Maximal arcs and extended cyclic codes

Stefaan De Winter1 · Cunsheng Ding2 · Vladimir D. Tonchev3

Received: 30 November 2017 / Revised: 18 April 2018 / Accepted: 26 June 2018 / Published online: 6 July 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

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 $\text{PG}(2, q)$, 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.

Keywords
Maximal arc · 2-Design · Two-weight code · Cyclic code

Mathematics Subject Classification
05B05 · 05B25 · 51E15 · 94B15

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 either 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 [22,23]; see also [7,15,16,20]), as well as in some non-Desarguesian planes of even order [11–14,18,21–23].

In [1] Abatangelo and Larato proved that a maximal arc $A$ in $\text{PG}(2, q)$, $q$ 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 $\text{PG}(2, q)$, being a cyclic group of order $q + 1$. Collineation groups of maximal arcs in $\text{PG}(2, 2^t)$ are further studied in [17].

Abatangelo–Larato’s characterization of Denniston’s arcs implies, in particular, that a regular hyperoval $H$ in $\text{PG}(2, 2^t)$ is characterized by the property that $H$ is stabilized by a cyclic collineation group of order $q + 1$ that fixes one point of $H$ and acts regularly on the remaining $q + 1$ points of $H$. Consequently, the two-weight $q$-ary code associated with $H$ (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 $\text{PG}(2, q)$ 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 $\text{AG}(2, q)$ 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 $x^2 + cx + 1$ is an irreducible quadratic form over $\mathbb{F}_q$, and let $F_1, l \in \mathbb{F}_q \cup \{\infty\}$, be the conic in $\text{PG}(2, q)$ with equation $x^2 + cxy + y^2 + lz^2 = 0$. It is clear that $F_0$, the point $(0, 0, 1)$ is the nucleus of each of the $q - 1$ nondegenerate conics $F_1, l \in \mathbb{F}^*_q$, and let $F_{\infty}$ be the line $z = 0$. We will partition the affine plane $\text{AG}(2, q) = \text{PG}(2, q) \setminus (z = 0)$.

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 $A = \cup F_i, l \in H$, 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:

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

This group is the direct product of

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

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 $F_1, l \in \mathbb{F}^*_q$. 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 $F_1, l \in H \setminus \{0\}$. As
$G_1$ and $G_2$ are coprime, it follows that $G$ is a cyclic group of automorphisms acting sharply transitively on the points of $A$ distinct from the nucleus.

Next, let $H_i^* = H \setminus \{0\}, H_2^*, \ldots, H_{d-1}^*$ 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 $\cup F_l, l \in H_l$. One easily concludes that the $\frac{q-1}{d-1}$ maximal Denniston arcs $A_i$ partition the plane in the desired way. □

**Theorem 2** Let $A_1$ be a maximal arc of degree $d$ in $AG(2, q)$. Furthermore assume that there is a linear cyclic group $L$ (of order $(d - 1)(q + 1)$) acting sharply transitively on the points of $A_1$. Then there exists a unique set of maximal arcs $A_i, i = 1, \ldots, \frac{q-1}{d-1}$ of degree $d$ sharing a unique point $P$ and partitioning the point set of $AG(2, q)$, such that $L$ acts sharply transitively on the points of $A_i, i = 1, \ldots, \frac{q-1}{d-1}$, distinct from $P$.

**Proof** We assume that $AG(2, q)$ is the affine plane obtained by deleting the line $z = 0$ from PG(2, $q$). Clearly $A_1$ is invariant under a linear group $C \leq L$ of collineations of PG(2, $q$) which is cyclic of order $q + 1$. It follows from [1] that $A_1$ 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 $P = (0, 0, 1)$ the nucleus of all conics of $A_1$. 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 (by applying a homology with center $P$ if necessary) 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 $\mathbb{F}_d \subset \mathbb{F}_q$, and so $q = 2^{km}$ and $d = 2^m$ for some $m$ and $k$. 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 $\mathbb{F}_d$.

By the previous theorem we now know that a partition as claimed in the theorem exists. We now show uniqueness. We first 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 $H_l$ be the additive subgroup associated with the maximal arc $A_i, i > 1$. Clearly the set $\{(0, h_i, 1) : h_i \in H_l\}$ is stabilized by the subgroup $S$ of $L$. It follows that $H_l$ is a multiplicative coset of the additive subgroup $H_l$ of $H$. 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. It follows that the partition is unique. □
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 \(d = 2^n\) 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

\[
q = 2^k m, \quad d = 2^m, \quad n = (q + 1)(d - 1), \quad N = (q - 1)/(d - 1), \quad r = q^2.
\]

By definition,

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

Since \(n|(q^2 - 1)\), it follows that \(\text{ord}_n(q) = 2\). Let \(\alpha\) be a generator of \(GF(r)^\times\). Put \(\beta = \alpha^N\). Then the order of \(\beta\) is \(n\). Let \(\text{Tr}(\cdot)\) denote the trace function from \(GF(r)\) to \(GF(q)\).

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

\[
C_{(q, 2, n)} = \{c_a : a \in GF(r)\},
\]

where

\[
c_a = (\text{Tr}(a\beta^0), \text{Tr}(a\beta^1), \text{Tr}(a\beta^2), \cdots, \text{Tr}(a\beta^{n-1})).
\]

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 \(C_{(q, 2, n)}\) of \((2)\) has parameters \([n, 2, n - d + 1]\) and has weight enumerator

\[
1 + (q^2 - 1)z^{(d-1)q}.
\]

Furthermore, the dual distance of \(C_{(q, 2, n)}\) 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 \(C_{(q, 2, n)}\) then follow from Theorem 15 in \[10\].

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

\[
E_{(q, 2, q + 1)} = \{e_a : a \in GF(r)\},
\]

where

\[
e_a = (\text{Tr}(a\beta^0), \text{Tr}(a\beta^1), \text{Tr}(a\beta^2), \cdots, \text{Tr}(a\beta^q)).
\]

Each codeword \(e_a\) in \(C_{(q, 2, n)}\) is related to the codeword \(e_a\) in \(E_{(q, 2, q + 1)}\) as follows:

\[
e_a = e_a || \beta^{(q + 1)}e_a || \beta^{(q + 2)}e_a || \cdots || \beta^{(q + 1)(d - 2)}e_a.
\]
where \( || \) denotes the concatenation of vectors. It is easy to prove
\[
\{ \beta^{(q+1)i} : i \in \{0, 1, \ldots, d - 2\} \} = \text{GF}(d)^* \subseteq \text{GF}(q)^*.
\]

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

The code \( C_{q,2}(q,n) \) is a one-weight code over \( \text{GF}(q) \). We need to study the augmented code of \( C_{q,2}(q,n) \). Let \( Z(a, b) \) denote the number of solutions \( x \in \text{GF}(r) \) of the equation
\[
\text{Tr}_{q/2}(ax^N) = ax^N + a^q x^{Nq} = b,
\]
where \( a \in \text{GF}(r) \) and \( b \in \text{GF}(q) \).

**Lemma 4** Let \( a \in \text{GF}(r)^* \) and \( b \in \text{GF}(q) \). Then
\[
Z(a, b) = \begin{cases} (d - 1)N + 1 & \text{if } b = 0, \\ dN \text{ or } 0 & \text{if } b \in \text{GF}(q)^*. \end{cases}
\]

**Proof** Let \( \alpha \) be a fixed primitive element of \( \text{GF}(q^2) \) as before. Define \( C_i^{(N,q^2)} = \langle \alpha^i \rangle \langle \alpha^N \rangle \) for \( i = 0, 1, \ldots, N - 1 \), where \( \langle \alpha^N \rangle \) denotes the subgroup of \( \text{GF}(q^2)^* \) generated by \( \alpha^N \).

The cosets \( C_i^{(N,q^2)} \) are called the cyclotomic classes of order \( N \) in \( \text{GF}(q^2) \). 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 \( \text{AG}(2,q) \). The points of \( \text{AG}(2,q) \) are the elements \( \text{GF}(q^2) \), with 0 naturally corresponding to the point \((0, 0) \). Let \( \text{GF}(q) = \{0, \beta_1, \beta_2, \ldots, \beta_{q-1}\} \). The lines of \( \text{AG}(2,q) \) 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 \( \text{AG}(2,q) \) are translates of these \( q + 1 \) lines. We now note that the statement of the second part of the lemma is equivalent with the statement that every line of \( \text{AG}(2,q) \) intersects \( C_i^{(N,q^2)} \) in \( 0 \) or \( d \) points. In this model of \( \text{AG}(2,q) \), multiplication by a non-zero element of \( \text{GF}(q^2) \) acts as a linear automorphism of \( \text{AG}(2,q) \) 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 \( \text{AG}(2,q) \). From [1], we know that all cyclic subgroups of order \( q + 1 \) of \( \text{PGL}(3,q) \) are conjugate. Hence it follows that the orbits of \( C \) on \( \text{AG}(2,q) \) 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 \( H = \{v_1, v_2, \ldots, v_{d-1}\} \) of \( \text{GF}(q^2) \) acts as a group of homologies.
with center \((0, 0)\) on \(\text{AG}(2, q)\). 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
\[
\tilde{C}_{(q, 2, n)} = \{c_a + b \mathbf{1} : a \in \text{GF}(r), \ b \in \text{GF}(q)\},
\]
where \(\mathbf{1}\) denotes the all-1 vector in \(\text{GF}(q)^n\). By definition, \(\tilde{C}_{(q, 2, n)}\) is the augmented code of \(C_{(q, 2, n)}\).

**Theorem 5** The cyclic code \(\tilde{C}_{(q, 2, n)}\) has length \(n\), dimension 3 and only the following nonzero weights:
\[
n - d, \ n - d + 1, \ n.
\]
The dual distance of \(\tilde{C}_{(q, 2, n)}\) is at least 3.

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

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

Let \(\tilde{d} \perp\) denote the dual distance of \(\tilde{C}_{(q, 2, n)}\). By definition, \(\tilde{C}_{(q, 2, n)}\) has generator matrix
\[
\tilde{G} = \begin{bmatrix}
\text{Tr}_{r/q}(\beta^0) & \text{Tr}_{r/q}(\beta^1) & \ldots & \text{Tr}_{r/q}(\beta^{n-1}) \\
\text{Tr}_{r/q}(\alpha \beta^0) & \text{Tr}_{r/q}(\alpha \beta^1) & \ldots & \text{Tr}_{r/q}(\alpha \beta^{q^{-1}}) \\
1 & 1 & \ldots & 1
\end{bmatrix}.
\]

Since no column of \(\tilde{G}\) is the zero vector, \(\tilde{d} \perp\) cannot be 1. Suppose that \(\tilde{d} \perp = 2\). Then two different columns of \(\tilde{G}\) must be linearly dependent over \(\text{GF}(q)\). Hence, there are two integers \(i\) and \(j\) with \(0 \leq i < j \leq n - 1\) and an element \(u \in \text{GF}(q)^*\) such that
\[
\begin{align*}
\text{Tr}_{r/q}(\beta^i) + u \text{Tr}_{r/q}(\beta^j) &= 0, \\
\text{Tr}_{r/q}(\alpha \beta^i) + u \text{Tr}_{r/q}(\alpha \beta^j) &= 0, \\
1 + u &= 0.
\end{align*}
\]
Put \(\delta = \beta^i - \beta^j\). Then Eq. (9) yields
\[
\begin{align*}
\text{Tr}_{r/q}(\delta) &= \delta + \delta^q = 0, \\
\text{Tr}_{r/q}(\alpha \delta) &= \alpha \delta + \alpha^q \delta^q = 0.
\end{align*}
\]
Solving (10) yields \(\delta(\alpha + \alpha^q) = 0\). Since \(\alpha\) is a generator of \(\text{GF}(r)^*\), \(\alpha + \alpha^q \neq 0\). Consequently, \(\delta = \beta^i - \beta^j = \beta^i (1 - \beta^{j-i}) = 0\). By definition, \(\beta\) is a primitive \(n\)-th root of unity. We then deduce that \(i = j\). This is contrary to the assumption that \(i < j\). The desired conclusion that \(\tilde{d} \perp \geq 3\) then follows. \(\square\)

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

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

\[
A(z) := 1 + \frac{(q^2 - 1)(n + 1)}{d} z^{n+1-d} + \frac{(q^3 - 1)d - (q^2 - 1)(n + 1)}{d} z^{n+1}. \tag{11}
\]

Furthermore, the dual distance of the code is 3 when \( m > 1 \) and 4 when \( m = 1 \).

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

\[
(c_a + b1, \bar{c}),
\]

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

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

\[
\text{wt}((c_a + b1, \bar{c})) = \text{wt}(c_a + b1) = n + 1 - d.
\]

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

\[
\text{wt}((c_a + b1, \bar{c})) = \begin{cases} 
  n - d + 1 & \text{if } Z(a, b) = dN, \\
  n + 1 & \text{if } Z(a, b) = 0.
\end{cases}
\]

When \( a = 0 \) and \( b \neq 0 \), it is obvious that \( \text{wt}((c_a + b1, \bar{c})) = n + 1 \). We then deduce that \( \overline{C}_{(q,2,n)} \) has only nonzero weights \( n + 1 - d \) and \( n + 1 \). By Theorem 5, the minimum distance of \( \overline{C}_{(q,2,n)} \) is at least 3. The weight enumerator of \( \overline{C}_{(q,2,n)} \) is obtained by solving the first two Pless power moments (see also [6]).

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

\[
u = \frac{(q^3 - 1)d - (q^2 - 1)(n + 1)}{d}, \quad v = \frac{(q^2 - 1)(n + 1)}{d}.
\]

By (11), the weight enumerator of \( \overline{C}_{(q,2,n)} \) is \( A(z) = 1 + uz^{n+1-d} + vz^{n+1} \). It then follows from the MacWilliams Identity that the weight enumerator \( \overline{A}^\perp(z) \) of \( \overline{C}_{(q,2,n)}^\perp \) is given by

\[
q^3 A^\perp(z) = (1 + (q - 1)z)^{n+1} A \left( \frac{1 - z}{1 + (q - 1)z} \right) = (1 + (q - 1)z)^{n+1} + u(1 - z)^{n+1-d} (1 + (q - 1)z)^d + v(1 - z)^{n+1}. \tag{12}
\]

We have

\[
(1 + (q - 1)z)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} (q - 1)^i z^i \tag{13}
\]

and

\[
v(1 - z)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} (-1)^i vz^i. \tag{14}
\]
It is straightforward to prove that

\[
(u(1 - z)^{n+1-d}(1 + (q - 1)z))^{d} = \sum_{\ell=0}^{n+1} \left( \sum_{i+j=\ell} \left( \begin{array}{c} n+1-d \\ i \end{array} \right) \left( \begin{array}{c} d \\ j \end{array} \right) (-1)^{i}(q - 1)^{j} \right) u^{\ell}. 
\]

(15)

Combining (12), (13), (14) and (15), we obtain that

\[
q^{3} A_{1}^{\perp} = \left( \begin{array}{c} n+1 \\ 1 \end{array} \right) [(q - 1) - v] 
+ \left[ \left( \begin{array}{c} n+1-d \\ 0 \end{array} \right) \left( \begin{array}{c} d \\ 1 \end{array} \right) (-1)^{0}(q - 1)^{1} + \left( \begin{array}{c} n+1-d \\ 1 \end{array} \right) \left( \begin{array}{c} d \\ 0 \end{array} \right) (-1)^{1}(q - 1)^{0} \right] u 
= (n+1)[(q - 1) - v] + [d(q - 1) - (n+1-d)]u 
= 0.
\]

Combining (12), (13), (14) and (15) again, we get that

\[
q^{3} A_{2}^{\perp} = \left( \begin{array}{c} n+1 \\ 2 \end{array} \right) [(q - 1)^{2} + v] + \left( \begin{array}{c} n+1-d \\ 0 \end{array} \right) \left( \begin{array}{c} d \\ 2 \end{array} \right) (-1)^{0}(q - 1)^{2}u 
+ \left( \begin{array}{c} n+1-d \\ 1 \end{array} \right) \left( \begin{array}{c} d \\ 1 \end{array} \right) (-1)^{1}(q - 1)^{1}u + \left( \begin{array}{c} n+1-d \\ 2 \end{array} \right) \left( \begin{array}{c} d \\ 0 \end{array} \right) (-1)^{2}(q - 1)^{0}u 
= \left( \begin{array}{c} n+1 \\ 2 \end{array} \right) [(q - 1)^{2} + v] 
+ \left( \begin{array}{c} d \\ 2 \end{array} \right)(q - 1)^{2} - (n+1-d)d(q - 1) + \left( \begin{array}{c} n+1-d \\ 2 \end{array} \right) u 
= 0.
\]

Combining (12), (13), (14) and (15) the third time, we arrive at

\[
q^{3} A_{3}^{\perp} = \left( \begin{array}{c} n+1 \\ 3 \end{array} \right) [(q - 1)^{3} - v] 
+ \left[ \left( \begin{array}{c} n+1-d \\ 0 \end{array} \right) \left( \begin{array}{c} d \\ 3 \end{array} \right) (-1)^{0}(q - 1)^{3} + \left( \begin{array}{c} n+1-d \\ 1 \end{array} \right) \left( \begin{array}{c} d \\ 2 \end{array} \right) (-1)^{1}(q - 1)^{2} \right] u 
+ \left[ \left( \begin{array}{c} n+1-d \\ 2 \end{array} \right) \left( \begin{array}{c} d \\ 1 \end{array} \right) (-1)^{2}(q - 1)^{1} + \left( \begin{array}{c} n+1-d \\ 3 \end{array} \right) \left( \begin{array}{c} d \\ 0 \end{array} \right) (-1)^{3}(q - 1)^{0} \right] u 
= \left( \begin{array}{c} n+1 \\ 3 \end{array} \right) [(q - 1)^{3} - v] 
+ \left( \begin{array}{c} d \\ 3 \end{array} \right)(q - 1)^{3} - \left( \begin{array}{c} n+1-d \\ 1 \end{array} \right) \left( \begin{array}{c} d \\ 2 \end{array} \right)(q - 1)^{2} \right] u 
+ \left( \begin{array}{c} n+1-d \\ 2 \end{array} \right) \left( \begin{array}{c} d \\ 1 \end{array} \right)(q - 1) - \left( \begin{array}{c} n+1-d \\ 3 \end{array} \right) u. 
\]

It then follows that

\[
6q^{3} A_{3}^{\perp} = q^{6}d^{3} - 4q^{6}d^{2} + 5q^{6}d - 2q^{6} + q^{5}d^{3} - 3q^{5}d^{2} + 2q^{5}d 
- q^{4}d^{3} + 4q^{4}d^{2} - 5q^{4}d + 2q^{4} - q^{3}d^{3} + 3q^{3}d^{2} - 2q^{3}d 
= (d - 2)(d - 1)q^{3}(q^{2} - 1)(qd - q + d).
\]
Thus,
\[ A_3^\perp = \frac{(d - 2)(d - 1)(q^2 - 1)(qd - q + d)}{6}. \]

(16)

When \( m > 1 \), we have \( d > 3 \). In this case, by (16) we have \( A_3^\perp > 0 \). When \( m = 1 \), by (16) 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 \( \overline{C}_{(q, 2, n)} \) is projective, hence is associated with a maximal \((n + 1, d)\)-arc in \( PG(2, q) \).

\[ \square \]

\textbf{Theorem 7} If \( mk > 1 \), the supports of the codewords with weight \( n + 1 - d \) in \( \overline{C}_{(q, 2, n)} \) form a 2-design \( D \) with parameters
\[ 2 - \left( n + 1, n + 1 - d, \frac{(n + 1 - d)(n - d)}{d(d - 1)} \right). \]

\textbf{Proof} The supports of the codewords of weight \( n + 1 - d \) in \( \overline{C}_{(q, 2, n)} \) 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,
\[ \lambda = \frac{(n + 1 - d)(n - d)}{d(d - 1)}. \]

\[ \square \]

\textbf{Remark 8} We note that if \( M \) is a \( 3 \times (n + 1) \) generator matrix of the two-weight code \( \overline{C}_{(q, 2, n)} \) from Theorem 7, the columns of \( M \) label the points of a maximal \((n + 1, d)\)-arc \( A \) in \( PG(2, q) \), and the complementary design \( D \) 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 \( PG(2, q) \).

\textbf{Theorem 9} If \( m > 1 \), the supports of the codewords with weight 3 in \( \overline{C}_{(q, 2, n)}^\perp \) form a 2-design with parameters
\[ 2 - (n + 1, 3, d - 2). \]

\textbf{Proof} Let \( m > 1 \). By Theorem 6 the code \( \overline{C}_{(q, 2, n)}^\perp \) has minimum distance 3. It follows from the Assmus–Mattson theorem that the supports of the codewords of weight 3 in \( \overline{C}_{(q, 2, n)}^\perp \) form a 2-design. We then deduce from (11) that the number of blocks in this design is
\[ b^\perp = \frac{(d - 2)n(n + 1)}{6}. \]

Consequently, \( \lambda^\perp = d - 2 \).

\[ \square \]
Acknowledgements  This material is based upon work that was done while the first author was serving at the National Science Foundation. The research of Cunsheng Ding was supported by the Hong Kong Grants Council, Proj. No. 16300415. Vladimir Tonchev acknowledges support by NSA Grant H98230-16-1-0011. The authors wish to thank the reviewers for their helpful remarks and suggestions that improved the manuscript.

References

1. Abatangelo V., Larato B.: A characterization of Denniston’s maximal arcs. Geom. Dedic. 30, 197–203 (1989).
2. Assmus Jr. E.F., Mattson H.F.: New 5-designs. J. Combin. Theory 6, 122–151 (1969).
3. Barlotti A.: Sui \( \{k; n\} \)-archi di un piano lineare finito. Boll. Un. Mat. Ital. 11, 553–556 (1956).
4. Baumert L.D., McEliece R.J.: Weights of irreducible cyclic codes. Inf. Control 20, 158–175 (1972).
5. Ball S., Blokhuis A., Mazzocca F.: Maximal arcs in Desarguesian planes of odd order do not exist. Combinatorica 17, 31–41 (1997).
6. Calderbank R., Kantor W.W.: The geometry of two-weight codes. Bull. Lond. Math. Soc. 18, 97–122 (1986).
7. De Clerk F., De Winter S., Maes T.: A geometric approach to Mathon maximal arcs. J. Combin. Theory Ser. A 118, 1196–1211 (2011).
8. Delsarte P.: Two-Weight Linear Codes and Strongly Regular Graphs, Report R160. MBL Research Laboratory, Brussels (1971).
9. Denniston R.H.F.: Some maximal arcs in finite projective planes. J. Combin. Theory 6, 317–319 (1969).
10. Ding C., Yang J.: Hamming weights in irreducible cyclic codes. Discrete Math. 313, 434–446 (2013).
11. Hamilton N.: Some maximal arcs in derived dual Hall planes. Eur. J. Combin. 15, 525–532 (1994).
12. Hamilton N.: Some maximal arcs in Hall planes. J. Geom. 52, 101–107 (1995).
13. Hamilton N.: Some inherited maximal arcs in derived dual translation planes. Geom. Dedic. 55, 165–173 (1995).
14. Hamilton N.: Maximal arcs in finite projective planes and associated in projective planes, PhD thesis, The University of Western Australia (1995).
15. Hamilton N., Mathon R.: More maximal arcs in Desarguesian projective planes and their geometric structure. Adv. Geom. 3, 251–261 (2003).
16. Hamilton N., Mathon R.: On the spectrum of non-Denniston maximal arcs in PG(2, 2^h). Eur. J. Combin. 25, 415–421 (2004).
17. Hamilton N., Penttila T.: Groups of maximal arcs. J. Combin. Theory Ser. A 94, 63–86 (2001).
18. Hamilton N., Stoichev S.D., Tonchev V.D.: Maximal arcs and disjoint maximal arcs in projective planes of order 16. J. Geom. 67, 117–126 (2000).
19. Hirschfeld J.W.P.: Projective Geometries over Finite Fields, 2nd edn. Oxford University Press, Oxford (1998).
20. Mathon R.: New maximal arcs in Desarguesian planes. J. Combin. Theory Ser. A 97, 353–368 (2002).
21. Penttila T., Royle G.F., Simpson M.K.: Hyperovals in the known projective planes of order 16. J. Combin. Des. 4, 59–65 (1996).
22. Thas J.A.: Construction of maximal arcs and partial geometries. Geom. Dedic. 3, 61–64 (1974).
23. Thas J.A.: Construction of maximal arcs and dual ovals in translation planes. Eur. J. Combin. 1, 189–192 (1980).

Publisher’s Note  Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.