Discrete Mathematics 313 (2013) 434–446

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

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

Perspective

Hamming weights in irreducible cyclic codes[☆]

Cunsheng Ding[a], Jing Yang[b,*]

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

[b] Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China

ARTICLE INFO

Article history:
Received 23 February 2012
Received in revised form 5 November 2012
Accepted 7 November 2012
Available online 4 December 2012

Keywords:
Cyclic codes
Cyclotomy
Difference sets
Gaussian periods
Irreducible cyclic codes
Weight distribution

ABSTRACT

The objectives of this paper are to survey and extend earlier results on the weight distributions of irreducible cyclic codes, present a divisibility theorem and develop bounds on the weights in irreducible cyclic codes.

1. Introduction

Irreducible cyclic codes are an interesting type of codes and have applications in space communications. They have been studied for decades and a lot of progress has been made.

Throughout this paper, let p be a prime, $q = p^s$ for a positive integer s, and $r = q^m$ for a positive integer m. A linear $[n, k, d]$ code 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 code $\mathcal{C}$ of length n. The *weight enumerator* of $\mathcal{C}$ is defined by

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

A linear $[n, k]$ code $\mathcal{C}$ over the finite field $\mathrm{GF}(q)$ is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$. Let $\gcd(n, q) = 1$. 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 code $\mathcal{C}$ of length n over $\mathrm{GF}(q)$ corresponds to a subset of $\mathrm{GF}(q)[x]/(x^n - 1)$. The 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 $\mathrm{GF}(q)[x]/(x^n - 1)$.

Note 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 $\deg(f)$ is minimal. Then $g(x)$ is called the *generator polynomial* and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check* polynomial of $\mathcal{C}$.

☆ C. Ding's research is supported by the Hong Kong Research Grants Council, Project No. 600812. J. Yang's research is supported in part by the National Natural Science Foundation of China (No. 10990011, 11001145, 11101233), the Ph.D. Programs Foundation of Ministry of Education of China (No. 20090002120013), and the Science and Technology on Information Assurance Laboratory Foundation (No. KJ-12-01).

* Corresponding author.
E-mail addresses: cding@ust.hk (C. Ding), jingyang@math.tsinghua.edu.cn (J. Yang).

0012-365X/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2012.11.009

Let $N > 1$ be an integer dividing $r-1$, and put $n = (r-1)/N$. Let α be a primitive element of GF(r) and let $\theta = \alpha^N$. The set

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

is called an *irreducible cyclic* $[n, m_0]$ *code* over GF(q), where $\mathrm{Tr}_{r/q}$ is the trace function from GF(r) onto GF(q), m_0 is the multiplicative order of q modulo n and m_0 divides m.

Irreducible cyclic codes have been an interesting subject of study for many years. The celebrated Golay code is an irreducible cyclic code and was used on the Mariner Jupiter–Saturn Mission. They form a special class of codes and are interesting in theory as they are minimal cyclic codes. The weight distribution, i.e., the vector $(1, A_1, A_2, \ldots, A_{n-1})$, of the irreducible cyclic codes has been determined for a small number of special cases.

The objectives of this paper are to survey and extend earlier results on the weight distributions of irreducible cyclic codes (see Theorems 23, 21, 15, 17, 18, 19 and 20 as extensions and generalizations of earlier results), to completely characterize one-weight irreducible cyclic codes (Theorem 16), which is an extension of the result in [28], and to present a divisibility theorem and develop bounds on the weights in irreducible cyclic codes (see Theorems 24 and 13).

2. Group characters, cyclotomy, and Gaussian periods

In this section, we present results on group characters, cyclotomy and Gaussian sums which will be needed in the sequel.

2.1. Group characters and Gaussian sums

Let $\mathrm{Tr}_{q/p}$ denote the trace function from GF(q) to GF(p). An *additive character* of GF(q) is a nonzero function χ from GF(q) to the set of complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \mathrm{GF}(q)^2$. For each $b \in \mathrm{GF}(q)$, the function

$$\chi_b(c) = e^{2\pi\sqrt{-1}\mathrm{Tr}_{q/p}(bc)/p} \quad \text{for all } c \in \mathrm{GF}(q) \tag{2}$$

defines an additive character of GF(q). When $b = 0$, $\chi_0(c) = 1$ for all $c \in \mathrm{GF}(q)$, and is called the *trivial additive character* of GF(q). The character χ_1 in (2) is called the *canonical additive character* of GF(q).

A *multiplicative character* of GF(q) is a nonzero function ψ from $\mathrm{GF}(q)^*$ to the set of complex numbers such that $\psi(xy) = \psi(x)\psi(y)$ for all pairs $(x, y) \in \mathrm{GF}(q)^* \times \mathrm{GF}(q)^*$. Let g be a fixed primitive element of GF(q). For each $j = 1, 2, \ldots, q-1$, the function ψ_j with

$$\psi_j(g^k) = e^{2\pi\sqrt{-1}jk/(q-1)} \quad \text{for } k = 0, 1, \ldots, q-2 \tag{3}$$

defines a multiplicative character with order $(q-1)/\gcd(q-1, j)$ of GF(q). When $j = q-1$, $\psi_0(c) = 1$ for all $c \in \mathrm{GF}(q)^*$, and is called the *trivial multiplicative character* of GF(q).

Let q be odd and $j = (q-1)/2$ in (3), we then get a multiplicative character η such that $\eta(c) = 1$ if c is the square of an element and $\eta(c) = -1$ otherwise. This η is called the *quadratic character* of GF(q).

Let ψ be a multiplicative character with order k where $k|(q-1)$ and χ an additive character of GF(q). Then the *Gaussian sum* $G(\psi, \chi)$ of order k is defined by

$$G(\psi, \chi) = \sum_{c \in \mathrm{GF}(q)^*} \psi(c)\chi(c).$$

Since $G(\psi, \chi_b) = \bar{\psi}(b)G(\psi, \chi_1)$, we just consider $G(\psi, \chi_1)$, briefly denoted as $G(\psi)$, in the sequel. If $\psi \neq \psi_0$, then

$$|G(\psi)| = q^{1/2}. \tag{4}$$

Generally, to explicitly determine the value of Gaussian sums is a challenging task. At present, they can be determined in a few cases. Among them is the following case of $k = 2$.

If $q = p^s$, where p is an odd prime and s is a positive integer, then

$$G(\eta) = \begin{cases} (-1)^{s-1}q^{1/2} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{s-1}(\sqrt{-1})^s q^{1/2} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{5}$$

The following result [15] is useful in the sequel.

Lemma 1. *Let χ be a nontrivial additive character of* GF(q) *with q odd, and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathrm{GF}(q)[x]$ with $a_2 \neq 0$. Then*

$$\sum_{c \in \mathrm{GF}(q)} \chi(f(c)) = \chi(a_0 - a_1^2(4a_2)^{-1})\eta(a_2)G(\eta). \tag{6}$$