Finite Fields and Their Applications 45 (2017) 183–202

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The weight distribution of a class of cyclic codes containing a subclass with optimal parameters ☆

Fengwei Li [a], Qin Yue [b,c,d,*], Fengmei Liu [e]

[a] *School of Mathematics and Statistics, Zaozhuang University, Zaozhuang, 277160, PR China*
[b] *Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, PR China*
[c] *State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, PR China*
[d] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, PR China*
[e] *Science and Technology on Information Assurance Laboratory, Beijing, 100072, PR China*

ARTICLE INFO

Article history:
Received 7 December 2015
Received in revised form 22 December 2016
Accepted 24 December 2016
Available online xxxx
Communicated by Jacques Wolfmann

MSC:
94B15
11T71
11T24

Keywords:
Weight distribution
Gauss sum
Cyclic code

ABSTRACT

Let α be a primitive element of a finite field $\mathbb{F}_r$, where $r = q^{m_1 m_2}$ and $\gcd(m_1, m_2) = d$, so $\alpha_1 = \alpha^{\frac{r-1}{q^{m_1}-1}}$ and $\alpha_2 = \alpha^{\frac{r-1}{q^{m_2}-1}}$ are primitive elements of $\mathbb{F}_{q^{m_1}}$ and $\mathbb{F}_{q^{m_2}}$, respectively. Let e be a positive integer such that $\gcd(e, \frac{q^{m_2}-1}{q^d-1}) = 1$, $\mathbb{F}_{q^{m_2}} = \mathbb{F}_q(\alpha_2^e)$, and α_1 and α_2^e are not conjugates over $\mathbb{F}_q$. We define a cyclic code

$$\mathcal{C} = \{c(a,b) : a \in \mathbb{F}_{q^{m_1}}, b \in \mathbb{F}_{q^{m_2}}\},$$

$$c(a,b) = (\mathrm{T}_1(a\alpha_1^i) + \mathrm{T}_2(b\alpha_2^{ei}))_{i=0}^{n-1},$$

where T_i denotes the trace function from $\mathbb{F}_{q^{m_i}}$ to $\mathbb{F}_q$ for $i = 1, 2$. In this paper, we use Gauss sums to investigate the weight distribution of $\mathcal{C}$, which generalizes the results of C. Li and Q. Yue in [13,14]. Furthermore, we explicitly determine the weight distribution of $\mathcal{C}$ if $d = 1, 2$. Moreover, we prove it is

☆ The paper is supported by National Natural Science Foundation of China (No. 11601475) and Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-15-009).
* Corresponding author.
E-mail addresses: lfwzzu@126.com (F. Li), yueqin@nuaa.edu.cn (Q. Yue), lfmei@sina.com (F. Liu).

http://dx.doi.org/10.1016/j.ffa.2016.12.004

optimal three-weight achieving the Griesmer bound if $d = 1$ and $\gcd(m_2 - em_1, q - 1) = 1$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^s$, p is a prime and s is a positive integer. Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_q$, i.e., it is a l-dimensional subspace of $\mathbb{F}_q^n$. If for each codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathcal{C}$, then we call $\mathcal{C}$ a cyclic code. We identify a codeword $(c_0, c_1, \ldots, c_{n-1})$ in $\mathcal{C}$ with the polynomial $c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}$ in $\mathbb{F}_q[x]/\langle x^n-1\rangle$. A code $\mathcal{C}$ of length n over $\mathbb{F}_q$ corresponds to a subset of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then $\mathcal{C}$ is a cyclic code if and only if the corresponding subset is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Note that every ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is principal. Hence $\mathcal{C} = \langle g(x)\rangle$, where $g(x)$ is a monic divisor of $x^n - 1$ over $\mathbb{F}_q$. In fact, $g(x)$ is called the generator polynomial and that $h(x) = (x^n - 1)/g(x)$ is referred to the parity-check polynomial of $\mathcal{C}$.

Let A_i be the number of codewords with Hamming weight i in the code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by

$$1 + A_1z + A_2z^2 + \cdots + A_nz^n.$$

The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of the code $\mathcal{C}$. In coding theory it is often desirable to know the weight distributions of the codes because they can be used to estimate the error correcting capability and the error probability of error detection and correction with respect to some algorithms. The weight distributions of cyclic codes have been studied for many years and are known in some cases. The weight distributions of irreducible cyclic codes have been extensively studied and for details we refer the readers to [5] and references therein. However, the problem of determining the weight distributions of cyclic codes turns out to be very difficult in general and is only settled for a few special cases in literature.

The weight distributions of cyclic codes have been extensively investigated for many years and are known in some cases [1,2,4,6,14,15,17,20–22,25–28]. Cyclic codes with few nonzero weights are of special interest in association schemes, secret sharing schemes, and frequency hopping sequences. The results of such cyclic codes were presented in [7,9,10,13,16,18,19,23,24].

In this paper, we shall assume that m_1, m_2 are positive integers with $d = \gcd(m_1, m_2)$ and e is a positive integer with $\gcd(e, \frac{q^{m_2}-1}{q^d-1}) = 1$. Let α be a primitive element of $\mathbb{F}_r$, $r = q^{m_1m_2}$, then $\alpha_1 = \alpha^{\frac{r-1}{q^{m_1}-1}}$ and $\alpha_2 = \alpha^{\frac{r-1}{q^{m_2}-1}}$ are primitive elements of $\mathbb{F}_{q^{m_1}}$ and $\mathbb{F}_{q^{m_2}}$, respectively. Furthermore, let α_1 and α_2^e be not conjugates over $\mathbb{F}_q$ and $\mathbb{F}_q(\alpha_2^e) = \mathbb{F}_{q^{m_2}}$.