A Family of Three-Weight Binary Linear Codes

Can Xiang

Abstract—In this paper, a family of three-weight binary linear codes is constructed. Some of the linear codes obtained are either optimal or almost optimal. These codes have applications in association schemes, authentication codes, and secret sharing schemes, in addition to their uses in consumer electronics, communication and data storage systems.

Index Terms—Association schemes, authentication codes, linear codes, secret sharing schemes.

I. INTRODUCTION

In this paper, let \( q = 2^m \) for some positive integer \( m \), and let \( GF(q) \) denote the finite field with \( q \) elements. An \( [n, k] \) binary code \( C \) is a \( k \)-dimensional subspace of \( GF(2)^n \). An \( [n, k, d] \) binary code \( C \) is a \( k \)-dimensional subspace of \( GF(2)^n \) with minimum (Hamming) distance \( d \).

Let \( A_i \) denote the number of codewords with Hamming weight \( i \) in a code \( C \) of length \( n \). The weight enumerator of \( C \) is defined by \( 1 + A_1 z + A_2 z^2 + \cdots + A_n z^n \). The weight distribution \( (A_1, A_2, \ldots, A_n) \) of a code \( C \) gives information as to estimate the error correcting capability and the probability of error detection and correction with respect to some algorithms.

A code \( C \) is said to have \( t \) weights if the number of nonzero \( A_i \) in the sequence \( (A_1, A_2, \ldots, A_n) \) is equal to \( t \). An \( [n, k, d] \) binary code \( C \) is called optimal if its parameters \( n, k \) and \( d \) meet a bound on linear codes [11] Chapter 2. An \( [n, k, d] \) binary code \( C \) is called almost optimal if \( [n, k, d+1] \) meets a bound on linear codes [11] Chapter 2.

Let \( D = \{d_1, d_2, \ldots, d_\ell \} \subseteq GF(q)^* \). Let \( Tr \) denote the trace function from \( GF(q) \) onto \( GF(2) \) throughout this paper. We define a linear code of length \( n \) over \( GF(2) \) by

\[
C_D = \{ (Tr(xd_1), Tr(xd_2), \ldots, Tr(xd_\ell)) : x \in GF(q) \}, \tag{1}
\]

and call \( D \) the defining set of this code \( C_D \). Different orderings of the elements of \( D \) result in different codes \( C_D \), but the codes are permutation equivalent [11] p. 20]. Permutation equivalent codes have the same length, dimension and weight distribution. Hence, any indexing of the elements of the defining set \( D \) will not affect the conclusions of the code \( C_D \) in the theorems of this paper.

This construction approach is generic in the sense that a number of classes of known codes could be produced by selecting the defining set \( D \subseteq GF(q) \) properly. It was employed in [5, 8, 7, 10, 14] for obtaining linear codes with a few weights.

The objective of this paper is to construct a family of binary linear codes with three nonzero weights. The duals of the linear codes with three weights obtained in this paper are either optimal or almost optimal. The binary linear codes with three weights presented in this paper have applications in secret sharing schemes [11], authentication codes [9], and association schemes [2], in addition to their applications in consumer electronics, communication and data storage systems.

II. THE BINARY LINEAR CODES AND THEIR PARAMETERS

In this section, we only describe the binary codes and introduce their parameters, but will present the proofs of their parameters in the next section.

In this paper, the defining set \( D \) of the code \( C_D \) of \( \text{I} \) is given by

\[
D = \{ x \in GF(q) : Tr(x^3 + x) = 0 \}. \tag{2}
\]

Since \( 0 \notin D \), the minimum distance \( d^\perp \) of the dual code \( C_D^\perp \) of \( C_D \) cannot be 1. Note that the elements in \( D \) are pairwise distinct, the minimum distance \( d^\perp \) of the dual code \( C_D^\perp \) cannot be 2. Hence, we have the following lemma.

Lemma 1. The minimum distance \( d^\perp \) of the dual code \( C_D^\perp \) of \( C_D \) is at least 3 if \( n = |D| \geq 3 \).

Theorem 2. Let \( m \geq 3 \) be odd, and let \( D \) be defined in \( \text{II} \).

Then the set \( C_D \) of \( \text{II} \) is a \( [2m^\perp - 1 + (\frac{2m^{-1}}{3}) 2, 2m^\perp - 1 \] binary code with the weight distribution in Table I The dual code \( C_D^\perp \) has parameters

\[
[2m^\perp - 1 + (\frac{2m^\perp}{3}) 2, 2m^\perp - 1 - (\frac{2m^\perp}{3}) 2 - m, d^\perp],
\]

where \( d^\perp \geq 3 \).

| Weight \( w \) | Multiplicity \( A_w \) |
|---|---|
| 1 | 1 |
| \( 2m^\perp - 2 + (\frac{2m^\perp}{3}) 2 \) | \( 2m^\perp - 2 + (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 \) |
| \( 2m^\perp - 2 + (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 \) | \( 2m^\perp - 2 \) |
| \( 2m^\perp - 2 + (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 \) | \( 2m^\perp - 2 - (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 - (\frac{2m^\perp}{3}) 2 \) |

Example 1. Let \( m = 5 \). Then the code \( C_D \) has parameters \([11, 5, 4]\) and weight enumerator \( 1 + 10z^4 + 16z^8 + 5z^{10} \). This code is optimal.

Example 2. Let \( m = 7 \). Then the code \( C_D \) has parameters \([71, 7, 32]\) and weight enumerator \( 1 + 35z^{32} + 64z^{36} + 28z^{40} \).

Theorem 3. Let \( m \geq 4 \) be even, and let \( D \) be defined in \( \text{II} \).

Then the set \( C_D \) of \( \text{II} \) is a \( [2m^\perp - 1, m] \) binary code with the weight distribution in Table \( \text{II} \) when \( m = 2 (\text{mod } 4) \), and a \([2m^\perp - 1 - 2\frac{m^{-1}}{2}, (\frac{2m^\perp}{3}) 2, m] \) binary code with the weight distribution in Table \( \text{II} \) when \( m = 0 (\text{mod } 4) \).
The dual code $C_D^*$ has parameters $[2^{m-1} - 1, 2^{m-1} - 1 - m, d^+ \geq 3]$ when $m \equiv 2 \pmod{4}$, and parameters $[2^{m-1} - 1 - 2^{3/4} (-1)^{3/4}, 2^{m-1} - 1 - 2^{3/4} (-1)^{3/4} - m, d^+ \geq 3]$ when $m \equiv 0 \pmod{4}$.

### Table II

| Weight $w$ | Multiplicity $A_w$ |
|------------|-------------------|
| 0          | 1                 |
| $2^{m-2}$  | $3 \cdot 2^{m-2} - 1$ |
| $2^{m-2} + \frac{2^{3/2}}{4}$ | $2^{m-3} - 2 \cdot \frac{2^{3/2}}{4}$ |
| $2^{m-2} - \frac{2^{3/2}}{4}$ | $2^{m-3} + 2 \cdot \frac{2^{3/2}}{4}$ |

### Table III

| Weight $w$ | Multiplicity $A_w$ |
|------------|-------------------|
| 0          | 1                 |
| $2^{m-2} - \frac{2^{3/2}}{4}$ | $3 \cdot 2^{m-2} - 1$ |
| $2^{m-2} - \frac{2^{3/2}}{4}$ | $2^{m-3} + 2 \cdot \frac{2^{3/2}}{4}$ |
| $2^{m-2} - \frac{2^{3/2}}{4}$ | $2^{m-3} - 2 \cdot \frac{2^{3/2}}{4}$ |

Example 3. Let $m = 6$. Then the code $C_D$ has parameters $[31, 6, 12]$ and weight enumerator $1 + 10z^{12} + 47z^{16} + 6z^{20}$.

Example 4. Let $m = 10$. Then the code $C_D$ has parameters $[511, 10, 240]$ and weight enumerator $1 + 136z^{240} + 767z^{256} + 120z^{272}$.

Example 5. Let $m = 4$. Then the code $C_D$ has parameters $[11, 4, 4]$ and weight enumerator $1 + 2z^4 + 12z^6 + z^8$. This code is almost optimal.

Example 6. Let $m = 8$. Then the code $C_D$ has parameters $[111, 8, 48]$ and weight enumerator $1 + 36z^{48} + 192z^{56} + 27z^{64}$.

### III. The Proofs of the Main Results

In this section we prove Theorems 2 and 3. Before doing this, we have to do some preparations. We start with an introduction of group characters.

An additive character of GF$(q)$ is a nonzero function $\chi$ from GF$(q)$ to the set of nonzero complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x,y) \in$ GF$(q)^2$. For each $b \in$ GF$(q)$, the function

$$\chi_b(c) = (-1)^{\text{Tr}(bc)} \quad \text{for all } c \in \text{GF}(q)$$

defines an additive character of GF$(q)$. When $b = 0$, $\chi_0(c) = 1$ for all $c \in$ GF$(q)$, and is called the trivial additive character of GF$(q)$. The character $\chi_1$ in (3) is called the canonical additive character of GF$(q)$. It is known that every additive character of GF$(q)$ can be written as $\chi_b(x) = \chi_1(bx)$ [12, Theorem 5.7].

For any $a$ and $b$ in GF$(q)$, we define the following exponential sum

$$S(a,b) = \sum_{x \in \text{GF}(q)} \chi_1(ax^3 + bx).$$

To prove the weight distributions of the codes in Theorems 2 and 3 we need the values of the sum $S(a,b)$.

We now define a constant as follows. Let

$$n_0 = \left| \{ x \in \text{GF}(q) : \text{Tr}(x^3 + x) = 0 \} \right|.$$

By definition, the length $n$ of the code $C_D$ of (1) is equal to $n_0 - 1$. We have

$$n_0 = \frac{1}{2} \sum_{y \in \text{GF}(2)} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}(x^3+y)} = \frac{1}{2} \sum_{y \in \text{GF}(2)} \sum_{x \in \text{GF}(q)} \chi_1(\text{Tr}(x^3 + yx)).$$

Then

$$n_0 = 2^{m-1} + \frac{1}{2} \sum_{x \in \text{GF}(q)} \chi_1(x^3 + x). \quad (5)$$

To prove Theorems 2 and 3 we also define the following parameter

$$N_b = \left| \{ x \in \text{GF}(q) : \text{Tr}(x^3 + x) = 0 \} \right|,$$

where $b \in$ GF$(q)^*$. By definition and the basic facts of additive characters, for any $b \in$ GF$(q)^*$ we have

$$N_b = \frac{1}{4} \sum_{x \in \text{GF}(q)} \left( \sum_{y \in \text{GF}(2)} (-1)^{\text{Tr}(x^3+y)} \right) \left( \sum_{z \in \text{GF}(2)} (-1)^{\text{Tr}(bz)} \right)$$

$$= \frac{1}{4} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}(bx)} + \frac{1}{4} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}(x^3 + x)} + \frac{1}{4} \sum_{x \in \text{GF}(q)} (-1)^{\text{Tr}(x^3 + (b+1)x)} + 2^{m-2}$$

$$= \frac{1}{4} \left( \sum_{x \in \text{GF}(q)} \chi_1(x^3 + x) + \chi_1(x^3 + (b+1)x) + 2^m \right). \quad (6)$$

For any $b \in$ GF$(q)^*$, the Hamming weight $w(c_b)$ of the following codeword

$$c_b = (\text{Tr}(xd_1), \text{Tr}(xd_2), \ldots, \text{Tr}(xd_n))$$

of the code $C_D$ of (1) is equal to $n_0 - N_b$.

#### A. The proof of Theorem 2

Let $m \geq 4$ be odd. It is well known that Tr$(x^3)$ is a semibent function from GF$(q)$ to GF$(2)$. Thus, we have

$$\sum_{x \in \text{GF}(q)} \chi_1(x^3 + (b+1)x) = \{0, 2^{m+1}, -2^{m+1}\} \quad (8)$$

for each $b \in$ GF$(q)^*$.

The following lemma is proved in [15, Theorem 2]

**Lemma 4.** When $m$ is odd, we have

$$S(1,1) = \sum_{x \in \text{GF}(q)} \chi_1(x^3 + x) = (-1)^{\frac{2^m - 1}{2}} 2^{\frac{m+1}{2}}.$$

We are now ready to prove Theorem 2. Let $m \geq 4$ be odd. It follows from (5) and Lemma 4 that the length $n$ of the code $C_D$ in Theorem 2 is equal to

$$2^{m-1} + (-1)^{\frac{2^m - 1}{2}} 2^{\frac{m+1}{2}} - 1,$$

as $n_0 = 2^{m-1} + (-1)^{\frac{2^m - 1}{2}} 2^{\frac{m+1}{2}}$. 

It follows from (4), (5), and Lemma 4 that
\[ N_b \in \left\{ 2m^{-2} + (-1)^{\frac{m^2-1}{2}} \frac{m+1}{2}, 2m^{-2} + \left[ (-1)^{\frac{m^2-1}{2}} \pm 1 \right] 2^{\frac{m+1}{2}} \right\} \]
for any \( b \in \text{GF}(q)^* \). Hence, the weight \( \text{wt}(c_b) \) of the codeword \( c_b \) in (7) satisfies
\[ \text{wt}(c_b) = n_0 - N_b \]
\[ \in \left\{ 2m^{-2} + (-1)^{\frac{m^2-1}{2}} \frac{m+1}{2}, 2m^{-2} + \left[ (-1)^{\frac{m^2-1}{2}} \pm 1 \right] 2^{\frac{m+1}{2}} \right\} \]
Define
\[ w_1 = 2m^{-2} + (-1)^{\frac{m^2-1}{2}} \frac{m+1}{2}, \]
\[ w_2 = 2m^{-2} + \left[ (-1)^{\frac{m^2-1}{2}} \pm 1 \right] 2^{\frac{m+1}{2}}, \]
\[ w_3 = 2m^{-2} + \left[ (-1)^{\frac{m^2-1}{2}} \pm 1 \right] 2^{\frac{m+1}{2}}. \]

We now determine the number \( A_{w_i} \) of codewords with weight \( w_i \) in \( C_D \). By Lemma 1 the minimum weight of the dual code \( C_D^\perp \) is at least 3. The first three Pless Power Moments (11) p.260] lead to the following system of equations:
\[ \left\{ \begin{align*}
A_{w_1} + A_{w_2} + A_{w_3} &= 2^{m-1}, \\
w_1 A_{w_1} + w_2 A_{w_2} + w_3 A_{w_3} &= n 2^{m-1}, \\
w_1^2 A_{w_1} + w_2^2 A_{w_2} + w_3^2 A_{w_3} &= n(n+1) 2^{m-2},
\end{align*} \right. \tag{9} \]
where \( n = 2^{m-1} + (-1)^{\frac{m^2+1}{2}} 2^{\frac{m+1}{2}} - 1 \). Solving the system of equations in (9) yields the weight distribution of Table I. The dimension of the code \( C_D \) is \( m \), as \( \text{wt}(c_b) > 0 \) for each \( b \in \text{GF}(q)^* \). The conclusions on the dual code \( C_D^\perp \) then follow on the length and the dimension of \( C_D \) and Lemma 1. This completes the proof of Theorem 2.

B. The proof of Theorem 3

Let \( m \geq 4 \) be even. To prove Theorem 5 we need the next two lemmas proved by Coulter 4.

Lemma 5. Let \( m \geq 4 \) be even and \( a \in \text{GF}(q)^* \). Then
\[ S(a,0) = \left\{ \begin{align*}
(-1)^\frac{m}{2} 2^{\frac{m}{2}} & \text{ if } a \neq g^{3t} \text{ for any } t, \\
(-1)^\frac{m}{2} 2^{\frac{m}{2}+1} & \text{ if } a = g^{3t} \text{ for some } t,
\end{align*} \right. \]
where \( g \) is a generator of \( \text{GF}(q)^* \).

Lemma 6. Let \( m \geq 4 \) be even, \( b \in \text{GF}(q)^* \) and \( f(x) = a^2 x^4 + ax \in \text{GF}(q)[x] \). There are two cases.
(i) If \( a \neq g^{3t} \) for any \( t \), then \( f(x) \) is a permutation polynomial of \( \text{GF}(q) \). Let \( x_0 \) be the unique element satisfying \( f(x_0) = b^2 \). Then
\[ S(a,b) = (-1)^\frac{m}{2} 2^{\frac{m}{2}} x_1(a x_0^3) = (-1)^\frac{m}{2} 2^{\frac{m}{2}} (-1)^{\text{Tr}(ax_0^3)}. \]
(ii) If \( a = g^{3t} \) for some \( t \), then \( S(a,b) = 0 \) unless the equation \( f(x) = b^2 \) is solvable. If this equation is solvable, with solution \( x_0 \) say, then
\[ S(a,b) = \left\{ \begin{align*}
(-1)^\frac{m}{2} 2^{\frac{m}{2}+1} (-1)^{\text{Tr}(ax_0^3)} & \text{ if } \text{Tr}(a) = 0, \\
(-1)^\frac{m}{2} 2^{\frac{m}{2}} (-1)^{\text{Tr}(ax_0^3)} & \text{ if } \text{Tr}(a) \neq 0,
\end{align*} \right. \]
where \( \text{Tr} \) is the trace function from \( \text{GF}(q) \) onto \( \text{GF}(2) \).

According to (10) p.29], the following lemma can be easily proved.

Lemma 7. Let \( m \geq 4 \) be even and \( f(x) = a^2 x^4 + ax \in \text{GF}(q)[x] \). If \( a = g^{3t} \) for some \( t \), then the equation \( f(x) = 1 \) is solvable if and only if \( m \equiv 0 \pmod{4} \), where \( g \) is a generator of \( \text{GF}(q)^* \).

The next lemma will be employed later.

Lemma 8. Let \( m \geq 4 \) be even. Then
\[ S(1,1) = \left\{ \begin{align*}
0 & \text{ if } m \equiv 2 \pmod{4}, \\
(-1)^\frac{m}{2} 2^{\frac{m}{2}+1} & \text{ if } m \equiv 0 \pmod{4}.
\end{align*} \right. \]

\textbf{Proof:} Let \( m \geq 4 \) be even. It is well known that \( \text{gcd}(3, 2^{m-1}) = 3 \). Hence, there exists \( t = \frac{m-1}{3} \) such that \( g^{3t} = 1 \). Note that \( \text{Tr}(1) = 0 \), as \( m \) is even. It then follows from Lemmas 6 and 7 that
\[ S(1,1) = \left\{ \begin{align*}
0 & \text{ if } m \equiv 2 \pmod{4}, \\
(-1)^\frac{m}{2} 2^{\frac{m}{2}+1} & \text{ if } m \equiv 0 \pmod{4}.
\end{align*} \right. \]
where \( x_0 \) is a solution of the equation \( x^4 + x = 1 \) when \( m \equiv 0 \pmod{4} \).

This completes the proof.

We are now ready to prove Theorem 3. Recall that \( m \geq 4 \) is even. It follows from (5) and Lemma 8 that the length \( n \) of the code \( C_D \) in Theorem 3 is given by
\[ n = \left\{ \begin{align*}
2^{m-1} - 1 & \text{ if } m \equiv 2 \pmod{4}, \\
2^{m-1} - 2^{\frac{m}{2}} (-1)^{\frac{m}{2}} - 1 & \text{ if } m \equiv 0 \pmod{4}.
\end{align*} \right. \tag{10} \]

Since \( \text{gcd}(3, 2^{m-1}) = 3 \), there exists \( t = \frac{m-1}{3} \) such that \( g^{3t} = 1 \). Note that \( \text{Tr}(1) = 0 \), as \( m \) is even. It follows from Lemmas 5 and 3 that
\[ S(1, b+1) \in \{0, \pm (-1)^{\frac{m}{2}} 2^{\frac{m}{2}+1}\} \tag{11} \]
for any \( b \in \text{GF}(q)^* \).

It then follows from (6), (11) and Lemma 8 that
\[ N_b \in \{u_1, \pm u_2 + u_1\} \]
when \( m \equiv 2 \pmod{4} \), and
\[ N_b \in \{u_1 - (-1)^{\frac{m}{2}} u_2, (-1)^{\frac{m}{2}} \pm 1) u_2 + u_1\} \]
when \( m \equiv 0 \pmod{4} \), for any \( b \in \text{GF}(q)^* \), where \( u_1 = 2^{m-2} \) and \( u_2 = 2^{\frac{m}{2} - 1} \). Hence, the weight \( \text{wt}(c_b) \) of the codeword of (7) satisfies
\[ \text{wt}(c_b) = n_0 - N_b \in \}
\[ \{u_1, u_1 \pm u_2\} \text{ if } m \equiv 2 \pmod{4} \\
\{u_1 - (-1)^{\frac{m}{2}} u_2, u_1 - (-1)^{\frac{m}{2}} \pm 1) u_2 \} \text{ if } m \equiv 0 \pmod{4} \]
and the code \( C_D \) has all the three weights in the set above. Define \( u_1 = 2^{m-2}, u_2 = 2^{\frac{m}{2} - 1}, u = u_1 - (-1)^{\frac{m}{2}} u_2 \) and
\[ \{w_1 = u_1, w_2 = u_1 + u_2, w_3 = u_1 - u_2 \} \text{ if } m \equiv 2 \pmod{4} \\
\{w_1 = u, w_2 = u - u_2, w_3 = u + u_2 \} \text{ if } m \equiv 0 \pmod{4} \]
We now determine the number \( A_{w_j} \) of codewords with weight \( w_j \) in \( C_D \). By Lemma 1, the minimum weight of the dual code \( C_D^\perp \) is at least 3. The first three Pless Power Moments [11, p. 260] lead to the following system of equations:

\[
\begin{align*}
A_{w_1} + A_{w_2} + A_{w_3} &= 2^m - 1, \\
w_1A_{w_1} + w_2A_{w_2} + w_3A_{w_3} &= n^2m - 1, \\
w_1^2A_{w_1} + w_2^2A_{w_2} + w_3^2A_{w_3} &= n(n + 1)2^{m - 2},
\end{align*}
\]

where \( n \) is given in (10). Solving the system of equations in (12) proves the weight distribution of the code \( C_D \) in Table 1. The dimension of the code \( C_D \) is \( m \), as \( \text{wt}(c_b) > 0 \) for each \( b \in \text{GF}(q)^* \). The conclusions on the dual code \( C_D^\perp \) then follow on the length and the dimension of \( C_D \) and Lemma 1. This completes the proof of Theorem 3.

IV. CONCLUDING REMARKS

The three-weight codes \( C_D \) of this paper yield association schemes with the framework introduced in [2]. Any linear code over \( \text{GF}(p) \) can be employed to construct secret sharing schemes [1, 3, 13]. In order to obtain secret sharing schemes with interesting access structures, one would like to have linear codes \( C \) such that \( w_{\text{min}}/w_{\text{max}} > \frac{p - 1}{n} \) [13], where \( w_{\text{min}} \) and \( w_{\text{max}} \) denote the minimum and maximum nonzero weight of the linear code.

When \( m \equiv 2 \pmod{4} \geq 6 \), the code \( C_D \) of this paper satisfies that

\[
\frac{w_{\text{min}}}{w_{\text{max}}} = \frac{2m - 2 - 2(m - 2)/2}{2m - 2 + 2m/2} > \frac{1}{2}.
\]

When \( m \equiv 4 \pmod{8} > 4 \), the code \( C_D \) of this paper satisfies that

\[
\frac{w_{\text{min}}}{w_{\text{max}}} = \frac{2m - 2}{2m - 2 + m/2} > \frac{1}{2}.
\]

When \( m \equiv 0 \pmod{8} \geq 8 \), the code \( C_D \) of this paper satisfies that

\[
\frac{w_{\text{min}}}{w_{\text{max}}} = \frac{2m - 2 - 2m/2}{2m - 2} > \frac{1}{2}.
\]

When \( m \equiv \pm 1 \pmod{8} \geq 7 \), the code \( C_D \) of this paper satisfies that

\[
\frac{w_{\text{min}}}{w_{\text{max}}} = \frac{2m - 2}{2m - 2 + (m - 1)/2} > \frac{1}{2}.
\]

When \( m \equiv \pm 3 \pmod{8} > 5 \), the code \( C_D \) of this paper satisfies that

\[
\frac{w_{\text{min}}}{w_{\text{max}}} = \frac{2m - 2 - 2(m - 1)/2}{2m - 2} > \frac{1}{2}.
\]

Hence, the linear codes \( C_D \) of this paper satisfy the condition that \( w_{\text{min}}/w_{\text{max}} > \frac{1}{2} \) when \( m \geq 8 \), and can thus be employed to obtain secret sharing schemes with interesting access structures using the framework in [13]. Note that binary linear codes can be employed for secret sharing bit by bit. Hence, a secret of any size can be shared with a secret sharing scheme based on a binary linear code. We remark that the dimension of the code \( C_D \) of this paper is small compared with its length and this makes it suitable for the application in secret sharing.