

Complete Weight Enumerators of a Class of Linear Codes From Weil Sums

SHUDI YANG 

School of Mathematical Sciences, Qufu Normal University, Jining 273165, China
e-mail: yangshudi@qfnu.edu.cn

This work was supported in part by the National Natural Science Foundation of China under Grant 12071247 and Grant 11701317.

ABSTRACT By appropriately choosing a defining set, we define a class of linear codes and determine their complete weight enumerators and weight enumerators using Weil sums. They only have two or three nonzero weights, and some of them are optimal with respect to the Griesmer bound or Markus Grassl's code tables. So they are suitable for applications in strongly regular graphs and secret sharing schemes.

INDEX TERMS Linear code, complete weight enumerator, Weil sum, weight enumerator.

I. INTRODUCTION


Throughout this article, we let p be an odd prime and \mathbb{F}_p the finite field with p elements. We introduce some basic concept on coding theory. An $[n, k, d]$ linear code \mathcal{C} over \mathbb{F}_p is a k -dimensional subspace of \mathbb{F}_p^n with minimum distance d . For a codeword $\mathbf{c} \in \mathcal{C}$ the Hamming weight $wt(\mathbf{c})$ is the number of nonzero coordinates in \mathbf{c} . Let A_i be the number of codewords with weight i . The polynomial $1 + A_1z + A_2z^2 + \dots + A_nz^n$ is referred as the weight enumerator of \mathcal{C} . The complete weight enumerator of a code \mathcal{C} over \mathbb{F}_p enumerates the codewords according to the number of symbols of each kind contained in each codeword. Write $\mathbb{F}_p = \{w_0 = 0, w_1, \dots, w_{p-1}\}$. For a codeword $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_p^n$, let $w[\mathbf{c}]$ be the complete weight enumerator of \mathbf{c} , which is defined as

$$w[\mathbf{c}] = w_0^{k_0} w_1^{k_1} \dots w_{p-1}^{k_{p-1}},$$

where k_j is the number of components of \mathbf{c} equal to w_j , $\sum_{j=0}^{p-1} k_j = n$. The complete weight enumerator of the code \mathcal{C} is then

$$\text{CWE}(\mathcal{C}) = \sum_{\mathbf{c} \in \mathcal{C}} w[\mathbf{c}].$$

It is well known that the complete weight enumerator gives the weight enumerator of a code. They contain important information which allows the computation of the error probability of error detection and correction with respect to some algorithms. They also have many applications in the areas of the deception probabilities of certain authentication codes [9].

The associate editor coordinating the review of this manuscript and approving it for publication was Keivan Navaei .

the constructions of optimal constant composition codes [8] and the computation of Walsh transform of monomial and quadratic bent functions over finite fields [13]. It is interesting to determine the complete weight enumerators and weight enumerators of linear codes. Recently, much attention has been paid to linear codes with few weights [1], [2], [5], [14], [16], [20], [22], [24]–[26], [30] due to their applications in strongly regular graphy [3] and cryptography [4], [29].

Now we introduce a generic construction of linear codes initiated by Ding *et al.* [10], [11]. Let $D = \{d_1, d_2, \dots, d_n\}$ be a subset of \mathbb{F}_q , where $q = p^m$ for an integer $m > 1$. Denote by Tr the absolute trace function from \mathbb{F}_q to \mathbb{F}_p . A linear code of length n is defined by

$$\mathcal{C}_D = \{(\text{Tr}(bd_1), \text{Tr}(bd_2), \dots, \text{Tr}(bd_n)) : b \in \mathbb{F}_q\}.$$

The set D is called the defining set. Many classes of linear codes were produced in this way, such as [1], [12], [15], [18], [19], [23], [27], [28]. Particularly, Kong and Yang [18] constructed some linear codes with two or three weights and presented their complete weight enumerators, by choosing $D = \{x \in \mathbb{F}_q^* : \text{Tr}(ax^{p^m+1}) = c\}$, where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, u is a positive integer, $a \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_p$. If we take $a = 1$ and $c = 0$, it is the case considered in [23]. In [12], [20], the authors investigated several classes of linear codes, which can be viewed as a generalization of cyclic codes whose duals have two zeros.

Throughout the paper, we let $\alpha, \beta \in \mathbb{F}_q^*$, m and u be positive integers and $q = p^m$. The purpose of this article is to study the complete weight enumerators of linear codes \mathcal{C}_{D_c} for $c \in \mathbb{F}_p$, defined as follows:

$$\mathcal{C}_{D_c} = \{\mathbf{c}(a, b) : a, b \in \mathbb{F}_q\}, \quad (1)$$

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

$$D_c = \{(x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} : \text{Tr}(\alpha x^2 + \beta y^{u+1}) = c\}. \quad (2)$$

We call D_c the defining set of \mathcal{C}_{D_c} . This is an extension for the work in [12], [18], [20], [23]. When $\alpha = t = 1$, the weight distribution of \mathcal{C}_{D_0} is determined in [12]. In this article, by employing Weil sums, we shall illustrate explicitly the complete weight enumerators of \mathcal{C}_{D_c} for all $c \in \mathbb{F}_p$. These linear codes are minimal with at most three weights and can be utilized to construct secret sharing schemes with good access structures.

Now we present the main results of this article and indicate their proofs in Section III. Let η (resp. η_p) be the quadratic character of \mathbb{F}_q (resp. \mathbb{F}_p). Denote $v = \text{gcd}(m, u)$. When m is even, we write $m = 2k$ for an integer k and define $s = k/v$. The complete weight enumerator of \mathcal{C}_{D_0} is given in the following three theorems.

Theorem 1: Let \mathcal{C}_{D_0} be defined by (1) and (2). If m/v is odd, the code \mathcal{C}_{D_0} is an $[n_0 - 1, 2m]$ two-weight linear code, where

$$n_0 = p^{2m-1} + \varepsilon_1(p-1)p^{m-1},$$

and ε_1 is defined by

$$\varepsilon_1 = \begin{cases} -\eta(\alpha\beta) & \text{if } p^v \equiv 3 \pmod{4}, \\ \eta(\alpha\beta) & \text{otherwise.} \end{cases} \quad (3)$$

The weight enumerator of \mathcal{C}_{D_0} is

$$1 + (n_0 - 1)z^{(p-1)p^{2m-2}} + (p^{2m} - n_0)z^{(p-1)p^{m-1}(p^{m-1} + \varepsilon_1)},$$

and the complete weight enumerator is

$$w_0^{n_0-1} + (n_0 - 1)w_0^{n_0-1-(p-1)p^{2m-2}} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{2m-2} + (p^{2m} - n_0)w_0^{p^{2m-2}-1} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{p^{m-1}(p^{m-1} + \varepsilon_1)}.$$

Theorem 2: If m/v is even and $\beta^{q-1} \neq (-1)^s$, then \mathcal{C}_{D_0} is an $[n_0 - 1, 2m]$ two-weight linear code, where

$$n_0 = p^{2m-1} + \varepsilon_2(p-1)p^{m-1}$$

and

$$\varepsilon_2 = \begin{cases} (-1)^s \eta(\alpha) & \text{if } p^k \equiv 3 \pmod{4}, \\ -(-1)^s \eta(\alpha) & \text{otherwise.} \end{cases} \quad (4)$$

Its weight enumerator is

$$1 + (n_0 - 1)z^{(p-1)p^{2m-2}} + (p^{2m} - n_0)z^{(p-1)p^{m-1}(p^{m-1} + \varepsilon_2)},$$

and its complete weight enumerator is

$$w_0^{n_0-1} + (n_0 - 1)w_0^{n_0-1-(p-1)p^{2m-2}} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{2m-2}$$

$$+ (p^{2m} - n_0)w_0^{p^{2m-2}-1} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{p^{m-1}(p^{m-1} + \varepsilon_2)}.$$

Theorem 3: If m/v is even and $\beta^{q-1} = (-1)^s$, then \mathcal{C}_{D_0} is an $[n_0 - 1, 2m,]$ three-weight linear code, where

$$n_0 = p^{2m-1} - \varepsilon_2(p-1)p^{m+v-1},$$

and ε_2 is given by (4). Define

$$\begin{aligned} F_1 &= (p^{m-v-1} - \varepsilon_2)(p^{m-v} + \varepsilon_2), \\ F_2 &= (p-1)p^{m-v-1}(p^{m-v} + \varepsilon_2), \\ F_3 &= p^{2m} - p^{2m-2v}. \end{aligned}$$

Its weight enumerator is

$$1 + F_1 z^{(p-1)p^{2m-2}} + F_2 z^{(p-1)p^{m-1}(p^{m-1} - \varepsilon_2 p^v)} + F_3 z^{(p-1)p^{m-2}(p^m - \varepsilon_2(p-1)p^v)},$$

and its complete weight enumerator is

$$\begin{aligned} w_0^{n_0-1} + F_1 w_0^{n_0-1-(p-1)p^{2m-2}} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{2m-2} \\ + F_2 w_0^{p^{2m-2}-1} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{p^{m-1}(p^{m-1} - \varepsilon_2 p^v)} \\ + F_3 w_0^{p^{2m-2}-1-\varepsilon_2(p-1)p^{m+v-2}} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{p^{m-2}(p^m - \varepsilon_2(p-1)p^v)}. \end{aligned}$$

Remark 1: Note that $\text{Tr}(\alpha x^2 + \beta y^{u+1}) = 0$ for all $a \in \mathbb{F}_p^*$ if $\text{Tr}(\alpha x^2 + \beta y^{u+1}) = 0$. So we can select a subset \bar{D}_0 of D_0 such that $\cup_{a \in \mathbb{F}_p^*} a\bar{D}_0$ is a partition of D_0 . The new code $\mathcal{C}_{\bar{D}_0}$ is a punctured version of the original code \mathcal{C}_{D_0} . Actually, the weights of the punctured code are obtained from the original code by dividing the common divisor $p-1$.

The following theorems show the complete weight enumerators and weight enumerators of \mathcal{C}_{D_c} for $c \neq 0$.

Theorem 4: Let g be a generator of \mathbb{F}_p^* and $c \in \mathbb{F}_p^*$. If m/v is odd, then \mathcal{C}_{D_c} is an $[n_c, 2m]$ two-weight linear code, where

$$n_c = p^{2m-1} - \varepsilon_1 p^{m-1},$$

and ε_1 is given in (3). Its weight enumerator is

$$1 + (p^{2m} - 1 - \frac{p-1}{2} n_c) z^{(p-1)p^{2m-2}} + \frac{p-1}{2} n_c z^{p^{m-1}((p-1)p^{m-1} - 2\varepsilon_1)},$$

and its complete weight enumerator is

$$\begin{aligned} w_0^{n_c} + (p^m - \varepsilon_1)(p^{m-1} + \varepsilon_1)w_0^{p^{m-1}(p^{m-1} - \varepsilon_1)} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{2m-2} \\ + n_c \sum_{t=1}^{\frac{p-1}{2}} \prod_{\rho \in \mathbb{F}_p} w_\rho^{p^{m-1}(p^{m-1} + \varepsilon_1) \eta_\rho(\rho^2 - g^{2t})} \\ + n_c \sum_{t=1}^{\frac{p-1}{2}} \prod_{\rho \in \mathbb{F}_p} w_\rho^{p^{m-1}(p^{m-1} + \varepsilon_1) \eta_\rho(\rho^2 - g^{2t+1})}. \end{aligned}$$

Theorem 5: Let g be a generator of \mathbb{F}_p^* and $c \in \mathbb{F}_p^*$. If m/v is even and $\beta^{\frac{q-1}{p^{v+1}}} \neq (-1)^s$, then \mathcal{C}_{D_c} is an $[n_c, 2m]$ two-weight linear code, where

$$n_c = p^{2m-1} - \varepsilon_2 p^{m-1},$$

and ε_2 is given in (4). Its weight enumerator is

$$1 + (p^{2m} - 1 - \frac{p-1}{2} n_c) z^{(p-1)p^{2m-2}} + \frac{p-1}{2} n_c z^{p^{m-1}((p-1)p^{m-1} - 2\varepsilon_2)},$$

and its complete weight enumerator is

$$w_0^{n_c} + (p^m - \varepsilon_2)(p^{m-1} + \varepsilon_2) w_0^{p^{m-1}(p^{m-1} - \varepsilon_2)} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{p^{2m-2}} + n_c \sum_{t=1}^{\frac{p-1}{2}} \prod_{\rho \in \mathbb{F}_p} w_\rho^{p^{m-1}(p^{m-1} + \varepsilon_2 \eta_\rho(\rho^2 - g^{2t}))} + n_c \sum_{t=1}^{\frac{p-1}{2}} \prod_{\rho \in \mathbb{F}_p} w_\rho^{p^{m-1}(p^{m-1} + \varepsilon_2 \eta_\rho(\rho^2 - g^{2t+1}))}.$$

Theorem 6: Let g be a generator of \mathbb{F}_p^* and $c \in \mathbb{F}_p^*$. If m/v is even and $\beta^{\frac{q-1}{p^{v+1}}} = (-1)^s$, then \mathcal{C}_{D_c} is an $[n_c, 2m]$ three-weight linear code, where

$$n_c = p^{2m-1} + \varepsilon_2 p^{m+v-1},$$

and ε_2 is given in (4). Define

$$B_1 = (p^{m-v-1} - \varepsilon_2)(p^{m-v} + \varepsilon_2), \\ B_2 = p^{m-v-1}(p^{m-v} + \varepsilon_2).$$

The weight enumerator is

$$1 + (p^{2m} - p^{2m-2v}) z^{(p-1)p^{m-2}(p^m + \varepsilon_2 p^v)} + (B_1 + \frac{p-1}{2} B_2) z^{(p-1)p^{2m-2}} + \frac{p-1}{2} B_2 z^{(p-1)p^{m-1}(p^{m-1} + 2\varepsilon_2)},$$

and the complete weight enumerator is

$$w_0^{n_c} + (p^{2m} - p^{2m-2v}) \prod_{\rho \in \mathbb{F}_p} w_\rho^{p^{m-2}(p^m + \varepsilon_2 p^v)} + B_1 w_0^{p^{m-1}(p^{m-1} + \varepsilon_2 p^v)} \prod_{\rho \in \mathbb{F}_p^*} w_\rho^{p^{2m-2}} + B_2 \sum_{t=1}^{\frac{p-1}{2}} \prod_{\rho \in \mathbb{F}_p} w_\rho^{p^{m-1}(p^{m-1} - \varepsilon_2 p^v \eta_\rho(\rho^2 - g^{2t}))} + B_2 \sum_{t=1}^{\frac{p-1}{2}} \prod_{\rho \in \mathbb{F}_p} w_\rho^{p^{m-1}(p^{m-1} - \varepsilon_2 p^v \eta_\rho(\rho^2 - g^{2t+1}))}.$$

Remark 2: From Theorems 4, 5 and 6, we know that all of the codes \mathcal{C}_{D_c} with $c \neq 0$ have the same complete weight enumerators and weight enumerators.

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

Example 1: Let $(p, m, u) = (3, 2, 4)$, $\mathbb{F}_3^* = \langle 2 \rangle$. Denote $\mathbb{F}_9^* = \langle \gamma \rangle$ and $\alpha = \gamma$, $\beta = \gamma^3$. Then $k = 1$, $v = 2$ and $m/v = 1$. If $c = 0$, by Theorem 1, the code \mathcal{C}_{D_0} has parameters $[32, 4, 18]$ with weight enumerator $1 + 32z^{18} + 48z^{24}$ and complete weight enumerator

$$w_0^{32} + 32w_0^{14}(w_1 w_2)^9 + 48w_0^8(w_1 w_2)^{12}.$$

If $c = 1$, by Theorem 4, the code \mathcal{C}_{D_1} is a $[24, 4, 12]$ linear code. Its weight enumerator is $1 + 24z^{12} + 56z^{18}$, and its complete weight enumerator is

$$w_0^{24} + 24w_0^{12}(w_1 w_2)^6 + 56w_0^6(w_1 w_2)^9.$$

Besides, the punctured code $\mathcal{C}_{\overline{D_0}}$ has parameters $[16, 4, 9]$ and weight enumerator $1 + 32z^9 + 48z^{12}$. It is optimal according to Markus Grassl's code tables available at <http://www.codetables.de/>.

Example 2: Let $(p, m, u) = (5, 2, 2)$, $\mathbb{F}_5^* = \langle 2 \rangle$. Denote $\mathbb{F}_{25}^* = \langle \gamma \rangle$, $\alpha = \gamma$ and $\beta = \gamma^2$. Then $k = 1$, $v = 2$ and $m/v = 1$. By Theorem 1, the code \mathcal{C}_{D_0} has parameters $[104, 4, 80]$ with weight enumerator $1 + 520z^{80} + 104z^{100}$ and complete weight enumerator

$$w_0^{104} + 520w_0^{24}(w_1 w_2 w_3 w_4)^{20} + 104w_0^4(w_1 w_2 w_3 w_4)^{25}.$$

The punctured code $\mathcal{C}_{\overline{D_0}}$ has parameters $[26, 4, 20]$ and weight enumerator $1 + 520z^{20} + 104z^{25}$. The code \mathcal{C}_{D_0} is almost optimal and $\mathcal{C}_{\overline{D_0}}$ is optimal according to Markus Grassl's code tables. By Theorem 4, the code \mathcal{C}_{D_1} is a $[130, 4, 100]$ linear code. Its weight enumerator is

$$1 + 364z^{100} + 260z^{110},$$

and its complete weight enumerator is

$$w_0^{130} + 104w_0^{30}(w_1 w_2 w_3 w_4)^{25} + 130(w_0 w_1 w_4)^{30}(w_2 w_3)^{20} + 130(w_0 w_2 w_3)^{30}(w_1 w_4)^{20} + 130w_0^{20}(w_1 w_4)^{25}(w_2 w_3)^{30} + 130w_0^{20}(w_1 w_4)^{30}(w_2 w_3)^{25}.$$

Example 3: Let $(p, m, u) = (3, 2, 3)$, $\mathbb{F}_3^* = \langle 2 \rangle$. Denote $\mathbb{F}_9^* = \langle \gamma \rangle$, $\alpha = \gamma^2$ and $\beta = \gamma$. Then $k = 1$, $v = s = 1$, $m/v = 2$ and $\beta^{\frac{q-1}{p^{v+1}}} \neq (-1)^s$. By Theorem 2, the code \mathcal{C}_{D_0} is a $[20, 4, 12]$ linear code with weight enumerator $1 + 60z^{12} + 20z^{18}$, and complete weight enumerator

$$w_0^{20} + 60w_0^8(w_1 w_2)^6 + 20w_0^2(w_1 w_2)^9.$$

If $c \neq 0$, by Theorem 5, the corresponding code \mathcal{C}_{D_c} has parameters $[30, 4, 18]$ with weight enumerator $1 + 50z^{18} + 30z^{24}$ and complete weight enumerator

$$w_0^{30} + 50w_0^{12}(w_1 w_2)^9 + 30w_0^6(w_1 w_2)^{12}.$$

Moreover, the punctured code $\mathcal{C}_{\overline{D_0}}$ has parameters $[10, 4, 6]$ and weight enumerator $1 + 60z^6 + 20z^9$. Both \mathcal{C}_{D_0} and $\mathcal{C}_{\overline{D_0}}$ are optimal with respect to the Griesmer bound.

Example 4: Let $(p, m, u) = (3, 4, 3)$, $\mathbb{F}_3^* = \langle 2 \rangle$. Denote $\mathbb{F}_{81}^* = \langle \gamma \rangle$, $\alpha = \gamma$ and $t = 1$. Then $k = 2$, $v = 1$, $s = 2$,

$m/v = 4$ and $\beta^{\frac{q-1}{p^{v+1}}} = (-1)^s$. By Theorem 3, the code C_{D_0} has parameters [2024, 8, 1296] with weight enumerator

$$1 + 504z^{1296} + 5832z^{1350} + 224z^{1458},$$

and complete weight enumerator

$$w_0^{2024} + 504w_0^{728}(w_1w_2)^{648} + 5832w_0^{674}(w_1w_2)^{675} + 224w_0^{566}(w_1w_2)^{729}.$$

By Theorem 6, the code C_{D_1} is a [2268, 8, 1458] linear code. Its weight enumerator is $1 + 476z^{1458} + 5832z^{1512} + 252z^{1620}$, and its complete weight enumerator is

$$w_0^{2268} + 476w_0^{810}(w_1w_2)^{729} + 5832(w_0w_1w_2)^{756} + 252w_0^{648}(w_1w_2)^{810}.$$

II. PRELIMINARIES

Let $q = p^m$. In this section, we present some results on group characters and exponential sums. For each $b \in \mathbb{F}_q$, an additive character χ_b of \mathbb{F}_q is defined by $\chi_b(x) = \zeta_p^{\text{Tr}(bx)}$ for all $x \in \mathbb{F}_q$, where $\zeta_p = \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$ and Tr is the absolute trace function from \mathbb{F}_q to \mathbb{F}_p . With each character χ_b , there is associated the conjugate character $\bar{\chi}_b$ defined by $\bar{\chi}_b(x) = \chi_b(x)$ for all $x \in \mathbb{F}_q$. Especially χ_1 is called the canonical additive character and is denoted by χ for simplicity.

Let η (resp. η_p) denote the quadratic multiplicative character of \mathbb{F}_q (resp. \mathbb{F}_p). When m is even, we know from Lemma 7 of [11] that $\eta(z) = 1$ for all $z \in \mathbb{F}_p^*$. The quadratic Gauss sum over \mathbb{F}_q is defined by

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

Lemma 1 (Theorem 5.15, [21]): The quadratic Gauss sums $G(\eta)$ and $G(\eta_p)$ are given by

$$G(\eta) = (-1)^{m-1} \sqrt{p^*}^m \text{ and } G(\eta_p) = \sqrt{p^*},$$

where $p^* = \eta_p(-1)p$.

Lemma 2 (Theorem 5.33, [21]): Let $q = p^m$ be odd and $f(x) = a_2x^2 + a_1x \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then

$$Q(a_2, a_1) = \sum_{x \in \mathbb{F}_q} \chi(f(x)) = \bar{\chi}(a_1^2(4a_2)^{-1})\eta(a_2)G(\eta),$$

where η is the quadratic character of \mathbb{F}_q .

For $\alpha, \beta \in \mathbb{F}_q$ and any positive integer u , the Weil sum $S_u(\alpha, \beta)$ is defined by

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

In [6], [7], Coulter evaluated some Weil sums $S_u(\alpha, \beta)$ for $\alpha \neq 0$ and q odd. Recall that $v = \gcd(m, u)$. When $m = 2k$ we denote $s = k/v$.

Lemma 3 (Theorem 1, [6]): If m/v is odd, then

$$S_u(\alpha, 0) = G(\eta)\eta(\alpha).$$

Lemma 4 (Theorem 2, [6]): If m/v is even, then

$$S_u(\alpha, 0) = \begin{cases} (-1)^s p^k & \text{if } \alpha^{\frac{q-1}{p^{v+1}}} \neq (-1)^s, \\ -(-1)^s p^{k+v} & \text{if } \alpha^{\frac{q-1}{p^{v+1}}} = (-1)^s. \end{cases}$$

Lemma 5 (Theorem 1, [7]): Suppose that $f_\alpha(X) = \alpha^{p^u}X^{p^{2u}} + \alpha X$ is a permutation polynomial over \mathbb{F}_q . Let x_0 be the unique solution of the equation $f(X) = -\beta^{p^u}$. The evaluation of $S_u(\alpha, \beta)$ partitions into the following two cases.

1. If m/v is odd, then

$$S_u(\alpha, \beta) = G(\eta)\eta(\alpha)\bar{\chi}(\alpha x_0^{p^u+1}).$$

2. If m/v is even, then $\alpha^{\frac{q-1}{p^{v+1}}} \neq (-1)^s$ and

$$S_u(\alpha, \beta) = (-1)^s p^k \bar{\chi}(\alpha x_0^{p^u+1}).$$

Lemma 6 (Theorem 2, [7]): Suppose that $f_\alpha(X) = \alpha^{p^u}X^{p^{2u}} + \alpha X$ is not a permutation polynomial over \mathbb{F}_q , then $S_u(\alpha, \beta) = 0$ unless the equation $f(X) = -\beta^{p^u}$ is solvable. If the equation is solvable, with some solution x_0 say, then

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

Lemma 7 (Lemma 9, [18]): With the notation introduced above, we denote

$$M = \{\beta \in \mathbb{F}_q : f_\alpha(X) = -\beta^{p^u} \text{ is solvable in } \mathbb{F}_q\}.$$

If $\alpha^{\frac{q-1}{p^{v+1}}} = (-1)^s$, then $|M| = p^{m-2v}$.

III. THE PROOFS OF THE MAIN RESULTS

In this section, we will prove our main results presented in Section I by fixing $\alpha, \beta \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_p$. For convenience, we denote

$$n_c = |\{(x, y) \in \mathbb{F}_q^2 : \text{Tr}(\alpha x^2 + \beta y^{p^u+1}) = c\}|. \quad (5)$$

Clearly the length of the code is $n_0 - 1$ if $c = 0$, and otherwise n_c for $c \neq 0$.

A. AUXILIARY RESULTS

Recall that ε_1 and ε_2 are defined in (3) and (4), respectively.

Lemma 8: Let n_0 be defined as (5) for $c = 0$. Then if m/v is odd, then

$$n_0 = p^{2m-1} + \varepsilon_1(p-1)p^{m-1}.$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s$, then

$$n_0 = p^{2m-1} + \varepsilon_2(p-1)p^{m-1}.$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} = (-1)^s$, then

$$n_0 = p^{2m-1} - \varepsilon_2(p-1)p^{m+v-1}.$$

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

$$n_0 = \frac{1}{p} \sum_{x, y \in \mathbb{F}_q} \sum_{z_1 \in \mathbb{F}_p} \zeta_p^{z_1 \text{Tr}(\alpha x^2 + \beta y^{p^u+1})}$$

$$= p^{2m-1} + p^{-1}\Omega, \quad (6)$$

where

$$\Omega = \sum_{z_1 \in \mathbb{F}_p^*} Q(z_1\alpha, 0)S_u(z_1\beta, 0).$$

Thus we only need to evaluate Ω . From Lemmas 2 and 3, if m/v is odd, then

$$\Omega = \eta(\alpha\beta)(p-1)G(\eta)^2. \quad (7)$$

From Lemmas 2 and 4, if m/v is even, then

$$\Omega = \begin{cases} (-1)^s \eta(\alpha)(p-1)p^k G(\eta) & \text{if } \beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s, \\ -(-1)^s \eta(\alpha)(p-1)p^{k+v} G(\eta) & \text{if } \beta^{\frac{q-1}{p^{v-1}}} = (-1)^s. \end{cases} \quad (8)$$

The desired conclusion then follows from (6), (7), (8) and Lemma 1. \square

Lemma 9: Let n_c be defined as (5) for $c \neq 0$. Then if m/v is odd, then

$$n_c = p^{2m-1} - \varepsilon_1 p^{m-1}.$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s$, then

$$n_c = p^{2m-1} - \varepsilon_2 p^{m-1}.$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} = (-1)^s$, then

$$n_c = p^{2m-1} + \varepsilon_2 p^{m+v-1}.$$

Proof: Again by the orthogonal property of additive characters

$$\begin{aligned} n_c &= \frac{1}{p} \sum_{x,y \in \mathbb{F}_q} \sum_{z_1 \in \mathbb{F}_p} \zeta_p^{z_1 \text{Tr}(\alpha x^2 + \beta y^{m+1}) - cz_1} \\ &= p^{2m-1} + p^{-1}\Gamma, \end{aligned} \quad (9)$$

where

$$\Gamma = \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-cz_1} Q(z_1\alpha, 0)S_u(z_1\beta, 0).$$

If m/v is odd, we have from Lemmas 2 and 3 that

$$\Gamma = -\eta(\alpha\beta)G(\eta)^2. \quad (10)$$

Otherwise if m/v is even, we have from Lemmas 2 and 4 that

$$\Gamma = \begin{cases} (-1)^s \eta(\alpha)p^k G(\eta) & \text{if } \beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s, \\ (-1)^s \eta(\alpha)p^{k+v} G(\eta) & \text{if } \beta^{\frac{q-1}{p^{v-1}}} = (-1)^s. \end{cases} \quad (11)$$

Using (9), (10) (11) and Lemma 1, we get the desired conclusions. \square

The Pless power moments are useful tools when we calculate the weight distribution of codes. Recall the code \mathcal{C}_{D_c} is defined by (1) and (2) with length $n = |D_c|$ and dimension $\kappa = \dim_{\mathbb{F}_p}(\mathcal{C}_{D_c})$. The weight distributions of \mathcal{C}_{D_c} and its dual code are denoted by $(1, A_1, \dots, A_n)$ and $(1, A_1^\perp, \dots, A_n^\perp)$,

respectively. Since $(0, 0) \notin D_c$, we must have $A_1^\perp = 0$. So the first two Pless power moments are given by [17, p.259]:

$$\begin{aligned} \sum_{j=0}^n A_j &= p^\kappa, \\ \sum_{j=0}^n jA_j &= p^{\kappa-1}(p-1)n. \end{aligned}$$

B. THE PROOFS OF THEOREMS

In order to investigate the weight enumerator of \mathcal{C}_{D_c} for $c \in \mathbb{F}_p$, we need to do some preparations. Observe that $a = b = 0$ gives the zero codeword. Hence, we assume that $(a, b) \neq (0, 0)$ unless otherwise stated. Let $N_{\rho,c}(a, b)$ denote the number of components $\text{Tr}(ax+by)$ of $\mathbf{c}(a, b)$ that are equal to ρ , where $\rho \in \mathbb{F}_p$, $(a, b) \neq (0, 0)$ and $c \in \mathbb{F}_p$. For $\rho \neq 0$, we have

$$N_{\rho,c}(a, b) = |\{(x, y) \in \mathbb{F}_q^2 : \text{Tr}(ax + by) = \rho, \text{Tr}(\alpha x^2 + \beta y^{m+1}) = c\}|. \quad (12)$$

Then the Hamming weight of $\mathbf{c}(a, b)$ is obtained by

$$wt(\mathbf{c}(a, b)) = \sum_{\rho \in \mathbb{F}_p} N_{\rho,c}(a, b) = n - N_{0,c}(a, b), \quad (13)$$

where $n = \#D_c$ is the length of the code.

By (12) and the orthogonal property of additive characters,

$$\begin{aligned} N_{\rho,c}(a, b) &= p^{-2} \sum_{x,y \in \mathbb{F}_q} \sum_{z_1 \in \mathbb{F}_p} \zeta_p^{z_1 \text{Tr}(\alpha x^2 + \beta y^{m+1}) - cz_1} \\ &\quad \times \sum_{z_2 \in \mathbb{F}_p} \zeta_p^{z_2 \text{Tr}(ax+by) - \rho z_2} \\ &= p^{-1}n_c + p^{-2}(\Omega_1 + \Omega_2^{(c)}), \end{aligned} \quad (14)$$

where

$$\begin{aligned} \Omega_1 &= \sum_{z_2 \in \mathbb{F}_p^*} \zeta_p^{-\rho z_2} \sum_{x,y \in \mathbb{F}_q} \zeta_p^{z_2 \text{Tr}(ax+by)} = 0, \\ \Omega_2^{(c)} &= \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-cz_1} \sum_{z_2 \in \mathbb{F}_p^*} \zeta_p^{-\rho z_2} Q(z_1\alpha, z_2a)S_u(z_1\beta, z_2b). \end{aligned} \quad (15)$$

Now we are going to determine the values of $\Omega_2^{(c)}$ for $c \in \mathbb{F}_p$ in Lemmas 10 and 11. Let $\alpha, \beta \in \mathbb{F}_q^*$ and $(a, b) \neq (0, 0)$. The equation

$$\beta^{p^u} X^{p^{2u}} + \beta X = -b^{p^u} \quad (16)$$

is not always solvable over \mathbb{F}_q if m/v is even. When $\beta^{p^u} X^{p^{2u}} + \beta X$ is a permutation polynomial over \mathbb{F}_q , it has a unique solution by Lemma 5. Let γ_b be some solution of (16) if it exists, then for $z_1, z_2 \in \mathbb{F}_p^*$, $z_3\gamma_b$ is a solution of the equation $(z_1\beta)^{p^u} X^{p^{2u}} + z_1\beta X = -(z_2b)^{p^u}$, where we denote $z_3 = z_1^{-1}z_2 \in \mathbb{F}_p^*$. For the simplicity of formulae, we use the symbol $\lambda_{a,b}$ to denote $\text{Tr}(\frac{a^2}{4\alpha} + \beta\gamma_b^{p^u+1})$ whenever γ_b exists.

Lemma 10: With notation be as before, the values of $\Omega_2^{(0)}$ for $(a, b) \neq (0, 0)$ are given as follows.

1. If m/v is odd, then

$$\Omega_2^{(0)} = \begin{cases} -(p-1)G(\eta)^2\eta(\alpha\beta) & \text{if } \lambda_{a,b} = 0, \\ G(\eta)^2\eta(\alpha\beta) & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

2. If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s$, then

$$\Omega_2^{(0)} = \begin{cases} -(-1)^s(p-1)p^k G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} = 0, \\ (-1)^s p^k G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

3. If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} = (-1)^s$, we have $\Omega_2^{(0)} = 0$, or if (16) is solvable, then

$$\Omega_2^{(0)} = \begin{cases} (-1)^s(p-1)p^{k+v}G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} = 0, \\ -(-1)^s p^{k+v}G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

Proof: If m/v is odd, by (15) and Lemma 5, we have

$$\begin{aligned} \Omega_2^{(0)} &= G(\eta)^2\eta(\alpha\beta) \sum_{z_2 \in \mathbb{F}_p^*} \zeta_p^{-\rho z_2} \\ &\quad \times \sum_{z_1 \in \mathbb{F}_p^*} \bar{\chi}\left(\frac{z_2^2 a^2}{4z_1 \alpha}\right) \bar{\chi}\left(z_1 \beta \left(\frac{z_2}{z_1} \gamma b\right)^{p^u+1}\right) \\ &= G(\eta)^2\eta(\alpha\beta) \sum_{z_2 \in \mathbb{F}_p^*} \zeta_p^{-\rho z_2} \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-z_1^{-1} z_2^2 \lambda_{a,b}} \\ &= \begin{cases} -(p-1)G(\eta)^2\eta(\alpha\beta) & \text{if } \lambda_{a,b} = 0, \\ G(\eta)^2\eta(\alpha\beta) & \text{if } \lambda_{a,b} \neq 0. \end{cases} \end{aligned}$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s$, again by (15) and Lemma 5, we have

$$\begin{aligned} \Omega_2^{(0)} &= (-1)^s p^k G(\eta)\eta(\alpha) \sum_{z_2 \in \mathbb{F}_p^*} \zeta_p^{-\rho z_2} \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-z_1^{-1} z_2^2 \lambda_{a,b}} \\ &= \begin{cases} -(-1)^s(p-1)p^k G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} = 0, \\ (-1)^s p^k G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} \neq 0. \end{cases} \end{aligned}$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} = (-1)^s$, from (15) and Lemma 6, we see that

$$\Omega_2^{(0)} = 0,$$

or if (16) is solvable, then

$$\begin{aligned} \Omega_2^{(0)} &= (-1)^{s+1} p^{k+v} G(\eta)\eta(\alpha) \sum_{z_2 \in \mathbb{F}_p^*} \zeta_p^{-\rho z_2} \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-z_1^{-1} z_2^2 \lambda_{a,b}} \\ &= \begin{cases} (-1)^s(p-1)p^{k+v}G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} = 0, \\ -(-1)^s p^{k+v}G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} \neq 0. \end{cases} \end{aligned}$$

Thus we get the desired assertions, completing the whole proof. \square

Lemma 11: Denote $\mathcal{K} = p\eta_p(\rho^2 - 4c\lambda_{a,b}) + 1$ for $\rho \in \mathbb{F}_p^*$. The values of $\Omega_2^{(c)}$ for $c \neq 0$ and $(a, b) \neq (0, 0)$ are given as follows.

1. If m/v is odd, then

$$\Omega_2^{(c)} = \begin{cases} G(\eta)^2\eta(\alpha\beta) & \text{if } \lambda_{a,b} = 0, \\ G(\eta)^2\eta(\alpha\beta)\mathcal{K} & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

2. If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s$, then

$$\Omega_2^{(c)} = \begin{cases} (-1)^s p^k G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} = 0, \\ (-1)^s p^k G(\eta)\eta(\alpha)\mathcal{K} & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

3. If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} = (-1)^s$, we have $\Omega_2^{(c)} = 0$, or if (16) is solvable, then

$$\Omega_2^{(c)} = \begin{cases} -(-1)^s p^{k+v} G(\eta)\eta(\alpha) & \text{if } \lambda_{a,b} = 0, \\ -(-1)^s p^{k+v} G(\eta)\eta(\alpha)\mathcal{K} & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

Proof: If m/v is odd, by (15), Lemmas 2 and 5, we have

$$\Omega_2^{(c)} = G(\eta)^2\eta(\alpha\beta) \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-cz_1} \sum_{z_3 \in \mathbb{F}_p^*} \zeta_p^{-z_1 z_3^2 \lambda_{a,b} - \rho z_1 z_3}.$$

If $\lambda_{a,b} = 0$, then

$$\Omega_2^{(c)} = G(\eta)^2\eta(\alpha\beta).$$

Otherwise if $\lambda_{a,b} \neq 0$, then

$$\Omega_2^{(c)} = G(\eta)^2\eta(\alpha\beta)(G(\eta_p)^2\eta_p(4c\lambda_{a,b} - \rho^2) + 1).$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} \neq (-1)^s$, again by (15), Lemmas 2 and 5, we have

$$\begin{aligned} \Omega_2^{(c)} &= (-1)^s p^k G(\eta)\eta(\alpha) \\ &\quad \times \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-cz_1} \sum_{z_3 \in \mathbb{F}_p^*} \zeta_p^{-z_1 z_3^2 \lambda_{a,b} - \rho z_1 z_3}. \end{aligned}$$

If $\lambda_{a,b} = 0$, then

$$\Omega_2^{(c)} = (-1)^s p^k G(\eta)\eta(\alpha).$$

Otherwise if $\lambda_{a,b} \neq 0$, then

$$\Omega_2^{(c)} = (-1)^s p^k G(\eta)\eta(\alpha)(G(\eta_p)^2\eta_p(4c\lambda_{a,b} - \rho^2) + 1).$$

If $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^{v-1}}} = (-1)^s$, from (15) and Lemma 6, we see that

$$\Omega_2^{(c)} = 0,$$

or if (16) is solvable, then

$$\begin{aligned} \Omega_2^{(c)} &= -(-1)^s p^{k+v} G(\eta)\eta(\alpha) \\ &\quad \times \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{-cz_1} \sum_{z_3 \in \mathbb{F}_p^*} \zeta_p^{-z_1 z_3^2 \lambda_{a,b} - \rho z_1 z_3}. \end{aligned}$$

If $\lambda_{a,b} = 0$, then

$$\Omega_2^{(c)} = -(-1)^s p^{k+v} G(\eta)\eta(\alpha).$$

Otherwise if $\lambda_{a,b} \neq 0$, then

$$\begin{aligned} \Omega_2^{(c)} &= -(-1)^s p^{k+v} G(\eta)\eta(\alpha) \\ &\quad \times (G(\eta_p)^2\eta_p(4c\lambda_{a,b} - \rho^2) + 1). \end{aligned}$$

By observing $G(\eta_p)^2 = p\eta_p(-1)$, we get the desired conclusions. \square

1) THE PROOFS OF THEOREMS 1, 2 AND 3

The code \mathcal{C}_{D_0} has length $n_0 - 1$, where n_0 is given in Lemma 8. For a codeword $\mathbf{c}(a, b)$, $(a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}$, we will show that it has nonzero components, which means that it has nonzero Hamming weight and the dimension of \mathcal{C}_{D_0} is therefore $2m$.

The values of $N_{\rho,0}(a, b)$ are calculated from (14) and Lemmas 1, 8 and 10.

If m/v is odd, then

$$N_{\rho,0}(a, b) = p^{-1}n_0 + p^{-2}\Omega_2^{(0)} \\ = \begin{cases} p^{2m-2} & \text{if } \lambda_{a,b} = 0, \\ p^{2m-2} + p^{-1}\eta(\alpha\beta)G(\eta)^2 & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

We observe that

$$\#\{(a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} : \lambda_{a,b} = 0\} \\ = \#\{(x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} : \text{Tr}\left(\frac{x^2}{4\alpha} + \beta y^{p^u+1}\right) = 0\} \\ = n_0 - 1.$$

Taking into account that

$$N_{0,0}(a, b) = n_0 - 1 - \sum_{\rho \in \mathbb{F}_p^*} N_{\rho,0}(a, b)$$

from (13), we obtain the complete weight enumerator of \mathcal{C}_{D_0} given in Theorem 1. Its weight enumerator then follows immediately from (13).

If $m/v \equiv 0 \pmod{2}$ and $\beta \frac{q-1}{p^{v-1}} \neq (-1)^s$, then

$$N_{\rho,0}(a, b) = \begin{cases} p^{2m-2} & \text{if } \lambda_{a,b} = 0, \\ p^{2m-2} + (-1)^s \eta(\alpha) p^{k-1} G(\eta) & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

By a similar argument as previous, we get the desired results given in Theorem 2.

Let us consider the case $m/v \equiv 0 \pmod{2}$ and $\beta \frac{q-1}{p^{v-1}} = (-1)^s$. If (16) is unsolvable over \mathbb{F}_q , then

$$N_{\rho,0}(a, b) = p^{2m-2} - \varepsilon_2(p-1)p^{m+v-2}.$$

Otherwise if (16) is solvable over \mathbb{F}_q , then

$$N_{\rho,0}(a, b) = \begin{cases} p^{2m-2} & \text{if } \lambda_{a,b} = 0, \\ p^{2m-2} - \varepsilon_2 p^{m+v-1} & \text{if } \lambda_{a,b} \neq 0. \end{cases}$$

Here ε_2 is defined in (4). Thus we know that the three nonzero weights of \mathcal{C}_{D_0} are

$$w_1 = (p-1)p^{2m-2}, \\ w_2 = (p-1)(p^{2m-2} - \varepsilon_2 p^{m+v-1}), \\ w_3 = (p-1)(p^{2m-2} - \varepsilon_2(p-1)p^{m+v-2}).$$

Let us calculate the frequency of each weight. It follows from Lemma 7 that

$$A_{w_3} \\ = |\{(a, b) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} : (16) \text{ has no solution over } \mathbb{F}_q\}| \\ = q(q - p^{m-2v}).$$

After a straightforward calculation from the first two Pless power moments, we derive that

$$A_{w_1} = (p^{m-v-1} - \varepsilon_2)(p^{m-v} + \varepsilon_2), \\ A_{w_2} = (p-1)p^{m-v-1}(p^{m-v} + \varepsilon_2).$$

This completes the proof of Theorem 3.

2) THE PROOFS OF THEOREMS 4, 5 AND 6

The proofs are similar to the previous theorems. The length of \mathcal{C}_{D_c} for $c \neq 0$ is given in Lemma 9. Let g be a generator of \mathbb{F}_p^* , that is to say $\mathbb{F}_p^* = \langle g \rangle$. For $(a, b) \neq (0, 0)$, the values of $N_{\rho,c}(a, b)$ are calculated from (14), Lemmas 1, 9 and 11.

We firstly assume that m/v is odd. If $\lambda_{a,b} = 0$, then

$$N_{\rho,c}(a, b) = p^{-1}n_c + p^{-2}\Omega_2^{(c)} = p^{2m-2}.$$

Otherwise if $\lambda_{a,b} \neq 0$, then

$$N_{\rho,c}(a, b) = p^{2m-2} + \varepsilon_1 p^{m-1} \eta_p(\rho^2 - 4c\lambda_{a,b}),$$

where ε_1 is defined in (3). If $4c\lambda_{a,b}$ is a square element in \mathbb{F}_p^* , which means that $4c\lambda_{a,b} \in \langle g^2 \rangle$, then

$$N_{\rho,c}(a, b) = p^{2m-2} + \varepsilon_1 p^{m-1} \eta_p(\rho^2 - g^{2t}),$$

where $1 \leq t \leq (p-1)/2$. According to Lemma 9, this value occurs n_c times.

If $4c\lambda_{a,b}$ is a nonsquare element in \mathbb{F}_p^* , i.e., $4c\lambda_{a,b} \in g\langle g^2 \rangle$, then

$$N_{\rho,c}(a, b) = p^{2m-2} + \varepsilon_1 p^{m-1} \eta_p(\rho^2 - g^{2t+1}),$$

where $1 \leq t \leq (p-1)/2$ and this value occurs n_c times.

At last if $\lambda_{a,b} = 0$, then

$$N_{\rho,c}(a, b) = p^{2m-2},$$

and this value occurs $p^{2m} - 1 - (p-1)n_c$.

We also need to determine $N_{0,c}(a, b)$. According to Theorem 5.48 in [21],

$$\sum_{\rho \in \mathbb{F}_p^*} \eta_p(\rho^2 - g^{2t+1}) = -1 + \eta_p(-1), \quad (17)$$

$$\sum_{\rho \in \mathbb{F}_p^*} \eta_p(\rho^2 - g^{2t}) = -1 - \eta_p(-1), \quad (18)$$

where $1 \leq t \leq (p-1)/2$. By (13), (17) and (18),

$$N_{0,c}(a, b) = n_c - \sum_{\rho \in \mathbb{F}_p^*} N_{\rho,c}(a, b) \\ = \begin{cases} p^{2m-2} + \varepsilon_1 \eta_p(-1) p^{m-1} & \text{if } 4c\lambda_{a,b} \in \langle g^2 \rangle, \\ p^{2m-2} - \varepsilon_1 \eta_p(-1) p^{m-1} & \text{if } 4c\lambda_{a,b} \in g\langle g^2 \rangle, \\ p^{2m-2} - \varepsilon_1 p^{m-1} & \text{if } \lambda_{a,b} = 0. \end{cases}$$

Combining the above all, we obtain the desired assertions in Theorem 4.

For the second case, we consider $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^v-1}} \neq (-1)^s$. It is derived that

$$N_{\rho,c}(a, b) = p^{-1}n_c + p^{-2}\Omega_2^{(c)} = \begin{cases} p^{2m-2} & \text{if } \lambda_{a,b} = 0, \\ p^{2m-2} + \varepsilon_2 p^{m-1} \eta_p(\rho^2 - 4c\lambda_{a,b}) & \text{if } \lambda_{a,b} \neq 0, \end{cases}$$

where ε_2 is defined in (4). By a similar argument as previous, we obtain the assertions given in Theorem 5.

The third case we consider is $m/v \equiv 0 \pmod{2}$ and $\beta^{\frac{q-1}{p^v-1}} = (-1)^s$. In this case, if (16) has no solution in \mathbb{F}_q , then

$$N_{\rho,c}(a, b) = p^{2m-2} + \varepsilon_2 p^{m+v-2},$$

for $\rho \neq 0$. Meanwhile from (13),

$$N_{0,c}(a, b) = p^{2m-2} + \varepsilon_2 p^{m+v-2}.$$

This value occurs $p^{2m} - p^{2m-2v}$ times.

If (16) is solvable over \mathbb{F}_q and $\lambda_{a,b} = 0$, then

$$N_{\rho,c}(a, b) = p^{2m-2},$$

for $\rho \neq 0$, and $N_{0,c}(a, b) = p^{2m-2} + \varepsilon_2 p^{m+v-1}$. The frequency of this value is denoted by B_1 .

Suppose that (16) is solvable over \mathbb{F}_q . Let $4c\lambda_{a,b}$ be a square element in \mathbb{F}_p^* , say $4c\lambda_{a,b} = g^{2t}$, where $1 \leq t \leq (p-1)/2$. Then

$$N_{\rho,c}(a, b) = p^{2m-2} - \varepsilon_2 p^{m+v-1} \eta_p(\rho^2 - g^{2t}).$$

Meanwhile from (13) and (18),

$$N_{0,c}(a, b) = p^{2m-2} - \varepsilon_2 \eta_p(-1) p^{m+v-1}.$$

The frequency of this value is denoted by B_2 .

If (16) is solvable and $4c\lambda_{a,b}$ is not a square element, then

$$N_{\rho,c}(a, b) = p^{2m-2} - \varepsilon_2 p^{m+v-1} \eta_p(\rho^2 - g^{2t+1}),$$

where $1 \leq t \leq (p-1)/2$. Consequently from (13) and (17),

$$N_{0,c}(a, b) = p^{2m-2} + \varepsilon_2 \eta_p(-1) p^{m+v-1}.$$

The frequency of this value is denoted by B_3 .

It is easily seen that $B_2 = B_3$. Calculating from the first two Pless power moments gives that

$$B_1 = (p^{m-v-1} - \varepsilon_2)(p^{m-v} + \varepsilon_2), \\ B_2 = p^{m-v-1}(p^{m-v} + \varepsilon_2).$$

This completes the whole proof of Theorem 6.

IV. CONCLUDING REMARKS

In this article, a class linear codes with two or three weights are constructed from a proper defining set. Their complete weight enumerators and weight enumerators are determined applying Weil sums. Some optimal and almost optimal codes are found using this construction. According to [29], a linear code over \mathbb{F}_p is suitable for constructions of secret sharing schemes if

$$\frac{w_{min}}{w_{max}} > \frac{p-1}{p}, \tag{19}$$

where w_{min} and w_{max} denote the minimum and maximum nonzero weights in \mathcal{C}_{D_c} , respectively. For the linear codes \mathcal{C}_{D_c} , the inequality (19) holds if $m \geq \max\{3, 3+v\}$. Also these codes have small dimension compared with their length. So they will be applied in secret sharing schemes with good access structures.

REFERENCES

- [1] J. Ahn, D. Ka, and C. Li, "Complete weight enumerators of a class of linear codes," *Des., Codes Cryptogr.*, vol. 83, no. 1, pp. 83–99, Apr. 2017.
- [2] S. Bae, C. Li, and Q. Yue, "On the complete weight enumerators of some reducible cyclic codes," *Discrete Math.*, vol. 338, no. 12, pp. 2275–2287, Dec. 2015.
- [3] 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.
- [4] 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.
- [5] P. Charpin, "Cyclic codes with few weights and niho exponents," *J. Combinat. Theory A*, vol. 108, no. 2, pp. 247–259, Nov. 2004.
- [6] R. Coulter, "Explicit evaluations of some Weil sums," *Acta Arithmetica*, vol. 83, no. 3, pp. 241–251, 1998.
- [7] R. Coulter, "Further evaluations of Weil sums," *Acta Arithmetica*, vol. 86, no. 3, pp. 217–226, 1998.
- [8] C. Ding and J. Yin, "A construction of optimal constant composition codes," *Des., Codes Cryptogr.*, vol. 40, no. 2, pp. 157–165, Aug. 2006.
- [9] C. Ding, T. Hellesteth, T. Klove, and X. Wang, "A generic construction of Cartesian authentication codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2229–2235, Jun. 2007.
- [10] K. Ding and C. Ding, "Binary linear codes with three weights," *IEEE Commun. Lett.*, vol. 18, no. 11, pp. 1879–1882, Nov. 2014.
- [11] 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.
- [12] G. Jian, Z. Lin, and R. Feng, "Two-weight and three-weight linear codes based on Weil sums," *Finite Fields Their Appl.*, vol. 57, pp. 92–107, May 2019.
- [13] T. Hellesteth and A. Kholosha, "Monomial and quadratic bent functions over the finite fields of odd characteristic," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2018–2032, May 2006.
- [14] Z. Heng, C. Ding, and Z. Zhou, "Minimal linear codes over finite fields," *Finite Fields Their Appl.*, vol. 54, pp. 176–196, Nov. 2018.
- [15] Z. Heng and Q. Yue, "Complete weight distributions of two classes of cyclic codes," *Cryptogr. Commun.*, vol. 9, no. 3, pp. 323–343, May 2017.
- [16] Z. Heng, W. Wang, and Y. Wang, "Projective binary linear codes from special Boolean functions," *Applicable Algebra Eng., Commun. Comput.*, Jan. 2020. [Online]. Available: <https://doi.org/10.1007/s00200-019-00412-z>
- [17] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
- [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, J. Ahn, S. Yang, and Z.-A. Yao, "Complete weight enumerators of some linear codes and their applications," *Des., Codes Cryptogr.*, vol. 81, no. 1, pp. 153–168, Oct. 2016.

- [20] C. Li, Q. Yue, and F.-W. Fu, "A construction of several classes of two-weight and three-weight linear codes," *Applicable Algebra Eng., Commun. Comput.*, vol. 28, no. 1, pp. 11–30, Jan. 2017.
- [21] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
- [22] G. McGuire, "On three weights in cyclic codes with two zeros," *Finite Fields Their Appl.*, vol. 10, no. 1, pp. 97–104, Jan. 2004.
- [23] Q. Wang, F. Li, K. Ding, and D. Lin, "Complete weight enumerators of two classes of linear codes," *Discrete Math.*, vol. 340, no. 3, pp. 467–480, Mar. 2017.
- [24] Y. Wu, Q. Yue, X. Zhu, and S. Yang, "Weight enumerators of reducible cyclic codes and their dual codes," *Discrete Math.*, vol. 342, no. 3, pp. 671–682, Mar. 2019.
- [25] 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, Aug. 2015.
- [26] 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 Their Appl.*, vol. 44, pp. 76–91, Mar. 2017.
- [27] 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.
- [28] 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.
- [29] 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.
- [30] Z. Zhou, C. Ding, J. Luo, and A. Zhang, "A family of five-weight cyclic codes and their weight enumerators," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6674–6682, Oct. 2013.



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.

• • •