INFINITE FAMILIES OF 2-DESIGNS FROM TWO CLASSES OF BINARY CYCLIC CODES WITH THREE NONZEROS

XIAONI DU
College of Mathematics and Statistics, Northwest Normal University
Lanzhou, Gansu 730070, China
and
Guangxi Key Laboratory of Cryptography and Information Security
Guilin University of Electronic Technology
Guilin, Guangxi 541004, China

RONG WANG∗
College of Mathematics and Statistics, Northwest Normal University
Lanzhou, Gansu 730070, China

CHUNMING TANG
School of Mathematics and Information, China West Normal University
Nanchong, Sichuan 637002, China

QI WANG
Department of Computer Science and Engineering
Southern University of Science and Technology
Shenzhen, Guangdong 518055, China

(Communicated by Maosheng Xiong)

Abstract. Combinatorial $t$-designs have been an interesting topic in combinatorics for decades. It is a basic fact that the codewords of a fixed weight in a code may hold a $t$-design. Till now only a small amount of work on constructing $t$-designs from codes has been done. In this paper, we determine the weight distributions of two classes of cyclic codes: one related to the triple-error correcting binary BCH codes, and the other related to the cyclic codes with parameters satisfying the generalized Kasami case, respectively. We then obtain infinite families of $2$-designs from these codes by proving that they are both affine-invariant codes, and explicitly determine their parameters. In particular, the codes derived from the dual of binary BCH codes hold five 3-designs when $m = 4$.

1. Introduction

Let $P$ be a set of $v ≥ 1$ elements and $B$ be a set of $k$-subsets of $P$, where $k$ is a positive integer with $1 ≤ k ≤ v$. Let $t$ be a positive integer with $t ≤ k$. If every $t$-subset of $P$ is contained in exactly $λ$ elements of $B$, then we call the pair $D = (P, B)$ a $t$-$(v, k, λ)$ design, or simply a $t$-design. The elements of $P$ are called points, and...
those of $\mathcal{B}$ are referred to as blocks. We often denote the number of blocks by $b$ and a $t$-design is simple when there is no repeated block in $\mathcal{B}$. A $t$-design is called symmetric if $v = b$ and trivial if $k = t$ or $k = v$. Throughout this paper we study only simple $t$-designs with $t < k < v$. When $t \geq 2$ and $\lambda = 1$, a $t$-design is called a Steiner system. Clearly, the parameters of a $t$-$(v,k,\lambda)$ design are restricted by the following identity.

$$b \binom{k}{t} = \lambda \binom{v}{t}.$$  

The interplay between codes and $t$-designs has been ongoing for decades. On one hand, the incidence matrix of a $t$-design over any finite field can serve as a generator matrix of a linear code and much progress has been made (see [1, 5, 11, 12, 17, 18]). On the other hand, linear and nonlinear codes may hold $t$-designs. As a classical example, 4-designs and 5-designs with certain parameters were derived from binary and ternary Golay codes. Recently, Ding and Li [8] obtained infinite families of 2-designs from $p$-ary Hamming codes, ternary projective cyclic codes, binary codes with two zeros and their duals. They also obtained 3-designs from the extended codes of these codes and Reed-Muller codes. More recently, infinite families of 2-designs and 3-designs from some classes of binary linear codes with five weights were given by Ding [7]. For other constructions of $t$-designs, for example, see [3, 4, 15, 16].

The objective of this paper is to construct 2-designs from two classes of cyclic codes obtained from the triple-error correcting narrow-sense primitive BCH codes and the cyclic codes related to the generalized Kasami case, respectively. In the following, we will first present the weight distributions of these two classes of cyclic codes, and then explicitly determine the parameters of the derived 2-designs.

2. The classical construction of $t$-designs from affine-invariant codes

Throughout this paper, let $p = 2$, $m = 2s$, $\gcd(s,l) = d$ and $\gcd(s + l, 2l) = d'$, where both $s \geq 2$ and $1 \leq l \leq m - 1$ are positive integers with $l \neq s$. Let $\mathbb{F}_q$ denote the finite field with $q = 2^m$ elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. An $[n,k,d]$ linear code $C$ over $\mathbb{F}_2$ is a $k$-dimensional subspace of $\mathbb{F}_2^n$ with minimum Hamming distance $d$, and is cyclic if any cyclic shift of a codeword is another codeword of $C$. Any cyclic code $C$ can be expressed as $C = \langle g(x) \rangle$, where $g(x)$ is monic and has the least degree. The polynomial $g(x)$ is called the generator polynomial and $h(x) = (x^n - 1)/g(x)$ is referred to as the parity-check polynomial of $C$. If the generator polynomial $g(x)$ (resp. the parity-check polynomial $h(x)$) can be factored into a product of $r$ irreducible polynomials over $\mathbb{F}_p$, then $C$ is called a cyclic code with $r$ zeros (resp. $r$ nonzeros). The code with the generator polynomial $x^k h(x^{-1})$ is called the dual of $C$ and denoted by $C^\perp$.

Furthermore, we define the extended code of a code $C$ to be the code

$$\mathcal{C} = \{(c_0, c_1, \ldots, c_n) \in \mathbb{F}_2^{n+1} : (c_0, c_1, \ldots, c_{n-1}) \in C \text{ with } \sum_{i=0}^{n} c_i = 0\}.$$  

The support of a codeword $c$ is defined by

$$\text{Suppt}(c) = \{0 \leq i \leq n - 1 : c_i \neq 0\}.$$
Let \( A_i \) be the number of codewords with Hamming weight \( i \) in a code \( C \). The **weight enumerator** of \( C \) is defined by

\[
1 + A_1 z + A_2 z^2 + \ldots + A_n z^n.
\]

The sequence \( (1, A_1, \ldots, A_n) \) is called the **weight distribution** of the code \( C \). If \( |\{1 \leq i \leq n : A_i \neq 0\}| = w \), then we call \( C \) a \( w \)-weight code.

Let \( n = q - 1 \), and \( \alpha \) be a generator of \( \mathbb{F}_q^* \). For any \( i \) with \( 0 \leq i \leq n - 1 \), let \( M_i(x) \) denote the minimal polynomial of \( \alpha^i \) over \( \mathbb{F}_2 \). For any \( 2 \leq \delta \leq n \), the code \( C_{(p,n,\delta)} = \langle g(p,n,\delta,1) \rangle \) with

\[
g(p,n,\delta,1)(x) = \text{lcm}(M_1(x), M_2(x), \ldots, M_{\delta-1}(x)),
\]

where lcm denotes the least common multiple of the polynomials, is called a **narrow-sense primitive BCH code** with designed distance \( \delta \).

For each \( i \) with \( A_i \neq 0 \), let \( B_i \) denote the set of the supports of all codewords with weight \( i \) in \( C \), where the coordinates of a codeword are indexed by \( (0, 1, 2, \ldots, n-1) \). Let \( \mathcal{P} = \{0, 1, \ldots, n-1\} \). The pair \( (\mathcal{P}, B_i) \) could be a \( t-(n, i, \lambda) \) design for a certain positive \( \lambda \) [17].

There exist two classical approaches to obtain \( t \)-designs from linear codes. The first one is to employ the Assmus-Mattson Theorem given in [2], and the second one is to study the automorphism group of a linear code \( C \). If the permutation part of the automorphism group acts \( t \)-transitively on a code \( C \), then the code \( C \) holds \( t \)-designs [1, 15]. In the following, we will use the latter method to construct 2-designs.

We conclude this section by summarizing some known results on affine-invariant codes related to 2-designs.

The 2-adic expansion of each \( e \in \mathcal{P} \) is given by

\[
e = \sum_{i=0}^{m-1} e_i 2^i, \quad 0 \leq e_i \leq 1, \quad 0 \leq i \leq m - 1.
\]

For any \( r = \sum_{i=0}^{m-1} r_i 2^i \in \mathcal{P} \), we say that \( r \leq e \) if \( r_i \leq e_i \) for all \( 0 \leq i \leq m - 1 \). By definition, we have \( r \leq e \) if \( r \leq e \).

The set of coordinate permutations that map a code \( C \) to itself forms a group, which is referred to as the **permutation automorphism group** of \( C \) and denoted by \( PAut(C) \). We define the **affine group** \( GA_1(\mathbb{F}_q) \) by the set of all permutations

\[
\sigma_{a,b} : x \mapsto ax + b
\]

of \( \mathbb{F}_q \), where \( a \in \mathbb{F}_q^* \) and \( b \in \mathbb{F}_q \). An affine-invariant code is an extended cyclic code \( \mathcal{C} \) over \( \mathbb{F}_2 \) such that \( GA_1(\mathbb{F}_q) \leq PAut(\mathcal{C}) \) [9].

For any integer \( 0 \leq j < n \), the 2-cyclo-tomic coset of \( j \) modulo \( 2^m - 1 \) is defined by

\[
C_j = \{jp^i \pmod{2^m - 1} : 0 \leq i \leq \ell_j - 1\},
\]

where \( \ell_j \) is the smallest positive integer such that \( j \equiv jp^{\ell_j} \pmod{2^m - 1} \). Let \( g(x) = \prod_{j \in C_j} (x - \alpha^j) \), where \( j \) runs through some subset of representatives of the 2-cyclo-tomic cosets \( C_j \) modulo \( 2^m - 1 \). The set \( T = \bigcup_j C_j \) is called the **defining set** of \( C \), which is the union of these 2-cyclo-tomic cosets.

Affine-invariance is an important property of an extended primitive cyclic code, for which the following lemma presented by Kasami, Lin and Peterson [10] provides a sufficient and necessary condition by examining the defining set of the code.
Lemma 1. [10] Let $\overline{C}$ be an extended cyclic code of length $2^m$ over $\mathbb{F}_2$ with defining set $T$. The code $\overline{C}$ is affine-invariant if and only if whenever $e \in T$ then $r \in T$ for all $r \in P$ with $r \leq e$.

Lemma 2. [6] The dual of an affine-invariant code $\overline{C}$ over $\mathbb{F}_2$ of length $n+1$ is also affine-invariant.

The importance of affine-invariant codes is partly due to Theorem 3 which will be used together with Lemmas 1 and 2 to derive the existence of 2-designs.

Theorem 3. [6] For each $i$ with $A_i \neq 0$ in an affine-invariant code $\overline{C}$, the supports of the codewords of weight $i$ form a 2-design.

3. Two classes of cyclic codes and their $t$-designs

In this section, we introduce the main results on the weight distributions of two classes of cyclic codes and the corresponding 2-designs. Their proofs will be presented in the subsequent section. In the following, let $T_{\overline{C}}^m$ denote the trace function from $\mathbb{F}_{2^m}$ onto $\mathbb{F}_2$.

3.1. Results on the cyclic code derived from triple-error correcting BCH code. We define

$$\overline{C}_1^{+1} := \{ (T_{\overline{C}}^m(ax^5 + bx^3 + cx) + h)_{x \in \mathbb{F}_2} : a, b, c \in \mathbb{F}_q, h \in \mathbb{F}_2 \},$$

where $C_1$ is the cyclic code of length $n$ with the parity-check polynomial $M_1(x)M_2(x)M_3(x)$. It is easily seen that $C_1^+$ is a BCH code with minimum distance $d \geq \delta = 7$. Note that for $C_1^+$, we only discuss the case of $m$ even since the complement case for $m$ odd has been studied in [7].

The following two theorems constitute the first part of our main results in the present paper.

Theorem 4. Let $s \geq 3$. The weight distributions of the code $\overline{C}_1^{+1}$ over $\mathbb{F}_2$ with length $n+1$ and $\dim(\overline{C}_1^{+1}) = 3m+1$ are given in Table 1.

Note that the codes defined in (2) are eight-weight.

Theorem 5. Let $s \geq 3$ be a positive integer. Then the supports of the codewords of weight $i$ with $A_i^{+1} \neq 0$ in $\overline{C}_1^{+1}$ form a 2-design. Moreover, let $P = \{0, 1, \ldots, 2^m -
Let \( \mathcal{C}_1 \) be the set of the supports of the codewords of \( \overline{C}_1^\perp \) with weight \( i \), where \( A_i^\perp \neq 0 \). Then \( \overline{C}_1^\perp \) holds \(-2^m, i, \lambda\) designs for the following pairs:

- \((i, \lambda) = (2^{2s-1}, (29 \times 2^{6s-5} - 33 \times 2^{4s-5} + 17 \times 2^{2s-3} - 2)(2^{2s-1} - 1) / (2^{2s} - 1)) \).
- \((i, \lambda) = (2^{2s-1} - 2^{s-1}, \frac{11}{15} \times 2^{2s-1} - (3 \times 2^{4s} + 5 \times 2^{2s} - 8)(2^{2s-1} - 2^{s-1} - 1) / (2^{s+1}) \).
- \((i, \lambda) = (2^{2s-1} - 2^{s-1} - 1, \frac{11}{15} \times 2^{2s-1} - (3 \times 2^{4s} + 5 \times 2^{2s} - 8)(2^{2s-1} - 2^{s-1} - 1) / (2^{s+1}) \).
- \((i, \lambda) = (2^{2s-1} - 2^{s+1}, \frac{11}{15} \times 2^{2s-1} - (3 \times 2^{4s} + 5 \times 2^{2s} - 8)(2^{2s-1} - 2^{s+1} - 1) / (2^{s+1}) \).
- \((i, \lambda) = (2^{2s-1} + 2^{s+1} - 1, \frac{1}{15} \times 2^{s-1} - (3 \times 2^{4s} + 5 \times 2^{2s} - 1)(2^{2s-1} - 2^{s+1} - 1) / (2^{s+1}) \).
- \((i, \lambda) = (2^{2s-1} - 2^{s+1} + 1, \frac{1}{15} \times 2^{s-1} - (3 \times 2^{4s} + 5 \times 2^{2s} - 1)(2^{2s-1} - 2^{s+1} - 1) / (2^{s+1}) \).

The following Examples 1 and 2 from Magma program confirm the main results in Theorems 4 and 5.

**Example 1.** If \( s = 3 \), then the code \( \overline{C}_1^\perp \) has parameters \([64, 19, 16]\) and weight enumerator \( 1 + 17136z^{16} + 37632z^{24} + 107520z^{28} + 233478z^{32} + 107520z^{36} + 37632z^{40} + 252z^{48} + z^{64} \). It gives \(-2(64, i, \lambda)\) designs with the following pairs \((i, \lambda)\):

\[
(16, 15), (24, 5152), (28, 20160), (32, 57443), (36, 33600), (40, 14560), (48, 141).
\]

**Example 2.** If \( s = 4 \), then the code \( \overline{C}_1^\perp \) has parameters \([256, 25, 96]\) and weight enumerator \( 1 + 17136z^{96} + 2437120z^{112} + 6754304z^{120} + 15137310z^{128} + 6754304z^{136} + 2437120z^{144} + 17136z^{160} + z^{256} \).

It is worth noting that, for \( m = 4 \), the code \( \overline{C}_1^\perp \) has parameters \([16, 11, 4]\) and weight enumerator \( 1 + 140z^4 + 448z^8 + 870z^{10} + 448z^{12} + 140z^{12} + z^{16} \). It forms \(3-(16, i, \lambda)\) designs with the following pairs \((i, \lambda)\):

\[
(4, 1), (6, 16), (8, 87), (10, 96), (12, 55).
\]

### 3.2. Results on the cyclic code related to the generalized Kasami case

We define

\[
\overline{C}_2^\perp := \{(T \alpha^x)^{d+1} + (b + c \alpha^{x^d+1}) + h)_{x \in F_q} : a \in F_2, b, c \in F_q, h \in F_2\},
\]

where \( C_2 \) is the cyclic code of length \( n \) with the parity-check polynomial \( M_1(x)M_{d+1}(x) \).

Note that \( \overline{C}_2^\perp \) is the dual of the cyclic code of the parameters satisfying the generalized Kasami case.

For \( \overline{C}_2^\perp \), we present the main results in the following two theorems.

**Theorem 6.** Let \( 1 \leq l \leq m - 1 \). The weight distributions of the code \( \overline{C}_2^\perp \) over \( F_2 \) with length \( n + 1 \) and \( \dim(\overline{C}_2^\perp) = \frac{5m}{2} + 1 \) are given in Tables 2 and 3.

Note that the code are six-weight when \( d = d' \) and eight-weight when \( d' = 2d \).

**Theorem 7.** Let \( s \geq 2 \) be a positive integer. Then the supports of the codewords of weight \( i \) with \( A_i^\perp \neq 0 \) in \( \overline{C}_2^\perp \) give a 2-design. Moreover, let \( \mathcal{P} = \{0, 1, \ldots, 2^m - 1\} \).
and \( \mathcal{B}_i \) be the set of supports of the codewords of \( \overline{C}_{2^{d'}}^\perp \) with weight \( i \), where \( \overline{A}_{d'}^\perp \neq 0 \). Then \( \overline{C}_{2^{d'}}^\perp \) holds \( 2 \cdot (2^m, i, \lambda) \) designs for the following pairs:

1) if \( d' = d \),

\[ (i, \lambda) = \left( 2^{2s-1} - 2^{s-1}, 2^{s-1} \left( 2^{2s-1} - 2^{s-1} - 1 \right) (2^{2s} - 2^{s-1} - 1) (2^{2s} + 2^{s-2d} + 2^{2d}) (2^{2s} + 2^{s-2d} + 2^{2d}) (2^{2s} - 2^{s-2d} + 2^{2d} + 2^{2s}) (2^{2s} - 2^{s-2d} + 2^{2d} + 2^{2s}) \right) / (2^{2d} - 1) \]

2) if \( d' = 2d \),

\[ (i, \lambda) = \left( 2^{2s-1} - 2^{s-1}, 2^{s-1} \left( 2^{2s-1} - 2^{s-1} - 1 \right) (2^{2s} - 2^{s-1} - 1) (2^{2s} - 2^{s-2d} + 2^{2d} + 2^{2s} - 2^{s-2d} + 2^{2d} + 2^{2s}) (2^{2s} - 2^{s-2d} + 2^{2d} + 2^{2s}) \right) / (2^{2d} - 1) \]
If Example 3. Let $\mathcal{C}$ be an $[n, k, d]$ binary linear code, then $\overline{\mathcal{C}}^\perp$ has parameters $[n + 1, k + 1, d^\perp - 1]$. Furthermore, $\overline{\mathcal{C}}^\perp$ has only even-weight codewords, and all the nonzero weights in $\overline{\mathcal{C}}^\perp$ are the following:

$$w_1, w_2, \ldots, w_t; n + 1 - w_1, n + 1 - w_2, \ldots, n + 1 - w_t; n + 1,$$

where $w_1, w_2, \ldots, w_t$ denote all the nonzero weights of $\mathcal{C}$.

The following Pless power moments given in [9] are notable variations of the MacWilliams identities, which is a fundamental result about weight distributions and is a set of linear relations between the weight distributions of $\mathcal{C}$ and $\overline{\mathcal{C}}^\perp$.

**Lemma 8.** [7] Let $\mathcal{C}$ be an $[n, k, d]$ binary linear code, then $\overline{\mathcal{C}}^\perp$ has parameters $[n + 1, k + 1, d^\perp - 1]$. Furthermore, $\overline{\mathcal{C}}^\perp$ has only even-weight codewords, and all the nonzero weights in $\overline{\mathcal{C}}^\perp$ are the following:

$$w_1, w_2, \ldots, w_t; n + 1 - w_1, n + 1 - w_2, \ldots, n + 1 - w_t; n + 1,$$

where $w_1, w_2, \ldots, w_t$ denote all the nonzero weights of $\mathcal{C}$.

**Lemma 9.** [9] Let $A_i$ and $A_i^\perp$ denote the number of code vectors of weight $i$ in a code $\mathcal{C}$ and $\overline{\mathcal{C}}^\perp$, respectively. If $A_i^\perp = 0$ for $0 \leq i \leq 6$, then the first seven Pless
The following lemma given by Luo, Tang and Wang [14], gives the weight distributions of the cyclic codes related to the generalized Kasami case.

**Lemma 10.** [14] The weight distributions of $C_2$ are given in Tables 4 and 5.

### Table 4. The weight distribution of $C_2$ when $d' = d$

| Weight | Multiplicity |
|--------|--------------|
| $2^{2s-1} - 2s-1$ | 1 |
| $2^{2s-1} + 2s-1$ | $2^{s-1}(2^{2s} - 1)(2^{2s} - 2^{(s-d)} - 2^{s-d} + 2^{s-d} - 1)/(2^{2d} - 1)$ |
| $2^{2s-1} + 2^{s+d-1}$ | $2^{s-1}(2^{s} - 1)^2(2^{2s} - 2^{s-d} - 2^{s-d} + 2^{2d})/(2^{2d} - 1)$ |
| $2^{2s-1} + 2^{s+d-1}$ | $2^{s-d-1}(2^{s+d} - 1)(2^{s} - 1)(2^{s-d} - 1)/(2^{2d} - 1)$ |
| $2^{2s-1}$ | $(2^{3s-d} - 2^{2(s-d)} + 1)/(2^{2s} - 1)$ |

### Table 5. The weight distribution of $C_2$ when $d' = 2d$

| Weight | Multiplicity |
|--------|--------------|
| $2^{2s-1} - 2s-1$ | 1 |
| $2^{2s-1} + 2s-1$ | $2^{s+3d-1}(2^{2s-1})(2^{2s} - 2^{s-d} - 2^{s-d} + 2^{s-d} + 1)/(2^{2d} + 1)$ |
| $2^{2s-1} + 2^{s+d-1}$ | $2^{s-1}(2^{2s} - 1)(2^{s} + 2^{s-d} + 2^{s-d} + 1)/(2^{2d} + 1)^2$ |
| $2^{2s-1} + 2^{s+d-1}$ | $2^{s-1}(2^{2s} - 1)/(2^{s} + 2^{s-d} + 2^{s-d} + 1)/(2^{2d} - 1)/(2^{2d} + 1)^2$ |
| $2^{2s-1}$ | $(2^{2s} - 1)/(2^{s-d} - 2^{s-d} + 2^{s-d} - 2^{s-d} + 2^{s-d} + 2^{s-d} + 2^{s-d} + 2^{s-d} + 1)$ |
| $2^{2s-1} + 2^{s+d-1}$ | $(2^{2s} - 1)/(2^{s-d} - 1)/(2^{s-d} - 1)/(2^{s-d} - 1)/(2^{s-d} - 1)$ |

The following lemma given by Luo, Tang and Wang [14], gives the weight distributions of the cyclic codes related to the generalized Kasami case.

4.2. Quadratic forms. To determine the parameters of the code $C_1^{m+1}$ defined in Eq. (2), we introduce the following function.

$$S(a, b, c) = \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}_m^a(ax^3 + bx^3 + cx)}, \quad a, b, c \in \mathbb{F}_q$$
The first tool to determine the values of exponential sums $S(a, b, c)$ is quadratic forms over $F_2$. Let $H$ be an $m \times m$ matrix over $F_2$. For the quadratic form

$$F : \mathbb{F}_2^m \to \mathbb{F}_2, \quad F(X) = XHX^T \quad (X = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_2^m),$$

we define $r_F$ of $F$ to be the rank of $H$ over $\mathbb{F}_2$.

The field $\mathbb{F}_q$ is a vector space over $\mathbb{F}_2$ with dimension $m$. We fix a basis $v_1, v_2, \ldots, v_m$. Thus each $x \in \mathbb{F}_q$ can be uniquely expressed as

$$x = x_1 v_1 + x_2 v_2 + \ldots + x_m v_m \quad (x_i \in \mathbb{F}_2).$$

Then we have the following $\mathbb{F}_2$-linear isomorphism $\mathbb{F}_q \to \mathbb{F}_2^m$:

$$x = x_1 v_1 + x_2 v_2 + \ldots + x_m v_m \mapsto X = (x_1, \ldots, x_m).$$

With the isomorphism, a function $f : \mathbb{F}_q \to \mathbb{F}_2$ induces a function $F : \mathbb{F}_2^m \to \mathbb{F}_2$ where for all $X = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$, $F(X) = f(x)$ where $x = x_1 v_1 + x_2 v_2 + \ldots + x_m v_m$. In this way, the function $f(x) = \text{Tr}_1^m(wx)$ for $w \in \mathbb{F}_q$ induces a linear form

$$F(X) = \sum_{i=1}^m \text{Tr}_1^m(wv_i)x_i = A_wX^T,$$

where $A_w = (\text{Tr}_1^m(wv_1), \ldots, \text{Tr}_1^m(wv_m))$.

For $(a, b, c) \in \mathbb{F}_q^3$, to determine the value of

$$S(a, b, c) = \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}_1^m(ax^5 + bx^3 + cx)} = \sum_{X \in \mathbb{F}_2^m} (-1)^{XH_{a,b}X^T + A_cX^T},$$

where $XH_{a,b}X^T$ is the quadratic form derived from $f_{a,b}(x) = \text{Tr}_1^m(ax^5 + bx^3)$ for $a, b \in \mathbb{F}_q$, we need to determine the rank of $H_{a,b}$ over $\mathbb{F}_2$. To this end, we have the following result.

**Lemma 11.** For $(a, b) \in \mathbb{F}_q^2/\{(0, 0)\}$, let $r_{a,b}$ be the rank of $H_{a,b}$. Then $r_{a,b} = m$, $m - 2$, or $m - 4$.

**Proof.** It is well known that the rank of the quadratic form $F(X)$ is defined as the codimension of the $\mathbb{F}_2$-vector space

$$V = \{x \in \mathbb{F}_q : f(x + y) - f(x) - f(y) = 0 \text{ for all } y \in \mathbb{F}_q\}.$$ 

The cardinality of $V$ is $|V| = 2^{m-r_F}$, where $r_F$ is the rank of $f(x)$.

The definition of the function $f_{a,b}(x)$ leads to

$$f_{a,b}(x + y) - f_{a,b}(x) - f_{a,b}(y) = \text{Tr}_1^m((ax^4 + bx^2 + a^2x^{m-2} x^2 + b^{2m-1} x^{m-1})y).$$

Let

$$\Phi_{(a,b)}(x) = ax^4 + bx^2 + a^2x^{m-2}x^2 + b^{2m-1}x^{m-1}.$$ 

Then $\Phi_{(a,b)}(x) = 0$ has $2^{m-r_{a,b}}$ solutions in $\mathbb{F}_q$. On the other hand, since $\Phi_{(a,b)}(x)$ is a 2-linearized polynomial, then the set of the zeros to $\Phi_{(a,b)}(x) = 0$ is equivalent to that of

$$a^4x^{16} + b^4x^8 + bx^2 + ax = 0$$

in $\mathbb{F}_q$ and forms an $\mathbb{F}_2$-vector space. Since $r_{a,b}$ is even, $r_{a,b} = m, m - 2, m - 4$. We then complete the proof.  

The following result, which was proved in [13], will be used in Section 4.3.
Lemma 12. [13] For the fixed quadratic form defined in (5), the value distribution of
\[ \sum_{X \in \mathbb{F}_2^n} (-1)^{F(X)+A_c X^T} \]
is 0, $2^{m-r}$, or $-2^{m-r}$, when $A_c$ runs through $\mathbb{F}_2^m$.

4.3. Proofs of the main results. Now we are ready to give the proofs of our main results. We begin this subsection by proving the weight distribution of the code $C_1^{\perp}$ given in Theorem 4.

Proof of Theorem 4. For each nonzero codeword $c(a,b,c) = (c_0, \ldots, c_n)$ in $C_1$, the Hamming weight of $c(a,b,c)$ is
\[ w_H(c(a,b,c)) = |\{i : 0 \leq i \leq n-1, c_i \neq 0\}| = n - \sum_{i=0}^{n-1} y \text{Tr}_1^m(a a^{3i} + b a^{3i+1} + c a^i) \]
is $2^{s-1}, 2^{s-1} - 2^s, 2^{s-1} - 2^s, 2^{s-1} + 2^s, 2^{s-1} - 2^{s+1}, 2^{s-1} + 2^{s+1}$. By Lemmas 11-12 and (6), we have that the Hamming weight of $c(a,b,c)$ is $2^{s-1}, 2^{s-1} - 2^s, 2^{s-1} + 2^s, 2^{s-1} - 2^{s+1}, 2^{s-1} + 2^{s+1}$.

Plugging these values to the Pless power moments given by Lemma 9 and after tedious calculations, we obtain
\[ A_{2^{s-1}} = 29 \times 2^{6s-6} - 33 \times 2^{4s-6} + 17 \times 2^{2s-4} - 1, \]
\[ A_{2^{s-1} - 2^s} = \frac{1}{15}(3 \times 2^{6s} + 3 \times 2^{4s} + 5 \times 2^{4s} + 5 \times 2^{3s} - 2^{2s+3} - 2^s + 1), \]
\[ A_{2^{s-1} + 2^s} = \frac{1}{15}(3 \times 2^{6s} + 3 \times 2^{4s} + 5 \times 2^{4s} - 5 \times 2^{3s} - 2^{2s+3} + 2^s + 1), \]
\[ A_{2^{s-1} - 2^s} = \frac{7}{3} \times 2^{3s-4}(2^{3s-1} + 2^s - 2^{s-1} - 1), \]
\[ A_{2^{s-1} + 2^s} = \frac{7}{3} \times 2^{3s-4}(2^{3s-1} + 2^s - 2^{s-1} + 1), \]
\[ A_{2^{s-1} - 2^{s+1}} = \frac{1}{15} \times 2^{s-3}(2^{3s-4} + 2^{4s-2} - 5 \times 2^{3s-4} - 5 \times 2^{2s-2} + 2^s - 2^s + 1), \]
\[ A_{2^{s-1} + 2^{s+1}} = \frac{1}{15} \times 2^{s-3}(2^{3s-4} - 2^{4s-2} - 5 \times 2^{3s-4} + 5 \times 2^{2s-2} + 2^s - 2^s - 1). \]
The desired conclusion then follows from Lemma 8. Thus the proof is completed. 

Then we prove the affine-invariance of the code $\overrightarrow{C_1^{\perp}}$.

Lemma 13. The extended codes $\overrightarrow{C_1^{\perp}}$ and $\overrightarrow{C_2^{\perp}}$ are affine-invariant.
Proof. We will prove the conclusion with Lemma 1. The defining set \( T \) of the cyclic code \( C_1^{-1} \) is \( T = C_1 \cup C_3 \cup C_5 \). Since \( 0 \not\in T \), the defining set \( \overline{T} \) of \( C_1^{-1} \) is given by \( \overline{T} = C_1 \cup C_3 \cup C_5 \cup \{0\} \). Let \( e \in \overline{T} \) and \( r \in P \). Assume that \( e \preceq s \). We need to prove that \( r \in \overline{T} \) by Lemma 1.

If \( r = 0 \), then obviously \( r \in \overline{T} \). Consider now the case \( r > 0 \). If \( e \in C_1 \), then the Hamming weight \( wt(e) = 1 \). Since \( r \preceq e \), \( wt(r) = 1 \). Consequently, \( r \in C_1 \subset \overline{T} \). If \( e \in C_3 \cup C_5 \), then the Hamming weight \( wt(e) = 2 \). Since \( r \preceq e \), either \( wt(r) = 1 \) or \( r = e \). In both cases, \( r \in \overline{T} \). The desired conclusion then follows from Lemma 1.

Similarly, we can prove that \( \overline{C_2^{-1}} \) is affine-invariant.

Thus we complete the proof.

Proof of Theorem 5. From the relation of \( \overline{C_1^{-1}} \) and \( \overline{C_1^{-1}} \), by Lemmas 2 and 13, we have \( \overline{C_1^{-1}} \) is affine-invariant. Then \( \overline{C_1^{-1}} \) holds 2-designs by Theorem 3.

Moreover, the number of supports of all codewords with weight \( i \neq 0 \) in the code \( \overline{C_1^{-1}} \) is equal to \( A_i^{-1} \) for each \( i \), where \( A_i^{-1} \) is given in Table 1. Then the desired conclusions follow from Eq.(1). Thus, we complete the proof.

From all the above, we have finished the proof of the results related to \( \overline{C_1^{-1}} \).

Now we prove Theorems 6 and 7 related to \( \overline{C_2^{-1}} \).

Proof of Theorem 6. The desired conclusion follows directly from Lemmas 8 and 10.

Proof of Theorem 7. The proof is similar to that of Theorem 5, thus is omitted here.

5. Conclusion

In this paper, we determined the weight distributions of two classes of binary cyclic codes. One is derived from the triple-error correcting BCH code and the other is from cyclic codes related to the generalized Kasami case. We proved that both classes of linear codes hold 2-designs and explicitly computed their parameters.

In particular, we get five 3-designs in \( \overline{C_1^{-1}} \) when \( m = 4 \).

Acknowledgments

The authors would like to thank the anonymous referees for their helpful comments and suggestions, which have greatly improved the presentation and quality of this paper.

References

[1] E. F. Assmus, Jr. and J. D. Key, Designs and Their Codes, volume 103 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 1992.
[2] E. F. Assmus, Jr. and H. F. Mattson, Jr, New 5-designs, J. Combinatorial Theory, 6 (1969), 122–151.
[3] T. Beth, D. Jungnickel and H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1986.
[4] C. J. Colbourn and R. Mathon, Steiner systems, In Handbook of Combinatorial Designs, Second Edition, pages 128–135, Chapman and Hall/CRC, 2006. https://www.researchgate.net/publication/329786723.
[5] C. Ding, Codes from Difference Sets, World Scientific, 2015.
[6] C. Ding, *Designs from Linear Codes*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2019.

[7] C. Ding, Infinite families of 3-designs from a type of five-weight code, *Des. Codes Cryptogr.*, **86** (2018), 703–719.

[8] C. Ding and C. Li, Infinite families of 2-designs and 3-designs from linear codes, *Discrete Math.*, **340** (2017), 2415–2431.

[9] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[10] T. Kasami, S. Lin and W. W. Peterson, Some results on cyclic codes which are invariant under the affine group and their applications, *Information and Control*, **11** 1967, 475–496.

[11] G. T. Kennedy and V. Pless, A coding-theoretic approach to extending designs, *Discrete Math.*, **142** (1995), 155–168.

[12] J.-L. Kim and V. Pless, Designs in additive codes over $GF(4)$, *Des. Codes Cryptogr.*, **30** (2003), 187–199.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[14] J. Luo, Y. Tang and H. Wang, Cyclic codes and sequences: The generalized Kasami case, *IEEE Trans. Inform. Theory*, **56** (2010), 2130–2142.

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes, I*, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[16] C. Reid and A. Rosa, Steiner systems $S(2,4,v)$-a survey, *The Electronic Journal of Combinatorics*, **DS18** (2010), 1–34. https://www.researchgate.net/publication/266996333.

[17] V. D. Tonchev, Codes and designs, In V. Pless and W. C. Huffman, editors, *Handbook of Coding Theory, Vol. I, II*, pages 1229–1267. North-Holland, Amsterdam, 1998. https://www.researchgate.net/publication/268549395.

[18] V. D. Tonchev, Codes, In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, Discrete Mathematics and its Applications (Boca Raton), pages xxii+984. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

Received for publication May 2020.

E-mail address: ymldxn@126.com
E-mail address: rongw113@126.com
E-mail address: tangchunmingmath@163.com
E-mail address: wangqi@sustech.edu.cn