Finite Fields and Their Applications 35 (2015) 78–85

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A note on the weight distribution of some cyclic codes

Liren Lin [a,*], Bocong Chen [b], Hongwei Liu [c]

[a] *Department of Physical Science and Technology, Central China Normal University, Wuhan, Hubei, 430079, China*
[b] *School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore, 637616, Singapore*
[c] *School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China*

ARTICLE INFO

Article history:
Received 25 June 2014
Received in revised form 4 March 2015
Accepted 5 March 2015
Available online 1 April 2015
Communicated by Anne Canteaut

MSC:
94B05
94B15

Keywords:
Cyclic code
Weight distribution
Generating idempotent
Finite field

ABSTRACT

Let $\mathbb{F}_q$ be the finite field with q elements and C_n be the cyclic group of order n, where n is a positive integer relatively prime to q. Let H, K be subgroups of C_n such that H is a proper subgroup of K. In this note, the weight distributions of the cyclic codes of length n over $\mathbb{F}_q$ with generating idempotents $\hat{K}$ and $e_{H,K} = \hat{H} - \hat{K}$ are explicitly determined, where $\hat{K} = 1/|K| \sum_{g \in K} g$ and $\hat{H} = 1/|H| \sum_{g \in H} g$. Our result naturally gives a new characterization of a theorem by Sharma and Bakshi [18] that determines the weight distribution of all irreducible cyclic codes of length p^m over $\mathbb{F}_q$, where p is an odd prime and q is a primitive root modulo p^m. Finally, two examples are presented to illustrate our results.

* Corresponding author.
E-mail addresses: L_R_Lin86@163.com (L. Lin), bocong_chen@yahoo.com (B. Chen), hwliu@mail.ccnu.edu.cn (H. Liu).

http://dx.doi.org/10.1016/j.ffa.2015.03.003
1071-5797/

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q and n be a positive integer relatively prime to q. A linear code C of length n over $\mathbb{F}_q$ is called *cyclic* if it is an ideal of the semisimple group algebra $\mathcal{R} = \mathbb{F}_q C_n$, where $C_n = \langle x \rangle$ is the cyclic group of order n. An element e of $\mathcal{R}$ satisfying $e^2 = e$ is called an *idempotent*. It is well known that each cyclic code of length n over $\mathbb{F}_q$ contains a unique idempotent which generates the code. This idempotent is called the *generating idempotent* of the cyclic code. A cyclic code is said to be *irreducible* if its generating idempotent is primitive (e.g. see [10, Ch. 4]). Irreducible cyclic codes are also known as minimal cyclic codes, which have been studied by many authors (e.g. see [1,2,9,12,15–18]).

Every row vector $a = (a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_q^n$ is identified with an element $\sum_{j=0}^{n-1} a_j x^j \in \mathcal{R}$. The *Hamming weight* of a, denoted by $wt(a)$, is the number of nonzero components of a. For a cyclic code C, the *Hamming weight* of C is defined as the smallest Hamming weight of nonzero codewords of C. Furthermore, the sequence $(A_0 = 1, A_1, \cdots, A_n)$ is called the *Hamming weight distribution* of C (weight distribution of C for short), where A_j denotes the number of codewords of Hamming weight j in C. Although the Hamming weight distribution does not completely specify a code, they provide important information on estimating the error correcting capability and the probability of error detection. The weight distribution of cyclic codes has been a hot subject of study. Different methods are employed to determine the specific weight distribution of cyclic codes, including the use of pseudorandom sequence, Gauss sums, Gauss periods, Gröbner basis and so on (e.g. see [3–8,11,13,17–23]). However, as mentioned in [23], the problem of determining the weight distribution of cyclic codes turns out to be very difficult in general and is only settled for a few special cases in literature.

Sharma and Bakshi in [18] determined the weight distribution of all irreducible cyclic codes of length p^m over $\mathbb{F}_q$, where p is an odd prime different from the characteristic of the field and q is a primitive root modulo p^m. The proof for [18, Theorem 2] is long, requiring several nontrivial lemmas, and the hardest part of the paper [18]. In this note, using an idea from [14], we extend this theorem to a more general setting. To be more specific, let H, K be subgroups of C_n such that H is a proper subgroup of K, i.e. H is a subgroup of K with $H \neq K$. The weight distributions of the cyclic codes of length n over $\mathbb{F}_q$ with generating idempotents

$$\hat{K} = \frac{1}{|K|} \sum_{g \in K} g \quad \text{and} \quad e_{H,K} = \hat{H} - \hat{K} = \frac{1}{|H|} \sum_{g \in H} g - \frac{1}{|K|} \sum_{g \in K} g \tag{1.1}$$

are explicitly determined, which yields a new characterization of [18, Theorem 2] in the sense that our result appears to be more compact and simple. Our main result is given as follows:

Theorem 1.1. *Let C_n be the cyclic group of order n with subgroups H and K, where n is a positive integer relatively prime to q and H is a proper subgroup of K. Let $\mathcal{R} = \mathbb{F}_q C_n$,*