

WEIGHT DISTRIBUTIONS AND WEIGHT HIERARCHIES OF TWO CLASSES OF BINARY LINEAR CODES

FEI LI AND XIUMEI LI

ABSTRACT. Linear codes with a few weights can be applied to communication, consumer electronics and data storage system. In addition, the weight hierarchy of linear codes has many applications such as on the type II wire-tap channel, dealing with t -resilient functions and trellis or branch complexity of linear codes and so on. In this paper, we first present a formula for computing the weight hierarchies of linear codes constructed by the generalized method of defining sets. Then, we construct two classes of binary linear codes with a few weights and determine their weight distributions and weight hierarchies completely. Some codes of them can be used in secret sharing schemes.

1. INTRODUCTION

For a prime number p and a positive integer s , let \mathbb{F}_{p^s} be the finite field with p^s elements and $\mathbb{F}_{p^s}^*$ be its multiplicative group.

An $[n, k, d]$ p -ary linear code C is a k -dimensional subspace of \mathbb{F}_p^n with minimum (Hamming) distance d . For $i \in \{1, 2, \dots, n\}$, denote by A_i the number of codewords in C with Hamming weight i . The sequence $(1, A_1, \dots, A_n)$ is called the weight distribution of C and the polynomial $1 + A_1x + A_2x^2 + \dots + A_nx^n$ is called the weight enumerator of C . If the sequence (A_1, \dots, A_n) has t nonzero A_i with $i = 1, 2, \dots, n$, then the code C is called a t -weight code. In coding theory, the weight distribution of linear codes is a classical research topic and attracts much attention. Furthermore, linear codes with a few weights have important applications in authentication codes [10], association schemes [5], secret sharing [33] and strongly regular graphs [6].

Motivated by applications to cryptography, generalized Hamming weight of linear codes was introduced in 1970s [12, 19]. For linear code C , denote by $[C, r]_p$ the set of all its \mathbb{F}_p -vector subspaces with dimension

2010 *Mathematics Subject Classification.* 94B05, 11T71.

Key words and phrases. Weight distribution, Weight hierarchy, Linear code, Generalized Hamming weight.

r . For $V \in [C, r]_p$, define $\text{Supp}(V) = \cup_{c \in V} \text{Supp}(c)$, where $\text{Supp}(c)$ is the set of coordinates where c is nonzero, that is,

$$\text{Supp}(V) = \{i : 1 \leq i \leq n, c_i \neq 0 \text{ for some } c = (c_1, c_2, \dots, c_n) \in V\}.$$

Definition 1.1. Let C be an $[n, k, d]$ linear code over \mathbb{F}_p . For $1 \leq r \leq k$,

$$d_r(C) = \min\{|\text{Supp}(V)| : V \in [C, r]_p\}$$

is called the r -th generalized Hamming weight (GHW) of C and $\{d_r(C) : 1 \leq r \leq k\}$ is called the weight hierarchy of C .

GHW can be thought of an extension of the minimum distance $d = d_1(C)$ and has become an important research object in coding theory after Wei's paper [31] in 1991. A detailed overview on the results of GHW up to 1995 was given in [30]. The weight hierarchy of linear codes has many applications such as completely characterizing the performance of the code on the type II wire-tap channel, dealing with t -resilient functions and trellis or branch complexity of linear codes and so on [13, 30, 31]. Much is known about weight hierarchy for several classes of codes: algebraic geometric codes, BCH codes, Reed-Muller codes, cyclic codes [1, 4, 14, 18, 32, 34]. Recently, there are research results about weight hierarchy of some classes of linear codes [3, 16, 26, 27].

The rest of this paper is organized as follows. In Sec. 2, we introduce a generalized method of constructing linear code by defining sets and give a corresponding formula for computing the generalized Hamming weights. In Sec. 3, we construct binary linear codes with a few weights and determine their weight distributions and weight hierarchies completely. In Sec. 4, we summarize the paper.

2. PRELIMINARIES

2.1. A generic construction of linear codes. Ding et al. [9] proposed a generic construction of linear codes as below. Denote by Tr the trace function from \mathbb{F}_{p^s} to \mathbb{F}_p . Let $D = \{d_1, d_2, \dots, d_n\}$ be a subset of $\mathbb{F}_{p^s}^*$. A p -ary linear code of length n is defined as follows:

$$(2.1) \quad C_D = \{(\text{Tr}(xd_1), \text{Tr}(xd_2), \dots, \text{Tr}(xd_n)) : x \in \mathbb{F}_{p^s}\},$$

and D is called the defining set of C_D . By choosing some proper defining sets, some optimal linear codes with a few weights can be constructed [7, 8, 11, 20, 21, 22, 29, 35, 36].

Li et al. generalized the above constructing method and also constructed some linear codes with a few weights [24, 25]. The generalized method is as follows. For a positive integer e , let $D = \{d_1, d_2, \dots, d_n\}$

be contained in $\mathbb{F}_{p^s}^e \setminus \{(0, 0, \dots, 0)\}$. For $u = (u_1, u_2, \dots, u_e)$, $v = (v_1, v_2, \dots, v_e)$, denote by $u \cdot v$ the ordinary inner product of u and v , that is,

$$u \cdot v = u_1v_1 + u_2v_2 + \dots + u_ev_e.$$

Define a p -ary linear code C_D with length n as follows:

$$(2.2) \quad C_D = \{(\text{Tr}(x \cdot d_1), \text{Tr}(x \cdot d_2), \dots, \text{Tr}(x \cdot d_n)) : x \in \mathbb{F}_{p^s}^e\}.$$

Here, D is also called the defining set. Using this method, some classes of linear codes with few weights were obtained by choosing proper defining sets [2, 17].

2.2. A formula for computing $d_r(C_D)$. For the linear code C_D in (2.2), a general formula in Proposition 2.1 will be employed to calculate the generalized Hamming weight $d_r(C_D)$. Indeed, the result of Proposition 2.1 can be regarded as a generalization of [26, Theorem 1].

Proposition 2.1. *For each r and $1 \leq r \leq es$, if the dimension of C_D is es , then*

$$d_r(C_D) = n - \max \{|D \cap H| : H \in [\mathbb{F}_{p^s}^e, es - r]_p\}.$$

Proof. Let f be a map from $\mathbb{F}_{p^s}^e$ to \mathbb{F}_p^n defined by

$$f(x) = (\text{Tr}(x \cdot d_1), \text{Tr}(x \cdot d_2), \dots, \text{Tr}(x \cdot d_n)).$$

Obviously, f is an \mathbb{F}_p -linear homomorphism and the image $f(\mathbb{F}_{p^s}^e)$ is C_D . By hypothesis, we know that the dimension of C_D is es . Hence, f is injective.

For any r -dimensional subspace $U_r \in [C_D, r]_p$, denote by $H_r = f^{-1}(U_r)$ the inverse image of U_r . So, H_r is also an r -dimensional subspace. Let $\{\beta_1, \beta_2, \dots, \beta_r\}$ be an \mathbb{F}_p -basis of H_r . By definition,

$$d_r(C_D) = n - \max\{N(U_r) : U_r \in [C_D, r]_p\},$$

where

$$\begin{aligned} N(U_r) &= \left| \{i : 1 \leq i \leq n, c_i = 0 \text{ for any } c = (c_1, c_2, \dots, c_n) \in U_r\} \right| \\ &= \left| \{i : 1 \leq i \leq n, \text{Tr}(\beta \cdot d_i) = 0 \text{ for any } \beta \in H_r\} \right| \\ &= \left| \{i : 1 \leq i \leq n, \text{Tr}(\beta_j \cdot d_i) = 0, j = 1, 2, \dots, r\} \right|. \end{aligned}$$

Then, by the orthogonal property of additive characters, we have

$$\begin{aligned}
N(U_r) &= \frac{1}{p^r} \sum_{i=1}^n \sum_{x_1 \in \mathbb{F}_p} \zeta_p^{\text{Tr}(x_1(\beta_1 \cdot d_i))} \cdots \sum_{x_r \in \mathbb{F}_p} \zeta_p^{\text{Tr}(x_r(\beta_r \cdot d_i))} \\
&= \frac{1}{p^r} \sum_{i=1}^n \sum_{x_1, \dots, x_r \in \mathbb{F}_p} \zeta_p^{\text{Tr}((\beta_1 x_1 + \dots + \beta_r x_r) \cdot d_i)} \\
&= \frac{1}{p^r} \sum_{i=1}^n \sum_{\beta \in H_r} \zeta_p^{\text{Tr}(\beta \cdot d_i)}.
\end{aligned}$$

For any k -dimensional subspace H of $\mathbb{F}_{p^s}^e$, let

$$H^\perp = \{v \in \mathbb{F}_{p^s}^e : \text{Tr}(u \cdot v) = 0 \text{ for any } u \in H\}.$$

We call H^\perp the dual space of H . Taking a \mathbb{F}_p -basis $\alpha_1, \alpha_2, \dots, \alpha_{es}$ of $\mathbb{F}_{p^s}^e$ and $\gamma_1, \gamma_2, \dots, \gamma_k$ of H , then the matrix $(\text{Tr}(\alpha_i \cdot \alpha_j))$ is an invertible matrix. For any $v = \sum_{i=1}^{es} x_i \alpha_i \in H^\perp$ with $x_i \in \mathbb{F}_p$, we have $\text{Tr}(\gamma_j \cdot v) = \sum_{i=1}^{es} x_i \text{Tr}(\gamma_j \cdot \alpha_i) = 0, j = 1, 2, \dots, k$. This is a system of linear equations of x_1, x_2, \dots, x_{es} and the rank of its coefficient matrix $(\text{Tr}(\gamma_j \cdot \alpha_i))$ is equal to k . Thus, $\dim_{\mathbb{F}_p}(H) + \dim_{\mathbb{F}_p}(H^\perp) = es$ and $(H^\perp)^\perp = H$. So, For $y \in \mathbb{F}_{p^s}^e$,

$$\sum_{\beta \in H_r} \zeta_p^{\text{Tr}(\beta \cdot y)} = \begin{cases} |H_r|, & \text{if } y \in H_r^\perp, \\ 0, & \text{otherwise.} \end{cases}$$

Hence, we have

$$N(U_r) = \frac{1}{p^r} \sum_{y \in D \cap H_r^\perp} |H_r| = |D \cap H_r^\perp|.$$

So, the desired result follows from the fact that there is a bijection between $[\mathbb{F}_{p^s}^e, r]_p$ and $[\mathbb{F}_{p^s}^e, es - r]_p$. We complete the proof. \square

3. TWO CLASSES OF BINARY LINEAR CODES

In this section, we construct two classes of binary linear codes and determine their parameters. We firstly present a few more auxiliary results which will be needed in proving our main results.

Let l be a prime such that 2 is a primitive root modulo l^m . Here and after, let $p = 2, q = 2^{\phi(l^m)}$, where ϕ is the Euler phi-function. Let γ be a fixed primitive element of \mathbb{F}_q^* and χ_1 be the *canonical additive character* over \mathbb{F}_q , then for any $x \in \mathbb{F}_q$, $\chi_1(x) = (-1)^{\text{Tr}(x)}$. Set $\alpha = \gamma^{\frac{q-1}{l^m}}$. See [23] for more information about additive characters over finite fields.

3.1. An exponential sum. For any $a, b \in \mathbb{F}_q$, we define

$$S(a, b) = \sum_{x \in \mathbb{F}_q^*} \chi_1 \left(ax^{\frac{q-1}{l^m}} + bx \right) \quad \text{and} \quad S(a) = \sum_{i=0}^{l^m-1} \chi_1(a\alpha^i).$$

Since 2 is a primitive root modulo l^m , we have that $\mathbb{F}_q = \mathbb{F}_2(\alpha)$. Expressing $u \in \mathbb{F}_q$ in the basis $\{\alpha, \alpha^2, \dots, \alpha^{\phi(l^m)}\}$, say

$$u = \sum_{i=1}^{\phi(l^m)} a_i \alpha^i,$$

where $a_i \in \mathbb{F}_2$. For $i = 0, 1, \dots, l^{m-1} - 1$, we denote by $u^{(i)}$ the following sub-vector of length $l - 1$ of the coordinate vector $u = (a_1, \dots, a_{\phi(l^m)})$ of u :

$$u^{(i)} = (a_{l^{m-1}-i}, a_{2l^{m-1}-i}, \dots, a_{(l-1)l^{m-1}-i}).$$

Recall that $\text{wt}(x)$ is the Hamming weight of binary vector x . For $a \in \mathbb{F}_q^*$, we define two subsets of \mathbb{F}_q^* as follows.

$$E_a = \{u \in \mathbb{F}_q^* : 2 \mid \text{wt}((au^{-\frac{q-1}{l^m}})^{(0)})\},$$

$$O_a = \{u \in \mathbb{F}_q^* : 2 \nmid \text{wt}((au^{-\frac{q-1}{l^m}})^{(0)})\}.$$

In subsection 3.3, we will give the cardinal numbers of E_a and O_a .

Now, we give some results on $S(a, b)$ and $S(a)$ in the following lemmas, which will play important roles in settling the parameters of our codes.

Lemma 3.1. [21, Lemma 4] *Let $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$ and let $c = ab^{-\frac{q-1}{l^m}}$ if $b \neq 0$. Then,*

$$S(a, b) = \begin{cases} \frac{q-1}{l^m} S(a), & \text{if } b = 0, \\ (-1)^{\text{wt}(c^{(0)})} \sqrt{q} - \frac{\sqrt{q}+1}{l^m} S(a), & \text{if } b \neq 0. \end{cases}$$

Lemma 3.2. [28, Theorem 1] *Let $a \in \mathbb{F}_q^*$. Then*

$$S(a) = \sum_{i=0}^{l^{m-1}-1} (-1)^{\text{wt}(a^{(i)})} (l - 2\text{wt}(a^{(i)})).$$

Lemma 3.3. [28, Theorem 3] *The value set of $S(a)$, as a runs over \mathbb{F}_q^* , is*

$$\{l^m - 4j \mid j = 1, \dots, \frac{l^{m-1}(l-1)}{2}\}.$$

3.2. Our defining sets and some auxiliary results. In this paper, we choose a defining set contained in \mathbb{F}_q^2 as follows. For $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, set

$D_{(a,b)} = \{(x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} : \text{Tr}(ax^{\frac{q-1}{l^m}} + by) = 0\} = \{d_1, d_2, \dots, d_n\}$
and the corresponding binary linear code $C_{D_{(a,b)}}$ is defined by

$$(3.1) \quad C_{D_{(a,b)}} = \left\{ (\text{Tr}(x \cdot d_1), \text{Tr}(x \cdot d_2), \dots, \text{Tr}(x \cdot d_n)) : x \in \mathbb{F}_q^2 \right\}.$$

Now, we first calculate the length of the linear codes $C_{D_{(a,b)}}$ and the Hamming weight of non-zero codewords in $C_{D_{(a,b)}}$.

Lemma 3.4. *For $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$. Then,*

$$n = |D_{(a,b)}| = \begin{cases} \frac{1}{2}q(q+1+S(a,0)) - 1, & \text{if } b = 0, \\ \frac{1}{2}q^2 - 1, & \text{if } b \neq 0. \end{cases}$$

Proof. By the orthogonal property of additive characters, we have

$$\begin{aligned} |D_{(a,b)}| &= \frac{1}{2} \sum_{x,y \in \mathbb{F}_q} \sum_{z \in \mathbb{F}_2} (-1)^{\text{Tr}(z(ax^{\frac{q-1}{l^m}} + by))} - 1 \\ &= \frac{1}{2} \sum_{x,y \in \mathbb{F}_q} (1 + (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}} + by)}) - 1 \\ &= \frac{1}{2}q^2 + \frac{1}{2} \sum_{x,y \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}} + by)} - 1 \\ &= \frac{1}{2}q^2 + \frac{1}{2} \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(by)} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}})} - 1. \end{aligned}$$

When $b = 0$, we have

$$\begin{aligned} |D_{(a,0)}| &= \frac{1}{2}q^2 + \frac{1}{2}q \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}})} - 1 \\ &= \frac{1}{2}q^2 + \frac{1}{2}q(1 + S(a,0)) - 1 \\ &= \frac{1}{2}q(q+1+S(a,0)) - 1. \end{aligned}$$

When $b \neq 0$, we have $\sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(by)} = 0$, which follows that $|D_{(a,b)}| = \frac{1}{2}q^2 - 1$. We complete the proof. \square

Let $c_{(u,v)}$ be the corresponding codeword in $C_{D_{(a,b)}}$ in (3.1) with $(u, v) \in \mathbb{F}_q^2$, that is,

$$c_{(u,v)} = \left(\text{Tr}(ux + vy) \right)_{(x,y) \in D_{(a,b)}}.$$

Obviously, $c_{(0,0)} = 0$ and $\text{wt}(c_{(0,0)}) = 0$. Now, we determine the Hamming weight $\text{wt}(c_{(u,v)})$ with $(u, v) \neq (0, 0)$ in the following lemma.

Lemma 3.5. *Let $(u, v) (\neq (0, 0)) \in \mathbb{F}_q^2$. We have*

(1) *If $b = 0$, then*

$$\text{wt}(c_{(u,v)}) = \begin{cases} \frac{1}{4}q(q+1+S(a,0)), & \text{if } v \neq 0, \\ \frac{1}{4}q(q+S(a,0)-S(a,u)), & \text{if } v = 0. \end{cases}$$

(2) *If $b \neq 0$, then*

$$\text{wt}(c_{(u,v)}) = \begin{cases} \frac{1}{4}q^2, & \text{if } v = 0 \text{ or } v \neq b, v \neq 0, \\ \frac{1}{4}q(q-1-S(a,u)), & \text{if } v = b. \end{cases}$$

Proof. Put $N(u, v) = \{(x, y) \in \mathbb{F}_q^2 : \text{Tr}(ax^{\frac{q-1}{l^m}} + by) = 0, \text{Tr}(ux + vy) = 0\}$, then

$$\begin{aligned} |N(u, v)| &= \frac{1}{4} \sum_{x, y \in \mathbb{F}_q} \left(\sum_{z_1 \in \mathbb{F}_2} (-1)^{\text{Tr}(z_1(ax^{\frac{q-1}{l^m}} + by))} \sum_{z_2 \in \mathbb{F}_2} (-1)^{\text{Tr}(z_2(ux + vy))} \right) \\ &= \frac{1}{4} \sum_{x, y \in \mathbb{F}_q} \left((1 + (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}} + by)}) (1 + (-1)^{\text{Tr}(ux + vy)}) \right) \\ &= \frac{1}{4}q^2 + \frac{1}{4} \sum_{x, y \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}} + by)} + \frac{1}{4} \sum_{x, y \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}} + ux + by + vy)}, \end{aligned}$$

where we use the fact that

$$\sum_{x, y \in \mathbb{F}_q} (-1)^{\text{Tr}(ux + vy)} = \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ux)} \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(vy)} = 0.$$

Now we discuss case by case on the term of $b = 0$ or $b \neq 0$.

(1) If $b = 0$, then

$$\begin{aligned} |N(u, v)| &= \frac{1}{4} \left(q^2 + \sum_{x, y \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}})} + \sum_{x, y \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}} + ux + vy)} \right) \\ &= \frac{1}{4} \left(q^2 + q \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}})} + \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(vy)} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax^{\frac{q-1}{l^m}} + ux)} \right) \\ &= \frac{1}{4} \left(q^2 + q(1 + S(a, 0)) + (1 + S(a, u)) \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(vy)} \right). \end{aligned}$$

So, we have

$$|N(u, v)| = \begin{cases} \frac{1}{4}q(q+1+S(a,0)), & \text{if } v \neq 0, \\ \frac{1}{4}q(q+2+S(a,0)+S(a,u)), & \text{if } v = 0. \end{cases}$$

Noting that $\text{wt}(c_{(u,v)}) = n - |N(u, v)| + 1$. By Lemma 3.4, we have

$$\text{wt}(c_{(u,v)}) = \begin{cases} \frac{1}{4}q(q+1+S(a,0)), & \text{if } v \neq 0, \\ \frac{1}{4}q(q+S(a,0)-S(a,u)), & \text{if } v = 0. \end{cases}$$

(2) If $b \neq 0$, then

$$\sum_{x,y \in \mathbb{F}_q} (-1)^{\text{Tr}(ax \frac{q-1}{l^m} + by)} = \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax \frac{q-1}{l^m})} \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(by)} = 0,$$

which follows that

$$\begin{aligned} |N(u, v)| &= \frac{1}{4}q^2 + \frac{1}{4} \sum_{x,y \in \mathbb{F}_q} (-1)^{\text{Tr}(ax \frac{q-1}{l^m} + by + ux + vy)} \\ &= \frac{1}{4}q^2 + \frac{1}{4} \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}((b+v)y)} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax \frac{q-1}{l^m} + ux)} \\ &= \frac{1}{4}q^2 + \frac{1}{4}(1 + S(a, u)) \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}((b+v)y)}. \end{aligned}$$

So, we have

$$|N(u, v)| = \begin{cases} \frac{1}{4}q^2, & \text{if } v = 0, \\ \frac{1}{4}q(q+1+S(a, u)), & \text{if } v = b, \\ \frac{1}{4}q^2, & \text{if } v \neq b, v \neq 0. \end{cases}$$

By Lemma 3.4 again, we have

$$\text{wt}(c_{(u,v)}) = \begin{cases} \frac{1}{4}q^2, & \text{if } v = 0, \\ \frac{1}{4}q(q-1-S(a, u)), & \text{if } v = b, \\ \frac{1}{4}q^2, & \text{if } v \neq b, v \neq 0. \end{cases}$$

The proof is finished. \square

Remark 3.6. By Lemma 3.5, we know that, for $(u, v) (\neq (0, 0)) \in \mathbb{F}_q^2$, we have $\text{wt}(c_{(u,v)}) > 0$. So, the map: $\mathbb{F}_q^2 \rightarrow C_{D_{(a,b)}}$ defined by $(u, v) \mapsto c_{(u,v)}$ is an isomorphism as linear spaces over \mathbb{F}_2 . Hence, the dimension of the codes $C_{D_{(a,b)}}$ in (3.1) is equal to $2\phi(l^m)$.

Lemma 3.7. Let $C_{D_{(a,b)}}$ be defined in (3.1). Then, the minimal distance of the dual code $C_{D_{(a,b)}}^\perp$ is at least 2.

Proof. We prove it by contradiction. If not, then there exists a coordinate i such that the i -th entry of all of the codewords of $C_{D_{(a,b)}}$ is 0, that is, $\text{Tr}(x \cdot d_i) = 0$ for all $x \in \mathbb{F}_q^2$, where $d_i \in D_{(a,b)}$. Thus, by the properties of the trace function, we have $d_i = 0$. It contradicts with $d_i \neq 0$. \square

3.3. Weight distribution of $C_{D_{(a,b)}}$ in (3.1). In this sequel, we determine the weight distributions of linear codes $C_{D_{(a,b)}}$ in (3.1).

Theorem 3.8. *Let $a \in \mathbb{F}_q^*$. The code $C_{D_{(a,0)}}$ in (3.1) is an $[n, 2\phi(l^m), d]$ binary linear code with the weight distribution in Table 1, where $d = \frac{1}{4}q(q - \sqrt{q} + \frac{(q+\sqrt{q})S(a)}{l^m})$ and $n = \frac{1}{2}q(q + 1 + \frac{q-1}{l^m}S(a)) - 1$.*

TABLE 1. The weight distribution of the codes of Theorem 1.

Weight ω	Multiplicity A_ω
0	1
$\frac{1}{4}q(q + 1 + \frac{(q-1)S(a)}{l^m})$	$q(q - 1)$
$\frac{1}{4}q(q + \sqrt{q} + \frac{(q+\sqrt{q})S(a)}{l^m})$	$\frac{1}{2}(q - 1)(1 + \frac{S(a)}{l^m})$
$\frac{1}{4}q(q - \sqrt{q} + \frac{(q+\sqrt{q})S(a)}{l^m})$	$\frac{1}{2}(q - 1)(1 - \frac{S(a)}{l^m})$

Proof. Assume that $(u, v) \neq (0, 0)$. By Lemma 3.1 and Lemma 3.5, $\text{wt}(c_{(u,v)})$ has only three values, that is,

$$\begin{cases} \omega_1 = \frac{1}{4}q(q + 1 + \frac{(q-1)S(a)}{l^m}), \\ \omega_2 = \frac{1}{4}q(q + \sqrt{q} + \frac{(q+\sqrt{q})S(a)}{l^m}), \\ \omega_3 = \frac{1}{4}q(q - \sqrt{q} + \frac{(q+\sqrt{q})S(a)}{l^m}). \end{cases}$$

Recall that A_{ω_i} is the multiplicity of ω_i . By Lemma 3.5, we have $A_{\omega_1} = q(q - 1)$. By Lemma 3.7 and the first two Pless Power Moment ([15, P. 260]), we obtain the system of linear equations as follows:

$$\begin{cases} A_{\omega_1} = q(q - 1), \\ A_{\omega_2} + A_{\omega_3} = q - 1, \\ \omega_1 A_{\omega_1} + \omega_2 A_{\omega_2} + \omega_3 A_{\omega_3} = \frac{1}{2}q^2n. \end{cases}$$

Solving the system, we get

$$\begin{cases} A_{\omega_1} = q(q - 1), \\ A_{\omega_2} = \frac{1}{2}(q - 1)(1 - \frac{S(a)}{l^m}), \\ A_{\omega_3} = \frac{1}{2}(q - 1)(1 + \frac{S(a)}{l^m}). \end{cases}$$

Then we get the weight distribution of Table 1. By Lemma 3.3, of all the non-zero weights, ω_3 is the smallest. So we get the value of minimum Hamming weight $d = \omega_3$. We complete the proof. \square

Corollary 3.9. *For each $a \in \mathbb{F}_q^*$, we have $|E_a| = \frac{1}{2}(q - 1)(1 + \frac{S(a)}{l^m})$ and $|O_a| = \frac{1}{2}(q - 1)(1 - \frac{S(a)}{l^m})$.*

Proof. Recall the definitions of E_a and O_a in Subsection 3.1. Obviously, $|E_a| + |O_a| = q - 1$. By Lemma 3.1,

$$S(a, u) = (-1)^{\text{wt}((au^{-\frac{q-1}{l^m}})^{(0)})} \sqrt{q} - \frac{\sqrt{q} + 1}{l^m} S(a).$$

For a code word $c_{(u,v)} \in C_{D_{(a,0)}}$, by the computing of $|N(u, v)|$, we know that $\text{wt}(c_{(u,v)}) = \frac{1}{4}q(q - \sqrt{q} + \frac{(q+\sqrt{q})S(a)}{l^m})$ if and only if $2|\text{wt}((au^{-\frac{q-1}{l^m}})^{(0)})|$. So the desired result follows from Theorem 3.8. The proof is completed. \square

Remark 3.10. By Lemma 3.3, we know that neither E_a nor O_a is empty for every $a \in \mathbb{F}_q^*$.

Example 3.11. Let $(l, m, a, b) = (3, 2, 1, 0)$. Then, the corresponding code $C_{D_{(1,0)}}$ has parameters $[3199, 12, 1536]$ and weight enumerator $1 + 49x^{1536} + 4032x^{1600} + 14x^{1792}$.

Theorem 3.12. Let $a, b \in \mathbb{F}_q^*$. The code $C_{D_{(a,b)}}$ in (3.1) is a $[\frac{1}{2}q^2 - 1, 2\phi(l^m)]$ binary linear code with the weight distribution in Table 2.

TABLE 2. The weight distribution of the codes of Theorem 2.

Weight ω	Multiplicity A_ω
0	1
$\frac{1}{4}q(q - 1 - \frac{(q-1)S(a)}{l^m})$	1
$\frac{1}{4}q(q - 1 - \sqrt{q} + \frac{(1+\sqrt{q})S(a)}{l^m})$	$\frac{1}{2}(q - 1)(1 + \frac{S(a)}{l^m})$
$\frac{1}{4}q(q - 1 + \sqrt{q} + \frac{(1+\sqrt{q})S(a)}{l^m})$	$\frac{1}{2}(q - 1)(1 - \frac{S(a)}{l^m})$
$\frac{1}{4}q^2$	$q^2 - q - 1$

Proof. Assume that $(u, v) \neq (0, 0)$. By Lemma 3.1 and Lemma 3.5, $\text{wt}(c_{(u,v)})$ has only four values, that is,

$$\begin{cases} \omega_1 = \frac{1}{4}q(q - 1 - \frac{(q-1)S(a)}{l^m}), \\ \omega_2 = \frac{1}{4}q(q - 1 - \sqrt{q} + \frac{(1+\sqrt{q})S(a)}{l^m}), \\ \omega_3 = \frac{1}{4}q(q - 1 + \sqrt{q} + \frac{(1+\sqrt{q})S(a)}{l^m}), \\ \omega_4 = \frac{1}{4}q^2. \end{cases}$$

By the computation of $|N(u, v)|$ in Lemma 3.5 and Corollary 3.9, it is easy to get the multiplicity A_{ω_i} of ω_i . They are listed as follows.

$$\begin{cases} A_{\omega_1} = 1, \\ A_{\omega_2} = \frac{1}{2}(q - 1)(1 + \frac{S(a)}{l^m}), \\ A_{\omega_3} = \frac{1}{2}(q - 1)(1 - \frac{S(a)}{l^m}), \\ A_{\omega_4} = q^2 - q - 1. \end{cases}$$

Then we get the weight distribution of Table 2. The proof is finished. \square

Example 3.13. Let $(l, m, a, b) = (3, 2, 1, 1)$. Then, the corresponding code $C_{D_{(a,b)}}$ has parameters $[2047, 12, 448]$ and weight enumerator $1 + x^{448} + 49x^{960} + 14x^{1216} + 4031x^{1024}$.

Example 3.14. Let $(l, m, a, b) = (5, 1, 1, 1)$. Then, the corresponding code $C_{D_{(a,b)}}$ has parameters $[127, 8, 32]$ and weight enumerator $1 + x^{96} + 251x^{64} + 3x^{32}$.

Remark 3.15. In Example 3, when $(l, m, a, b) = (5, 1, 1, 1)$, the last two weights of $C_{D_{(a,b)}}$ equal. So it is a 3-weight code.

3.4. Weight hierarchy of $C_{D_{(a,b)}}$ in (3.1). Let H_r be an r -dimensional subspace of \mathbb{F}_q^2 and $\beta_1, \beta_2, \dots, \beta_r$ be an \mathbb{F}_2 -basis of H_r . We set

$$N(H_r) = \{x = (x, y) \in \mathbb{F}_q^2 : \text{Tr}(ax^{\frac{q-1}{m}} + by) = 0, \text{Tr}(x \cdot \beta_j) = 0, 1 \leq j \leq r\}.$$

Then, $N(H_r) = (D_{(a,b)} \cap H_r^\perp) \cup \{(0, 0)\}$, which concludes that $|N(H_r)| = |D_{(a,b)} \cap H_r^\perp| + 1$.

So, by Remark 3.6 and the proof of proposition 2.1, we have

$$\begin{aligned} d_r(C_{D_{(a,b)}}) \\ (3.2) \end{aligned} = n - \max \left\{ |D_{(a,b)} \cap H_{2\phi(l^m)-r}| : H_{2\phi(l^m)-r} \in [\mathbb{F}_q^2, 2\phi(l^m) - r]_p \right\}$$

$$\begin{aligned} (3.3) \\ = n - \max \left\{ |N(H_r)| : H_r \in [\mathbb{F}_q^2, r]_p \right\} + 1. \end{aligned}$$

Proposition 3.16. Define $B_{H_r} = \sum_{(x,y) \in \mathbb{F}_q^2} \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot (x,y) + ax^{\frac{q-1}{m}} + by)}$. Then,

$$d_r(C_{D_{(a,b)}}) = n - \frac{1}{2^{r+1}} q^2 - \frac{1}{2^{r+1}} \max \left\{ B_{H_r} : H_r \in [\mathbb{F}_q^2, r]_p \right\} + 1.$$

Proof. By the orthogonal property of additive characters, we have

$$\begin{aligned}
& 2^{r+1}|N(H_r)| \\
&= \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \left(\sum_{z \in \mathbb{F}_2} (-1)^{\text{Tr}(z(ax \frac{q-1}{l^m} + by))} \prod_{i=1}^r \sum_{x_i \in \mathbb{F}_2} (-1)^{\text{Tr}(x_i(x \cdot \beta_i))} \right) \\
&= \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \left(\sum_{z \in \mathbb{F}_2} (-1)^{\text{Tr}(z(ax \frac{q-1}{l^m} + by))} \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot \mathbf{x})} \right) \\
&= \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \left((1 + (-1)^{\text{Tr}(ax \frac{q-1}{l^m} + by)}) \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot \mathbf{x})} \right) \\
&= \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot \mathbf{x})} + \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot \mathbf{x} + ax \frac{q-1}{l^m} + by)} \\
&= q^2 + \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot \mathbf{x} + ax \frac{q-1}{l^m} + by)},
\end{aligned}$$

where the last equation comes from

$$\begin{aligned}
\sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot \mathbf{x})} &= \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} 1 + \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} \sum_{(0,0) \neq \beta \in H_r} (-1)^{\text{Tr}(\beta \cdot \mathbf{x})} \\
&= q^2 + \sum_{(0,0) \neq \beta \in H_r} \sum_{\mathbf{x}=(x,y) \in \mathbb{F}_q^2} (-1)^{\text{Tr}(\beta \cdot \mathbf{x})} = q^2.
\end{aligned}$$

So, the desired result is obtained. Thus, we complete the proof. \square

In the following sequel, we shall determine the weight hierarchy of $C_{D(a,b)}$ by calculating B_{H_r} in Proposition 3.16 and $|D_{(a,b)} \cap H_{2\phi(l^m)-r}|$ in (3.2).

Theorem 3.17. *Let $a \in \mathbb{F}_q^*$ and $C_{D(a,0)}$ defined in (3.1). Then*

$$d_r(C_{D(a,0)}) = \begin{cases} \frac{1}{2}q \left(1 - \frac{1}{2^r}\right) \left(q - \sqrt{q} + \frac{(q+\sqrt{q})S(a)}{l^m}\right), & \text{if } 1 \leq r \leq \frac{1}{2}\phi(l^m), \\ \frac{1}{2}q \left(q + 1 + \frac{(q-1)S(a)}{l^m}\right) - \frac{1}{2^r}q^2, & \text{if } \frac{1}{2}\phi(l^m) < r \leq 2\phi(l^m). \end{cases}$$

Proof. When $1 \leq r \leq \frac{1}{2}\phi(l^m)$, by the definition of B_{H_r} , we have

$$\begin{aligned}
B_{H_r} &= \sum_{x=(x,y) \in \mathbb{F}_q^2} \sum_{\beta \in H_r} (-1)^{\text{Tr}(\beta \cdot x + ax \frac{q-1}{l^m})} \\
&= \sum_{(x,y) \in \mathbb{F}_q^2} \left(\sum_{(\beta_1, 0) \in H_r} (-1)^{\text{Tr}(\beta_1 x + ax \frac{q-1}{l^m})} + \sum_{\substack{(\beta_1, \beta_2) \in H_r \\ \beta_2 \neq 0}} (-1)^{\text{Tr}(\beta_1 x + \beta_2 y + ax \frac{q-1}{l^m})} \right) \\
&= q \sum_{(\beta_1, 0) \in H_r} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(\beta_1 x + ax \frac{q-1}{l^m})} \\
&= q \sum_{(\beta_1, 0) \in H_r} \left(1 + S(a, \beta_1) \right).
\end{aligned}$$

So, by lemma 3.1, we obtain

$$\begin{aligned}
\frac{1}{q} B_{H_r} &= \sum_{(\beta_1, 0) \in H_r} \left(1 - \frac{(\sqrt{q} + 1)S(a)}{l^m} \right) + \sqrt{q} \sum_{\substack{(\beta_1, 0) \in H_r \\ \beta_1 \neq 0}} (-1)^{\text{wt}((a\beta_1^{-\frac{q-1}{l^m}})^{(0)})} \\
&\quad + \frac{(\sqrt{q} + q)S(a)}{l^m}.
\end{aligned}$$

By Corollary 3.9, there is an element $\beta \in \mathbb{F}_q^*$ such that $\text{wt}((a\beta^{-\frac{q-1}{l^m}})^{(0)})$ is even. Recall that 2 is a primitive root modulo l^m and $q = 2^{\phi(l^m)}$, we have $q \equiv 1 \pmod{l^m}$, which concludes that $\sqrt{q} \equiv -1 \pmod{l^m}$, i.e. $l^m \mid \sqrt{q} + 1$. Since $\sqrt{q} - 1$ and $\sqrt{q} + 1$ are coprime, we have $(\beta u)^{-\frac{q-1}{l^m}} = \beta^{-\frac{q-1}{l^m}} (u\sqrt{q}-1)^{-\frac{\sqrt{q}+1}{l^m}} = \beta^{-\frac{q-1}{l^m}}$ for any $u \in \mathbb{F}_{\sqrt{q}}^*$. Take an r -dimensional subspace L_r contained in $\beta \mathbb{F}_{\sqrt{q}}$ and Put $H_r = L_r \times O$, then, for any $(\beta_1, 0) \in H_r$, we have $\text{wt}((a\beta_1^{-\frac{q-1}{l^m}})^{(0)})$ is even. Furthermore, by Lemma 3.3, we have $-\sqrt{q} < 1 - \frac{(\sqrt{q}+1)S(a)}{l^m} < \sqrt{q}$, which follows that $1 - \frac{(\sqrt{q}+1)S(a)}{l^m} + \sqrt{q} > 0$. Hence, $\frac{1}{q} B_{H_r}$ reaches its maximum

$$2^r \left(1 - \frac{(\sqrt{q} + 1)S(a)}{l^m} + \sqrt{q} \right) + \frac{(\sqrt{q} + q)S(a)}{l^m} - \sqrt{q}.$$

So, by Proposition 3.16, we obtain the generalized Hamming weights $d_r(C_{D(a,0)})$ for $1 \leq r \leq \frac{1}{2}\phi(l^m)$.

When $\frac{1}{2}\phi(l^m) < r < 2\phi(l^m)$, we have $1 \leq 2\phi(l^m) - r < \frac{3}{2}\phi(l^m)$. By Lemma 3.4 and Lemma 3.3, there exists an element $(x, y) \in D(a,0)$ such that $x \in \mathbb{F}_q^*$, that is, $\text{Tr}(ax \frac{q-1}{l^m}) = 0$ and $x \neq 0$. Then, for any $u \in \mathbb{F}_{\sqrt{q}}^*$, we have $\text{Tr}(a(xu) \frac{q-1}{l^m}) = \text{Tr}(ax \frac{q-1}{l^m}) = 0$. So, $x\mathbb{F}_{\sqrt{q}} \times \mathbb{F}_q \subset D(a,0)$. Note that the dimension of the subspace $x\mathbb{F}_{\sqrt{q}} \times \mathbb{F}_q \subset \mathbb{F}_q^2$ is $\frac{3}{2}\phi(l^m)$. Let

$H_{2\phi(l^m)-r}$ be a $(2\phi(l^m) - r)$ -dimensional subspace of $x\mathbb{F}_{\sqrt{q}} \times \mathbb{F}_q$. So,

$$|H_{2\phi(l^m)-r} \cap D_{(a,0)}| = 2^{2\phi(l^m)-r} - 1,$$

Then,

$$\max\{|D_{(a,0)} \cap H| : H \in [\mathbb{F}_{p^m}, 2\phi(l^m) - r]_p\} = 2^{2\phi(l^m)-r} - 1.$$

By the equation (2.1), for $\frac{1}{2}\phi(l^m) < r < 2\phi(l^m)$, we have

$$\begin{aligned} d_r(C_{D_{(a,0)}}) &= n - 2^{2\phi(l^m)-r} + 1 \\ &= \frac{1}{2}q \left(q + 1 + \frac{(q-1)S(a)}{l^m} \right) - \frac{1}{2r}q^2. \end{aligned}$$

Thus, we complete the proof. \square

Theorem 3.18. *Let $a, b \in \mathbb{F}_q^*$ and $C_{D_{(a,b)}}$ defined in (3.1). Then,*

(1) *If $1 \leq r \leq \frac{1}{2}\phi(l^m)$, we have*

$$d_r(C_{D_{(a,b)}}) = \begin{cases} \frac{1}{2}q^2 \left(1 - \frac{1}{2^r} \right) - \frac{q(\sqrt{q}+1)}{4} \left(1 - \frac{S(a)}{l^m} \right), & \text{if } S(a) < 0, \\ \frac{1}{2}q^2 \left(1 - \frac{1}{2^r} \right) - \frac{q(\sqrt{q}+1)}{4} \left(1 - \frac{S(a)}{l^m} \right) + \frac{q\sqrt{q}}{2^{r+1}} \left(1 - \frac{\sqrt{q}+1}{l^m} S(a) \right), & \text{if } S(a) > 0. \end{cases}$$

(2) *If $\frac{1}{2}\phi(l^m) < r \leq 2\phi(l^m)$, we have*

$$d_r(C_{D_{(a,b)}}) = \frac{1}{2}q^2 \left(1 - \frac{1}{2^{r-1}} \right).$$

Proof. (1) When $1 \leq r \leq \frac{1}{2}\phi(l^m)$, by the definition of B_{H_r} , we have

$$\begin{aligned} B_{H_r} &= \sum_{(x,y) \in \mathbb{F}_q^2} \sum_{(\beta_1, \beta_2) \in H_r} (-1)^{\text{Tr}(ax \frac{q-1}{l^m} + \beta_1 x + \beta_2 y + by)} \\ &= \sum_{(\beta_1, \beta_2) \in H_r} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax \frac{q-1}{l^m} + \beta_1 x)} \sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(\beta_2 y + by)}. \end{aligned}$$

Let Prj_2 be the second projection from \mathbb{F}_q^2 to \mathbb{F}_q defined by $(x, y) \mapsto y$.

If $b \notin \text{Prj}_2(H_r)$, then $\sum_{y \in \mathbb{F}_q} (-1)^{\text{Tr}(\beta_2 y + by)} = 0$ for any $(\beta_1, \beta_2) \in H_r$, which follows that $B_{H_r} = 0$.

If $b \in \text{Prj}_2(H_r)$, by Lemma 3.1 again, we have

$$\frac{1}{q} B_{H_r} = \sum_{(\beta_1, b) \in H_r} \sum_{x \in \mathbb{F}_q} (-1)^{\text{Tr}(ax \frac{q-1}{l^m} + \beta_1 x)} = \sum_{(\beta_1, b) \in H_r} 1 + \sum_{(\beta_1, b) \in H_r} S(a, \beta_1)$$

$$= \begin{cases} \sum_{\substack{(\beta_1, b) \in H_r \\ \beta_1 \neq 0}} \left(1 - \frac{\sqrt{q}+1}{l^m} S(a) + (-1)^{\text{wt}((a\beta_1^{-\frac{q-1}{l^m}})^{(0)})} \sqrt{q} \right), & \text{if } (0, b) \notin H_r, \\ \sum_{\substack{(\beta_1, b) \in H_r \\ \beta_1 \neq 0}} \left(1 - \frac{\sqrt{q}+1}{l^m} S(a) + (-1)^{\text{wt}((a\beta_1^{-\frac{q-1}{l^m}})^{(0)})} \sqrt{q} \right) + 1 + \frac{q-1}{l^m} S(a), & \text{if } (0, b) \in H_r. \end{cases}$$

By Lemma 3.3, we have $1 - \frac{(\sqrt{q}+1)S(a)}{l^m} + \sqrt{q} > 0$. Take an element $\beta \in \mathbb{F}_q^*$ so that $\text{wt}((a\beta^{-\frac{q-1}{l^m}})^{(0)})$ is even and an $(r-1)$ -dimensional space L_{r-1} of $\beta\mathbb{F}_{\sqrt{q}}$. Then, we have $(\beta u)^{-\frac{q-1}{l^m}} = \beta^{-\frac{q-1}{l^m}} (u\sqrt{q-1})^{-\frac{\sqrt{q}+1}{l^m}} = \beta^{-\frac{q-1}{l^m}}$ for any $u \in \mathbb{F}_{\sqrt{q}}^*$. So, for any non-zero element $\beta_1 \in L_{r-1}$, $\text{wt}((a\beta_1^{-\frac{q-1}{l^m}})^{(0)})$ is even.

If $S(a) < 0$, set $H_r = \{(u, 0) : u \in L_{r-1}\} \cup \{(\xi + u, b) : u \in L_{r-1}\}$, where $\xi \in \beta\mathbb{F}_{\sqrt{q}} \setminus L_{r-1}$. Then, $(0, b) \notin H_r$. In this case, $\frac{1}{q}B_{H_r}$ reaches its maximum

$$2^{r-1} \left(1 - \frac{(\sqrt{q}+1)S(a)}{l^m} + \sqrt{q} \right).$$

If $S(a) > 0$, set $H_r = L_{r-1} \times b\mathbb{F}_2$. Then, $(0, b) \in H_r$. In this case, $\frac{1}{q}B_{H_r}$ reaches its maximum

$$2^{r-1} \left(1 - \frac{(\sqrt{q}+1)S(a)}{l^m} + \sqrt{q} \right) + \frac{(\sqrt{q}+q)S(a)}{l^m} - \sqrt{q}.$$

So, by Proposition 3.16, we obtain the generalized Hamming weights $d_r(C_{D(a,b)})$ for $1 \leq r \leq \frac{1}{2}\phi(l^m)$.

(2) For $\frac{1}{2}\phi(l^m) < r \leq 2\phi(l^m)$, we have $1 \leq 2\phi(l^m) - r \leq \frac{3}{2}\phi(l^m) - 1$. Take an element $x \in \mathbb{F}_q^*$ such that $\text{Tr}(ax^{\frac{q-1}{l^m}}) = 0$. Then, for any $u \in \mathbb{F}_{\sqrt{q}}^*$, we have $\text{Tr}(a(xu)^{\frac{q-1}{l^m}}) = \text{Tr}(ax^{\frac{q-1}{l^m}}) = 0$. Let $T_b = \{y \in \mathbb{F}_q : \text{Tr}(by) = 0\}$, which is a $(\phi(l^m) - 1)$ -dimensional subspace. So, $x\mathbb{F}_{\sqrt{q}} \times T_b \subset D_{(a,b)}$. Note that the dimension of the subspace $x\mathbb{F}_{\sqrt{q}} \times T_b \subset \mathbb{F}_q^2$ is $\frac{3}{2}\phi(l^m) - 1$. Let $H_{2\phi(l^m)-r}$ be a $(2\phi(l^m) - r)$ -dimensional subspace of $x\mathbb{F}_{\sqrt{q}} \times T_b$. So,

$$|H_{2\phi(l^m)-r} \cap D_{(a,b)}| = 2^{2\phi(l^m)-r} - 1,$$

Then,

$$\max\{|D_{(a,b)} \cap H| : H \in [\mathbb{F}_{p^m}, 2\phi(l^m) - r]_p\} = 2^{2\phi(l^m)-r} - 1.$$

By the equation (2.1), for $\frac{1}{2}\phi(l^m) < r < 2\phi(l^m)$, we have

$$d_r(C_{D(a,b)}) = n - \frac{1}{2r}q^2 = \frac{1}{2}q^2 \left(1 - \frac{1}{2^{r-1}} \right).$$

Thus, we complete the proof. \square

4. CONCLUDING REMARKS

The method of constructing linear codes by defining sets can be generalized. In this paper, we give a formula for calculating the weight hierarchies of linear codes constructed by the generalizes method. Then we construct two classes of 3-weight or 4-weight binary linear codes based on the generalized method. By the exponential sum theory, we give the weight distributions of these codes. Using our formula, we determine the weight hierarchies of these codes completely.

Let ω_{\min} and ω_{\max} be the minimum and maximum nonzero weight of the linear code $C_{D(a,0)}$, respectively. It is easy to check that

$$\frac{\omega_{\min}}{\omega_{\max}} > \frac{1}{2}.$$

By the results in [33], the binary linear codes $C_{D(a,0)}$ in Theorem 1 are suitable for constructing secret sharing schemes with interesting properties.

ACKNOWLEDGEMENT

For the research, the first author was supported by the National Science Foundation of China Grant No. 11701001 and Anhui Provincial Natural Science Foundation No. 1908085MA02, and the second author was supported by the National Science Foundation of China Grant No. 11701317.

REFERENCES

- [1] M. Bras-Amorós, K. Lee, and A. Vico-Oton, New lower bounds on the generalized Hamming weights of AG codes, *IEEE Trans. Inf. Theory* 60(10)(2014) 5930-5937.
- [2] J. Ahn, D. Ka, C. Li, Complete weight enumerators of a class of linear codes. *Des. Codes and Cryptogr.* 83(1)(2017) 83-99.
- [3] P. Beelen, A note on the generalized Hamming weights of Reed-Muller codes. *AAECC* 30(2019) 233-242 doi:10.1007/s00200-018-0369-8.
- [4] J. Cheng and C. Chao, On generalized Hamming weights of binary primitive BCH codes with minimum distance one less than a power of two. *IEEE Trans. Inf. Theory* 43(1)(1997) 294-298.
- [5] A. R. Calderbank, J. M. Goethals, Three-weight codes and association schemes. *Philips J. Res.* 39(1984) 143-152.
- [6] A. R. Calderbank, W. M. Kantor, The geometry of two-weight codes. *Bull. Lond. Math. Soc.* 18(1986) 97-122.
- [7] C. Ding, Linear codes from some 2-designs, *IEEE Trans. Inf. Theory* 61(6)(2015) 3265-3275.
- [8] K. Ding, C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, *IEEE Trans. Inf. Theory* 61(11)(2015) 5835-5842.
- [9] K. Ding, C. Ding, Binary linear codes with three weights, *IEEE Commun. Letters* 18(11)(2014) 1879-1882.

- [10] C. Ding, T. Helleseeth, T. Kløve, X. Wang, A generic construction of Cartesian authentication codes. *IEEE Trans. Inf. Theory* 53(6)(2007) 2229-2235.
- [11] C. Ding, C. Li, N. Li, Z. Zhou, Three-weight cyclic codes and their weight distributions. *Discrete Math.* 339(2)(2016) 415-427.
- [12] T. Helleseeth, T. Kløve, J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/N)$, *Discrete Math.* 18 (2) (1977): 179 - 211.
- [13] T. Helleseeth, T. Kløve, and O. Ytrehus, Generalized HammingWeights of Linear Codes, *IEEE Trans. Inf. Theory* 38(3)(1992)1133-1140.
- [14] P. Heijnen and R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, *IEEE Trans. Inf. Theory* 44(1)(1998) 181-196.
- [15] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge (2003).
- [16] G. Jian, R. Feng and H. Wu, Generalized Hamming weights of three classes of linear codes, *Finite Fields Th. App.* 45(2017) 341-354.
- [17] G. Jian, C. Lin and R. Feng, Two-weight and three-weight linear codes based on Weil sums, *Finite Fields Th. App.* 57(2019) 92-107.
- [18] H. Janwa and A. K. Lal, On the generalized Hamming weights of cyclic codes, *IEEE Trans. Inf. Theory* 43(1)(1997) 299-308.
- [19] T. Kløve, The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$, *Discrete Math.* 23 (2) (1978): 159 - 168.
- [20] X. Kong, S. Yang, Complete weight enumerators of a class of linear codes with two or three weights. *Discrete Math.* 342(11)(2019) 3166-3176.
- [21] Y. W. Liu and Z. H. Liu, On some classes of codes with a few weights, *Adv. Math. Commun.*, 12(2)(2018) 415-428.
- [22] H. Liu, Q. Liao, Several classes of linear codes with a few weights from defining sets over $F_p + uF_p$, *Des. Codes Cryptogr.* 87(1)(2017) 15-29.
- [23] R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, New York (1997).
- [24] C. Li, S. Bae, S. Yang, Some results on two-weight and three-weight linear codes, *Adv. Math. Commun.* 13(1) 195- 211. doi: 10.3934/amc.2019013.
- [25] C. Li, Q. Yue, F. Fu, A construction of several classes of two-weight and three-weight linear codes. *Applicable Algebra in Engineering Communication and Computing*, 28(1)(2018) 1-20.
- [26] F. Li, A class of cyclotomic linear codes and their generalized Hamming weights, *Applicable Algebra in Engineering, Communication and Computing* 29(2018) 501-511.
- [27] Z. Liu, J. Wang, Notes on generalized Hamming weights of some classes of binary codes. *Cryptogr. Commun.* (2019) doi:10.1007/s12095-019-00404-3
- [28] M. Moisio, Explicit evaluation of some exponential sums. *Finite Fields Th. App.* 15(6)(2009) 644-651.
- [29] C. Tang, C. Xiang, K. Feng, Linear codes with few weights from inhomogeneous quadratic functions. *Des. Codes Cryptogr.* 83(3)(2017) 691-714.
- [30] M. A. Tsfasman, S. G. Vlăduț, Geometric approach to higher weights, *IEEE Trans. Inf. Theory* 41(6)(1995) 1564-1588.
- [31] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inf. Theory* 37(5)(1991) 1412-1418.
- [32] M. Xiong, S. Li, and G. Ge, The weight hierarchy of some reducible cyclic codes. *IEEE Trans. Inf. Theory* 62(7)(2016) 4071-4080.
- [33] J. Yuan, C. Ding, Secret sharing schemes from three classes of linear codes. *IEEE Trans. Inf. Theory*, 52(1)(2006) 206-212.

- [34] M. Yang, J. Li, K. Feng and D. Lin, Generalized Hamming weights of irreducible cyclic codes, IEEE Trans. Inf. Theory 61(9)(2015) 4905-4913.
- [35] S. Yang, Z. A. Yao, C. A. Zhao, The weight distributions of two classes of p-ary cyclic codes with few weights. Finite Fields Th. App., 44(2017) 76-91.
- [36] Z. Zhou, N. Li, C. Fan and T. Helleseeth, Linear codes with two or three weights from quadratic bent functions, Des. Codes Cryptogr. 81(2)(2016) 283-295.

FACULTY OF SCHOOL OF STATISTICS AND APPLIED MATHEMATICS, ANHUI UNIVERSITY OF FINANCE AND ECONOMICS, BENGBU, ANHUI PROVINCE, 233030, CHINA

E-mail address: cczxlf@163.com; 120110029@aufe.edu.cn

SCHOOL OF MATHEMATICAL SCIENCES, QUFU NORMAL UNIVERSITY, QUFU SHANDONG, 273165, CHINA

E-mail address: lxiumei2013@qfnu.edu.cn