ARTICLE IN PRESS

Discrete Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Mathematics

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

Complete weight enumerators of a class of linear codes with two weights

Guangkui Xu [a,b,*], Xiwang Cao [b,c], Shanding Xu [b,d], Jingshui Ping [a]

[a] Department of Applied Mathematics, Huainan Normal University, Huainan 232038, China
[b] Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[d] Department of Mathematics and Physics, Nanjing Institute of Technology, Nanjing 210016, China

ARTICLE INFO

Article history:
Received 16 February 2017
Received in revised form 2 July 2017
Accepted 18 September 2017
Available online xxxx

Keywords:
Complete weight enumerators
Linear codes
Authentication codes
Secret sharing schemes

ABSTRACT

In this paper, a class of p-ary linear codes with two weights is constructed by using the properties of cyclotomic classes of $\mathbb{F}_{p^2}^*$. The complete weight enumerators of these linear codes are also determined. In some cases, they are optimal and can be employed to obtain secret sharing schemes with interesting access structures and asymptotically optimal systematic authentication codes.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

Let p be an odd prime and $q = p^{2m}$ for a positive integer m. Let $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$. An $[n, k, d]$ linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d. The *weight enumerator* of $\mathcal{C}$ is the polynomial

$$1 + A_1 z^1 + A_2 z^2 + \cdots + A_n z^n,$$

where A_i is the number of codewords of weight i. The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the *weight distribution* of the code $\mathcal{C}$. It is well known that the weight distribution gives the minimum distance of the code and contains important information for estimating the probability of error detection and correction. Information on the weight distribution of linear codes can be found in [9,15,21,34,25,26]. A t-weight code is a code $\mathcal{C}$ for which $|\{i | i \neq 0 \text{ and } A_i \neq 0\}| = t$. Linear codes with a few weights have been extensively investigated because of their importance in secret sharing schemes [33], authentication codes [11] and strongly regular graphs [5].

Let us denote $\mathbb{F}_p = \{f_0, f_1, \ldots, f_{p-1}\}$, where $f_0 = 0$. The complete weight enumerator $w[\mathbf{c}]$ of a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_p^n$ is defined as

$$w[\mathbf{c}] = f_0^{t_0} f_1^{t_1} \cdots f_{p-1}^{t_{p-1}},$$

* Corresponding author at: Department of Applied Mathematics, Huainan Normal University, Huainan 232038, China.
E-mail addresses: xuguangkuiy@163.com (G. Xu), xwcao@nuaa.edu.cn (X. Cao), sdxzx11@163.com (S. Xu), kepuduolong@163.com (J. Ping).

https://doi.org/10.1016/j.disc.2017.09.021
0012-365X/© 2017 Elsevier B.V. All rights reserved.

Please cite this article in press as: G. Xu, et al., Complete weight enumerators of a class of linear codes with two weights, Discrete Mathematics (2017), https://doi.org/10.1016/j.disc.2017.09.021.

where t_i is the number of coordinates of $\mathbf{c}$ equal to f_i. Obviously, $\sum_{i=0}^{p-1} t_i = n$. The complete weight enumerator of a code $\mathcal{C}$ is the polynomial

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

It is clear that the ordinary weight enumerators of binary linear codes are just the complete weight enumerators and the weight enumerators of nonbinary linear codes can follow directly from their complete weight enumerators. Determining the complete weight enumerators of linear codes is an interesting topic. Blake and Kith [4] proved that the complete weight enumerators of Reed–Solomon codes could be helpful in soft decision decoding. In [11,10], the authors used the complete weight enumerator to calculate the deception probabilities of certain authentication codes. In [12,6], Ding et al. constructed some families of optimal constant composition codes whose complete weight enumerators have one term. In general, determining the complete weight enumerator of a given linear code is not an easy task and there are only a few papers [1,19,3,20,22,31,32,18] that involved this topic.

Let s be a divisor of $2m$. The trace function from $\mathbb{F}_{p^{2m}}$ onto its subfield $\mathbb{F}_{p^s}$ is denoted by $\mathrm{Tr}_s^{2m}(x)$. The absolute trace function (i.e., for $s = 1$) is simply denoted by $\mathrm{Tr}(x)$. For a subset $D = \{d_1, d_2, \ldots, d_n\}$ of $\mathbb{F}_q$, we can define a linear code $\mathcal{C}_D$ of length n over $\mathbb{F}_p$ by

$$\mathcal{C}_D = \{\mathbf{c}_b = (\mathrm{Tr}(bd_1), \mathrm{Tr}(bd_2), \ldots, \mathrm{Tr}(bd_n)) \mid b \in \mathbb{F}_q\}, \tag{1}$$

and call D the *defining set* of this code $\mathcal{C}_D$. This construction technique can generate many classes of known codes with a few weights by selecting the suitable defining set D [13,14,7,24,30,27–29,35].

Let $h \geq 2$ be an integer and e be the least positive integer satisfying $p^e \equiv -1 \pmod h$. Li and Yue [21] gave the value distribution of Walsh transform of the monomial $f(x) = \mathrm{Tr}(ax^{\frac{p^{2em}-1}{h}})$ for $a \in \mathbb{F}^*_{p^{2em}}$ in terms of the Gauss sums and Gauss periods. By calculating the values of some Gauss periods, Heng and Yue [17] constructed two classes of two-weight binary or ternary linear codes from the monomial $f(x) = \mathrm{Tr}(x^{\frac{p^{2em}-1}{h}})$ for small values of h. In this paper, we generalize some results of Heng and Yue [17] to p-ary linear codes with two weights where p is an arbitrary odd prime. The proofs of our main results are based on a discussion of cyclotomic classes without the values of Gauss periods. To investigate the complete weight enumerators of linear codes obtained in this paper, a crucial problem is to determine in which cyclotomic class of $\mathbb{F}^*_{p^2}$ the elements of $\mathbb{F}^*_p$ are. This approach is quite different from the previous ones in [17]. In addition, two-weight codes obtained here can be used to construct systematic authentication codes [11,8] and secret sharing schemes with interesting access structures [33].

2. Preliminaries

In this section, we state some introduction of characters, Gauss periods and Gauss sums.

Let F_r be the finite field with r elements. An *additive character* of $\mathbb{F}_r$ is a homomorphism from $\mathbb{F}_r$ into the multiplicative group of complex numbers of absolute value 1. For each $u \in \mathbb{F}_r$, we can define an additive character of $\mathbb{F}_r$ as follows:

$$\psi_u(x) = \zeta_p^{\mathrm{Tr}(ux)},$$

where $\zeta_p = e^{2\pi\sqrt{-1}/p}$ is the pth primitive root of unity. The character ψ_1, denoted by ψ, is called the *canonical additive character* of $\mathbb{F}_r$.

Let $\lambda : \mathbb{F}_r^* \to \mathbb{C}^*$ be a multiplicative character of $\mathbb{F}_r^*$. *Gauss sums* over $\mathbb{F}_r$ is defined by

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

The following two lemmas will be used to determine the complete weight distributions of the proposed linear codes in the sequel.

Lemma 1 ([23, Theorem 5.15]). *Let F_r be a finite field with $r = p^s$ and η be the quadratic multiplicative character of F_r. Then*

$$G(\eta, \psi) = \begin{cases} (-1)^{s-1}\sqrt{r} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{s-1}(\sqrt{-1})^s\sqrt{r} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Lemma 2 ([23, Theorem 5.33]). *Let $r = p^s$ and $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_r[x]$ with $a_2 \neq 0$. Then*

$$\sum_{x\in\mathbb{F}_r} \psi(f(x)) = \psi(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G(\eta, \psi).$$

Download English Version:

https://daneshyari.com/en/article/8903128

Download Persian Version:

https://daneshyari.com/article/8903128

Daneshyari.com