Discrete Mathematics 339 (2016) 415–427

Contents lists available at ScienceDirect

Discrete Mathematics

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

Three-weight cyclic codes and their weight distributions[☆]

Cunsheng Ding[a], Chunlei Li[b], Nian Li[c], Zhengchun Zhou[d,*]

[a] Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

[b] Department of Electrical Engineering and Computer Science, University of Stavanger, 4036, Stavanger, Norway

[c] Department of Informatics, University of Bergen, N-5020 Bergen, Norway

[d] School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China

ARTICLE INFO

Article history:
Received 31 May 2014
Received in revised form 23 August 2015
Accepted 2 September 2015
Available online 1 October 2015

Keywords:
Cyclic codes
Linear codes
Permutation monomials
Weight distribution

ABSTRACT

Cyclic codes have been an important topic of both mathematics and engineering for decades. They have been widely used in consumer electronics, data transmission technologies, broadcast systems, and computer applications as they have efficient encoding and decoding algorithms. The objective of this paper is to provide a survey of three-weight cyclic codes and their weight distributions. Information about the duals of these codes is also given when it is available.

1. Introduction

Let q be a prime power. A linear $[n, \kappa, d; q]$ code over $\mathrm{GF}(q)$ is a κ-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum nonzero (Hamming) weight d. An $[n, \kappa]$ linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. By identifying any vector $(c_0, c_1, \ldots, c_{n-1}) \in \mathrm{GF}(q)^n$ with

$$c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in \mathrm{GF}(q)[x]/(x^n - 1),$$

any linear code $\mathcal{C}$ of length n over $\mathrm{GF}(q)$ corresponds to a subset of the ring $\mathrm{GF}(q)[x]/(x^n - 1)$. A linear code $\mathcal{C}$ 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 $\mathcal{C} = (g(x))$ be a cyclic code, where $g(x)$ is monic and has the smallest degree among all the generators of $\mathcal{C}$. Then $g(x)$ is unique and called the *generator polynomial,* and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check* polynomial of $\mathcal{C}$. If the parity check polynomial $h(x)$ of a code $\mathcal{C}$ of length n over $\mathrm{GF}(q)$ is the product of s distinct irreducible polynomials over $\mathrm{GF}(q)$, we say that the dual code $\mathcal{C}^\perp$ has s zeros.

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

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

[☆] C. Ding's research was supported by The Hong Kong Research Grants Council, Proj. No. 16300415. Z. Zhou's research was supported by the Natural Science Foundation of China, Proj. No. 61201243, the Sichuan Provincial Youth Science and Technology Fund under Grant 2015JQ0004, and the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2013D10.

[*] Corresponding author.
E-mail addresses: cding@ust.hk (C. Ding), chunlei.li@uis.no (C. Li), nianli.2010@gmail.com (N. Li), zzc@home.swjtu.edu.cn (Z. Zhou).

http://dx.doi.org/10.1016/j.disc.2015.09.001
0012-365X/© 2015 Elsevier B.V. All rights reserved.

The *weight distribution* $(1, A_1, \dots, A_n)$ is an important research topic in coding theory. First, it contains crucial information as to estimate the error correcting capability and the probability of error detection and correction with respect to some algorithms [39]. Second, due to rich algebraic structures of cyclic codes, the weight distribution is often related to interesting and challenging problems in number theory. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \dots, A_n)$ is equal to t.

Cyclic codes have been widely used in consumer electronics, data transmission technologies, broadcast systems, and computer applications as they have efficient encoding and decoding algorithms. Cyclic codes with a few weights are of special interest in authentication codes as certain parameters of the authentication codes constructed from these cyclic codes are easy to compute [22], and in secret sharing schemes as the access structures of such secret sharing schemes derived from such cyclic codes are easy to determine [8,21,62]. Cyclic codes with a few weights are also of special interest in designing frequency hopping sequences [17]. Three-weight cyclic codes have also applications in association schemes [3]. These are some of the motivations for studying cyclic codes with a few weights.

There is a nice survey of two-weight linear codes by Calderbank and Kantor [4]. To the best of our knowledge, there is no such reference on two-weight cyclic codes in literature. The reader is referred to [27] and the references therein for recent progress in two-weight cyclic codes. The objective of this paper is to provide a survey on three-weight cyclic codes and their weight distributions. Information on the duals of these three-weight codes is also given when it is available.

The remainder of this paper is organized as follows. Section 2 fixes some notations for this paper. Section 3 surveys three-weight cyclic codes whose duals have only one zero. Section 4 gives a well-rounded treatment of three-weight cyclic codes whose duals have two zeros. Section 5 presents a generic construction of three-weight cyclic codes. Section 6 introduces a method of shortening some three-weight cyclic codes. Section 7 makes some concluding remarks.

2. Some notations fixed throughout this paper

Throughout this paper, we adopt the following notations unless otherwise stated:

(a) p is a prime, and q is a positive power of p.
(b) $r = q^m$, where m is a positive integer.
(c) n denotes the length of a cyclic code over $\mathrm{GF}(q)$ and is either $r-1$ or a divisor of $r-1$.
(d) $\mathbb{Z}_M = \{0, 1, \dots, M-1\}$ denotes the ring of integers modulo M.
(e) $\mathrm{Tr}_{q^\ell/q}(x)$ is the trace function from $\mathrm{GF}(q^\ell)$ to $\mathrm{GF}(q)$.
(f) $\mathtt{C}_a$ denotes the q-cyclotomic coset modulo n containing a, where a is any integer with $0 \le a \le n-1$, and $\ell_a := |\mathtt{C}_a|$, which is the size of the q-cyclotomic coset $\mathtt{C}_a$.

3. Three-weight cyclic codes whose duals have one zero

Let $N > 1$ be an integer dividing $r-1$, and put $n = (r-1)/N$. Let γ be a generator of $\mathrm{GF}(r)^*$ and let $\theta = \gamma^N$. The set

$$\mathcal{C}(r, N) = \{(\mathrm{Tr}_{r/q}(\beta), \mathrm{Tr}_{r/q}(\beta\theta), \dots, \mathrm{Tr}_{r/q}(\beta\theta^{n-1})) : \beta \in \mathrm{GF}(r)\} \tag{1}$$

is called an $[n, m_0]$ *irreducible cyclic code* over $\mathrm{GF}(q)$, where $\mathrm{Tr}_{r/q}$ is the trace function from $\mathrm{GF}(r)$ onto $\mathrm{GF}(q)$, m_0 is the multiplicative order of q modulo n and m_0 divides m. The parity-check polynomial of $\mathcal{C}(r, N)$ is the minimal polynomial over $\mathrm{GF}(q)$ of θ^{-1} and is irreducible.

Irreducible cyclic codes are an interesting topic of study for decades. The celebrated Golay code is an irreducible cyclic code and was used on the Mariner Jupiter–Saturn Mission. Irreducible cyclic codes form a special class of cyclic codes and are interesting in theory as they are minimal cyclic codes. The total number of nonzero Hamming weights in an irreducible cyclic code could be any positive integer. Their weight distributions are extremely complicated. The reader is referred to [23] for information on the weight distribution of irreducible cyclic codes.

The following theorem documents a class of three-weight irreducible cyclic codes [13,23].

Theorem 3.1. *Let N be a divisor of $r-1$. When $\gcd((r-1)/(q-1), N) = 3$ and $p \equiv 1 \pmod 3$, the set $\mathcal{C}(r, N)$ in (1) is a $[(q^m-1)/N, m]$ code with the following weight enumerator:*

$$1 + \frac{r-1}{3} z^{\frac{(q-1)(r-c_1 r^{\frac{1}{3}})}{Nq}} + \frac{r-1}{3} z^{\frac{(q-1)[r+\frac{1}{2}(c_1+9d_1)r^{\frac{1}{3}}]}{Nq}} + \frac{r-1}{3} z^{\frac{(q-1)[r+\frac{1}{2}(c_1-9d_1)r^{\frac{1}{3}}]}{Nq}},$$

where c_1 and d_1 are uniquely given by $4q^{m/3} = c_1^2 + 27d_1^2$, $c_1 \equiv 1 \pmod 3$ and $\gcd(c_1, p) = 1$.

4. Three-weight cyclic codes whose duals have two zeros

In this section, we deal with three-weight cyclic codes whose duals have two zeros, and distinguish between the binary and nonbinary cases. We will also discuss relations between the weight distribution of a cyclic code whose dual has two zeros and the correlation value distribution of two related maximum-length sequences.