ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

Complete weight enumerators of some irreducible cyclic codes

Zexia Shi *, Fang-Wei Fu

Chern Institute of Mathematics, Nankai University, Tianjin 300071, PR China

ARTICLE INFO

Article history:
Received 27 March 2016
Received in revised form 30 October 2016
Accepted 6 November 2016
Available online xxxx

Keywords:
Complete weight enumerator
Gaussian periods
Combination
Optimal constant composition code

ABSTRACT

In this paper, we investigate the complete weight enumerators of two classes of irreducible cyclic codes. We present the explicit complete weight enumerator of the irreducible cyclic codes. Furthermore, we obtain a class of optimal constant composition codes from irreducible cyclic codes.

1. Introduction

Throughout this paper, let p be a prime, $q = p^s$ for a positive integer s. Let $\mathbb{F}_r$ be a finite field with $r = q^m$ elements and α be a generator of $\mathbb{F}_r^* = \mathbb{F}_r \setminus \{0\}$. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance d. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is called cyclic if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Moreover a cyclic code $\mathcal{C}$ can be viewed as an ideal of the quotient ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Note that every ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is principal. Let $\mathcal{C} = \langle g(x)\rangle$, where $g(x)$ is the monic polynomial of the least degree and $g(x)$ is a divisor of $x^n - 1$. Then $g(x)$ and $h(x) = (x^n - 1)/g(x)$ are called the generator polynomial and the check polynomial of $\mathcal{C}$, respectively. If $h(x)$ is irreducible over $\mathbb{F}_q$, we call $\mathcal{C}$ an irreducible cyclic code.

Let the elements of $\mathbb{F}_q$ be denoted by $b_0 = 0, b_1, b_2, \ldots, b_{q-1}$, in some fixed order. For a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, the composition of $\mathbf{c}$ denoted by $comp(\mathbf{c})$, is $(\omega_0, \omega_1, \ldots, \omega_{q-1})$ where $\omega_i = \omega_i(\mathbf{c})$ is the number of components c_j $(0 \le j \le n-1)$ equals b_i. Clearly, $\sum_{i=0}^{q-1} \omega_i = n$. Then the complete weight enumerator of $\mathcal{C}$ is

$$W_{\mathcal{C}}(z_0, z_1, \ldots, z_{q-1}) = \sum_{\mathbf{c}\in\mathcal{C}} z_0^{\omega_0(\mathbf{c})} z_1^{\omega_1(\mathbf{c})} \ldots z_{q-1}^{\omega_{q-1}(\mathbf{c})}.$$

The weight enumerators of cyclic codes have been extensively investigated for many years (see [8,10,9,17,19,23]). It is not difficult to see that the weight enumerators can be obtained from the complete weight enumerators. Blake and Kith [3,14] presented the complete weight enumerator of a special class of Reed–Solomon codes. The complete weight enumerators of generalized Kerdock code and related linear codes over Galois rings were studied by Kuzmin and Nechaev [15,16]. Recently, the complete weight enumerators of some cyclic codes have been established with exponential sums and Galois theory [1,12,18].

An $(n, M, d, [\omega_0, \omega_1, \ldots, \omega_{q-1}])_q$ constant composition code (CCC in short) is a code over the abelian group $\{b_0, b_1, \ldots, b_{q-1}\}$, with length n, size M, and minimum Hamming distance d such that in every codeword the element b_i

* Corresponding author.

http://dx.doi.org/10.1016/j.dam.2016.11.008
0166-218X/

Please cite this article in press as: Z. Shi, F.-W. Fu, Complete weight enumerators of some irreducible cyclic codes, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.11.008

appears exactly ω_i times for every i. Two constant composition codes are said to be equivalent if one can be obtained from the other by coordinate permutations.

Let $N > 1$ be an integer dividing $r-1$, $n = (r-1)/N$, and $\theta = \alpha^N$. Then

$$\mathcal{C} = \{\mathbf{c}(a) = (\mathrm{Tr}_{r/q}(a), \mathrm{Tr}_{r/q}(a\theta), \ldots, \mathrm{Tr}_{r/q}(a\theta^{n-1})) : a \in \mathbb{F}_r\} \tag{1}$$

is called an irreducible cyclic $[n, m_0]$ code over $\mathbb{F}_q$, where m_0 is the multiplicative order of q modulo n, and $\mathrm{Tr}_{r/q}$ is the trace function from $\mathbb{F}_r$ onto $\mathbb{F}_q$. By Delsarte's Theorem [6], the check polynomial of $\mathcal{C}$ is the minimal polynomial of θ^{-1} over $\mathbb{F}_q$.

In this paper, we investigate the complete weight enumerators of irreducible cyclic codes in the following two cases:

1. $q = p^{2t\gamma_1}$ for some integer γ_1, where t is the least positive integer such that $p^t \equiv -1 \bmod N$.
2. $n = l^v$ and $m = l^{v_1}$, where l is a prime, $q - 1 = l^{v_2}b$ with $\gcd(l, b) = 1$, $v = v_1 + v_2$ and $v_1, v_2 > 0$. Moreover $4 \mid (q-1)$ if $l = 2$.

It should be remarked that the weight enumerator of $\mathcal{C}$ has been determined [24] for Case 2. Li et al. [18] used Gauss sums to determine the explicit complete weight enumerators of $\mathcal{C}$ in some cases. In this paper, we give the explicit complete weight enumerator of $\mathcal{C}$ for Case 1 by using Gaussian periods and obtain a class of optimal constant composition codes. Moreover we use a combinatorial method to present the explicit complete weight enumerator of $\mathcal{C}$ for Case 2.

The rest of the paper is organized as follows. In Section 2, we introduce some basic definitions and properties about character and Gaussian periods. In Section 3, we present the explicit complete weight enumerator of $\mathcal{C}$ for Case 1 by using Gaussian periods and then obtain a class of optimal constant composition codes. In Section 4, we use a combinatorial method to give the explicit complete weight enumerator of $\mathcal{C}$ for Case 2.

2. Gaussian periods

Let $\mathbb{F}_r$ be the finite field with r elements, where r is a power of prime p. An additive character of $\mathbb{F}_r$ is a nonzero function χ from $\mathbb{F}_r$ to the set of complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \mathbb{F}_r \times \mathbb{F}_r$. For each $a \in \mathbb{F}_r$, the function

$$\chi_a(x) = e^{\frac{2\pi\sqrt{-1}\mathrm{Tr}_{r/p}(ax)}{p}},$$

where $\mathrm{Tr}_{r/p}$ denotes the trace function from $\mathbb{F}_r$ onto $\mathbb{F}_p$, defines an additive character of $\mathbb{F}_r$. In particular, χ_0 is called the trivial additive character of $\mathbb{F}_r$ and χ_1 is called the canonical additive character of $\mathbb{F}_r$. The orthogonal property of additive character which can be found in [20] is given by

$$\sum_{x\in\mathbb{F}_r} \chi_a(x) = 0 \quad \text{for } a \neq 0.$$

Let $r - 1 = nN$ and let α be a fixed primitive element of $\mathbb{F}_r$. Define $C_i^{(N,r)} = \alpha^i\langle\alpha^N\rangle$ for $i = 0, 1, \ldots, N-1$, where $\langle\alpha^N\rangle$ denotes the subgroup of $\mathbb{F}_r^*$ generated by α^N. The Gaussian periods are defined by

$$\eta_i^{(N,r)} = \sum_{x\in C_i^{(N,r)}} \chi(x), \quad i = 0, 1, \ldots, N-1,$$

where χ is the canonical additive character of $\mathbb{F}_r$.

The Gaussian periods in the semiprimitive case are known and are described in the following lemma.

Lemma 1 ([2,22]). *Assume that $N \geq 2$ and there exists a least positive integer t such that $p^t \equiv -1 \bmod N$. Let $r = p^{2t\gamma}$ for some integer γ.*

1. *If γ, p and $(p^t+1)/N$ are all odd, then*
$$\eta_{\frac{N}{2}}^{(N,r)} = \frac{(N-1)\sqrt{r}-1}{N}, \qquad \eta_k^{(N,r)} = -\frac{\sqrt{r}+1}{N} \quad \text{for } k \neq \frac{N}{2}.$$
2. *In all other cases,*
$$\eta_0^{(N,r)} = \frac{(-1)^{\gamma+1}(N-1)\sqrt{r}-1}{N}, \qquad \eta_k^{(N,r)} = \frac{(-1)^{\gamma}\sqrt{r}-1}{N} \quad \text{for } k \neq 0.$$

3. The first case

In this section, we use Gaussian periods to give the explicit complete weight enumerator of the irreducible cyclic code $\mathcal{C}$ defined by (1) for Case 1, and obtain a class of optimal constant composition codes.

Please cite this article in press as: Z. Shi, F.-W. Fu, Complete weight enumerators of some irreducible cyclic codes, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.11.008