Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
Journal of Combinatorial Theory, Series A 108 (2004) 99–122
Journal of Combinatorial Theory Series A
http://www.elsevier.com/locate/jcta

On Mathon's construction of maximal arcs in Desarguesian planes II

Frank Fiedler,[a] Ka Hin Leung,[b] and Qing Xiang[a]

[a] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*
[b] *Department of Mathematics, National University of Singapore, Kent Ridge, Singapore*

Received 6 January 2004

Available online 22 July 2004

Abstract

In a recent paper, Mathon (J. Combin. Theory (A) 97 (2002) 353) gives a new construction of maximal arcs which generalizes the construction of Denniston. In relation to this construction, Mathon asks the question of determining the largest degree of a non-Denniston maximal arc arising from his new construction. In this paper, we give a nearly complete answer to this problem. Specifically, we prove that when $m \geqslant 5$ and $m \neq 9$, 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 is $(\lfloor \frac{m}{2} \rfloor + 1)$. This confirms our conjecture in (Fiedler et al. (Adv. Geom. (2003) (Suppl.) S119)). For $\{p, q\}$-maps, we prove that if $m \geqslant 7$ and $m \neq 9$, then the largest d of a non-Denniston maximal arc of degree 2^d in $\mathrm{PG}(2, 2^m)$ generated by a $\{p, q\}$-map is either $\lfloor \frac{m}{2} \rfloor + 1$ or $\lfloor \frac{m}{2} \rfloor + 2$.

Keywords: Arc; Linearized polynomial; Maximal arc; Moore determinant; Quadratic form

1. Introduction

Let $\mathrm{PG}(2, q)$ denote the Desarguesian projective plane of order q, where q is a prime power, and let $k \geqslant 1$, $n \geqslant 2$ be integers. A set $\mathcal{K}$ of k points in $\mathrm{PG}(2, q)$ is called a (k, n)-*arc* if no $n + 1$ points of $\mathcal{K}$ are collinear. The integer n is called the *degree* of the arc $\mathcal{K}$. Let P be a point of a (k, n)-arc $\mathcal{K}$. Each of the $q + 1$ lines through P contains at most $n - 1$ points of $\mathcal{K}$. Therefore

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

E-mail addresses: fiedler@math.udel.edu (F. Fiedler), matlkh@nus.edu.sg (K.H. Leung), xiang@math.udel.edu (Q. Xiang).

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2004.06.005

The (k,n)-arc $\mathcal{K}$ is said to be *maximal* if k attains this upper bound, that is, $k = q(n-1)+n$. In this case, every line of $\mathrm{PG}(2,q)$ that contains a point of $\mathcal{K}$ has to intersect it in exactly n points. Therefore, the degree n of a maximal arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$ must divide q.

In the case where $q = 2^m$, maximal arcs of degree 2 in $\mathrm{PG}(2,q)$ are usually called *hyperovals*. A classical example of a hyperoval in $\mathrm{PG}(2,2^m)$ is a non-degenerate conic (i.e., non-singular quadric in $\mathrm{PG}(2,2^m)$) plus its nucleus. There is an extensive literature devoted to ovals and hyperovals, see a recent survey in [P]. The study of maximal arcs of degree greater than two was started by Barlotti [B] in 1956. At the beginning, maximal arcs were studied as extremal objects in finite geometry and coding theory. Later it was discovered that maximal arcs can give rise to many interesting incidence structures such as partial geometries and resolvable Steiner 2-designs [T1,W]. The constructions of Thas [T1,T2] also show connections of maximal arcs with ovoids, quadrics and polar spaces. Of course, maximal arcs can also give rise to two-weight codes and strongly regular graphs since they are two-intersection sets in $\mathrm{PG}(2,q)$. For these reasons maximal arcs occupy a very special place in finite geometry, design theory and coding theory.

For $q = 2^m$, Denniston [D] constructed maximal arcs of degree 2^d in $\mathrm{PG}(2,2^m)$ for every d, $1 \leqslant d \leqslant m$. Thas [T1,T2] also gave two other constructions of maximal arcs in $\mathrm{PG}(2,2^m)$ of certain degrees when m is even. For odd prime power q, Ball et al. [BBM] proved that maximal arcs of degree n do not exist in $\mathrm{PG}(2,q)$, when $n<q$. Recently, Mathon [M] presented a new construction of maximal arcs which generalizes the construction of Denniston. In the following, we will briefly describe the constructions of Denniston and Mathon of maximal arcs.

Let $Q(x,y) = ax^2 + hxy + by^2$ be an irreducible quadratic form over $\mathbb{F}_{2^m}$ (that is, $\mathrm{Tr}(\frac{ab}{h^2}) = 1$, where Tr is the trace from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$). Let A be an additive subgroup of $\mathbb{F}_{2^m}$ and let (x,y,z) be right-normalized homogeneous coordinates in $\mathrm{PG}(2,2^m)$. Then

$$\mathcal{K} = \{(x,y,1) \in \mathrm{PG}(2,2^m) \mid Q(x,y) \in A\} \tag{1.1}$$

is a maximal arc of degree $|A|$. This is Denniston's construction of maximal arcs [D]. We may decompose $\mathcal{K}$ as

$$\mathcal{K} = \cup_{\lambda \in A} F_\lambda,$$

where for each $\lambda \in A\backslash\{0\}$, $F_\lambda = \{(x,y,1) \mid Q(x,y) = \lambda\}$ is a non-degenerate conic, and $F_0 = \{(0,0,1)\}$ contains one point only. Note that the point $(0,0,1)$ is the common nucleus of the conics F_λ, $\lambda \in A\backslash\{0\}$. The arc $\mathcal{K}$ in (1.1), and those projectively equivalent to $\mathcal{K}$ are called *Denniston maximal arcs*.

Now let $\mathcal{C}$ be the set of 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 $\lambda \in \mathbb{F}_{2^m} \cup \{\infty\}$ and $\alpha, \beta \in \mathbb{F}_{2^m}^*$ such that $\alpha x^2 + x + \beta$ is irreducible over $\mathbb{F}_{2^m}$. Note that $F_0 := F_{\alpha,\beta,0} = \{(0,0,1)\}$ is the common nucleus of the non-degenerate conics in $\mathcal{C}$, and $F_\infty := F_{\alpha,\beta,\infty}$ is the line at infinity $z = 0$. Given two non-degenerate conics

$F_{\alpha,\beta,\lambda}$ and $F_{\alpha',\beta',\lambda'}$ in $\mathcal{C}$, Mathon [M] defined a composition

$$F_{\alpha,\beta,\lambda} \oplus F_{\alpha',\beta',\lambda'} = F_{\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda'}, \tag{1.2}$$

where if $\lambda \neq \lambda'$, then

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

and if $\lambda = \lambda'$, then

$$F_{\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda'} = F_0.$$

A subset of non-degenerate conics of $\mathcal{C}$ that is closed under the above composition is called a *closed* set of conics, and such a set must contain $2^d - 1$ conics for some d, $1 \leqslant d \leqslant m$ [M, Corollary 2.3]. Mathon [M] showed that closed sets of conics can be used to construct maximal arcs.

Theorem 1.1 (Mathon [M, Theorem 2.4]). *Let $\mathcal{F} \subset \mathcal{C}$ be a closed set of $2^d - 1$ non-degenerate conics with a common nucleus F_0 in $\mathrm{PG}(2, 2^m)$, $1 \leqslant d \leqslant m$. Then the set of points of all conics in $\mathcal{F}$ together with F_0 form a maximal $(2^{m+d} - 2^m + 2^d, 2^d)$-arc $\mathcal{K}$ in $\mathrm{PG}(2, 2^m)$.*

The construction in Theorem 1.1 clearly contains Denniston's construction of maximal arcs as a special case. Let A be an additive subgroup of $\mathbb{F}_{2^m}$, let $a, b, h \in \mathbb{F}_{2^m}$ be fixed such that $\mathrm{Tr}(\frac{ab}{h^2}) = 1$, and let $\mathcal{F} = \{F_{ah^{-1},bh^{-1},\lambda h^{-1}} \in \mathcal{C} \mid \lambda \in A \setminus \{0\}\}$. Then $\mathcal{F}$ is clearly closed under the composition in (1.2), and the maximal arc obtained via Theorem 1.1 from $\mathcal{F}$ is exactly the Denniston arc in (1.1).

Let $\mathcal{F} \subset \mathcal{C}$ be a closed set of $(2^d - 1)$ non-degenerate conics, and let

$$A^* = \{\lambda \mid \text{there exist } \alpha, \beta \in \mathbb{F}_{2^m}^* \text{ such that } F_{\alpha,\beta,\lambda} \in \mathcal{F}\}.$$

Then $A := A^* \cup \{0\}$ is an additive subgroup of $\mathbb{F}_{2^m}$. Moreover, for each $\lambda \in A^*$ there corresponds a unique conic $F_{\alpha,\beta,\lambda}$ in $\mathcal{F}$ (otherwise, $F_0 \in \mathcal{F}$, a contradiction), hence α and β in the indices of $F_{\alpha,\beta,\lambda}$ can be interpreted as functional values of some functions $p : A \to \mathbb{F}_{2^m}$ and $q : A \to \mathbb{F}_{2^m}$, respectively. Since $\mathcal{F}$ is closed under the composition defined in (1.2), we have

$$p(\lambda + \lambda')(\lambda + \lambda') = p(\lambda)\lambda + p(\lambda')\lambda',$$

$$q(\lambda + \lambda')(\lambda + \lambda') = q(\lambda)\lambda + q(\lambda')\lambda'$$

for all $\lambda, \lambda' \in A$. Thus, the maps $\bar{p} : A \to \mathbb{F}_{2^m}$ and $\bar{q} : A \to \mathbb{F}_{2^m}$ defined, respectively, by $\bar{p}(\lambda) = p(\lambda)\lambda$ and $\bar{q}(\lambda) = q(\lambda)\lambda$ are linear on A. Since A is an $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^m}$, we can extend $\bar{p}$ and $\bar{q}$ linearly to $\mathbb{F}_{2^m}$, and we denote the extended maps still by $\bar{p}$ and $\bar{q}$. Now that $\bar{p}$ and $\bar{q}$ are both linear on $\mathbb{F}_{2^m}$, there exist linearized polynomials $\sum_{i=0}^{m-1} c_i x^{2^i}$ and $\sum_{i=0}^{m-1} d_i x^{2^i}$ in $\mathbb{F}_{2^m}[x]$ such that for all $a \in \mathbb{F}_{2^m}$, $\bar{p}(a) = \sum_{i=0}^{m-1} c_i a^{2^i}$ and $\bar{q}(a) = \sum_{i=0}^{m-1} d_i a^{2^i}$. Furthermore, by "division algorithm" (cf. [FLX, Proposition 3.1]), there exist linearized polynomials $L(x) = \sum_{i=0}^{d-1} a_i x^{2^i}$ and $M(x) = \sum_{i=0}^{d-1} b_i x^{2^i}$ in $\mathbb{F}_{2^m}[x]$ such that $\bar{p}(\lambda) = L(\lambda)$ and $\bar{q}(\lambda) = M(\lambda)$ for all $\lambda \in A$. This shows that each closed set $\mathcal{F} \subset \mathcal{C}$ of $(2^d - 1)$ conics can be written in the form

$$\left\{ F_{\frac{L(\lambda)}{\lambda}, \frac{M(\lambda)}{\lambda}, \lambda} \mid \lambda \in A \backslash \{0\} \right\},$$

where A is some additive subgroup of $\mathbb{F}_{2^m}$ of size 2^d, and $L(x), M(x) \in \mathbb{F}_{2^m}[x]$ are given above.

Theorem 1.2 (Mathon [M, Theorem 2.5]). *Let* $p(x) = \sum_{i=0}^{d-1} a_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$ *and* $q(x) = \sum_{i=0}^{d-1} b_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$ *be polynomials with coefficients in* $\mathbb{F}_{2^m}$. *For an additive subgroup A of order* 2^d *of* $\mathbb{F}_{2^m}$ *let* $\mathcal{F} = \{F_{p(\lambda), q(\lambda), \lambda} \mid \lambda \in A \backslash \{0\}\}$ *be a set of conics with a common nucleus* F_0. *If* $\mathrm{Tr}(p(\lambda)q(\lambda)) = 1$ *for every* $\lambda \in A \backslash \{0\}$, *then* $\mathcal{F}$ *is a closed subset of* $\mathcal{C}$ *and the set of points on all conics in* $\mathcal{F}$ *together with* F_0 *forms a maximal* $(2^{m+d} - 2^m + 2^d, 2^d)$*-arc* $\mathcal{K}$ *in* $\mathrm{PG}(2, 2^m)$. *If both* $p(x), q(x)$ *have degree* $\leqslant 2$, *then* $\mathcal{K}$ *is a Denniston maximal arc.*

We will call maximal arcs generated by polynomials as in the above theorem *maximal arcs generated by* $\{p, q\}$*-maps*. Mathon posed several problems related to the construction in Theorem 1.2 at the end of his paper [M]. The third problem he posed is: What is the largest d of a non-Denniston maximal arc of degree 2^d in $\mathrm{PG}(2, 2^m)$ generated by a $\{p, q\}$-map via Theorem 1.2? We give a nearly complete answer to this problem in this paper (see details below). The techniques we use are algebraic. Polynomials over finite fields play an important role throughout our investigation. Combinatorial and linear algebraic tools are used to study these polynomials in this paper. We hope that these techniques will find more applications in finite geometry and combinatorial designs.

Our main results are summarized as follows. In Section 2, we prove that if $m \geqslant 5$ and $m \neq 9$, then the largest degree of a non-Denniston maximal arc in $\mathrm{PG}(2, 2^m)$ generated by a $\{p, 1\}$-map is less than or equal to $2^{\lfloor \frac{m}{2} \rfloor + 1}$. On the other hand, known constructions in [FLX,HM,M] show that there are always $\{p, 1\}$-maps that generate non-Denniston maximal arcs in $\mathrm{PG}(2, 2^m)$ of degree $2^{\lfloor \frac{m}{2} \rfloor + 1}$ when $m \geqslant 5$. Therefore, for $\{p, 1\}$-maps, we have a complete answer to Mathon's question mentioned above. That is, when $m \geqslant 5$ and $m \neq 9$, 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 1.2 is $\lfloor \frac{m}{2} \rfloor + 1$. This confirms our conjecture in [FLX]. In Section 3 we try to extend this result to $\{p, q\}$-maps. We prove that if $m \geqslant 7$ and $m \neq 9$, then the largest degree of a non-Denniston maximal arc in $\mathrm{PG}(2, 2^m)$ generated by a $\{p, q\}$-map is less than or equal to $2^{\lfloor \frac{m}{2} \rfloor + 2}$. However, at present we are not able to find a construction of $\{p, q\}$-maps to produce (via Theorem 1.2) a non-Denniston maximal arc in $\mathrm{PG}(2, 2^m)$ of degree $2^{\lfloor \frac{m}{2} \rfloor + 2}$. Therefore our upper bound together with previously known constructions in [FLX,HM,M], yields that for $m \geqslant 7$ and $m \neq 9$, the largest d of a non-Denniston maximal arc of degree 2^d in $\mathrm{PG}(2, 2^m)$ generated by a $\{p, q\}$-map is either $\lfloor \frac{m}{2} \rfloor + 1$ or $\lfloor \frac{m}{2} \rfloor + 2$.

2. The largest degree of non-Denniston maximal arcs generated by $\{p, 1\}$-maps

We first prove the following theorem, which establishes the upper bound mentioned in Section 1 on the largest degree of non-Denniston maximal arcs generated by a $\{p, 1\}$-map.

Theorem 2.1. *Let A be an additive subgroup of size 2^d in $\mathbb{F}_{2^m}$, and let $p(x) = \sum_{i=0}^{d-1} a_i x^{2^i-1} \in \mathbb{F}_{2^m}[x]$. Assume that $m \geqslant 5$ but $m \neq 9$, and $m > d > \frac{m}{2} + 1$. If $\mathrm{Tr}(p(\lambda)) = 1$ for all $\lambda \in A \backslash \{0\}$, then $a_2 = a_3 = \cdots = a_{d-1} = 0$. That is, $p(x)$ is linear and the maximal arc obtained from the $\{p, 1\}$-map via Theorem 1.2 is a Denniston maximal arc.*

In order to prove this theorem we need some preparation. For convenience, let $r = m - d$. We will represent the $\mathbb{F}_2$-subspace A of $\mathbb{F}_{2^m}$ as the intersection of r hyperplanes, say

$$A = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}(\mu_i x) = 0, 1 \leqslant i \leqslant r\},$$

where $\mu_i \in \mathbb{F}_{2^m}^*$ are linearly independent over $\mathbb{F}_2$. Thus, the defining equation for A is

$$\prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) = 1.$$

The key to the proof of Theorem 2.1 is to study the polynomial $\prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x))$, where $\mathrm{Tr}(\mu_i x) = \sum_{j=0}^{m-1} \mu_i^{2^j} x^{2^j}$ is a polynomial in $\mathbb{F}_{2^m}[x]$. We define $S(x)$ to be the polynomial of degree less than or equal to $2^m - 1$ such that

$$S(x) \equiv \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) \pmod{x^{2^m} - x}.$$

For $s \geqslant 1$ and $m - 1 \geqslant i_1 > i_2 > \cdots > i_s \geqslant 0$, we use $c(i_1, i_2, \ldots, i_s)$ to denote the coefficient of $x^{2^{i_1}+2^{i_2}+\cdots+2^{i_s}}$ in $S(x)$. It is clear that $c(i_1, i_2, \ldots, i_s)$ is zero if $s > r$. Moreover, as $S(x)^2 \equiv S(x) \pmod{x^{2^m} - x}$, we see that when $s \leqslant r$,

$$c(i_1, i_2, \ldots, i_s)^2 = \begin{cases} c(i_1 + 1, i_2 + 1, \ldots, i_s + 1) & \text{if } i_1 < m - 1, \\ c(i_2 + 1, \ldots, i_s + 1, 0) & \text{if } i_1 = m - 1. \end{cases} \tag{2.1}$$

If $s = r$, then

$$c(i_1, i_2, \ldots, i_r) = \det(\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \ldots, \mathbf{v}_{i_r}), \tag{2.2}$$

where $\mathbf{v}_i = (\mu_1^{2^i}, \mu_2^{2^i}, \ldots, \mu_r^{2^i})^{\mathsf{T}}$. We remark that since $\mu_j^{2^m} = \mu_j$, we have $\mathbf{v}_m = \mathbf{v}_0$, and we will read the indices of $\mathbf{v}_i$ modulo m.

Since the μ_i are linearly independent over $\mathbb{F}_2$, $c(r-1, r-2, \ldots, 1, 0) = \det(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{r-1})$ is non-zero. For a proof of this fact, see [G, p. 5] or [LN, Lemma 3.5]. Indeed, $\det(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{r-1})$ is usually called a *Moore determinant*, which can be viewed as a q-analogue of the familiar Vandermonde determinants. It follows from (2.1) that $\det(\mathbf{v}_i, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_{i+r-1}) = c(i + r - 1, \ldots, i + 1, i) \neq 0$ for all i.

Therefore, any r consecutive vectors $\mathbf{v}_i, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_{i+r-1}$ from $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{m-1}$ are linearly independent over $\mathbb{F}_{2^m}$.

The following lemma reveals more surprising relations among the coefficients of $S(x)$. We will use this lemma in the proof of Theorem 2.1.

Lemma 2.2. $c(r, r-1, \ldots, 2, 0) = c(r-1, r-2, \ldots, 1, 0)c(r-1, r-2, \ldots, 2, 1)$.

Proof. First note that $c(r-1, r-2, \ldots, 1, 0) = \det(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{r-1}) \neq 0$. In order to prove the lemma, we show that

$$c(r-1, r-2, \ldots, 2, 1) = \frac{c(r, r-1, \ldots, 2, 0)}{c(r-1, r-2, \ldots, 1, 0)}.$$

Now notice that $c(r, r-1, \ldots, 2, 0) = \det(\mathbf{v}_0, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_r)$, so we are trying to prove that $c(r-1, r-2, \ldots, 2, 1)$ is a quotient of two determinants. This motivates us to consider the following linear system:

$$\begin{pmatrix} \mu_1 & \mu_1^2 & \cdots & \mu_1^{2^{r-1}} \\ \mu_2 & \mu_2^2 & & \mu_2^{2^{r-1}} \\ \vdots & & \ddots & \vdots \\ \mu_r & \mu_r^2 & \cdots & \mu_r^{2^{r-1}} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{r-1} \end{pmatrix} = \begin{pmatrix} \mu_1^{2^r} \\ \mu_2^{2^r} \\ \vdots \\ \mu_r^{2^r} \end{pmatrix}. \tag{2.3}$$

The determinant of the coefficient matrix of this system is $c(r-1, r-2, \ldots, 1, 0) \neq 0$. Thus the system has a unique solution. In particular, by Cramer's rule,

$$b_1 = \frac{\begin{vmatrix} \mu_1 & \mu_1^{2^r} & \mu_1^{2^2} & \cdots & \mu_1^{2^{r-1}} \\ \mu_2 & \mu_2^{2^r} & \mu_2^{2^2} & & \mu_2^{2^{r-1}} \\ \vdots & & & \ddots & \vdots \\ \mu_r & \mu_r^{2^r} & \mu_r^{2^2} & \cdots & \mu_r^{2^{r-1}} \end{vmatrix}}{\begin{vmatrix} \mu_1 & \mu_1^2 & \mu_1^{2^2} & \cdots & \mu_1^{2^{r-1}} \\ \mu_2 & \mu_2^2 & \mu_2^{2^2} & & \mu_2^{2^{r-1}} \\ \vdots & & & \ddots & \vdots \\ \mu_r & \mu_r^2 & \mu_r^{2^2} & \cdots & \mu_r^{2^{r-1}} \end{vmatrix}} = \frac{c(r, r-1, \ldots, 2, 0)}{c(r-1, \ldots, 1, 0)}.$$

Next we calculate b_js explicitly in a different way. In particular, we will show that $b_1 = c(r-1, r-2, \ldots, 2, 1)$. To this end, we consider the formal power series

$$f_t(x) = \left(\sum_{j=0}^{\infty} \mu_t^{2^j} x^{2^j}\right) \prod_{i=1}^{r} \left(1 + \sum_{j=0}^{\infty} \mu_i^{2^j} x^{2^j}\right) \in \mathbb{F}_{2^m}[[x]]$$

for $1 \leqslant t \leqslant r$. We have

$$\left(\sum_{j=0}^{\infty} \mu_t^{2^j} x^{2^j}\right) \prod_{i=1}^{r} \left(1 + \sum_{j=0}^{\infty} \mu_i^{2^j} x^{2^j}\right) = \left(\sum_{j=0}^{\infty} \mu_t^{2^j} x^{2^j}\right)\left(1 + \sum_{j=0}^{\infty} \mu_t^{2^j} x^{2^j}\right) \times \prod_{\substack{i=1 \\ i \neq t}}^{r} \left(1 + \sum_{j=0}^{\infty} \mu_i^{2^j} x^{2^j}\right) = \mu_t x \prod_{\substack{i=1 \\ i \neq t}}^{r} \left(1 + \sum_{j=0}^{\infty} \mu_i^{2^j} x^{2^j}\right).$$

For any integer $s \leqslant r$ and $i_1 > i_2 > \cdots > i_s \geqslant 0$, we denote the coefficient of $x^{2^{i_1}+2^{i_2}+\cdots+2^{i_s}}$ in $\prod_{i=1}^{r}(1 + \sum_{j=0}^{\infty} \mu_i^{2^j} x^{2^j})$ by $c'(i_1, i_2, \ldots, i_s)$. Note that $c'(i_1, i_2, \ldots, i_s)$ is not necessarily the same as $c(i_1, i_2, \ldots, i_s)$ defined earlier. The former is the coefficient in a formal power series $\prod_{i=1}^{r}(1 + \sum_{j=0}^{\infty} \mu_i^{2^j} x^{2^j}) \in \mathbb{F}_{2^m}[[x]]$ while the latter is the coefficient in $S(x) \in \mathbb{F}_{2^m}[x]/(x^{2^m} - x)$.

Clearly, the coefficient of x^{2^r-1} in $\prod_{i=1, i \neq t}^{r}(1 + \sum_{j=0}^{\infty} \mu_i^{2^j} x^{2^j})$ is 0. This shows that the coefficient of x^{2^r} in $f_t(x)$ is 0. On the other hand, from the definition of $f_t(x)$, we see that this coefficient is $\mu_t^{2^r} + \sum_{j=0}^{r-1} \mu_t^{2^j} c'(r-1, \ldots, j)$. Thus, we obtain

$$\mu_t^{2^r} = \sum_{j=0}^{r-1} \mu_t^{2^j} c'(r-1, \ldots, j+1, j) \tag{2.4}$$

for all $1 \leqslant t \leqslant r$. Combining (2.3) and (2.4) we have $b_j = c'(r-1, \ldots, j+1, j)$. In particular, $b_1 = c'(r-1, \ldots, 2, 1)$. To finish the proof, we have to show that $c'(r-1, \ldots, 2, 1) = c(r-1, \ldots, 2, 1)$. Clearly, it suffices to show that if s, $j_1, \ldots, j_s$ are integers with $s \leqslant r$ and $0 \leqslant j_1, \ldots, j_s \leqslant m-1$ such that

$$2^{j_1} + 2^{j_2} + \cdots + 2^{j_s} \equiv 2^{r-1} + 2^{r-2} + \cdots + 2 \pmod{2^m - 1} \tag{2.5}$$

then $2^{j_1} + 2^{j_2} + \cdots + 2^{j_s} < 2^m - 1$.

For any integer a not divisible by $2^m - 1$, we use $w(a)$ to denote the sum of the digits of $a \pmod{2^m - 1}$ written in base 2 representation. Note that if $a + b \not\equiv 0 \pmod{2^m - 1}$, then $w(a+b) \leqslant w(a) + w(b)$, and $w(a) + w(b) - w(a+b)$ is the number of carries that occurred in the addition of a and b. Applying this to the above congruence we see that $s \geqslant r-1$, thus $s = r$ or $r-1$. Moreover, if $s = r$, then exactly one carry occurs in the (modular) addition $2^{j_1} + 2^{j_2} + \cdots + 2^{j_s}$, and if $s = r-1$, then necessarily $\{j_1, j_2, \ldots, j_s\} = \{1, 2, \ldots, r-1\}$ and $2^{j_1} + 2^{j_2} + \cdots + 2^{j_s} < 2^m - 1$.

Now suppose that $2^{j_1} + 2^{j_2} + \cdots + 2^{j_s} \geqslant 2^m - 1$. Then, by our previous observation, $s = r$ and exactly one carry occurs in the addition $2^{j_1} + 2^{j_2} + \cdots + 2^{j_s}$. This shows that exactly two or exactly three exponents among $j_1, j_2, \ldots, j_s$ are equal. Without loss of generality, we assume that either $j_1 = j_2$ ($j_3 > j_4 > \cdots > j_s$ and they are not equal to j_1) or $j_1 = j_2 = j_3$ ($j_4 > j_5 > \cdots > j_s$ and they are not equal to j_1). In the former case we must have $m-1=j_1=j_2>j_3>j_4>\cdots>j_s>0$, and

$$2^{j_1}+2^{j_2}+\cdots+2^{j_s}\equiv 2^{j_3}+2^{j_4}+\cdots+2^{j_s}+2^0\ (\mathrm{mod}\ 2^m-1),$$

contradicting (2.5). In the latter case, we must have $m-1=j_1=j_2=j_3>j_4>j_5>\cdots>j_s>0$, and

$$2^{j_1}+2^{j_2}+\cdots+2^{j_s}\equiv 2^{m-1}+2^{j_4}+2^{j_5}+\cdots+2^{j_s}+2^0\ (\mathrm{mod}\ 2^m-1),$$

again contradicting (2.5). This completes the proof of the lemma. □

We will also need the following lemma in the proof of Theorem 2.1.

Lemma 2.3. *Let*

$$\begin{aligned}\Delta=&\,c(m-1,m-2,\ldots,m-r+1,m-r-1)c(m-2,m-3,\ldots,m-r,0)\\&+c(m-2,m-3,\ldots,m-r+1,m-r-1,0)c(m-1,m-2,\ldots,m-r).\end{aligned}$$

Then $\Delta\neq 0$.

Proof. Recall that

$$c(m-1,m-2,\ldots,m-r+1,m-r-1)=\det(\mathbf{v}_{m-1},\mathbf{v}_{m-2},\ldots,\mathbf{v}_{m-r+1},\mathbf{v}_{m-r-1}),$$

$$c(m-2,m-3,\ldots,m-r,0)=\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r},\mathbf{v}_0),$$

$$c(m-2,m-3,\ldots,m-r+1,m-r-1,0)=\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r+1},\mathbf{v}_{m-r-1},\mathbf{v}_0),$$

$$c(m-1,m-2,\ldots,m-r)=\det(\mathbf{v}_{m-1},\mathbf{v}_{m-2},\ldots,\mathbf{v}_{m-r}).$$

Since $\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r-1}$ form a basis of the $\mathbb{F}_{2^m}$-span of $\{\mathbf{v}_0,\mathbf{v}_1,\ldots,\mathbf{v}_{m-1}\}$, there exist α_is and β_is in $\mathbb{F}_{2^m}$ such that

$$\mathbf{v}_{m-1}=\alpha_{m-2}\mathbf{v}_{m-2}+\cdots+\alpha_{m-r}\mathbf{v}_{m-r}+\alpha_{m-r-1}\mathbf{v}_{m-r-1},\tag{2.6}$$

$$\mathbf{v}_0=\beta_{m-2}\mathbf{v}_{m-2}+\cdots+\beta_{m-r}\mathbf{v}_{m-r}+\beta_{m-r-1}\mathbf{v}_{m-r-1}.\tag{2.7}$$

Then

$$c(m-1,m-2,\ldots,m-r+1,m-r-1)=\alpha_{m-r}\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r},\mathbf{v}_{m-r-1}),$$

$$c(m-2,m-3,\ldots,m-r,0)=\beta_{m-r-1}\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r},\mathbf{v}_{m-r-1}),$$

$$c(m-2,m-3,\ldots,m-r+1,m-r-1,0)=\beta_{m-r}\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r},\mathbf{v}_{m-r-1}),$$

$$c(m-1,m-2,\ldots,m-r)=\alpha_{m-r-1}\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r},\mathbf{v}_{m-r-1}).$$

Hence we have

$$\Delta=\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r},\mathbf{v}_{m-r-1})^2\begin{vmatrix}\alpha_{m-r}&\alpha_{m-r-1}\\\beta_{m-r}&\beta_{m-r-1}\end{vmatrix}.$$

Since $\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r-1}$ are linearly independent over $\mathbb{F}_{2^m}$, $\det(\mathbf{v}_{m-2},\mathbf{v}_{m-3},\ldots,\mathbf{v}_{m-r-1})$ is non-zero. The second determinant in the right-hand side (RHS) of the above equation has to be non-zero for otherwise (2.6) and (2.7) give a dependence relation for the r consecutive vectors $\mathbf{v}_{m-1}, \mathbf{v}_{m-2}, \ldots, \mathbf{v}_{m-r+1}, \mathbf{v}_0$ (note that $\mathbf{v}_0 = \mathbf{v}_m$). This shows that $\Delta \neq 0$. □

We are now ready to give the proof of Theorem 2.1.

Proof of Theorem 2.1. Recall that we assume the defining equation for A is

$$\prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) = 1,$$

where $r = m - d$. Suppose that $\mathrm{Tr}(a_0) = 0$. Then $(1 + \mathrm{Tr}(\sum_{i=1}^{d-1} a_i \lambda^{2^i - 1})) = 0$ for all $\lambda \in A \backslash \{0\}$. Thus, the function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ associated with the polynomial $(1 + \mathrm{Tr}(\sum_{i=1}^{d-1} a_i x^{2^i - 1})) \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x))$ is the characteristic function of $\{0\}$ in $\mathbb{F}_{2^m}$. Hence, we have

$$\left(1 + \mathrm{Tr}\left(\sum_{j=1}^{d-1} a_j x^{2^j - 1}\right)\right) \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) \equiv x^{2^m - 1} - 1 \pmod{x^{2^m} - x}. \tag{2.8}$$

The binary representation of the exponent of $x^{2^m - 1}$ (in the LHS of (2.8)) is $11\ldots1$ (m ones altogether). Throughout this paper, we write the most significant bit (i.e., the $(m-1)$th bit) to the least significant bit (i.e., the 0th bit) from left-to-right. Note that the binary representation of the exponent of any term in $\prod_{i=1}^{r}(1 + \mathrm{Tr}(\mu_i x))$ cannot have more than r ones. The binary representation of the exponent of any term in $(1 + \mathrm{Tr}(\sum_{j=1}^{d-1} a_j x^{2^j - 1}))$ has at most $d - 1$ ones. Thus, the maximum number of ones in the binary representation of the exponent of any term on the left-hand side (LHS) of (2.8) is $r + (d - 1) = m - 1$. Therefore, the coefficient of $x^{2^m - 1}$ on the LHS of (2.8) is 0. This contradicts (2.8). So this case does not occur.

From now on we assume that $\mathrm{Tr}(a_0) = 1$. Then $\mathrm{Tr}(\sum_{i=1}^{d-1} a_i \lambda^{2^i - 1}) = 0$ for all $\lambda \in A \backslash \{0\}$. Therefore, the function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ associated with the polynomial

$$\mathrm{Tr}\left(\sum_{j=1}^{d-1} a_j x^{2^j - 1}\right) \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) \in \mathbb{F}_{2^m}[x]$$

is the zero function. That is, in $\mathbb{F}_{2^m}[x]$, we have the following congruence:

$$\mathrm{Tr}\left(\sum_{j=1}^{d-1} a_j x^{2^j - 1}\right) \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) \equiv 0 \pmod{x^{2^m} - x}. \tag{2.9}$$

For later use, we let $T(x)$ and $S(x)$ be polynomials in $\mathbb{F}_{2^m}[x]$ of degree less than or equal to $2^m - 1$ such that $T(x) \equiv \mathrm{Tr}(\sum_{j=1}^{d-1} a_j x^{2^j - 1}) \pmod{x^{2^m} - x}$ and $S(x) \equiv \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) \pmod{x^{2^m} - x}$.

Now the proof proceeds as follows. We will first prove that $a_{d-1} = a_{d-2} = 0$. Next, we will show that the "upper half" coefficients of $p(x)$ are zero. More precisely, we prove that $a_{m-d+1} = a_{m-d+2} = \cdots = a_{d-3} = 0$. Finally, we show that the "lower half" coefficients of $p(x)$ are also zero. That is, $a_2 = a_3 = \cdots = a_{m-d} = 0$ (here we assume that $m - d \geqslant 2$).

Claim. $a_{d-1} = a_{d-2} = 0$: Consider the coefficient of the monomial $x^{(2^{m-1}-1)-2^{d-2}}$ in $T(x)S(x)$, i.e., the LHS of (2.9). The binary expansion of its exponent is

$$0\overbrace{1\ldots11}^{r}0\overbrace{1\ldots1}^{d-2}.$$

The number of 1's in this expansion is $(m-2)$. The maximum number of 1's in the exponent of any summand in $S(x)$ is r and the maximum number of 1's in the exponent of any summand in $T(x)$ is $d-1$. When adding two exponents (written in their binary representations), any carry that may occur reduces the number of 1's in the sum. Since we are interested in an exponent whose number of 1's is $(m-2)$, it can only be obtained as a sum of two exponents (one is the exponent of a summand in $T(x)$, the other in $S(x)$) with at most one carry.

If $(2^{m-1}-1) - 2^{d-2}$ is obtained as a sum without carry then there is only one possibility.

$$0\overbrace{1\ldots11}^{r}0\overbrace{1\ldots1}^{d-2} = 0\overbrace{1\ldots11}^{r}000\ldots00 + 00\ldots000\overbrace{11\ldots11}^{d-2}.$$

Using the assumption that $2d > m+2$, we see that $r < d-2$ and thus, the $d-2$ consecutive 1's have to come from the term $x^{2^{d-2}-1}$ in $T(x)$, whose coefficient is a_{d-2}.

If $(2^{m-1}-1) - 2^{d-2}$ is obtained as a sum with exactly one carry, then that carry has to happen at position $d-2$ and so

$$0\overbrace{1\ldots11}^{r}0\overbrace{1\ldots1}^{d-2} = 0\overbrace{1\ldots1}^{r}0100\ldots00 + 00\ldots00\overbrace{111\ldots11}^{d-1}.$$

Again, the $d-1$ consecutive 1's have to come from the term $x^{2^{d-1}-1}$ in $T(x)$, whose coefficient is a_{d-1}. Hence by (2.9), we have

$$\begin{aligned} &c(m-2, m-3, \ldots, d, d-1)a_{d-2} \\ &\quad + c(m-2, m-3, \ldots, d, d-2)a_{d-1} = 0. \end{aligned} \tag{2.10}$$

Next, we look at the coefficient of $x^{(2^{m-1}-1)-2^{d-1}}$ in $T(x)S(x)$. As before, the number of 1's in the binary expansion of $(2^{m-1}-1) - 2^{d-1}$ is $m-2$. Hence at most one carry may occur. Again, using $r-1 < d-1$ there are only three ways of obtaining $(2^{m-1}-1)-2^{d-1}$ as a sum of two exponents without carry.

$$
\begin{aligned}
0\overbrace{1\ldots1}^{r-1}0\overbrace{11\ldots1}^{d-1} &= 0\overbrace{1\ldots11}^{r-1}000\ldots00+00\ldots000\overbrace{11\ldots11}^{d-1}\\
&= 0\overbrace{1\ldots11}^{r-1}01\overbrace{0\ldots00}^{d-2}+00\ldots0000\overbrace{1\ldots11}^{d-2}\\
&= 0\overbrace{1\ldots11}^{r-1}0\overbrace{00\ldots0}^{d-2}1+00\ldots000\overbrace{11\ldots1}^{d-2}0.
\end{aligned}
$$

If a carry occurs, then it has to be at position $d-1$.

$$0\overbrace{1\ldots1}^{r-1}0\overbrace{11\ldots1}^{d-1} = 0\overbrace{1\ldots1}^{r-2}0100\ldots01+00\ldots00\overbrace{111\ldots1}^{d-1}0.$$

It follows from (2.9) that

$$
\begin{aligned}
&c(m-2,m-3,\ldots,d)a_{d-1}+c(m-2,m-3,\ldots,d,d-2)a_{d-2}\\
&\quad+c(m-2,m-3,\ldots,d,0)a_{d-2}^2\\
&\quad+c(m-2,m-3,\ldots,d+1,d-1,0)a_{d-1}^2=0.
\end{aligned}
\tag{2.11}
$$

Now, we claim that

$$c(m-2,m-3,\ldots,d)a_{d-1}+c(m-2,m-3,\ldots,d,d-2)a_{d-2}=0. \tag{2.12}$$

In order to prove (2.12), we will show that

$$\begin{vmatrix} c(m-2,m-3,\ldots,d,d-2) & c(m-2,m-3,\ldots,d-1)\\ c(m-2,m-3,\ldots,d) & c(m-2,m-3,\ldots,d,d-2)\end{vmatrix}=0.$$

Once we prove this, it is clear that (2.12) will follow from (2.10). Hence, we need to show that

$$
\begin{aligned}
c(m-2,m-3,\ldots,d,d-2)^2 &= c(m-2,m-3,\ldots,d-1)\\
&\quad\times c(m-2,m-3,\ldots,d),
\end{aligned}
\tag{2.13}
$$

which, by (2.1) is the same as

$$
\begin{aligned}
c(m-1,m-2,\ldots,d+1,d-1) &= c(m-2,m-3,\ldots,d-1)\\
&\quad\times c(m-2,m-3,\ldots,d).
\end{aligned}
$$

Making appropriate shifts using (2.1), the above equation is further equivalent to

$$c(r,r-1,\ldots,2,0)=c(r-1,r-2,\ldots,1,0)c(r-1,\ldots,2,1).$$

Hence, by Lemma 2.2, we have proved (2.12).

Now the combination of (2.10)–(2.12) yields that

$$\begin{pmatrix} c(m-2,\dots,d,d-2)^2 & c(m-2,\dots,d,d-1)^2 \\ c(m-2,\dots,d+1,d-1,0) & c(m-2,\dots,d,0) \end{pmatrix} \begin{pmatrix} a_{d-1}^2 \\ a_{d-2}^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{2.14}$$

By Lemma 2.3 the determinant of the coefficient matrix in (2.14) is non-zero and thus, $a_{d-1} = a_{d-2} = 0$.

Claim. $a_{d-3} = \cdots = a_{r+1} = 0$: Now let $d-2 > k > r$ and suppose that $a_j = 0$ for all $d-1 \geqslant j > k$. We want to show that $a_k = 0$. To this end, consider the coefficient of $x^{(2^{m-1}-2^{d-1})+(2^k-1)}$ in $T(x)S(x)$. Since $k > r$ there is only one way of attaining this exponent when multiplying $T(x)$ and $S(x)$.

$$0\overbrace{1\dots1}^{r}0\dots0\overbrace{11\dots1}^{k} = 0\overbrace{1\dots11}^{r}000\dots00 + 00\dots000\overbrace{11\dots11}^{k}.$$

Hence by (2.9), $c(m-2, m-3, \dots, d-1)a_k = 0$. *As noted before*, $c(m-2, m-3, \dots, d-1) \neq 0$ *so we have* $a_k = 0$.

At this point we note that if $d = m-1$, i.e., $r = 1$, then the above two claims already show that $a_2 = a_3 = \cdots = a_{d-1} = 0$, and the theorem is proved in this case. So from now on, we assume that $m-1 > d > \frac{m}{2}+1$. Also we will assume that $m \geqslant 10$. The case where $5 \leqslant m \leqslant 8$ will be dealt with separately at the very end of the proof.

Claim. $a_3 = \cdots = a_r = 0$: For any integer t, $3 \leqslant t \leqslant r$, suppose that $a_j = 0$ for all $j > t$, we will prove that $a_t = 0$. Here we need the following result, whose proof will be given right after our proof of Theorem 2.1.

Result 1. *Assume that* $m \geqslant 10$ *and* $\lfloor \frac{m-3}{2} \rfloor \geqslant r \geqslant t \geqslant 3$. *There exist* $0 = i_1 < \cdots < i_r \leqslant m-t-3$ *such that*

(i) $c(i_1, i_2, \dots, i_r) \neq 0$, *and*
(ii) *the number of consecutive integers in the set* $\{i_1, i_2, \dots, i_r\}$ *is less than or equal to* $t-1$.

With Result 1, we will look at the coefficient of $x^{(2^{m-1}-2^{m-t-1})+\sum_{j=1}^{r} 2^{i_j}}$ in $T(x)S(x)$, i.e., the LHS of (2.9). Note that the exponent of this monomial has the m-bit binary representation

$$0\underbrace{11\dots1}_{t}0\underbrace{0\dots1\dots1\dots1}_{m-t-2},$$

where at the i_jth bit, there is a 1, for each $j = 1, 2, \dots, r$.

Since the number of consecutive integers in the set $\{i_1, i_2, \dots, i_r\}$ is less than or equal to $t-1$, there is only one way to get the term $x^{(2^{m-1}-2^{m-t-1})+\sum_{j=1}^{r} 2^{i_j}}$ when multiplying $T(x)$ with $S(x)$, namely

$$0\underbrace{11\dots1}_{t}0\underbrace{0\dots1\dots1\dots1}_{m-t-2} = 0\underbrace{00\dots0}_{t}0\underbrace{0\dots1\dots1\dots1}_{m-t-2} + 0\underbrace{11\dots1}_{t}0\underbrace{00\dots0}_{m-t-2}.$$

Therefore, the coefficient of $x^{(2^{m-1}-2^{m-t-1})+\sum_{j=1}^{r} 2^{i_j}}$ in $T(x)S(x)$ is $c(i_1, i_2, \dots, i_r)a_t^{2^{m-t-1}}$. It follows now from (2.9) that

$$c(i_1, i_2, \dots, i_r)a_t^{2^{m-t-1}} = 0.$$

Noting that $c(i_1, i_2, \dots, i_r) \neq 0$ we have $a_t = 0$.

Claim. $a_2 = 0$: Suppose that $a_2 \neq 0$: Let $Q(x) = \mathrm{Tr}(a_2x^3 + a_1x)$ and let $V = \mathbb{F}_{2^m}$. Note that since $\mathrm{Tr}(a_0) = 1$, the assumption that $\mathrm{Tr}(p(\lambda)) = 1$ for all $\lambda \in A\backslash\{0\}$ implies that $Q(\lambda) = 0$ for all $\lambda \in A$, where $|A| = 2^d$. The map $Q : V \to \mathbb{F}_2$ is a quadratic form with associated bilinear form

$$\begin{aligned} B(x, y) &= Q(x + y) - Q(x) - Q(y) \\ &= \mathrm{Tr}(a_2(xy^2 + yx^2)). \end{aligned}$$

We will show that the maximum dimension of a subspace of V on which Q vanishes is less than d. This will force $a_2 = 0$.

Let $\mathrm{Rad}\, V = \{x \in V \mid B(x, y) = 0,\ \forall y \in V\}$. Note that in even characteristic Q does not have to be zero on $\mathrm{Rad}\, V$. Therefore, we consider $V_0 = \{x \in \mathrm{Rad}\, V \mid Q(x) = 0\}$. We call Q *non-singular* if $V_0 = \{0\}$. By Witt's theorem, the maximum dimension of a totally singular subspace of a non-singular quadratic space (V, Q) is at most $\lfloor \frac{1}{2} \dim V \rfloor$. In our case we have $\mathrm{Rad}\, V = \{x \in V \mid x = a_2x^4\}$. In particular, $\dim V_0 \leqslant 2$. If Q is nonsingular then the maximum dimension of a totally singular subspace is at most $\lfloor \frac{m}{2} \rfloor$. If Q is singular then we consider the induced (nonsingular) quadratic form $\bar{Q} : V/V_0 \to \mathbb{F}_2$. The maximum dimension of a subspace U of V/V_0 on which $\bar{Q}$ vanishes is at most $\frac{1}{2}(m - \dim V_0)$. The maximum dimension of a subspace of V on which Q vanishes is less than or equal to $\dim(U \perp V_0) \leqslant \frac{1}{2}(m + \dim V_0) \leqslant \frac{m}{2} + 1$. It follows that in either case the maximum dimension of a subspace of V on which Q vanishes is less than d, hence a_2 has to be 0.

Finally, we deal with the case where $5 \leqslant m \leqslant 8$. When $m = 5$ or 6, there is no admissible d satisfying the restriction that $m - 1 > d > \frac{m}{2} + 1$. When $m = 7$ (resp. $m = 8$), the only admissible d is 5 (resp. 6). In both cases, $r = m - d = 2$, and by the first two claims, we have $a_3 = a_4 = \cdots = a_{d-1} = 0$. Now by the same argument using quadratic forms as above, we can further prove that $a_2 = 0$.

The proof of the theorem will be complete once we proof Result 1 above. □

We now give the promised proof of Result 1. This result can be thought as a generalization of the fact that a Moore determinant is nonzero, and it may be of independent interest. The proof of Result 1 we give here is elementary, but quite technical. The reader may want to skip the proof in a first reading of the paper.

We state Result 1 formally as

Theorem 2.4. *Let m, r, t be positive integers, and let $\mu_1, \dots, \mu_r \in \mathbb{F}_{2^m}$ be linearly independent over $\mathbb{F}_2$. If $m \geqslant 10$ and $\lfloor \frac{m-3}{2} \rfloor \geqslant r \geqslant t \geqslant 3$, then there exist $0 = i_1 < i_2 < \cdots < i_r \leqslant m - (t+3)$ such that*

(1) $$\det \begin{pmatrix} \mu_1^{2^{i_1}} & \mu_2^{2^{i_1}} & \cdots & \mu_r^{2^{i_1}} \\ \vdots & & \ddots & \vdots \\ \mu_1^{2^{i_r}} & \mu_2^{2^{i_r}} & \cdots & \mu_r^{2^{i_r}} \end{pmatrix} \neq 0, \text{ and}$$

(2) *the number of consecutive integers in the set $\{i_1, i_2, \dots, i_r\}$ is at most $t - 1$.*

We first fix some notation. Let V be the $\mathbb{F}_{2^m}$-span of $\{\mathbf{v}_0, \dots, \mathbf{v}_{m-1}\}$, where $\mathbf{v}_i = (\mu_1^{2^i}, \mu_2^{2^i}, \dots, \mu_r^{2^i})^\mathsf{T}$. As before, all indices of the vectors $\mathbf{v}_i$ are to be read modulo m. We have $\dim_{\mathbb{F}_{2^m}} V = r$ and $\{\mathbf{v}_i, \mathbf{v}_{i+1}, \dots, \mathbf{v}_{i+r-1}\}$ is a basis of V for all $i \geqslant 0$ [LN, Lemma 3.5]. By $\mathbf{v}_i^{2^j}$ we mean component-wise exponentiation of $\mathbf{v}_i$ by 2^j. Hence $\mathbf{v}_i^{2^j} = \mathbf{v}_{i+j}$. We will use binary vectors to denote subsets of $\{\mathbf{v}_0, \dots, \mathbf{v}_{m-1}\}$ as follows. Let $\mathbf{u} = (u_0, u_1, \dots, u_i) \in \mathbb{F}_2^{i+1}$ be a vector of length $i+1$. By $\Lambda(\mathbf{u})$ we will denote the $\mathbb{F}_{2^m}$-span of $\{\mathbf{v}_j \mid u_j = 1\}$. We also allow concatenation of binary vectors. If $\mathbf{u} = (u_0, u_1, \dots, u_i)$ and $\mathbf{u}' = (u_0', u_1', \dots, u_j')$ then

$$\mathbf{u} * \mathbf{u}' = (u_0, u_1, \dots, u_i, u_0', u_1', \dots, u_j').$$

If we concatenate several copies, say $i \geqslant 1$, of the same vector $\mathbf{u}$ then we denote the resulting vector by $\mathbf{u}^{*i}$. Sometimes it may happen that we have a concatenated vector $\mathbf{u}' * \mathbf{u}^{*i}$ with $i = 0$. In this case we assume that no copy of $\mathbf{u}$ had been appended to $\mathbf{u}'$, that is, $\mathbf{u}' * \mathbf{u}^{*0} = \mathbf{u}'$.

Now Theorem 2.4 can be reformulated as follows.

Theorem (2.4′). *For $r \leqslant \lfloor \frac{m-3}{2} \rfloor$ there exists a binary vector $\mathbf{w}$ of length at most $m - (t+2)$ such that $\Lambda(\mathbf{w}) = V$ and the number of consecutive* 1's *in* $\mathbf{w}$ *is at most $t - 1$.*

First of all, note that it suffices to prove the theorem in the case where r is equal to $\lfloor \frac{m-3}{2} \rfloor$. Indeed, if we have found a vector $\mathbf{w}$ for $\lfloor \frac{m-3}{2} \rfloor = R$ then the same vector $\mathbf{w}$ will satisfy our requirements for smaller r. The reason is as follows. Suppose that $r < R$. We can extend the set $\{\mu_1, \mu_2, \dots, \mu_r\}$ to a set of R elements $\{\mu_1, \mu_2, \dots, \mu_r, \dots, \mu_R\}$ in $\mathbb{F}_{2^m}$ that are linearly independent over $\mathbb{F}_2$. By assumption, we can find $0 = i_1 < i_2 < \cdots < i_R < m - (t+3)$ such that $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \dots, \mathbf{v}_{i_R}$ form a basis of $\mathbb{F}_{2^m}^R$, where $\mathbf{v}_{i_j} = (\mu_1^{2^{i_j}}, \mu_2^{2^{i_j}}, \dots, \mu_R^{2^{i_j}})^\mathsf{T}$. Let $\mathbf{v}_{i_j}'$ be the projection of $\mathbf{v}_{i_j}$ onto the first r coordinates, that is,

${\mathbf{v}_{i_j}}' = (\mu_1^{2^{i_j}}, \mu_2^{2^{i_j}}, \ldots, \mu_r^{2^{i_j}})^{\mathsf{T}}$ for $1 \leqslant j \leqslant R$. Then $\{{\mathbf{v}_{i_1}}', {\mathbf{v}_{i_2}}', \ldots, {\mathbf{v}_{i_R}}'\}$ spans $\mathbb{F}_{2^m}^r$. Hence this set contains r vectors ${\mathbf{v}_{i_{j_1}}}', {\mathbf{v}_{i_{j_2}}}', \ldots, {\mathbf{v}_{i_{j_r}}}'$ that are linearly independent over $\mathbb{F}_{2^m}$. By assumption, $0 \leqslant i_{j_1} < i_{j_2} < \cdots < i_{j_r} < m - (t+3)$ and the number of consecutive integers in $\{i_{j_1}, i_{j_2}, \ldots, i_{j_r}\}$ is at most $t-1$. If $i_{j_1} \neq 0$ then it is clear that we can use $\{0, i_{j_2} - i_{j_1}, \ldots, i_{j_r} - i_{j_1}\}$ instead. From now on, we will assume that $r = \lfloor \frac{m-3}{2} \rfloor$.

We write $r = kt + a$, where $0 \leqslant a \leqslant t-1$. Since $r \geqslant t$, we have $k \geqslant 1$. Let $\mathbf{a} = (1, \ldots, 1) \in \mathbb{F}_2^a$, $\mathbf{u} = (0, 1, \ldots, 1) \in \mathbb{F}_2^t$, $\bar{\mathbf{u}} = (1, 0, \ldots, 0) \in \mathbb{F}_2^t$, and $\mathbf{0} = (0, \ldots, 0) \in \mathbb{F}_2^t$. Then $\dim \Lambda(\mathbf{a} * \mathbf{u}^{*k}) = r - k$ since $\mathbf{a} * \mathbf{u}^{*k}$ is a vector of length r with exactly k zeros. We will append copies of $\mathbf{u}$ or $\bar{\mathbf{u}}$ to $\mathbf{a} * \mathbf{u}^{*k}$ to describe a set of vectors $\mathbf{v}_i$ that generate V. Note that by appending $\mathbf{u}$ to $\mathbf{a} * \mathbf{u}^{*(k+b)}$, $0 \leqslant b < k$, we have

$$\dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+1)}) \geqslant \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}).$$

Lemma 2.5. (1) *If* $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+1)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)})$, *then* $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+i)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)})$ *for any positive integer* i.

(2) *If* $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+1)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*k}) + \mathbb{F}_{2^m}\mathbf{v}_{r+\ell}$ *where* $1 \leqslant \ell \leqslant t-1$, *then* $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+1)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) + \mathbb{F}_{2^m}\mathbf{v}_{r+bt+\ell}$ *for any positive integer* b.

(3) *Let* $\mathbf{y}$ *be a binary vector of length* ℓ *and* $\mathbf{1}_t = (1, 1, \ldots, 1) \in \mathbb{F}_2^t$. *Suppose* $\Lambda(\mathbf{y})$ *is a proper subspace in* V *and there exists a vector* $\mathbf{z} \in \mathbb{F}_2^t$ *such that* $\{\mathbf{v}_i \mid (\mathbf{z} * \mathbf{y})_i = 1\} \subseteq \{\mathbf{v}_i \mid (\mathbf{y} * \mathbf{1}_t)_i = 1\}$. *Then* $\Lambda(\mathbf{y}) \subsetneq \Lambda(\mathbf{y} * \mathbf{1}_t)$.

Proof. (1) Observe that since $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+1)})$, we have dependence relations $\mathbf{v}_{r+bt+j} = \sum_{i=0}^{r+bt-1} c_i \mathbf{v}_i$ for $1 \leqslant j \leqslant t-1$ where $c_i = 0$ if i is of the form $a + st$. This gives dependence relations $\mathbf{v}_{r+bt+j}^{2^t} = \mathbf{v}_{r+(b+1)t+j} = \sum_{i=0}^{r+bt-1} c_i^{2^t} \mathbf{v}_{i+t}$, hence $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+2)}) \subseteq \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+1)})$.

(2) Observe that our assumption implies that for $1 \leqslant j \leqslant t-1$ with $j \neq \ell$, we have dependence relations $\mathbf{v}_{r+j} = c_{r+\ell}\mathbf{v}_{r+\ell} + \sum_{i=0}^{r-1} c_i \mathbf{v}_i$ where $c_i = 0$ if i is of the form $a + st$. As before, we then obtain the relation $\mathbf{v}_{r+bt+j} = c_{r+\ell}^{2^{bt}} \mathbf{v}_{r+bt+\ell} + \sum_{i=0}^{r-1} c_i^{2^{bt}} \mathbf{v}_{i+bt}$ where $c_i = 0$ if i is of the form $a + st$. Clearly, $\sum_{i=0}^{r-1} c_i^{2^{bt}} \mathbf{v}_{i+bt} \in \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)})$ as $c_i = 0$ if i is of the form $a + st$. We thus obtain (2).

(3) Suppose $\Lambda(\mathbf{y}) = \Lambda(\mathbf{y} * \mathbf{1}_t)$. Then the t consecutive vectors $\mathbf{v}_\ell, \mathbf{v}_{\ell+1}, \ldots, \mathbf{v}_{\ell+(t-1)}$ are all in $\Lambda(\mathbf{y})$. On the other hand,

$$\{x^{2^t} \mid x \in \Lambda(\mathbf{y})\} \subseteq \Lambda(\mathbf{z} * \mathbf{y}) \subseteq \Lambda(\mathbf{y} * \mathbf{1}_t) = \Lambda(\mathbf{y}).$$

It follows that for any $x \in \Lambda(\mathbf{y})$, we have $x^{2^t} \in \Lambda(\mathbf{y})$. In particular, $\mathbf{v}_{\ell+it}, \mathbf{v}_{\ell+1+it}, \ldots, \mathbf{v}_{\ell+(t-1)+it}$ are all in $\Lambda(\mathbf{y})$ for every positive integer i. We thus have $\mathbf{v}_0, \ldots, \mathbf{v}_{r-1} \in \Lambda(\mathbf{y})$. This contradicts our assumption that $V \neq \Lambda(\mathbf{y})$. □

We are now ready to prove Theorem 2.4′. Recall that $k \geqslant 1$ and we may assume $r = \lfloor \frac{m-3}{2} \rfloor$.

Proof. We will consider two cases.

Case $\Lambda(\mathbf{a} * \mathbf{u}^{*k} * \mathbf{u}^{*i}) \neq V$ *for all* $i > 0$: In this case the dimensions of the subspaces in the nested sequence

$$\Lambda(\mathbf{a} * \mathbf{u}^{*k}) \subseteq \Lambda(\mathbf{a} * \mathbf{u}^{*(k+1)}) \subseteq \cdots \Lambda(\mathbf{a} * \mathbf{u}^{*(k+i)}) \subseteq \cdots$$

stop growing eventually. Let b be the largest integer such that $\dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) > \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b-1)})$. Since $r > \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) \geqslant r - k + b$, we have $0 \leqslant b < k$. By repeated application of Lemma 2.5, part 3, we see that

$$V = \begin{cases} \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+1)} * \mathbf{1}_t^{*(k-b-1)}) & \text{if } \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) > r - k + b, \\ \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)} * \mathbf{1}_t^{*(k-b)}) & \text{if } \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = r - k + b. \end{cases}$$

Since $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b+i)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)})$ for all positive integer i,

$$V = \begin{cases} \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)} * \mathbf{0} * \bar{\mathbf{u}}^{*(k-b-1)}) & \text{if } \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) > r - k + b, \\ \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)} * \bar{\mathbf{u}}^{*(k-b)}) & \text{if } \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = r - k + b. \end{cases}$$

Subcase $\dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) > r - k + b$: We define $\mathbf{w}$ to be the vector obtained by dropping the last $(t-1)$ zeros from the last copy of $\bar{\mathbf{u}}$ in the vector $\mathbf{a} * \mathbf{u}^{*(k+b)} * \mathbf{0} * \bar{\mathbf{u}}^{*(k-b-1)}$. Note that the length of $\mathbf{w}$ is at most $m - (t+2)$, $\Lambda(\mathbf{w}) = V$, and the number of consecutive 1's in $\mathbf{w}$ is at most $t-1$.

Subcase $\dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = r - k + b$ *and* $b > 0$: Appending the $(k+b)$th copy of $\mathbf{u}$ increased the dimension of $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b-1)})$ by exactly one, i.e., $\dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = 1 + \dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b-1)})$. Thus, $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b-1)}) + \mathbb{F}_{2^m}\mathbf{v}_{r+(b-1)t+i}$ for some $1 \leqslant i \leqslant t-1$. Let $\mathbf{u}_i \in \mathbb{F}_2^t$ be the vector with $(i+1)$th entry being one and all other entries 0. Then it is clear that $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b-1)} * \mathbf{u}_i)$. Recall that $V = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)} * \bar{\mathbf{u}}^{*(k-b)})$. Therefore, we deduce

$$V = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b-1)} * \mathbf{u}_i * \bar{\mathbf{u}}^{*(k-b)}).$$

To find the required vector $\mathbf{w}$, we simply drop the last $(t-1)$ zeros from the last copy of $\bar{\mathbf{u}}$ in $\mathbf{a} * \mathbf{u}^{*(k+b-1)} * \mathbf{u}_i * \bar{\mathbf{u}}^{*(k-b)}$. Clearly, the resulting vector is of length $r + (k-1)t + 1$ which is at most $m - (t+2)$ and satisfies what we require.

Subcase $\dim \Lambda(\mathbf{a} * \mathbf{u}^{*(k+b)}) = r - k + b$ *and* $b = 0$: In this case we have $\Lambda(\mathbf{a} * \mathbf{u}^{*k}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(k+i)})$ for all $i > 0$. It follows that for any $0 \leqslant j \leqslant r-1$ and for any i, $\mathbf{v}_{j+it} \in \Lambda(\mathbf{a} * \mathbf{u}^{*k})$ if and only if $j \not\equiv a \pmod{t}$. As $\mathbf{v}_{a+m} \notin \Lambda(\mathbf{a} * \mathbf{u}^{*k})$, it follows that $a + m \equiv a \pmod{t}$. Hence, we have $t \mid m$. Since we may assume $r = \lfloor \frac{m-3}{2} \rfloor$ it follows that $t = 2a+3$, $t = 2a+4$, or $t = a+2$. In each case, $0 \leqslant a \leqslant t-2$.

First we will assume $t - 2 \geqslant a \geqslant 1$. It follows that $\mathbf{v}_{t-1} \in \Lambda(\mathbf{a} * \mathbf{u}^{*k})$ and thus $\mathbf{v}_{m-1} \in \Lambda(\mathbf{a} * \mathbf{u}^{*k})$. Recall that any r consecutive vectors in $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{m-1}\}$ are linearly independent. In particular, $\{\mathbf{v}_{m-1}, \mathbf{v}_0, \ldots, \mathbf{v}_{r-2}\}$ are linearly independent. Let $\mathbf{z} = (0, \ldots, 0, 1) \in \mathbb{F}_2^{m-r-kt}$. It is clear that $\Lambda(\mathbf{a} * \mathbf{u}^{k-1} * (0, \underbrace{1, 1, \ldots, 1}_{t-2}, 0) * \mathbf{0}^{*k} * \mathbf{z})$ is an

$(r-k)$ dimensional subspace in $\Lambda(\mathbf{a}*\mathbf{u}^{*k})$. As dim $\Lambda(\mathbf{a}*\mathbf{u}^{*k}) = r-k$, it follows that

$$\Lambda(\mathbf{a}*\mathbf{u}^{*(k-1)}*(0,\underbrace{1,1,\dots,1}_{t-2},0)*\mathbf{0}^{*k}*\mathbf{z}) = \Lambda(\mathbf{a}*\mathbf{u}^{*k}).$$

Consequently, by Lemma 2.5, part 3, we conclude that

$$\Lambda(\mathbf{a}*\mathbf{u}^{*(k-1)}*(0,\underbrace{1,1,\dots,1}_{t-2},0)*\bar{\mathbf{u}}^{*k}*\mathbf{z}) = \Lambda(\mathbf{a}*\mathbf{u}^{*k}*\bar{\mathbf{u}}^{*k}*\mathbf{z}) = V.$$

The vector $\mathbf{a}*\mathbf{u}^{*(k-1)}*(0,\overbrace{1,1,\dots,1}^{t-2},0)*\bar{\mathbf{u}}^{*k}*\mathbf{z}$ does not have more than $t-1$ consecutive 1's since $a \leqslant t-2$. Shifting this vector by one to the right it follows that

$$V = \Lambda((1)*\mathbf{a}*\mathbf{u}^{*k-1}*(0,\underbrace{1,1,\dots,1}_{t-2},0)*\bar{\mathbf{u}}^{*k-1}*(1)).$$

The length of the vector $\mathbf{w} = (1)*\mathbf{a}*\mathbf{u}^{*k-1}*(0,\overbrace{1,1,\dots,1}^{t-2},0)*\bar{\mathbf{u}}^{*k-1}*(1)$ is $r+(k-1)t+2$, which is at most $m-(t+2)-(a-1)$. We are done as $a \geqslant 1$.

It remains to deal with the case where $a=0$. Recall that $t \geqslant 3$ and $t=2a+3$, $t=2a+4$, or $t=a+2$. This forces $t=3$ or 4. Consequently, $m=6k+3$ when $t=3$, or $t=4$ and $m=8k+4$.

Since $\mathbf{v}_{r+1} \in \Lambda(\mathbf{u}^{*k})$, there exist c_is in $\mathbb{F}_{2^m}$ such that

$$\mathbf{v}_{r+1} = \sum_{j=1}^{t-1}\sum_{i=0}^{k-1} c_{j+ti}\mathbf{v}_{j+ti}.$$

It follows that

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

Since $t>2$ we have $\mathbf{v}_{r+2} \in \Lambda(\mathbf{u}^{*k})$. Note that also $\sum_{j=1}^{t-2}\sum_{i=0}^{k-1} c_{j+ti}^2\mathbf{v}_{j+1+ti} \in \Lambda(\mathbf{u}^{*k})$ and thus, $\sum_{i=0}^{k-1} c_{t-1+ti}^2\mathbf{v}_{t(i+1)} \in \Lambda(\mathbf{u}^{*k})$. However, we also have $\sum_{i=0}^{k-1} c_{t-1+ti}^2\mathbf{v}_{t(i+1)} \in \Lambda(\mathbf{0}*\bar{\mathbf{u}}^{*k})$. Now observe that V is spanned by the r linearly independent vectors $\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_{kt}$, $\Lambda(\mathbf{0}*\bar{\mathbf{u}}^{*k})$ is spanned by the k vectors $\mathbf{v}_t,\mathbf{v}_{2t},\dots,\mathbf{v}_{kt}$, and $\Lambda(\mathbf{u}^{*k})$ is spanned by the $r-k$ vectors in $\{\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_{kt}\}\setminus\{\mathbf{v}_t,\mathbf{v}_{2t},\dots,\mathbf{v}_{kt}\}$. Therefore, $\sum_{i=0}^{k-1} c_{t-1+ti}^2\mathbf{v}_{t(i+1)} \in \Lambda(\mathbf{u}^{*k}) \cap \Lambda(\mathbf{0}*\bar{\mathbf{u}}^{*k})$ has to be the zero vector in $\mathbb{F}_{2^m}^r$. This forces $c_{t-1} = c_{(t-1)+t} = \cdots = c_{(t-1)+(k-1)t} = 0$.

If $t=4$, then by applying a similar argument on $\mathbf{v}_{r+3}$, we see that $c_{t-2} = c_{(t-2)+t} = \cdots = c_{(t-2)+(k-1)t} = 0$. Thus, in both cases, we obtain

$$\mathbf{v}_{r+1} = \sum_{i=0}^{k-1} c_{1+ti}\mathbf{v}_{1+ti}.$$

Let h be the largest integer such that $c_{1+th} \neq 0$. If $h \neq k-1$, then $\mathbf{v}_{r+1+(k-h-1)t} = \sum_{i=0}^{k-1} c_{1+ti}{}'\mathbf{v}_{1+ti}$ where $c_{1+t(k-1)}{}' = c_{1+th}^{2^{t(k-h-1)}} \neq 0$. Hence, it follows that

$$V = \begin{cases} \Lambda(\mathbf{u}^{*(k-1)} * (0,0,1) * \bar{\mathbf{u}}^{*(k-h-1)} * (1,1,0) * \bar{\mathbf{u}}^{*h}) & \text{if } t=3, \\ \Lambda(\mathbf{u}^{*(k-1)} * (0,0,1,1) * \bar{\mathbf{u}}^{*(k-h-1)} * (1,1,0,0) * \bar{\mathbf{u}}^{*h}) & \text{if } t=4. \end{cases}$$

If $h = k-1$, i.e., $c_{1+t(k-1)} \neq 0$, then we see that

$$V = \begin{cases} \Lambda(\mathbf{u}^{*(k-1)} * (0,1,0) * (1,0,1) * \bar{\mathbf{u}}^{*(k-1)}) & \text{if } t=3, \\ \Lambda(\mathbf{u}^{*(k-1)} * (0,1,0,1) * (1,0,1,0) * \bar{\mathbf{u}}^{*(k-1)}) & \text{if } t=4. \end{cases}$$

When $k \geqslant 2$, after dropping the zero in the first copy of $\mathbf{u}$ and the last zero in the last copy of $\bar{\mathbf{u}}$, we obtain a vector we require in each case. When $k=1$, we deduce that $t=4$ as $m=9$ is excluded (cf. Example 2.7), and clearly the required vector is then $(1,0,1,1,0,1)$.

Case $\Lambda(\mathbf{a} * \mathbf{u}^{*k} * \mathbf{u}^{*b}) = V$ *for some* $b \leqslant k$: We consider two subcases depending on the increase in dimension in the nested sequence $\Lambda(\mathbf{a} * \mathbf{u}^{*k}) \subsetneq \Lambda(\mathbf{a} * \mathbf{u}^{*(k+1)}) \subsetneq \cdots \subsetneq V$.

Subcase $b<k$: The dimension of one of the subspaces in the sequence increases by more than one compared to that of its predecessor, and $1 \leqslant b \leqslant k-1$. Thus, $\mathbf{a} * \mathbf{u}^{*(k+b)}$ is a vector of 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 and we are done.

Subcase $b=k$: The dimension of each vector space in the nested sequence $\Lambda(\mathbf{a} * \mathbf{u}^{*k}) \subsetneq \cdots \subsetneq \Lambda(\mathbf{a} * \mathbf{u}^{*(2k)}) = V$ increases by exactly one compared to that of its predecessor. Hence there is a smallest index j, $1 \leqslant j \leqslant t-1$, such that $\mathbf{v}_{a+kt+j} \notin \Lambda(\mathbf{a} * \mathbf{u}^{*k})$ and $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+1)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*k}) + \mathbb{F}_{2^m}\mathbf{v}_{a+kt+j}$. It follows from Lemma 2.5, part 2, that $V = \Lambda(\mathbf{a} * \mathbf{u}^{*2k}) = \Lambda(\mathbf{a} * \mathbf{u}^{*(2k-1)}) + \mathbb{F}_{2^m}\mathbf{v}_{a+(2k-1)t+j}$. Therefore, we conclude

$$V = \Lambda(\mathbf{a} * \mathbf{u}^{*(2k-1)} * (\underbrace{0,\ldots,0}_{j},1)).$$

Note that the length of the vector $\mathbf{a} * \mathbf{u}^{*(2k-1)} * (\overbrace{0,\ldots,0}^{j},1)$ is $r+(k-1)t+(j+1)$, which is at most $m-(t+2)-(a-j)$. By construction, it does not have more than $t-1$ consecutive 1's. Therefore, we are done if $j \leqslant a$.

We still have to deal with the case where $j>a$. In this case,

$$\Lambda(\mathbf{a} * \mathbf{u}^{*k}) = \Lambda(\mathbf{a} * \mathbf{u}^{*k} * (0,\underbrace{1,\ldots,1}_{j-1}))$$

since j was the smallest index such that $\Lambda(\mathbf{a} * \mathbf{u}^{*(k+1)}) = \Lambda(\mathbf{a} * \mathbf{u}^{*k}) + \mathbb{F}_{2^m}\mathbf{v}_{r+j}$. However, it is clear that the set $\{\mathbf{v}_j,\ldots,\mathbf{v}_{r+(j-1)}\} \backslash \{\mathbf{v}_{a+t},\ldots,\mathbf{v}_{a+kt}\}$ is linearly independent. Therefore,

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

as both spaces have the same dimension. It follows that

$$V = \Lambda(\mathbf{a} * \mathbf{u}^{*(2k-1)} * (0, \underbrace{1, \ldots, 1}_{j})) = \Lambda((\underbrace{0, \ldots, 0}_{j}, \underbrace{1, \ldots, 1}_{t+a-j}) * \mathbf{u}^{*(2k-2)} * (0, \underbrace{1, \ldots, 1}_{j})).$$

Deleting leading and tailing zeros, we obtain a vector that has length at most $m-(t+2)-a$. This completes our proof. $\square$

Combining Theorem 2.1 with known constructions, we have

Theorem 2.6. *Let $m \geqslant 5$ but $m \neq 9$. Then 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 1.2 is $\lfloor \frac{m}{2} \rfloor + 1$.*

Proof. Let $p(x) = \sum_{i=0}^{d-1} a_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$. Assume that $\mathrm{Tr}(p(\lambda)) = 1$ for all $\lambda \in A \backslash \{0\}$, where A is an additive subgroup of $\mathbb{F}_{2^d}$. If $m \geqslant 5$ but $m \neq 9$, and if $m > d > \frac{m}{2} + 1$, then by Theorem 2.1, $p(x)$ is a linear polynomial, hence the maximal arc generated by the $\{p, 1\}$-map is a Denniston maximal arc. This shows that when $m \geqslant 5$ but $m \neq 9$, the largest d of a non-Denniston maximal arc of degree d in $\mathrm{PG}(2, 2^m)$ generated by a $\{p, 1\}$-map via Theorem 1.2 is $\leqslant \lfloor \frac{m}{2} \rfloor + 1$.

On the other hand, there are always $\{p, 1\}$-maps generating non-Denniston maximal arcs of degree $2^{\lfloor \frac{m}{2} \rfloor + 1}$ if $m \geqslant 5$ (see [FLX,HM,M]). The conclusion of the theorem now follows. $\square$

We remark that when $m = 9$, there is an example of $\{p, 1\}$-maps that generates a non-Denniston maximal arc of degree 2^6. This example appears in [HM].

Example 2.7 (Hamilton and Mathon [HM]). Let g be a primitive element in $\mathbb{F}_{2^9}$. Note that $73(2^3 - 1) = 2^9 - 1$, so $b = g^{73}$ is a primitive element in $\mathbb{F}_{2^3}$. Let $\mu_i = b^i$ for $i = 0, 1, 2$ and $A = \{x \in \mathbb{F}_{2^9} \mid \mathrm{Tr}(\mu_i x) = 0, \ \forall i = 0, 1, 2\}$. That is, $A = \{x \in \mathbb{F}_{2^9} \mid \mathrm{Tr}_{2^9/2^3}(x) = 0\}$ since μ_1, μ_2, μ_3 are linearly independent over $\mathbb{F}_2$. Let $p(x) = x^7 + 1$. Direct computations show that $\mathrm{Tr}(p(\lambda)) = 1$ for all $\lambda \in A \backslash \{0\}$. Therefore, the set of points on the conics in $\{F_{p(\lambda),1,\lambda} \mid \lambda \in A \backslash \{0\}\}$ together with the common nucleus F_0 forms a non-Denniston maximal arc of degree 2^6.

3. Upper bound for the degree of non-Denniston maximal arcs in $\mathrm{PG}(2, 2^m)$ generated by $\{p, q\}$-maps

In this section we try to extend the result in previous section to $\{p, q\}$-maps, where q is not necessarily 1.

Theorem 3.1. *Let A be an additive subgroup of size 2^d in $\mathbb{F}_{2^m}$, and let $p(x) = \sum_{i=0}^{d-1} a_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$, $q(x) = \sum_{i=0}^{d-1} b_i x^{2^i - 1} \in \mathbb{F}_{2^m}[x]$. Assume that $m \geqslant 7$ but $m \neq 9$, and*

$m > d > \frac{m}{2} + 2$. If $\mathrm{Tr}(p(\lambda)q(\lambda)) = 1$ for all $\lambda \in A \backslash \{0\}$, then $a_2 = a_3 = \cdots = a_{d-1} = 0$ and $b_2 = b_3 = \cdots = b_{d-1} = 0$. That is, $p(x)$ and $q(x)$ are both linear and the maximal arc obtained from the $\{p, q\}$-map via Theorem 1.2 is a Denniston maximal arc.

Proof. Let $r = m - d$. As in the proof of Theorem 2.1, we assume that the defining equation of A is

$$\prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) = 1,$$

where $\mu_i \in \mathbb{F}_{2^m}^*$ are linearly independent over $\mathbb{F}_2$. Also as argued in the proof of Theorem 2.1, we may assume that $\mathrm{Tr}(a_0 b_0) = 1$. Then

$$\mathrm{Tr}(p(x)q(x) + a_0 b_0) \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) \equiv 0 \ (\mathrm{mod}\, x^{2^m} - x). \tag{3.1}$$

For convenience, set $T(x) = \mathrm{Tr}(p(x)q(x) + a_0 b_0) \ (\mathrm{mod}\, x^{2^m} - x)$ and $S(x) = \prod_{i=1}^{r} (1 + \mathrm{Tr}(\mu_i x)) \ (\mathrm{mod}\, x^{2^m} - x)$. Also as before denote the coefficient of $x^{2^{i_1} + 2^{i_2} + \cdots + 2^{i_s}}$ in $S(x)$ by $c(i_1, i_2, \ldots, i_s)$, where $1 \leqslant s \leqslant r$ and $m - 1 \geqslant i_1 > i_2 > \cdots > i_s \geqslant 0$. The remarks about $c(i_1, i_2, \ldots, i_s)$ in the course of proving Theorem 2.1 are of course valid here.

In the proof of Theorem 2.1 we use the fact that the exponent of any term in the expansion of $\mathrm{Tr}(p(x))$ is a cyclic shift of $(2^i - 1)$ for some i. This is no longer true for $T(x) = \mathrm{Tr}(p(x)q(x) + a_0 b_0)$ if $q(x)$ is not a constant. Instead, the exponent of any term in the expansion of $T(x)$ is $2^s((2^j - 1) + (2^k - 1))$, where $m - 1 \geqslant s \geqslant 0$, $d - 1 \geqslant j \geqslant k \geqslant 0$. If $k \geqslant 1$ then the binary representation of $2^s((2^j - 1) + (2^k - 1))$ is a cyclic shift of

$$0 \ldots 01 \overbrace{0 \ldots 0}^{j-k} \ \overbrace{1 \ldots 1}^{k-1} 0.$$

The number of 1's in this representation is k. If $k = 0$ then it is a cyclic shift of

$$0 \ldots 0 \overbrace{1 \ldots 1}^{j}.$$

The number of 1's is j. This shows that the maximum number of 1's in the binary representations of such exponents is $d - 1$. Note that if $k = 0$ or $k = j$ then such an exponent is $2^s(2^i - 1)$ for some s and i, hence its binary representation is a shift of i consecutive 1's.

We want to use techniques similar to those in the proofs of Theorem 2.1. That is, we will be looking at the coefficients of various terms in $T(x)S(x)$. We will be particularly interested in terms x^e in $T(x)$, where the exponent e has $(d - 1)$ or $(d - 2)$ ones in its binary representation. If e has $(d - 1)$ ones, it must be a shift of $2^d - 2$ or $2^{d-1} - 1$. The coefficients of $x^{2^d - 2}$ and $x^{2^{d-1} - 1}$ in $T(x)$ are $a_{d-1} b_{d-1}$ and $a_0 b_{d-1} + a_{d-1} b_0$, respectively. If e has $(d - 2)$ ones, then it must be a shift of one of

$2^{d-2}-1$, $2^{d-1}-2$, $2^{d-1}+2^{d-2}-2$. The coefficients of $x^{2^{d-2}-1}$, $x^{2^{d-1}-2}$, $x^{2^{d-1}+2^{d-2}-2}$ are $a_0b_{d-2}+a_{d-2}b_0$, $a_{d-2}b_{d-2}$ and $a_{d-1}b_{d-2}+a_{d-2}b_{d-1}$, respectively.

Claim. $a_{d-2}b_{d-1}+a_{d-1}b_{d-2}=0$: Consider the coefficient of $x^{2^m-2^{d-2}-2}$ in $T(x)S(x)$. The binary representation of the exponent is

$$\overbrace{1\dots1}^{r}10\overbrace{1\dots1}^{d-3}0,$$

which has $(m-2)$ ones. The maximum number of 1's in the exponent of any summand in $S(x)$ is r and the maximum number of 1's in the exponent of any summand in $T(x)$ is $d-1$. When adding two exponents (written in their binary representations), any carry that may occur reduces the number of 1's in the sum. Since we are interested in an exponent whose number of 1's is $(m-2)$, it can only be obtained as a sum of two exponents (one is the exponent of a summand in $T(x)$, the other in $S(x)$) with at most one carry.

Suppose the exponent $2^m-2^{d-2}-2$ is obtained without carry. Using the assumption that $d>\frac{m}{2}+2$, we have $d-3>r+1$. So there is only one possibility.

$$\overbrace{1\dots1}^{r}\ 10\overbrace{1\dots1}^{d-3}0=\overbrace{1\dots1}^{r}000\dots00+0\dots010\overbrace{1\dots1}^{d-3}0.$$

Hence $0\dots010\overbrace{1\dots1}^{d-3}0$ must come from the exponent of $x^{2^{d-1}+2^{d-2}-2}$ in $T(x)$, whose coefficient is $a_{d-2}b_{d-1}+a_{d-1}b_{d-2}$, and $\overbrace{1\dots1}^{r}000\dots00$ must come from $x^{2^{m-1}+\cdots+2^d}$ in $S(x)$, whose coefficient is $c(m-1,m-2,\dots,d)$.

Now suppose that the exponent $2^m-2^{d-2}-2$ is obtained with a carry, which means that the contribution from $T(x)$ is a shift of $2^{d-1}-1$. Then it has to be exactly one carry which has to occur at position $d-2$ since $d-3>r+1$. There is no way of realizing this with any shift of $2^{d-1}-1$.

Therefore the coefficient of $x^{2^m-2^{d-2}-2}$ in $T(x)S(x)$ is $(a_{d-2}b_{d-1}+a_{d-1}b_{d-2})c(m-1,m-2,\dots,d)$, and by (3.1), we have

$$(a_{d-2}b_{d-1}+a_{d-1}b_{d-2})c(m-1,m-2,\dots,d)=0.$$

Noting that $c(m-1,m-2,\dots,d)$ is a Moore determinant, which is non-zero, we conclude that $a_{d-2}b_{d-1}+a_{d-1}b_{d-2}=0$.

After proving the above claim, observe that now the exponent of any term in $T(x)$ whose number of 1's is $d-1$ or $d-2$ has to be a cyclic shift of $2^{d-1}-1$ or $2^{d-2}-1$. Thus, we are ready to proceed as in the proof of Theorem 2.1.

Claim. $a_0^2b_{d-2}^2 + a_{d-2}b_{d-2} + b_0^2a_{d-2}^2 = a_0^2b_{d-1}^2 + a_{d-1}b_{d-1} + b_0^2a_{d-1}^2 = 0$: The coefficient of $x^{2^{d-1}-2}$ in $T(x)$ is

$$a_0^2b_{d-2}^2 + a_{d-2}b_{d-2} + b_0^2a_{d-2}^2 \tag{3.2}$$

and the coefficient of $x^{2(2^{d-1}-1)}$ is

$$a_0^2b_{d-1}^2 + a_{d-1}b_{d-1} + b_0^2a_{d-1}^2. \tag{3.3}$$

Considering the coefficient of $x^{2^m-2^{d-1}-2}$ and that of $x^{2^m-2^d-2}$ in $T(x)S(x)$, we obtain equations similar to (2.10) and (2.11) with the expressions in (3.2) and (3.3) taking the place of a_{d-2} and a_{d-1} in (2.10) and (2.11), respectively. Thus, using the same reasoning as in the proof of Theorem 2.1, our claim follows.

Claim. $a_{d-1} = a_{d-2} = b_{d-1} = b_{d-2} = 0$: Since $\mathrm{Tr}(a_0b_0) = 1$, the binary quadratic form $a_0^2x^2 + xy + b_0^2y^2$ over $\mathbb{F}_{2^m}$ has only trivial zeros. Therefore, from

$$a_0^2b_{d-2}^2 + a_{d-2}b_{d-2} + b_0^2a_{d-2}^2 = 0,$$

$$a_0^2b_{d-1}^2 + a_{d-1}b_{d-1} + b_0^2a_{d-1}^2 = 0,$$

we obtain $a_{d-2} = b_{d-2} = 0$ and $a_{d-1} = b_{d-1} = 0$.

Claim. $a_{d-3} = \cdots = a_{r+1} = b_{d-3} = \cdots = b_{r+1} = 0$: Let $d-2>k>r$ and suppose that $a_j = b_j = 0$ for $j>k$. Consider the coefficient of $x^{2^m-2^d+2^{k+1}-2}$ in $T(x)S(x)$. The exponent of this monomial has binary representation

$$\overbrace{1\ldots1}^{r}\overbrace{0\ldots0}^{d-k-1}\overbrace{1\ldots1}^{k}0,$$

which has $(m-1)$ ones. This exponent can only be obtained as a sum of two exponents (one is the exponent of a summand in $T(x)$, the other in $S(x)$) without carry. As we discussed previously, there are three ways such that the number of 1's in the binary representation of 2^j-1+2^k-1 is $k>0$. These are 2^k-1+2^0-1 (the coefficient of $x^{2^k-1+2^0-1}$ in $T(x)$ is $a_kb_0 + a_0b_k$), 2^k-1+2^k-1 (the coefficient of $x^{2^k-1+2^k-1}$ in $T(x)$ is a_kb_k), and 2^j-1+2^k-1 where $j>k$. In the last case, the coefficient of $x^{2^j-1+2^k-1}$ is $\sum_{j>k}(a_kb_j + b_ka_j)$, which is zero since $a_j = b_j = 0$ for $j>k$.

Hence the coefficient of $x^{2^m-2^d+2^{k+1}-2}$ in $T(x)S(x)$ is

$$(b_0^2a_k^2 + a_kb_k + a_0^2b_k^2)c(m-1, m-2, \ldots, d) = 0.$$

As before, $c(m-1, m-2, \ldots, d)$ is a Moore determinant, which is non-zero. Therefore $(b_0^2a_k^2 + a_kb_k + a_0^2b_k^2) = 0$. Since $\mathrm{Tr}(a_0b_0) = 1$, we have $a_k = b_k = 0$.

Note that in the case where $d = m-1$, the above claims already show that $a_2 = a_3 = \cdots = a_{d-1} = 0$ and $b_2 = b_3 = \cdots = b_{d-1} = 0$, so $p(x)$ and $q(x)$ are both linear. Also observe that when $m = 7$ (resp. 8), the only admissible d is 6 (resp. 7). In both cases, $m-d=1$, so $p(x)$ and $q(x)$ are both linear. Hence from now on, we will assume that $m \geqslant 10$ and $m-1 > d > \frac{m}{2}+2$.

Claim. $a_r = \cdots = a_3 = b_r = \cdots = b_3 = 0$: Let $3 \leqslant t \leqslant r$ and assume that $a_j = b_j = 0$ for $j > t$. Since $r \leqslant \frac{m-3}{2}$ and $m \geqslant 10$, by Theorem 2.4, there exist $0 = i_1 < i_2 < \cdots < i_r \leqslant m-t-3$ such that $c(i_1, i_2, \ldots, i_r) \neq 0$ and the number of consecutive 1's in $\{i_1, i_2, \ldots, i_r\}$ is at most $t-1$. Now, we consider the exponent $2^m - 2^{m-t} + \sum_{j=1}^{r} 2^{i_j}$ and we see that it can only be obtained in one way as a sum of two exponents, one from $T(x)$, the other from $S(x)$.

$$0\overbrace{1\ldots1}^{k}0\overbrace{\ldots1\ldots1}^{m-k-2} = 0\overbrace{0\ldots0}^{k}0\overbrace{\ldots1\ldots1}^{m-k-2} + 0\overbrace{1\ldots1}^{k}0\overbrace{0\ldots0}^{m-k-2}.$$

It follows from (3.1) that

$$(b_0^2 a_k^2 + a_k b_k + a_0^2 b_k^2)c(i_1, i_2, \ldots, i_r) = 0$$

and hence, $a_k = b_k = 0$.

Claim. $a_2 = b_2 = 0$: As in Theorem 2.1 we consider the quadratic form $Q(x) = \mathrm{Tr}(p(x)q(x) + a_0 b_0)$ over $V = \mathbb{F}_{2^m}$. Note that since $\mathrm{Tr}(a_0 b_0) = 1$, the assumption that $\mathrm{Tr}(p(\lambda)q(\lambda)) = 1$ for all $\lambda \in A \backslash \{0\}$ implies that $Q(\lambda) = 0$ for all $\lambda \in A$, where $|A| = 2^d$. The bilinear form associated with $Q(x)$ is

$$B(x,y) = \mathrm{Tr}((a_0^2 b_2^2 + a_2 b_2 + a_2^2 b_0^2)(xy^2 + yx^2)^2),$$

$$\begin{aligned}\mathrm{Rad}\, V &= \{x \in V \mid \mathrm{Tr}((a_0^2 b_2^2 + a_2 b_2 + a_2^2 b_0^2)(xy^2 + yx^2)^2) = 0 \ \forall_{y \in V}\} \\ &= \{x \in V \mid x^3 = (a_0^2 b_2^2 + a_2 b_2 + a_2^2 b_0^2)^{-\frac{1}{2}}\} \cup \{0\}.\end{aligned}$$

As discussed in the proof of Theorem 2.1, if $a_0^2 b_2^2 + a_2 b_2 + a_2^2 b_0^2 \neq 0$, then the maximum dimension of a subspace of V on which Q vanishes is at most $\lfloor \frac{m}{2} \rfloor + 1$. But we knew that $Q(x)$ vanishes on A, which has $\mathbb{F}_2$-dimension d, and $d > \frac{m}{2} + 2$. This is a contradiction. Hence $a_0^2 b_2^2 + a_2 b_2 + a_2^2 b_0^2 = 0$. Combining this with $\mathrm{Tr}(a_0 b_0) = 1$, we obtain $a_2 = b_2 = 0$.

So we have proven that both $p(x)$ and $q(x)$ must be linear, by the last part of Theorem 1.2, the maximal arc generated by this $\{p, q\}$-map is a Denniston maximal arc. This completes the proof. □

Combining Theorem 3.1 with known constructions in [FLX,HM,M], we have

Theorem 3.2. *Let $m \geqslant 7$ but $m \neq 9$. Then the largest d of a non-Denniston maximal arc of degree 2^d in $\mathrm{PG}(2, 2^m)$ generated by a $\{p, q\}$-map via Theorem 1.2 is either $\lfloor \frac{m}{2} \rfloor + 1$ or $\lfloor \frac{m}{2} \rfloor + 2$.*

It is an interesting question whether there exists a $\{p, q\}$-map generating a non-Denniston maximal arc in $PG(2, 2^m)$ of degree $\lfloor \frac{m}{2} \rfloor + 2$ when $m \geqslant 7$. We remark that in the case $m = 5$, there is an example of $\{p, q\}$-maps which generates a non-Denniston maximal arc of degree 16 in $PG(2, 32)$ [M, p. 362].

Acknowledgments

We thank Henk D.L. Hollmann for useful discussions on Mathon's construction of maximal arcs. Part of this work was carried out during a visit of Qing Xiang to National University of Singapore. Qing Xiang thanks the Department of Mathematics, National University of Singapore for its hospitality. The research of Qing Xiang was also partially supported by NSA Grant MDA 904-03-1-0095.

References

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

[B] A. Barlotti, Su $\{k; n\}$-archi di un piano lineare finito, Boll. Un. Mat. Ital. 11 (1956) 553–556.

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

[FLX] F. Fiedler, K.H. Leung, Q. Xiang, On Mathon's construction of maximal arcs in Desarguesian planes, Adv. Geom. (2003) (Suppl.) S119–S139.

[G] D. Goss, Basic Structures of Function Field Arithmetic. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Vol. 35, Springer, Berlin, 1996.

[HM] N. Hamilton, R. Mathon, On the spectrum of non-Denniston maximal arcs in $PG(2, 2^h)$, European J. Combin. 25 (2004) 415–421.

[LN] R. Lidl, H. Niederreiter, Finite Fields, 2nd Edition, Cambridge University Press, Cambridge, 1997.

[M] R. Mathon, New maximal arcs in Desarguesian planes, J. Combin. Theory (A) 97 (2002) 353–368.

[P] T. Pentilla, Configurations of ovals, J. Geom. 76 (2003) 233–255.

[T1] J. Thas, Construction of maximal arcs and partial geometries, Geom. Dedicata 3 (1974) 61–64.

[T2] J. Thas, Construction of maximal arcs and dual ovals in translation planes, European J. Combin. 1 (1980) 189–192.

[W] W.D. Wallis, Configurations arising from maximal arcs, J. Combin. Theory (A) 14 (1973) 115–119.