Discrete Mathematics 340 (2017) 729–739

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Complete weight enumerators of a class of linear codes[☆]

Shudi Yang[a,b], Zheng-An Yao[c,*]

[a] *Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, PR China*
[b] *School of Mathematical Sciences, Qufu Normal University, Shandong 273165, PR China*
[c] *School of Mathematics, Sun Yat-sen University, Guangzhou 510275, PR China*

ARTICLE INFO

Article history:
Received 2 July 2016
Received in revised form 28 October 2016
Accepted 24 November 2016
Available online 27 December 2016

Keywords:
Linear code
Complete weight enumerator
Gauss sum

ABSTRACT

Recently, linear codes constructed from defining sets have been studied extensively. They may have a few weights if the defining set is chosen properly. Let m and t be positive integers. For an odd prime p, let $r = p^m$ and Tr be the absolute trace function from $\mathbb{F}_r$ to $\mathbb{F}_p$. In this paper, for $b \in \mathbb{F}_p^*$, we define $D_b = \left\{(x_1, \ldots, x_t) \in \mathbb{F}_r^t : \mathrm{Tr}\,(x_1 + \cdots + x_t) = b\right\}$, and determine the complete weight enumerator of a class of p-ary linear codes given by

$$C_{D_b} = \{\mathsf{c}(a_1, a_2, \ldots, a_t) : a_1, \ldots, a_t \in \mathbb{F}_r\},$$

where

$$\mathsf{c}(a_1, a_2, \ldots, a_t) = (\mathrm{Tr}\,(a_1 x_1^2 + \cdots + a_t x_t^2))_{(x_1, \ldots, x_t) \in D_b}.$$

Then we get their weight enumerators explicitly, which will give us several linear codes with a few weights. As a generalization of Wang et al. (arXiv:1512.03866), this paper extends the result of Ahn et al. (2016).

1. Introduction

Throughout this paper, let $r = p^m$ for an odd prime p and a positive integer m. Denote by $\mathbb{F}_r$ a finite field with r elements. 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 (see [19]). Denote elements of the field by $\mathbb{F}_p = \{z_0, z_1, \ldots, z_{p-1}\}$, where $z_0 = 0$. For a vector $\mathsf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_p^n$, the composition of v, denoted by $\mathrm{comp}(\mathsf{v})$, is defined as

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

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

☆ 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 is also partially supported by the NSFC (Grant No. 61472457) and Guangdong Natural Science Foundation (Grant No. 2014A030313161).

* Corresponding author.
E-mail addresses: yangshudi7902@126.com (S. Yang), mcsyao@mail.sysu.edu.cn (Z. Yao).

http://dx.doi.org/10.1016/j.disc.2016.11.029
0012-365X/

enumerator of the code C is the polynomial

$$\begin{aligned}\mathrm{CWE}(C) &= \sum_{\mathrm{c}\in C} z_0^{k_0} z_1^{k_1}\cdots z_{p-1}^{k_{p-1}}\\ &= \sum_{(k_0,k_1,\ldots,k_{p-1})\in B_n} A(k_0,k_1,\ldots,k_{p-1}) z_0^{k_0} z_1^{k_1}\cdots z_{p-1}^{k_{p-1}},\end{aligned}$$

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

The complete weight enumerators of linear codes are of vital use because they not only give the weight enumerators but also show the frequency of each symbol appearing in each codeword. Blake and Kith investigated the complete weight enumerator of Reed–Solomon codes and showed that they could be helpful in soft decision decoding [2,13]. Kuzmin and Nechaev investigated the generalized Kerdock code and related linear codes over Galois rings and determined their complete weight enumerators in [14] and [15]. In [12], the study of the monomial and quadratic bent functions was related to the complete weight enumerators of linear codes. Recently, a lot of progress has been made on this subject. Ding et al. [9,10] showed that complete weight enumerators can be applied to the calculation of the deception probabilities of certain authentication codes. In [4,5,11], the authors studied the complete weight enumerators of some constant composition codes and presented some families of optimal constant composition codes.

We introduce the generic construction of linear codes developed by Ding et al. in [6–8]. Set $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathbb{F}_r$, where $r = p^m$. Denote by Tr the absolute trace function. A linear code associated with D is defined by

$$C_D = \{(\mathrm{Tr}\,(ax))_{x\in D} : a \in \mathbb{F}_r\}.$$

Then D is called the defining set of this code C_D. Along this line, a great deal of research is devoted to the computation of the complete weight enumerators and weight enumerators of specific codes, see [1,16,17,21,22,25]. In [8], the code C_D with two or three weights was proposed with $D = \{x \in \mathbb{F}_r^* : \mathrm{Tr}\,(x^2) = 0\}$, and its complete weight enumerator was established in [16,23]. If $D = \{x \in \mathbb{F}_r^* : \mathrm{Tr}\,(x) = 0\}$, Yang and Yao [24] presented the complete weight enumerator of $C_D = \{(\mathrm{Tr}\,(ax^2))_{x\in D} : a \in \mathbb{F}_r\}$. If $D = \{x \in \mathbb{F}_r^* : \mathrm{Tr}\,(x) = b \neq 0\}$, Wang, Li and Lin [22] studied its weight enumerator. We mention that the result of [24] was generalized by Ahn, Ka and Li [1] considering $D = \left\{(x_1, \ldots, x_t) \in \mathbb{F}_r^t \setminus \{(0, \ldots, 0)\} : \mathrm{Tr}\,(x_1 + \cdots + x_t) = 0\right\}$ and

$$C_D = \{\mathrm{c}(a_1, a_2, \ldots, a_t) : a_1, \ldots, a_t \in \mathbb{F}_r\}, \tag{1}$$

where

$$\mathrm{c}(a_1, a_2, \ldots, a_t) = (\mathrm{Tr}\,(a_1x_1^2 + \cdots + a_tx_t^2))_{(x_1,\ldots,x_t)\in D}. \tag{2}$$

In this paper, for $b \in \mathbb{F}_p^*$, we define

$$D_b = \left\{(x_1, \ldots, x_t) \in \mathbb{F}_r^t : \mathrm{Tr}\,(x_1 + \cdots + x_t) = b\right\},$$

and examine the corresponding code C_{D_b} defined by (1) and (2). This work is strongly inspired by the above construction. Actually, the code C_{D_b} is equal to C_{D_1}, which will be shown later. Therefore, if the context is clear, we may write D_1 as D, and then investigate the code C_D. To be precise, we present explicitly its complete weight enumerator and obtain several linear codes with a few weights, which may have many applications in association schemes [3] and secret sharing schemes [8]. In this paper, we extend the main result of Ahn, Ka and Li [1]. Also notice that this is a generalization of [22] where the case $t = 1$ was settled. In addition, some examples are included to illustrate our results.

2. Mathematical foundations

We begin with cyclotomic classes and Gaussian periods over finite fields. Recall that $r = p^m$. Let α be a primitive element of $\mathbb{F}_r$ and $r - 1 = sN$ for two positive integers $s > 1, N > 1$. The *cyclotomic classes* of order N in $\mathbb{F}_r$ are the cosets $C_i^{(N,r)} = \alpha^i\langle\alpha^N\rangle$ for $i = 0, 1, \ldots, N-1$, where $\langle\alpha^N\rangle$ denotes the subgroup of $\mathbb{F}_r^*$ generated by α^N. We know that $\#C_i^{(N,r)} = \frac{r-1}{N}$.

Set $\zeta_p = \exp\left(\frac{2\pi\sqrt{-1}}{p}\right)$. Then Gaussian periods of order N are defined by

$$\eta_i^{(N,r)} = \sum_{x\in C_i^{(N,r)}} \zeta_p^{\mathrm{Tr}\,(x)},$$

where Tr is the absolute trace function from $\mathbb{F}_r$ to $\mathbb{F}_p$.

If λ is a multiplicative character of $\mathbb{F}_r^*$, then we can define Gauss sum $G(\lambda)$ over $\mathbb{F}_r$ as

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

Next, let us review some results on Gaussian periods and Gauss sums.