Gold type codes of higher relative dimension

Chunlei Liu∗†

Abstract

Let $m, d, e, k$ be fixed positive integers such that

$$e = (m, d) = (m, 2d), \quad 2 \leq k \leq \frac{m + e}{2e}.$$ 

Let $s$ be a fixed maximum-length binary sequence of length $2^m - 1$. Let $(s_1, s_2, \cdots, s_{k-1})$ be a system of circular decimations of $s$ whose decimation factors are respectively

$$2^d + 1, 2^{2d} + 1, \cdots, 2^{(k-1)d} + 1,$$

or respectively

$$2^d + 1, 2^{3d} + 1, \cdots, 2^{(2k-3)d} + 1,$$

or respectively

$$2^{(m-e)d} + 1, 2^{(m-3e)d} + 1, \cdots, 2^{(m-3e-k)d} + 1.$$ 

Then $s_1, \cdots, s_{k-1}$ are maximum-length binary sequences of length $2^m - 1$. Let $C$ be the $\mathbb{F}_2$-vector space generated by all circular shifts of $s, s_1, \cdots, s_{k-1}$. Then $C$ has an $\mathbb{F}_{2^m}$-vector space structure, and is of dimension $k$ over $\mathbb{F}_{2^m}$. When $k = 2$, $C$ is the Gold code. So we regard $C$ as a Gold type code of relative dimension $k$. The DC component distribution of $C$ is explicitly calculated out in the present paper.

Key phrases: Gold code, cyclic code, alternating form

MSC: 94B15, 11T71.

1 INTRODUCTION

Let $q$ be a prime power, and $C$ an $[n, k]$-linear code over $\mathbb{F}_q$. The weight of a codeword $c = (c_0, c_1, \cdots, c_{n-1})$ of $C$ is defined to be

$$\text{wt}(c) = \# \{ 0 \leq i \leq n-1 \mid c_i \neq 0 \}.$$ 

For each $i = 0, 1, \cdots, n$, define

$$A_i = \# \{ c \in C \mid \text{wt}(c) = i \}.$$ 

∗Dept. of math., Shanghai Jiao Tong Univ., Sahanghai 200240, China, clliu@sjtu.edu.cn.
†Dengbi Technologies Cooperation Limited., Yichun 336099, China, 714232747@qq.com.
The sequence \((A_0, A_1, \cdots, A_n)\) is called the weight distribution of \(\mathcal{C}\). Given a linear code \(\mathcal{C}\), it is challenging to determine its weight distribution. The weight distribution of Gold codes was determined by Gold [G66]. The weight distribution of Kasami codes was determined by Kasami [K66]. The weight enumerators of Gold type and Kasami type codes of higher relative dimension were determined by Berlekamp [Ber] and Kasami [K71]. The weight distribution of the \(p\)-ary analogue of Gold codes was determined by Trachtenberg [Tr]. The weight distribution of the circular decimation of the \(p\)-ary analogue of Gold codes with decimation factor 2 was determined by Feng-Luo [FL]. The weight distribution of the \(p\)-ary analogue of Gold type codes of relative dimension 3 was determined by Zhou-Ding-Luo-Zhang [ZDLZ]. The weight distribution of the circular decimation with decimation factor 2 of the \(p\)-ary analogue of Gold type codes of relative dimension 3 was determined by Zheng-Wang-Hu-Zeng [ZWHZ]. The weight distribution of (the \(p\)-ary analogue of) Kasami type codes of maximum relative dimension was determined by Li-Hu-Feng-Ge [LHFG]. The weight distribution of the \(p\)-ary analogue of Gold type codes of higher relative dimension was determined by Schmidt [Sch]. The weight distribution of some other classes of cyclic codes was determined in the papers [AL], [BEW], [BMC], [BMC10], [BMY], [DE], [DLMZ], [DY], [FE], [FM], [KL], [LF], [LHFG], [LN], [LYL], [LTW], [MCE], [MCG], [MO], [MR], [MY], [MZLF], [RP], [SC], [VE], [WTQYX], [XI], [XII2], [YCD], [YXDL] and [ZHJYC].

Let \(m, d, e, k\) be fixed positive integers such that

\[ e = (m, d) = (m, 2d), \quad 2 \leq k \leq \frac{m + e}{2e}. \]

Let \(s\) be a fixed maximum-length binary sequence of length \(2^m - 1\). Let \((s_1, s_2, \cdots, s_{k-1})\) be a system of circular decimations of \(s\) whose decimation factors are respectively

\[ 2^d + 1, 2^{2d} + 1, \cdots, 2^{(k-1)d} + 1, \]

or respectively

\[ 2^d + 1, 2^{3d} + 1, \cdots, 2^{(2k-3)d} + 1, \]

or respectively

\[ 2^d + 1, 2^{(m+2e)d} + 1, \cdots, 2^{(m+2e-k)d} + 1. \]

Then \(s_1, \cdots, s_{k-1}\) are maximum-length binary sequences of length \(2^m - 1\). Let \(\mathcal{C}\) be the \(\mathbb{F}_2\)-vector space generated by all circular shifts of \(s, s_1, \cdots, s_{k-1}\). If \(d = e = 1\), then \(\mathcal{C}\) is the code studied by Berlekamp [Ber] and Kasami [K71]. Let \(\{\overrightarrow{a}\}\) be the system

\[ Q_{\overrightarrow{a}}(x) = \text{Tr}_{\mathbb{F}_2^m / \mathbb{F}_2^n}(a_0 x) + \sum_{j=1}^{k-1} \text{Tr}_{\mathbb{F}_2^m / \mathbb{F}_2^n}(a_j x^{2^j + 1}), \quad \overrightarrow{a} \in \mathbb{F}_2^k, \]

or the system

\[ Q_{\overrightarrow{a}}(x) = \text{Tr}_{\mathbb{F}_2^m / \mathbb{F}_2^n}(a_0 x) + \sum_{j=1}^{k-1} \text{Tr}_{\mathbb{F}_2^m / \mathbb{F}_2^n}(a_j x^{2^{(2j-1)} + 1}), \quad \overrightarrow{a} \in \mathbb{F}_2^k, \]
or the system
\[ Q_a(x) = \text{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2} (a_0 x) + \sum_{j=1}^{k-1} \text{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2} (a_j x^{2^j - 1} + 1), \ a \in \mathbb{F}_{2^m}^k. \]

Then
\[ C = \{ c_{\alpha} \mid \alpha \in \mathbb{F}_{2^m}^k \}, \]
where \( c_{\alpha} = (\text{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2} (Q_a(\pi^i)))_{i=0}^{2^m - 2} \) with \( \pi \) being a primitive element of \( \mathbb{F}_{2^m} \). The correspondence \( \alpha \mapsto c_{\alpha} \) defines an \( \mathbb{F}_{2^m} \)-vector space structure on \( C \), and \( C \) is of dimension \( k \) over \( \mathbb{F}_{2^m} \). When \( k = 2 \), \( C \) is the Gold code. So we call \( C \) a Gold type code of relative dimension \( k \).

One can prove the following.

**Theorem 1.1** If \( c \in C \) is nonzero, then
\[ \text{DC}(c) \in \{-1, -1 + \pm 2 \frac{m-e}{2} i^j \varepsilon \mid j = 0, 1, 2, \ldots, k - 2\}, \]
where
\[ \text{DC}(c) = 2^m - 1 - 2\text{wt}(c) = \sum_{i=0}^{2^m - 2} (-1)^i \]
is the DC component of \( c = (c_0, c_1, \ldots, c_{2^m-2}) \in C \).

The present paper is concerned with the frequencies
\[ \alpha_{r,\varepsilon} = \# \{ 0 \neq c \in C \mid \text{DC}(c) = -1 + \varepsilon 2^{m-\frac{m-e}{2}} \}, \ r = 0, 2, 4, \ldots, \frac{m-e}{e}. \tag{1} \]

The main result of the present paper is the following.

**Theorem 1.2** For each \( j = 0, 1, \ldots, k - 2 \), and for each \( \varepsilon = \pm 1 \), we have
\[ \alpha_{m-e-2i,\varepsilon} = \frac{1}{2} (2^{m-e-2i} + \varepsilon 2^{m-\frac{m-e}{2}}) \sum_{j=i}^{k-2} (1^{j-i} 4^k i^{(j-i)} \left( \frac{m-e}{2} \right) i^{4^j} (m-2^j) - 1), \]
where \( \left( \frac{i}{j} \right)_q \) is a Gaussian binomial coefficient.

From the above theorem one can deduce the following.

**Theorem 1.3** We have
\[ \# \{ c \in C \mid \text{DC}(c) = -1 \} \]
\[ = 2^{mk} - 1 - \sum_{u=0}^{k-2} (-1)^u 2^{-e(u+1)^2} (2^{m(k-u)} - 2^m \prod_{j=0}^{u-1} (2^{m-2^j+1})) \]
\[ \approx 2^{mk} (1 - \sum_{u=0}^{k-2} (-1)^u 2^{-e(u+1)^2}). \]

If \( d = e = 1 \), then the weight enumerator of \( C \) is determined by Berlekamp [Ber] and Kasami [K71]. However, some extra calculations are needed to explicitly write out the coefficients of the weight enumerators in [Ber,K71].
2 ENTERING BILINEAR FORMS I

In this section we shall prove Theorem 1.1.

Note that
\[ 1 + DC(\bar{a}) = \sum_{x \in \mathbb{F}_{2m}} (-1)^{\text{Tr}_{\mathbb{F}_{2} / \mathbb{F}_{2}}(Q_{\bar{a}}(x))}. \]  

(2)

It is well-known that
\[ \sum_{x \in \mathbb{F}_{2m}} (-1)^{\text{Tr}_{\mathbb{F}_{2} / \mathbb{F}_{2}}(Q_{\bar{a}}(x))} = \begin{cases} 0, & 2 \nmid \text{rk}(Q_{\bar{a}}), \\ \pm 2^{m-e^{\text{rk}(Q_{\bar{a}})}/2}, & 2 | \text{rk}(Q_{\bar{a}}). \end{cases} \quad \] (3)

Let
\[ B_{\bar{a}}(x, y) = Q_{\bar{a}}(x + y) - Q_{\bar{a}}(x) - Q_{\bar{a}}(y). \]

Then \{B_{\bar{a}}\} is either the system
\[ B_{\bar{a}}(x, y) = \sum_{j=1}^{k-1} \text{Tr}_{\mathbb{F}_{2m} / \mathbb{F}_{2}}(a_{j}(x y^{2^{(2j-1)d}} + x^{2^{(2j-1)d}} y)), \bar{a} \in \mathbb{F}_{2m}^{k}, \]  

(4)

or the system
\[ B_{\bar{a}}(x, y) = \sum_{j=1}^{k-1} \text{Tr}_{\mathbb{F}_{2m} / \mathbb{F}_{2}}(a_{j}(x y^{2^{(2j-1)d}} + x^{2^{(2j-1)d}} y)), \bar{a} \in \mathbb{F}_{2m}^{k}, \]  

(5)

or the system
\[ B_{\bar{a}}(x, y) = \sum_{j=1}^{k-1} \text{Tr}_{\mathbb{F}_{2m} / \mathbb{F}_{2}}(a_{j}(x y^{2^{(2j-1)d}} + x^{2^{(2j-1)d}} y)), \bar{a} \in \mathbb{F}_{2m}^{k}. \]  

(6)

It is well-known that
\[ \text{rk}(B_{\bar{a}}) = \begin{cases} \text{rk}(Q_{\bar{a}}), & 2 \nmid \text{rk}(Q_{\bar{a}}), \\ \text{rk}(Q_{\bar{a}}) - 1, & 2 | \text{rk}(Q_{\bar{a}}). \end{cases} \]  

(7)

We now prove Theorem 1.1. By (2), (3) and (7), it suffices to prove the following.

**Theorem 2.1** If \((a_{1}, \cdots, a_{k-1}) \neq 0\), then
\[ \text{rk}(B_{\bar{a}}) \geq m - \frac{e}{e} - 2(k - 2). \]

**Proof.** Suppose that \((a_{1}, \cdots, a_{k-1}) \neq 0\). It suffices to show that
\[ \dim_{\mathbb{F}_{2}} \text{Rad}(B_{\bar{a}}) \leq 2(k - 1), \]

where
\[ \text{Rad}(B_{\bar{a}}) = \{ x \in \mathbb{F}_{2m} \mid B_{\bar{a}}(x, y) = 0, \forall y \in \mathbb{F}_{2m} \}. \]
Without loss of generality, we assume that \( \{B_d\} \) is the system (4). Then

\[
\text{Rad}(B_d) = \{ x \in F_{2^m} \mid \sum_{j=1}^{k-1} (a_j^2 x^{2j} + a_j x^{2j}) x^{-j} = 0 \}
\]

\[
= \{ x \in F_{2^m} \mid \sum_{j=1}^{k-1} (a_j^{2(k-1)-d} x^{2(k-1)-d} + a_j^{2(k-1)-d} x^{2(k-1)+d}) = 0 \}.
\]

Note that

\[
\{ x \in F_{2^{m(d/e)}} \mid \sum_{j=1}^{k-1} (a_j^{2(k-1)-d} x^{2(k-1)-d} + a_j^{2(k-1)-d} x^{2(k-1)+d}) = 0 \}
\]

is a subspace of \( F_{2^{m(d/e)}} \) over \( F_{2^d} \) of dimension \( \leq 2(k-1) \). As \( (m, d) = e \), a basis of \( F_{2^m} \) over \( F_{2^e} \) is also a basis of \( F_{2^{m(d/e)}} \) over \( F_{2^d} \). It follows that

\[
\dim_{F_{2^e}} \text{Rad}(B_d) \leq 2(k-1).
\]

The theorem is proved. □

3 ENTERING BILINEAR EQUATIONS II

In this section we shall reduce Theorem 1.2 to the following.

Theorem 3.1 We have, for \( 0 \leq i \leq k-2 \),

\[
\beta_{m-e}^{m-2i} = \sum_{j=i}^{k-2} (-1)^{j-i} 2^{(j-i)(j-i-1)} \binom{j}{i} \left( \frac{m-e}{2} \right) 4^e (2^{m(k-1-j)} - 1),
\]

where

\[
\beta_r = 2^{-m} \# \{ \vec{a} \in F_{2^m} \mid \text{rk}(\text{B}_d) = r, \ (a_1, \ldots, a_{k-1}) \neq 0 \}.
\]

It suffices to prove the following.

Theorem 3.2 For each \( r = 0, 2, \cdots, \frac{m-e}{e} \),

\[
\alpha_{r,e} = \frac{1}{2} (2^r + \epsilon 2^\frac{r}{2}) \beta_r,
\]

Proof. By (1), (2), (3), (7), and (8),

\[
2^{m-\frac{r}{2}} (\alpha_{r,1} - \alpha_{r,-1})
\]

\[
= \sum_{rk(B_d)=r} \sum_{x \in F_{2^m}} (-1)^{\text{Tr}_{F_{2^e}}/F_2 (Q_d(x))}
\]

\[
= 2^{-m} \sum_{c \in F_{2^m}} \sum_{rk(B_d)=r} \sum_{x \in F_{2^m}} (-1)^{\text{Tr}_{F_{2^e}}/F_2 (\text{Tr}_{F_{2^m}/F_{2^e}}(cx) + Q_d(x))}
\]

\[
= 2^{-m} \sum_{rk(B_d)=r} \sum_{x \in F_{2^m}} (-1)^{\text{Tr}_{F_{2^e}}/F_2 (Q_d(x))} \sum_{c \in F_{2^m}} (-1)^{\text{Tr}_{F_{2^m}/F_2} (cx)}
\]

\[
= 2^m \beta_r.
\]
Similarly,

\[
2^{2m-er}(\alpha_{r,1} + \alpha_{r,-1}) = \sum_{\text{rk}(B_{\vec{d}})=r} x \in \mathbb{F}_{2m} (-1)^{\text{Tr}_{2e}/2} (Q_{\vec{a}}(x))^2
\]

\[
= 2^{-m} \sum_{c \in \mathbb{F}_{2m}} \sum_{\text{rk}(B_{\vec{d}})=r} x \in \mathbb{F}_{2m} (-1)^{\text{Tr}_{2e}/2} (\text{Tr}_{2m/e}(cx) + Q_{\vec{a}}(x))^2
\]

\[
= 2^{-m} \sum_{\text{rk}(B_{\vec{d}})=r} x, y \in \mathbb{F}_{2m} (-1)^{\text{Tr}_{2e}/2} (Q_{\vec{a}}(x) + Q_{\vec{a}}(y)) \sum_{c \in \mathbb{F}_{2m}} (-1)^{\text{Tr}_{2m/e}(c(x+y))}
\]

\[
= 2^{2m} \beta_r.
\]

The theorem is proved.

4 ASSOCIATION SCHEME THEORETIC APPROACH

In this section we shall use the following theorem of Delarte-Goethals to prove Theorem 3.1.

Theorem 4.1 (DG) Let \( M \) be an odd number, \( X \) the space of alternating bilinear forms on an \( M \)-dimension vector space over \( \mathbb{F}_q \), \( Y \) a subspace of \( X \), and

\[
d(Y) = \min \{ \text{rk}(y) \mid 0 \neq y \in Y \}.
\]

Then

\[
|Y| \leq q^{M(M-d(Y)+1)/2}.
\]

Moreover, if the equality holds, then, for \( i \leq (M-1-d(Y))/2 \),

\[
\# \{ y \in Y \mid \text{rk}(y) = M - 1 - 2i \} = \frac{(M-1-d(Y))/2}{2^i} q^{(j-i)(j-i-1)/2} q^{(M-1)/j} (q^{M(M-d(Y)+1-2j)/2} - 1).
\]

We now the above theorem to prove Theorem 3.1.

Let \( X \) be the space of alternating \( \mathbb{F}_{2e} \)-bilinear forms on \( \mathbb{F}_{2m} \). Fix a system \( \{ B_{\vec{a}} \} \). Set

\[
Y = \{ B_{\vec{a}} \mid \vec{a} \in \mathbb{F}_2^k, a_0 = 0 \}.
\]

By Theorem 2.1

\[
d(Y) \geq \frac{m-e}{e} - 2(k-2).
\]

By Delsarte-Goethals' theorem,

\[
|Y| \leq 2^m(\frac{m+e}{m})^{-d(Y)/2} \leq 2^m(k-1).
\]

As \( |Y| = 2^m(k-1) \), we arrive at

\[
|Y| = 2^m(\frac{m+e}{m})^{-d(Y)/2} = 2^m(k-1),
\]
In particular, \( d(Y) = \frac{m-e}{e} - 2(k-2) \). Applying Delsarte-Goethals’ theorem one more time, we have, for \( 0 \leq i \leq k-2 \),

\[
\# \{ \vec{a} \in \mathbb{F}_{2m}^k \mid \text{rk}(B_{\vec{a}}) = \frac{m-e}{e} - 2i, a_0 = 0 \} = \sum_{j=i}^{k-2} (-1)^{i-j} 2^{e(j-i)(j-i-1)} \binom{j}{i} \binom{m-e}{j} 4^e \left( 2^m(k-1-j) - 1 \right).
\]

Theorem 3.1 is proved.

5 NUMBER THEORETIC APPROACH

The theorem of Delarte-Goethals we used in the last section is proved by developing the theory of association schemes. To make the present paper self-contained, we shall develop a number theoretic approach, which is similar to the approach of Berlekamp [Ber] and Kasami [K71].

Let \( V_{s,u} \) be the set of solutions \( (x_1, x_2, \cdots, x_{2u}) \in \mathbb{F}_{2m}^{2u} \) of one of the systems

\[
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{2j} + x_{2i-1}x_{2i}) = 0, \quad j = 1, 2, \cdots, s, \tag{9}
\]

\[
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{2(2i-1)} + x_{2i-1}x_{2i}) = 0, \quad j = 1, 2, \cdots, s, \tag{10}
\]

and

\[
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{2(m+e-j)} + x_{2i-1}x_{2i}) = 0, \quad j = 1, 2, \cdots, s. \tag{11}
\]

In this section we shall use the following theorem to prove Theorem 3.1.

**Theorem 5.1** If \( s \geq u \geq 1 \), then \( V_{s,u} = V_{u,u} \).

We now prove Theorem 5.1. We shall make repeated use of the following \( q \)-binomial formula

\[
\prod_{i=0}^{u-1} (1 + qt^i) = \sum_{i=0}^{u} \binom{i}{u} q^i t^i.
\]

By the orthogonality of characters and Theorem 5.1, we have

\[
\sum_{\vec{a} \in \mathbb{F}_{2m}^k} \left( \sum_{x,y \in \mathbb{F}_{2m}} (-1)^{\text{Tr}_{\mathbb{F}_2^e/\mathbb{F}_2}(B_{\vec{a}}(x,y))} \right)^u = 2^m |V_{u,u}|, \quad 0 \leq u \leq k-1,
\]

where \( |V_{0,0}| = 1 \). Applying the identity

\[
\sum_{x,y \in \mathbb{F}_{2m}} (-1)^{\text{Tr}_{\mathbb{F}_2^e/\mathbb{F}_2}(B_{\vec{a}}(x,y))} = 2^{m-e \cdot \text{rk}(B_{\vec{a}})},
\]

we arrive at

\[
\sum_{0 \leq u \leq k-1} \beta_u 2^u (2m-e \cdot u) = 2^m(k-1)|V_{u,u}| - 2^{2m}u, \quad 0 \leq u \leq k-1.
\]
That is,
\[ \sum_{i=0}^{k-2} \beta \frac{m - e - 2i}{u} 4^{ui} = 2^{m(k-1)-(m+e)u} |V_{u,u}| - 2^{(m-e)u}, \quad 0 \leq u \leq k - 1. \]

Consider the equation
\[ \sum_{i=0}^{k-2} \beta \frac{m - e - 2i}{u} \left( \begin{array}{c} 1 \\ 4^{ei} \\ \vdots \\ 4^{e(k-1)i} \end{array} \right) = \left( \begin{array}{c} 2^{m(k-1)} |V_{0,0}| - 1 \\ 2^{m(k-1)-(m+e)} |V_{1,1}| - 2^{m-e} \\ \vdots \\ 2^{-(k-1)e} |V_{k-1,k-1}| - 2^{u(m-e)} \end{array} \right). \]

Multiplying on the left by the row vector \((-1)^{k-1-i} 4^e (k-1-i) \binom{k-1}{i} \), and applying the \(q\)-binomial formula once more, we arrive at
\[ \sum_{i=0}^{k-1} (-1)^{k-1-i} 4^e (k-1-i) \binom{k-1}{i} 2^{m(k-1)-(m+e)i} |V_{i,i}| = \prod_{i=0}^{k-1} (2^{(m-e)i} - 4^e). \]

Replacing \(k - 1\) with an arbitrary positive integer \(u\), we arrive at
\[ \sum_{i=0}^{u} (-1)^{u-i} 4^e \binom{u-1}{i} \binom{u}{i} 2^{mu-(m+e)i} |V_{i,i}| = \prod_{i=0}^{k-1} (2^{(m-e)i} - 4^e). \]

That is,
\[ \sum_{i=0}^{u} (-1)^{u-i} 4^e \binom{u-1}{i} \binom{u}{i} 2^{-(m+e)i} |V_{i,i}| = 2^{-mu} \prod_{i=0}^{k-1} (2^{(m-e)i} - 4^e). \] \hspace{1cm} (12)

Now fix \(0 \leq u \leq k - 1\), and consider the equation
\[ \sum_{i=0}^{k-2} \beta \frac{m - e - 2i}{u} \left( \begin{array}{c} 1 \\ 4^{ei} \\ \vdots \\ 4^{eui} \end{array} \right) = \left( \begin{array}{c} 2^{m(k-1)} |V_{0,0}| - 1 \\ 2^{m(k-1)-(m+e)} |V_{1,1}| - 2^{m-e} \\ \vdots \\ 2^{-(k-1)e} |V_{u,u}| - 2^{u(m-e)} \end{array} \right). \]

Multiplying on the left by the row vector \((-1)^{u-i} q^e \binom{u-1}{i} \binom{u}{i} \) for \(i = 0, \ldots, k-1\), and applying the \(q\)-binomial formula as well as (12), we arrive at
\[ \sum_{i=0}^{k-2} \beta \frac{m - e - 2i}{u} \prod_{0 \leq h \leq u-1} (4^{hi} - 4^{eh}) = (2^{m(k-1-u)} - 1) \prod_{0 \leq h \leq u-1} (2^{m-e} - 4^{eh}). \]

Dividing both sides by \(\prod_{0 \leq h \leq u-1} (4^{eu} - 4^{eh})\), we arrive at
\[ \sum_{i=0}^{k-2} \beta \frac{m - e - 2i}{u} \binom{i}{u} 4^e = \binom{m-u}{u} 4^e (2^{m(k-1-u)} - 1). \]
Applying the \( q \)-binomial Möbius inversion formula
\[
\sum_{i=v}^{u} (-1)^{i-v} q^{(i-v)} \binom{i}{v} q^{(i)} q^{(u)} = \begin{cases} 
1, & u = v, \\
0, & u \neq v,
\end{cases}
\]
we arrive at
\[
\beta_{m-2j} = \sum_{u=j}^{k-2} (-1)^{u-j} 4^e (\binom{\beta}{u}) 4^e (\binom{\beta}{j}) (2^{(k-1)-u} - 1).
\]
Theorem 3.1 is proved.

6 SYSTEMS OF BILINEAR EQUATIONS

In this section we shall prove Theorem 5.1. We begin with the following.

**Theorem 6.1** The systems (9), (10), and (11) are respectively equivalent to the systems

\[
\begin{align*}
\sum_{i=1}^{u} (x_{2i-1} x_{2i}^{2d} + x_{2i-1}^{2d} x_{2i}) = 0, \\
\sum_{i=1}^{u} (\tilde{x}_{2i-1} \tilde{x}_{2i}^{2d} + \tilde{x}_{2i-1}^{2d} \tilde{x}_{2i}) = 0,
\end{align*}
\]
\(j = 1, 2, \ldots, s-1,\) \hspace{1cm} (13)

and

\[
\begin{align*}
\sum_{i=1}^{u} (x_{2i-1} \tilde{x}_{2i}^{2d} + x_{2i-1}^{2d} \tilde{x}_{2i}) = 0, \\
\sum_{i=1}^{u} (\tilde{x}_{2i-1} \tilde{x}_{2i} x_{2i}^{2d} + \tilde{x}_{2i-1} x_{2i}^{2d} \tilde{x}_{2i}) = 0,
\end{align*}
\]
\(j = 1, 2, \ldots, s-1,\) \hspace{1cm} (14)

and

\[
\begin{align*}
\sum_{i=1}^{u} (\tilde{x}_{2i-1} x_{2i}^{2d} + \tilde{x}_{2i-1}^{2d} x_{2i}) = 0, \\
\sum_{i=1}^{u} (\tilde{x}_{2i-1} \tilde{x}_{2i} x_{2i}^{2d} + \tilde{x}_{2i-1} x_{2i}^{2d} \tilde{x}_{2i}) = 0,
\end{align*}
\]
\(j = 1, 2, \ldots, s-1,\) \hspace{1cm} (15)

where \( \tilde{x}_i = x_i + x_i^{2d}, \) \( x_i + x_i^{2d}, \) and \( x_i + x_i^{2d} \) respectively.

**Proof.** We deal with the system (9) first. Adding \( 2^d \)-th power of the \( (j-1) \)-th equation to the \( j \)-th equation, we arrive at

\[
\begin{align*}
\sum_{i=1}^{u} (x_{2i-1} x_{2i}^{2d} + x_{2i-1}^{2d} x_{2i}) = 0, \\
\sum_{i=1}^{u} (x_{2i-1} x_{2i}^{2d} + x_{2i-1}^{2d} x_{2i}) = 0.
\end{align*}
\]
\(j = 2, 3, \ldots, s.\)

Adding the \( (j-1) \)-th equation to the \( j \)-th equation in the above system, we arrive at the system (13).
We now deal with the system (10). Adding \(2^{2d}\)-th power of the \((j - 1)\)-th equation to the \(j\)-th equation, we arrive at

\[
\begin{cases}
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{2d} + x_{2i}^{2d}) = 0, \\
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{2(2j-1)d} + x_{2i}^{2(2j-1)d}) = 0, \\
\quad j = 2, 3, \ldots, s.
\end{cases}
\]

Adding the \((j - 1)\)-th equation to the \(j\)-th equation in the above system, we arrive at the system (14).

Finally we deal with the system (11). Inserting \(2^{\frac{m+n}{2}}\)-th power of the first equation to the system, we arrive at the system

\[
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{\frac{m+n}{2}} + x_{2i}^{\frac{m+n}{2}}) = 0, \quad j = 0, 1, 2, \ldots, s.
\]

Adding the \(2^{-d}\)-th power of the \((j - 1)\)-th equation to the \(j\)-th equation in the above system, we arrive at

\[
\begin{cases}
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{\frac{m+n}{2} - jd} + x_{2i}^{\frac{m+n}{2} - jd}) = 0, \\
\sum_{i=1}^{u} (x_{2i-1}x_{2i}^{\frac{m+n}{2} - (j+1)d} + x_{2i}^{\frac{m+n}{2} - (j+1)d}) = 0, \\
\quad j = 1, 2, \ldots, s.
\end{cases}
\]

Adding the \((j - 1)\)-th equation to the \(j\)-th equation in the above system, we arrive at the system (15). Theorem 6.1 is proved. ■

We now prove Theorem 5.1. If \(u = 1\), then \(V_{s,u} = V_{u,u}\) trivially. Now assume that \(u \geq 2\). Suppose that \((x_1, x_2, \ldots, x_{2u})\) belongs to \(V_{u,u}\). We are going to show that \((x_1, x_2, \ldots, x_{2u})\) belongs to \(V_{s,u}\). By induction, we may assume that \(x_{2u} \neq 0\). Then we may further assume that \(x_{2u} = 1\). By Theorem 6.1, \((\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{2u})\) is in \(V_{u-1,u}\). As \(\tilde{x}_{2u} = 0\), we see that \((\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{2u-2})\) is in \(V_{u-1,u-1}\). By induction, \((\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{2u-2})\) is in \(V_{s-1,u-1}\). As \(\tilde{x}_{2u} = 0\), we see that \((\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{2u})\) is in \(V_{s-1,u}\). By Theorem 6.1, \((x_1, x_2, \ldots, x_{2u})\) belongs to \(V_{s,u}\). Theorem 5.1 is proved.
7 THE NUMBER OF BALANCED SEQUENCES

In this section we prove Theorem 1.3. We have

\[ \# \{ c \in C \mid DC(c) = -1 \} \]

\[ = 2^{mk} - 1 - \sum_{j=0}^{u-m-2} 2^{m-e-2ej} \sum_{u=j}^{k-2} (-1)^{u-j} 4^e \left( \frac{u-j}{2} \right) \left( \frac{u}{j} \right) 4^e \left( 2^{m(k-1-u)} - 1 \right) \]

\[ = 2^{mk} - 1 - 2^{m-e} \sum_{u=0}^{k-2} 4^{-eu} \left( \frac{m-e}{u} \right) 4^e \left( 2^{m(k-1-u)} - 1 \right) \sum_{j=0}^{u} (-1)^j 4^e \left( \frac{u}{j} \right) 4^e \left( u-j \right) \]

\[ = 2^{mk} - 1 - 2^{m-e} \sum_{u=0}^{k-2} 4^{-eu} \left( \frac{m-e}{u} \right) 4^e \left( 2^{m(k-1-u)} - 1 \right) \prod_{j=1}^{u} (1 - 4^e j) \]

\[ \approx 2^{mk} \left( 1 - \sum_{u=0}^{k-2} (-1)^u 2^{-e(u+1)^2} \right). \]

Theorem 1.3 is proved.

Acknowledgement. The author thanks Kai-Uwe Schmidt for telling him the background of this subject.

References

[AL] Y. Aubry, P. Langevin, On the weights of binary irreducible cyclic codes, in Proc. Int. Conf. Cod. Cryptography, 2006, pp. 46-54.

[BMC] L. D. Baumert, R. J. McEliece, Weights of irreducible cyclic codes, Inf. Control, vol. 20, no. 2, pp. 158-175, 1972.

[BMY] L. D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Progress Rep., vol. 16, pp. 128-131, 1973.

[Ber] E. R. Berlekamp, The weight enumerators for certain subcodes of the 2nd order Reed-Muller codes, Inf. Contr., 17: 485-500, 1970.

[BEW] B. C. Berndt, R. J. Evans, K. S. Williams, Gauss and Jacobi Sums. New York, NY, USA: Wiley, 1997.

[BMC10] N. Boston, G. McGuire, The weight distributions of cyclic codes with two zeros and zeta functions, J. Symbol. Comput., vol. 45, no. 7, pp. 723-733, 2010.

[De] P. Delsarte, On subfield subcodes of modified reed-solomon codes, IEEE Trans. Inf. Theory, vol. 21, no. 5, pp. 575-576, 1975.

[DG] P. Delsarte, J.-M. Goethals, Alternating bilinear forms over GF(q), J. Comb. Theory (A) 19 (1): 26-50, 1975.
[DLMZ] C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, IEEE Trans. Inf. Theory, vol. 57, no. 12, pp. 8000-8006, 2011.

[DY] C. Ding, J. Yang, Hamming weights in irreducible cyclic codes, Discr. Math., vol. 313, pp. 434-446, 2013.

[FL] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl., vol. 14, no. 2, pp. 390-409, 2008.

[FE] T. Feng, On cyclic codes of length $2^{2r}$ with two zeros whose dual codes have three weights, Des. Codes Cryptogr., vol. 62, pp. 253-258, 2012.

[FM] T. Feng, K. Momihara, Evaluation of the weight distribution of a class of cyclic codes based on Index 2 Gauss sums, 2012, preprint.

[G66] R. Gold, Characteristic linear sequences and their coset functions, J. SIAM Appl. Math. 14 (5): 980-985, 1966.

[G67] R. Gold, Optimal binary sequences for spread spectrum multiplexing, IEEE Trans. Inform. Theory 13 (4): 619-621, 1967.

[G68] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inform. Theory 14 (1): 154-156, 1968.

[K66] T. Kasami, Weight distribution formula for some cyclic codes, Univ. of Illinois, Rept. R-265, 1966.

[K71] T. Kasami, Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes, Inf. Contr., 18: 369-394, 1971.

[KL] T. Kløve, Codes for Error Detection. Hackensack, NJ, USA: World Scientific, 2007.

[LHFG] S. X. Li, S. H. Hu, T. Feng and G. Ge, The weight distribution of a class of cyclic codes related to Hermitian graphs, IEEE Trans. Inf. Theory, vol. 59, no. 5, pp. 3064-3067, 2013.

[LN] R. Lidl H. Niederreuter, Finite Fields. NewYork, NY, USA: Addision-Wesley, 1983.

[LYL] Y. Liu, H. Yan and C. Liu, A class of six-weight cyclic codes and their weight distribution, Des. Codes Cryptogr., to appear.

[LF] J. Luo K. Feng, On the weight distribution of two classes of cyclic codes, IEEE Trans. Inf. Theory, vol. 54, no. 12, pp. 5332-5344, Dec. 2008.

[LTW] J. Luo, Y. Tang, H. Wang, Cyclic codes and sequences: the generalized Kasami case, IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 2130-2142, May 2010.

[MZLF] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, IEEE Trans. Inf. Theory, vol. 57, no. 1, pp. 397-402, Jan. 2011.

[MCE] R. J. McEliece, Irreducible cyclic codes and Gauss sums, in Part 1: Theory of Designs, Finite Geometry and Coding Theory, Math. Centre Tracts, Math. Centrum, ser. Combinatorics: NATO Advanced Study Institute Series. Amsterdam, The Netherlands: Springer, 1974, pp. 179-196.
[MCG] G. McGuire, On three weights in cyclic codes with two zeros, Finite Fields Appl., vol. 10, no. 1, pp. 97-104, 2004.

[MO] M. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, IEEE Trans. Inf. Theory, vol. 53, no. 2, pp. 843-847, Feb. 2007.

[MR] M. Moisio, K. Ranto, Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros, Finite Fields Appl., vol. 13, no. 4, pp. 922-935, 2007.

[MY] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith., vol. 39, pp. 251-264, 1981.

[RP] A. Rao, N. Pinnawala, A family of two-weight irreducible cyclic codes, IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 2568-2570, Jun. 2010.

[SC] R. Schoof, Families of curves and weight distribution of codes, Bull. Amer. Math. Soc., vol. 32, no. 2, pp. 171-183, 1995.

[Sch] K. Schmidt, Symmetric bilinear forms over finite fields with applications to coding theory, arXiv: 1410.7184.

[Tr] H. M. Trachtenberg, On the correlation functions of maximal linear recurring sequences, Ph. D. dissertation, Univ. Southern California, Los Angeles, CA, USA, 1970.

[VE] G. Vega, The weight distribution of an extended class of reducible cyclic codes, IEEE Trans. Inf. Theory, vol. 58, no. 7, pp. 4862-4869, Jul. 2012.

[WTQYX] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, The weight distributions of cyclic codes and elliptic curves, IEEE Trans. Inf. Theory, vol. 58, no. 12, pp. 7253C7259, Dec. 2012.

[XI12] M. Xiong, The weight distributions of a class of cyclic codes, Finite Fields Appl., vol. 18, no. 5, pp. 933-945, 2012.

[XI] M. Xiong, The weight distributions of a class of cyclic codes II, Design Codes Cryptography, to be published.

[YXDL] J. Yang, M. Xiong, C. Ding and J. Luo, Weight distribution of a class of cyclic codes with arbitrary number of zeros, IEEE Trans. Inform. Theory, vol. 59, no. 9, pp. 5985-5993, 2013.

[YCD] J. Yuan, C. Carlet, C. Ding, The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 712-717, Feb. 2006.

[ZHJYC] X. Zeng, L. Hu, W. Jiang, Q. Yue, X. Cao, The weight distribution of a class of p-ary cyclic codes, Finite Fields Appl., vol. 16, no. 1, pp. 56-73, 2010.

[ZWHZ] D. Zheng, X. Wang, L. Hu, X. Zeng, The weight distribution of a class of p-ary cyclic codes, Finite Fields Appl. 16 (5): 933-945, 2012.

[ZDLZ] Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, IEEE Trans. Inf. Theory 59 (10): 6674-6682, 2013.