Discrete Mathematics 340 (2017) 467–480

Contents lists available at ScienceDirect

Discrete Mathematics

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

Complete weight enumerators of two classes of linear codes[☆]

Qiuyan Wang[a,c], Fei Li[b,*], Kelan Ding[c], Dongdai Lin[c]

[a] School of Computer Science and Software Engineering, Tianjin Polytechnic University, Tianjin 300387, China
[b] School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu City, 233000, Anhui Province, China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China

ARTICLE INFO

Article history:
Received 3 January 2016
Received in revised form 15 August 2016
Accepted 6 September 2016
Available online 16 November 2016

Keywords:
Linear codes
Complete weight enumerator
Gauss sum

ABSTRACT

Recently, linear codes with a few weights have been constructed and extensively studied. In this paper, for an odd prime p, we determine the complete weight enumerator of two classes of p-ary linear codes constructed from defining set. Our results show that the codes have at most seven weights and may have applications in secret sharing schemes.

1. Introduction

Throughout this article p denotes an odd prime and assume $q = p^e$ for some positive integer e. Let $\mathbb{F}_p$ and $\mathbb{F}_q$ denote the finite field with p and q elements, respectively. Let α be a natural number and $d = \gcd(\alpha, e)$. We denote by Tr the absolute trace function and use $\mathbb{F}_q^*$ to denote the multiplicative group of $\mathbb{F}_q$.

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 [19]. Let A_i be the number of codewords of weight i in $\mathcal{C}$ of length n. The (Hamming) weight enumerator of $\mathcal{C}$ is defined by [19]

$$1 + A_1x + A_2x^2 + \cdots + A_nx^n.$$

The list A_i $(0 \le i \le n)$ is called the weight distribution or weight spectrum of $\mathcal{C}$. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzeros A_i with $1 \le i \le n$ is equal to t. Clearly, the minimum distance of $\mathcal{C}$ can be derived from the weight distribution of the code $\mathcal{C}$. For error detection and error correction algorithms [21], the weight distribution of a code can be applied to compute the error probability of error detection and correction. Thus, weight distribution is a significant research topic in coding theory and was studied in [2,4,5,8–10,12,13,17,29,30,34,35].

For a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \subseteq \mathbb{F}_p^n$, the complete weight enumerator of $\mathbf{c}$ is the monomial

$$w(\mathbf{c}) = w_0^{t_0} w_1^{t_1} \cdots w_{p-1}^{t_{p-1}}$$

in the variables $w_0, w_1, \ldots, w_{p-1}$, where t_i $(0 \le i \le p-1)$ denotes the number of components c_j $(0 \le j \le n-1)$ of $\mathbf{c}$ that equals i. Then the complete weight enumerator of the linear code $\mathcal{C}$ is the homogeneous polynomial

$$\mathrm{CWE}(\mathcal{C}) = \sum_{\mathbf{c} \in \mathcal{C}} w(\mathbf{c})$$

of degree n (see [27,28]).

[☆] This work is supported by a National Key Basic Research Project of China (2011CB302400), National Science Foundation of China (61379139), the "Strategic Priority Research Program" of the Chinese Academy of Sciences, Grant No. XDA06010701 and Foundation of NSSFC (No. 13CTJ006).

[*] Corresponding author.

E-mail addresses: wangyan198801@163.com (Q. Wang), cczxlf@163.com (F. Li), dingkelan@iie.ac.cn (K. Ding), ddlin@iie.ac.cn (D. Lin).

http://dx.doi.org/10.1016/j.disc.2016.09.003
0012-365X/© 2016 Elsevier B.V. All rights reserved.

Table 1
The weight distribution of the codes of Theorem 2.

Weight w	Multiplicity A
0	1
$(p-1)p^{e-2}$	$p^{e-1}-(p-1)p^{m-1}-1$
$(p-1)(p^{e-2}-p^{m-1})$	$(p-1)(p^{e-1}+p^{m-1})$

By definition, the complete weight enumerators of binary linear codes are just the weight enumerators. For nonbinary linear codes, the (Hamming) weight enumerators can be obtained from the complete weight enumerators. Furthermore, the complete weight enumerators are closely related to the deception probability of some authentication codes constructed from linear codes [14], and used to compute the Walsh transform of monomial functions over finite fields [18]. Thus, a great deal of research is devoted to the computation of the complete weight distribution of specific codes [1,3,20,22–24].

Let $\mathbb{F}_q$ be the finite field with q elements and $D=\{d_1,d_2,\dots,d_n\}$ be a nonempty subset of $\mathbb{F}_q$. A generic construction of linear codes over $\mathbb{F}_p$ is given by

$$\mathcal{C}_D=\{\mathbf{c}_x=(\mathrm{Tr}(xd_1),\mathrm{Tr}(xd_2),\dots,\mathrm{Tr}(xd_n)):x\in\mathbb{F}_q\},\tag{1.1}$$

where Tr denotes the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_p$ [26]. The set D is called the *defining set* of $\mathcal{C}_D$. This construction technique is employed in many papers to get linear codes with a few weights. The readers are referred to [11,15,25,31,35] for more information.

Naturally, a generalization of the code $\mathcal{C}_D$ of (1.1) is defined by [32]

$$\overline{\mathcal{C}}_D=\{(\mathrm{Tr}(xd_1)+u,\mathrm{Tr}(xd_2)+u,\dots,\mathrm{Tr}(xd_n)+u):u\in\mathbb{F}_p,\ x\in\mathbb{F}_q\}.\tag{1.2}$$

The objective of this paper is to present linear codes over $\mathbb{F}_p$ with at most seven weights using the above two construction methods. Moreover, the complete weight enumerators of the two proposed linear codes are also calculated. The codes in this paper may have applications in authentication codes [16], secret sharing schemes [33] and consumer electronics.

2. The main results

In this section, we only present the p-ary linear codes and introduce their parameters. The proofs of their parameters will be given later.

In this paper, for $a\in\mathbb{F}_p$, the defining set is given by

$$D_a=\{x\in\mathbb{F}_q^*:\mathrm{Tr}(x^{p^\alpha+1})=a\},\tag{2.1}$$

where α is any natural number. It should be remarked that, for $p=2$, the weight enumerator of $\mathcal{C}_{D_0}$ of (1.1) has been determined in [11]. Thus, we assume that p is an odd prime in this paper.

Lemma 1 *([6], Lemma 2.6).* *Let $d=\gcd(\alpha,e)$ and p be odd. Then*

$$\gcd(p^\alpha+1,p^e-1)=\begin{cases}2, & \text{if } e/d \text{ is odd},\\ p^d+1, & \text{if } e/d \text{ is even}.\end{cases}$$

Note that $\gcd(p^\alpha+1,p^e-1)=2$ leads to

$$\{x^{p^\alpha+1}:x\in\mathbb{F}_q^*\}=\{x^2:x\in\mathbb{F}_q^*\}$$

which means that

$$\begin{aligned}D_0&=\{x\in\mathbb{F}_q^*:\mathrm{Tr}(x^{p^\alpha+1})=0\}\\&=\{x\in\mathbb{F}_q^*:\mathrm{Tr}(x^2)=0\}.\end{aligned}$$

By Lemma 1, if e/d is odd, the code $\mathcal{C}_{D_0}$ of (1.1) and the code $\mathcal{C}_D$ in [12] are the same. Hence, we will assume e/d is even and $e=2m$ for a positive integer m. The main results of this paper are given below.

Theorem 2. *Let $m\ge 2$. If $m/d\equiv 1 \bmod 2$, then the code $\mathcal{C}_{D_0}$ of (1.1) is a $[p^{e-1}-(p-1)p^{m-1}-1,e]$ linear code with the weight distribution in Table 1 and its complete weight enumerator is*

$$w_0^{p^{e-1}-(p-1)p^{m-1}-1}+\left(p^{e-1}-(p-1)p^{m-1}-1\right)w_0^{p^{e-2}-(p-1)p^{m-1}-1}\prod_{i=1}^{p-1}w_i^{p^{e-2}}$$
$$+(p-1)(p^{e-1}+p^{m-1})w_0^{p^{e-2}-1}\prod_{i=1}^{p-1}w_i^{p^{e-2}-p^{m-1}}.$$