Finite Fields and Their Applications 45 (2017) 237–263

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The dimension and minimum distance of two classes of primitive BCH codes ☆

Cunsheng Ding [a], Cuiling Fan [b,*], Zhengchun Zhou [b]

[a] Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China
[b] School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China

A R T I C L E I N F O

Article history:
Received 12 May 2016
Received in revised form 18 November 2016
Accepted 16 December 2016
Available online xxxx
Communicated by Chaoping Xing

MSC:
94B15
11T71

Keywords:
BCH codes
Cyclic codes
Linear codes
Secret sharing
Weight distribution
Weight enumerator

A B S T R A C T

Cyclic Reed–Solomon codes, a type of BCH codes, are widely used in consumer electronics, communication systems, and data storage devices. This fact demonstrates the importance of BCH codes – a family of cyclic codes – in practice. In theory, BCH codes are among the best cyclic codes in terms of their error-correcting capability. A subclass of BCH codes are the narrow-sense primitive BCH codes. However, the dimension and minimum distance of these codes are not known in general. The objective of this paper is to determine the dimension and minimum distances of two classes of narrow-sense primitive BCH codes with designed distances $\delta = (q-1)q^{m-1} - 1 - q^{\lfloor (m-1)/2 \rfloor}$ and $\delta = (q-1)q^{m-1} - 1 - q^{\lfloor (m+1)/2 \rfloor}$. The weight distributions of some of these BCH codes are also reported. As will be seen, the two classes of

☆ C. Ding's research was supported by the Hong Kong Research Grants Council, Proj. No. 16300415. C. Fan and Z. Zhou were supported by the Natural Science Foundation of China under Grants 11571285 and 61672028, and also the Sichuan Provincial Youth Science and Technology Fund under Grant 2015JQ0004 and 2016JQ0004. C. Fan is also with State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093).

* Corresponding author.
E-mail addresses: cding@ust.hk (C. Ding), fcl@swjtu.edu.cn (C. Fan), zzc@home.swjtu.edu.cn (Z. Zhou).

http://dx.doi.org/10.1016/j.ffa.2016.12.009

BCH codes are sometimes optimal and sometimes among the best linear codes known.

1. Introduction

Throughout this paper, q always denotes a power of a prime p. An $[n, k, d]$ linear code $\mathbb{C}$ over $\mathrm{GF}(q)$ is a k-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum Hamming distance d. Let A_i denote the number of codewords with Hamming weight i in a linear code $\mathbb{C}$ of length n. The *weight enumerator* of $\mathbb{C}$ is defined by

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

The *weight distribution* of $\mathbb{C}$ is the sequence $(1, A_1, \ldots, A_n)$.

A linear code $\mathbb{C}$ over $\mathrm{GF}(q)$ is *cyclic* if $(c_0, c_1, \cdots, c_{n-1}) \in \mathbb{C}$ implies $(c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathbb{C}$. We may identify a vector $(c_0, c_1, \cdots, c_{n-1}) \in \mathrm{GF}(q)^n$ with the polynomial

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathrm{GF}(q)[x]/(x^n - 1).$$

In this way, a code $\mathbb{C}$ of length n over $\mathrm{GF}(q)$ always corresponds to a subset of the quotient ring $\mathrm{GF}(q)[x]/(x^n - 1)$. A linear code $\mathbb{C}$ is cyclic if and only if the corresponding subset in $\mathrm{GF}(q)[x]/(x^n - 1)$ is an ideal of the ring $\mathrm{GF}(q)[x]/(x^n - 1)$.

It is well-known that every ideal of $\mathrm{GF}(q)[x]/(x^n - 1)$ is principal. Let $\mathbb{C} = \langle g(x) \rangle$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the generators of $\mathbb{C}$. Then $g(x)$ is unique and called the *generator polynomial,* and $h(x) = (x^n - 1)/g(x)$ is referred to as the *check polynomial* of $\mathbb{C}$.

From now on, let $m > 1$ be a positive integer, and let $n = q^m - 1$. Let α be a generator of $\mathrm{GF}(q^m)^*$, which is the multiplicative group of $\mathrm{GF}(q^m)$. For any integer i with $0 \le i \le q^m - 2$, let $m_i(x)$ denote the minimal polynomial of α^i over $\mathrm{GF}(q)$. For any $2 \le \delta < n$, define

$$g_{(q,m,\delta)}(x) = \mathrm{lcm}(m_1(x), m_2(x), \cdots, m_{\delta-1}(x)),$$

where lcm denotes the least common multiple of these minimal polynomials. We also define

$$\tilde{g}_{(q,m,\delta)}(x) = (x - 1) g_{(q,m,\delta)}(x).$$

Throughout this paper, let $\mathbb{C}_{(q,m,\delta)}$ and $\tilde{\mathbb{C}}_{(q,m,\delta)}$ denote the cyclic codes of length n over $\mathrm{GF}(q)$ with generator polynomials $g_{(q,m,\delta)}(x)$ and $\tilde{g}_{(q,m,\delta)}(x)$, respectively. This set $\mathbb{C}_{(q,m,\delta)}$ is called a *narrow-sense primitive BCH code* with *designed distance* δ, and $\tilde{\mathbb{C}}_{(q,m,\delta)}$ is referred to as a *primitive BCH code* with *designed distance* $\delta + 1$.