Maximal arcs and extended cyclic codes

Stefaan De Winter,* Cunsheng Ding,† and Vladimir D. Tonchev‡

Abstract

It is proved that for every $d \geq 2$ such that $d-1$ divides $q-1$, where q is a power of 2, there exists a Denniston maximal arc A of degree d in $\mathrm{PG}(2,q)$, being invariant under a cyclic linear group that fixes one point of A and acts regularly on the set of the remaining points of A. Two alternative proofs are given, one geometric proof based on Abatangelo-Larato's characterization of Denniston arcs, and a second coding-theoretical proof based on cyclotomy and the link between maximal arcs and two-weight codes.

MSC 2010 codes: 05B05, 05B25, 51E15, 94B15

Keywords: Maximal arc, 2-design, two-weight code, cyclic code.

1 Introduction

Suppose that P is a projective plane of order $q = ds$. A *maximal* $((sd-s+1)d,d)$-*arc* (or a maximal arc of degree d), is a set A of $(sd-s+1)d$ points of P such that every line of P is ether disjoint from A or meets A in exactly d points [3], [19]. The collection of lines of P which have no points in common with A determines a maximal $((sd-d+1)s,s)$-arc $A^{\perp}$ (called a *dual arc*) in the dual plane $P^{\perp}$. A *hyperoval* is a maximal arc of degree 2.

Maximal arcs of degree d with $1 < d < q$ do not exist in any Desarguesian plane of odd order q [5], and are known to exist in every Desarguesian plane of even order (Denniston [9], Thas [23], [24]; see also [7], [15], [16], [20]), as well as in some non-Desarguesian planes of even order [11], [12], [13], [14], [18], [22], [23], [24].

In [1] Abatangelo and Larato proved that a maximal arc A in $\mathrm{PG}(2,q)$, q even, is a Denniston arc (that is, A can be obtained via Denniston's construction [9]), if and only if A is invariant under a linear collineation of $\mathrm{PG}(2,q)$, being a cyclic group of order $q+1$. Collineation groups of maximal arcs in $\mathrm{PG}(2,2^t)$ are further studied in [17].

*Michigan Technological University, Houghton, MI 49921, USA
†The Hong Kong University of Science and Technology, Hong Kong
‡Michigan Technological University Houghton, MI 49931, USA

Abatangelo-Larato's characterization of Denniston's arcs implies, in particular, that a regular hyperoval $\mathcal{H}$ in $\mathrm{PG}(2,2^t)$ is characterized by the property that $\mathcal{H}$ is stabilized by a cyclic collineation group of order $q+1$ that fixes one point of $\mathcal{H}$ and acts regularly on the remaining $q+1$ points of $\mathcal{H}$. Consequently, the two-weight q-ary code associated with $\mathcal{H}$ (cf. [6]), is an extended cyclic code.

The subject of this paper is a class of maximal arcs that generalize this property of regular hyperovals. It is proved that for every $d \geq 2$ such that $d-1$ divides $q-1$, where q is a power of 2, there exists a maximal arc A of degree d in $\mathrm{PG}(2,q)$ that is invariant under a cyclic linear group that fixes one point of A and acts regularly on the set of the remaining points of A, hence, the two-weight code C associated with A is an extended cyclic code. Two alternative proofs are given, one geometric proof based on Abatangelo-Larato's characterization of Denniston arcs, and a coding-theoretic proof based on cyclotomy.

2 Maximal arcs with a cyclic automorphism group

Theorem 1. *Let $q = 2^{km}$ and $d = 2^m$, $(m,k \geq 1)$. There exists a partition of $AG(2,q)$ into $\frac{q-1}{d-1}$ maximal Denniston arcs of degree d sharing a unique point, and such that there is a cyclic group G acting sharply transitively on the points of each of the arcs distinct from the nucleus.*

Proof. Assume x^2+bx+1 is an irreducible quadratic form over $\mathbb{F}_q$, and let F_l, $l \in \mathbb{F}_q \cup \{\infty\}$, be the conic in $\mathrm{PG}(2,q)$ with equation $x^2+bxy+y^2+lz^2 = 0$. It is clear that F_0, the point $(0,0,1)$ is the nucleus of each of the $q-1$ nondegenerate conics F_l, $l \in \mathbb{F}_q^*$, and let F_∞ be the line $z = 0$. We will partition the affine plane $\mathrm{AG}(2,q) = \mathrm{PG}(2,q) \setminus (z=0)$.

Let $\mathbb{F}_d$ be the unique subfield of order d of $\mathbb{F}_q$. Let H be the additive group of $\mathbb{F}_d$. By Denniston's construction of maximal arcs [9], it follows that $A = \cup F_l$, $l \in H$, is a maximal arc of degree d.

We will show that A admits a cyclic group of automorphisms acting sharply transitively on the points of the arc distinct from the nucleus. Consider the following group:

$$G = \left\{ \begin{pmatrix} \alpha + a\beta & \beta & 0 \\ \beta & \alpha & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \alpha,\beta \in \mathbb{F}_q, \alpha^2 + a\alpha\beta + \beta^2 = 1, \gamma \in \mathbb{F}_d^* \right\}.$$

This group is the direct product of

$$G_1 = \left\{ \begin{pmatrix} \alpha + a\beta & \beta & 0 \\ \beta & \alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} : \alpha,\beta \in \mathbb{F}_q, \alpha^2 + a\alpha\beta + \beta^2 = 1 \right\},$$

and

$$G_2 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \gamma \in \mathbb{F}_d^* \right\}.$$

By a result of Abatangelo and Larato [1] G_1 is a cyclic group of order $q+1$ acting sharply transitively on the points of each of the conics F_l, $l \in \mathbb{F}_q^*$. On the other hand it is clear that G_2 is a cyclic group of order $d-1$ that acts transitively on the set of conics F_l, $l \in H \setminus \{0\}$. It follows that G is a cyclic group of automorphisms acting sharply transitively on the points of A distinct from the nucleus.

Next, let $H_1^* = H \setminus \{0\}, H_2^*, \ldots, H^*_{\frac{q-1}{d-1}}$ be the (multiplicative) cosets of $H \setminus \{0\}$ in the multiplicative group of $\mathbb{F}_q$. Set $H_i = H_i^* \cup \{0\}$ for all i. We now make the following two observations:

- H_i is an additive subgroup of order d of the additive group of $\mathbb{F}_q$, for all $i \in \{1, \ldots, \frac{q-1}{d-1}\}$;
- $H_i \cap H_j = \{0\}$ for all $i \neq j$.

The first observation follows immediately from the fact that H is an additive subgroup of $\mathbb{F}_q$, whereas the second observation follows directly from the fact that $H \setminus \{0\}$ is a subgroup of the multiplicative subgroup of $\mathbb{F}_q$.

For $i \in \{1, \ldots, \frac{q-1}{d-1}\}$ define A_i to be the Denniston maximal arc $\cup F_l$, $l \in H_i$. One easily concludes that the $\frac{q-1}{d-1}$ maximal Denniston arcs A_i partition the plane in the desired way. $\square$

Theorem 2. *Let A_i, $i = 1, \ldots, \frac{q-1}{d-1}$ be a set of maximal arcs of degree d sharing a unique point P and partitioning the point set of $AG(2,q)$. Furthermore assume that there is a linear cyclic group L (of order $(d-1)(q+1)$) acting sharply transitively on the points of A_i, $i = 1, \ldots, \frac{q-1}{d-1}$, distinct from P. Then the set of maximal arcs A_i arises as in Theorem 1.*

Proof. We assume that $\mathrm{AG}(2,q)$ is the affine plane obtained by deleting the line $z = 0$ from $\mathrm{PG}(2,q)$. Clearly A_1 is invariant under a linear group $C \leq L$ of collineations of $\mathrm{PG}(2,q)$ which is cyclic of order $q+1$. It follows from [1] that A_1 (and hence each of the A_i) is of Denniston type. Note that this group C of order $q+1$ stabilizes each of the conics in the maximal arc A_1. Hence we can assume that the plane is coordinatized in such a way that A_1 is contained in the standard pencil with $P = (0,0,1)$. It follows that the group C is the unique cyclic linear group of order $q+1$ stabilizing all conics in the standard pencil, and hence is actually the group G_1 from the previous theorem. Let H be the additive group associated with A_1. Without loss of generality we may assume that $1 \in H$. The stabilizer S in L of the line $x = 0$ clearly has order $d-1$, is cyclic, and fixes the points $P = (0,0,1)$ and $(0,1,1)$. As the orbit of $(0,1,1)$ under S consists of the points $(0,h,1)$, $h \in H \setminus \{0\}$, it follows that H is actually that additive group of the subfield $\mathbb{F}_d \subset \mathbb{F}_q$. Note that this implies that the action of S on all points of the line $x = 0$ is known (the action of S on this line corresponds to multiplying the second coordinate of $(0, y, 1)$ by a non-zero element of $\mathbb{F}_d$. Also, clearly all A_i are isomorphic.

We next show that all A_i, $i > 1$, are contained in the standard pencil. Clearly L contains a unique cyclic subgroup C of order $q+1$. Assume that A_i contains the points $(0, h_i, 1)$, $h_i \in H_i$ for some subset $H_i \subset \mathbb{F}_q$ on the line $x = 0$. Then, whenever $h_i \neq 0$, clearly the orbit of $(0, h_i, 1)$ under C is a conic in the standard pencil, and belongs to A_i. It follows that A_i consists of conics contained in the standard pencil.

Now let H_i be the additive subgroup associated with the maximal arc A_i, $i > 1$. Clearly the set $\{(0, h_i, 1) : h_i \in H_i\}$ is stabilized by the subgroup S of L. It follows that H_i is a multiplicative coset of the additive subgroup H. It now easily follows that the set of maximal arcs A_i arises as in the previous theorem, and the group L is actually the group G from Theorem 1. $\square$

3 A family of extended cyclic two-weight codes

It is known that the existence of a maximal $((sd-s+1)d, d)$-arc in $PG(2, q)$ is equivalent to the existence of a linear projective two-weight code L over $GF(q)$ of length $(sd-s+1)d$ and dimension 3, having nonzero weights $w_1 = (sd-s)d$ and $w_2 = (sd-s+1)d$ [6], [8]. If A is a maximal arc of degree $d = 2^m$ in $PG(2, 2^{km})$ satisfying the conditions of Theorem 1, the code L is an extended cyclic code. We will give a coding-theoretical description of this code based on cyclotomy.

Let m and k be positive integers. Define

$$q = 2^{km},\ d = 2^m,\ n = (q+1)(d-1),\ N = (q-1)/(d-1),\ r = q^2. \tag{1}$$

By definition,

$$N = \frac{r-1}{n} = \frac{q-1}{d-1} = (2^m)^{k-1} + (2^m)^{k-2} + \cdots + 2^m + 1.$$

It is straightforward to see that $\mathrm{ord}_n(q) = 2$. Let α be a generator of $\mathrm{GF}(r)^*$. Put $\beta = \alpha^N$. Then the order of β is n. Let $\mathrm{Tr}(\cdot)$ denote the trace function from $\mathrm{GF}(r)$ to $\mathrm{GF}(q)$.

The irreducible cyclic code of length n over $\mathrm{GF}(q)$ is defined by

$$C_{(q,2,n)} = \{\mathbf{c}_a : a \in \mathrm{GF}(r)\}, \tag{2}$$

where

$$\mathbf{c}_a = (\mathrm{Tr}(a\beta^0), \mathrm{Tr}(a\beta^1), \mathrm{Tr}(a\beta^2), \cdots, \mathrm{Tr}(a\beta^{n-1})). \tag{3}$$

The complete weight distribution of some irreducible cyclic codes was determined in [4]. However, the results in [4] do not apply to the cyclic code $C_{(q,2,n)}$ of (2), as our q is usually not a prime. The weight distribution of $C_{(q,2,n)}$ is given in the following theorem.

Theorem 3. *The code $\mathcal{C}_{(q,2,n)}$ of* (2) *has parameters* $[n, 2, n-d+1]$ *and has weight enumerator*

$$1+(q^2-1)z^{(d-1)q}.$$

Further, the dual distance of $\mathcal{C}_{(q,2,n)}$ equals 3 *if* $m=1$*, and* 2 *if* $m>1$.

Proof. Since q is even, $\gcd(q+1, q-1)=1$. It then follows that

$$\gcd\left(\frac{r-1}{q-1}, N\right) = \gcd\left(q+1, \frac{q-1}{d-1}\right) = 1.$$

The desired conclusions regarding the dimension and weight enumerator of $\mathcal{C}_{(q,2,n)}$ then follow from Theorem 15 in [10].

We now prove the conclusions on the minimum distance of the dual code of $\mathcal{C}_{(q,2,n)}$. To this end, we define a linear code of length $q+1$ over $\mathrm{GF}(q)$ by

$$\mathcal{E}_{(q,2,q+1)} = \{\mathbf{e}_a : a \in \mathrm{GF}(r)\}, \tag{4}$$

where

$$\mathbf{e}_a = (\mathrm{Tr}(a\beta^0), \mathrm{Tr}(a\beta^1), \mathrm{Tr}(a\beta^2), \cdots, \mathrm{Tr}(a\beta^q)). \tag{5}$$

Each code $\mathbf{c}_a$ in $\mathcal{C}_{(q,2,n)}$ is related to the codeword $\mathbf{e}_a$ in $\mathcal{E}_{(q,2,q+1)}$ as follows:

$$\mathbf{c}_a = \mathbf{e}_a || \beta^{(q+1)}\mathbf{e}_a || \beta^{(q+1)2}\mathbf{e}_a || \cdots || \beta^{(q+1)(d-2)}\mathbf{e}_a, \tag{6}$$

where $||$ denotes the concatenation of vectors. It is easy to prove

$$\{\beta^{(q+1)i} : i \in \{0, 1, \cdots, d-2\}\} = \mathrm{GF}(d)^* \subseteq \mathrm{GF}(q)^*.$$

It then follows that $\mathcal{E}_{(q,2,q+1)}$ has the same dimension as $\mathcal{C}_{(q,2,n)}$. Consequently, the dimension of $\mathcal{E}_{(q,2,q+1)}$ is 2, and the dual code $\mathcal{E}^{\perp}_{(q,2,q+1)}$ has dimension $q-1$. It then follows from the Singleton bound that the minimum distance $d_E^{\perp}$ of $\mathcal{E}^{\perp}_{(q,2,q+1)}$ is at most 3. Obviously, $d_E^{\perp} \neq 1$. Suppose that $d_E^{\perp} = 2$. Then there are an element $u \in \mathrm{GF}(q)^*$ and two integers i, j with $0 \leq i < j \leq q$ such that $\mathrm{Tr}(a(\beta^i - u\beta^j)) = 0$ for all $a \in \mathrm{GF}(r)$. It then follows that $\beta^i(1-u\beta^{j-i}) = 0$. As a result, $\beta^{j-i} = \alpha^{(q-1)(j-i)/(d-1)} = u^{-1} \in \mathrm{GF}(q)^*$, which is impossible, as $0 < j-i \leq q$ and $\gcd(q+1, (q-1)/(d-1)) = 1$. Hence, $d_E^{\perp} = 3$. Since $\mathcal{E}^{\perp}_{(q,2,q+1)}$ is a $[q+1, q-1, 3]$ MDS code, $\mathcal{E}_{(q,2,q+1)}$ is $[q+1, 2, q]$ MDS code. When $m=1$, we have $d=2$ and hence $\mathcal{C}_{(q,2,n)} = \mathcal{E}_{(q,2,q+1)}$. Consequently, the dual distance of $\mathcal{C}_{(q,2,n)}$ is 3 when $m=1$. When $m>1$, we have $d-1>1$. In this case, by (6) $\mathcal{C}^{\perp}_{(q,2,n)}$ has the following codeword

$$(\beta^{q+1}, \mathbf{0}, 1, 0, 0, \cdots, 0, 0),$$

which has Hamming weight 2, where $\mathbf{0}$ is the zero vector of length q. Hence, $\mathcal{C}^{\perp}_{(q,2,n)}$ has minimum distance 2 if $m>1$. This completes the proof. $\square$

The code $\mathcal{C}_{(q,2,n)}$ is a one-weight code over $\mathrm{GF}(q)$. We need to study the augmented code of $\mathcal{C}_{(q,2,n)}$. Let $Z(a,b)$ denote the number of solutions $x \in \mathrm{GF}(r)$ of the equation

$$\mathrm{Tr}_{r/q}(ax^N) = ax^N + a^q x^{Nq} = b, \tag{7}$$

where $a \in \mathrm{GF}(r)$ and $b \in \mathrm{GF}(q)$.

Lemma 4. *Let $a \in \mathrm{GF}(r)^*$ and $b \in \mathrm{GF}(q)$. Then*

$$Z(a,b) = \begin{cases} (d-1)N+1 & \text{if } b=0, \\ dN \text{ or } 0 & \text{if } b \in \mathrm{GF}(q)^*. \end{cases}$$

Proof. Let α be a fixed primitive element of $\mathrm{GF}(q^2)$ as before. Define $C_i^{(N,q^2)} = \alpha^i \langle \alpha^N \rangle$ for $i = 0, 1, ..., N-1$, where $\langle \alpha^N \rangle$ denotes the subgroup of $\mathrm{GF}(q^2)^*$ generated by α^N. The cosets $C_i^{(N,q^2)}$ are called the cyclotomic classes of order N in $\mathrm{GF}(q^2)$. When $b=0$, it follows from Theorem 3 that $Z(a,b) = (d-1)N+1$. Below we give a geometric proof of the conclusion of the second part.

We first recall the following natural model for $\mathrm{AG}(2,q)$. The points of $\mathrm{AG}(2,q)$ are the elements $\mathrm{GF}(q^2)$, with 0 naturally corresponding to the point $(0,0)$. Let $\mathrm{GF}(q) = \{0, \beta_1, \beta_2, \ldots, \beta_{q-1}\}$. The lines of $\mathrm{AG}(2,q)$ through $(0,0)$ are of the form $\{0, \alpha^i\beta_1, \alpha^i\beta_2, \ldots, \alpha^i\beta_{q-1}\}$ for $i = 0, q-1, 2(q-1), \ldots, q(q-1)$. The rest of the lines of $\mathrm{AG}(2,q)$ are translates of these $q+1$ lines. In this model, multiplication by a nonzero element of $\mathrm{GF}(q^2)$ acts as a linear automorphism of $\mathrm{AG}(2,q)$ fixing $(0,0)$ and acting fix point free on the other points. Hence $C = \{1, \alpha^{q-1}, \alpha^{2(q-1)}, \ldots, \alpha^{q(q-1)}\}$ is a cyclic group of order $q+1$ acting on $AG(2,q)$. From [1], we know that all cyclic subgroups of order $q+1$ of $\mathrm{PGL}(3,q)$ are conjugate. Hence it follows that the orbits of C on $\mathrm{AG}(2,q)$ must consist of a unique fixed point (namely $(0,0)$) and $q-1$ orbits of size $q+1$, each of which is a conic. Now the multiplicative subgroup $H = \{\nu_1, \nu_2, \ldots, \nu_{d-1}\}$ of $\mathrm{GF}(q^2)$ acts as a group of homologies with center $(0,0)$ on $\mathrm{AG}(2,q)$. It follows that C acts as the group G_1 and H as the group G_2 from Theorem 1. Hence the orbit of the point "1" under the cyclic group $< C, H >$, together with the point "0", is a maximal arc of degree d. On the other hand $< C, H >= C_0^{(N,q^2)}$. The desired conclusion then follows. $\square$

Define

$$\widetilde{\mathcal{C}}_{(q,2,n)} = \{\mathbf{c}_a + b\mathbf{1} : a \in \mathrm{GF}(r), b \in \mathrm{GF}(q)\}, \tag{8}$$

where $\mathbf{1}$ denotes the all-1 vector in $\mathrm{GF}(q)^n$. By definition, $\widetilde{\mathcal{C}}_{(q,2,n)}$ is the augmented code of $\mathcal{C}_{(q,2,n)}$.

Theorem 5. *The cyclic code $\widetilde{\mathcal{C}}_{(q,2,n)}$ has length n, dimension 3 and only the following nonzero weights:*

$$n-d,\ n-d+1,\ n.$$

The dual distance of $\widetilde{\mathcal{C}}_{(q,2,n)}$ is 4 if $m=1$, and 3 if $m>1$.

Proof. By definition, every codeword in $\widetilde{\mathcal{C}}_{(q,2,n)}$ is given by $\mathbf{c}_a + b\mathbf{1}$, where $a \in \mathrm{GF}(r)$ and $b \in \mathrm{GF}(q)$. By Theorem 3, the codeword $\mathbf{c}_a + b\mathbf{1}$ is the zero codeword if and only if $(a,b) = (0,0)$. Consequently, the dimension of $\widetilde{\mathcal{C}}_{(q,2,n)}$ is 3.

When $a = 0$ and $b \neq 0$, the codeword $\mathbf{c}_a + b\mathbf{1}$ has weight n. When $a \neq 0$ and $b = 0$, by Theorem 3, the codeword $\mathbf{c}_a + b\mathbf{1}$ has weight $n - d + 1$. When $a \neq 0$ and $b \neq 0$, by Lemma 4, the weight of the codeword $\mathbf{c}_a + b\mathbf{1}$ is either n or $n - d$, depending on $Z(a,b) = 0$ or $Z(a,b) = dN$.

The proof of the conclusions on the dual distance of $\widetilde{\mathcal{C}}_{(q,2,n)}$ is left to the reader. □

Let $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ denote the extended code of $\widetilde{\mathcal{C}}_{(q,2,n)}$. The next theorem gives the parameters of this extended code.

Theorem 6. *Let $mk \geq 1$, and let $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ be a linear code over $\mathrm{GF}(q)$ with parameters $[n+1, 3, n+1-d]$ and nonzero weights $n+1-d$ and $n+1$. Then the weight enumerator of $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ is given by*

$$A(z) := 1 + \frac{(q^2-1)(n+1)}{d} z^{n+1-d} + \frac{(q^3-1)d - (q^2-1)(n+1)}{d} z^{n+1}. \tag{9}$$

Furthermore, the dual distance of the code is 3 *when $m > 1$ and* 4 *when $m = 1$.*

Proof. By definition, every codeword of $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ is given by

$$(\mathbf{c}_a + b\mathbf{1}, \bar{c}),$$

where $\bar{c}$ denotes the extended coordinate of the codeword. Note that $\sum_{i=0}^{n-1} \beta^i = 0$. We have

$$\bar{c} = nb = b.$$

When $a \neq 0$ and $b = 0$, by Theorem 3,

$$\mathtt{wt}((\mathbf{c}_a + b\mathbf{1}, \bar{c})) = \mathtt{wt}(\mathbf{c}_a + b\mathbf{1}) = n + 1 - d.$$

When $a \neq 0$ and $b \neq 0$, by the proof of Theorem 5,

$$\mathtt{wt}((\mathbf{c}_a + b\mathbf{1}, \bar{c})) = \begin{cases} n - d + 1 & \text{if } Z(a,b) = dN, \\ n + 1 & \text{if } Z(a,b) = 0. \end{cases}$$

When $a = 0$ and $b \neq 0$, it is obvious that $\mathtt{wt}((\mathbf{c}_a + b\mathbf{1}, \bar{c})) = n + 1$. We then deduce that $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ has only nonzero weights $n+1-d$ and $n+1$. By Theorem 5, the minimum distance of $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}^{\perp}$ is either 3 or 4. The weight enumerator of $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ is obtained by solvingi the first two Pless power moments (see also [6]).

We now prove the conclusions on the dual distance of $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$. For simplicity, we put

$$u = \frac{(q^2-1)(n+1)}{d} z^{n+1-d}, \; v = \frac{(q^3-1)d - (q^2-1)(n+1)}{d}.$$

By (9), the weight enumerator of $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ is $A(z) = 1 + uz^{n+1-d} + vz^{n+1}$. It then follows from the MacWilliam Identity that the weight enumerator $A^{\perp}(z)$ of $\overline{\widetilde{\mathcal{C}}}^{\perp}_{(q,2,n)}$ is given by

$$\begin{aligned} q^3 A^{\perp}(z) &= (1+(q-1)z)^{n+1} A\left(\frac{1-z}{1+(q-1)z}\right) \\ &= (1+(q-1)z)^{n+1} + u(1-z)^{n+1-d}(1+(q-1)z)^d + v(1-z)^{n+1}. \end{aligned} \tag{10}$$

We have

$$(1+(q-1)z)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} (q-1)^i z^i \tag{11}$$

and

$$v(1-z)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} (-1)^i v z^i. \tag{12}$$

It is straightforward to prove that

$$u(1-z)^{n+1-d}(1+(q-1)z)^d = \sum_{\ell=0}^{n+1} \left(\sum_{i+j=\ell} \binom{n+1-d}{i} \binom{d}{j} (-1)^i (q-1)^j \right) u z^{\ell}. \tag{13}$$

Combining (10), (11), (12) and (13), we obtain that

$$\begin{aligned} q^3 A_1^{\perp} &= \binom{n+1}{1}[(q-1)-v] + \\ &\quad \left[\binom{n+1-d}{0}\binom{d}{1}(-1)^0(q-1)^1 + \binom{n+1-d}{1}\binom{d}{0}(-1)^1(q-1)^0\right] u \\ &= (n+1)[(q-1)-v] + [d(q-1)-(n+1-d)]u \\ &= 0. \end{aligned}$$

Combining (10), (11), (12) and (13) again, we get that

$$\begin{aligned} q^3 A_2^{\perp} &= \binom{n+1}{2}[(q-1)^2+v] + \binom{n+1-d}{0}\binom{d}{2}(-1)^0(q-1)^2 u + \\ &\quad \binom{n+1-d}{1}\binom{d}{1}(-1)^1(q-1)^1 u + \binom{n+1-d}{2}\binom{d}{0}(-1)^2(q-1)^0 u \\ &= \binom{n+1}{2}[(q-1)^2+v] + \\ &\quad \left[\binom{d}{2}(q-1)^2 - (n+1-d)d(q-1) + \binom{n+1-d}{2}\right] u \\ &= 0. \end{aligned}$$

Combining (10), (11), (12) and (13) the third time, we arrive at

$$\begin{aligned}
q^3A_3^{\perp} &= \binom{n+1}{3}[(q-1)^3-v]+ \\
&\quad \left[\binom{n+1-d}{0}\binom{d}{3}(-1)^0(q-1)^3+\binom{n+1-d}{1}\binom{d}{2}(-1)^1(q-1)^2\right]u+ \\
&\quad \left[\binom{n+1-d}{2}\binom{d}{1}(-1)^2(q-1)^1+\binom{n+1-d}{3}\binom{d}{0}(-1)^3(q-1)^0\right]u \\
&= \binom{n+1}{3}[(q-1)^3-v]+ \\
&\quad \left[\binom{d}{3}(q-1)^3-\binom{n+1-d}{1}\binom{d}{2}(q-1)^2\right]u+ \\
&\quad \left[\binom{n+1-d}{2}\binom{d}{1}(q-1)-\binom{n+1-d}{3}\right]u.
\end{aligned}$$

It then follows that

$$\begin{aligned}
6q^3A_3^{\perp} &= q^6d^3-4q^6d^2+5q^6d-2q^6+q^5d^3-3q^5d^2+2q^5d- \\
&\quad q^4d^3+4q^4d^2-5q^4d+2q^4-q^3d^3+3q^3d^2-2q^3d \\
&= (d-2)(d-1)q^3(q^2-1)(qd-q+d).
\end{aligned}$$

Thus,

$$A_3^{\perp} = \frac{(d-2)(d-1)(q^2-1)(qd-q+d)}{6}. \tag{14}$$

When $m>1$, we have $d>3$. In this case, by (14) we have $A_3^{\perp}>0$. When $m=1$, by (14) we have $A_3^{\perp}=0$. As a result, the dual distance is at least 4 when $m=1$. On the other hand, the Singleton bound tells us that the dual distance is at most 4 when $m=1$. Whence, the dual distance must be 4 when $m=1$.

Thus, in all cases, the extended code $\overline{\overline{\mathcal{C}}}_{(q,2,n)}$ is projective, hence is associated with a maximal $(n+1,d)$-arc in $PG(2,q)$.

□

Theorem 7. *If $mk>1$, the supports of the codewords with weight $n+1-d$ in $\overline{\overline{\mathcal{C}}}_{(q,2,n)}$ form a 2-design D with parameters*

$$2-\left(n+1,\ n+1-d,\ \frac{(n+1-d)(n-d)}{d(d-1)}\right).$$

Proof. The supports of the codewords of weight $n+1-d$ in $\overline{\overline{\mathcal{C}}}_{(q,2,n)}$ form a 2-design by the Assmus-Mattson theorem [2] Since $n+1-d$ is the minimum distance of the code, the total number of blocks in the design is given by

$$\frac{(q^2-1)(n+1)}{(q-1)d} = \frac{(q+1)(n+1)}{d}.$$

As a result,

$$\lambda = \frac{(n+1-d)(n-d)}{d(d-1)}.$$

$\square$

Remark 8. We note that if M is a $3 \times (n+1)$ generator matrix of the two-weight code $\overline{\widetilde{\mathcal{C}}}_{(q,2,n)}$ from Theorem 7, the columns of M label the points of a maximal $(n+1,d)$-arc A in $\mathrm{PG}(2,q)$, and the complementary design $\bar{D}$ of the 2-design D from Theorem 7 is a Steiner 2-$(n+1,d,1)$ design having as blocks the nonempty intersections of A with the lines of $\mathrm{PG}(2,q)$.

Theorem 9. *If $m > 1$, the supports of the codewords with weight 3 in $\overline{\widetilde{\mathcal{C}}}^{\perp}_{(q,2,n)}$ form a 2-design with parameters*

$$2-(n+1,\ 3,\ d-2)\,.$$

Proof. Let $m > 1$. By Theorem 6 the code $\overline{\widetilde{\mathcal{C}}}^{\perp}_{(q,2,n)}$ has minimum distance 3. It follows from the Assmus-Mattson theorem that the supports of the codewords of weight 3 in $\overline{\widetilde{\mathcal{C}}}^{\perp}_{(q,2,n)}$ form a 2-design. We then deduce from (9) that the number of blocks in this design is

$$b^{\perp} = \frac{(d-2)n(n+1)}{6}.$$

Consequently, $\lambda^{\perp} = d-2$. $\square$

4 Acknowledgments

This material is based upon work that was done while the first author was serving at the National Science Foundation. Vladimir Tonchev acknowledges support by NSA Grant H98230-16-1-0011.

References

[1] V. Abatangelo and B. Larato, A characterization of Denniston's maximal arcs, *Geom. Dedicata* **30** (1989), 197–203.

[2] E. F. Assmus, Jr., H. F. Mattson, New 5-designs, *J. Combin. Theory* **6** (1969), 122 - 151.

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

[4] L. D. Baumert, R. J. McEliece, Weights of irreducible cyclic codes, Information and Control **20** (1972), 158–175.

[5] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica* **17** (1997), 31-41.

[6] R. Calderbank, W. W. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* **18** (1986), 97–122.

[7] F. De Clerk, S. De Winter, T. Maes, A geometric approach to Mathon maximal arcs, *J. Combin. Theory* Ser. A **118** (2011), 1196-1211.

[8] P. Delsarte, Two-weight linear codes and strongly regular graphs, Report R160, MBLE Res. Lab., Brussels, 1971.

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

[10] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, *Discrete Mathematics* **313** (2013), 434–446.

[11] N. Hamilton, Some maximal arcs in Hall planes, *J. Geom.* **52** (1995), 101-107.

[12] N. Hamilton, Some inherited maximal arcs in derived dual dual translation planes, *Geom. Dedicata* **55** (1995), 165 –173.

[13] N. Hamilton, Some maximal arcs in derived dual Hall planes, *European J. Combin.* **15** (1994), 525 – 532.

[14] N. Hamilton, Maximal arcs in finite projective planes and associated in projective planes, PhD thesis, The University of Western Australia (1995).

[15] N. Hamilton, R. Mathon, More maximal arcs in Desarguesian projective planes and their geometric structure,*Adv. Geom.* **3** (2003), 251 – 261.

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

[17] N. Hamilton, T. Penttila, Groups of maximal arcs, *J. Combin. Theory* Ser. A **94** (2001), 63 - 86.

[18] N. Hamilton, S. D. Stoichev, V. D. Tonchev, Maximal arcs and disjoint maximal arcs in projective planes of order 16. *J. Geometry* **67**, 117-126 (2000).

[19] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields (2nd edition).* Oxford University Press (1998).

[20] R. Mathon, New maximal arcs in Desarguesian planes, *J. Combin. Theory* Ser. A **97** (2002), 353368.

[21] G. Myerson, Period polynomials and Gauss sums for finite fields, *Acta Arith.* **39** (1981), 251–264.

[22] T. Penttila, G. F. Royle, M. K. Simpson, Hyperovals in the known projective planes of order 16. *J. Combin. Designs* **4** (1996), 59 - 65.

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

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