Two Classes of Linear Codes From Weil Sums

HONG LU AND SHUDI YANG

School of Mathematical Sciences, Qufu Normal University, Jining 273165, China
Corresponding author: Shudi Yang (yangshudi@qfnu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 11701317.

ABSTRACT In this article, we consider two classes of $p$-ary linear codes. This article is a generalization of the recent construction methods given by Jian, Lin and Feng (2019). By choosing different defining sets, two classes of two-weight or three-weight linear codes over finite fields are constructed and their weight distributions are determined based on Weil sums. We also give some examples and some of the linear codes are almost optimal with respect to the Griesmer bound which can be directly employed to obtain democratic secret sharing schemes. Additionally, all nonzero codewords are minimal and they are crucial to apply in association schemes, strongly regular graphs, weakly regular plateaued functions and authentication codes.

INDEX TERMS Linear codes, weight distributions, Weil sums, the Pless power moments.

I. INTRODUCTION

Throughout this article, let $F_p$ be the finite field with $p$ elements, where $p$ is an odd prime. An $[n, k, d_H]$ linear code $C$ over $F_p$ is a $k$-dimensional subspace of $F_p^n$ with minimum Hamming distance $d_H$. Let $A_i$ denote the number of codewords with Hamming weight $i$ in a code $C$. The weight enumerator of $C$ is defined by the polynomial

$$A(z) = 1 + A_1 z + A_2 z^2 + \cdots + A_n z^n.$$ 

The sequence $(A_1, A_2, \cdots, A_n)$ is called the weight distribution of the code $C$. A code $C$ is said to be a $t$-weight code if the number of nonzero $A_i$ in the sequence $(A_1, A_2, \cdots, A_n)$ is equal to $t$.

The weight distribution of a linear code is of vital use in coding theory. It provides significant information on the error correcting capability and the error probability of its error detection and correction [27]. That is why it has attracted a lot of interests for many years. In addition, much attention has been paid to two-weight and three-weight linear codes [9], [13], [14], [17]–[20], [22] due to their applications in secret sharing schemes [11], [25], [35], association schemes [1], [26], strongly regular graphs [2], weakly regular plateaued functions [24] and authentication codes [6]. We refer the reader to [12], [28]–[34] and references therein for an overview of the related data distributions of linear codes.

Let $m$ be a positive integer and $q = p^m$. The trace function from $F_q$ to $F_p$ is denoted by $Tr$. For a set $D = \{d_1, d_2, \cdots, d_n\} \subseteq F_q$, we define a $p$-ary linear code by

$$C_D = \{C(a) = (Tr(ad_1), Tr(ad_2), \cdots, Tr(ad_n)) : a \in F_q\}.$$ 

The set $D$ is called the defining set of $C_D$. Ding et al. in [7] first proposed this construction and many classes of known codes could be produced by appropriately selecting different defining sets.

In [16], Jian, Lin and Feng defined $p$-ary linear codes by

$$C_D = \{C(a, b) = (Tr(ax + by))_{(x, y) \in D} : a, b \in F_q\},$$

which can be viewed as a generalization of cyclic codes whose dual codes have two zeros. Let $u$ be a positive integer. They chose the linear codes with the defining sets given by

$$D^{(0)}_1 = \{(x, y) \in F_q^2 \setminus \{(0, 0)\} : Tr(x + y^{p+1}) = 0\},$$

$$D^{(0)}_2 = \{(x, y) \in F_q^2 \setminus \{(0, 0)\} : Tr(x^2 + y^{p+1}) = 0\}$$

determined their weight distributions.

Motivated by the generic construction and the work of [16], we generalize the results by choosing the defining sets given by

$$D_1 = \{(x, y) \in F_q^2 : Tr(x + y^{p+1}) = 1\},$$

and

$$D_2 = \{(x, y) \in F_q^2 : Tr(x^2 + y^{p+1}) = 1\}.$$ 

In this way, the linear code $C_D$ with the defining sets given by $D^{(c)}_1 = \{(x, y) \in F_q^2 \setminus \{(0, 0)\} : Tr(x + y^{p+1}) = c\}$ and $D^{(c)}_2 = \{(x, y) \in F_q^2 \setminus \{(0, 0)\} : Tr(x^2 + y^{p+1}) = c\}$ for all $c \in F_q$ can be attained.

For this two classes of linear codes, we will study their parameters and weight distributions using Weil sums.
As proved later, they are linear codes with two or three nonzero weights. In particular, some of the linear codes obtained are almost optimal with respect to the Griesmer bound [10]. All of linear codes obtained are minimal, which indicates that the linear codes can be of use in secret sharing schemes.

The remainder of this article is organized as follows. In Section II we present the parameters of two classes of two-weight or three-weight linear codes and also give some examples. In Section III we recall some basic notations and results on group characters, exponential sums and the Pless power moments, which will be employed later. Section IV is devoted to giving the proofs of the main results. Section V shows that every nonzero codeword of the codes is minimal. Section VI concludes this article.

II. MAIN RESULTS

We introduce a few auxiliary parameters. Let \( m, u \) be positive integers \( m \geq 2 \) and \( p \) be an odd prime, denote \( q = p^m \) and \( s = \frac{m}{2} \) if \( 2 | m \). Let \( d = \gcd(m, u) \) be the greatest common divisor of \( m \) and \( u \). In this section, we describe the codes, introduce their parameters and give some examples. The proofs of their parameters will be given in Section IV.

**Theorem 1:** The code \( C_{D_1} \) is defined by (1) and (2). If \( m \) is odd, then \( C_{D_1} \) is a \( \left[p^{2m-1}, 2m, (p - 1)p^{2m-2} - p^{\frac{3m-4}{2}}\right] \) three-weight linear code with weight distribution given in Table 1, where \( A_w = 0 \) for all other weights \( w \) not listed in the table.

**Example 1.1:** Let \((p, m) = (3, 3)\). By Theorem 1 the code \( C_{D_1} \) has parameters \([243, 6, 135]\) and weight enumerator \(1 + 12z^{135} + 698z^{162} + 18z^{189}\).

**Example 1.2:** Let \((p, m) = (3, 5)\). By Theorem 1 the code \( C_{D_1} \) has parameters \([19683, 10, 12393]\) and weight enumerator \(1 + 162z^{12393} + 58706z^{13122} + 180z^{13851}\).

**Theorem 2:** The code \( C_{D_1} \) is defined by (1) and (2). If \( \frac{m}{2} \) is odd and \( d \) is even, then \( C_{D_1} \) is a \( \left[p^{2m-1}, 2m, d_H\right] \) three-weight linear code with weight distribution given in Table 2, where

\[
d_H = \begin{cases} 
(p - 1)p^{2m-2} - p^{\frac{3m-4}{2}}, & \text{if } p \equiv 3 \pmod{4} \text{ and } s \text{ is odd,} \\
(p - 1)p^{2m-2} - p^{\frac{3m-4}{2}}, & \text{otherwise.}
\end{cases}
\]

**Example 2.1:** Let \((p, m, u) = (3, 4, 4)\). Then \( d = \gcd(m, u) = 4, \frac{m}{2} = 1 \) and \( s = 2 \). By Theorem 2 the code \( C_{D_1} \) has parameters \([2187, 8, 1377]\) and weight enumerator \(1 + 102z^{1377} + 6398z^{1458} + 60z^{1620}\).

**Example 2.2:** Let \((p, m, u) = (3, 2, 4)\). Then \( d = \gcd(m, u) = 2, \frac{m}{2} = 1 \) and \( s = 1 \). By Theorem 2 the code \( C_{D_1} \) has parameters \([27, 4, 12]\) and weight enumerator \(1 + 14z^{12} + 62z^{18} + 14z^{21}\).

**Theorem 3:** The code \( C_{D_1} \) is defined by (1) and (2). If \( \frac{m}{2} \equiv 2 \pmod{4} \), then \( C_{D_1} \) is a \( \left[p^{2m-1}, 2m, (p - 1)p^{2m-2} - p^{\frac{3m-4}{2}}\right] \) three-weight linear code with weight distribution given in Table 3, where \( A_w = 0 \) for all other weights \( w \) not listed in the table.

**Example 3.1:** Let \((p, m, u) = (3, 2, 3)\). Then \( d = \gcd(m, u) = 1, \frac{m}{2} = 2 \) and \( s = 1 \). By Theorem 3 the code \( C_{D_1} \) has parameters \([27, 4, 15]\) and weight enumerator \(1 + 10z^{15} + 62z^{18} + 8z^{24}\).

**Example 3.2:** Let \((p, m, u) = (3, 3, 2)\). Then \( d = \gcd(m, u) = 3, \frac{m}{2} = 1 \) and \( s = 1 \). By Theorem 3 the code \( C_{D_1} \) has parameters \([27, 4, 15]\) and weight enumerator \(1 + 10z^{15} + 62z^{18} + 8z^{24}\).

**Example 4.1:** Let \((p, m, u) = (3, 3, 3)\). Then \( d = \gcd(m, u) = 3, \frac{m}{2} = 1 \) and \( s = 1 \). By Theorem 3 the code \( C_{D_1} \) has parameters \([27, 4, 15]\) and weight enumerator \(1 + 10z^{15} + 62z^{18} + 8z^{24}\).
TABLE 4. The weight distribution of $C_{D_1}$ if $\frac{n}{d} = 0 \pmod{4}$.

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

TABLE 5. The weight distribution of $C_{D_2}$ if $\frac{m}{d}$ is odd or $\frac{m}{d} = 2 \pmod{4}$.

| Weight $w$ | Multiplicity $A_w$ |
|------------|-------------------|
| $(a)$ $p \equiv 3 \pmod{4}$ and $d$ is odd | $1$ |
| $0$ | $\frac{1}{2}p^{m-1}(p^{m+1} - p + p^n) + 1$ |
| $(p-1)p^{2m-2}$ | $\frac{1}{2}p^{m-1}(p-1)(p^{m+1} + 1)$ |
| $(p-1)p^{2m-2} + 2p^{m-1}$ | $\frac{1}{2}p^{m-1}(p-1)(p^{m+1} + 1)$ |
| $(b)$ otherwise | $0$ |
| $0$ | $\frac{1}{2}p^{m-1}(p^{m+1} - p + p^n) + 1$ |
| $(p-1)p^{2m-2}$ | $\frac{1}{2}p^{m-1}(p-1)(p^{m+1} + 1)$ |
| $(p-1)p^{2m-2} - 2p^{m-1}$ | $\frac{1}{2}p^{m-1}(p-1)(p^{m+1} + 1)$ |

given in Table 4, where $A_w = 0$ for all other weights $w$ not listed in the table.

Example 4.1: Let $(p, m, u) = (3, 4, 3)$. Then $d = \gcd(m, u) = 1$, $\frac{m}{d} = 4$ and $s = 1$. By Theorem 4 the code $C_{D_1}$ has parameters $[2187, 8, 1215]$ and weight enumerator $1 + 10z^{215} + 6542z^{1458} + 8z^{1444}$.

Theorem 5: The code $C_{D_2}$ is defined by (1) and (3). If $\frac{m}{d}$ is odd or $\frac{m}{d} = 2 \pmod{4}$, then $C_{D_2}$ is an $[n, 2m, d_H]$ two-weight linear code with weight distribution given in Table 5, where

$$n = \begin{cases} p^{2m-1} + p^{m-1}, & \text{if } p \equiv 3 \pmod{4} \text{ and } d \text{ is odd,} \\ p^{2m-1} - p^{m-1}, & \text{otherwise,} \end{cases}$$

and

$$d_H = \begin{cases} (p-1)p^{2m-2}, & \text{if } p \equiv 3 \pmod{4} \text{ and } d \text{ is odd,} \\ (p-1)p^{2m-2} - 2p^{m-1}, & \text{otherwise.} \end{cases}$$

Example 5.1: Let $(p, m, u) = (3, 3, 3)$. Then $d = \gcd(m, u) = 3$ and $\frac{m}{d} = 1$. By Theorem 5 the code $C_{D_2}$ has parameters $[252, 6, 162]$ and weight enumerator $1 + 476z^{162} + 252z^{180}$.

Example 5.2: Let $(p, m, u) = (5, 2, 2)$. Then $d = \gcd(m, u) = 2$ and $\frac{m}{d} = 1$. By Theorem 5 the code $C_{D_2}$ has parameters $[120, 4, 90]$ and weight enumerator $1 + 240z^{200} + 384z^{100}$.

Example 5.3: Let $(p, m, u) = (3, 2, 3)$. Then $d = \gcd(m, u) = 1$ and $\frac{m}{d} = 2$. By Theorem 5 the code $C_{D_2}$ has parameters $[30, 4, 18]$ and weight enumerator $1 + 50z^{18} + 30z^{24}$, which is almost optimal as the best linear code of length 30 and dimension 4 over $\mathbb{F}_3$ has minimum weight 19 according to the Griesmer bound.

TABLE 6. The weight distribution of $C_{D_2}$ if $\frac{m}{d} = 0 \pmod{4}$.

| Weight $w$ | Multiplicity $A_w$ |
|------------|-------------------|
| $0$        | $1$               |
| $(p-1)p^{2m-2}$ | $p^{2m-2d} - 1 + \frac{1}{2}(p-1)p^{m-d-1}(p^{m-d-1} - 1)$ |
| $(p-1)(p^{2m-2} - p^{m+d-2})$ | $p^{2m-2d} - 1 + \frac{1}{2}(p-1)p^{m-d-1}(p^{m-d-1} - 1)$ |
| $(p-1)p^{2m-2} - 2p^{m+d-1}$ | $\frac{1}{2}(p-1)p^{m-d-1}(p^{m-d-1} - 1)$ |

Example 5.4: Let $(p, m, u) = (3, 4, 2)$. Then $d = \gcd(m, u) = 2$ and $\frac{m}{d} = 2$. By Theorem 5 the code $C_{D_2}$ has parameters $[2160, 8, 1404]$ and weight enumerator $1 + 2160z^{1404} + 4400z^{1458}$.

Theorem 6: The code $C_{D_2}$ is defined by (1) and (3). If $\frac{m}{d} \equiv 0 \pmod{4}$, then $C_{D_2}$ is a $[p^{2m-1} - p^{m+d-1}, 2m, (p-1)p^{2m-2} - 2p^{m+d-1}]$ three-weight linear code with weight distribution given in Table 6, where $A_w = 0$ for all other weights $w$ not listed in the table.

Example 6.1: Let $(p, m, u) = (3, 4, 3)$. Then $d = \gcd(m, u) = 1$, $\frac{m}{d} = 4$ and $s = 2$. By Theorem 6 the code $C_{D_2}$ has parameters $[2160, 8, 1296]$ and weight enumerator $1 + 234z^{1296} + 5832z^{1404} + 494z^{1458}$.

III. PRELIMINARIES

A. GROUP CHARACTERS AND GAUSS SUMS

Let $Tr$ denote the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$, and $\zeta_p = e^{\frac{2\pi i}{p}}$ be the primitive $p$-th root of unity. A character $\chi$ of $\mathbb{F}_q$ is a homomorphism from $\mathbb{F}_q$ into the multiplicative group $U$ of complex numbers of absolute value 1 — that is, a mapping from $\mathbb{F}_q$ into $U$ with $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in \mathbb{F}_q$. For each $b \in \mathbb{F}_q$, the function

$$\chi_b(x) = \zeta_p^{Tr(bx)} \text{ for all } x \in \mathbb{F}_q,$$

defines an additive character of $\mathbb{F}_q$. The character $\chi := \chi_1$ is called the canonical additive character of $\mathbb{F}_q$. It is clear that $\chi_b(x) = \chi(bx)$ for all $b, x \in \mathbb{F}_q$. With each character $\chi$ of $\mathbb{F}_q$ there is associated the conjugate character $\overline{\chi}$ defined by $\overline{\chi}(g) = \chi(g)$ for all $g \in \mathbb{F}_q$. The orthogonal property of additive characters is given by

$$\sum_{x \in \mathbb{F}_q} \chi_b(x) = \begin{cases} q, & \text{if } b = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ and $\psi$ be a multiplicative character of $\mathbb{F}_q^*$, we define the Gauss sum over $\mathbb{F}_q$ by

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x).$$

For certain special characters, the associated Gauss sums can be evaluated explicitly. Let $\eta$ and $\eta_p$ denote the quadratic multiplicative characters of $\mathbb{F}_q$ and $\mathbb{F}_p$ respectively. Then for $x \in \mathbb{F}_p^*$, $\eta(x) = 1$ if $m$ is even and $\eta(x) = \eta_p(x)$ if $m$ is odd. The quadratic Gauss sums are known and given in the following lemma.
Lemma 1: [23, Theorem 5.15]  
\[ G(\eta) = (-1)^{m-1}\sqrt{p^s} \]  
\[ = \begin{cases} 
(-1)^{m-1}\sqrt{q}, & \text{if } p \equiv 1 \pmod{4}, \\
(-1)^{m-1}(\sqrt{-1})^{m}\sqrt{q}, & \text{if } p \equiv 3 \pmod{4},
\end{cases} \]

where \( p^s = (-1)\frac{p-1}{2} p \).

B. WEIL SUMS

Weil sums are defined by \( \sum_{x} \chi(f(x)) \) where \( f(x) \in \mathbb{F}_q[x] \). Coulter evaluated some Weil sums in [3], [4] given by

\[ S_n(a, b) = \sum_{x \in \mathbb{F}_q} \chi(ax^{p^s+1} + bx), \quad a \in \mathbb{F}_q^n, \quad b \in \mathbb{F}_q. \]

Lemma 2: [3, Theorem 1] If \( \frac{m}{d} \) is odd, then

\[ S_n(a, 0) = G(\eta)\eta(a) = \begin{cases} 
(-1)^{m-1}\sqrt{q}\eta(a), & \text{if } p \equiv 1 \pmod{4}, \\
(-1)^{m-1}(\sqrt{-1})^{m}\sqrt{q}\eta(a), & \text{if } p \equiv 3 \pmod{4}. 
\end{cases} \]

Lemma 3: [3, Theorem 2] If \( \frac{m}{d} \) is even, then

\[ S_n(a, 0) = \begin{cases} 
p^s, & \text{if } \frac{s}{d} \text{ is even and } \frac{q-1}{2} \neq (-1)^{\frac{s}{2}}, \\
-p^{s+d}, & \text{if } \frac{s}{d} \text{ is even and } \frac{q-1}{2} = (-1)^{\frac{s}{2}}, \\
-p^s, & \text{if } \frac{s}{d} \text{ is odd and } \frac{q-1}{2} \neq (-1)^{\frac{s}{2}}, \\
p^{s+d}, & \text{if } \frac{s}{d} \text{ is odd and } \frac{q-1}{2} = (-1)^{\frac{s}{2}}. 
\end{cases} \]

Lemma 4: [3, Theorem 4.1] The equation

\[ a^m x^{p^s} + ax = 0 \]

is solvable for \( x \in \mathbb{F}^m_2 \) if and only if \( \frac{m}{d} \) is even and \( \frac{q-1}{2} = (-1)^{\frac{s}{2}} \), where \( m = 2s \). In such cases there are \( p^{sd} - 1 \) nonzero solutions.

Lemma 5: [4, Theorem 1] Suppose \( f(x) = a^m x^{p^s} + ax \) is a permutation polynomial over \( \mathbb{F}_q \). Let \( x_0 \) be the unique solution of the equation \( f(x) = -b^m \), where \( b \neq 0 \). The evaluation of \( S_n(a, b) \) partitions into the following two cases.

(i) If \( \frac{m}{d} \) is odd, then

\[ S_n(a, b) = G(\eta)\eta(a)\chi(ax_0^{p^s+1}) = \begin{cases} 
(-1)^{m-1}\sqrt{q}\eta(a)\chi(ax_0^{p^s+1}), & \text{if } p \equiv 1 \pmod{4}, \\
(-1)^{m-1}(\sqrt{-1})^{m}\sqrt{q}\eta(a)\chi(ax_0^{p^s+1}), & \text{if } p \equiv 3 \pmod{4}. 
\end{cases} \]

(ii) If \( \frac{m}{d} \) is even, then \( \frac{q-1}{2} \neq (-1)^{\frac{s}{2}} \) and \( \chi(ax_0^{p^s+1}) = (-1)^{\frac{s}{2}} p^s \chi(ax_0^{p^s+1}) \).

Lemma 6: [4, Theorem 2] Suppose \( f(x) = a^m x^{p^s} + ax \) is not a permutation polynomial over \( \mathbb{F}_q \). Then for \( b \neq 0 \) we have \( S_n(a, b) = 0 \) unless the equation \( f(x) = -b^m \) is solvable. If this equation is solvable, with some solution \( x_0 \), say, then

\[ S_n(a, b) = (-1)^{\frac{s}{2}} p^{s+d} \chi(ax_0^{p^s+1}). \]

Lemma 7: [23, Theorem 5.33] Let \( ax^2 + bx \in \mathbb{F}_q[x] \) with \( a \neq 0 \). Then

\[ Q(a, b) = \sum_{x \in \mathbb{F}_q} \chi(ax^2 + bx) = G(\eta)\eta(a)\chi(4a^2b^2). \]

C. THE PLESS POWER MOMENTS

Let \( C \) be a linear code of length \( n \) and dimension \( k \). The first two Pless power moments are given as follows [15, p.259]:

\[ \sum_{j=0}^{n} A_j = p^k, \]

\[ \sum_{j=0}^{n} jA_j = p^{k-1}(pn - n - A_1^1), \]

where \( (1, A_1, A_2, \ldots, A_n) \) is the weight distribution of \( C \) and \( A_1^1 \) is the number of codewords with Hamming weight 1 in its dual code \( C^\perp \). For the code \( D \) defined by (1), \( A_1^1 = 0 \) because \( (0, 0) \notin D \).

IV. THE PROOFS OF THE MAIN RESULTS

We present a few auxiliary results before proving the main results of this article.

Lemma 8: Let

\[ n_1 = |D_1| = |\{(x, y) \in \mathbb{F}^2_2 : \text{Tr}(x + y^{p^s+1}) = 1\} |, \]

then \( n_1 = p^{2m-1} \).

Proof: By the orthogonal property of additive characters

\[ n_1 = \sum_{x, y \in \mathbb{F}_2} \frac{1}{p} \sum_{z \in \mathbb{F}_p} \zeta_p^{\text{Tr}(x+y^{p^s+1})-1} \]

\[ = \frac{1}{p} \left( \sum_{x, y \in \mathbb{F}_2} 1 + \sum_{z \in \mathbb{F}_p} \zeta_p^{-z} \sum_{x, y \in \mathbb{F}_2} \zeta_p^{\text{Tr}(x+y^{p^s+1})} \right) \]

\[ = p^{2m-1} - 1 + \frac{1}{p} \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_2} \zeta_p^{\text{Tr}(x)} S_n(z, 0) = p^{2m-1}. \]

Lemma 9: [16, Lemma 10] If \( \frac{m}{d} \) is even, then for \( x \in \mathbb{F}^m_2 \),

\[ x^{q-1}x^{p^s+1} = 1. \]

Lemma 10: Let

\[ n_2 = |D_2| = |\{(x, y) \in \mathbb{F}^2_2 : \text{Tr}(x^2 + y^{p^s+1}) = 1\} |.

180474 VOLUME 8, 2020
Then if \( \frac{m}{d} \) is odd or \( \frac{m}{d} \equiv 2 \pmod{4},
\[
\begin{cases}
p^2 m - 1 + p^{m - 1} & \text{if } p \equiv 3 \pmod{4} \text{ and } d \text{ is odd}, \\
p^2 m - 1 - p^{m - 1} & \text{otherwise}.
\end{cases}
\]
If \( \frac{m}{d} \equiv 0 \pmod{4}, \)
\[
n_2 = p^{2 m - 1} - p^{m + d - 1}.
\]

**Proof:** By the orthogonal property of additive characters,
\[
n_2 = \sum_{x, y \in \mathbb{F}_q} \sum_{z_1 \in \mathbb{F}_p} \zeta_p(z_1) \left( \sum_{y' \in \mathbb{F}_p} \zeta_p^{-z_1} Q(z_1 , 0) S_a (z_1 , 0) \right)
\]
\[
= \frac{1}{p} \left( \sum_{z_1 \in \mathbb{F}_p} \zeta_p^{-z_1} Q(z_1 , 0) S_a (z_1 , 0) \right)
\]
\[
= p^{2 m - 1} + \frac{1}{p} \Omega_1,
\]
where \( \Omega_1 = \sum_{z_1 \in \mathbb{F}_p} \zeta_p^{-z_1} Q(z_1 , 0) S_a (z_1 , 0). \) Then we evaluate \( \Omega_1 \) through the following three cases.

(i) If \( \frac{m}{d} \) is odd, by Lemma 1
\[
G(\eta)^2 = \left( p^s \right)^m
\]
\[
= \begin{cases} 
p^m, & \text{if } p \equiv 3 \pmod{4} \text{ and } d \text{ is odd}, \\
-p^m, & \text{otherwise}.
\end{cases}
\]
From Lemmas 2 and 7
\[
\Omega_1 = \sum_{z_1 \in \mathbb{F}_p} \frac{G(\eta)^2 \eta(z_1)^2 \zeta_p^{-z_1}}{\zeta_p} = \sum_{z_1 \in \mathbb{F}_p} \frac{G(\eta)^2 \eta(z_1) \zeta_p^{-z_1}}{\zeta_p}
\]
\[
= \begin{cases} 
p^m, & \text{if } p \equiv 3 \pmod{4} \text{ and } d \text{ is odd}, \\
-p^m, & \text{otherwise}.
\end{cases}
\]
(ii) If \( \frac{m}{d} \equiv 2 \pmod{4}, \) by Lemma 1
\[
G(\eta) = -(p^s)^s
\]
\[
= \begin{cases} 
p^s, & \text{if } p \equiv 3 \pmod{4} \text{ and } d \text{ is odd}, \\
-p^s, & \text{otherwise}.
\end{cases}
\]
From Lemmas 3, 7 and 9
\[
\Omega_1 = -p^s G(\eta) \sum_{z_1 \in \mathbb{F}_p} \eta(z_1) \zeta_p^{-z_1} = p^s G(\eta)
\]
\[
= \begin{cases} 
p^m, & \text{if } p \equiv 3 \pmod{4} \text{ and } d \text{ is odd}, \\
-p^m, & \text{otherwise}.
\end{cases}
\]
(iii) If \( \frac{m}{d} \equiv 0 \pmod{4}, \) by Lemma 1
\[
G(\eta) = -p^s
\]
and from Lemmas 3, 7 and 9
\[
\Omega_1 = -p^{s + d} G(\eta) \sum_{z_1 \in \mathbb{F}_p} \eta(z_1) \zeta_p^{-z_1}
\]
\[
= p^{s + d} G(\eta) = -p^{m + d}.
\]
By above all we complete the proof.

**Lemma 11:** If \( m \) is odd, then
\[
B_1 = \left\{ x \in \mathbb{F}_q : \operatorname{Tr}(x^{m + 1}) = -1 \right\}
\]
\[
= \begin{cases} 
p^{m - 1} - p^{m + 1}, & \text{if } p \equiv 3 \pmod{4} \text{ and } \frac{m + 1}{2} \text{ is odd}, \\
p^{m - 1} + p^{m + 1}, & \text{otherwise}.
\end{cases}
\]

**Proof:** By Lemma 1
\[
G(\eta) G(\eta) = (p^s)^{m + 1}.
\]

**Through Lemma 2 and (5)**
\[
B_1 = \left\{ x \in \mathbb{F}_q : \frac{1}{p} \left( \sum_{z_1 \in \mathbb{F}_p} \sum_{z_1 \in \mathbb{F}_p} \eta(z_1) \zeta_p^{-z_1} \right) \right\}
\]
\[
= \frac{1}{p} \left( \sum_{z_1 \in \mathbb{F}_p} \eta(z_1) \zeta_p^{-z_1} \right)
\]
\[
= p^{m - 1} + \frac{1}{p} G(\eta) G(\eta)
\]
\[
= p^{m - 1} - p^{m + 1},
\]
\[
= \begin{cases} 
p^{m - 1} - p^{m + 1}, & \text{if } p \equiv 3 \pmod{4} \text{ and } \frac{m + 1}{2} \text{ is odd}, \\
p^{m - 1} + p^{m + 1}, & \text{otherwise}.
\end{cases}
\]

**A. THE PROOFS OF THEOREMS 2.1, 2.4, 2.7 AND 2.9**
By Lemma 8 the code \( C_{D_1} \) has length \( n_1 = p^{2 m - 1} \). For a codeword \( C(a, b) = (\operatorname{Tr}(ax + by))_{(x, y) \in D_1} \) \( (a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} \), we will show that the Hamming weight of the codeword \( C(a, b) \) satisfies \( W_H(C(a, b)) > 0 \), so the dimension of \( C_{D_1} \) is \( 2m \). We start with the following equation:
\[
x^{p^{2 m}} + x = (a^{-1} b)^p.
\]

By Lemmas 4 and 12, if \( \frac{m}{d} \equiv 0 \pmod{4}, \) either the equation is not solvable over \( \mathbb{F}_q \) or it is solvable and has a unique solution. Let \( y_{a,b} \) be some solution of (6) if it exists. Note that for \( a, b \in \mathbb{F}_q \), the equation \( (a^{-1} b)^p + z_2 a x = (a b)^p \) is equivalent to (6). For \( (a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} \), we consider
\[
N_1(a, b) = \left\{ (x, y) \in \mathbb{F}_q^2 : \operatorname{Tr}(x + y^{p + 1}) = 1 \text{ and } \operatorname{Tr}(ax + by) = 0 \right\}
\]
\[
= \sum_{x, y \in \mathbb{F}_q} \sum_{z_1 \in \mathbb{F}_p} \left( \frac{1}{p} \sum_{z_1 \in \mathbb{F}_p} \left( \frac{1}{p} \sum_{z_2 \in \mathbb{F}_p} \zeta_{z_2} \operatorname{Tr}(x + y^{p + 1}) \right) \right)
\]
\[
\times \left( \frac{1}{p} \sum_{z_2 \in \mathbb{F}_p} \zeta_{z_2} \operatorname{Tr}(ax + by) \right).
\]
\[
\begin{align*}
&= \frac{1}{p^2} \sum_{x,y \in \mathbb{F}_q} \left( 1 + \sum_{z \in \mathbb{F}_p^*} \zeta_p^{z (x+y^{p^m-1}) - z^*} \right) \\
&\times \left( 1 + \sum_{z \in \mathbb{F}_p^*} \zeta_p^{z (x+y^b)} \right) \\
&= p^{2m-2} + \frac{1}{p^2} \left( \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{z_1} \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \zeta_p^{z_1 x} S_a(z_1,0) \right) \\
&+ \sum_{z \in \mathbb{F}_p^*} \xi_p^{z_1} \sum_{x \in \mathbb{F}_q} \zeta_p^{z_1 z_2 (x+y^b)} S_a(z_1,z_2b) \\
&= p^{2m-2} + \frac{1}{p^2} \sum_{z_1,z_2 \in \mathbb{F}_p^*} \xi_p^{z_1} \sum_{x \in \mathbb{F}_q} \zeta_p^{z_1 z_2 (x+y^b)} S_a(z_1,z_2b) \\
&= \begin{cases} 
p^m - 1, & \text{if } a \not\in \mathbb{F}_p^* \\
p^2 - p^m + p^{m-2} \Omega_2, & \text{if } a \in \mathbb{F}_p^* 
\end{cases}
\end{align*}
\]

where
\[
\Omega_2 = \sum_{z \in \mathbb{F}_p^*} \xi_p^{z_2} S_a(-z_2a,z_2b).
\]

It is clear that the Hamming weight of the codeword \( \mathcal{C}(a,b) \) is
\[
W_2(\mathcal{C}(a,b)) = n_1 - N_1(a,b).
\]

If \( m \) is odd, by Lemma 5
\[
\Omega_2 = G(\eta) \sum_{z \in \mathbb{F}_p^*} \eta_p(-z_2a) z_2 a (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} \\
= G(\eta) \sum_{z \in \mathbb{F}_p^*} \eta_p(-z_2a) z_2 a (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} \\
= G(\eta) \sum_{z \in \mathbb{F}_p^*} \eta_p(-z_2a) \xi_p^{z_2a} (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} \\
= \begin{cases} 
0, & \text{if } \gamma_{a,b}^{p^m+1} = -1 \\
G(\eta) G(\eta_p) \eta_p(-\gamma_{a,b}^{p^m+1}) - 1, & \text{if } \gamma_{a,b}^{p^m+1} \neq -1. \end{cases}
\]

By (5), (7), (8) and (9) we know that the three nonzero weights of \( \mathcal{C}_D \) are
\[
w_1 = (p-1)p^{2m-2}, \\
w_2 = (p-1)p^{2m-2} - p^{\frac{m+1}{2}}, \\
w_3 = (p-1)p^{2m-2} + p^{\frac{m+1}{2}}.
\]

From Lemma 11,
\[
A_{w_2} + A_{w_3} = |\{(a, b) \in \mathbb{F}_q^2 : a \in \mathbb{F}_p^* \text{ and } \text{Tr}(\gamma_{a,b}^{p^m+1}) \neq -1\}| \\
= \begin{cases} 
(p-1)(p^m - p^{m-1} + p^{\frac{m+1}{2}}), & \text{if } p \equiv 3 \pmod{4} \text{ and } \frac{m+1}{2} \text{ is odd}, \\
(p-1)(p^m - p^{m-1} - p^{\frac{m+1}{2}}), & \text{otherwise.} \end{cases}
\]

And by the first two Pless power moments we can obtain the multiplicities of the three nonzero weights of \( \mathcal{C}_D \). Through the above, we complete the proof of Theorem 1.

If \( \frac{d}{2} \) is odd and \( d \) is even, by Lemma 5
\[
\Omega_2 = G(\eta) \sum_{z \in \mathbb{F}_p^*} \eta_p(-z_2a) z_2 a (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} \\
= G(\eta) \sum_{z \in \mathbb{F}_p^*} \eta_p(-z_2a) (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} + \eta_p(-z_2a) (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} \\
= \begin{cases} 
(p-1)G(\eta), & \text{if } \gamma_{a,b}^{p^m+1} = -1, \\
-G(\eta), & \text{if } \gamma_{a,b}^{p^m+1} \neq -1. \end{cases}
\]

From Lemma 1,
\[
G(\eta) = \begin{cases} 
p^s, & \text{if } p \equiv 3 \pmod{4} \text{ and } s \text{ is odd,} \\
-p^s, & \text{otherwise.} \end{cases}
\]

And by (7), (8) and (10) we know that the three nonzero weights of \( \mathcal{C}_D \) are
\[
w_1 = (p-1)p^{2m-2}, \\
w_2 = (p-1)(p^{2m-2} - p^{m-2}G(\eta)) \\
= \begin{cases} 
(p-1)(p^{2m-2} - p^{\frac{3m-2}{2}}), & \text{if } p \equiv 3 \pmod{4} \text{ and } s \text{ is odd,} \\
(p-1)(p^{2m-2} - p^{\frac{3m-2}{2}}), & \text{otherwise.} \end{cases}
\]
\[
w_3 = (p-1)p^{2m-2} + p^{m-2}G(\eta) \\
= \begin{cases} 
(p-1)p^{2m-2} + p^{\frac{3m-2}{2}}, & \text{if } p \equiv 3 \pmod{4} \text{ and } s \text{ is odd,} \\
(p-1)p^{2m-2} - p^{\frac{3m-2}{2}}, & \text{otherwise.} \end{cases}
\]

Note that
\[
A_{w_2} + A_{w_3} = |\{(a, b) \in \mathbb{F}_q^2 : a \in \mathbb{F}_p^* \}| = (p-1)p^m.
\]

We get the multiplicities of the three nonzero weights of \( \mathcal{C}_D \) from the first two Pless power moments. Through the above, we complete the proof of Theorem 2.

If \( \frac{d}{2} \equiv 2 \pmod{4} \), by Lemma 5
\[
\Omega_2 = -p^s \sum_{z \in \mathbb{F}_p^*} \eta_p(-z_2a) z_2 a (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} \\
= -p^s \sum_{z \in \mathbb{F}_p^*} \xi_p^{z_2a} (\gamma_{a,b}^{p^m+1}) \xi_p^{z_2a} \\
= \begin{cases} 
-(p-1)p^s, & \text{if } \gamma_{a,b}^{p^m+1} = -1, \\
p^s, & \text{if } \gamma_{a,b}^{p^m+1} \neq -1. \end{cases}
\]
By (7), (8) and (11) we know that the three nonzero weights of $C_{D_1}$ are

$$w_1 = (p - 1)p^{2m-2},$$
$$w_2 = (p - 1)(p^{2m-2} + p^{\frac{3m+2d-4}{2}}),$$
$$w_3 = (p - 1)p^{2m-2} - p^{\frac{3m+2d-4}{2}}.$$

Again

$$A_{w_2} + A_{w_3} = |\{(a, b) \in \mathbb{F}_q^2 : a \in \mathbb{F}_q^* \}| = (p - 1)p^m.$$

Solving the equations from the first two Pless power moments gives us the multiplicities of the three nonzero weights of $C_{D_1}$. Through the above, we complete the proof of Theorem 3.

If $\frac{q}{2} \equiv 0 \pmod{4}$, by Lemma 6, if (6) is not solvable over $\mathbb{F}_q$

$$\Omega_2 = 0$$

and if (6) is solvable over $\mathbb{F}_q$

$$\Omega_2 = -p^{s+d} \sum_{z \in \mathbb{F}_p^*} \left( -z^2 \alpha_{a,b} \gamma^{p^{s+1}} \right) \zeta_p^z a$$

$$= -p^{s+d} \sum_{z \in \mathbb{F}_p^*} \zeta_p^z \left( \text{Tr}(\gamma^{p^s+1}) + 1 \right)$$

where

$$\Omega_2 = \sum_{z \in \mathbb{F}_p^*} \zeta_p^{z-1} Q(z_1, 0) S_u(z_1, 0)$$

and

$$\Omega_3 = \sum_{z \in \mathbb{F}_p^*} \zeta_p^{z-1} \gamma(z_1, z_2) S_u(z_1, z_2) \zeta_p^{z-1}.$$

Note that we have already discussed $\Omega_1$ in Lemma 10. Let $\gamma_b \in \mathbb{F}_q$ be some solution of the equation

$$x^{p^{2n}} + x = -b^{p^n}$$

if it exists, then for $z_1, z_2 \in \mathbb{F}_q^*$, $z_3 \gamma_b$ is the solution of $z_1^2 x^{p^{2n}} + z_1 x = -(z_2 b) \gamma_b$, where $z_3 = z_1^{-1} z_2$.

By Lemmas 5 and 7, if $\frac{q}{2} \equiv 0$, we have

$$\Omega_1 = (p - 1) \eta(\gamma_b) q \zeta_p^{z-1} Q(z_1, 0) S_u(z_1, 0)$$

and

$$\Omega_3 = (p - 1) \eta(\gamma_b) \gamma(z_1, z_2) S_u(z_1, z_2) \zeta_p^{z-1}.$$

If $\text{Tr}(\frac{q}{2} + y_b^{p^{m+1}}) \neq 0$,

$$\Omega_3 = (p - 1) \eta(\gamma_b) \gamma(z_1, z_2) S_u(z_1, z_2) \zeta_p^{z-1}.$$

If $\text{Tr}(\frac{q}{2} + y_b^{p^{m+1}}) = 0$,

$$\Omega_3 = (p - 1) \eta(\gamma_b) \gamma(z_1, z_2) S_u(z_1, z_2) \zeta_p^{z-1}.$$
By Lemma 1, (18) and (19) we get the following results.
(i) If $\frac{m}{d}$ is odd, $p \equiv 3 \pmod{4}$ and $d$ is odd,

$$\Omega_3 = \begin{cases} 
-(p+1)^m, \\
(p+1)^m, \\
(p-1)^m, \\
(p-1)^m, \\
(p-1)^m.
\end{cases}$$

(ii) If $\frac{m}{d}$ is odd and $p$, $d$ satisfy the condition except that in (i),

$$\Omega_3 = \begin{cases} 
-(p+1)^m, \\
(p+1)^m, \\
(p-1)^m. \\
\end{cases}$$

Through Lemma 10, we have that the two nonzero weights of $C_{D_2}$

$$w_1 = (p-1)^{2m-2},$$

$$w_2 = (p-1)^{2m-2} + 2p^{m-1}.$$

We can obtain the multiplicities of the two nonzero weights of $C_{D_2}$

From the first two Pless power moments.

We note that $\Omega_3$ is the same as (20) and (21) in the previous condition. Through the above, we complete the proof of Theorem 5.

Let $\frac{m}{d} \equiv 0 \pmod{4}$, by Lemmas 1, 6 and 7, if (17) is not solvable over $\mathbb{F}_q$,

$$\Omega_3 = 0$$

and if (17) is solvable over $\mathbb{F}_q$,

$$\Omega_3 = -p^{s+d} G(\eta) \times \sum_{z_1 \in \mathbb{F}_q^*} \sum_{z_3 \in \mathbb{F}_q^*} \sum_{z_2 \in \mathbb{F}_q^*} (21)$$

By (4), (14), (15), (16), (22) and (23) we know that the three nonzero weights of $C_{D_2}$ are

$$w_1 = (p-1)^{2m-2},$$

$$w_2 = (p-1)^{2m-2} - 2p^{m-1}.$$
based on the dual code $C^\perp$ corresponding to the minimal codewords in $C$ may have nice access structure [5], [8], [9], [35]. The question now is how to construct such a linear code. The following lemma provides an approach [9].

**Lemma 13:** [9, Lemma 13] Every nonzero codeword of a linear code $C$ over $\mathbb{F}_p$ is minimal provided that

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p},$$

where $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero weights in code $C$, respectively.

**A. MINIMAL CODEWORDS IN $C_{D_1}$**

If $m \equiv 0 \pmod{4}$, by Theorem 4 and Lemma 13 we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-d}-1}{(p-1)p^{m-d}+p-1} > \frac{p-1}{p}$$

if $m-2d \geq 4$.

Otherwise, by Theorems 1, 2, 3 and Lemma 13 we have

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$$

if $m \geq 4$.

Then we know that each nonzero codeword of $C_{D_1}$ is minimal if $m \geq \max\{4, 4+2d\}$.

**B. MINIMAL CODEWORDS IN $C_{D_2}$**

Let $\frac{m}{d}$ be odd or $\frac{m}{d} \equiv 2 \pmod{4}$. By Theorem 5 and Lemma 13 we have

$$\frac{w_{\min}}{w_{\max}} = \frac{(p-1)p^{m-1}-2}{(p-1)p^{m-1}+2} > \frac{p-1}{p}$$

if $m \geq 2$.

Let $m \equiv 0 \pmod{4}$. By Theorem 6 and Lemma 13 we have

$$\frac{w_{\min}}{w_{\max}} = \frac{1-2}{(p-1)p^{m-d}} > \frac{p-1}{p}$$

if $m-d \geq 1$.

Then we know that each nonzero codeword of $C_{D_2}$ is minimal if $m \geq \max\{2, 1+d\}$.

By above all we conclude that all the nonzero codewords of $C_{D_1}$ and $C_{D_2}$ are minimal. Therefore, we can construct secret sharing schemes based on the dual codes with nice access structures.

**VI. CONCLUSION**

In this article, inspired by the work in [16], two classes of linear codes were constructed based on Weil sums and their weight distributions were presented explicitly. Some of the almost optimal linear codes were found with respect to the Griesmer bound. We also showed that every nonzero codeword of $C_{D_1}$ and $C_{D_2}$ is minimal.

**REFERENCES**

[1] A. R. Calderbank and J. M. Goethals, “Three-weight codes and association schemes,” *Philips J. Res.*, vol. 39, nos. 4–5, pp. 143–152, 1984.

[2] R. Calderbank and W. M. Kantor, “The geometry of two-weight codes,” *Bull. London Math. Soc.*, vol. 18, no. 2, pp. 97–122, Mar. 1986.

[3] R. Coulter, “Explicit evaluations of some Weil sums,” *Acta Arithmetica*, vol. 83, no. 3, pp. 241–251, 1998.

[4] R. Coulter, “Further evaluations of Weil sums,” *Acta Arithmetica*, vol. 86, no. 3, pp. 217–226, 1998.

[5] C. Carlet, C. Ding, and J. Yuan, “Linear codes from perfect nonlinear mappings and their secret sharing schemes,” *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2089–2102, Jun. 2005.

[6] C. Ding and X. Wang, “A coding theory construction of new systematic authentication codes,” *Theor. Comput. Sci.*, vol. 330, no. 1, pp. 81–99, Jan. 2005.

[7] C. Ding and H. Niederreiter, “Cyclotomic linear codes of order 3,” *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2274–2277, Jun. 2007.

[8] C. Ding and J. Yuan, “Covering and secret sharing with linear codes,” in *Discrete Mathematics and Theoretical Computer Science* ( Lecture Notes in Computer Science), vol. 2731. Berlin, Germany: Springer, Jun. 2003, pp. 11–25.

[9] K. Ding and C. Ding, “A class of two-weight and three-weight codes and their applications in secret sharing,” *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5835–5842, Nov. 2015.

[10] J. H. Griesmer, “A bound for error-correcting codes,” *IBM J. Res. Develop.*, vol. 4, no. 5, pp. 532–542, Nov. 1960.

[11] Z. Heng, C. Ding, and Z. Zhou, “Minimal linear codes over finite fields,” *Finite Fields Their Appl.*, vol. 54, pp. 176–196, Nov. 2018.

[12] Z. Heng, W. Wang, and Y. Wang, “Projective binary linear codes from special Boolean functions,” *Applicable Algebra Eng., Commun. Comput.*, vol. 2, pp. 1–32, Jan. 2020.

[13] Z. Heng and Q. Yue, “Two classes of two-weight linear codes,” *Finite Fields Their Appl.*, vol. 38, pp. 72–92, Mar. 2016.

[14] Z. Heng and Q. Yue, “A construction of q-ary linear codes with two weights,” *Finite Fields Their Appl.*, vol. 48, pp. 20–42, Nov. 2017.

[15] W. C. Huffman and V. Pless, *Fundamentals Error-Correcting Codes*. New York, NY, USA: Cambridge Univ. Press, 2010.

[16] G. Jian, Z. Lin, and R. Feng, “Two-weight and three-weight linear codes based on Weil sums,” *Finite Fields Appl.*, vol. 57, pp. 92–107, May 2019.

[17] X. Kong and S. Yang, “A class of linear codes and their complete weight enumerators,” *IEEE Access*, vol. 7, pp. 127833–127838, 2019.

[18] X. Kong and S. Yang, “Complete weight enumerators of a class of linear codes with two or three weights,” *Discrete Math.*, vol. 342, no. 11, pp. 3166–3176, Nov. 2019.

[19] C. Li, S. Bae, and S. Yang, “Some two-weight and three-weight linear codes,” *Adv. Math. Commun.*, vol. 13, no. 1, pp. 195–211, Feb. 2019.

[20] C. Li, Q. Yue, and F. Li, “Hamming weights of the duals of cyclic codes with two zeros,” *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 3895–3902, Jul. 2014.

[21] C. Li, Q. Yue, and F.-W. Fu, “A construction of several classes of two-weight and three-weight linear codes,” *Appl. Algebra Eng., Commun. Comput.*, vol. 28, no. 1, pp. 11–30, Jan. 2017.

[22] G. Luo, X. Cao, S. Xu, and J. Mi, “Binary linear codes with two or three weights from nilo exponents,” *Cryptograph. Commun.*, vol. 10, no. 2, pp. 301–318, Mar. 2018.

[23] R. Lidl and H. Niederreiter, *Finite Fields*. New York, NY, USA: Cambridge Univ. Press, 1997.

[24] S. Mesnager, F. Özbudak, and A. Sänak, “Linear codes from weakly regular plateaued functions and their secret sharing schemes,” *Des., Codes Cryptograph.*, vol. 87, nos. 2–3, pp. 463–480, Mar. 2019.

[25] D. R. Stinson, *An explication of secret sharing schemes,* *Des., Codes Cryptograph.*, vol. 2, no. 4, pp. 357–390, Dec. 1992.

[26] K. See and S. Y. Song, “Association schemes of small order,” *J. Stat. Planning Inference*, vol. 73, nos. 1–2, pp. 225–271, Sep. 1998.

[27] K. Torleiv, *Codes for Error Detection*. Singapore: World Scientific, 2007.

[28] Y. Wu and Q. Yue, “Factorizations of binomial polynomials and enumerations of LCD and self-dual constacyclic codes,” *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1740–1751, Mar. 2019.

[29] Y. Wu and Q. Yue, “Factorizations of binomial polynomials and enumerations of LCD and self-dual constacyclic codes,” *Adv. Math. Commun.*, vol. 13, no. 1, pp. 227–271, Jan. 2019.

[30] S. Yang, Z.-A. Yao, and C.-A. Zhao, “The weight enumerator of the duals of a class of cyclic codes with three zeros,” *Applicable Algebra Eng., Commun. Comput.*, vol. 26, no. 4, pp. 347–367, Mar. 2015.
[31] S. Yang, Z.-A. Yao, and C.-A. Zhao, “The weight distributions of two classes of \(p\)-ary cyclic codes with few weights,” *Finite Fields Appl.*, vol. 44, pp. 76–91, Mar. 2017.

[32] S. Yang, X. Kong, and C. Tang, “A construction of linear codes and their complete weight enumerators,” *Finite Fields Their Appl.*, vol. 48, pp. 196–226, Nov. 2017.

[33] S. Yang and Z.-A. Yao, “Complete weight enumerators of a class of linear codes,” *Discrete Math.*, vol. 340, no. 4, pp. 729–739, Apr. 2017.

[34] S. Yang, X. Kong, and X. Shi, “Complete weight enumerators of a class of linear codes over finite fields,” *Adv. Math. Commun.*, Apr. 2019, doi: 10.3934/amc.2020045.

[35] 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, Jan. 2006.

HONG LU received the B.S. degree in mathematics from Qufu Normal University, Shandong, China, in 2019, where she is currently pursuing the master’s degree in exponential sums and coding theory.

SHUDI YANG received the Ph.D. degree in mathematics from Sun Yat-sen University, Guangzhou, China, in 2016. From August 2016 to January 2019, she was a Postdoctoral Researcher with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. She is currently an Associate Professor with Qufu Normal University, China. Her research interests include exponential sums and coding theory.

**IEEE Access**

VOLUME 8, 2020