Finite Fields and Their Applications 48 (2017) 196–226

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A construction of linear codes and their complete weight enumerators ☆

Shudi Yang [a,b,*], Xiangli Kong [a], Chunming Tang [c]

[a] *School of Mathematical Sciences, Qufu Normal University, Shandong 273165, PR China*
[b] *Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, PR China*
[c] *School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, PR China*

A R T I C L E   I N F O

Article history:
Received 19 January 2017
Received in revised form 2 July 2017
Accepted 1 August 2017
Available online xxxx
Communicated by Pascale Charpin

MSC:
94B15
11T71

Keywords:
Linear code
Complete weight enumerator
Gauss sum
Cyclotomic number

A B S T R A C T

Recently, linear codes constructed from defining sets have been studied extensively. They may have excellent parameters if the defining set is chosen properly. Let $m > 2$ be a positive integer. For an odd prime p, let $r = p^m$ and Tr be the absolute trace function from $\mathbb{F}_r$ onto $\mathbb{F}_p$. In this paper, we give a construction of linear codes by defining the code

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

where $D = \{x \in \mathbb{F}_r : \mathrm{Tr}(x) = 1, \mathrm{Tr}(x^2) = 0\}$. Its complete weight enumerator and weight enumerator are determined explicitly by employing cyclotomic numbers and Gauss sums. However, we find that the code is optimal with respect to the Griesmer bound provided that $m = 3$. In fact, it is MDS when $m = 3$. Moreover, the codes presented have higher rate compared with other codes, which enables them to have

☆ This work is partially supported by China Postdoctoral Science Foundation funded Project (Project No. 2017M611801). This work is also partially supported by the Open Project Program of the Key Lab of Information Security, Guangzhou University (Grant No. GDXXAQ2016-08) and the Natural Science Foundation of Shandong Province of China (ZR2016AM04).

* Corresponding author at: School of Mathematical Sciences, Qufu Normal University, Shandong 273165, PR China.

E-mail addresses: yangshudi7902@126.com (S. Yang), kongxiangli@126.com (X. Kong), ctang@gzhu.edu.cn (C. Tang).

http://dx.doi.org/10.1016/j.ffa.2017.08.001
1071-5797/

essential applications in areas such as association schemes and secret sharing schemes.

1. Introduction

Throughout this paper, let p be an odd prime, and let $r = p^m$ for a positive integer $m > 2$. Denote by $\mathbb{F}_r$ a finite field with r elements. The absolute trace function is denoted by Tr. An $[n, k, d]$ linear code C over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum distance d. The fraction k/n is called the rate, or information rate, and gives a measure of the number of information coordinates relative to the total number of coordinates. The higher the rate, the higher the proportion of coordinates in a codeword actually contain information rather than redundancy (see [1]). The complete weight enumerator of a code C over $\mathbb{F}_p$, will enumerate the codewords according to the number of symbols of each kind contained in each codeword (see [2]). Denote elements of the field by $\mathbb{F}_p = \{z_0, z_1, \cdots, z_{p-1}\}$, where $z_0 = 0$. 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 z_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

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

where $B_n = \{(k_0, k_1, \cdots, k_{p-1}) : 0 \leqslant k_j \leqslant n, \sum_{j=0}^{p-1} k_j = n\}$. One sees that the key to determining $\mathrm{CWE}(C)$ of a code C is determining those $\mathrm{comp}(\mathsf{c})$ and $A(k_0, k_1, \cdots, k_{p-1})$ such that $A(k_0, k_1, \cdots, k_{p-1}) \neq 0$.

The complete weight enumerators of linear codes have been of fundamental importance to theories and practices since they not only give the weight enumerators but also demonstrate 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 [3,4]. Kuzmin and Nechaev studied the generalized Kerdock code and related linear codes over Galois rings and estimated their complete weight enumerators in [5] and [6]. Nebe et al. [7] described the complete weight