be obtained by using linearized polynomials over $\mathbb{F}_{2^m}$. Specifically, Mathon proved the following theorem.

Theorem 1.1 ([9, Theorem 2.5]). *Let* $p(x) = \sum_{i=0}^{d-1} a_i x^{2^i-1}$ *and* $q(x) = \sum_{i=0}^{d-1} b_i x^{2^i-1}$ *be polynomials with coefficients in* $\mathbb{F}_{2^m}$. *For an additive subgroup* A *of order* 2^d *in* $\mathbb{F}_{2^m}$ *let* $\mathscr{F} = \{F_{p(\lambda),q(\lambda),\lambda} \mid \lambda \in A\backslash\{0\}\} \subset \mathscr{C}$ *be a set of conics with common nucleus* F_0. *If* $\mathrm{Tr}_{2^m/2}(p(\lambda)q(\lambda)) = 1$ *for every* $\lambda \in A\backslash\{0\}$, *then the set of points on all conics in* $\mathscr{F}$ *together with* F_0 *forms a maximal* $(2^{m+d} - 2^m + 2^d, 2^d)$*-arc* $\mathscr{K}$ *in* $\mathrm{PG}(2, 2^m)$. *If both* $p(x)$, $q(x)$ *have* $d \leqslant 2$, *then* $\mathscr{K}$ *is a Denniston arc.*

Hamilton [4] gave the following test for when the arc $\mathscr{K}$ in Theorem 1.1 is a Denniston arc.

Theorem 1.2 ([4, Theorem 2.1]). *Let* $p(x)$ *and* $q(x)$ *be the same polynomials as given in Theorem* 1.1, *let* A *be an additive subgroup of size* 2^d *in* $\mathbb{F}_{2^m}$, *and let* $\mathscr{K}$ *be the maximal arc obtained in Theorem* 1.1. *Then* $\mathscr{K}$ *is of Denniston type if and only if for all* $\lambda, \lambda' \in A\backslash\{0\}$, $\lambda \neq \lambda'$, *both* $(p(\lambda) + p(\lambda'))/(\lambda + \lambda')$ *and* $(q(\lambda) + q(\lambda'))/(\lambda + \lambda')$ *are constant.*

Mathon posed several problems at the end of his paper [9]. The third problem he posed is: What is the largest d of a non-Denniston maximal arc of degree 2^d generated by a $\{p, q\}$-map in $PG(2, 2^m)$ via Theorem 1.1? When m is even, Mathon [9] showed that there exists a non-Denniston maximal arc of degree $2^{m/2+1}$ generated by a $\{p, 1\}$-map in $PG(2, 2^m)$. When m is odd, Hamilton [4] showed that there exists a non-Denniston maximal arc of degree 8 generated by a $\{p, 1\}$-map in $PG(2, 2^m)$, where $m \geqslant 5$. In this paper, we concentrate on the following restricted version of Mathon's problem: What is the largest d of a non-Denniston maximal arc of degree 2^d generated by a $\{p, 1\}$-map in $PG(2, 2^m)$ via Theorem 1.1? In Section 2, we show that there are $\{p, 1\}$-maps that generate non-Denniston maximal arcs of degree $2^{(m+1)/2}$, where $m \geqslant 5$ is odd. Together with Mathon's result [9, Theorem 3.2] in the m even case, this shows that there are always $\{p, 1\}$-maps generating non-Denniston maximal arcs of degree $2^{\lfloor (m+2)/2 \rfloor}$ in $PG(2, 2^m)$. In Section 3 we prove that if a maximal arc generated by a $\{p, 1\}$-map via Theorem 1.1 has degree 2^{m-1} or 2^{m-2} and $m \geqslant 7$, then it is a Denniston maximal arc. Hence when $m \geqslant 7$, the largest degree of a non-Denniston maximal arc constructed using a $\{p, 1\}$-map via Theorem 1.1 is less than or equal to 2^{m-3}. We conjecture that when $m > 9$, this largest degree is actually $2^{\lfloor (m+2)/2 \rfloor}$ and provide some evidence for this conjecture.

2 Maximal arcs in $PG(2, 2^m)$, m odd

In this section m is always an odd positive integer, and γ always denotes an element of $\mathbb{F}_{2^m}$ with $\mathrm{Tr}_{2^m/2}(\gamma) = 1$. To simplify notation, from now on, we will use Tr in place of $\mathrm{Tr}_{2^m/2}$ if there is no confusion. We start with the following lemma.

Lemma 2.1. *Let* $S_\gamma = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}(\gamma x + x^3) = 0\}$. *Then there exists a choice of* $\gamma \in \mathbb{F}_{2^m}$ *such that* S_γ *contains an* $\mathbb{F}_2$*-subspace* A *with* $\dim(A) = \frac{m+1}{2}$.

Proof. Let $Q_\gamma(x) = \mathrm{Tr}(\gamma x + x^3)$ and let $V = \mathbb{F}_{2^m}$. The map $Q_\gamma : V \to \mathbb{F}_2$ is a quadratic form on V over $\mathbb{F}_2$. The corresponding bilinear form B is given by $B(x, y) = Q_\gamma(x + y) - Q_\gamma(x) - Q_\gamma(y) = \mathrm{Tr}(x^2 y + x y^2)$, hence

$$\begin{aligned}
\mathrm{Rad}\, V &= \{x \in V \mid B(x, y) = 0 \text{ for each } y \in V\} \\
&= \{x \in V \mid \mathrm{Tr}(x^2 y + x y^2) = 0 \text{ for each } y \in V\} \\
&= \{x \in V \mid \mathrm{Tr}(y(x^2 + \sqrt{x})) = 0 \text{ for each } y \in V\} \\
&= \{x \in V \mid x^2 = \sqrt{x}\}.
\end{aligned}$$

Since m is odd, we conclude that $\mathrm{Rad}\, V = \mathbb{F}_2$. Note that in characteristic 2, the quadratic form $Q_\gamma(x)$ is not necessarily zero on $\mathrm{Rad}\, V$. Therefore we define

$$V_0 = \{x \in \mathrm{Rad}\, V \mid Q_\gamma(x) = 0\}.$$

This is an $\mathbb{F}_2$-space of dimension equal to $\dim(\mathrm{Rad}\, V)$ or $\dim(\mathrm{Rad}\, V) - 1$. Since $\mathrm{Tr}(\gamma) = 1$, we have $V_0 = \mathrm{Rad}\, V = \mathbb{F}_2$. Hence $\mathrm{rank}(Q_\gamma) = m - 1$ is even and Q_γ is either hyperbolic or elliptic. It is always possible to choose $\gamma \in \mathbb{F}_{2^m}$, with $\mathrm{Tr}(\gamma) = 1$, such that Q_γ is hyperbolic on V/V_0. (This can be seen from the weight distribution of the dual of the double-error-correcting BCH code, see [8, p. 451]). With this choice of γ, the maximum dimension of a subspace of V/V_0 on which Q_γ vanishes is $\frac{m-1}{2}$. Let U be such a subspace and let $A = U \perp V_0$. Then $\dim(A) = \frac{m+1}{2}$ and $Q_\gamma(x)$ vanishes on A, hence $A \subset S_\gamma$. This completes the proof. □

Now let $\gamma \in \mathbb{F}_{2^m}$ be chosen such that $\mathrm{Tr}(\gamma) = 1$ and $S_\gamma = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}(\gamma x + x^3) = 0\}$ contains an $\mathbb{F}_2$-subspace A of $\mathbb{F}_{2^m}$ of dimension $\frac{m+1}{2}$. Let $p(x) = 1 + \gamma x + x^3$. Then we have the following corollary of Theorem 1.1.

Theorem 2.2. *The set of points on the conics* $\mathscr{F} = \{F_{p(\lambda),1,\lambda} \mid \lambda \in A \backslash \{0\}\}$ *together with the common nucleus* F_0 *forms a maximal arc* $\mathscr{K}$ *in* $\mathrm{PG}(2, 2^m)$ *of degree* $2^{(m+1)/2}$. *When* $m \geqslant 5$, *the maximal arc* $\mathscr{K}$ *is non-Denniston.*

Proof. Let $p(\lambda) = 1 + \gamma\lambda + \lambda^3$, with the choice of γ as above, and let A be the $(\frac{m+1}{2})$-dimensional $\mathbb{F}_2$-subspace in S_γ given by Lemma 2.1. Then we have $\mathrm{Tr}(p(\lambda)) = \mathrm{Tr}(1) = 1$ for every $\lambda \in A \backslash \{0\}$. By Theorem 1.1, the first part of the theorem follows.

When $m \geqslant 5$, the maximal arc $\mathscr{K}$ is non-Denniston. This can be seen as follows. For $\lambda, \lambda' \in A \backslash \{0\}$, $(p(\lambda) + p(\lambda'))/(\lambda + \lambda') = \gamma + \lambda^2 + \lambda\lambda' + \lambda'^2$. When $|A| \geqslant 8$, this expression cannot be constant when λ, λ', $\lambda \neq \lambda'$, run through $A \backslash \{0\}$. Therefore by Theorem 1.2, the arc $\mathscr{K}$ is not of Denniston type. □

Theorem 2.2 together with Mathon's result ([9, Theorem 3.2]) in the m even case shows that there are always $\{p, 1\}$-maps generating non-Denniston maximal arcs of degree $2^{\lfloor (m+2)/2 \rfloor}$ in $\mathrm{PG}(2, 2^m)$, when $m \geqslant 5$.

3 Some upper bounds on the degree of non-Denniston maximal arcs from $\{p, 1\}$-maps

We start this section by making some remarks about Theorem 1.1. In Theorem 1.1, Mathon restricted the degrees of the polynomials $p(\lambda)$, $q(\lambda)$ to be less than or equal to $2^{d-1} - 1$, where the subspace $A \subset \mathbb{F}_{2^m}$ involved has size 2^d. We will show that there is no loss of generality in doing so.

Proposition 3.1. *Let* $f(x) = \sum_{i=0}^{m-1} a_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$, *and let* A *be an* $\mathbb{F}_2$-*subspace in* $\mathbb{F}_{2^m}$ *of size* 2^d, *where* $d \leqslant m - 1$. *Then there exists a polynomial* $f_1(x) = \sum_{i=0}^{d-1} b_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$ *such that* $f(\lambda) = f_1(\lambda)$ *for every* $\lambda \in A \backslash \{0\}$.

Proof. Let $A(x) = \prod_{\lambda \in A}(x - \lambda)$. This is a degree 2^d linearized polynomial in $\mathbb{F}_{2^m}[x]$ (see [7, p. 110], also [8, p. 119]), that is,

$$A(x) = x^{2^d} + c_{d-1}x^{2^{d-1}} + \cdots + c_0 x,$$

where $c_i \in \mathbb{F}_{2^m}$. Let $a(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$. The polynomials $A(x)$ and $a(x)$ are called 2-*associates* of each other (see [7, p. 115]). Let $f(x) = G(x)/x$, where $G(x) =$

$\sum_{i=0}^{m-1} a_i x^{2^i}$, and let $g(x) = \sum_{i=0}^{m-1} a_i x^i$ be the 2-associate of $G(x)$. Using the division algorithm, we write

$$g(x) = k(x)a(x) + r(x), \tag{3.1}$$

where $\deg r(x) < \deg a(x) = d$. Let $K(x)$ and $R(x)$ be the 2-associates of $k(x)$ and $r(x)$ respectively. Turning (3.1) into linearized 2-associates, and noting that the 2-associate of $k(x)a(x)$ is $K(A(x))$, the composition of $A(x)$ with $K(x)$ (cf. [7, p. 115], Lemma 3.59), we get

$$G(x) = K(A(x)) + R(x), \tag{3.2}$$

with $\deg R(x) \leqslant 2^{d-1}$. With $f_1(x) = R(x)/x$, we see from (3.2) that $f(\lambda) = f_1(\lambda)$ for every $\lambda \in A\backslash\{0\}$. □

We note that if one does not restrict the degree of the polynomials $p(x)$, $q(x)$ to be less than or equal to $2^{d-1} - 1$ (where $2^d = |A|$), Theorem 1.1 still holds, but then it sometimes leads to Denniston maximal arcs, which, at first sight, may not look like Denniston. We give a couple of examples of this situation below. So by restricting the degrees of the polynomials $p(x)$, $q(x)$ to be less than or equal to $2^{d-1} - 1$ in Theorem 1.1, not only is there no loss of generality (by Proposition 3.1), but also some "trivial" examples are avoided.

Example 3.2. Let $p(x) = a_0 + \frac{x + x^2 + x^4 + \cdots + x^{2^{m-1}}}{x} \in \mathbb{F}_{2^m}[x]$, where $\mathrm{Tr}(a_0) = 1$. Let $A = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}(x) = 0\}$. Then we have $\mathrm{Tr}(p(\lambda)) = 1$ for every $\lambda \in A\backslash\{0\}$. This $p(x)$ indeed gives rise to a maximal arc of degree 2^{m-1} in $\mathrm{PG}(2, 2^m)$ by Mathon's construction. But the maximal arc in this example is of Denniston type by Theorem 1.2 since for every $\lambda \in A\backslash\{0\}$, we have $p(\lambda) = a_0$, a constant.

Example 3.3. Let $p(x) = \sum_{i=0}^{m-1} a_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$, where $\mathrm{Tr}(a_0) = 1$. We may choose $a_1, a_2, \ldots, a_{m-1} \in \mathbb{F}_{2^m}$ such that $A = \{\lambda \in \mathbb{F}_{2^m} \mid a_1\lambda^2 + a_2\lambda^{2^2} + \cdots + a_{m-1}\lambda^{2^{m-1}} = 0\}$ has dimension $m - 2$ over $\mathbb{F}_2$. Then we have $\mathrm{Tr}(p(\lambda)) = 1$ for every $\lambda \in A\backslash\{0\}$. This $p(x)$ gives rise to a maximal arc of degree 2^{m-2} in $\mathrm{PG}(2, 2^m)$ by Mathon's construction. But the maximal arc in this example is again of Denniston type by Theorem 1.2 since for every $\lambda \in A\backslash\{0\}$, $p(\lambda) = a_0$, a constant.

Next we prove that when $m \geqslant 5$ the largest d of a non-Denniston maximal arc of degree 2^d generated by a $\{p, 1\}$-map via Theorem 1.1 is less than $m - 1$.

Theorem 3.4. *Let A be an additive subgroup of size 2^{m-1} in $\mathbb{F}_{2^m}$, where $m \geqslant 5$. Let $p(x) = \sum_{i=0}^{m-2} a_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$. If $\mathrm{Tr}(p(\lambda)) = 1$ for all $\lambda \in A\backslash\{0\}$, then $a_2 = a_3 = \cdots = a_{m-2} = 0$, thus $p(x)$ is linear and the maximal arc obtained via Theorem* 1.1 *is of Denniston type.*

Proof. Every hyperplane in $\mathbb{F}_{2^m}$ can be written as $\{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}(ax) = 0\}$ for some nonzero $a \in \mathbb{F}_{2^m}$. By making a change of variable in $p(x)$, we may assume that $A = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}(x) = 0\}$. We consider two cases.

Case 1: $\mathrm{Tr}(a_0) = 1$. In this case, if $\mathrm{Tr}(p(\lambda)) = 1$ for all $\lambda \in A\backslash\{0\}$, then $\mathrm{Tr}(\sum_{i=1}^{m-2} a_i \lambda^{2^i-1}) = 0$ for all $\lambda \in A\backslash\{0\}$. Thus, $(1 + \mathrm{Tr}(x))\,\mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1})$, viewed as a function from $\mathbb{F}_{2^m}$ to itself, is identically zero. That is, in $\mathbb{F}_{2^m}[x]$, we have

$$(1 + \mathrm{Tr}(x)) \cdot \mathrm{Tr}\left(\sum_{i=1}^{m-2} a_i x^{2^i-1}\right) \equiv 0 \pmod{x^{2^m} - x} \tag{3.3}$$

Let $t(x) = \text{LHS of (3.3)} = (1 + x + x^2 + \cdots + x^{2^{m-1}})\,\mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1})$.

Claim: The coefficient of $x^{2^m-2^r+2}$ in $t(x)$ is $a_{m-r}^{2^r} + a_{m-r+1}^{2^r}$ for $3 \leqslant r \leqslant m-2$.

The m-bit binary representation of $2^m - 2^r + 2$ is

$$\underbrace{1\ldots1}_{m-r\geqslant 2}\underbrace{0\ldots0}_{r-2\geqslant 1}10,$$

which contains two blocks of 1's (separated by 0's). (We will always number the bits from right to left as $0, 1, 2, \ldots, m-1$.) Note that the exponents of the summands in $1 + \mathrm{Tr}(x)$, written in m-bit binary representation, are $000\ldots000$, $000\ldots001$, $000\ldots010, \ldots, 100\ldots000$, and the exponents of the summands in $\mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1})$ are cyclic shifts of

$$000\ldots001, 000\ldots011, 000\ldots0111, 000\ldots01111, \ldots \quad \text{and} \quad \underbrace{00}_{2}\underbrace{11\ldots111}_{m-2}.$$

When we multiply $1 + \mathrm{Tr}(x)$ with $\mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1})$, there are two ways to obtain $x^{2^m-2^r+2}$, namely adding the exponent of a summand in $1 + \mathrm{Tr}(x)$ to the exponent of a summand in $\mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1})$ with or without carry.

Suppose that we are in the latter case. The exponent from $1 + \mathrm{Tr}(x)$ must be 2 while the exponent from $\mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1})$ is a shift of $2^{m-r} - 1$.

$$\underbrace{1\ldots1}_{m-r\geqslant 2}0\ldots010 = 0\ldots010 + \underbrace{1\ldots1}_{m-r\geqslant 2}\underbrace{0\ldots0}_{r}$$

Thus, this case contributes the coefficient $a_{m-r}^{2^r}$.

Now suppose that we are in the former case. Since bit-1 of $2^m - 2^r + 2$ is 1 while bit-0 is 0, the exponent $2^m - 2^r + 2$ must be obtained as 2^0 added to $(2^m - 2^r) + (2^1 - 2^0)$:

$$\underbrace{1\ldots1}_{m-r\geqslant 2}0\ldots010 = 0\ldots01 + \underbrace{1\ldots1}_{m-r\geqslant 2}0\ldots01,$$

so this case contributes the coefficient $a_{m-r+1}^{2^r}$. The claim now follows. In particular, by (3.3), we find that $a_2 = a_3 = \cdots = a_{m-2}$.

Claim: The coefficient of x^{2^m-4} in $t(x)$ is $a_{m-2}^4 + a_{m-3}^4 + a_{m-3}^8$.

Clearly the exponent $(2^m - 4) = 11\dots100$ can be obtained by

$$11\dots100 = 00\dots000 + 11\dots100$$

This contributes the coefficient a_{m-2}^4.

Also the exponent $2^m - 4$ can be obtained by adding a non-zero exponent in $1 + \mathrm{Tr}(x)$ to an exponent from $\mathrm{Tr}(\sum_{i=2}^{m-2} a_i x^{2^i-1})$. Suppose that when adding the exponents, there is no carry. We have two ways to obtain $2^m - 4$, namely,

$$11\dots100 = 10\dots0 + 011\dots100,$$
$$11\dots100 = 0\dots0100 + 11\dots1000.$$

This contributes the coefficient $a_{m-3}^4 + a_{m-3}^8$. Finally we note that there is no way of getting $2^m - 4$ as a sum of exponents inducing a carry. Thus, the coefficient of x^{2^m-4} in $t(x)$ is as claimed. This implies $a_{m-3} = 0$, which yields $a_2 = a_3 = \cdots = a_{m-2} = 0$. Hence $p(\lambda) = a_0 + a_1\lambda$.

Case 2: $\mathrm{Tr}(a_0) = 0$. We have $\mathrm{Tr}(\sum_{i=1}^{m-2} a_i \lambda^{2^i-1}) = 1$ for all $\lambda \in A\backslash\{0\}$. Hence $(1 + \mathrm{Tr}(x)) \cdot (1 + \mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1}))$, viewed as a function from $\mathbb{F}_{2^m}$ to itself, is the characteristic function of the subset $\{0\}$ of $\mathbb{F}_{2^m}$. Therefore,

$$(1 + \mathrm{Tr}(x)) + (1 + \mathrm{Tr}(x)) \cdot \mathrm{Tr}\left(\sum_{i=1}^{m-2} a_i x^{2^i-1}\right) \equiv 1 - x^{2^m-1} \pmod{x^{2^m} - x} \quad (3.4)$$

Note that the binary representation of the exponent of x^{2^m-1} is $111\dots1$ (m ones altogether), while in the left hand side of (3.4), the binary representation of the exponent of any term in the product $(1 + \mathrm{Tr}(x)) \cdot \mathrm{Tr}(\sum_{i=1}^{m-2} a_i x^{2^i-1})$ cannot have more than $1 + (m - 2) = m - 1$ ones. So (3.4) cannot hold. Thus, this case does not occur. This completes our proof. □

Remarks. (1) Theorem 3.4 is not true when $m = 4$. In PG(2, 16), there exists a degree 8 non-Denniston maximal arc (cf. Section 4.1 of [9]).

(2) It is interesting to note that when $m \geqslant 5$ a non-Denniston maximal arc of degree 2^{m-1} (i.e., the dual of a hyperoval) in $\mathrm{PG}(2, 2^m)$ can be obtained from $\{p, q\}$-maps via Theorem 1.1, with $q(x) \neq 1$. See [9, p. 362] for an example in PG(2, 32). Theorem 3.4 shows that this cannot be achieved if $m \geqslant 5$ and $q(x)$ is restricted to be 1.

The ideas in the proof of Theorem 3.4 can be further used to prove the following theorem. The proof contains more complicated computations.

Theorem 3.5. *Let A be an additive subgroup of size 2^{m-2} in $\mathbb{F}_{2^m}$, where $m \geqslant 7$. Let $p(x) = \sum_{i=0}^{m-3} a_i x^{2^i-1} \in \mathbb{F}_{2^m}[x]$. If $\mathrm{Tr}(p(\lambda)) = 1$ for all $\lambda \in A\backslash\{0\}$ then $a_2 = a_3 = \cdots = a_{m-3} = 0$, thus $p(x)$ is linear and the maximal arc obtained via Theorem* 1.1 *is of Denniston type.*

Proof. Since A has dimension $m-2$ over $\mathbb{F}_2$, we may assume that $A = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}(x) = 0 \text{ and } \mathrm{Tr}(\mu x) = 0\}$ for some $\mu \in \mathbb{F}_{2^m}^*$ with $\mu \neq 1$. Again we consider two cases.

Case 1: $\mathrm{Tr}(a_0) = 1$. Then

$$(1+\mathrm{Tr}(x))(1+\mathrm{Tr}(\mu x))\,\mathrm{Tr}\left(\sum_{i=1}^{m-3} a_i x^{2^i-1}\right) \equiv 0 \pmod{x^{2^m}-x}$$

$$(1+\mathrm{Tr}(x)+\mathrm{Tr}(\mu x)+\mathrm{Tr}(x)\,\mathrm{Tr}(\mu x))\cdot\mathrm{Tr}\left(\sum_{i=1}^{m-3} a_i x^{2^i-1}\right) \equiv 0 \pmod{x^{2^m}-x} \tag{3.5}$$

Let $r(x)$ denote the LHS of (3.5), $s(x) = 1+\mathrm{Tr}(x)+\mathrm{Tr}(\mu x)+\mathrm{Tr}(x)\,\mathrm{Tr}(\mu x)$, and $t(x) = \mathrm{Tr}(\sum_{i=1}^{m-3} a_i x^{2^i-1})$. The exponent of each term in $r(x)$ is a sum of the exponent of a summand in $s(x)$ and the exponent of some summand in $t(x)$. Similar to the proof of Theorem 3.4, exponents of the summands in $t(x)$ are 2^i-1, $1 \leqslant i \leqslant m-3$, and their cyclic shifts. Exponents from $s(x)$ are 0; 2^i; and 2^i+2^j, $i \neq j$. The terms x^0, x^{2^i}, and $x^{2^i+2^j}$ $(i \neq j)$ in $s(x)$ have coefficients 1, $1+\mu^{2^i}+\mu^{2^{i-1}}$, and $\mu^{2^i}+\mu^{2^j}$, respectively.

Claim: The coefficient of $x^{(2^m-1)-2^{m-2}-2^{m-4}}$ in $r(x)$ is

$$a_{m-3}^{2^{m-1}}(1+\mu^{2^{m-3}}+\mu^{2^{m-4}}) + a_{m-4}(\mu^{2^{m-1}}+\mu^{2^{m-3}})$$
$$+ a_{m-4}^{2^{m-1}}(\mu^{2^{m-3}}+\mu^{2^{m-5}}) + a_{m-3}(\mu^{2^{m-1}}+\mu^{2^{m-4}}).$$

The binary representation of the exponent of any term in $r(x)$ cannot have more than $2+(m-3) = m-1$ ones. The binary expansion of $(2^m-1)-2^{m-2}-2^{m-4}$ is $101011\ldots1$. This involves $m-2$ ones, so it can be obtained as a sum of two exponents (one from $s(x)$, the other from $t(x)$) without carry or with *exactly* one carry. Assume that we are in the former case. There are only three ways to obtain $(2^m-1)-2^{m-2}-2^{m-4}$, namely,

$$\begin{aligned} 101011\ldots1 &= 001000\ldots0 + 100011\ldots1 \\ &= 101000\ldots0 + 000011\ldots1 \\ &= 001010\ldots0 + 100001\ldots1. \end{aligned}$$

These contribute the coefficient $(1+\mu^{2^{m-3}}+\mu^{2^{m-4}})a_{m-3}^{2^{m-1}} + (\mu^{2^{m-1}}+\mu^{2^{m-3}})a_{m-4} + (\mu^{2^{m-3}}+\mu^{2^{m-5}})a_{m-4}^{2^{m-1}}$ for $x^{(2^m-1)-2^{m-2}-2^{m-4}}$ in $r(x)$. (Here we used the assumption that $m \geqslant 7$. If $m = 5$, the coefficient of the term $x^{2^4+2^2+1}$ in $r(x)$ is not the same as in our claim. The reason is that, for example, $10101 = 00100 + 10001$ leads to another possibility, namely 00100 comes from $a_1^4 x^4$ in $t(x)$, and 10001 comes from $(\mu^{2^0}+\mu^{2^4})x^{2^0+2^4}$ in $s(x)$. This cannot happen if $m \geqslant 7$.)

Now assume that a carry had been induced. The last carry-over must have occurred either at bit-$(m-3)$ or bit-$(m-1)$. The latter case cannot occur.

$$10101\ldots 1 = 10010\ldots 0 + 0001\ldots 1.$$

This contributes the coefficient $(\mu^{2^{m-1}} + \mu^{2^{m-4}})a_{m-3}$. This proves the claim. By (3.5), we have

$$\begin{aligned} &a_{m-3}^{2^{m-1}}(1+\mu^{2^{m-3}}+\mu^{2^{m-4}}) + a_{m-4}(\mu^{2^{m-1}}+\mu^{2^{m-3}}) \\ &\quad + a_{m-4}^{2^{m-1}}(\mu^{2^{m-3}}+\mu^{2^{m-5}}) + a_{m-3}(\mu^{2^{m-1}}+\mu^{2^{m-4}}) = 0 \end{aligned} \tag{3.6}$$

Claim: The coefficient of $x^{(2^m-1)-2^{m-1}-2^{m-4}}$ is

$$a_{m-4}(\mu^{2^{m-2}}+\mu^{2^{m-3}}) + a_{m-3}(\mu^{2^{m-2}}+\mu^{2^{m-4}}).$$

The binary expansion of $(2^m-1)-2^{m-1}-2^{m-4}$ is $011011\ldots 1$. Suppose it is obtained as a sum of exponents from $s(x)$ and $t(x)$ without carry. Then

$$01101\ldots 1 = 0110\ldots 0 + 00001\ldots 1$$

which contributes $(\mu^{2^{m-2}}+\mu^{2^{m-3}})a_{m-4}$. (Here again we have used the assumption that $m \geqslant 7$. If $m=6$, the coefficient of the term $x^{2^4+2^3+2+1}$ in $r(x)$ is not the same as in our claim. The reason is that $011011 = 011000 + 000011$ leads to another possibility, namely 011000 comes from $a_2^8 x^{2^4+2^3}$ in $t(x)$, and 000011 comes from $(\mu^{2^0}+\mu^2)x^{2^0+2}$ in $s(x)$. This cannot happen if $m \geqslant 7$.)

If $(2^m-1)-2^{m-1}-2^{m-4}$ is obtained as a sum of exponents from $s(x)$ and $t(x)$ with a carry, the last carry-over must occur at bit-$(m-2)$ or bit-0.

$$01101\ldots 1 = 01010\ldots 00 + 00011\ldots 11.$$

This contributes the coefficient $(\mu^{2^{m-2}}+\mu^{2^{m-4}})a_{m-3}$. Therefore the claim is proved, and by (3.5), we have

$$a_{m-4}(\mu^{2^{m-2}}+\mu^{2^{m-3}}) = a_{m-3}(\mu^{2^{m-2}}+\mu^{2^{m-4}}). \tag{3.7}$$

Claim: $a_{m-3}^{2^{m-1}}(1+\mu^{2^{m-3}}+\mu^{2^{m-4}}) + a_{m-4}^{2^{m-1}}(\mu^{2^{m-3}}+\mu^{2^{m-5}}) = 0$.

The claim is equivalent to

$$a_{m-3}(1+\mu^{2^{m-2}}+\mu^{2^{m-3}}) + a_{m-4}(\mu^{2^{m-2}}+\mu^{2^{m-4}}) = 0.$$

Consider the expression

$$\begin{aligned} E &= (a_{m-3}(1+\mu^{2^{m-2}}+\mu^{2^{m-3}}) + a_{m-4}(\mu^{2^{m-2}}+\mu^{2^{m-4}}))(\mu^{2^{m-2}}+\mu^{2^{m-3}}) \\ &= a_{m-3}(\mu^{2^{m-2}}+\mu^{2^{m-3}}) + a_{m-3}(\mu^{2^{m-2}}+\mu^{2^{m-3}})^2 \\ &\quad + a_{m-4}(\mu^{2^{m-2}}+\mu^{2^{m-4}})(\mu^{2^{m-2}}+\mu^{2^{m-3}}). \end{aligned}$$

Using (3.7), we have

$$\begin{aligned} E &= a_{m-3}(\mu^{2^{m-2}} + \mu^{2^{m-3}}) + a_{m-3}(\mu^{2^{m-1}} + \mu^{2^{m-2}}) + a_{m-3}(\mu^{2^{m-2}} + \mu^{2^{m-4}})^2 \\ &= 0. \end{aligned}$$

Since $\mu \neq 0, 1$ we have $(\mu^{2^{m-2}} + \mu^{2^{m-3}}) \neq 0$ and our claim follows. In particular, by (3.6) it implies $a_{m-4}(\mu^{2^{m-1}} + \mu^{2^{m-3}}) = a_{m-3}(\mu^{2^{m-1}} + \mu^{2^{m-4}})$. Adding this to (3.7) we get

$$a_{m-4}(\mu^{2^{m-1}} + \mu^{2^{m-2}}) = a_{m-3}(\mu^{2^{m-1}} + \mu^{2^{m-2}}).$$

Hence $a_{m-4} = a_{m-3}$. Substituting a_{m-4} in (3.7) by a_{m-3}, we have $a_{m-3} = 0$.

Claim: Let $m - 4 > k > 2$. If $a_j = 0$ for all $m - 3 > j > k$ then $a_k = 0$.

We will use a similar argument to that in (3.7). To this end we consider the coefficient of $x^{(2^k-1)+2^{m-2}+2^{m-3}}$ in $r(x)$. The binary expansion of its exponent is $0110\ldots01\ldots1$. This includes $2+k$ ones. All a_j with $j > k$ are zero. The sum of an exponent from $1 + \mathrm{Tr}(x) + \mathrm{Tr}(\mu x) + \mathrm{Tr}(x)\,\mathrm{Tr}(\mu x)$ and an exponent from $\mathrm{Tr}(\sum_{i=0}^{k} a_i x^{2^i-1})$ has at most $2+k$ ones. Since $k > 2$ there is only one way to obtain $(2^k - 1) + 2^{m-2} + 2^{m-3}$, namely,

$$0110\ldots0\underbrace{1\ldots1}_{k>2} = 0110\ldots0 + 0\ldots0\underbrace{1\ldots1}_{k>2}.$$

It follows that $(\mu^{2^{m-2}} + \mu^{2^{m-3}})a_k = 0$. Hence $a_k = 0$.

Since $a_{m-3} = a_{m-4} = 0$ we find that $a_3 = \cdots = a_{m-4} = a_{m-3} = 0$ by induction.

Claim: $a_2 = 0$.

Consider the coefficients of x^{2^4+7} and x^{2^5+7}. Since for all $j > 2$ we have $a_j = 0$ there are only two ways to obtain each exponent.

$$\begin{aligned} 0\ldots0010111 &= 0\ldots0010100 + 0\ldots0000011 \\ &= 0\ldots0010001 + 0\ldots0000110 \\ 0\ldots0100111 &= 0\ldots0100100 + 0\ldots0000011 \\ &= 0\ldots0100001 + 0\ldots0000110. \end{aligned}$$

Hence the coefficient of x^{2^4+7} is $(\mu^4 + \mu^{16})a_2 + (\mu + \mu^{16})a_2^2$ and the coefficient of x^{2^5+7} is $(\mu^4 + \mu^{32})a_2 + (\mu + \mu^{32})a_2^2$. Adding both values we find

$$a_2(\mu^{16} + \mu^{32}) + a_2^2(\mu^{16} + \mu^{32}) = 0.$$

Thus, a_2 is either 0 or 1. Now look at the coefficient of x^{15}. There are only three ways of obtaining 15 as a sum with the exponents we can use.

$$\begin{aligned} 0\ldots01111 &= 0\ldots01100 + 0\ldots00011 \\ &= 0\ldots01001 + 0\ldots00110 \\ &= 0\ldots00011 + 0\ldots01100. \end{aligned}$$

Hence $(\mu^4+\mu^8)a_2 + (\mu+\mu^8)a_2^2 + (\mu+\mu^2)a_2^4 = 0$. If $a_2 = 1$ then $\mu^2+\mu^4 = 0$ which is a contradiction. Thus, $a_2 = 0$.

It follows that $a_2 = \cdots = a_{m-3} = 0$.

Case 2: $\mathrm{Tr}(a_0) = 0$. Then $\mathrm{Tr}(\sum_{i=1}^{m-3} a_i\lambda^{2^i-1}) = 1$ for all $\lambda \in A\backslash\{0\}$. Hence if we view

$$(1+\mathrm{Tr}(x)+\mathrm{Tr}(\mu x)+\mathrm{Tr}(x)\,\mathrm{Tr}(\mu x))\cdot\left(1+\mathrm{Tr}\left(\sum_{i=1}^{m-3} a_i x^{2^i-1}\right)\right)$$

as a function from $\mathbb{F}_{2^m}$ to itself, it is the characteristic function of the subset $\{0\}$ of $\mathbb{F}_{2^m}$. Therefore,

$$\begin{aligned} &(1+\mathrm{Tr}(x)+\mathrm{Tr}(\mu x)+\mathrm{Tr}(x)\,\mathrm{Tr}(\mu x)) + (1+\mathrm{Tr}(x)+\mathrm{Tr}(\mu x)+\mathrm{Tr}(x)\,\mathrm{Tr}(\mu x)) \\ &\quad \cdot \mathrm{Tr}\left(\sum_{i=1}^{m-3} a_i x^{2^i-1}\right) \equiv 1 - x^{2^m-1} \pmod{x^{2^m}-x}. \end{aligned} \tag{3.8}$$

Note that the binary representation of the exponent of x^{2^m-1} is $111\ldots1$ (m ones altogether), while in the left hand side of (3.8), the binary representation of the exponent of any term in the product

$$(1+\mathrm{Tr}(x)+\mathrm{Tr}(\mu x)+\mathrm{Tr}(x)\,\mathrm{Tr}(\mu x))\cdot\mathrm{Tr}\left(\sum_{i=1}^{m-3} a_i x^{2^i-1}\right)$$

cannot have more than $2+(m-3) = m-1$ ones. So (3.8) cannot hold. Thus, this case does not occur. This completes our proof. □

Combining Theorem 3.4 and Theorem 3.5 with the constructive result in Section 2 and Theorem 3.2 in [9], we find that when $m \geqslant 7$, the largest d of a non-Denniston maximal arc of degree 2^d in $\mathrm{PG}(2,2^m)$ generated by a $\{p,1\}$-map via Theorem 1.1 satisfies

$$\left\lfloor \frac{m+2}{2} \right\rfloor \leqslant d \leqslant m-3.$$

We have the following conjecture.

Conjecture 3.6. *When $m > 9$, the largest d of a non-Denniston maximal arc of degree 2^d in* $\mathrm{PG}(2,2^m)$ *generated by a $\{p,1\}$-map via Theorem* 1.1 *is* $\lfloor \frac{m+2}{2} \rfloor$.

In order to prove the above conjecture, it suffices to prove the following. Let A be an additive subgroup in $\mathbb{F}_{2^m}$ of size 2^d, where $m > 9$, $p(x) = a_0 + a_1x + \cdots + a_{d-1}x^{2^{d-1}-1} \in \mathbb{F}_{2^m}[x]$. If $d \geqslant \lfloor \frac{m+2}{2} \rfloor + 1$, $\mathrm{Tr}(p(\lambda)) = 1$ for every $\lambda \in A\backslash\{0\}$, then $a_2 = a_3 = \cdots = a_{d-1} = 0$. So far we can only prove some partial results in this direction.

Theorem 3.7. *Let A be an additive subgroup in $\mathbb{F}_{2^m}$ of size 2^d, where $d \leqslant m-1$, and let $p(x) = a_0 + a_1x + \cdots + a_{d-2}x^{2^{d-2}-1} \in \mathbb{F}_{2^m}[x]$, with $a_{d-2} \neq 0$. If $\mathrm{Tr}(p(\lambda)) = 1$ for every $\lambda \in A\backslash\{0\}$, then $d \leqslant \frac{m+2}{2}$.*

Proof. Assume to the contrary that $d > \frac{m+2}{2}$; we will show that $a_{d-2} = 0$. Assume that the defining equation for A is

$$(1 + \mathrm{Tr}(\mu_1x))(1 + \mathrm{Tr}(\mu_2x)) \ldots (1 + \mathrm{Tr}(\mu_{m-d}x)) = 1,$$

where $\mu_i \in \mathbb{F}_{2^m}$, $i = 1, 2, \ldots, m-d$, are linearly independent over $\mathbb{F}_2$. We consider two cases:

Case 1: $\mathrm{Tr}(a_0) = 1$. Then

$$\begin{aligned}(1 + \mathrm{Tr}(\mu_1x))(1 + \mathrm{Tr}(\mu_2x)) \ldots (1 + \mathrm{Tr}(\mu_{m-d}x))\\ \cdot \mathrm{Tr}\left(\sum_{i=1}^{d-2} a_ix^{2^i-1}\right) \equiv 0 \pmod{x^{2^m} - x}.\end{aligned} \tag{3.9}$$

Claim: The coefficient of $x^{1+2+2^2+\cdots+2^{d-3}+2^{d-1}+2^d+\cdots+2^{m-2}}$ is

$$\left(\sum_{\sigma \in S_{m-d}} \mu_{\sigma(1)}^{2^{m-2}} \mu_{\sigma(2)}^{2^{m-3}} \ldots \mu_{\sigma(m-d)}^{2^{d-1}}\right) a_{d-2},$$

where S_{m-d} is the symmetric group on $m-d$ letters.

The exponent of $x^{1+2+2^2+\cdots+2^{d-3}+2^{d-1}+2^d+\cdots+2^{m-2}}$ has m-bit binary representation

$$0\underbrace{11\ldots1}_{m-d}0\underbrace{11\ldots1}_{d-2}.$$

Since $d > \frac{m+2}{2}$, we see that $d-2 > m-d$, there is only one way to get the term $x^{1+2+2^2+\cdots+2^{d-3}+2^{d-1}+2^d+\cdots+2^{m-2}}$ when multiplying $(1 + \mathrm{Tr}(\mu_1x))(1 + \mathrm{Tr}(\mu_2x)) \ldots (1 + \mathrm{Tr}(\mu_{m-d}x))$ with $\mathrm{Tr}(\sum_{i=1}^{d-2} a_ix^{2^i-1})$, namely

$$0\underbrace{11\ldots1}_{m-d}0\underbrace{11\ldots1}_{d-2} = 0\underbrace{00\ldots0}_{m-d}0\underbrace{11\ldots1}_{d-2} + 0\underbrace{11\ldots1}_{m-d}0\underbrace{00\ldots0}_{d-2}.$$

Therefore the claim follows. By (3.9), we see that

$$\left(\sum_{\sigma\in S_{m-d}} \mu_{\sigma(1)}^{2^{m-2}} \mu_{\sigma(2)}^{2^{m-3}} \cdots \mu_{\sigma(m-d)}^{2^{d-1}}\right) a_{d-2} = 0. \tag{3.10}$$

Now set $r = m - d$. Then

$$\sum_{\sigma\in S_{m-d}} \mu_{\sigma(1)}^{2^{m-2}} \mu_{\sigma(2)}^{2^{m-3}} \cdots \mu_{\sigma(m-d)}^{2^{d-1}} = \left(\sum_{\sigma\in S_r} \mu_{\sigma(1)}^{2^{r-1}} \mu_{\sigma(2)}^{2^{r-2}} \cdots \mu_{\sigma(r)}\right)^{2^{d-1}}.$$

Note that

$$\sum_{\sigma\in S_r} \mu_{\sigma(1)}^{2^{r-1}} \mu_{\sigma(2)}^{2^{r-2}} \cdots \mu_{\sigma(r)} = \det\begin{pmatrix} \mu_1 & \mu_2 & \cdots & \mu_r \\ \mu_1^2 & \mu_2^2 & \cdots & \mu_r^2 \\ & & \cdots & \\ \mu_1^{2^{r-1}} & \mu_2^{2^{r-1}} & \cdots & \mu_r^{2^{r-1}} \end{pmatrix}.$$

We will use $\Delta(\mu_1, \mu_2, \ldots, \mu_r)$ to denote this last determinant. Since μ_i, $i = 1, 2, \ldots, r$, are linearly independent over $\mathbb{F}_2$, we see that $\Delta(\mu_1, \mu_2, \ldots, \mu_r) \neq 0$ (cf. [7, p. 109]). By (3.10), this shows that $a_{d-2} = 0$.

Case 2: $\mathrm{Tr}(a_0) = 0$. As before, this case can be easily seen not to occur.

This completes the proof. □

In order to extend the result in Theorem 3.7, we need to introduce more notation. Let $\mu_1, \mu_2, \ldots, \mu_r$ be elements in $\mathbb{F}_{2^m}$ that are linearly independent over $\mathbb{F}_2$. Let $0 = \alpha_1 < \alpha_2 < \cdots < \alpha_r \leqslant m - 1$ be integers. We define

$$T(\alpha_1, \alpha_2, \ldots, \alpha_r) = \sum_{\sigma\in S_r} \mu_{\sigma(1)}^{2^{\alpha_1}} \mu_{\sigma(2)}^{2^{\alpha_2}} \cdots \mu_{\sigma(r)}^{2^{\alpha_r}}.$$

Using the above notation, we have the following lemma.

Lemma 3.8. *Let $m > 9$ be an odd integer, let $r = \frac{m-3}{2}$, and let t be an integer such that $3 \leqslant t \leqslant \frac{m-1}{2}$. Then there exist $0 = \alpha_1 < \alpha_2 < \cdots < \alpha_r \leqslant m - 1$ such that*

(i) $\alpha_r \leqslant m - t - 3$,

(ii) $T(\alpha_1, \alpha_2, \ldots, \alpha_r) \neq 0$, *and*

(iii) *the number of consecutive integers in the set $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is less than or equal to $t - 1$.*

We postpone the proof of this lemma to the appendix. With this lemma, we can prove the following theorem.

Theorem 3.9. *Let $m > 9$ be an odd integer, let A be an additive subgroup in $\mathbb{F}_{2^m}$ of size 2^d, where $d \leqslant m-1$, and let $p(x) = a_0 + a_1 x + a_2 x^3 + \cdots + a_t x^{2^t - 1} \in \mathbb{F}_{2^m}[x]$, with $a_t \neq 0$ and $t \leqslant (d-1)$. If $3 \leqslant t \leqslant \frac{m-1}{2}$, and $\mathrm{Tr}(p(\lambda)) = 1$ for every $\lambda \in A \setminus \{0\}$, then $d \leqslant \frac{m+1}{2}$.*

Proof. Assume to the contrary that $d > \frac{m+1}{2}$; we will show that $a_t = 0$. Without loss of generality, assume that $d = \frac{m+3}{2}$, and let $r = m - d = \frac{m-3}{2}$. Assume that the defining equation for A is

$$(1 + \mathrm{Tr}(\mu_1 x))(1 + \mathrm{Tr}(\mu_2 x)) \ldots (1 + \mathrm{Tr}(\mu_r x)) = 1,$$

where $\mu_i \in \mathbb{F}_{2^m}$, $i = 1, 2, \ldots, r$, are linearly independent over $\mathbb{F}_2$. As in the proof of Theorem 3.7, we only need to consider the case where $\mathrm{Tr}(a_0) = 1$. Hence we have

$$(1 + \mathrm{Tr}(\mu_1 x))(1 + \mathrm{Tr}(\mu_2 x)) \ldots (1 + \mathrm{Tr}(\mu_r x)) \,\mathrm{Tr}\left(\sum_{i=1}^{t} a_i x^{2^i - 1} \right) \equiv 0 \pmod{x^{2^m} - x}. \tag{3.11}$$

By Lemma 3.8, there exist $0 = \alpha_1 < \alpha_2 < \cdots < \alpha_r \leqslant m-1$ such that

(i) $\alpha_r \leqslant m - t - 3$,

(ii) $T(\alpha_1, \alpha_2, \ldots, \alpha_r) \neq 0$, and

(iii) the number of consecutive integers in the set $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is less than or equal to $t-1$.

We will look at the coefficient of $x^{1+2^{\alpha_2}+\cdots+2^{\alpha_r}+2^{m-2}+2^{m-3}+\cdots+2^{m-t-1}}$ in the left hand side of (3.11). Note that the exponent of this monomial has the m-bit binary representation

$$0\underbrace{11\ldots1}_{t}0\underbrace{0\ldots1\ldots1\ldots1}_{m-t-2},$$

where at the α_ith bit there is a 1, for each $i = 1, 2, \ldots, r$.

Since the number of consecutive integers in the set $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is less than or equal to $t-1$, there is only one way to get the term

$$x^{1+2^{\alpha_2}+\cdots+2^{\alpha_r}+2^{m-2}+2^{m-3}+\cdots+2^{m-t-1}}$$

when multiplying

$$(1 + \mathrm{Tr}(\mu_1 x))(1 + \mathrm{Tr}(\mu_2 x)) \ldots (1 + \mathrm{Tr}(\mu_r x)) \quad \text{with} \quad \mathrm{Tr}(\textstyle\sum_{i=1}^{t} a_i x^{2^i-1}),$$

namely

$$0\underbrace{11\ldots1}_{t}0\underbrace{0\ldots1\ldots1\ldots1}_{m-t-2} = 0\underbrace{00\ldots0}_{t}0\underbrace{0\ldots1\ldots1\ldots1}_{m-t-2} + 0\underbrace{11\ldots1}_{t}0\underbrace{00\ldots0}_{m-t-2}.$$

Therefore, the coefficient of $x^{1+2^{\alpha_2}+\cdots+2^{\alpha_r}+2^{m-2}+2^{m-3}+\cdots+2^{m-t-1}}$ in the left hand side of (3.11) is

$$\left(\sum_{\sigma \in S_r} \mu_{\sigma(1)}^{2^{\alpha_1}} \mu_{\sigma(2)}^{2^{\alpha_2}} \cdots \mu_{\sigma(r)}^{2^{\alpha_r}}\right) a_t^{2^{m-t-1}} = T(\alpha_1, \ldots, \alpha_r) a_t^{2^{m-t-1}}.$$

By (3.11), we see that $T(\alpha_1, \ldots, \alpha_r) a_t^{2^{m-t-1}} = 0$. Since $T(\alpha_1, \ldots, \alpha_r) \neq 0$, we have $a_t = 0$. This completes the proof. □

4 Appendix

In this appendix, we give a proof of Lemma 3.8. First, we introduce some notation. Let $x_1, \ldots, x_r$ be elements in $\mathbb{F}_{2^m}$ that are linearly independent over $\mathbb{F}_2$. For any integer i, we set $\boldsymbol{v}_i = (x_1^{2^i}, \ldots, x_r^{2^i})$. We use $\boldsymbol{v}_i^{2^j}$ to denote component-wise exponentiation of $\boldsymbol{v}_i$ by 2^j. Hence $\boldsymbol{v}_i^{2^j} = \boldsymbol{v}_{i+j}$. Since $x_\ell^{2^m} = x_\ell$ for all $\ell = 1, 2, \ldots, r$, we have $\boldsymbol{v}_m = \boldsymbol{v}_0$. So in what follows, the indices of $\boldsymbol{v}_i$ are to be read modulo m. Now condition (ii) of Lemma 3.8 is equivalent to the vectors

$$\boldsymbol{v}_{\alpha_1}, \ldots, \boldsymbol{v}_{\alpha_r}$$

being linearly independent over $\mathbb{F}_{2^m}$, i.e.,

$$\det \begin{pmatrix} x_1^{2^{\alpha_1}} & \cdots & x_r^{2^{\alpha_1}} \\ \vdots & \ddots & \vdots \\ x_1^{2^{\alpha_r}} & \cdots & x_r^{2^{\alpha_r}} \end{pmatrix} \neq 0.$$

Let V be the $\mathbb{F}_{2^m}$-span of $\boldsymbol{v}_0, \ldots, \boldsymbol{v}_{m-1}$. By [7, Lemma 3.51], $\dim_{\mathbb{F}_{2^m}} V = r$ and $\{\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_{i+r-1}\}$ is an $\mathbb{F}_{2^m}$-basis of V for any $0 \leqslant i \leqslant m - r$.

In the following, we will be considering subspaces of V spanned by some vectors in $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m-1}\}$. To this end, we will use binary vectors to represent subsets of $\{\boldsymbol{v}_0, \ldots, \boldsymbol{v}_{m-1}\}$. Let $\boldsymbol{u} = (u_0, u_1, \ldots, u_{i-1})$ be a vector with entries in $\{0, 1\}$. Then the subset of $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m-1}\}$ represented by $\boldsymbol{u}$ is

$$S(\boldsymbol{u}) = \{\boldsymbol{v}_\ell \mid u_\ell \neq 0, 0 \leqslant \ell \leqslant i - 1\}.$$

By $V(\boldsymbol{u})$ we will denote the $\mathbb{F}_{2^m}$-span of the vectors in $S(\boldsymbol{u})$. For example, if $\boldsymbol{u} = (1, 1, 0, 1)$ then $V(\boldsymbol{u}) = \mathbb{F}_{2^m}\boldsymbol{v}_0 + \mathbb{F}_{2^m}\boldsymbol{v}_1 + \mathbb{F}_{2^m}\boldsymbol{v}_3$. For convenience, we also allow concatenation of binary vectors. If $\boldsymbol{u} = (u_0, u_1, \ldots, u_{i-1})$ and $\boldsymbol{u}' = (u'_0, \ldots, u'_{j-1})$ then the concatenation of $\boldsymbol{u}$ with $\boldsymbol{u}'$ is

$$\boldsymbol{u} * \boldsymbol{u}' = (u_0, \ldots, u_{i-1}, u'_0, \ldots, u'_{j-1}).$$

Moreover $\underbrace{\boldsymbol{u} * \boldsymbol{u} * \cdots * \boldsymbol{u}}_{\ell}$ is abbreviated to $\boldsymbol{u}^{*\ell}$.

Now we can reformulate Lemma 3.8 as follows: For every integer t such that $3 \leqslant t \leqslant \frac{m-1}{2}$, there exists a binary vector $\boldsymbol{u}$ of length at most $m - (t + 2)$ such that $V(\boldsymbol{u}) = V$ and the number of consecutive 1's in $\boldsymbol{u}$ is at most $t - 1$. It is this reformulation that we will prove in this appendix.

One final preparation before we give the proof. Given integers i and $j > 0$, let $I(i, j)$ denote the $\mathbb{F}_{2^m}$-span of $\boldsymbol{v}_i, \boldsymbol{v}_{i+1}, \ldots, \boldsymbol{v}_{i+j-1}$. Given a subspace W of V, we define $W^{2^t} = \{w^{2^t} \mid w \in W\}$, where w^{2^t} means component-wise exponentiation of w by 2^t. We will need the following lemma.

Lemma 4.1. *Suppose that* $W = V(\boldsymbol{u})$ *where* $\boldsymbol{u} = (u_0, u_1, \ldots, u_{s-1}) \in \mathbb{F}_2^s$. *If* $I(s, t) \subset W$ *and* $W^{2^t} \cap I(0, s) \subset W$ *then* $W = V$.

Proof. By assumption, W is spanned by a subset of $\{\boldsymbol{v}_0, \ldots, \boldsymbol{v}_{s-1}\}$. Let $\boldsymbol{v}_i \in W$, $0 \leqslant i \leqslant s-1$, be one of the generating vectors. If $i + t \leqslant s - 1$, then $\boldsymbol{v}_i^{2^t} = \boldsymbol{v}_{i+t} \in I(0, s) \cap W^{2^t} \subset W$. If $i + t > s - 1$, then $\boldsymbol{v}_i^{2^t} = \boldsymbol{v}_{i+t} \in I(s, t) \subset W$. Hence for any vector $\boldsymbol{v}_i \in W$, $0 \leqslant i \leqslant s-1$, we have $\boldsymbol{v}_{i+t} \in W$. Extending this property to linear combinations of the generating vectors of W, we see that $I(s + t, t) \subset W$ since $I(s, t) \subset W$. That is, $I(s + \ell t, t) \subset W$ for all $\ell \geqslant 0$. Hence $\boldsymbol{v}_i \in W$ for all $0 \leqslant i \leqslant m - 1$ and $W = V$. $\square$

Proof of Lemma 3.8. Write $r = kt + a$ where $0 \leqslant a \leqslant t - 1$. Since $r = \frac{m-3}{2}$, we have $m = 2kt + 2a + 3$. Set $\boldsymbol{a} = (1, 1, \ldots, 1) \in \mathbb{F}_2^a$ and $\boldsymbol{u} = (0, 1, \ldots, 1) \in \mathbb{F}_2^t$. Let

$$V(i) = V(\boldsymbol{a} * \boldsymbol{u}^{*i}).$$

That is, $V(i)$ is the space spanned by the vectors in $S(\boldsymbol{a} * \boldsymbol{u}^{*i})$. Then $V(k)$ is the $\mathbb{F}_{2^m}$-span of $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{r-1}\} \backslash \{\boldsymbol{v}_a, \boldsymbol{v}_{a+t}, \ldots, \boldsymbol{v}_{a+(k-1)t}\}$. Since $\{\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{r-1}\}$ is a basis for V, we see that $\dim V(k) = r - k$. Let b be the smallest nonnegative integer such that $V(k + b) = V(k + b + 1)$. In particular, $V(k + i)$ is a proper subspace of $V(k + i + 1)$ if $0 \leqslant i < b$. We observe that $0 \leqslant b \leqslant k$. There are three cases to consider.

Case 1: $\dim V(k + 1) \geqslant r - k + 2$. In this case $b \leqslant k - 1$. If $V(k + b) = V$, then $S(\boldsymbol{a} * \boldsymbol{u}^{*(k+b)})$ spans V. Note that $\boldsymbol{a} * \boldsymbol{u}^{*(k+b)}$ has length $a + (k + b)t \leqslant a + (2k - 1)t = m - a - (t + 3)$. By construction this vector does not have more than $t - 1$ consecutive 1's. So we are done in this case.

If $V(k + b) \neq V$ then $b \leqslant k - 2$. Let $\boldsymbol{0} = (0, 0, \ldots, 0) \in \mathbb{F}_2^t$ and $\boldsymbol{a}' = (1, 0, \ldots, 0) \in \mathbb{F}_2^t$. Let

$$\boldsymbol{w}_i = \boldsymbol{a} * \boldsymbol{u}^{*(k+b)} * \boldsymbol{0} * \boldsymbol{a}'^{*i}.$$

We define $W(i) = V(\boldsymbol{w}_i)$ to be the $\mathbb{F}_{2^m}$-span of the vectors in $S(\boldsymbol{w}_i)$. In particular, $W(0) = V(k + b)$. Let b' be the smallest nonnegative integer such that $W(b') = W(b' + 1)$.

$$\begin{aligned} \dim W(0) &= \dim V(k + b) \\ &\geqslant \dim V(k + 1) + (b - 1) \\ &\geqslant r - k + 2 + b - 1 \\ &= r - (k - b - 1). \end{aligned}$$

Hence $0 \leqslant b' \leqslant k - 1 - b$. We claim that

(i) $W(b') \supset I(a + (b + k + i + 1)t, t)$

(ii) $W(b') \supset W(b')^{2^t} \cap I(0, a + (b + k + i + 1)t)$

for all $i \geqslant 0$. By Lemma 4.1, these two claims imply that $W(b') = V$. The length of $\boldsymbol{w}_{b'}$ is

$$a + (k + b + 1 + b')t \leqslant a + 2kt = m - a - 3.$$

Note that the last $t - 1$ entries in $\boldsymbol{w}_{b'}$ are zero. Dropping these $t - 1$ positions we obtain a vector of length $m - a - (t + 2)$. This vector does not have more than $t - 1$ consecutive 1's and it corresponds to a subset of $\{\boldsymbol{v}_{\alpha_1}, \ldots, \boldsymbol{v}_{\alpha_r}\}$ that spans V, hence Lemma 3.8 is proved in this case once we prove the above two claims.

To prove the first claim, we recall that $W(b') = V(\boldsymbol{a} * \boldsymbol{u}^{*(k+b)} * \boldsymbol{0} * \boldsymbol{a}'^{*b'})$. Hence $\boldsymbol{v}_{a+(k+b+1+i)t} \in W(b')$ for all $i \geqslant 0$ since this vector corresponds to the first position in the i-th copy of $\boldsymbol{a}'$. Now $W(b') \supseteq V(k + b) = V(k + b + 1 + i)$ for all $i \geqslant 0$, we also have $S(\boldsymbol{a} * \boldsymbol{u}^{*(k+b+1+i)}) \subset W(b')$. Thus

$$\boldsymbol{v}_{a+(k+b+1+i)t+1}, \ldots, \boldsymbol{v}_{a+(k+b+1+i)t+(t-1)} \in W(b'),$$

since these vectors correspond to the nonzero positions in the last copy of $\boldsymbol{u}$ in $\boldsymbol{a} * \boldsymbol{u}^{*(k+b+2+i)}$. This proves our first claim.

For the second claim it suffices to show that $S(\boldsymbol{0} * \boldsymbol{a} * \boldsymbol{u}^{*(k+b)} * \boldsymbol{0} * \boldsymbol{a}'^{*i}) \subseteq W(b')$. Hence we need to show that the vectors corresponding to the $(k + b)$-th copy of $\boldsymbol{u}$ and the i-th copy of $\boldsymbol{a}'$, respectively, are in $W(b')$. The former is true since $W(b')$ includes $S(\boldsymbol{a} * \boldsymbol{u}^{*(k+b+1)})$ which spans $V(k + b + 1)$. The latter holds because $W(b') = W(b' + 1)$ which includes the vectors in $S(\boldsymbol{a} * \boldsymbol{u}^{*(k+b)} * \boldsymbol{0} * \boldsymbol{a}'^{*(b'+1)})$. This proves our second claim.

Case 2: $\dim V(k + 1) = r - k + 1 = \dim V(k) + 1$. In this case, one of the vectors $\boldsymbol{v}_{r+1}, \ldots, \boldsymbol{v}_{r+(t-1)}$ does not belong to $V(k)$. Suppose that vector is $\boldsymbol{v}_{r+j} = \boldsymbol{v}_{a+kt+j}$, $1 \leqslant j \leqslant t - 1$. Then $V(k + 1) = V(k) + \mathbb{F}_{2^m}\boldsymbol{v}_{r+j}$. Since any linear dependence relation translates to a linear dependence relation when both sides are raised to the 2^tth power, we get $\dim V(k + i) \leqslant \dim V(k) + i$, $i \geqslant 0$.

Subcase 1: $V(k + b) \neq V$, i.e., $b < k$. As seen above, all vectors $\boldsymbol{v}_{r+1}, \ldots, \boldsymbol{v}_{r+(t-1)}$ were linearly dependent on vectors in $V(k)$ and $\boldsymbol{v}_{r+j}$. Any such linear dependence translates to a linear dependence of $\boldsymbol{v}_{r+(b-1)t+i}$, $i \neq j$, on vectors in $V(k + b - 1)$ and $\boldsymbol{v}_{r+(b-1)t+j}$. Hence the vector $\boldsymbol{v}_{r+(b-1)t+j}$ must be a vector among $\boldsymbol{v}_{r+(b-1)t+1}, \ldots, \boldsymbol{v}_{r+(b-1)t+(t-1)}$ that is not in $V(k + b - 1)$. Therefore, we can replace those positions in the last copy of $\boldsymbol{u}$ in $\boldsymbol{a} * \boldsymbol{u}^{*(k+b-1)} * \boldsymbol{u}$ that do not correspond to $\boldsymbol{v}_{r+(b-1)t+j}$ by 0; we will denote the modified vector by $\boldsymbol{a} * \boldsymbol{u}^{*(k+b-1)} * \boldsymbol{u}^{(j)}$, where $\boldsymbol{u}^{(j)}$ contains only one 1. By our discussion above, we see that

$$V(k + b) = V(\boldsymbol{a} * \boldsymbol{u}^{*(k+b-1)} * \boldsymbol{u}^{(j)}),$$

and dim $V(k+b) = r - k + b = r - (k - b)$. Let $\boldsymbol{a}'$ be as defined in Case 1, and let $\boldsymbol{w}_i' = \boldsymbol{a} * \boldsymbol{u}^{*(k+b-1)} * \boldsymbol{u}^{(j)} * \boldsymbol{a}'^{*i}$. Define $W(i) = V(\boldsymbol{w}_i')$. Let b' be the smallest nonnegative integer such that $W(b') = W(b'+1)$. Then $0 \leqslant b' \leqslant k - b$. Similar to Case 1, we have

(i) $W(b') \supset I(a + (k+b+i)t, t)$

(ii) $W(b') \supset W(b')^{2^t} \cap I(0, a + (k+b+i)t)$.

Thus, by Lemma 4.1 we have $V(\boldsymbol{w}_{b'}') = W(b') = V$. The length of $\boldsymbol{w}_{b'}'$ is $a + (k+b)t + b't \leqslant a + 2kt$. Dropping the last $t-1$ zeros in $\boldsymbol{w}_{b'}'$, we get a vector of length $m - a - (t+2)$, which does not contain more than $t-1$ consecutive 1's. So Lemma 3.8 is proved in this subcase.

Subcase 2: $V(k+b) = V$, i.e., $b = k$. Since $V(k+b) = V(\boldsymbol{a} * \boldsymbol{u}^{*(k+b-1)} * \boldsymbol{u}^{(j)})$ (cf. Subcase 1), we have

$$V = V(\boldsymbol{a} * \boldsymbol{u}^{*(k+b-1)} * \boldsymbol{u}^{(j)}).$$

Note that the binary vector $\boldsymbol{a} * \boldsymbol{u}^{*(k+b-1)} * \boldsymbol{u}^{(j)}$ has length $a + (k+b-1)t + (j+1) = m - (t+2) - (a-j)$ and does not have more than $t-1$ consecutive 1's. If $a \geqslant j$ this vector will work. So we assume that $j > a$. Recall that $\boldsymbol{v}_{r+1}, \ldots, \boldsymbol{v}_{r+(j-1)} \in V(k)$ but $\boldsymbol{v}_{r+j} \notin V(k)$ by our choice of j. Let $(0, 1, \ldots, 1) \in \mathbb{F}_2^j$ and $\boldsymbol{w}' = \boldsymbol{a} * \boldsymbol{u}^{*k} * (0, 1, \ldots, 1)$. Then $V(\boldsymbol{w}') = V(k)$.

Let $\boldsymbol{z} = (\underbrace{1, 1, \ldots, 1}_{t-j}, 0, \underbrace{1, 1, \ldots, 1}_{j-1}) \in \mathbb{F}_2^t$, and let $V'(i)$ be the $\mathbb{F}_{2^m}$-span of $S(\boldsymbol{a} * \boldsymbol{z}^{*i})$, i.e., $V'(i) = V(\boldsymbol{a} * \boldsymbol{z}^{*i})$. Observe that when we shift the vector $\boldsymbol{a} * \boldsymbol{z}^{*k}$ to the right by j positions, we get

$$\underbrace{(0, \ldots, 0)}_{j} * \underbrace{(1, \ldots, 1)}_{t+(a-j)} * \boldsymbol{u}^{*(k-1)} * \underbrace{(0, 1, \ldots, 1)}_{j}.$$

The subset represented by this vector is

$$\{\boldsymbol{v}_j, \boldsymbol{v}_{j+1}, \ldots, \boldsymbol{v}_{r+j-1}\} \setminus \{\boldsymbol{v}_{a+t}, \boldsymbol{v}_{a+2t}, \ldots, \boldsymbol{v}_{a+kt}\}.$$

Hence $V'(k)^{2^j} \subseteq V(k) + \sum_{i=1}^{j-1} \mathbb{F}_{2^m} v_{r+i} = V(k)$. In fact, $V'(k)^{2^j} = V(k)$ since the two subspaces have the same dimension $r - k$. Similarly, $V'(k+1)^{2^j} = V(k+1)$. Moreover, since $\boldsymbol{v}_r^{2^j} = \boldsymbol{v}_{r+j} \notin V(k)$ we have $\boldsymbol{v}_r \notin V'(k)$. Hence $V'(k+1) = V'(k) + \mathbb{F}_{2^m} \boldsymbol{v}_r$. It follows that $V'(k+i) = V'(k+i-1) + \mathbb{F}_{2^m} \boldsymbol{v}_{r+it}$ for $1 \leqslant i \leqslant k$. In particular, $V'(2k) = V$. Since $V'(2k) = V'(2k-1) + \mathbb{F}_{2^m} \boldsymbol{v}_{r+(k-1)t}$, we see that actually

$$V'(2k) = V(\boldsymbol{a} * \boldsymbol{z}^{*(2k-1)} * (\underbrace{1, 0, \ldots, 0}_{t})).$$

The length of the vector $\boldsymbol{a} * \boldsymbol{z}^{*(2k-1)} * (\underbrace{1, 0, \ldots, 0}_{t})$ is $a + (2k-1)t + 1 = m - (t+2) - a$. So we are also done in this subcase.

Case 3: $V(k) = V(k+1)$, i.e., $\dim V(k+1) = r-k$. In this case V is spanned by $S(\boldsymbol{a} * \boldsymbol{u}^{*k} * \boldsymbol{a}'^{*k})$. Thus, we have

$$\boldsymbol{v}_{r+1} = \sum_{i=0}^{r-1} c_i \boldsymbol{v}_i,$$

where $c_{a+nt} = 0$ for all $0 \leqslant n \leqslant k$. Let ℓ be the largest index such that $c_\ell \neq 0$. We consider three subcases.

Subcase 1: $\ell = a + jt + s$ with $2 \leqslant s \leqslant t-1$ and $0 \leqslant j \leqslant k-1$. Now

$$(\boldsymbol{v}_{r+1})^{2^{(k-j-1)t}} = \boldsymbol{v}_{r+1+(k-j-1)t} = \sum_{i=0}^{r-1} c_i^{2^{(k-j-1)t}} \boldsymbol{v}_{i+(k-j-1)t}.$$

Note that $r - t + 2 \leqslant \ell + (k-j-1)t \leqslant r-1$. Hence $\boldsymbol{v}_{i+(k-j-1)t} \in S(\boldsymbol{a} * \boldsymbol{u}^{*k}) = V(k)$ for all $\boldsymbol{v}_i$ with $c_i \neq 0$. Therefore we can express $\boldsymbol{v}_{\ell+(k-j-1)t} = \boldsymbol{v}_{a+(k-1)t+s}$ as a linear combination of $\boldsymbol{v}_{r+1+(k-j-1)t}$ and some vector in $V(k)$. It follows that V is spanned by $S(\boldsymbol{a} * \boldsymbol{u}^{*(k-1)} * \boldsymbol{u}^{(\ell)} * \boldsymbol{a}'^{*(k-j-1)} * (1,1,0,\ldots,0) * \boldsymbol{a}'^{*j})$ where $(1,1,0,\ldots,0) \in \mathbb{F}_2^t$ and $\boldsymbol{u}^{(\ell)} = (0, \underbrace{1,1,\ldots,1}_{s-1}, 0, 1, 1, \ldots, 1) \in \mathbb{F}_2^t$. For convenience, denote the vector $\boldsymbol{a} * \boldsymbol{u}^{*(k-1)} * \boldsymbol{u}^{(\ell)} * \boldsymbol{a}'^{*(k-j-1)} * (1,1,0,\ldots,0) * \boldsymbol{a}'^{*j}$ by $\boldsymbol{z}$. If $j > 0$, then we can drop $t-1$ zeros from the last copy of $\boldsymbol{a}'$ in $\boldsymbol{z}$ to obtain a binary vector of length $m - a - (t+2)$, which contains no more than $t-1$ consecutive 1's. If $j = 0$ we can still drop the last $t-2$ zeros from $\boldsymbol{z}$. The resulting vector has length no more than $m - (t+2)$ if $a \geqslant 1$. Hence we only need to consider the case $j = 0$ and $a = 0$. In that case V is spanned by $S(\boldsymbol{u}^{*(k-1)} * \boldsymbol{u}^{(\ell)} * \boldsymbol{a}'^{*(k-1)} * (1,1))$ and $\boldsymbol{v}_0$ is not in the generating set. Thus, we can shift every entry in $\boldsymbol{u}^{*(k-1)} * \boldsymbol{u}^{(\ell)} * \boldsymbol{a}'^{*(k-1)} * (1,1)$ to the left by one position. This still is a generating vector for V which has length $m - (t+2)$.

Subcase 2: $\ell = a + jt + 1$ with $0 \leqslant j \leqslant k-1$. If $j < k-1$, the same vector $\boldsymbol{z}$ as in Subcase 1 will suit our purpose since it does not contain more than $t-1$ consecutive 1's. So we will assume $j = k-1$. We have

$$\boldsymbol{v}_{r+2} = \boldsymbol{v}_{r+1}^2 = \sum_{i=0}^{r-1} c_i^2 \boldsymbol{v}_{i+1}.$$

Since $\ell = a + (k-1)t + 1$, we have $c_{a+kt-1} = 0$. Note that some of the $\boldsymbol{v}_{i+1}$ might be of the form $\boldsymbol{v}_{a+nt}$. However, since $\boldsymbol{v}_{r+2} \in V(k)$ we must have $\sum_{n=0}^{k-1} c_{a+nt-1}^2 \boldsymbol{v}_{a+nt} = 0$. Hence we have that $\boldsymbol{v}_\ell = \boldsymbol{v}_{a+(k-1)t+1}$ is a linear combination of $\boldsymbol{v}_{r+2}$ and some vector in $V(k)$. It follows that V is spanned by $S(\boldsymbol{a} * \boldsymbol{u}^{*(k-1)} * (0,1,0,1,\ldots,1) * (1,0,1,0,\ldots,0) * \boldsymbol{a}'^{*(k-1)})$. Denote the vector $\boldsymbol{a} * \boldsymbol{u}^{*(k-1)} * (0,1,0,1,\ldots,1) * (1,0,1,0,\ldots,0) * \boldsymbol{a}'^{*(k-1)}$ by $\boldsymbol{z}'$. We see that $\boldsymbol{z}'$ contains no more than $t-1$ consecutive 1's. If

$k-1>0$ then we can drop the last $t-1$ zeros of $\boldsymbol{z}'$ and obtain a vector of length $m-a-(t+2)$. If $k-1=0$ we can drop the last $t-3$ zeros of $\boldsymbol{z}'$. If $a \geqslant 2$ this vector will have length at most $m-(t+2)$. We need to consider the case $k=1$ and $a \leqslant 1$. Suppose $a=0$ (so $r=t$). Then $\boldsymbol{v}_{r+1}=c_1\boldsymbol{v}_1$ with $c_1 \neq 0$. Keep squaring both sides of this equation, we see that $\boldsymbol{v}_{r+1+m}$ is a nonzero scalar multiple of $\boldsymbol{v}_{r+4}$. If $r>3$ then this contradicts the fact that any r consecutive vectors in the set $\{\boldsymbol{v}_0,\dots,\boldsymbol{v}_{m-1}\}$ are linearly independent. So $r \leqslant 3$. Since $t \geqslant 3$ and $r=t$ we have $r \geqslant 3$. Thus $m=9$. But we assumed that $m>9$, so the case $a=0$ cannot happen.

Now suppose $a=1$. Then $\boldsymbol{v}_{r+1}=c_0\boldsymbol{v}_0+c_2\boldsymbol{v}_2$ and $c_0 \neq 0$, hence $\boldsymbol{v}_{r+2}=c_0^2\boldsymbol{v}_1+c_2^2\boldsymbol{v}_3$. Note that since $a=1$, we have $V(k)=V(1)=V((10\underbrace{11\dots1}_{t-1}))$. So the previous equation implies that $\boldsymbol{v}_{r+2}\notin V(1)$, contradicting the assumption that $V(k+1)=V(k)$.

Subcase 3: $0 \leqslant \ell \leqslant a-1$. Observe that $v_{r+1}, v_{r+2},\dots,v_{r+t-1}\in V(k)$ as well. Note that $v_{r+1}^{2^{a-\ell}}=c_\ell^{2^{a-\ell}}v_a+\cdots\notin V(k)$ as $v_a\notin V(k)$. It follows that $a-\ell>t-2$. Since $a \leqslant t-1$ this is only possible when $\ell=0$. But then $\boldsymbol{v}_{r+1}=c_0\boldsymbol{v}_0$, with $c_0\neq 0$. This implies that $\boldsymbol{v}_m=\boldsymbol{v}_0=c_0^{2^{r+2}+2}\boldsymbol{v}_1$, which is impossible. This completes the proof. □

Acknowledgements. The third author thanks the Department of Mathematics, National University of Singapore for a research visit in January 2002, which brought the second and the third author together to work on this subject. The research of the third author was also partially supported by NSA grant MDA 904-01-1-0036. After we submitted the paper, we learned (in February 2003) that an idea similar to that given in Section 2 for constructing maximal arcs was discussed in Hamilton's talk in Oberwolfach in December 2001.

References

[1] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica* **17** (1997), 31–41. MR 98h:51014 Zbl 0880.51003

[2] A. Barlotti, Sui $\{k;n\}$-archi di un piano lineare finito. *Boll. Un. Mat. Ital.* (3) **11** (1956), 553–556. MR 18,666e Zbl 0072.38103

[3] R. H. F. Denniston, Some maximal arcs in finite projective planes. *J. Combin. Theory* **6** (1969), 317–319. MR 39 #1345 Zbl 0167.49106

[4] N. Hamilton, Degree 8 maximal arcs in $\mathrm{PG}(2,2^h)$, h odd. *J. Combin. Theory Ser. A* **100** (2002), 265–276. MR 1 940 336

[5] N. Hamilton, R. Mathon, More maximal arcs in Desarguesian projective planes and their geometric structure. Preprint.

[6] J. W. P. Hirschfeld, *Projective geometries over finite fields*. Oxford Univ. Press 1998. MR 99b:51006 Zbl 0899.51002

[7] R. Lidl, H. Niederreiter, *Finite fields*. Cambridge Univ. Press 1997. MR 97i:11115 Zbl 0866.11069

[8] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes.* North-Holland 1977. MR 57 #5408a Zbl 0369.94008

[9] R. Mathon, New maximal arcs in Desarguesian planes. *J. Combin. Theory Ser. A* **97** (2002), 353–368. MR 2002k:51012 Zbl 01763788

[10] J. A. Thas, Construction of maximal arcs and partial geometries. *Geom. Dedicata* **3** (1974), 61–64. MR 50 #1931 Zbl 0285.50018
[11] J. A. Thas, Construction of maximal arcs and dual ovals in translation planes. *European J. Combin.* **1** (1980), 189–192. MR 82a:05031 Zbl 0449.51011

Received 9 October, 2002

F. Fiedler, Q. Xiang, Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA
Email: {fiedler, xiang}@math.udel.edu

K. H. Leung, Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260
Email: matlkh@nus.edu.sg