Finite Fields and Their Applications 40 (2016) 126–137

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Several classes of optimal ternary cyclic codes with minimal distance four

Lisha Wang [a], Gaofei Wu [b,*]

[a] *Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu, 610031, China*
[b] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China*

ARTICLE INFO

Article history:
Received 30 July 2015
Received in revised form 13 January 2016
Accepted 28 March 2016
Available online 25 April 2016
Communicated by Chaoping Xing

MSC:
94B15
11T71

Keywords:
Cyclic codes
Linear codes
Optimal codes
Sphere packing bound

ABSTRACT

In this paper, by analyzing the solutions of certain equations over $\mathbb{F}_{3^m}$, we present four classes of optimal ternary cyclic codes with parameters $[3^m-1, 3^m-1-2m, 4]$. It is shown that some recent work on this class of optimal ternary cyclic codes are special cases of our results.

1. Introduction

Throughout this paper, let $q = p^m$ be a power of a prime, where p is a prime and m is a positive integer. Denote the finite field of q elements by $\mathbb{F}_{p^m}$. An $[n, k, d]$ linear

* Corresponding author.
E-mail addresses: wangtaolisha@163.com (L. Wang), wugf@nipc.org.cn (G. Wu).

http://dx.doi.org/10.1016/j.ffa.2016.03.007
1071-5797/

code over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d. An $[n,k]$ *cyclic* code $\mathcal{C}$ is an $[n,k]$ linear code with the property that any cyclic shift of a codeword is another codeword of $\mathcal{C}$. Let $\gcd(n,p)=1$. By identifying any codeword $(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$ with

$$c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}\in\mathbb{F}_p[x]/(x^n-1),$$

any cyclic code of length n over $\mathbb{F}_p$ corresponds to an ideal of the polynomial ring $\mathbb{F}_p[x]/(x^n-1)$. It is well known that every ideal of $\mathbb{F}_p[x]/(x^n-1)$ is principal. Thus, any cyclic code can be expressed as $\langle g(x)\rangle$, where $g(x)$ is monic and has the least degree. The polynomial $g(x)$ is called the *generator polynomial* and $h(x)=(x^n-1)/g(x)$ is called the *parity-check polynomial* of $\mathcal{C}$. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by

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

Cyclic codes are an important subclass of linear codes. Due to their efficient encoding and decoding algorithms [2,7,12], cyclic codes have many applications in consumer electronics, data storage systems, and communication systems. The reader is referred to [1,3,5,6,9,10,13–16] for some recent work on cyclic codes. In 2013, Ding and Helleseth [4] constructed several classes of optimal ternary cyclic codes with parameters $[3^m-1,3^m-1-2m,4]$ by using almost perfect nonlinear monomials and some other monomials over $\mathbb{F}_{3^m}$. Nine open problems about this class of optimal ternary cyclic codes were also proposed in [4]. By analyzing irreducible factors of certain polynomials with low degrees over finite fields, one of the open problems was solved by Li et al. [11]. In [11], the authors also presented several classes of optimal cyclic codes with parameters $[3^m-1,3^m-1-2m,4]$ and $[3^m-1,3^m-2-2m,5]$.

In this paper, we will present several new classes of optimal ternary cyclic codes with parameters $[3^m-1,3^m-1-2m,4]$ by analyzing the solutions of certain equations over $\mathbb{F}_{3^m}$. It will be shown that some previous results about this class of optimal ternary cyclic codes given in [4,11] are special cases of our results.

2. Preliminaries

Let α be a generator of $\mathbb{F}_{3^m}^*=\mathbb{F}_{3^m}\setminus\{0\}$ and $m_{\alpha^i}(x)$ be the minimal polynomial of α^i over $\mathbb{F}_3$. For any $1\le e\le 3^m-1$, let $\mathcal{C}_{(1,e)}$ denote the cyclic code over $\mathbb{F}_3$ with generator polynomial $m_\alpha(x)m_{\alpha^e}(x)$, where e is not in the 3-cyclotomic coset modulo 3^m-1 containing 1.

For a prime p, the p-cyclotomic coset modulo p^m-1 containing j is defined as

$$C_j=\{j\cdot p^s \bmod (p^m-1): s=0,1,\cdots,m-1\}.$$