AIMS Mathematics, 6(8): 8600–8610.
DOI: 10.3934/math.2021499
Received: 28 January 2021
Accepted: 01 June 2021
Published: 07 June 2021

http://www.aimspress.com/journal/Math

Research article

Weight distributions for projective binary linear codes from Weil sums

Shudi Yang[1,*] **and Zheng-An Yao**[2]

[1] School of Mathematical Sciences, Qufu Normal University, Shandong 273165, China
[2] School of Mathematics, Sun Yat-sen University, Guangzhou 510275, China

* **Correspondence:** Email: yangshudi@qfnu.edu.cn.

Abstract: A class of projective binary linear codes are constructed and their weight distributions are investigated using Weil sums. They have at most three nonzero weights, containing some optimal codes. Their dual codes are also studied and some of them are either optimal or almost optimal.

Keywords: linear codes, weight enumerators, Weil sums
Mathematics Subject Classification: 94B15, 11T71

1. Introduction

Throughout this paper, we let $q = 2^m$ for a positive integer m. An $[n, \kappa, d]$ linear code C over the finite field $\mathbb{F}_2$ is a κ-dimensional subspace of $\mathbb{F}_2^n$ with minimum distance d. A linear code C is called projective if its dual code has minimum distance at least 3. For a codeword $\mathsf{c} \in C$ the Hamming weight $wt(\mathsf{c})$ is the number of nonzero coordinates in c. Let A_i be the number of codewords with weight i in C of length n. The sequence $(1, A_1, \ldots, A_n)$ is referred as the weight distribution of C. If the number of nonzero A_i in the sequence $(A_1, \ldots, A_n)$ is equal to t, we call C a t-weight code.

The weight distribution contains important information of a code. In classic coding theory, it gives the minimum distance of the code which determines the error correction capability of the code. In addition, the weight distribution allows the computation of the error probability of error detection and error correction with respect to some algorithms [2, 16, 31]. Thus, it is desirable to determine the weight distributions of linear codes. Moreover, linear codes with a few nonzero weights have many applications in constant composition codes [10], authentication codes [11] and secret sharing schemes [38] and some other fields. So it has provoked tremendous interests in determining the weight distributions of linear codes in literature. Different kinds of linear codes over finite fields and rings have been investigated explicitly for the past two decades, see [5, 9, 13, 15, 17–19, 24, 27, 29, 30, 34, 35, 39]. In particular, Ding et al. [13] studied the weight distributions of a class of binary linear codes. Heng et al. dealt with projective binary linear codes from special Boolean functions in their recent work [18].

Huang et al. [19] constructed primitive binary LCD BCH codes and determined their parameters.

Let $q = p^m$ for a prime p. Choose a subset $D = \{d_1, d_2, \ldots, d_n\}$ of $\mathbb{F}_q^*$, where $\mathbb{F}_q^*$ is the multiplicative group of $\mathbb{F}_q$. Denote by Tr the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. A linear code of length n is defined by

$$C_D = \{(\mathrm{Tr}(bd_1), \mathrm{Tr}(bd_2), \ldots, \mathrm{Tr}(bd_n)) : b \in \mathbb{F}_q\}. \tag{1.1}$$

The set D is called the defining set. Ding [12] pointed out that the defining-set construction is a fundamental approach and is equivalent to the generator matrix construction of all linear codes. Therefore it has attracted extensive attention and many families of linear codes were proposed following this way [1, 13, 14, 21–23, 33, 36, 37], most of which have good parameters. Particularly, Wu et al. [33] investigated three-weight binary linear codes from generalized Moisio's exponential sums. We refer the reader to [25, 28] and the references therein for an overall survey on recent results and problems on constructions of linear codes from cryptographic functions.

In the rest of the paper, we always take $p = 2$ unless otherwise stated. In [13], a class of three-weight binary code C_D of (1.1) is constructed using the defining set

$$D = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x^{2^h+1}) = 0\},$$

where $q = 2^m$ and $1 \leqslant h < m/2$.

Let $\alpha, \beta \in \mathbb{F}_q^*$, and u a positive integer less than m. We consider a special case of the defining-set construction by defining a class of linear codes

$$C_D = \{\mathsf{c}(a, b) : a, b \in \mathbb{F}_q\}, \tag{1.2}$$

where $\mathsf{c}(a, b) = (\mathrm{Tr}(ax + by))_{(x,y)\in D}$ and

$$D = \{(x, y) \in \mathbb{F}_q^2 \backslash \{(0, 0)\} : \mathrm{Tr}(\alpha x^{2^u+1} + \beta y^{2^u+1}) = 0\}. \tag{1.3}$$

The set D is also called the defining set of C_D. Clearly, this is an extension of the work in [13]. The purpose of this paper is to study the weight distributions of C_D by employing Weil sums. These linear codes are projective with at most three nonzero weights and can be utilized to construct secret sharing schemes with good access structures.

Now we present the main results of this paper and their proofs are given in Section 3. Let $v = \gcd(m, u)$ stand for the greatest common divisor of m and u. Let g be a generator of the cyclic group $\mathbb{F}_q^*$. Namely, $\mathbb{F}_q^* = \langle g \rangle$. The weight distributions of C_D are given in the following four theorems.

Theorem 1.1. *Let C_D be defined by* (1.2) *and* (1.3). *If m/v is odd, then C_D is a $[2^{2m-1} - 1, 2m, 2^{2m-2} - 2^{m+v-2}]$ three-weight binary code with the weight distribution in Table 1.*

Table 1. The weight distribution of C_D in Theorem 1.1.

Weight w	Multiplicity A_w
0	1
$2^{2m-2} - 2^{m+v-2}$	$2^{m-v-1}(2^{m-v} + 1)$
2^{2m-2}	$2^{2m} - 1 - 2^{2m-2v}$
$2^{2m-2} + 2^{m+v-2}$	$2^{m-v-1}(2^{m-v} - 1)$

Theorem 1.2. *Suppose that m/v is even and $\alpha, \beta \notin \langle g^{2^v+1} \rangle$. Then C_D is a $[2^{2m-1} + 2^{m-1} - 1, 2m, 2^{2m-2}]$ two-weight binary code with the weight distribution in Table 2.*

Table 2. The weight distribution of C_D in Theorem 1.2.

Weight w	Multiplicity A_w
0	1
2^{2m-2}	$2^{2m-1} + 2^{m-1} - 1$
$2^{2m-2} + 2^{m-1}$	$2^{2m-1} - 2^{m-1}$

Theorem 1.3. *Let m/v be even and $\alpha, \beta \in \langle g^{2^v+1} \rangle$. If $u \neq m/2$, then C_D is a $[2^{2m-1}+2^{m+2v-1}-1, 2m, 2^{2m-2}]$ three-weight binary code with the weight distribution in Table 3. If $u = m/2$, then C_D is a simplex code with parameters $[2^{2m} - 1, 2m, 2^{2m-1}]$ and the only nonzero weight 2^{2m-1}. Moreover, the simplex code meets the Griesmer bound.*

Table 3. The weight distribution of C_D in Theorem 1.3.

Weight w	Multiplicity A_w
0	1
2^{2m-2}	$2^{m-2v-1}(2^{m-2v} + 1) - 1$
$2^{2m-2} + 2^{m+2v-2}$	$2^{2m-4v}(2^{4v} - 1)$
$2^{2m-2} + 2^{m+2v-1}$	$2^{m-2v-1}(2^{m-2v} - 1)$

Theorem 1.4. *Suppose that m/v is even and only one of α and β is in $\langle g^{2^v+1} \rangle$, then C_D is a $[2^{2m-1} - 2^{m+v-1} - 1, 2m, 2^{2m-2} - 2^{m+v-1}]$ three-weight binary code with the weight distribution in Table 4.*

Table 4. The weight distribution of C_D in Theorem 1.4.

Weight w	Multiplicity A_w
0	1
$2^{2m-2} - 2^{m+v-1}$	$2^{m-v-1}(2^{m-v} + 1)$
$2^{2m-2} - 2^{m+v-2}$	$2^{2m} - 2^{2m-2v}$
2^{2m-2}	$2^{m-v-1}(2^{m-v} - 1) - 1$

Some examples are provided to illustrate our main results. All of the numerical results are verified by Magma programs.

Example 1. Let $(m, u) = (3, 1)$. By Theorem 1.1, the binary code C_D has parameters $[31, 6, 12]$. Its weight enumerator is $1 + 10z^{12} + 47z^{16} + 6z^{20}$.

Example 2. Let $(m,u) = (2,1)$ and $\mathbb{F}_4^* = \langle g \rangle$. If we take $\alpha = g^2$ and $\beta = g$, from Theorem 1.2 the binary code C_D has parameters $[9,4,4]$. Its weight enumerator is $1 + 9z^4 + 6z^6$. It is optimal according to Markus Grassl's code tables available at http://www.codetables.de/.

Example 3. Let $(m,u) = (4,2)$. Write $\mathbb{F}_{16}^* = \langle g \rangle$ and $\alpha = \beta = g^5$. By Theorem 1.3, the code C_D has parameters $[255,8,128]$ and it is an optimal simplex code with the only nonzero weight 128.

Example 4. Let $(m,u) = (4,1)$, $\mathbb{F}_{16}^* = \langle g \rangle$, $\alpha = g^3$ and $\beta = g$. By Theorem 1.4, the code C_D has parameters $[111,8,48]$. Its weight enumerator is $1 + 36z^{48} + 192z^{56} + 27z^{64}$.

2. Preliminaries

In this section, we present some results on group characters and Weil sums. Let G be a finite abelian group (written multiplicatively). A character χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. That is, χ is a mapping from G into U with $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in G$. Let $q = 2^m$. For each $b \in \mathbb{F}_q$, the function

$$\chi_b(x) = (-1)^{\mathrm{Tr}(bx)} \text{ for all } x \in \mathbb{F}_q$$

defines an additive character of $\mathbb{F}_q$, where Tr is the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$. The additive character χ_0 is called *trivial*, whereas other characters χ_b with $b \in \mathbb{F}_q^*$ are called *nontrivial*. Especially χ_1 is called the canonical additive character and is denoted by χ for simplicity. See [26] for more information about characters over finite fields.

In [7], Coulter determined the value of Weil sums $S_u(\alpha,\beta)$ defined by

$$S_u(\alpha,\beta) = \sum_{x \in \mathbb{F}_q} \chi(\alpha x^{2^u+1} + \beta x),$$

for all $\alpha, \beta \in \mathbb{F}_q$, where $q = 2^m$ and u is a positive integer. Recall that $v = \gcd(m,u)$ is the greatest common divisor of m and u.

Lemma 2.1 (Theorem 4.1, [7])**.** *If m/v is odd, then*

$$S_u(\alpha,0) = \begin{cases} q & \text{if } \alpha = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2.2 (Theorem 4.2, [7])**.** *Let $\beta \in \mathbb{F}_q^*$ and suppose m/v is odd. Then $S_u(\alpha,\beta) = S_u(1,\beta\gamma^{-1})$, where $\gamma \in \mathbb{F}_q^*$ is the unique element satisfying $\gamma^{2^u+1} = \alpha$. Further, we have*

$$S_u(1,\beta) = \begin{cases} 0 & \text{if } \mathrm{Tr}_v(\beta) \neq 1, \\ \pm 2^{\frac{m+v}{2}} & \text{if } \mathrm{Tr}_v(\beta) = 1, \end{cases}$$

where and hereafter Tr_v is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_{2^v}$.

Lemma 2.3 (Theorem 5.2, [7])**.** *Let m/v be even so that $m = 2k$ for some integer k. Then*

$$S_u(\alpha,0) = \begin{cases} (-1)^{k/v} 2^k & \text{if } \alpha \neq g^{t(2^v+1)} \text{ for any integer } t, \\ -(-1)^{k/v} 2^{k+v} & \text{if } \alpha = g^{t(2^v+1)} \text{ for some integer } t, \end{cases}$$

where g is a generator of $\mathbb{F}_q^*$.

When m/v is even, the evaluation of $S_u(\alpha,\beta)$ for $p=2$, where $\beta\neq 0$, was due to Coulter [7], and it can be similarly proved as the case of an odd prime p, see the poofs of Theorems 1 and 2 in [6].

Lemma 2.4 (Theorem 5.3, [7]). *Let $\beta\in\mathbb{F}_q^*$ and suppose m/v is even such that $m=2k$ for some integer k. Let $f_\alpha(x)=\alpha^{2^u}x^{2^{2u}}+\alpha x\in\mathbb{F}_q[x]$. There are two cases.*
(i) If $\alpha\neq g^{t(2^v+1)}$ for any integer t then f_α is a permutation polynomial. Let $x_0\in\mathbb{F}_q$ be the unique element satisfying $f_\alpha(x_0)=\beta^{2^u}$. Then

$$S_u(\alpha,\beta)=(-1)^{k/v}2^k\chi(\alpha x_0^{2^u+1}).$$

(ii) If $\alpha=g^{t(2^v+1)}$ for some integer t then $S_u(\alpha,\beta)=0$ unless the equation $f_\alpha(x)=\beta^{2^u}$ is solvable. If the equation is solvable, with solution x_0 say, then

$$S_u(\alpha,\beta)=-(-1)^{k/v}2^{k+v}\chi(\alpha x_0^{2^u+1}).$$

3. The proofs of the main results

In this section, we always fix $\alpha,\beta\in\mathbb{F}_q^*$ and let g be a generator of $\mathbb{F}_q^*$.

3.1. Auxiliary results

The code length is defined by

$$n=|D|=|\{(x,y)\in\mathbb{F}_q^2\backslash\{(0,0)\}:\mathrm{Tr}(\alpha x^{2^u+1}+\beta y^{2^u+1})=0\}|. \tag{3.1}$$

Lemma 3.1. *The code length n of* (3.1) *is given as follows.*
(i) If m/v is odd, then $n=2^{2m-1}-1$.
(ii) If m/v is even, then

$$n=\begin{cases}2^{2m-1}+2^{m-1}-1 & \text{if } \alpha,\beta\notin\langle g^{2^v+1}\rangle,\\ 2^{2m-1}+2^{m+2v-1}-1 & \text{if } \alpha,\beta\in\langle g^{2^v+1}\rangle,\\ 2^{2m-1}-2^{m+v-1}-1 & \text{otherwise.}\end{cases}$$

Proof. It follows from the orthogonal property of additive characters that

$$\begin{aligned}n&=\frac{1}{2}\sum_{x,y\in\mathbb{F}_q}\sum_{z_1\in\mathbb{F}_2}(-1)^{z_1\,\mathrm{Tr}(\alpha x^{2^u+1}+\beta y^{2^u+1})}-1\\&=2^{2m-1}+\frac{1}{2}\sum_{x,y\in\mathbb{F}_q}(-1)^{\mathrm{Tr}(\alpha x^{2^u+1}+\beta y^{2^u+1})}-1\\&=2^{2m-1}-1+\frac{1}{2}S_u(\alpha,0)S_u(\beta,0).\end{aligned}$$

Thus we obtain the desired conclusions from Lemmas 2.1 and 2.3. □

The Pless power moments are useful tools when we calculate the weight distribution of a given code. Recall that the code C_D is defined by (1.2) and (1.3) with length n and dimension $\kappa=\dim_{\mathbb{F}_2}(C_D)$.

The weight distributions of C_D and its dual $C_D^\perp$ are denoted by $(1, A_1, \ldots, A_n)$ and $(1, A_1^\perp, \ldots, A_n^\perp)$, respectively. As we will prove later in Theorem 4.1, the minimum weight of the dual code $C_D^\perp$ is at least 3. So $A_1^\perp = 0$, $A_2^\perp = 0$ and consequently the first three Pless power moments are given by [20, p.260]:

$$\sum_{j=0}^{n} A_j = 2^\kappa,$$
$$\sum_{j=0}^{n} jA_j = 2^{\kappa-1}n,$$
$$\sum_{j=0}^{n} j^2A_j = 2^{\kappa-2}n(n+1).$$

3.2. The proofs of Theorems 1.1, 1.2, 1.3 and 1.4

In this subsection, we will prove the weight distributions of C_D given in Theorems 1.1, 1.2, 1.3 and 1.4. The code length n is given in Lemma 3.1. Assume that $(a, b) \neq (0, 0)$ unless otherwise stated. We define

$$N_0(a, b) = |\{(x, y) \in \mathbb{F}_q^2 : \mathrm{Tr}(\alpha x^{2^u+1} + \beta y^{2^u+1}) = 0,\ \mathrm{Tr}(ax + by) = 0\}|. \tag{3.2}$$

Then the Hamming weight of $\mathsf{c}(a, b)$ is expressed as

$$wt(\mathsf{c}(a, b)) = n - N_0(a, b) + 1. \tag{3.3}$$

By (3.2) and the orthogonal property of additive characters,

$$\begin{aligned} N_0(a, b) &= 2^{-2} \sum_{x,y\in\mathbb{F}_q} \sum_{z_1\in\mathbb{F}_2} (-1)^{z_1 \mathrm{Tr}(\alpha x^{2^u+1}+\beta y^{2^u+1})} \sum_{z_2\in\mathbb{F}_2} (-1)^{z_2 \mathrm{Tr}(ax+by)} \\ &= 2^{-2} \sum_{x,y\in\mathbb{F}_q} (1 + (-1)^{\mathrm{Tr}(\alpha x^{2^u+1}+\beta y^{2^u+1})})(1 + (-1)^{\mathrm{Tr}(ax+by)}) \\ &= 2^{2m-2} + 2^{-2}(S_u(\alpha, 0)S_u(\beta, 0) + S_u(\alpha, a)S_u(\beta, b)). \end{aligned} \tag{3.4}$$

Now we are going to determine the values of $N_0(a, b)$ given by (3.4). There are four cases to consider according to the parity of m/v and the values of α and β.

In the first case, if m/v is odd, the length is $n = 2^{2m-1} - 1$. At first glance, when $a = 0$ and $b \neq 0$, we have $S_u(\alpha, 0) = 0$ by Lemma 2.1. So $N_0(a, b) = 2^{2m-2}$. Similarly when $a \neq 0$ and $b = 0$, $N_0(a, b) = 2^{2m-2}$. Assume that $a \in \mathbb{F}_q^*$, we have from Lemma 2.2 that

$$S_u(\alpha, a) = S_u(1, a\gamma^{-1}) = \begin{cases} 0 & \text{if } \mathrm{Tr}_v(a\gamma^{-1}) \neq 1, \\ \pm 2^{\frac{m+v}{2}} & \text{if } \mathrm{Tr}_v(a\gamma^{-1}) = 1, \end{cases}$$

where $\gamma \in \mathbb{F}_q^*$ is the unique element satisfying $\gamma^{2^u+1} = \alpha$. Thus it follows from (3.4), Lemmas 2.1 and 2.2 that

$$N_0(a, b) \in \{2^{2m-2},\ 2^{2m-2} + 2^{m+v-2},\ 2^{2m-2} - 2^{m+v-2}\}.$$

Hence, by (3.3), the weight $wt(\mathsf{c}(a,b))$ of the codeword $\mathsf{c}(a,b)$ satisfies

$$wt(\mathsf{c}(a,b)) \in \{2^{2m-2},\ 2^{2m-2}+2^{m+v-2},\ 2^{2m-2}-2^{m+v-2}\}.$$

Put

$$w_1 = 2^{2m-2}-2^{m+v-2},\ w_2 = 2^{2m-2},\ w_3 = 2^{2m-2}+2^{m+v-2}.$$

We now determine the number A_{w_i} of codewords with weight w_i in C_D. The first three Pless power moments yield the following system of equations:

$$\begin{cases} A_{w_1}+A_{w_2}+A_{w_3} = 2^{2m}-1, \\ w_1A_{w_1}+w_2A_{w_2}+w_3A_{w_3} = 2^{2m-1}n, \\ w_1^2A_{w_1}+w_2^2A_{w_2}+w_3^2A_{w_3} = 2^{2m-2}n(n+1), \end{cases} \tag{3.5}$$

where $n = 2^{2m-1}-1$. Solving the system of equations in (3.5) leads to the weight distribution given in Table 1. This proves Theorem 1.1.

In the second case, if m/v is even and $\alpha,\beta \notin \langle g^{2^v+1}\rangle$, the length is $n = 2^{2m-1}+2^{m-1}-1$. It follows from Lemmas 2.3 and 2.4 that

$$\begin{aligned} S_u(\alpha,0) &= (-1)^{k/v}2^k, \\ S_u(\alpha,a) &= (-1)^{k/v}2^k\chi(\alpha x_0^{2^u+1}), \end{aligned}$$

where $a \neq 0$ and x_0 satisfies $f_\alpha(x_0) = a^{2^u}$. By (3.4),

$$N_0(a,b) \in \{2^{2m-2},\ 2^{2m-2}+2^{m-1}\}.$$

From (3.3), the weight $wt(\mathsf{c}(a,b))$ belongs to the set

$$\{2^{2m-2},\ 2^{2m-2}+2^{m-1}\}.$$

Let

$$w_1 = 2^{2m-2},\ w_2 = 2^{2m-2}+2^{m-1}.$$

Again by solving the system of equations

$$\begin{cases} A_{w_1}+A_{w_2} = 2^{2m}-1, \\ w_1A_{w_1}+w_2A_{w_2} = 2^{2m-1}n, \end{cases} \tag{3.6}$$

where $n = 2^{2m-1}+2^{m-1}-1$, we get the weight distribution given in Table 2. This finishes the proof of Theorem 1.2.

In the third case, if m/v is even and $\alpha,\beta \in \langle g^{2^v+1}\rangle$, the length is $n = 2^{2m-1}+2^{m+2v-1}-1$. Again from Lemma 2.3, we have

$$S_u(\alpha,0) = -(-1)^{k/v}2^{k+v}.$$

Let $a \neq 0$. It follows from Lemma 2.4 that $S_u(\alpha, a) = 0$ or if the equation $f_\alpha(x) = a^{2^u}$ is solvable with a solution $x_0 \in \mathbb{F}_q$, then

$$S_u(\alpha, a) = -(-1)^{k/v} 2^{k+v} \chi(\alpha x_0^{2^u+1}).$$

By (3.3) and (3.4), the weight $wt(\mathsf{c}(a, b))$ belongs to the set

$$\{2^{2m-2},\ 2^{2m-2} + 2^{m+2v-2},\ 2^{2m-2} + 2^{m+2v-1}\}.$$

Write

$$w_1 = 2^{2m-2},\ w_2 = 2^{2m-2} + 2^{m+2v-2},\ w_3 = 2^{2m-2} + 2^{m+2v-1}.$$

The first three Pless power moments are given by (3.5), where $n = 2^{2m-1} + 2^{m+2v-1} - 1$. Solving these equations yields the weight distribution given in Table 3. This completes the proof of Theorem 1.3.

The last case is that m/v is even and $\alpha \in \langle g^{2^v+1} \rangle$, $\beta \notin \langle g^{2^v+1} \rangle$ (or $\beta \in \langle g^{2^v+1} \rangle$, $\alpha \notin \langle g^{2^v+1} \rangle$). In this case, $n = 2^{2m-1} - 2^{m+v-1} - 1$. After a similar argument as we have done in the previous case, we obtain from (3.3) and (3.4) that $wt(\mathsf{c}(a, b))$ belongs to the set

$$\{2^{2m-2},\ 2^{2m-2} - 2^{m+v-2},\ 2^{2m-2} - 2^{m+v-1}\}.$$

Set

$$w_1 = 2^{2m-2} - 2^{m+v-1},\ w_2 = 2^{2m-2} - 2^{m+v-2},\ w_3 = 2^{2m-2}.$$

From the first three Pless power moments (3.5), we get the weight distribution given in Table 4, completing the proof of Theorem 1.4.

4. The dual of the code C_D

For the dual $C_D^\perp$ of the code C_D, we have the following conclusion.

Theorem 4.1. *Let $m \geqslant 2$ and $\alpha, \beta \in \mathbb{F}_q^*$. The dual $C_D^\perp$ of the code C_D is a binary code with parameters $[n, n - 2m, d^\perp]$, where n is given in Lemma 3.1 and $d^\perp = 3$ if m is even and $3 \leqslant d^\perp \leqslant 4$ if m is odd.*

Proof. The dimension of the code $C_D^\perp$ is obvious. Since D does not contain the zero element of $\mathbb{F}_q^2$, the minimum distance of $C_D^\perp$ cannot be one. Similarly, since D is not a multiset, any two elements d_i and d_j of D must be distinct if $i \neq j$. Hence, the minimum distance $C_D^\perp$ cannot be 2. So we have $d^\perp \geqslant 3$.

When m is even, we assume that $(x_1, 0)$, $(0, y_2) \in D$. We claim that (x_1, y_2) is in D. Actually,

$$\mathrm{Tr}(\alpha x_1^{2^u+1} + \beta y_2^{2^u+1}) = \mathrm{Tr}(\alpha x_1^{2^u+1}) + \mathrm{Tr}(\beta y_2^{2^u+1}) = 0.$$

Therefore, the minimum distance of $C_D^\perp$ is 3.

When m is odd, $n = 2^{2m-1} - 1$ by Theorem 1.1. Let $D = \{d_i = (d_{1i}, d_{2i}) : i = 1, 2, \ldots, n\}$. Consider the sums $d_i + d_j$ for $i \neq j$. The total number of such sums is equal to $(2^{2m-1} - 1)(2^{2m-2} - 1) > 2^{2m}$ for $m \geqslant 2$. Hence, there must be four distinct integers $i, j, k, l \in \{1, 2, \ldots, n\}$ such that $d_i + d_j = d_k + d_l$. This means that $C_D^\perp$ has a codeword with Hamming weight 4. So we have $3 \leqslant d^\perp \leqslant 4$, completing the whole proof. □

When m is odd, the code $C_D^{\perp}$ is at least almost optimal. This is because the minimum weight of any binary code with length $2^{2m-1}-1$ and dimension $2^{2m-1}-1-2m$ is at most 4 according to the sphere packing bound.

Example 5. Let $(m,u)=(2,1)$, $\alpha=g^2$ and $\beta=g$, where $\mathbb{F}_4^*=\langle g\rangle$. Magma programs show that the binary code $C_D^{\perp}$ has parameters $[9,5,3]$ and it is optimal. If we take $\alpha=\beta=g^3$, then $C_D^{\perp}$ has parameters $[15,11,3]$ and it is optimal, too.

Example 6. Let $(m,u)=(3,1)$. Then the binary code $C_D^{\perp}$ has parameters $[31,25,3]$ and it is almost optimal, while the optimal binary code has parameters $[31,25,4]$.

5. Conclusions

In this paper, a class of projective binary codes with two or three weights were constructed from a proper defining set. Their weight distributions were determined by applying Weil sums and the first three Pless power moments. Furthermore, we determined the parameters of their dual codes. Some optimal and almost optimal codes were also constructed. Due to [38], a linear code over $\mathbb{F}_2$ is suitable to construct secret sharing schemes with interesting access structures if

$$\frac{w_{\min}}{w_{\max}}>\frac{1}{2}, \tag{5.1}$$

where $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero weights of the code, respectively. For the linear codes C_D in Theorems 1.1–1.4, the inequality (5.1) always holds if $m\geqslant 2v+2$. So they can be used in secret sharing schemes with good access structures. Additionally, projective two-weight codes in Theorem 1.2 can be applied in strongly regular graphs [4,8] and projective three-weight codes in Theorems 1.1, 1.3 and 1.4 are related to association schemes with three classes [3].

Acknowledgment

The authors would like to thank the referee for his/her thorough review with constructive suggestions and valuable comments. The work is partly supported by the National Natural Science Foundation of China under Grant 12071247, Grant 11701317, Grant U1811461 and Grant 11971496.

Conflict of interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

1. J. Ahn, D. Ka, C. Li, Complete weight enumerators of a class of linear codes, *Design. Code. Cryptogr.*, **83** (2017), 83–99.
2. I. F. Blake, K. Kith, On the complete weight enumerator of Reed-Solomon codes, *SIAM J. Discret. Math.*, **4** (1991), 164–171.

3. A. R. Calderbank, J. M. Goethals, Three-weight codes and association schemes, *Philips J. Res.*, **39** (1984), 143–152.
4. R. Calderbank, W. M. Kanter, The geometry of two-weight codes, *Bull. Lond. Math. Soc.*, **18** (1986), 97–122.
5. P. Charpin, Cyclic codes with few weights and Niho exponents, *J. Comb. Theory A*, **108** (2004), 247–259.
6. R. S. Coulter, Further evaluations of Weil sums, *Acta Arithmetica*, **86** (1998), 217–226.
7. R. S. Coulter, On the evaluation of a class of Weil sums in characteristic 2, *New Zealand J. Math.*, **28** (1999), 171–184.
8. P. Delsarte, Weights of linear codes and strongly regular normed spaces, *Discrete Math.*, **3** (1972), 47–64.
9. L. Diao, J. Gao, J. Lu, Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes, *Adv. Math. Commun.*, **14** (2020), 555–572.
10. C. Ding, J. Yin, A construction of optimal constant composition codes, *Design. Code. Cryptogr.*, **40** (2006), 157–165.
11. C. Ding, T. Helleseth, T. Kløve, X. Wang, A generic construction of Cartesian authentication codes, *IEEE T. Inform. Theory*, **53** (2007), 2229–2235.
12. C. Ding, The construction and weight distributions of all projective binary linear codes, (2020). Available from: `arXiv:2010.03184.`
13. K. Ding, C. Ding, Binary linear codes with three weights, *IEEE Commun. Lett.*, **18** (2014), 1879–1882.
14. K. Ding, C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, *IEEE T. Inform. Theory*, **61** (2015), 5835–5842.
15. S. T. Dougherty, J. Gildea, A. Kaya, B. Yildiz, New self-dual and formally self-dual codes from group ring constructions, *Adv. Math. Commun.*, **14** (2020), 11–22.
16. V. Guruswami, M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometry codes, *IEEE T. Inform. Theory*, **45** (1999), 1757–1767.
17. Z. Heng, C. Ding, Z. Zhou, Minimal linear codes over finite fields, *Finite Fields Appl.*, **54** (2018) 176–196.
18. Z. Heng, W. Wang, Y. Wang, Projective binary linear codes from special Boolean functions, *Appl. Algebr. Eng. Comm. Comput.* (2020), Available from: `https://doi.org/10.1007/s00200-019-00412-z.`
19. X. Huang, Q. Yue, Y. Wu, X. Shi, J. Michel, Binary primitive LCD BCH codes, *Design. Code. Cryptogr.*, **88** (2020), 2453–2473.
20. W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge: Cambridge University Press, 2003.
21. G. Jian, Z. Lin, R. Feng, Two-weight and three-weight linear codes based on Weil sums, *Finite Fields Th. Appl.*, **57** (2019), 92–107.

22. X. Kong, S. Yang, Complete weight enumerators of a class of linear codes with two or three weights, *Discrete Math.*, **342** (2019), 3166–3176.
23. C. Li, S. Bae, J. Ahn, S. Yang, Z. Yao, Complete weight enumerators of some linear codes and their applications, *Design. Code. Cryptogr.*, **81** (2016), 153–168.
24. C. Li, Q. Yue, F. Fu, A construction of several classes of two-weight and three-weight linear codes, *Appl. Algebra Eng. Comm. Comput.*, **28** (2017), 11–30.
25. N. Li, S. Mesnager, Recent results and problems on constructions of linear codes from cryptographic functions, *Cryptog. Commun.*, **12** (2020), 965–986.
26. R. Lidl, H. Niederreiter, *Finite Fields*, 2 Eds., Cambridge: Cambridge University Press, 1997.
27. G. Mcguire, On three weights in cyclic codes with two zeros, *Finite Fields Th. Appl.*, **10** (2004), 97–104.
28. S. Mesnager, Linear codes from functions, Chapter 20 in *Concise Encyclopedia of Coding Theory*, London: CRC Press/Taylor and Francis Group, 2021.
29. M. Shi, R. Wu, Y. Liu, P. Solé, Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$, *Cryptog. Commun.*, **9** (2017), 637–646.
30. M. Shi, Y. Guan, P. Solé, Two new families of two-weight codes, *IEEE T. Inform. Theory*, **63** (2017), 6240–6246.
31. M. Sudan, Decoding of Reed-Solomon codes beyond the error-correction bound, *J. Complexity*, **13** (1997), 180–193.
32. Y. Wu, Q. Yue, X. Zhu, S. Yang, Weight enumerators of reducible cyclic codes and their dual codes, *Discrete Math.*, **342** (2019), 671–682.
33. Y. Wu, Q. Yue, X. Shi, At most three-weight binary linear codes from generalized Moisio's exponential sums, *Design. Code. Cryptogr.*, **87** (2019), 1927–1943.
34. S. Yang, Z. Yao, C. Zhao, The weight enumerator of the duals of a class of cyclic codes with three zeros, *Appl. Algebra Eng. Commun. Comput.*, **26** (2015), 347–367.
35. S. Yang, Z. Yao, C. Zhao, The weight distributions of two classes of p-ary cyclic codes with few weights, *Finite Fields Th. Appl.*, **44** (2017), 76–91.
36. S. Yang, X. Kong, C. Tang, A construction of linear codes and their complete weight enumerators, *Finite Fields Th. Appl.*, **48** (2017), 196–226.
37. S. Yang, Z. Yao, Complete weight enumerators of a class of linear codes, *Discrete Math.*, **340** (2017), 729–739.
38. J. Yuan, C. Ding, Secret sharing schemes from three classes of linear codes, *IEEE T. Inform. Theory*, **52** (2006), 206–212.
39. Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, *IEEE T. Inform. Theory*, **59** (2013), 6674–6682.

AIMS Press