Cryptogr. Commun. (2017) 9:133–149
DOI 10.1007/s12095-016-0187-4

A class of three-weight linear codes and their complete weight enumerators

Shudi Yang[1,2] · Zheng-An Yao[1] · Chang-An Zhao[1]

Received: 8 January 2016 / Accepted: 8 April 2016 / Published online: 21 April 2016

Abstract Recently, linear codes constructed from defining sets have been investigated extensively and they have many applications. In this paper, for an odd prime p, we propose a class of p-ary linear codes by choosing a proper defining set. Their weight enumerators and complete weight enumerators are presented explicitly. Our results show that they are linear codes with three weights and suitable for the constructions of authentication codes and secret sharing schemes.

Keywords Linear code · Complete weight enumerator · Weight enumerator · Gauss sum · Gauss period

Mathematics Subject Classification (2010) 94B15 · 11T71

✉ Chang-An Zhao
zhaochan3@mail.sysu.edu.cn

Shudi Yang
yangshd3@mail2.sysu.edu.cn

Zheng-An Yao
mcsyao@mail.sysu.edu.cn

[1] Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, People's Republic of China

[2] School of Mathematical Sciences, Qufu Normal University, Shandong 273165, People's Republic of China

1 Introduction

Throughout this paper, let p be an odd prime and $r = p^m$ for an integer $m \geqslant 2$. Denote by $\mathbb{F}_r$ a finite field with r elements. An $[n, \kappa, \delta]$ linear code C over $\mathbb{F}_p$ is a κ-dimensional subspace of $\mathbb{F}_p^n$ with minimum distance δ (see [8, 27]).

Let A_i denote the number of codewords with Hamming weight i in a linear code C of length n. The weight enumerator of C is defined by $A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n$, where $A_0 = 1$. The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the weight distribution of the code C.

The complete weight enumerator of a code C over $\mathbb{F}_p$ enumerates the codewords according to the number of symbols of each kind contained in each codeword. Denote elements of the field by $\mathbb{F}_p = \{w_0, w_1, \cdots, w_{p-1}\}$, where $w_0 = 0$. For a vector $\mathsf{v} = (v_0, v_1, \cdots, v_{n-1}) \in \mathbb{F}_p^n$, the composition of v, denoted by $\mathrm{comp}(\mathsf{v})$, is defined as

$$\mathrm{comp}(\mathsf{v}) = (k_0, k_1, \cdots, k_{p-1}),$$

where k_j is the number of components $v_i (0 \leqslant i \leqslant n-1)$ of v that equal to w_j. It is easy to see that $\sum_{j=0}^{p-1} k_j = n$. Let $A(k_0, k_1, \cdots, k_{p-1})$ be the number of codewords $\mathsf{c} \in C$ with $\mathrm{comp}(\mathsf{c}) = (k_0, k_1, \cdots, k_{p-1})$. Then the complete weight enumerator of the code C is the polynomial

$$\begin{aligned} \mathrm{CWE}(C) &= \sum_{\mathsf{c} \in C} w_0^{k_0} w_1^{k_1} \cdots w_{p-1}^{k_{p-1}} \\ &= \sum_{(k_0, k_1, \cdots, k_{p-1}) \in B_n} A(k_0, k_1, \cdots, k_{p-1}) w_0^{k_0} w_1^{k_1} \cdots w_{p-1}^{k_{p-1}}, \end{aligned}$$

where $B_n = \left\{ (k_0, k_1, \cdots, k_{p-1}) : 0 \leqslant k_j \leqslant n, \sum_{j=0}^{p-1} k_j = n \right\}$.

The weight distributions of linear codes have been well studied in the literature (see [12, 16, 17, 26, 29, 31, 32, 35–38] and references therein). The information of the complete weight enumerators of linear codes is of vital use because they not only give the weight enumerators but also show the frequency of each symbol appearing in each codeword. Therefore, they have many applications. Blake and Kith investigated the complete weight enumerator of Reed-Solomon codes and showed that they could be helpful in soft decision decoding [4, 20]. In [18], the study of the monomial and quadratic bent functions was related to the complete weight enumerators of linear codes. It was illustrated by Ding et al. [10, 11] that complete weight enumerators can be applied to the calculation of the deception probabilities of certain authentication codes. In [6, 7, 13], the authors studied the complete weight enumerators of some constant composition codes and presented some families of optimal constant composition codes.

However, it is extremely difficult to evaluate the complete weight enumerators of linear codes in general and there is little information on this topic in the literature besides the above mentioned [4, 6, 7, 13, 20]. Kuzmin and Nechaev investigated the generalized Kerdock code and related linear codes over Galois rings and determined their complete weight enumerators in [21] and [22]. Further recent progress on the complete weight enumerators of linear codes can be found in [1, 2, 19, 23, 24, 33]. The results of [1] and [2] can be viewed as generalizations of [34] and [15], respectively. In [19, 23, 24, 33], the authors treated the complete weight enumerators of some linear or cyclic codes using exponential sums and Galois theory. Recently Tang et al. constructed linear codes with two or three weights from weakly regular bent functions in [30]. We shall extend this construction to non-bent functions.

The authors of [9, 14, 15] gave the generic construction of linear codes. Set $\bar{D} = \{d_1, d_2, \cdots, d_n\} \subseteq \mathbb{F}_r$. Denote by Tr the absolute trace function. A linear code associated with $\bar{D}$ is defined by

$$C_{\bar{D}} = \{(\mathrm{Tr}(ad_1), \mathrm{Tr}(ad_2), \cdots, \mathrm{Tr}(ad_n)) : a \in \mathbb{F}_r\}.$$

Then $\bar{D}$ is called the defining set of this code $C_{\bar{D}}$.

Motivated by the above construction and the idea of [30], we define linear codes C_D and C_{D_1} by

$$\begin{aligned} C_D &= \{(\mathrm{Tr}(ax^2))_{x \in D} : a \in \mathbb{F}_r\}, \\ C_{D_1} &= \{(\mathrm{Tr}(ax^2))_{x \in D_1} : a \in \mathbb{F}_r\}, \end{aligned} \tag{1}$$

where

$$\begin{aligned} D &= \{x \in \mathbb{F}_r^* : \mathrm{Tr}(x) \in Sq\}, \\ D_1 &= \{x \in \mathbb{F}_r^* : \mathrm{Tr}(x) \in Nsq\}, \end{aligned}$$

which are called defining sets. Here Sq and Nsq denote the set of all squares and nonsquares in $\mathbb{F}_p^*$, respectively. By definition, these codes have length $n = (p-1)p^{m-1}/2$ and dimension at most m. Further, we will demonstrate that C_D is equal to C_{D_1}. Actually, for a fixed $b \in Nsq$, there exists a mapping ϕ_b such that

$$\begin{aligned} \phi_b : D &\to D_1 \\ x &\mapsto bx \end{aligned}$$

which implies that $\mathrm{Tr}(a(\phi_b(x))^2) = \mathrm{Tr}(ab^2x^2)$ for all $x \in D$ and $a \in \mathbb{F}_r$. As a runs through $\mathbb{F}_r$, so does ab^2. This means they have the same codewords. Hence, we only describe all the information of C_D. In this paper, the complete weight enumerator of C_D is investigated by employing exponential sums and Gauss periods. This gives its weight enumerator immediately. As it turns out, this code is a three-weight linear code which will be of special interest in authentication codes [11] and secret sharing schemes [5].

The remainder of this paper is organized as follows. In Section 2, we describe the main results of this paper and give some examples. Section 3 briefly recalls some definitions and results on Gauss periods and Gauss sums, then proves the main results. Finally, Section 4 is devoted to conclusions.

2 Main results

In this section, we only introduce the complete weight enumerator and weight enumerator of C_D described in (1). The main results of this paper are presented below, whose proofs will be given in Section 3.

First of all, we establish the complete weight enumerator of C_D in the following three theorems, then we give some examples to illustrate these results.

Theorem 1 *Let $p \equiv 3 \mod 4$ and ρ, z be elements in $\mathbb{F}_p$. Then the code C_D defined by (1) is a $\left[\frac{p-1}{2}p^{m-1}, m\right]$ three-weight linear code and we have the following assertions.*

(i) *If m is even, then the complete weight enumerator of C_D is given by*

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

$$+\frac{p-1}{4}\left(p^{m-1}+p^{\frac{m-2}{2}}\right) w_0^{\frac{p-1}{2}\left(p^{m-2}-p^{\frac{m-2}{2}}\right)} \sum_{i\in\{1,-1\}} \prod_{\left(\frac{\rho}{p}\right)=i} w_\rho^{\frac{p-1}{2}p^{m-2}} \prod_{\left(\frac{z}{p}\right)=-i} w_z^{A_1}$$

$$+\frac{p-1}{4}\left(p^{m-1}-p^{\frac{m-2}{2}}\right) w_0^{\frac{p-1}{2}(p^{m-2}+p^{\frac{m-2}{2}})} \sum_{i\in\{1,-1\}} \prod_{\left(\frac{\rho}{p}\right)=i} w_\rho^{\frac{p-1}{2}p^{m-2}} \prod_{\left(\frac{z}{p}\right)=-i} w_z^{A_{-1}},$$

where, for $\varepsilon \in \{1, -1\}$,

$$A_\varepsilon = \frac{p-1}{2}p^{m-2} + \varepsilon p^{\frac{m-2}{2}}.$$

(ii) *If m is odd, then the complete weight enumerator of C_D is given by*

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

$$+\frac{p-1}{4}\left(p^{m-1}+p^{\frac{m-1}{2}}\right) w_0^{\frac{p-1}{2}\left(p^{m-2}-p^{\frac{m-3}{2}}\right)} \sum_{i\in\{1,-1\}} \prod_{\left(\frac{\rho}{p}\right)=i} w_\rho^{A_1} \prod_{\left(\frac{z}{p}\right)=-i} w_z^{B_1}$$

$$+\frac{p-1}{4}\left(p^{m-1}-p^{\frac{m-1}{2}}\right) w_0^{\frac{p-1}{2}\left(p^{m-2}+p^{\frac{m-3}{2}}\right)} \sum_{i\in\{1,-1\}} \prod_{\left(\frac{\rho}{p}\right)=i} w_\rho^{A_{-1}} \prod_{\left(\frac{z}{p}\right)=-i} w_z^{B_{-1}},$$

where, for $\varepsilon \in \{1, -1\}$,

$$\begin{aligned} A_\varepsilon &= \frac{p-1}{2}\left(p^{m-2} - \varepsilon p^{\frac{m-3}{2}}\right), \\ B_\varepsilon &= \frac{p-1}{2}p^{m-2} + \varepsilon\frac{p+1}{2}p^{\frac{m-3}{2}}. \end{aligned}$$

Example 1 (i) Let $(p, m) = (3, 5)$. Then by Theorem 1, the code C_D has parameters $[81, 5, 51]$ and complete weight enumerator

$$\begin{aligned} w_0^{81} &+ 36w_0^{30}w_1^{30}w_2^{21} + 36w_0^{30}w_1^{21}w_2^{30} + 80w_0^{27}w_1^{27}w_2^{27} \\ &+ 45w_0^{24}w_1^{33}w_2^{24} + 45w_0^{24}w_1^{24}w_2^{33}, \end{aligned}$$

which is confirmed by Magma. This is a three-weight linear code.

(ii) Let $(p, m) = (7, 2)$. Then by Theorem 1, the code C_D is a $[21, 2, 15]$ three-weight linear code with complete weight enumerator

$$\begin{aligned} w_0^{21} &+ 6(w_0w_1w_2w_3w_4w_5w_6)^3 + 9w_0^6(w_1w_2w_4)^3(w_3w_5w_6)^2 \\ &+ 9w_0^6(w_1w_2w_4)^2(w_3w_5w_6)^3 + 12(w_1w_2w_4)^4(w_3w_5w_6)^3 \\ &+ 12(w_1w_2w_4)^3(w_3w_5w_6)^4, \end{aligned}$$

which is confirmed by Magma.

Let $p \equiv 1 \mod 4$. For $i = 0, 1, 2, 3$, we denote the cyclotomic classes of order 4 in $\mathbb{F}_p$ by $C_i^{(4,p)}$, which is simplified as C_i in the sequel and defined in Section 3.1.

Theorem 2 *Let* $p \equiv 1 \mod 4$ *and* m *be odd. Then the code* C_D *of* (1) *is a* $\left[\frac{p-1}{2}p^{m-1}, m\right]$ *three-weight linear code with complete weight enumerator*

$$\begin{aligned} & w_0^{\frac{p-1}{2}p^{m-1}} + (p^{m-1}-1)\prod_{\rho\in\mathbb{F}_p} w_\rho^{\frac{p-1}{2}p^{m-2}} \\ & +\frac{p-1}{8}\left(p^{m-1}+p^{\frac{m-1}{2}}\right)\sum_{i=0}^{3} w_0^{\frac{p-1}{2}\left(p^{m-2}-p^{\frac{m-3}{2}}\right)}\prod_{\rho\in C_i} w_\rho^{A_1}\prod_{z\in\mathbb{F}_p^*\backslash C_i} w_z^{B_1} \\ & +\frac{p-1}{8}\left(p^{m-1}-p^{\frac{m-1}{2}}\right)\sum_{i=0}^{3} w_0^{\frac{p-1}{2}\left(p^{m-2}+p^{\frac{m-3}{2}}\right)}\prod_{\rho\in C_i} w_\rho^{A_{-1}}\prod_{z\in\mathbb{F}_p^*\backslash C_i} w_z^{B_{-1}}, \end{aligned}$$

where, for $\varepsilon \in \{1, -1\}$,

$$\begin{aligned} A_\varepsilon &= \frac{p-1}{2}p^{m-2} + \frac{\varepsilon}{2}\left(3p^{\frac{m-1}{2}} + p^{\frac{m-3}{2}}\right), \\ B_\varepsilon &= \frac{p-1}{2}p^{m-2} - \frac{\varepsilon}{2}\left(p^{\frac{m-1}{2}} - p^{\frac{m-3}{2}}\right). \end{aligned}$$

Example 2 Let $(p, m) = (5, 3)$. Then by Theorem 2, the code C_D is a three-weight linear code with parameters [50, 3, 38] and complete weight enumerator

$$\begin{aligned} w_0^{50} &+ 10(w_0w_1w_2w_3)^{12}w_4^2 + 10(w_0w_1w_2w_4)^{12}w_3^2 + 10(w_0w_1w_3w_4)^{12}w_2^2 \\ &+ 10(w_0w_2w_3w_4)^{12}w_1^2 + 24(w_0w_1w_2w_3w_4)^{10} + 15(w_0w_1w_2w_3)^8w_4^{18} \\ &+ 15(w_0w_1w_2w_4)^8w_3^{18} + 15(w_0w_1w_3w_4)^8w_2^{18} + 15(w_0w_2w_3w_4)^8w_1^{18}. \end{aligned}$$

These results coincide with numerical computation by Magma.

Theorem 3 *Let* $p \equiv 1 \mod 4$ *and* m *be even. Let* s *and* t *be defined by* $p = s^2 + t^2$, $s \equiv 1 \mod 4$. *Then the code* C_D *of* (1) *is a* $\left[\frac{p-1}{2}p^{m-1}, m\right]$ *three-weight linear code with complete weight enumerator*

$$\begin{aligned} & w_0^{\frac{p-1}{2}p^{m-1}} + (p^{m-1}-1)\prod_{\rho\in\mathbb{F}_p} w_\rho^{\frac{p-1}{2}p^{m-2}} \\ & +\frac{p-1}{8}\left(p^{m-1}+p^{\frac{m-2}{2}}\right)\sum_{i=0}^{3} w_0^{K_1}\prod_{\rho_0\in C_i} w_{\rho_0}^{L_1}\prod_{\rho_1\in C_{i+1}} w_{\rho_1}^{R_1}\prod_{\rho_2\in C_{i+2}} w_{\rho_2}^{S_1}\prod_{\rho_3\in C_{i+3}} w_{\rho_3}^{T_1} \\ & +\frac{p-1}{8}\left(p^{m-1}-p^{\frac{m-2}{2}}\right)\sum_{i=0}^{3} w_0^{K_{-1}}\prod_{\rho_0\in C_i} w_{\rho_0}^{L_{-1}}\prod_{\rho_1\in C_{i+1}} w_{\rho_1}^{R_{-1}}\prod_{\rho_2\in C_{i+2}} w_{\rho_2}^{S_{-1}}\prod_{\rho_3\in C_{i+3}} w_{\rho_3}^{T_{-1}}, \end{aligned}$$

Table 1 The weight distribution of C_D when m is even

Weight i	Frequency A_i
$\frac{(p-1)^2}{2}p^{m-2}$	$p^{m-1}-1$
$\frac{p-1}{2}\left((p-1)p^{m-2}+p^{\frac{m-2}{2}}\right)$	$\frac{p-1}{2}(p^{m-1}+p^{\frac{m-2}{2}})$
$\frac{p-1}{2}\left((p-1)p^{m-2}-p^{\frac{m-2}{2}}\right)$	$\frac{p-1}{2}(p^{m-1}-p^{\frac{m-2}{2}})$
0	1

where, for $\varepsilon \in \{1, -1\}$,

$$\begin{aligned} K_\varepsilon &= \frac{p-1}{2}(p^{m-2}-\varepsilon p^{\frac{m-2}{2}}), \\ L_\varepsilon &= \frac{p-1}{2}p^{m-2}+\varepsilon p^{\frac{m-2}{2}}(1+s), \\ R_\varepsilon &= \frac{p-1}{2}p^{m-2}-\varepsilon p^{\frac{m-2}{2}}t, \\ S_\varepsilon &= \frac{p-1}{2}p^{m-2}+\varepsilon p^{\frac{m-2}{2}}(1-s), \\ T_\varepsilon &= \frac{p-1}{2}p^{m-2}+\varepsilon p^{\frac{m-2}{2}}t. \end{aligned}$$

Example 3 Let $(p, m) = (5, 4)$. Then by Theorem 3, the code C_D has parameters $[250, 4, 190]$ and complete weight enumerator

$$\begin{aligned} w_0^{250} &+ 60w_0^{60}w_1^{60}w_2^{40}w_3^{50}w_4^{40} + 60w_0^{60}w_1^{50}w_2^{60}w_3^{40}w_4^{40} + 60w_0^{60}w_1^{40}w_2^{50}w_3^{40}w_4^{60} \\ &+ 60w_0^{60}w_1^{40}w_2^{40}w_3^{60}w_4^{50} + 124(w_0w_1w_2w_3w_4)^{50} + 65w_0^{40}w_1^{60}w_2^{60}w_3^{40}w_4^{50} \\ &+ 65w_0^{40}w_1^{60}w_2^{50}w_3^{60}w_4^{40} + 65w_0^{40}w_1^{50}w_2^{40}w_3^{60}w_4^{60} + 65w_0^{40}w_1^{40}w_2^{60}w_3^{50}w_4^{60}, \end{aligned}$$

which is verified by Magma. This is a three-weight linear code.

The following corollary gives the weight enumerator of C_D, which follows immediately from its complete weight enumerator.

Corollary 1 *The code C_D of* (1) *has the weight distribution given in* Table 1 *if m is even and* Table 2 *if m is odd.*

From Tables 1 and 2, we observe that the weights of C_D have a common divisor $(p-1)/2$. This implies that it can be punctured into a shorter code as follows.

Let $a \in Sq$. Note that $\mathrm{Tr}(ax) = a\mathrm{Tr}(x)$ for any $x \in \mathbb{F}_r$. This indicates that $\mathrm{Tr}(ax)$ is a square (nonsquare) in $\mathbb{F}_p^*$ if and only if $\mathrm{Tr}(x)$ is a square (nonsquare) in $\mathbb{F}_p^*$. Then we

Table 2 The weight distribution of C_D when m is odd

Weight i	Frequency A_i
$\frac{(p-1)^2}{2}p^{m-2}$	$p^{m-1}-1$
$\frac{p-1}{2}\left((p-1)p^{m-2}+p^{\frac{m-3}{2}}\right)$	$\frac{p-1}{2}(p^{m-1}+p^{\frac{m-1}{2}})$
$\frac{p-1}{2}\left((p-1)p^{m-2}-p^{\frac{m-3}{2}}\right)$	$\frac{p-1}{2}(p^{m-1}-p^{\frac{m-1}{2}})$
0	1

Table 3 The weight distribution of $C_{\tilde{D}}$ when m is even

Weight i	Frequency A_i
$(p-1)p^{m-2}$	$p^{m-1}-1$
$(p-1)p^{m-2}+p^{\frac{m-2}{2}}$	$\frac{p-1}{2}(p^{m-1}+p^{\frac{m-2}{2}})$
$(p-1)p^{m-2}-p^{\frac{m-2}{2}}$	$\frac{p-1}{2}(p^{m-1}-p^{\frac{m-2}{2}})$
0	1

can select a subset $\tilde{D}$ of the set D such that $\cup_{a\in Sq} a\tilde{D}$ is just a partition of D. Hence, the corresponding linear code $C_{\tilde{D}}$ is the punctured version of C_D. The following corollary states the parameters and weight distribution of $C_{\tilde{D}}$, which directly follows from Corollary 1.

Corollary 2 *The code $C_{\tilde{D}}$ is a $[p^{m-1}, m]$ three-weight linear code with the weight distribution given in* Table 3 *if m is even and* Table 4 *if m is odd.*

In the following, we give the punctured version $C_{\tilde{D}}$ of C_D from the previous examples.

Example 4 (i) Let $(p, m) = (5, 3)$. Then the code $C_{\tilde{D}}$ in Corollary 2 has parameters $[25, 3, 19]$ and weight enumerator

$$1 + 40z^{19} + 24z^{20} + 60z^{21}.$$

This code is almost optimal in the sense that the best known code over $\mathbb{F}_5$ of length 25 and dimension 3 has minimum distance 20 according to Markus Grassl's table (see http://www.codetables.de/).

(ii) Let $(p, m) = (7, 2)$. From Corollary 2, we know that $C_{\tilde{D}}$ has parameters $[7, 2, 5]$ and weight enumerator

$$1 + 18z^5 + 6z^6 + 24z^7.$$

This code is almost optimal since the best known code over $\mathbb{F}_7$ of length 7 and dimension 2 has minimum distance 6 according to Markus Grassl's table.

3 The proofs of the main results

3.1 Auxiliary results

In order to prove Theorems 1, 2 and 3 proposed in Section 2, we will use several results which are depicted and proved in the sequel. We start with cyclotomic classes and group characters.

Table 4 The weight distribution of $C_{\tilde{D}}$ when m is odd

Weight i	Frequency A_i
$(p-1)p^{m-2}$	$p^{m-1}-1$
$(p-1)p^{m-2}+p^{\frac{m-3}{2}}$	$\frac{p-1}{2}(p^{m-1}+p^{\frac{m-1}{2}})$
$(p-1)p^{m-2}-p^{\frac{m-3}{2}}$	$\frac{p-1}{2}(p^{m-1}-p^{\frac{m-1}{2}})$
0	1

Recall that $r = p^m$. Let α be a fixed primitive element of $\mathbb{F}_r$ and $r-1 = sN$, where s, N are two integers with $s > 1$ and $N > 1$. Define $C_i^{(N,r)} = \alpha^i \langle \alpha^N \rangle$ for $i = 0, 1, \cdots, N-1$, where $\langle \alpha^N \rangle$ denotes the subgroup of $\mathbb{F}_r^*$ generated by α^N. The cosets $C_i^{(N,r)}$ are called the *cyclotomic classes* of order N in $\mathbb{F}_r$.

For each $b \in \mathbb{F}_r$, let χ_b be an additive character of $\mathbb{F}_r$, which is defined by

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

where $\zeta_p = \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$ and Tr is the absolute trace function. Especially when $b = 1$, χ_1 is called the canonical additive character of $\mathbb{F}_r$. The orthogonal property of additive characters χ, which can be easily checked, is given by

$$\sum_{x \in \mathbb{F}_r} \chi(ax) = \begin{cases} r & \text{if } a = 0, \\ 0 & \text{if } a \in \mathbb{F}_r^*. \end{cases} \tag{2}$$

The Gauss periods of order N are defined by

$$\eta_i^{(N,r)} = \sum_{x \in C_i^{(N,r)}} \chi_1(x), i = 0, 1, \cdots, N-1.$$

Let λ be a multiplicative and χ an additive character of $\mathbb{F}_r$. Then the Gauss sum $G(\lambda, \chi)$ is defined by

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

Let η denote the quadratic character of $\mathbb{F}_r$. The associated Gauss sum $G(\eta, \chi_1)$ over $\mathbb{F}_r$ is denoted by $G(\eta)$. And the Gauss sum $G(\hat{\eta}, \hat{\chi}_1)$ over $\mathbb{F}_p$ is denoted by $G(\hat{\eta})$, where $\hat{\eta}$ and $\hat{\chi}_1$ are the quadratic character and canonical additive character of $\mathbb{F}_p$, respectively.

For each $y \in \mathbb{F}_p^*$, we have $\eta(y) = 1$ if $m \geqslant 2$ is even, and otherwise $\eta(y) = \hat{\eta}(y)$. Moreover, it is well known that $G(\eta) = (-1)^{m-1}\sqrt{p^*}^m$ and $G(\hat{\eta}) = \sqrt{p^*}$, where $p^* = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$. See [15, 25] for more information.

The following lemmas will be required in the sequel.

Lemma 1 *(See Theorem 5.30 of* [25]*) Let χ be a nontrivial additive character of $\mathbb{F}_r$, $k \in \mathbb{N}$, and λ a multiplicative character of $\mathbb{F}_r$ of order $d = \gcd(k, r-1)$. Then*

$$\sum_{x \in \mathbb{F}_r} \chi(ax^k + b) = \chi(b) \sum_{j=1}^{d-1} \bar{\lambda}^j(a) G(\lambda^j, \chi)$$

for any $a, b \in \mathbb{F}_r$ with $a \neq 0$, where $\bar{\lambda}$ denotes the conjugate character of λ.

For $\rho \in \mathbb{F}_p^*$ and $a \in \mathbb{F}_r$, in order to study the complete weight enumerator, we define

$$\begin{aligned} N_0(\rho) &= \#\{x \in \mathbb{F}_r : \mathrm{Tr}(x) = 0, \mathrm{Tr}(ax^2) = \rho\}, \\ N(\rho) &= \#\{x \in \mathbb{F}_r : \mathrm{Tr}(x) \in Sq, \mathrm{Tr}(ax^2) = \rho\}, \\ N_1(\rho) &= \#\{x \in \mathbb{F}_r : \mathrm{Tr}(x) \in Nsq, \mathrm{Tr}(ax^2) = \rho\}. \end{aligned}$$

The values of $N(\rho)$, $N_0(\rho)$ and $N_1(\rho)$, which depend mainly on the choice of a, are given in the following two lemmas.

Lemma 2 *([34]) Let $a \in \mathbb{F}_r^*$ and $\rho \in \mathbb{F}_p^*$. Then*

$$N_0(\rho) = \begin{cases} p^{m-2} + (-1)^{\frac{p-1}{2}\frac{m-1}{2}}\eta(a)\hat{\eta}(\rho)p^{\frac{m-1}{2}} & if\ m\ odd, \mathrm{Tr}(a^{-1}) = 0, \\ p^{m-2} - (-1)^{\frac{p-1}{2}\frac{m-1}{2}}\eta(a)\hat{\eta}(\mathrm{Tr}(a^{-1}))p^{\frac{m-3}{2}} & if\ m\ odd, \mathrm{Tr}(a^{-1}) \neq 0, \\ p^{m-2} + (-1)^{\frac{p-1}{2}\frac{m}{2}}\eta(a)p^{\frac{m-2}{2}} & if\ m\ even, \mathrm{Tr}(a^{-1}) = 0, \\ p^{m-2} - (-1)^{\frac{p-1}{2}\frac{m-2}{2}}\eta(a)\hat{\eta}(\rho\mathrm{Tr}(a^{-1}))p^{\frac{m-2}{2}} & if\ m\ even, \mathrm{Tr}(a^{-1}) \neq 0. \end{cases}$$

Lemma 3 *Let $a \in \mathbb{F}_r^*$ and $\rho \in \mathbb{F}_p^*$. Then we have the following assertion.*

$$\begin{aligned} & N(\rho) + N_1(\rho) \\ &= \begin{cases} p^{m-1} - p^{m-2} & if\ m\ even,\ \mathrm{Tr}(a^{-1}) = 0, \\ p^{m-1} - p^{m-2} & if\ m\ odd,\ \mathrm{Tr}(a^{-1}) = 0, \\ p^{m-1} - p^{m-2} + \eta(a)(-1)^{\frac{p-1}{2}\frac{m}{2}}p^{\frac{m-2}{2}}\left(1 + \hat{\eta}(-\rho\ \mathrm{Tr}(a^{-1}))\right) & if\ m\ even,\ \mathrm{Tr}(a^{-1}) \neq 0, \\ p^{m-1} - p^{m-2} + \eta(a)(-1)^{\frac{p-1}{2}\frac{m-1}{2}}p^{\frac{m-3}{2}}\left(\hat{\eta}(\rho)p + \hat{\eta}\ (\mathrm{Tr}(a^{-1}))\right) & if\ m\ odd,\ \mathrm{Tr}(a^{-1}) \neq 0. \end{cases} \end{aligned}$$

Proof Note that

$$N_0(\rho) + N(\rho) + N_1(\rho) = \#\{x \in \mathbb{F}_r : \mathrm{Tr}(ax^2) = \rho\},$$

where $\rho \in \mathbb{F}_p^*$. This leads to

$$N_0(\rho) + N(\rho) + N_1(\rho) = p^{m-1} + p^{-1}\sum_{z \in \mathbb{F}_p^*}\zeta_p^{-z\rho}\sum_{x \in \mathbb{F}_r}\zeta_p^{z\ \mathrm{Tr}(ax^2)}.$$

Applying Theorem 5.33 of [25], we can deduce that

$$\sum_{z \in \mathbb{F}_p^*}\sum_{x \in \mathbb{F}_r}\zeta_p^{z\ \mathrm{Tr}(ax^2) - z\rho} = \begin{cases} \eta(a)(-1)^{\frac{p-1}{2}\frac{m}{2}}p^{\frac{m}{2}} & \text{if } m \text{ even,} \\ \eta(a)\hat{\eta}(\rho)(-1)^{\frac{p-1}{2}\frac{m-1}{2}}p^{\frac{m+1}{2}} & \text{if } m \text{ odd.} \end{cases}$$

The desired conclusion then follows from Lemma 2. □

The following two lemmas will help us to determine the frequency of each composition in C_D.

Lemma 4 *([34]) For any $a \in \mathbb{F}_r^*$, let*

$$n_{i,j} = \#\{a \in \mathbb{F}_r^* : \eta(a) = i, \hat{\eta}(\mathrm{Tr}(a^{-1})) = j\}, \quad i, j \in \{1, -1\}. \tag{3}$$

(i) *If m is even, then we have*

$$n_{1,1} = n_{1,-1} = \frac{p-1}{4}\left(p^{m-1} + (-1)^{\frac{p-1}{2}\frac{m}{2}}p^{\frac{m-2}{2}}\right).$$

(ii) *If m is odd, then we have*

$$\begin{cases} n_{1,1} &= \frac{p-1}{4}\left(p^{m-1} + (-1)^{\frac{p-1}{2}\frac{m-1}{2}}p^{\frac{m-1}{2}}\right), \\ n_{1,-1} &= \frac{p-1}{4}\left(p^{m-1} - (-1)^{\frac{p-1}{2}\frac{m-1}{2}}p^{\frac{m-1}{2}}\right). \end{cases}$$

Lemma 5 *For any $a \in \mathbb{F}_r^*$, let $n_{i,j}$ be defined by (3).*

(i) *If m is even, then we have*

$$n_{-1,1}=n_{-1,-1}=\frac{p-1}{4}\left(p^{m-1}-(-1)^{\frac{p-1}{2}\frac{m}{2}}p^{\frac{m-2}{2}}\right).$$

(ii) *If m is odd, then we have*

$$\begin{cases} n_{-1,1} &= \frac{p-1}{4}\left(p^{m-1}-(-1)^{\frac{p-1}{2}\frac{m-1}{2}}p^{\frac{m-1}{2}}\right), \\ n_{-1,-1} &= \frac{p-1}{4}\left(p^{m-1}+(-1)^{\frac{p-1}{2}\frac{m-1}{2}}p^{\frac{m-1}{2}}\right). \end{cases}$$

Proof We point out that

$$n_{1,j}+n_{-1,j}=\#\{a\in\mathbb{F}_r^*:\hat{\eta}(\mathrm{Tr}(a^{-1}))=j\}=\frac{p-1}{2}p^{m-1},$$

with $j\in\{1,-1\}$.

The desired conclusion then follows from Lemma 4. □

Consider $p\equiv 1 \mod 4$. Recall that $\eta_i^{(4,p)}=\sum_{x\in C_i^{(4,p)}}\zeta_p^x$, where $C_i^{(4,p)}=\beta^i\langle\beta^4\rangle$ for $i=0,1,2,3$, and β is a primitive element of $\mathbb{F}_p$. In the sequel, we write $\eta_i^{(4,p)}$ and $C_i^{(4,p)}$ as η_i and C_i, respectively. The following lemma plays an important role in determining the complete weight enumerator, in which the value of η_0 coincides with the result of Theorem 4.2.4 of [3].

Lemma 6 *Let* $p\equiv 1 \mod 4$. *Let s and t be defined by* $p=s^2+t^2$, $s\equiv 1 \mod 4$. *The Gauss periods of order 4 over* $\mathbb{F}_p$ *are given as follows.*

(i) *If* $p\equiv 5 \mod 8$*, then*

$$\{\eta_0,\eta_2\}=\left\{\frac{\sqrt{p}-1}{4}\pm\frac{\sqrt{2}}{4}\sqrt{-\sqrt{p}s-p}\right\},$$

$$\{\eta_1,\eta_3\}=\left\{-\frac{\sqrt{p}+1}{4}\pm\frac{\sqrt{2}}{4}\sqrt{\sqrt{p}s-p}\right\}.$$

(ii) *If* $p\equiv 1 \mod 8$*, then*

$$\{\eta_0,\eta_2\}=\left\{\frac{\sqrt{p}-1}{4}\pm\frac{\sqrt{2}}{4}\sqrt{p-\sqrt{p}s}\right\},$$

$$\{\eta_1,\eta_3\}=\left\{-\frac{\sqrt{p}+1}{4}\pm\frac{\sqrt{2}}{4}\sqrt{p+\sqrt{p}s}\right\}.$$

Proof Let β be a primitive element of $\mathbb{F}_p$. According to [28], the Gauss sums G_i are given by

$$G_i=\sum_{x\in\mathbb{F}_p}\zeta_p^{\beta^i x^4},\ i=0,1,2,3,$$

and they are roots of a polynomial $F_4(X)$, i.e.,

$$F_4(X)=\prod_{i=0}^{3}(X-G_i),$$

which is called reduced (or modified) period polynomial. By Theorem 14 of [28] (see also Theorem 10.10.6 of [3]), we have

$$F_4(X) = \begin{cases} (X^2+3p)^2 - 4p(X-s)^2 & \text{if } p \equiv 5 \mod 8, \\ (X^2-p)^2 - 4p(X-s)^2 & \text{if } p \equiv 1 \mod 8, \end{cases}$$

where $p = s^2 + t^2$ with $s \equiv 1 \mod 4$.

In the following, we give the proof of the case $p \equiv 5 \mod 8$ since that of the case $p \equiv 1 \mod 8$ is similarly verified.

In the case of $p \equiv 5 \mod 8$, we have

$$F_4(X) = \left(X^2 + 3p - 2\sqrt{p}(X-s)\right)\left(X^2 + 3p + 2\sqrt{p}(X-s)\right).$$

Note that $\eta_0 + \eta_2 = \eta_0^{(2,p)} = \frac{1}{2}(\sqrt{p}-1)$ yields that $G_0 + G_2 = 2\sqrt{p}$, since $G_i = 4\eta_i + 1$. Hence, we see that G_0, G_2 are roots of

$$X^2 + 3p - 2\sqrt{p}(X-s) = 0.$$

Therefore, G_1, G_3 are roots of

$$X^2 + 3p + 2\sqrt{p}(X-s) = 0.$$

It is straightforward that

$$\begin{aligned} G_0 + G_2 &= 2\sqrt{p}, & G_0G_2 &= 3p + 2\sqrt{p}s, \\ G_1 + G_2 &= -2\sqrt{p}, & G_1G_3 &= 3p - 2\sqrt{p}s. \end{aligned}$$

Moreover, we obtain that

$$\begin{aligned} \eta_0\eta_2 &= \frac{1}{16}(3p + 1 - 2\sqrt{p}(1-s)), \\ \eta_1\eta_3 &= \frac{1}{16}(3p + 1 + 2\sqrt{p}(1-s)), \\ \eta_0^2 + \eta_2^2 &= \frac{1}{8}(1 - p - 2\sqrt{p}(1+s)), \\ \eta_1^2 + \eta_3^2 &= \frac{1}{8}(1 - p + 2\sqrt{p}(1+s)). \end{aligned}$$

Consequently, we have

$$\begin{aligned} (\eta_0 + \eta_2)^2 &= \tfrac{1}{4}(\sqrt{p}-1)^2, & (\eta_0 - \eta_2)^2 &= \frac{1}{2}(-\sqrt{p}s - p), \\ (\eta_1 + \eta_3)^2 &= \tfrac{1}{4}(\sqrt{p}+1)^2, & (\eta_1 - \eta_3)^2 &= \frac{1}{2}(\sqrt{p}s - p). \end{aligned}$$

The desired conclusions follow from the facts that $\eta_0 + \eta_2 = \frac{1}{2}(\sqrt{p}-1)$ and $\eta_0 + \eta_1 + \eta_2 + \eta_3 = -1$. □

3.2 The proof of Theorem 1

Observe that $a = 0$ gives the zero codeword and the contribution to the complete weight enumerator is w_0^n, where $n = \frac{p-1}{2}p^{m-1}$. This value occurs only once. Hence, we assume that $a \in \mathbb{F}_r^*$ for the rest of the proof.

For $\rho \in \mathbb{F}_p^*$, we consider

$$A = \sum_{x\in\mathbb{F}_r}\sum_{y\in\mathbb{F}_p}\zeta_p^{y^2\mathrm{Tr}(x)}\sum_{z\in\mathbb{F}_p}\zeta_p^{z\ \mathrm{Tr}(ax^2)-z\rho}.$$

Then, it is easy to see that

$$A = N_0(\rho)p^2 + (N(\rho)-N_1(\rho))p\sqrt{p^*}, \tag{4}$$

since

$$\sum_{y\in\mathbb{F}_p}\zeta_p^{y^2\mathrm{Tr}(x)} = \begin{cases} p & \text{if } \mathrm{Tr}(x)=0,\\ \sqrt{p^*} & \text{if } \mathrm{Tr}(x)\in Sq,\\ -\sqrt{p^*} & \text{if } \mathrm{Tr}(x)\in Nsq,\end{cases}$$

and

$$\sum_{z\in\mathbb{F}_p}\zeta_p^{z\ \mathrm{Tr}(ax^2)-z\rho} = \begin{cases} p & \text{if } \mathrm{Tr}(ax^2)=\rho,\\ 0 & \text{if } \mathrm{Tr}(ax^2)\neq\rho.\end{cases}$$

On the other hand, from Theorem 5.33 of [25] and (2), we get

$$\begin{aligned} A &= r + \sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_r}\zeta_p^{y^2\ \mathrm{Tr}(x)} + \sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_r}\zeta_p^{\mathrm{Tr}(azx^2+y^2x)}\\ &= r + \sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\sum_{y\in\mathbb{F}_p}\zeta_p^{\mathrm{Tr}(-\frac{y^4}{4az})}\eta(az)G(\eta)\\ &= r + \eta(a)G(\eta)\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(z)\sum_{y\in\mathbb{F}_p}\zeta_p^{-\frac{\mathrm{Tr}(a^{-1})}{4z}y^4}. \end{aligned} \tag{5}$$

In the following, we calculate the value A of (5) by distinguishing the cases of $\mathrm{Tr}(a^{-1}) = 0$ and $\mathrm{Tr}(a^{-1}) \neq 0$.

Case 1 $\mathrm{Tr}(a^{-1}) = 0$.

In this case, from (5), we know that

$$A = \begin{cases} r - p\eta(a)G(\eta) & \text{if } m \text{ even},\\ r + p\eta(a)\hat{\eta}(-\rho)G(\eta)G(\hat{\eta}) & \text{if } m \text{ odd},\end{cases}$$

which leads to $N(\rho) = N_1(\rho)$ compared with (4) and Lemma 2. It follows from Lemma 3 that $N(\rho) = \frac{p-1}{2}p^{m-2}$. This value occurs $p^{m-1}-1$ times.

Case 2 $\mathrm{Tr}(a^{-1}) \neq 0$.

Recall that $p \equiv 3 \mod 4$. Thus, $\gcd(4, p-1) = 2$. From (5) and Lemma 1, we have

$$\begin{aligned} A &= r + \eta(a)G(\eta)\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(z)\hat{\eta}\left(-\frac{\mathrm{Tr}(a^{-1})}{4z}\right)G(\hat{\eta}) \\ &= r + \eta(a)G(\eta)\hat{\eta}(-\mathrm{Tr}(a^{-1}))\sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(z)\hat{\eta}(z)G(\hat{\eta}) \\ &= \begin{cases} r + \eta(a)\hat{\eta}(\rho\,\mathrm{Tr}(a^{-1}))G(\eta)G(\hat{\eta})^2 & \text{if } m \text{ even,} \\ r - \eta(a)\hat{\eta}(-\mathrm{Tr}(a^{-1}))G(\eta)G(\hat{\eta}) & \text{if } m \text{ odd,} \end{cases} \end{aligned}$$

which also leads to $N(\rho) = N_1(\rho)$ from (4) and Lemma 2. It then follows from Lemma 3 that

$$N(\rho) = \begin{cases} \frac{p-1}{2}p^{m-2} & \text{if } \hat{\eta}(\rho\,\mathrm{Tr}(a^{-1})) = 1 \\ \frac{p-1}{2}p^{m-2} + \eta(a)(-1)^{\frac{m}{2}}p^{\frac{m-2}{2}} & \text{if } \hat{\eta}(\rho\,\mathrm{Tr}(a^{-1})) = -1 \end{cases}$$

for even m, and otherwise,

$$N(\rho) = \frac{p-1}{2}p^{m-2} + \frac{1}{2}\eta(a)(-1)^{\frac{m-1}{2}}p^{\frac{m-3}{2}}(p\hat{\eta}(\rho) + \hat{\eta}(\mathrm{Tr}(a^{-1}))).$$

Note that $N(0) = \frac{p-1}{2}p^{m-1} - \sum_{\rho\in\mathbb{F}_p^*}N(\rho)$. The desired conclusion then follows from Lemmas 4 and 5.

This completes the proof of Theorem 1.

3.3 The proof of Theorem 2

By the proof of Theorem 1, we only need to consider the case $\mathrm{Tr}(a^{-1}) \neq 0$ with $a \in \mathbb{F}_r^*$, since the cases of $a = 0$ and $\mathrm{Tr}(a^{-1}) = 0$ have already been determined. For this purpose, we write (5) as

$$A = r + \eta(a)G(\eta)B, \tag{6}$$

where

$$B = \sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\eta(z)\sum_{y\in\mathbb{F}_p}\zeta_p^{-\frac{\mathrm{Tr}(a^{-1})}{4z}y^4}. \tag{7}$$

Let notations be as aforementioned and $p \equiv 1 \mod 4$. When $\mathrm{Tr}(a^{-1}) \neq 0$, the value B of (7) can be determined by

$$\begin{aligned} B &= \sum_{z\in\mathbb{F}_p^*}\zeta_p^{-z\rho}\hat{\eta}(z)\left(4\eta_{-\frac{\mathrm{Tr}(a^{-1})}{4z}} + 1\right) \\ &= \left(\sum_{z\in C_0} + \sum_{z\in C_2} - \sum_{z\in C_1} - \sum_{z\in C_3}\right)4\zeta_p^{-z\rho}\eta_{-\frac{\mathrm{Tr}(a^{-1})}{4z}} + \hat{\eta}(-\rho)G(\hat{\eta}) \\ &= \left(\sum_{z\in C_0} + \sum_{z\in C_2} - \sum_{z\in C_1} - \sum_{z\in C_3}\right)4\zeta_p^{-z\rho}\eta_{-\frac{\mathrm{Tr}(a^{-1})}{4z}} + \hat{\eta}(\rho)\sqrt{p}, \end{aligned} \tag{8}$$

since m is odd. By (4), (6), and Lemma 3, we have

$$\begin{cases} N(\rho)+N_1(\rho) = p^{m-1}-p^{m-2}+\eta(a)p^{\frac{m-3}{2}}\left(\hat{\eta}(\rho)p+\hat{\eta}(\mathrm{Tr}(a^{-1}))\right), \\ N(\rho)-N_1(\rho) = \eta(a)\left(\hat{\eta}(\mathrm{Tr}(a^{-1}))p^{\frac{m-2}{2}}+p^{\frac{m-3}{2}}B\right). \end{cases} \tag{9}$$

Now, we assume that $p \equiv 5 \mod 8$.

Clearly, -1 and 4 are both in C_2. In the following, the value B of (8) will be computed according to the choices of $\mathrm{Tr}(a^{-1})$ and ρ.

Case 1 $\mathrm{Tr}(a^{-1}) \in C_0$, $\rho \in C_0$.

In this case, by Lemma 6 and (8), we obtain

$$B = 4\left(2\eta_0\eta_2-\eta_1^2-\eta_3^2\right)+\sqrt{p} = 2p-\sqrt{p}.$$

It follows from (9) that

$$\begin{aligned} N(\rho) &= \frac{p-1}{2}p^{m-2}+\frac{1}{2}\eta(a)\left(3p^{\frac{m-1}{2}}+p^{\frac{m-3}{2}}\right), \\ N_1(\rho) &= \frac{p-1}{2}p^{m-2}-\frac{1}{2}\eta(a)\left(p^{\frac{m-1}{2}}-p^{\frac{m-3}{2}}\right). \end{aligned}$$

Case 2 $\mathrm{Tr}(a^{-1}) \in C_0$, $\rho \in C_1$.

In this case, we deduce that

$$B = 4(\eta_3\eta_0+\eta_1\eta_2-\eta_0\eta_3-\eta_2\eta_1)-\sqrt{p} = -\sqrt{p},$$

which indicates that

$$N(\rho) = N_1(\rho) = \frac{p-1}{2}p^{m-2}-\frac{1}{2}\eta(a)\left(p^{\frac{m-1}{2}}-p^{\frac{m-3}{2}}\right).$$

Case 3 $\mathrm{Tr}(a^{-1}) \in C_0$, $\rho \in C_2$.

In this case, we have

$$B = 4\left(\eta_0^2+\eta_2^2-2\eta_1\eta_3\right)+\sqrt{p} = -2p-\sqrt{p},$$

which gives that

$$\begin{aligned} N(\rho) &= \frac{p-1}{2}p^{m-2}-\frac{1}{2}\eta(a)\left(p^{\frac{m-1}{2}}-p^{\frac{m-3}{2}}\right), \\ N_1(\rho) &= \frac{p-1}{2}p^{m-2}+\frac{1}{2}\eta(a)\left(3p^{\frac{m-1}{2}}+p^{\frac{m-3}{2}}\right). \end{aligned}$$

Case 4 $\mathrm{Tr}(a^{-1}) \in C_0$, $\rho \in C_3$.

In this case, we obtain

$$B = 4(\eta_1\eta_0+\eta_3\eta_2-\eta_2\eta_3-\eta_0\eta_1)-\sqrt{p} = -\sqrt{p}.$$

As a consequence, we get

$$N(\rho) = N_1(\rho) = \frac{p-1}{2}p^{m-2}-\frac{1}{2}\eta(a)\left(p^{\frac{m-1}{2}}-p^{\frac{m-3}{2}}\right).$$

Moreover, for $\mathrm{Tr}(a^{-1}) \in C_0$, the number of a satisfying $\eta(a) = 1$ is

$$\#\{a \in \mathbb{F}_r^* : \eta(a) = 1, \mathrm{Tr}(a^{-1}) \in C_0\} = \frac{1}{2} n_{1,1} = \frac{p-1}{8} \left(p^{m-1} + p^{\frac{m-1}{2}}\right),$$

by Lemma 4. In a similar way, the number of a satisfying $\eta(a) = -1$ is

$$\#\{a \in \mathbb{F}_r^* : \eta(a) = -1, \mathrm{Tr}(a^{-1}) \in C_0\} = \frac{1}{2} n_{-1,1} = \frac{p-1}{8} \left(p^{m-1} - p^{\frac{m-1}{2}}\right),$$

by Lemma 5.

There are sixteen cases all together to be considered. Other cases can be similarly calculated, which are omitted here.

Note that the case of $p \equiv 1 \mod 8$ can be analyzed in an analogous fashion. The proof of Theorem 2 is finished.

3.4 The proof of Theorem 3

This proof is similar to that of Theorem 2 by observing that

$$B = \left(\sum_{z \in C_0} + \sum_{z \in C_1} + \sum_{z \in C_2} + \sum_{z \in C_3} \right) 4 \zeta_p^{-z\rho} \eta_{-\frac{\mathrm{Tr}(a^{-1})}{4z}} - 1,$$

from (7), since m is even. Thus, we omit the details here.

4 Concluding remarks

Inspired by the original ideas of [15, 30], we constructed a class of three-weight linear codes. By employing some mathematical tools, we presented explicitly their complete weight enumerators and weight enumerators. Their punctured codes contain some almost optimal codes. By Theorem 1, it is easy to check that

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

for $m \geqslant 4$. Here w_{min} and w_{max} denote the minimum and maximum nonzero weights in C_D, respectively. Therefore, the code C_D can be used for secret sharing schemes with interesting access structures. We also mention that the complete weight enumerators, presented in Theorems 1, 2 and 3, can be applied to compute the deception probabilities of certain authentication codes constructed from linear codes. Furthermore, if r is large enough, these authentication codes are asymptotically optimal. See [11, 15, 23].

Note that $\gcd(4, p-1) = 4$ if $p \equiv 1 \mod 4$. This implies that we can prove Theorems 2 and 3 with a similar method used in Section 3.2. One can see that it works well though it is indeed very complicated. However, we gave a simpler proof by employing Gauss periods to determine the complete weight enumerator of C_D for the case of $p \equiv 1 \mod 4$.

To conclude this paper, we remark that the codes proposed in this paper can be extended to a more general case, that is, for an integer $t \geqslant 2$, define

$$C_{D'} = \left\{ \left(\mathrm{Tr}(a_1 x_1^2 + \cdots + a_t x_t^2) \right)_{(x_1, \cdots, x_t) \in D} : a_1, \cdots, a_t \in \mathbb{F}_r \right\},$$

where

$$D' = \left\{ (x_1, \cdots, x_t) \in \mathbb{F}_r^t : \mathrm{Tr}(x_1 + \cdots + x_t) \in Sq \right\}.$$

For this kind of linear codes, it will be interesting to settle their complete weight enumerators.

Acknowledgments The authors are very grateful to the editor and the three anonymous referees for their useful comments and important suggestions, which have improved the presentation of this paper. The work of Zheng-An Yao is partially supported by the NSFC (Grant No.11271381), the NSFC (Grant No.11431015) and China 973 Program (Grant No. 2011CB808000). The work of Chang-An Zhao is partially supported by the NSFC (Grant No. 61472457). This work is also partially supported by Guangdong Natural Science Foundation (Grant No. 2014A030313161).

References

1. Ahn, J., Ka, D., Li, C.: Complete weight enumerators of a class of linear codes, preprint (2016)
2. Bae, S., Li, C., Yue, Q.: Some results on two-weight and three-weight linear codes, preprint (2015)
3. Berndt, B.C., Evans, R.J., Williams, K.S.: Gauss and Jacobi Sums. Wiley, New York (1998)
4. Blake, I.F., Kith, K.: On the complete weight enumerator of Reed-Solomon codes. SIAM J. Discret. Math. **4**(2), 164–171 (1991)
5. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089–2102 (2005)
6. Chu, W., Colbourn, C.J., Dukes, P.: On constant composition codes. Discret. Appl. Math. **154**(6), 912–929 (2006)
7. Ding, C.: Optimal constant composition codes from zero-difference balanced functions. IEEE Trans. Inf. Theory **54**(12), 5766–5770 (2008)
8. Ding, C.: Codes from Difference Sets. World Scientific, Singapore (2015)
9. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015)
10. Ding, C., Helleseth, T., Klove, T., Wang, X.: A generic construction of Cartesian authentication codes. IEEE Trans. Inf. Theory **53**(6), 2229–2235 (2007)
11. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**(1), 81–99 (2005)
12. Ding, C., Yang, J.: Hamming weights in irreducible cyclic codes. Discret. Math. **313**(4), 434–446 (2013)
13. Ding, C., Yin, J.: A construction of optimal constant composition codes. Des. Codes Crypt. **40**(2), 157–165 (2006)
14. Ding, K., Ding, C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014)
15. Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory **61**(11), 5835–5842 (2015)
16. Dinh, H.Q., Li, C., Yue, Q.: Recent progress on weight distributions of cyclic codes over finite fields. J. Algebra Comb. Discret. Struct. Appl. **2**(1), 39–63 (2015)
17. Feng, K., Luo, J.: Weight distribution of some reducible cyclic codes. Finite Fields Appl. **14**(2), 390–409 (2008)
18. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
19. Heng, Z., Yue, Q.: Complete weight distributions of two classes of cyclic codes. Cryptogr. Commun. (2016). doi:10.1007/s12095-015-0177-y
20. Kith, K.: Complete weight enumeration of Reed-Solomon codes. Master's thesis, Department of Electrical and Computing Engineering, University of Waterloo, Waterloo (1989)
21. Kuzmin, A., Nechaev, A.: Complete weight enumerators of generalized Kerdock code and linear recursive codes over Galois ring. In: Workshop on coding and cryptography, pp. 333–336 (1999)
22. Kuzmin, A., Nechaev, A.: Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring. Discret. Appl. Math. **111**(1), 117–137 (2001)
23. Li, C., Bae, S., Ahn, J., Yang, S., Yao, Z.A.: Complete weight enumerators of some linear codes and their applications. Des. Codes Crypt. (2015). doi:10.1007/s10623-015-0136-9
24. Li, C., Yue, Q., Fu, F.W.: Complete weight enumerators of some cyclic codes. Des. Codes Crypt. (2015). doi:10.1007/s10623-015-0091-5
25. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, vol. 20. Addison-Wesley, Reading (1983)

26. Luo, J., Feng, K.: On the weight distributions of two classes of cyclic codes. IEEE Trans. Inf. Theory **54**(12), 5332–5344 (2008)
27. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes, vol. 16. North-Holland Publishing, Amsterdam (1977)
28. Myerson, G.: Period polynomials and Gauss sums for finite fields. Acta Arith. **39**(3), 251–264 (1981)
29. Sharma, A., Bakshi, G.K.: The weight distribution of some irreducible cyclic codes. Finite Fields Appl. **18**(1), 144–159 (2012)
30. Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166–1176 (2016)
31. Vega, G.: The weight distribution of an extended class of reducible cyclic codes. IEEE Trans. Inf. Theory **58**(7), 4862–4869 (2012)
32. Wang, B., Tang, C., Qi, Y., Yang, Y., Xu, M.: The weight distributions of cyclic codes and elliptic curves. IEEE Trans. Inf. Theory **58**(12), 7253–7259 (2012)
33. Wang, Q., Li, F., Ding, K., Lin, D.: Complete weight enumerators of two classes of linear codes. arXiv:1512.07341 (2015)
34. Yang, S., Yao, Z.A.: Complete weight enumerators of a family of three-weight linear codes. Des. Codes Crypt. (2016). doi:10.1007/s10623-016-0191-x
35. Yu, L., Liu, H.: The weight distribution of a family of p-ary cyclic codes. Des. Codes Crypt. (2014). doi:10.1007/s10623-014-0029-3
36. Yuan, J., Carlet, C., Ding, C.: The weight distribution of a class of linear codes from perfect nonlinear functions. IEEE Trans. Inf. Theory **52**(2), 712–717 (2006)
37. Zheng, D., Wang, X., Yu, L., Liu, H.: The weight enumerators of several classes of p-ary cyclic codes. Discret. Math. **338**(7), 1264–1276 (2015)
38. Zhou, Z., Ding, C., Luo, J., Zhang, A.: A family of five-weight cyclic codes and their weight enumerators. IEEE Trans. Inf. Theory **59**(10), 6674–6682 (2013)