

Minimal linear codes from characteristic functions

Sihem Mesnager, Yanfeng Qi, Hongming Ru, Chunming Tang

Abstract

Minimal linear codes have interesting applications in secret sharing schemes and secure two-party computation. This paper uses characteristic functions of some subsets of \mathbb{F}_q to construct minimal linear codes. By properties of characteristic functions, we can obtain more minimal binary linear codes from known minimal binary linear codes, which generalizes results of Ding et al. [IEEE Trans. Inf. Theory, vol. 64, no. 10, pp. 6536-6545, 2018]. By characteristic functions corresponding to some subspaces of \mathbb{F}_q , we obtain many minimal linear codes, which generalizes results of [IEEE Trans. Inf. Theory, vol. 64, no. 10, pp. 6536-6545, 2018] and [IEEE Trans. Inf. Theory, vol. 65, no. 11, pp. 7067-7078, 2019]. Finally, we use characteristic functions to present a characterization of minimal linear codes from the defining set method and present a class of minimal linear codes.

Index Terms

Minimal linear code, characteristic function, subspace, weight distribution

I. INTRODUCTION

Throughout this paper, let p be a prime and $q = p^m$, where m is a positive integer. Let \mathbb{F}_q be the finite field with q elements and let \mathbb{F}_q^* be the multiplicative group of \mathbb{F}_q . An $[n, k, d]$ linear code \mathcal{C} over \mathbb{F}_q is a k -dimensional subspace of \mathbb{F}_q^n with minimum (Hamming) distance d . Let A_i be the number of codewords with Hamming weight i in \mathcal{C} . The weight enumerator of \mathcal{C} is the polynomial $1 + A_1z + \cdots + A_nz^n$ and the weight distribution of \mathcal{C} is $(1, A_1, \dots, A_n)$. The minimum distance d determines the error-correcting capability of \mathcal{C} . The weight distribution contains important information for estimating the probability of error detection and correction. Hence, the weight distribution attracts much attention in coding theory and many papers focus on the determination of the weight distributions of linear codes. Let t be the number of nonzero A_i in the weight distribution. Then the code \mathcal{C} is called a t -weight code. Linear codes can be applied in consumer electronics, communication and data storage system. Linear codes with few weights are important in secret sharing [11], [37], authentication codes [23], [26], association schemes [5] and strongly regular graphs [6].

For a vector $a = (a_1, \dots, a_n) \in \mathbb{F}_q^n$, let $\text{Suppt}(a) = \{1 \leq i \leq n : a_i \neq 0\}$ be the support of a and let $wt(a)$ be the Hamming weight of a . Note that $wt(a) = |\text{Suppt}(a)|$. A vector $a \in \mathbb{F}_q^n$ covers a vector $b \in \mathbb{F}_q^n$ if $\text{Suppt}(b) \subseteq \text{Suppt}(a)$. A codeword a in a linear code \mathcal{C} is minimal if a covers only the codeword ua for all $u \in \mathbb{F}_q^*$, but no other codewords in \mathcal{C} . A linear code \mathcal{C} is minimal if any codeword of \mathcal{C} is minimal. Minimal linear codes have interesting applications in secret sharing schemes [11], [25], [30], [37] and secure two-party computation [2], [16], [19]. A sufficient condition for a linear code to be minimal is given in the following lemma.

Lemma 1.1: [1] A linear code \mathcal{C} over \mathbb{F}_q is minimal if $\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}$, where w_{\min} and w_{\max} denote the minimum and maximum nonzero Hamming weights in the code \mathcal{C} respectively.

This work was supported by the National Natural Science Foundation of China (Grant No. 11871058, 11531002, 11701129). S. Mesnager is supported by the ANR CHIST-ERA project SECODE. Y. Qi also acknowledges support from Zhejiang provincial Natural Science Foundation of China (LQ17A010008, LQ16A010005). C. Tang also acknowledges support from 14E013, CXTD2014-4 and the Meritocracy Research Funds of China West Normal University.

S. Mesnager is with the Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, with LAGA UMR 7539, CNRS, Sorbonne Paris Cité, University of Paris XIII, 93430 Paris, France, and also with Telecom ParisTech, 75013 Paris, France (e-mail: smesnager@univ-paris8.fr).

Y. Qi is with School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China (e-mail: qianfeng07@163.com).

H. Ru and C. Tang are with the School of Mathematics and Information, China West Normal University, Nanchong 637002, China (tangchunmingmath@163.com, hongming_2436@163.com). C. Tang is also with the Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong.

Some minimal linear codes with few weights can be constructed by the defining set method [21], [22]. Let $D = \{d_1, d_2, \dots, d_n\}$ be a subset of \mathbb{F}_q . Then a linear code of length n over \mathbb{F}_p is defined by

$$\mathcal{C}_D = \{(Tr(\beta x))_{x \in D} : \beta \in \mathbb{F}_q\}, \quad (1)$$

where D is called the defining set of \mathcal{C}_D and $Tr(x) = \sum_{i=0}^{m-1} x^{p^i}$ is the trace function from \mathbb{F}_q to \mathbb{F}_p . From this construction, many minimal linear codes can be constructed by different choices of D . Most of them satisfy the sufficient condition $\frac{w_{min}}{w_{max}} > \frac{p-1}{p}$. This sufficient condition is not necessary [7]. Chang and Hyun [17] made a breakthrough and constructed an infinite family of minimal binary linear codes with $\frac{w_{min}}{w_{max}} < \frac{1}{2}$. Heng et al. [27] presented a sufficient and necessary condition for minimal linear codes in the following theorem.

Theorem 1.2: Let \mathcal{C} be a linear code over \mathbb{F}_p . Then \mathcal{C} is minimal if and only if

$$\sum_{c \in \mathbb{F}_p^*} wt(a + cb) \neq (p-1)wt(a) - wt(b) \quad (2)$$

for any \mathbb{F}_p linearly independent codewords $a, b \in \mathcal{C}$.

They also constructed an infinite family of minimal ternary linear codes with $\frac{w_{min}}{w_{max}} < \frac{2}{3}$. Ding et al. [24] presented more necessary and sufficient conditions for minimal binary linear codes and constructed three infinite families of minimal binary linear codes. Zhang et al. [38] constructed four families of minimal binary linear codes from Krawtchouk polynomials. Xu and Qu [36] studied minimal linear codes for odd p and presented three infinite families of minimal linear codes. Bartoli and Bonini [3] generalized the third class of minimal linear codes in [24] from binary case to odd characteristic case and presented a class of minimal linear codes in odd characteristic. Bonini and Borello [4] presented many minimal linear codes from particular blocking sets. These minimal linear codes are constructed from the following method [10], [17], [32], [34], [35]. Let f be a function from \mathbb{F}_q to \mathbb{F}_p such that

$$\begin{cases} f(0) = 0, \\ f(x) \neq Tr(wx) \text{ for all } w \in \mathbb{F}_q. \end{cases} \quad (3)$$

A linear code over \mathbb{F}_p can be defined by

$$\mathcal{C}_f = \{(uf(x) - Tr(vx))_{x \in \mathbb{F}_q^*} : u \in \mathbb{F}_p, v \in \mathbb{F}_q\} \quad (4)$$

By the choice of f , many linear codes with good properties can be defined.

Inspired by these recent results, we use the characteristic function of a subset of \mathbb{F}_q to construct minimal linear codes in (4). For binary case, by a simple property of characteristic functions, we can present more minimal binary linear codes from known minimal binary linear codes. Furthermore, we employ characteristic functions corresponding to some subspaces to construct minimal linear codes, which generalize [24] and [36].

The rest of this paper is organized as follows. In Section 2, we present some basic results on p -ary functions, Krawchouk polynomials, and minimal linear codes. In Section 3, we present more minimal linear codes from characteristic functions. In Section 4, we use characteristic functions to present a characterization of minimal linear codes from the defining set method and obtain a class of minimal linear codes. Section 5 makes a conclusion.

II. PRELIMINARIES

In this section, we will introduce some results on p -ary functions, Krawchouk polynomials, and minimal linear codes.

A. p -ary functions

A p -ary function is a function from \mathbb{F}_q or \mathbb{F}_p^m to \mathbb{F}_p . The Walsh transform of a p -ary function f at a point $w \in \mathbb{F}_q$ is defined by

$$\hat{f}(w) := \sum_{x \in \mathbb{F}_q} \zeta_p^{f(x) - \text{Tr}(wx)},$$

where $\zeta_p = e^{2\pi\sqrt{-1}/p}$ is the primitive p -th root of unity and Tr is the trace function from \mathbb{F}_q to \mathbb{F}_p . The Walsh transform of a p -ary function f at a point $w \in \mathbb{F}_p^m$ is defined by

$$\hat{f}(w) := \sum_{x \in \mathbb{F}_p^m} \zeta_p^{f(x) - \langle w, x \rangle},$$

where $\langle w, x \rangle$ is the inner product of w and x . A function $f(x)$ is called a p -ary bent function, if $|\hat{f}(w)| = p^{\frac{m}{2}}$ for any $w \in \mathbb{F}_q$. When $p = 2$, a p -ary (bent) function f is just a Boolean (bent) function.

An important class of Boolean functions is the general Maiorana-McFarland class, which can be used to generate Boolean functions with good cryptographic properties [9], [12], [20], [29], [31]. Let m be a positive integer and let s, t be two positive integers such that $s + t = m$. The function in the general Maiorana-McFarland class has the form

$$f(x, y) = \langle \phi(x), y \rangle + g(x), \quad (5)$$

where $x \in \mathbb{F}_2^s$, $y \in \mathbb{F}_2^t$, ϕ is a mapping from \mathbb{F}_2^s to \mathbb{F}_2^t , and g is a Boolean function in s variables.

Krawchouk polynomials [15], [28] are useful in bent functions and coding theory. Let m be a positive integer. The Krawchouk polynomial is defined by

$$P_k(x) = \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{m-x}{k-j}, \quad (6)$$

where $0 \leq k \leq m$. The Krawchouk polynomials satisfy

- $P_k(0) = \binom{m}{k}$,
- $P_k(1) = \frac{m-2k}{m} \binom{m}{k}$,
- $P_m(k) = (-1)^k$,
- $P_k(i) = (-1)^i P_{m-k}(i)$ for $0 \leq i \leq m$,
- $\sum_{k=0}^m \binom{m-k}{m-j} P_k(x) = 2^j \binom{m-x}{j}$,
- $P_k(x) = (-1)^k P_k(m-k)$.
- $\sum_{wt(v)=k} (-1)^{u \cdot v} = P_k(i)$, where $u \in \mathbb{F}_2^m$ such that $wt(u) = i$.

B. Linear codes

In this subsection, we present some results on linear codes defined in (4).

Parameters of binary linear codes in (4) can be determined by the following Theorem.

Theorem 2.1 ([24]): Let $p = 2$ and let \mathcal{C}_f be defined in (4) by a Boolean function f satisfying (3). The code \mathcal{C}_f has length $q - 1$ and dimension $m + 1$. The weight distribution of \mathcal{C}_f is given by the following multiset union

$$\left\{ \frac{q - \hat{f}(w)}{2} : w \in \mathbb{F}_q \right\} \cup \{2^{m-1} : w \in \mathbb{F}_q^*\} \cup \{0\}.$$

A necessary and sufficient condition of a minimal binary linear code in (4) is given in the following theorem, which is more efficient than Theorem 1.2.

Theorem 2.2 ([24]): Let $p = 2$ and let \mathcal{C}_f be defined in (4) from a Boolean function f satisfying (3). Then \mathcal{C}_f is minimal if and only if $\hat{f}(h) + \hat{f}(l) \neq q$ and $\hat{f}(h) - \hat{f}(l) \neq q$ for every pair of distinct elements h and l in \mathbb{F}_q .

Let $Q(\zeta_p)$ be the p -th cyclotomic field over the rational field Q . Then the field extension $Q(\zeta_p)/Q$ is Galois of degree $p - 1$ and the Galois group is $Gal(Q(\zeta_p)/Q) = \{\sigma_a : a \in \mathbb{F}_p^*\}$, where σ_a is an automorphism of $Q(\zeta_p)$ defined by $\sigma_a(\zeta_p) = \zeta_p^a$. Parameters of a linear code in (4) for odd p can be given in the following lemma.

Lemma 2.3 ([32]): Let p be an odd prime and let \mathcal{C}_f be defined in (4). Then \mathcal{C}_f is a $[p^m - 1, m + 1]$ code and the Hamming weight of a codeword $(uf(x) - Tr(vx))_{x \in \mathbb{F}_q^*}$ is given by

$$\begin{cases} 0, & \text{if } u = 0, v = 0; \\ p^m - p^{m-1}, & \text{if } u = 0, v \neq 0; \\ p^m - p^{m-1} - \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \sigma_a \left(\sigma_u \left(\hat{f}(u^{-1}v) \right) \right), & \text{otherwise.} \end{cases}$$

III. MINIMAL LINEAR CODES FROM CHARACTERISTIC FUNCTIONS

In this section, we will present some minimal linear codes from characteristic functions associated with different subsets of \mathbb{F}_q .

Let $D \subset \mathbb{F}_q^*$. The characteristic function of D is

$$f_D(x) = \begin{cases} 1, & \text{if } x \in D \\ 0, & \text{otherwise.} \end{cases}$$

From the characteristic function f_D , a linear code \mathcal{C}_{f_D} can be constructed by

$$\mathcal{C}_{f_D} = \{(uf_D(x) - Tr(vx))_{x \in \mathbb{F}_q^*} : u \in \mathbb{F}_p, v \in \mathbb{F}_q\}. \quad (7)$$

We first give some properties of characteristic functions.

Lemma 3.1: Let $D \subset \mathbb{F}_q^*$ and let $\overline{D} = \mathbb{F}_q^* \setminus D$. Then

$$\hat{f}_D(w) + \hat{f}_{\overline{D}}(w) = \begin{cases} (q-1)\zeta_p + q + 1, & \text{if } w = 0, \\ 1 - \zeta_p, & \text{otherwise.} \end{cases}$$

Proof:

$$\begin{aligned} \hat{f}_D(w) &= \sum_{x \in \mathbb{F}_q} \zeta_p^{f_D(x) - Tr(wx)} \\ &= \sum_{x \in D} \zeta_p^{f_D(x) - Tr(wx)} + \sum_{x \in \mathbb{F}_q \setminus D} \zeta_p^{-Tr(wx)} \\ &= \sum_{x \in D} (\zeta_p^{f_D(x) - Tr(wx)} - \zeta_p^{-Tr(wx)}) + \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)} \\ &= (\zeta_p - 1) \sum_{x \in D} \zeta_p^{-Tr(wx)} + \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)} \end{aligned}$$

and

$$\hat{f}_{\overline{D}}(w) = (\zeta_p - 1) \sum_{x \in \overline{D}} \zeta_p^{-Tr(wx)} + \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)}.$$

Then

$$\begin{aligned} \hat{f}_D(w) + \hat{f}_{\overline{D}}(w) &= (\zeta_p - 1) \left(\sum_{x \in D} \zeta_p^{-Tr(wx)} + \sum_{x \in \overline{D}} \zeta_p^{-Tr(wx)} \right) + 2 \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)} \\ &= (\zeta_p - 1) \left(\sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)} - 1 \right) + 2 \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)} \\ &= 1 - \zeta_p + (\zeta_p + 1) \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)}. \end{aligned}$$

Since $\sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)} = 0$ for any $w \in \mathbb{F}_q^*$, this lemma follows. ■

Lemma 3.2: Let $D_1 \subset \mathbb{F}_q^*$ and $D_2 \subset \mathbb{F}_q^*$ such that $D_1 \cap D_2 = \emptyset$. Let $D = D_1 \cup D_2$. Then

$$\hat{f}_D(w) = \begin{cases} \hat{f}_{D_1}(w) + \hat{f}_{D_2}(w) - q, & \text{if } w = 0, \\ \hat{f}_{D_1}(w) + \hat{f}_{D_2}(w), & \text{otherwise.} \end{cases}$$

Proof: Note that

$$\begin{aligned} \hat{f}_{D_1}(w) &= (\zeta_p - 1) \sum_{x \in D_1} \zeta_p^{-Tr(wx)} + \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)}, \\ \hat{f}_{D_2}(w) &= (\zeta_p - 1) \sum_{x \in D_2} \zeta_p^{-Tr(wx)} + \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)}, \\ \hat{f}_D(w) &= (\zeta_p - 1) \sum_{x \in D} \zeta_p^{-Tr(wx)} + \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(wx)}. \end{aligned}$$

By $\sum_{x \in D} \zeta_p^{-Tr(wx)} = \sum_{x \in D_1} \zeta_p^{-Tr(wx)} + \sum_{x \in D_2} \zeta_p^{-Tr(wx)}$, we have this lemma. ■

Using these properties of characteristic functions, we can give more linear codes $\mathcal{C}_{f_{\overline{D}}}$ from \mathcal{C}_{f_D} . When $p = 2$, we have $\hat{f}_D(w) + \hat{f}_{\overline{D}}(w) = 2$ for any $w \in \mathbb{F}_q$. If $D \subset \mathbb{F}_2^m \setminus \{0\}$, $\overline{D} = \mathbb{F}_2^m \setminus (\{0\} \cup D)$, we also have $\hat{f}_D(w) + \hat{f}_{\overline{D}}(w) = 2$ for any $w \in \mathbb{F}_p^m$. By Theorem 2.1 and Lemma 3.1, we have the following corollary.

Corollary 3.3: Let $p = 2$. Let $D \subset \mathbb{F}_q^*$ and $\overline{D} = \mathbb{F}_q^* \setminus D$ such that their characteristic functions f_D and $f_{\overline{D}}$ satisfy (3). Then the code $\mathcal{C}_{f_{\overline{D}}}$ has length $q - 1$ and dimension $m + 1$. The weight distribution of $\mathcal{C}_{f_{\overline{D}}}$ is given by the following multiset union

$$\begin{aligned} & \left\{ \frac{q - \hat{f}_{\overline{D}}(w)}{2} : w \in \mathbb{F}_q \right\} \cup \{2^{m-1} : w \in \mathbb{F}_q^*\} \cup \{0\} \\ &= \left\{ \frac{q - 2 + \hat{f}_D(w)}{2} : w \in \mathbb{F}_q \right\} \cup \{2^{m-1} : w \in \mathbb{F}_q^*\} \cup \{0\}. \end{aligned}$$

Remark 1: Let f be a bent or semi-bent function satisfying (3). Let $D = \text{Suppt}(f)$. The Walsh transforms of f are given in [18]. By Theorem 2.2, the codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ are minimal. They satisfy that $\frac{w_{\min}}{w_{\max}} \geq 1/2$.

By Lemma 2.3 and Lemma 3.1, we have the following corollary.

Corollary 3.4: Let p be an odd prime. Let $D \subset \mathbb{F}_q^*$ and $\overline{D} = \mathbb{F}_q^* \setminus D$ such that their characteristic functions f_D and $f_{\overline{D}}$ satisfy (3). Then $\mathcal{C}_{f_{\overline{D}}}$ is a $[p^m - 1, m + 1]$ code and the Hamming weight of a codeword $(uf_{\overline{D}}(x) - Tr(vx))_{x \in \mathbb{F}_q^*}$ is given by

$$\begin{aligned} & \begin{cases} 0, & \text{if } u = 0, v = 0; \\ p^m - p^{m-1}, & \text{if } u = 0, v \neq 0; \\ p^m - p^{m-1} - \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \sigma_a \left(\sigma_u \left(\hat{f}_{\overline{D}}(0) \right) \right), & \text{if } u \neq 0, v = 0; \\ p^m - p^{m-1} - \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \sigma_a \left(\sigma_u \left(\hat{f}_{\overline{D}}(u^{-1}v) \right) \right), & \text{if } u \neq 0, v \neq 0. \end{cases} \\ &= \begin{cases} 0, & \text{if } u = 0, v = 0; \\ p^m - p^{m-1}, & \text{if } u = 0, v \neq 0; \\ p^{m-1} - 1 + \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \sigma_a \left(\sigma_u \left(\hat{f}_D(0) \right) \right), & \text{if } u \neq 0, v = 0; \\ p^m - p^{m-1} - 1 + \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \sigma_a \left(\sigma_u \left(\hat{f}_D(u^{-1}v) \right) \right), & \text{if } u \neq 0, v \neq 0. \end{cases} \end{aligned}$$

Remark 2: By Corollary 3.3 and Corollary 3.4, we can obtain $\mathcal{C}_{f_{\overline{D}}}$ from known \mathcal{C}_{f_D} .

In the following, we will use concrete subsets D to construct more minimal linear codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$.

A. Some minimal binary linear codes from known minimal binary linear codes

In this subsection, we will present more minimal binary linear codes from known minimal binary linear codes in [24].

The following theorem generalizes Theorem 23 in [24] and obtains minimal linear codes from Boolean functions in the general Maiorana-McFarland class.

Theorem 3.5: Let $m \geq 7$ be an odd integer, $s = \frac{m+1}{2}$, and $t = \frac{m-1}{2}$. Let $U = \{x \in \mathbb{F}_2^s : wt(x) \geq 2\}$ and let $V = \{0\}$. Let f be the Boolean function defined in (5), where $g \equiv 1$, ϕ is an injection from $\mathbb{F}_2^s \setminus U$ to $\mathbb{F}_2^t \setminus V$, and $\phi(x) = \mathbf{0}$ for any $x \in U$. Let $D = \text{Suppt}(f)$. The code $\mathcal{C}_{f_{\overline{D}}}$ defined in (7) is a $[2^m - 1, m + 1, 2^{m-1} - 2^{t-1}(2^s - s - 1) - 1]$ minimal code with $\frac{w_{\min}}{w_{\max}} \leq 1/2$. The weight distribution of $\mathcal{C}_{f_{\overline{D}}}$ is given in Table I (resp. Table II) when s is odd (resp. even).

TABLE I
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{f_{\overline{D}}}$ IN THEOREM 3.5 FOR s ODD

Weight	Frequency
0	1
$2^{m-1} - 1$	$2^s(2^t - s - 2) + \binom{s}{(1+s)/2}$
2^{m-1}	$2^m - 1$
$2^{m-1} - 2^{t-1} - 1$	$s2^{s-1}$
$2^{m-1} + 2^{t-1} - 1$	$2^s + s2^{s-1}$
$2^{m-1} + 2^{t-1}(s + 1 - 2i) - 1$ for $1 \leq i \leq s$ and $i \neq (1+s)/2$	$\binom{s}{i}$
$2^{m-1} - 2^{t-1}(2^s - s - 1) - 1$	1

TABLE II
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{f_{\overline{D}}}$ IN THEOREM 3.5 FOR s EVEN

Weight	Frequency
0	1
$2^{m-1} - 1$	$2^s(2^t - s - 2)$
2^{m-1}	$2^m - 1$
$2^{m-1} - 2^{t-1} - 1$	$s2^{s-1} + \binom{s}{(s+2)/2}$
$2^{m-1} + 2^{t-1} - 1$	$2^s + s2^{s-1} + \binom{s}{s/2}$
$2^{m-1} + 2^{t-1}(s + 1 - 2i) - 1$ for $1 \leq i \leq s$ and $i \notin \{s/2, (2+s)/2\}$	$\binom{s}{i}$
$2^{m-1} - 2^{t-1}(2^s - s - 1) - 1$	1

Proof: Note that

$$\hat{f}_D(h_1, h_2) = \begin{cases} -2^t(2^s - s - 1), & \text{if } h_1 = \mathbf{0} \text{ and } h_2 = \mathbf{0} \\ 2^t(s + 1 - 2i), & \text{if } h_1 \neq \mathbf{0}, wt(h_1) = i \text{ and } h_2 = \mathbf{0} \\ -2^t(-1)^{h_1 \cdot \phi^{-1}(h_2)}, & \text{if } h_2 \in \text{Im } \phi \setminus \{\mathbf{0}\} \\ 0, & \text{if } h_2 \notin \text{Im } \phi \end{cases}$$

where r runs from 1 to s , and $|\text{Im } \phi| = s + 2$. By Lemma 3.1, we have

$$\hat{f}_{\overline{D}}(h_1, h_2) = 2 - \hat{f}_D(h_1, h_2) = \begin{cases} 2 + 2^t(2^s - s - 1), & \text{if } h_1 = \mathbf{0} \text{ and } h_2 = \mathbf{0} \\ 2 - 2^t(s + 1 - 2i), & \text{if } h_1 \neq \mathbf{0}, wt(h_1) = i \text{ and } h_2 = \mathbf{0} \\ 2 + 2^t(-1)^{h_1 \cdot \phi^{-1}(h_2)}, & \text{if } h_2 \in \text{Im } \phi \setminus \{\mathbf{0}\} \\ 2, & \text{if } h_2 \notin \text{Im } \phi \end{cases}$$

Note that $\hat{f}_{\overline{D}}(h_1, h_2) \pm \hat{f}_{\overline{D}}(l_1, l_2) \neq 2^m$ for any pair of distinct $(h_1, h_2), (l_1, l_2)$. By Theorem 2.2, The code $\mathcal{C}_{f_{\overline{D}}}$ is minimal. By Theorem 2.1, we have the weight distribution of $\mathcal{C}_{f_{\overline{D}}}$. Note that $w_{\min} = 2^{m-1} - 2^{t-1}(2^s - s - 1) - 1$ and $w_{\max} = 2^{m-1} + 2^{t-1}(s - 1) - 1$. Then $\frac{w_{\min}}{w_{\max}} \leq 1/2$. This theorem follows. ■

The following theorem generalizes Theorem 26 [24].

TABLE III
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{f_{\overline{D}}}$ IN THEOREM 3.6

Weight	Frequency
0	1
$2^{m-1} - \sum_{j=1}^k P_j(i) - 1$ for $1 \leq i \leq m$	$\binom{m}{i}$
2^{m-1}	$2^m - 1$
$2^m - \sum_{j=1}^k \binom{m}{j} - 1$	1

Theorem 3.6: Let k be a positive integer and let $D = \{\alpha \in \mathbb{F}_2^m : 1 \leq wt(\alpha) \leq k\}$. The code $\mathcal{C}_{f_{\overline{D}}}$ defined in (7) has length $2^m - 1$, dimension $m + 1$, and the weight distribution in Table III.

Proof: Note that

$$\hat{f}_{\overline{D}}(w) = 2 - \hat{f}_D = \begin{cases} 2 - 2^m + 2 \sum_{j=1}^k \binom{m}{j}, & \text{if } w = 0 \\ 2 + 2 \sum_{j=1}^k P_j(i), & \text{if } w \neq 0 \text{ and } wt(w) = i \end{cases}$$

where $P_j(i)$ are Krawchouk polynomials defined in (6). By Theorem 2.1, we have the distribution of $\mathcal{C}_{f_{\overline{D}}}$ in Table III. ■

Remark 3: By Theorem 2.2, conditions of $\mathcal{C}_{f_{\overline{D}}}$ to be minimal can be obtained.

B. Minimal linear codes from characteristic functions corresponding to subspaces

In this subsection, we will give some minimal linear codes from characteristic functions corresponding to some subspaces.

We first consider some subspaces in the following proposition.

Proposition 3.7: Let E_1, \dots, E_s be s subspaces of \mathbb{F}_q such that

$$\begin{cases} \dim(E_i) = t_i, \forall 1 \leq i \leq s \\ E_i \cap E_j = \{0\}, \forall 1 \leq i \neq j \leq s \\ E_i^\perp \cap E_j^\perp = \{0\}, \forall 1 \leq i \neq j \leq s. \end{cases} \quad (8)$$

where $1 \leq t_1 \leq t_2 \leq \dots \leq t_s \leq m - 1$. Then one of the following conditions holds:

- (i) $s = 1$;
- (ii) $s = 2$ and $t_1 + t_2 = m$;
- (iii) $s > 2$, m is even and $t_1 = \dots = t_s = \frac{m}{2}$.

Proof: Conditions (i) and (ii) can be obtained when $s = 1$ or $s = 2$.

Suppose that $s > 2$. If $t_1 = \dim(E_1) < \frac{m}{2}$, by $\dim(E_i) \cap \dim(E_j) = \{0\}$ ($i \neq j$), then we have $t_2 > \frac{m}{2}, \dots, t_s > \frac{m}{2}$, which makes a contradiction with $\dim(E_2) \cap \dim(E_s) = \{0\}$. Hence, $t_1 \geq \frac{m}{2}$. Similarly, $t_2 \geq \frac{m}{2}, \dots, t_s \geq \frac{m}{2}$. By $\dim(E_i) \cap \dim(E_j) = \{0\}$ ($i \neq j$), we have $t_1 = t_2 = \dots = t_s = \frac{m}{2}$ and m is even.

Hence, this proposition follows. ■

Let $D = \cup_{i=1}^s E_i \setminus \{0\}$, where E_1, \dots, E_s are subspaces satisfying (8). Note that

$$\begin{aligned}
\hat{f}_D(w) &= \sum_{x \in \mathbb{F}_q} \zeta_p^{f_D(x) - \text{Tr}(wx)} \\
&= \sum_{x \in D} \zeta_p^{f_D(x) - \text{Tr}(wx)} + \sum_{x \in \mathbb{F}_q \setminus D} \zeta_p^{-\text{Tr}(wx)} \\
&= \sum_{x \in D} (\zeta_p^{f_D(x) - \text{Tr}(wx)} - \zeta_p^{-\text{Tr}(wx)}) + \sum_{x \in \mathbb{F}_q} \zeta_p^{-\text{Tr}(wx)} \\
&= \sum_{i=1}^s (\zeta_p - 1) \left(\sum_{x \in E_i} \zeta_p^{-\text{Tr}(wx)} - 1 \right) + \sum_{x \in \mathbb{F}_q} \zeta_p^{-\text{Tr}(wx)} \\
&= \begin{cases} p^m + (\zeta_p - 1)(\sum_{i=1}^s |E_i| - s), & \text{if } w = 0; \\ (\zeta_p - 1)(|E_i| - s), & \text{if } w \in E_i^\perp \setminus \{0\} \text{ for } 1 \leq i \leq s; \\ -(\zeta_p - 1)s, & \text{if } w \in \mathbb{F}_q \setminus (\cup_{i=1}^s E_i^\perp), \end{cases} \quad (9)
\end{aligned}$$

where $|E_i| = p^{t_i}$. Then we have linear codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ in the following theorem.

Theorem 3.8: Let $D = \cup_{i=1}^s E_i \setminus \{0\}$, where E_1, \dots, E_s satisfy (8). Let \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ be defined in (7). Then \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ are $[q-1, m+1]$ codes with the weight distributions in Table IV and Table V, respectively.

TABLE IV
THE WEIGHT DISTRIBUTION OF \mathcal{C}_{f_D} IN THEOREM 3.8

Weight	Frequency
0	1
$p^m - p^{m-1}$	$p^m - 1$
$\sum_{i=1}^s p^{t_i} - s$	$p - 1$
$p^m - p^{m-1} + p^{t_i} - s$ for $1 \leq i \leq s$	$(p-1)(p^{m-t_i} - 1)$
$p^m - p^{m-1} - s$	$(p-1)(p^m - \sum_{i=1}^s p^{m-t_i} + s - 1)$

TABLE V
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{f_{\overline{D}}}$ IN THEOREM 3.8

Weight	Frequency
0	1
$p^m - p^{m-1}$	$p^m - 1$
$p^m - 1 - \sum_{i=1}^s p^{t_i} + s$	$p - 1$
$p^m - p^{m-1} - 1 - p^{t_i} + s$ for $1 \leq i \leq s$	$(p-1)(p^{m-t_i} - 1)$
$p^m - p^{m-1} - 1 + s$	$(p-1)(p^m - \sum_{i=1}^s p^{m-t_i} + s - 1)$

Proof: By (9), Theorem 2.1 and Corollary 3.3, for $p = 2$, we have the weight distributions of \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$. By (9), Lemma 2.3 and Corollary 3.4, for p odd, we have the weight distributions of \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$. Hence, this theorem follows. ■

By choosing different subspaces E_i in Theorem 3.8, we can obtain many minimal linear codes, in which we can find minimal codes with $\frac{w_{\min}}{w_{\max}} \leq \frac{p-1}{p}$. Note that the codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ can not be minimal if $s = 1$. We just consider Condition (ii) and Condition (iii) in Proposition 3.7.

We first discuss linear codes satisfying Condition (iii). When $p = 2$ and m is even, we have the following theorem on minimal linear codes.

Theorem 3.9 (Theorem 18, [24]): Let $p = 2$, m be even, and $s \geq 2$. Let $D = \cup_{i=1}^s E_i \setminus \{0\}$, where E_1, \dots, E_s satisfy (8), $t_1 = \dots = t_s = t = \frac{m}{2}$. Then \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ are minimal if and only if $s \notin \{2^t, 2^t + 1\}$. Furthermore, if $s \leq 2^{t-2}$, the code \mathcal{C}_{f_D} satisfies that $\frac{w_{\min}}{w_{\max}} \leq \frac{1}{2}$. If $s > 3 \cdot 2^{t-2}$, then $\mathcal{C}_{f_{\overline{D}}}$ satisfies that $\frac{w_{\min}}{w_{\max}} \leq \frac{1}{2}$.

For odd p , the following theorem gives minimal linear codes.

Theorem 3.10: Let p be odd and m be even. Let $D = \cup_{i=1}^s E_i \setminus \{0\}$, where E_1, \dots, E_s satisfy (8) and $t_1 = \dots = t_s = t = \frac{m}{2}$. If $p-2 < s < p^t - p^{t-1}$ (resp. $s > p^{t-1} + 1$), then \mathcal{C}_{f_D} (resp. $\mathcal{C}_{f_{\overline{D}}}$) is minimal. Furthermore, if $s \leq p^t - 2p^{t-1} + p^{t-2}$ (resp. $s > 2p^{t-1} - p^{t-2}$), the code \mathcal{C}_{f_D} (resp. $\mathcal{C}_{f_{\overline{D}}}$) satisfies that $\frac{w_{\min}}{w_{\max}} \leq \frac{p-1}{p}$.

Proof: By the weight distribution of \mathcal{C}_{f_D} in Table IV, we have weights of nonzero codewords of \mathcal{C}_{f_D} : $w_1 = sp^t - s$, $w_2 = p^m - p^{m-1} - s$, $w_3 = p^m - p^{m-1}$, and $w_4 = p^m - p^{m-1} + p^t - s$. Obviously, $w_1 < w_2 < w_3 < w_4$. Let $H_i = \{wt(a) = w_i : a \in \mathcal{C}_{f_D}\}$ for $1 \leq i \leq 4$. Take two \mathbb{F}_p linearly independent codewords $a = (u_1 f(x) + Tr(v_1 x))_{x \in \mathbb{F}_q^*}$, $b = (u_2 f(x) + Tr(v_2 x))_{x \in \mathbb{F}_q^*}$, where $u_1, u_2 \in \mathbb{F}_p$ and $v_1, v_2 \in \mathbb{F}_q$. Note that

$$\begin{aligned} a &\in H_1 \text{ if and only if } u_1 \neq 0, v_1 = 0; \\ a &\in H_2 \text{ if and only if } u_1 \neq 0, v_1 \in \mathbb{F}_q \setminus \cup_{i=1}^s E_i^\perp; \\ a &\in H_3 \text{ if and only if } u_1 = 0, v_1 \neq 0; \\ a &\in H_4 \text{ if and only if } u_1 \neq 0, v_1 \in \cup_{i=1}^s E_i^\perp \setminus \{0\}. \end{aligned}$$

By Theorem 1.2, we just need to verify (2) for different cases of a, b .

Case 1: $a, b \in H_i$, where $i = 1, 2, 3, 4$. Note that any two codewords in H_1 are linearly dependent and codewords with $u = 0$ forms a one-weight code. Hence, (2) holds for $a, b \in H_1$ or $a, b \in H_3$. We just consider $a, b \in H_2$ or $a, b \in H_4$. When $a, b \in H_2$, then $u_1, u_2, v_1, v_2 \neq 0$. There exists only one $c \in \mathbb{F}_p^*$ such that $a + cb \in H_3$, and there exists at most one $c \in \mathbb{F}_p^*$ such that $a + cb \in H_1$. Hence,

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) \geq w_1 + (p-3)w_2 + w_3 > (p-2)w_2 = (p-1)wt(a) - wt(b).$$

Similarly, when $a, b \in H_4$, by $s > p-2$,

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) \geq w_1 + w_3 + (p-3)w_2 > (p-2)w_4 = (p-1)wt(a) - wt(b).$$

Hence, (2) holds for $a, b \in H_i$ for $1 \leq i \leq 4$.

Case 2: $b \in H_1$, $a \in H_2$ or H_4 . Suppose that $a \in H_2$. Then there exists only one $c \in \mathbb{F}_p$ such that $a + cb \in H_3$. For other $c \in \mathbb{F}_p$, $a + cb \in H_2$.

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) = (p-2)w_2 + w_3 > (p-1)w_2 - w_1 = (p-1)wt(a) - wt(b).$$

This also holds for $a \in H_4$.

Case 3: $b \in H_1$, $a \in H_3$. Then $a + cb \in H_2$ or H_4 , where $c \in \mathbb{F}_p^*$. We have

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) \geq (p-1)w_2 > (p-1)w_3 - w_1 = (p-1)wt(a) - wt(b).$$

Case 4: $b \in H_2$, $a \in H_3$. There exists at most one $c \in \mathbb{F}_p$ such that $a + cb \in H_1$. For other $c \in \mathbb{F}_p$, $a + cb \in H_2$ or H_4 . We have

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) \geq (p-2)w_2 + w_1 > (p-1)w_3 - w_2 = (p-1)wt(a) - wt(b).$$

Case 5: $b \in H_2$, $a \in H_4$. There exists only one $c \in \mathbb{F}_p$ such that $a + cb \in H_3$. For other $c \in \mathbb{F}_p$, $a + cb \in H_2$ or H_4 . We have

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) \geq (p-2)w_2 + w_3 > (p-1)w_4 - w_2 = (p-1)wt(a) - wt(b).$$

Case 6: $b \in H_3$, $a \in H_4$. There exists at most one $c_0 \in \mathbb{F}_p^*$ such that $a + c_0 b \in H_1$. If such c_0 exists, then $v_1 + c_0 v_2 = 0$ and $v_2 = -\frac{1}{c_0} v_1 \in \cup_{i=1}^s E_i^\perp \setminus \{0\}$. For $c \in \mathbb{F}_p^* \setminus \{c_0\}$, $a + cb \in H_4$.

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) \geq (p-2)w_4 + w_1 > (p-1)w_4 - w_3 = (p-1)wt(a) - wt(b).$$

If such c_0 does not exist, then $a + cb \in H_2$ or H_4 .

$$\sum_{c \in \mathbb{F}_q^*} wt(a + cb) \geq (p-1)w_2 > (p-1)w_4 - w_3 = (p-1)wt(a) - wt(b).$$

Hence, (2) holds. By Theorem 1.2, the code \mathcal{C}_{f_D} is minimal. Furthermore, if $s \leq p^t - 2p^{t-1} + p^{t-2}$, $\frac{w_{min}}{w_{max}} = \frac{w_1}{w_4} \leq \frac{p-1}{p}$.

By the weight distribution of $\mathcal{C}_{f_{\overline{D}}}$ in Table V, we have weights of nonzero codewords of \mathcal{C}_{f_D} : $w'_1 = p^m - 1 - sp^t + s$, $w'_2 = p^m - p^{m-1} - 1 - p^t + s$, $w'_3 = p^m - p^{m-1}$, $w'_4 = p^m - p^{m-1} + s - 1$. By $s > p^{t-1} + 1$, $w'_1 < w'_2 < w'_3 < w'_4$. Results on $\mathcal{C}_{f_{\overline{D}}}$ can be similarly obtained. ■

Remark 4: Let $m = 2t$. A partial spread of \mathbb{F}_q is a set of pairwise supplementary t -dimensional subspaces of \mathbb{F}_q . Let U_0, U_1, \dots, U_{p^t} be a partial spread of \mathbb{F}_q , where U_i ($0 \leq i \leq p^t$) are t -dimensional subspaces of \mathbb{F}_q . Take $s(p-1)$ subspaces $E_1, \dots, E_{s(p-1)}$ from U_0, U_1, \dots, U_{p^t} . Let $D = \cup_{i=1}^{s(p-1)} \{0\}$. Then \mathcal{C}_{f_D} has the same parameters and weight distribution with the third family of minimal linear codes in [36].

In the following theorem, we will consider minimal linear codes satisfying Condition (ii) in Proposition 3.7.

Theorem 3.11: Let p be a prime and let $D = (E_1 \cup E_2) \setminus \{0\}$, where E_1, E_2 are two subspaces of \mathbb{F}_q satisfying (8), $t_1 + t_2 = m$, and $2 \leq t_1 < t_2 \leq m-2$. Then the codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ defined in (7) are $[p^m - 1, m+1]$ minimal codes such that $\frac{w_{min}}{w_{max}} \leq \frac{p-1}{p}$.

Proof: When $p = 2$, by (9), Theorem 2.2, and Theorem 3.8, the codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ defined in (7) are $[2^m - 1, m+1]$ minimal codes such that $\frac{w_{min}}{w_{max}} \leq \frac{1}{2}$.

When p is odd, by Theorem 3.8 and a similar proof with Theorem 3.10, the codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ defined in (7) are $[p^m - 1, m+1]$ minimal codes such that $\frac{w_{min}}{w_{max}} \leq \frac{p-1}{p}$. ■

Remark 5: Note that E_1 and E_2 can be identified as two linear codes over \mathbb{F}_p . By $E_1 + E_2 = \mathbb{F}_q$ and $E_1 \cap E_2 = \{0\}$, (E_1, E_2) is a linear complementary pair (LCP) of codes over \mathbb{F}_p [7], [8]. We can take two subspaces E_1 and E_2 of \mathbb{F}_q , where $E_2 = E_1^\perp$ and $E_1 + E_2 = \mathbb{F}_q$. Then E_1 is a linear complementary dual (LCD) code. There are many LCD codes constructed in [13], [14], [33], [39]. Those LCD codes can be used in Theorem 3.11 to construct minimal linear codes.

Example 1: Let $p = 2$ and let $m = 5$. Let w be a primitive element of \mathbb{F}_q such that $w^5 + w^2 + 1 = 0$. Take $E_1 = \{0, w, w^9, w^{21}\}$ and $E_2 = \{0, w^6, w^7, w^{14}, w^{18}, w^{24}, w^{26}, w^{29}\}$. Then $E_2 = E_1^\perp$ and $E_1 + E_2 = \mathbb{F}_q$. The code \mathcal{C}_{f_D} is a minimal binary $[31, 6, 10]$ code with the weight enumerator $1 + z^{10} + 21z^{14} + 31z^{16} + 7z^{18} + 3z^{22}$. The code $\mathcal{C}_{f_{\overline{D}}}$ is a minimal binary $[31, 6, 9]$ code with the weight enumerator $1 + 3z^9 + 7z^{13} + 31z^{16} + 21z^{17} + z^{21}$.

Example 2: Let $p = 3$ and let $m = 5$. Let w be a primitive element of \mathbb{F}_q such that $w^5 + 2w^2 + 1 = 0$. Take E_1 as a subspace of \mathbb{F}_q generated by w^4 and w^{33} . Let $E_2 = E_1^\perp$. Then $E_1 + E_2 = \mathbb{F}_q$. The code \mathcal{C}_{f_D} is a minimal $[242, 6, 34]$ code with the weight enumerator $1 + 2z^{34} + 416z^{160} + 242z^{162} + 52z^{169} + 16z^{187}$. The code $\mathcal{C}_{f_{\overline{D}}}$ is a minimal $[242, 6, 136]$ code with the weight enumerator $1 + 16z^{136} + 52z^{154} + 242z^{162} + 416z^{163} + 2z^{208}$.

For some subspaces which do not satisfy (8), we have the following theorem on minimal linear codes.

Theorem 3.12: Let p be a prime and let $D = \cup_{i=1}^3 E_i \setminus \{0\}$, where E_1, E_2, E_3 are three subspaces of \mathbb{F}_q , $E_j \cap E_j = \{0\}$ for $1 \leq i \neq j \leq 3$, $\cap_{i=1}^3 E_i^\perp = \{0\}$, and $1 \leq t_1 = t_2 < t_3 \leq m-2$. Let t_{ij} be the dimension of $E_i^\perp \cap E_j^\perp$ for $1 \leq i \neq j \leq 3$. Then the codes \mathcal{C}_{f_D} and $\mathcal{C}_{f_{\overline{D}}}$ defined in (7) are $[p^m - 1, m+1]$ codes, whose weight distributions are in Table VI and Table VII, respectively. Furthermore, the code \mathcal{C}_{f_D} is minimal such that $\frac{w_{min}}{w_{max}} \leq \frac{p-1}{p}$.

TABLE VI
THE WEIGHT DISTRIBUTION OF \mathcal{C}_{f_D} IN THEOREM 3.12

Weight	Frequency
0	1
$p^m - p^{m-1}$	$p^m - 1$
$\sum_{i=1}^3 p^{t_i} - 3$	$p - 1$
$p^m - p^{m-1} + p^{t_i} - 3$ for $1 \leq i \leq 3$	$(p-1)(p^{m-t_i} - \sum_{j \neq i} p^{t_{ij}} + 1)$
$p^m - p^{m-1} + p^{t_i} + p^{t_j} - 3$ for $1 \leq i < j \leq 3$	$(p-1)(p^{t_{ij}} - 1)$
$p^m - p^{m-1} - 3$	$(p-1)(p^m - \cup_{i=1}^3 E_i^\perp)$

TABLE VII
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_{f_{\overline{D}}}$ IN THEOREM 3.12

Weight	Frequency
0	1
$p^m - p^{m-1}$	$p^m - 1$
$p^m + 2 - \sum_{i=1}^3 p^{t_i}$	$p - 1$
$p^m - p^{m-1} + 2 - p^{t_i} - p^{t_j}$ for $1 \leq i < j \leq 3$	$(p-1)(p^{m-t_{ij}} - 1)$
$p^m - p^{m-1} + 2 - p^{t_i}$ for $1 \leq i \leq 3$	$(p-1)(p^{m-t_i} - \sum_{j \neq i} p^{t_{ij}} + 1)$
$p^m - p^{m-1} + 2$	$(p-1)(p^m - \cup_{i=1}^3 E_i^\perp)$

Proof: Note that

$$\hat{f}_D(w) = \begin{cases} p^m + (\zeta_p - 1)(\sum_{i=1}^s |E_i| - s), & \text{if } w = 0; \\ (\zeta_p - 1)(|E_i| - s), & \text{if } w \in E_i^\perp \setminus \{0\} \text{ and } w \notin E_j^\perp \text{ for } 1 \leq i \leq s; \\ (\zeta_p - 1)(|E_i| + |E_j| - s), & \text{if } w \in (E_i^\perp \cap E_j^\perp) \setminus \{0\} \text{ for } 1 \leq i \neq j \leq s; \\ -(\zeta_p - 1)s, & \text{if } w \in \mathbb{F}_q \setminus (\cup_{i=1}^s E_i^\perp), \end{cases}$$

where $|E_i| = p^{t_i}$. By a similar proof, this theorem follows. \blacksquare

Example 3: Let $p = 2$ and let $m = 5$. Let w be a primitive element of \mathbb{F}_q such that $w^5 + w^2 + 1 = 0$. Take $E_1 = \langle w^3 \rangle$, $E_2 = \langle w^4 \rangle$ and $E_3 = \langle w^6, w^{10}, w^{28} \rangle$. Then $E_i \cap E_j = \{0\}$ for $1 \leq i \neq j \leq 3$, $t_1 = t_2 = 1$, $t_3 = 3$, $\dim(E_1^\perp \cap E_2^\perp) = 3$, $\dim(E_1^\perp \cap E_3^\perp) = 1$, $\dim(E_2^\perp \cap E_3^\perp) = 1$, and $\cap_{i=1}^3 E_i^\perp = \{0\}$. The code \mathcal{C}_{f_D} is a minimal binary $[31, 6, 9]$ code with the weight enumerator $1 + z^9 + 7z^{13} + 14z^{15} + 31z^{16} + 7z^{17} + z^{21} + 2z^{23}$. The code $\mathcal{C}_{f_{\overline{D}}}$ is a binary $[31, 6, 8]$ code with the weight enumerator $1 + 2z^8 + z^{10} + 7z^{14} + 45z^{16} + 7z^{18} + z^{22}$.

Example 4: Let $p = 3$ and let $m = 5$. Let w be a primitive element of \mathbb{F}_q such that $w^5 + 2w^2 + 1 = 0$. Take $E_1 = \langle w^{75} \rangle$, $E_2 = \langle w^{223} \rangle$ and $E_3 = \langle w^5, w^{56}, w^{142} \rangle$. Then $E_i \cap E_j = \{0\}$ for $1 \leq i \neq j \leq 3$, $t_1 = t_2 = 1$, $t_3 = 3$, $\dim(E_1^\perp \cap E_2^\perp) = 3$, $\dim(E_1^\perp \cap E_3^\perp) = 1$, $\dim(E_2^\perp \cap E_3^\perp) = 1$, and $\cap_{i=1}^3 E_i^\perp = \{0\}$. The code \mathcal{C}_{f_D} is a minimal binary $[242, 6, 30]$ code with the weight enumerator $1 + 2z^{30} + 208z^{159} + 450z^{162} + 52z^{165} + 8z^{186} + 8z^{189}$. The code $\mathcal{C}_{f_{\overline{D}}}$ is a minimal binary $[242, 6, 134]$ code with the weight enumerator $1 + 8z^{134} + 8z^{137} + 52z^{158} + 208z^{161} + 242z^{162} + 208z^{164} + 2z^{212}$.

IV. MINIMAL LINEAR CODES FROM THE DEFINING SET METHOD

In this section, by a defining set $D \subset \mathbb{F}_q^*$, we use the characteristic function f_D to give a characterization of a minimal linear code \mathcal{C}_D in (1). For any $\beta \in \mathbb{F}_q$, let $\mathbf{c}_\beta = (Tr(\beta x))_{x \in D}$. For $\beta \neq 0$, note that

$$\begin{aligned}
wt(\mathbf{c}_\beta) &= |D| - \frac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in D} \zeta_p^{-y Tr(\beta x)} \\
&= |D| - \frac{1}{p} |D| - \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in D} \zeta_p^{-Tr(y\beta x)} \\
&= \frac{p-1}{p} |D| - \frac{1}{p\zeta_p} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in D} \zeta_p^{1-Tr(y\beta x)} \\
&= \frac{p-1}{p} |D| - \frac{1}{p\zeta_p} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in D} \zeta_p^{f_D(x) - Tr(y\beta x)} \\
&= \frac{p-1}{p} |D| - \frac{1}{p\zeta_p} \sum_{y \in \mathbb{F}_p^*} \left(\sum_{x \in \mathbb{F}_q} \zeta_p^{f_D(x) - Tr(y\beta x)} - \sum_{x \in \mathbb{F}_q \setminus D} \zeta_p^{f_D(x) - Tr(y\beta x)} \right) \\
&= \frac{p-1}{p} |D| - \frac{1}{p\zeta_p} \sum_{y \in \mathbb{F}_p^*} \left(\hat{f}_D(y\beta) - \sum_{x \in \mathbb{F}_q \setminus D} \zeta_p^{-Tr(y\beta x)} \right) \\
&= \frac{p-1}{p} |D| - \frac{1}{p\zeta_p} \sum_{y \in \mathbb{F}_p^*} \left(\hat{f}_D(y\beta) - \sum_{x \in \mathbb{F}_q} \zeta_p^{-Tr(y\beta x)} + \sum_{x \in D} \zeta_p^{-Tr(y\beta x)} \right) \\
&= \frac{p-1}{p} |D| - \frac{1}{p\zeta_p} \sum_{y \in \mathbb{F}_p^*} \left(\hat{f}_D(y\beta) + \sum_{x \in D} \zeta_p^{-Tr(y\beta x)} \right) \\
&= \frac{p-1}{p} |D| - \frac{1}{p\zeta_p} \sum_{y \in \mathbb{F}_p^*} \left(\hat{f}_D(y\beta) + \frac{1}{\zeta_p - 1} \hat{f}_D(y\beta) \right) \\
&= \frac{p-1}{p} |D| - \frac{1}{p(\zeta_p - 1)} \sum_{y \in \mathbb{F}_p^*} \hat{f}_D(y\beta). \tag{10}
\end{aligned}$$

For any two $\beta_1, \beta_2 \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_p^*$, we have $\mathbf{c}_{\beta_1} + c\mathbf{c}_{\beta_2} = \mathbf{c}_{\beta_1 + c\beta_2}$. By Theorem 1.2, we have the following theorem.

Theorem 4.1: Let $D \subset \mathbb{F}_q^*$ and let \mathcal{C}_D be a linear code of dimension m over \mathbb{F}_p defined in (1). Then \mathcal{C}_D is a minimal code if and only if

$$\sum_{y \in \mathbb{F}_p^*} \left(\sum_{c \in \mathbb{F}_p^*} \hat{f}_D(y\beta_1 + yc\beta_2) + \hat{f}_D(y\beta_2) - (p-1)\hat{f}_D(y\beta_1) \right) \neq (\zeta_p - 1)(p-1)|D| \tag{11}$$

for any \mathbb{F}_p linearly independent $\beta_1, \beta_2 \in \mathbb{F}_q^*$.

Remark 6: Take D as a subset of $\mathbb{F}_p^m \setminus \{0\}$. By the defining method, we can also define a linear code \mathcal{C}_D from D , where the trace function is replace by the inner product. For any $\beta \in \mathbb{F}_p^m$, the weight of a codeword \mathbf{c}_β can also be determined by the Walsh transform of the characteristic function of D in (10). Hence, Theorem 4.1 also holds for a subset D of $\mathbb{F}_p^m \setminus \{0\}$.

When $p = 2$, we have a characterization of minimal linear codes \mathcal{C}_D and $\mathcal{C}_{\overline{D}}$.

Theorem 4.2: Let $p = 2$. Let $D \subset \mathbb{F}_q^*$ and let \mathcal{C}_D be a linear code of dimension m over \mathbb{F}_p defined in (1). Then \mathcal{C}_D is a minimal code if and only if $\hat{f}_D(\beta_1 + \beta_2) - \hat{f}_D(\beta_1) - \hat{f}_D(\beta_2) \neq 2|D|$ for any $\beta_1 \neq \beta_2 \in \mathbb{F}_q^*$. Furthermore, if $|\hat{f}_D(\beta)| < \frac{2}{3}|D|$ for any $\beta \in \mathbb{F}_q^*$, then \mathcal{C} is minimal.

Corollary 4.3: Let $p = 2$. Let $D \subset \mathbb{F}_q^*$ and let $\mathcal{C}_{\overline{D}}$ be a linear code of dimension m over \mathbb{F}_p defined in (1), where $\overline{D} = \mathbb{F}_q^* \setminus D$. The code $\mathcal{C}_{\overline{D}}$ is a minimal code if and only if $\hat{f}_D(\beta_1) + \hat{f}_D(\beta_2) - \hat{f}_D(\beta_1 + \beta_2) \neq 2(2^m - |D|)$ for any $\beta_1 \neq \beta_2 \in \mathbb{F}_q^*$.

In the following, we will give minimal linear codes from subsets of $\mathbb{F}_p^m \setminus \{\mathbf{0}\}$. Define

$$D_{12} = \{\beta : \beta \in \mathbb{F}_p^m, 1 \leq wt(\beta) \leq 2\}. \quad (12)$$

Then

$$\begin{aligned} |D_{12}| &= (p-1) \binom{m}{1} + (p-1)^2 \binom{m}{2} \\ &= \frac{p-1}{2} m(pm - p - m + 3). \end{aligned}$$

For a $\beta = (b_0, \dots, b_{m-1}) \in \mathbb{F}_p^m \setminus \{\mathbf{0}\}$, let $t = wt(\beta)$, $s = m - t$ and $A = \sum_{x \in D_{12}} \zeta_p^{-\langle \beta, x \rangle}$. We have $\hat{f}_{D_{12}}(\beta) = (\zeta_p - 1) \sum_{x \in D_{12}} \zeta_p^{-\langle \beta, x \rangle} = (\zeta_p - 1)A$ and

$$\begin{aligned} A &= \sum_{x \in D_{12}, wt(x)=1} \zeta_p^{-\langle \beta, x \rangle} + \sum_{x \in D_{12}, wt(x)=2} \zeta_p^{-\langle \beta, x \rangle} \\ &= \sum_{y \in \mathbb{F}_p^*} \sum_{i=0}^{m-1} \zeta_p^{-yb_i} + \sum_{y_1, y_2 \in \mathbb{F}_p^*} \sum_{0 \leq i < j \leq m-1} \zeta_p^{-(y_1 b_i + y_2 b_j)} \\ &= \sum_{i=0}^{m-1} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-yb_i} + \sum_{0 \leq i < j \leq m-1} \sum_{y_1 \in \mathbb{F}_p^*} \zeta_p^{-y_1 b_i} \sum_{y_2 \in \mathbb{F}_p^*} \zeta_p^{-y_2 b_j}. \end{aligned}$$

Note that $\sum_{y \in \mathbb{F}_p^*} \zeta_p^{-yb_i} = p-1$ for $b_i = 0$ and $\sum_{y \in \mathbb{F}_p^*} \zeta_p^{-yb_i} = -1$ for $b_i \neq 0$. We have

$$\begin{aligned} A &= s(p-1) + t(-1) + \binom{s}{2}(p-1)(p-1) + st(-1)(p-1) + \binom{t}{2}(-1)(-1) \\ &= \frac{p^2}{2}t^2 - \frac{1}{2}(2p(p-1)m + 4p - p^2)t + \frac{p-1}{2}m(pm - p - m + 3). \end{aligned}$$

We have $\hat{f}_{D_{12}}(\beta) = (\zeta_p - 1)A$, $\hat{f}_{D_{12}}(y\beta) = \hat{f}_{D_{12}}(\beta)$ ($y \in \mathbb{F}_p^*$), and

$$\begin{aligned} wt(\mathbf{c}_\beta) &= \frac{p-1}{p} |D_{12}| - \frac{1}{p(\zeta_p - 1)} \sum_{y \in \mathbb{F}_p^*} \hat{f}_{D_{12}}(y\beta) \\ &= \frac{p-1}{p} |D_{12}| - \frac{p-1}{p} A \\ &= \frac{p-1}{2} (-pt^2 + (2(p-1)m + 4 - p)t). \end{aligned}$$

Hence, the weight of the codeword \mathbf{c}_β is determined by the weight $wt(\beta)$. Given p and m , we can determine the minimum and maximum nonzero Hamming weights. We need the following lemma to prove that the code $\mathcal{C}_{D_{12}}$ is minimal.

Lemma 4.4: Let D be a subset of \mathbb{F}_p^m satisfying $yD = D$ for any $y \in \mathbb{F}_p^*$. Then for any $\beta \in \mathbb{F}_p^*$,

$$\sum_{x \in D} \zeta_p^{-\langle \beta, x \rangle} = \frac{1}{p-1} (-|D| + p|\{x \in D : \langle \beta, x \rangle = 0\}|). \quad (13)$$

Proof: For any $y \in \mathbb{F}_p^*$, $yD = D$. We have

$$\begin{aligned}
\sum_{x \in D} \zeta_p^{-\langle \beta, x \rangle} &= \frac{1}{p-1} \sum_{x \in D} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-\langle y\beta, x \rangle} \\
&= \frac{1}{p-1} \left(\sum_{x \in D, \langle \beta, x \rangle = 0} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-y\langle \beta, x \rangle} + \sum_{x \in D, \langle \beta, x \rangle \neq 0} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-y\langle \beta, x \rangle} \right) \\
&= \frac{1}{p-1} \left(\sum_{x \in D, \langle \beta, x \rangle = 0} (p-1) + \sum_{x \in D, \langle \beta, x \rangle \neq 0} (-1) \right) \\
&= \frac{1}{p-1} (-|D| + p|\{x \in D : \langle \beta, x \rangle = 0\}|).
\end{aligned}$$

■

Using Theorem 4.2, we have the following theorem on minimal linear codes $\mathcal{C}_{D_{12}}$.

Theorem 4.5: Let D_{12} be defined in (12). Then the code $\mathcal{C}_{D_{12}}$ is a minimal linear code. Further, when $m \geq 6$, the code $\mathcal{C}_{D_{12}}$ satisfies $\frac{w_{\min}}{w_{\max}} \leq \frac{p-1}{p}$.

Proof: By Theorem 4.1, we just need to prove that $\mathcal{C}_{D_{12}}$ satisfies (11). For any \mathbb{F}_p linearly independent $\beta_1, \beta_2 \in \mathbb{F}_p^m$, define

$$M = \sum_{y \in \mathbb{F}_p^*} \left(\sum_{c \in \mathbb{F}_p^*} \hat{f}_{D_{12}}(y\beta_1 + yc\beta_2) + \hat{f}_{D_{12}}(y\beta_2) - (p-1)\hat{f}_{D_{12}}(y\beta_1) \right).$$

Note that D_{12} satisfies Lemma 4.4, $\hat{f}_{D_{12}}(\beta) = (\zeta_p - 1) \sum_{x \in D_{12}} \zeta_p^{-\langle \beta, x \rangle}$, and $\hat{f}_{D_{12}}(y\beta) = \hat{f}_{D_{12}}(\beta)$, where $y \in \mathbb{F}_p^*$. We have

$$\begin{aligned}
M &= (p-1) \left(\sum_{c \in \mathbb{F}_p^*} \hat{f}_{D_{12}}(\beta_1 + c\beta_2) + \hat{f}_{D_{12}}(\beta_2) - (p-1)\hat{f}_{D_{12}}(\beta_1) \right) \\
&= (p-1)(\zeta_p - 1)(A_1 + A_2 - A_3)
\end{aligned}$$

where $A_1 = \sum_{c \in \mathbb{F}_p^*} \sum_{x \in D_{12}} \zeta_p^{-\langle \beta_1 + c\beta_2, x \rangle}$, $A_2 = \sum_{x \in D_{12}} \zeta_p^{-\langle \beta_2, x \rangle}$ and $A_3 = (p-1) \sum_{x \in D_{12}} \zeta_p^{-\langle \beta_1, x \rangle}$. Note that

$$\begin{aligned}
A_1 &= \sum_{x \in D_{12}} \zeta_p^{-\langle \beta_1, x \rangle} \sum_{c \in \mathbb{F}_p^*} \zeta_p^{-\langle c\beta_2, x \rangle} \\
&= \sum_{x \in D_{12}, \langle \beta_2, x \rangle = 0} (p-1)\zeta_p^{-\langle \beta_1, x \rangle} + \sum_{x \in D_{12}, \langle \beta_2, x \rangle \neq 0} (-1)\zeta_p^{-\langle \beta_1, x \rangle} \\
&= p \sum_{x \in D_{12}, \langle \beta_2, x \rangle = 0} \zeta_p^{-\langle \beta_1, x \rangle} - \sum_{x \in D_{12}} \zeta_p^{-\langle \beta_1, x \rangle}.
\end{aligned}$$

By Lemma 4.4, we have

$$\begin{aligned}
M &= (p-1)(\zeta_p - 1) \left(p \left(\sum_{x \in D_{12}, \langle \beta_2, x \rangle = 0} \zeta_p^{-\langle \beta_1, x \rangle} - \sum_{x \in D_{12}} \zeta_p^{-\langle \beta_1, x \rangle} \right) + \sum_{x \in D_{12}} \zeta_p^{-\langle \beta_2, x \rangle} \right) \\
&= (p-1)(\zeta_p - 1) \left(\sum_{x \in D_{12}} \zeta_p^{-\langle \beta_2, x \rangle} - p \sum_{x \in D_{12}, \langle \beta_2, x \rangle \neq 0} \zeta_p^{-\langle \beta_1, x \rangle} \right) \\
&= (\zeta_p - 1) \left(-|D_{12}| + p|\{x \in D_{12} : \langle \beta_2, x \rangle = 0\}| \right. \\
&\quad \left. - p(-|\{x \in D_{12} : \langle \beta_2, x \rangle \neq 0\}| + p|\{x \in D_{12} : \langle \beta_2, x \rangle \neq 0, \langle \beta_1, x \rangle = 0\}|) \right) \\
&= (\zeta_p - 1) ((p-1)|D_{12}| - p^2|\{x \in D_{12} : \langle \beta_2, x \rangle \neq 0, \langle \beta_1, x \rangle = 0\}|).
\end{aligned}$$

Hence, we need to prove that $|\{x \in D_{12} : \langle \beta_2, x \rangle \neq 0, \langle \beta_1, x \rangle = 0\}| > 0$. Since $\beta_1 = (b_{11}, \dots, b_{1m}), \beta_2 = (b_{21}, \dots, b_{2m}) \in \mathbb{F}_p^m$ are linearly independent, there exist i and j such that (b_{1i}, b_{2i}) and (b_{1j}, b_{2j}) are linearly independent, where $1 \leq i \neq j \leq m$. Then there exist $c_1, c_2 \in \mathbb{F}_p$ such that $c_1(b_{1i}, b_{2i}) + c_2(b_{1j}, b_{2j}) = (0, 1)$. Take a vector $v = (v_1, \dots, v_m) \in \mathbb{F}_p^m$, where $v_i = c_1, v_j = c_2$, and $v_k = 0$ for $k \neq i, j$. Then $wt(v) = 1$ or 2 , and $v \in D_{12}$ such that $\langle \beta_2, v \rangle \neq 0, \langle \beta_1, v \rangle = 0$. Hence, $|\{x \in D_{12} : \langle \beta_2, x \rangle \neq 0, \langle \beta_1, x \rangle = 0\}| > 0$ and $M \neq (\zeta_p - 1)(p - 1)|D_{12}|$. By Theorem 4.1, $\mathcal{C}_{D_{12}}$ is a minimal linear code.

The weight of the codeword \mathbf{c}_β is determined by the weight $wt(\beta)$. When $wt(\beta) = 1$, $\mathbf{c}_\beta = (p - 1)(pm - m - p + 2)$. When $wt(\beta) = m$, $\mathbf{c}_\beta = \frac{1}{2}(p - 1)m(pm - 2m - p + 4)$. When $p = 2$ and $m \geq 6$, we can verify that $\frac{w_{min}}{w_{max}} \leq \frac{1}{2}$. When $p \geq 3$ and $m \geq 5$, we have

$$\begin{aligned} \frac{w_{min}}{w_{max}} &\leq \frac{2(pm - m - p + 2)}{m(pm - 2m - p + 4)} \\ &\leq \frac{2(p - 1)}{(p - 2)m - p + 4} \\ &\leq \frac{2(p - 1)}{(p - 2) \cdot 5 - p + 4} \\ &\leq \frac{p - 1}{p}. \end{aligned}$$

Hence, this theorem follows. ■

Remark 7: When $p = 2$, these codes have been studied in [38].

Example 5: Let $p = 2$ and let $m = 5$. Take $D = \{x \in \mathbb{F}_p^m \setminus \{0\} : wt(x) = 1, 2, m\}$. Then $|\hat{f}_D(\beta)| < \frac{2}{3}|D|$ for any $\beta \in \mathbb{F}_q^*$. The code \mathcal{C}_{f_D} is a minimal binary $[16, 5, 6]$ code with the weight enumerator $1 + 6z^6 + 15z^8 + 10z^{10}$. The code $\mathcal{C}_{f_{\overline{D}}}$ is a minimal binary $[15, 5, 6]$ code with the weight enumerator $1 + 10z^6 + 15z^8 + 6z^{10}$.

Example 6: Let $p = 3$ and let $m = 6$. Take $D_{12} = \{x \in \mathbb{F}_p^m \setminus \{0\} : wt(x) = 1, 2\}$. The code $\mathcal{C}_{f_{D_{12}}}$ is a minimal $[72, 6, 22]$ code with the weight enumerator $1 + 12z^{22} + 60z^{38} + 64z^{42} + 160z^{48} + 192z^{50} + 240z^{52}$, and it satisfies that $\frac{w_{min}}{w_{max}} \leq \frac{2}{3}$.

Example 7: Let $p = 5$ and let $m = 4$. Take $D_{12} = \{x \in \mathbb{F}_p^m \setminus \{0\} : wt(x) = 1, 2\}$. The code $\mathcal{C}_{f_{D_{12}}}$ is a minimal $[112, 4, 52]$ code with the weight enumerator $1 + 16z^{52} + 96z^{84} + 256z^{88} + 256z^{96}$, and it satisfies that $\frac{w_{min}}{w_{max}} \leq \frac{4}{5}$.

V. CONCLUSION

By characteristic functions of subsets of \mathbb{F}_q , we can construct more minimal linear codes, which generalizes results in [24] for the binary case and [36] for p odd. These minimal linear codes satisfy $\frac{w_{min}}{w_{max}} \leq \frac{p-1}{p}$. It is interesting to construct more minimal linear codes. We also use characteristic functions to present a characterization of minimal linear codes from the defining set method. Theorem 2.2 is efficient to determine a minimal binary linear code. Theorem 1.2 is not efficient enough for a minimal linear code for p odd. It would be interesting to present more efficient results to determine minimal linear codes for p odd.

REFERENCES

- [1] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 2010-2017, 1998.
- [2] A. Ashikhmin, A. Barg, G. Cohen, and L. Huguët, "Variations on minimal codewords in linear codes," in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-11) (Lecture Notes in Computer Science, vol. 948), G. Cohen, M. Giusti, and T. Mora, Eds. Berlin: Springer-Verlag, pp. 96-105, 1995.
- [3] D. Bartoli and M. Bonini, "Minimal linear codes in odd characteristic," IEEE Trans. Inf. Theory, vol. 65, no. 7, pp. 4152-4155, 2019.
- [4] M. Bonini, M. Borello, "Minimal linear codes arising from blocking sets," <https://arxiv.org/abs/1907.04626v1>.
- [5] A. R. Calderbank and J. M. Goethals, "Three-weight codes and association schemes," Philips J. Res., vol. 39, no. 4-5, pp. 143-152, 1984.
- [6] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," Bull. London Math. Soc., vol. 18, no. 2, pp. 97-122, 1986.

- [7] C. Carlet et al., "Optimized linear complementary codes implementation for hardware trojan prevention," in Proc. 22nd Eur. Conf. Circuit Theory Design (ECCTD), 2015, pp. 1-4.
- [8] C. Carlet and S. Guilley, "Complementary dual codes for countermeasures to side-channel attacks," J. Adv. Math. Commun., vol. 10, no. 1, pp. 131C150, 2016.
- [9] C. Carlet, "Boolean functions for cryptography and error correcting codes," in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257-397.
- [10] C. Carlet and C. Ding, "Nonlinearities of S-boxes," Finite Fields and Their Applications, vol. 13, pp. 121-135, 2007.
- [11] C. Carlet, C. Ding, and J. Yuan, "Linear codes from highly nonlinear functions and their secret sharing schemes," IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 2089-2102, 2005.
- [12] C. Carlet and S. Mesnager, "Four decades of research on bent functions," Des. Codes Cryptogr., vol. 78, no. 1, pp. 5-50, 2016.
- [13] C. Carlet, S. Mesnager, C. Tang, Y. Qi, "Euclidean and Hermitian LCD MDS codes," Des. Codes Cryptogr., vol. 86, no. 11, pp. 2605-2618, 2018.
- [14] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaan, "Linear codes over \mathbb{F}_q are equivalent to LCD codes for $q > 3$," IEEE Trans. Inf. Theory, vol. 64, no. 4, pp. 3010-3017, 2018.
- [15] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," Des. Codes Cryptogr., vol. 52, pp. 303-338, 2009.
- [16] H. Chabanne, G. Cohen, and A. Patey, "Towards secure two-party computation from the wire-tap channel," in: Proceedings of ICISC 2013 (Lecture Notes in Computer Science, vol. 8565), H.-S. Lee and D.-G. Han Eds. Berlin: Springer-Verlag, pp. 34-46, 2014.
- [17] S. Chang and J. Y. Hyun, "Linear codes from simplicial complexes," Des. Codes Cryptogr., vol. 86, no. 10, pp. 2167-2181, 2018.
- [18] P. Charpin, E. Pasalic, C. Tavernier, "On bent and semi-bent quadratic Boolean functions," IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4286-4298, 2005.
- [19] G. Cohen, S. Mesnager, and A. Patey, "On minimal and quasi-minimal linear codes" in: Proceedings of IMACC (Lecture Notes in Computer Science, vol. 8308), M. Stam, Eds. Berlin: Springer-Verlag, pp. 85-98, 2003.
- [20] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. thesis, Univ. of Maryland, 1974.
- [21] C. Ding, "Linear codes from some 2-designs," IEEE Trans. Inf. Theory, vol. 60, no. 6, pp. 3265-3275, 2015.
- [22] C. Ding, "A construction of binary linear codes from Boolean functions," Discrete Mathematics, vol. 339, pp. 2288-2303, 2016.
- [23] C. Ding, T. Hellese, T. Kløve and X. Wang, "A Generic Construction of Cartesian Authentication Codes," IEEE Trans. Inf. Theory, vol. 53, no. 6, pp. 2229-2235, 2007.
- [24] C. Ding, Z. Heng, and Z. Zhou, "Minimal binary linear codes," IEEE Trans. Inf. Theory, vol. 64, no. 10, pp. 6536 - 6545, 2018.
- [25] C. Ding and J. Yuan, "Covering and secret sharing with linear codes," in: Discrete Mathematics and Theoretical Computer Science, Lecture Notes in Computer Science 2731, 2003, Springer Verlag, pp. 11-25.
- [26] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," Theor. Comp. Sci., vol. 330, no. 1, pp. 81-99, 2005.
- [27] Z. Heng, C. Ding, and Z. Zhou, "Minimal linear codes over finite fields," Finite Fields Appl., vol. 54, pp. 176-196, 2018.
- [28] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
- [29] R. L. McFarland, "A family of difference sets in non-cyclic groups," Journal of Combinatorial Theory, Series A, vol. 15, no. 1, pp. 1-10, 1973.
- [30] J. L. Massey, "Minimal codewords and secret sharing," in: Proc. 6th Joint Swedish-Russian Workshop on Information Theory (Molle, Sweden, 1993), pp. 246-249.
- [31] S. Mesnager, "Bent functions: fundamentals and results," in Springer Verlag, Switzerland, 2016.
- [32] S. Mesnager, "Linear codes with few weights from weakly regular bent functions based on a generic construction," Cryptogr. Commun., vol. 9, pp. 71-84, 2017.
- [33] S. Mesnager, C. Tang, Y. Qi, "Complementary dual algebraic geometry codes," IEEE Trans. Inf. Theory, vol. 64, no. 4, pp. 2390-2397, 2018.
- [34] S. Mesnager, F. Ozbudak, A. Sınak, "Linear codes from weakly regular plateaued functions and their secret sharing schemes," Des. Codes Cryptogr., vol. 87, no. 2-3, pp. 463-480, 2019.
- [35] T. Wadayama, T. Hada, K. Wakasugi, and M. Kasahara, "Upper and lower bounds on maximum nonlinearity of n-input m-output Boolean function," Des. Codes Cryptogr., vol. 23, pp. 23-33, 2001.
- [36] G. Xu, L. Qu, "Three classes of minimal linear codes over the finite fields of odd characteristic," IEEE Trans. Inf. Theory, vol. 65, no. 11, pp. 7067-7078, 2019.
- [37] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," IEEE Trans. Inf. Theory, vol. 52, no. 1, pp. 206-212, 2006.
- [38] W. Zhang, H. Yan, and H. Wei, "Four families of minimal binary linear codes with $w_{min}/w_{max} \leq 1/2$," Appl. Algebra Eng. Commun. Comput., vol. 30, no. 2, pp. 175-184, 2019.
- [39] Z. Zhou, X. Li, C. Tang, C. Ding, "Binary LCD codes and self-orthogonal codes from a generic construction," IEEE Trans. Inf. Theory, vol. 65, no. 1, pp. 16-27, 2019.