Discrete Mathematics 339 (2016) 2070–2078

Contents lists available at ScienceDirect

Discrete Mathematics

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

On the weight distributions of some cyclic codes

Guanghui Zhang

School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China

ARTICLE INFO

Article history:
Received 30 March 2015
Received in revised form 16 September 2015
Accepted 12 February 2016
Available online 27 April 2016

Keywords:
Cyclic code
Weight distribution
Generating idempotent

ABSTRACT

Finding the weight distributions of specific cyclic codes has been an interesting area of research. Although the class of cyclic codes has been studied for many years, their weight distributions are known only for a few cases. In this paper, we use matrix method to determine the weight distribution of a family of cyclic codes.

1. Introduction

One of the most important classes of linear codes is the class of cyclic codes. These codes have found wide applications in communication systems and data storage systems. The weight distributions of cyclic codes have been interesting subjects of study for many years. However, determining explicitly the weight distribution of cyclic codes, in general, is a very hard problem. Although some special cases have been studied by many authors, it remains an open problem for most cyclic codes. For recent surveys on this topic, the reader is referred to [3] and [5].

Let $\mathbb{F}_q$ be the finite field of order q and let n be a positive integer relatively prime to q. An $[n, k, d]$ *code* over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum (Hamming) distance d. Let A_j be the number of codewords with Hamming weight j in a code of length n. The sequence $(A_0, A_1, \ldots, A_n)$ is called the *weight distribution* of the code. In coding theory, the minimum distance determines the error correcting capability of the code, and a knowledge of its weight distribution can be used to determine the probability of improperly decoding received vectors (e.g. see [21, Ch. 3]).

An element e of a ring satisfying $e^2 = e$ is called an *idempotent*. It is well known that any *cyclic code* of length n over $\mathbb{F}_q$ can be identified as an ideal in the semi-simple ring $\mathbb{F}_q[X]/\langle X^n - 1\rangle$. Therefore, each cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ contains a unique idempotent which generates the code. This idempotent, say $e(X)$, is called the *generating idempotent* of $\mathcal{C}$. In this case, $g(X) = \gcd\big(e(X), X^n - 1\big)$ is called the *generator polynomial* of $\mathcal{C}$, and $h(X) = (X^n - 1)/g(X)$ is referred to as the *check polynomial* (e.g. see [10, Ch. 4] or [17, Ch. 8]).

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_q$ with check polynomial $h(X)$. If $h(X)$ has ℓ irreducible factors over $\mathbb{F}_q$, we call $\mathcal{C}$ *the dual of the cyclic code with* ℓ *zeros*. Theoretically, the weight distributions of cyclic codes can be expressed via some exponential sums. However, finding such evaluations of exponential sums is complicated, and it becomes extremely difficult when the dual of the cyclic code has more zeros. Hence, most of the works in the literature consider the cases where the dual of the cyclic code has at most three zeros. The weight distributions of cyclic codes of which the dual of the code has arbitrary zeros are known only for a very small number of cases. See, for example, [1,8,7,11,12,14,13,15,16] and [18,21,22,20,23–28,31,32,29,30].

E-mail address: zghlsh@163.com.

http://dx.doi.org/10.1016/j.disc.2016.02.007

Recently, Lin et al. in [15] determined the weight distribution of a family of cyclic codes from their generating idempotents. In this paper we use the approach presented in [15] to solve one more special case. The cyclic codes under consideration are the ones whose dual may have more than three zeros. More specifically, let n be an odd positive integer. Suppose that C_n is a cyclic group of order n with three subgroups H_1, H_2 and H_3 satisfying $H_1 \subset H_2 \subset H_3$, i.e., H_i is a proper subgroup of $H_{i+1}, i = 1, 2$. Then $\mathcal{R} = \mathbb{F}_{2^m}C_n$ is the semi-simple group algebra of C_n over $\mathbb{F}_{2^m}$. For any subgroup H of C_n, $H^\dagger$ is defined as $H^\dagger = \sum_{h\in H} h$. It is readily seen that $H^\dagger$ is an idempotent of $\mathcal{R}$. We study the weight distribution of the cyclic code $\mathcal{C}$ of length n over $\mathbb{F}_{2^m}$ with generating idempotent $H_1^\dagger + H_2^\dagger + H_3^\dagger$. In Section 2, we show that every element of $\mathcal{C}$ is associated with a series of matrices satisfying certain conditions. From this algebraic characterization, the problem of determining the weight distribution of the code $\mathcal{C}$ is then transformed into enumerating matrices satisfying certain properties. In particular, the dimension and the minimum distance of $\mathcal{C}$ are explicitly exhibited. In Section 3, we give two illustrative examples. These examples are the cases where the dual of the cyclic codes having at least 4 zeros. Finally, we give some concluding remarks in Section 4.

2. Results and proofs

Let $C_n = \langle g\rangle$ be a cyclic group of order n, where n is an odd positive integer. Suppose C_n has three subgroups H_1, H_2 and H_3 satisfying $H_1 \subset H_2 \subset H_3$, i.e., H_i is a proper subgroup of H_{i+1}, $i = 1, 2$. Without loss of generality, we assume that $H_3 = \langle g^s\rangle$, where s is a divisor of n. Then

$$S = \left\{1, g, g^2, \dots, g^{s-1}\right\} \tag{2.1}$$

is an ordered transversal of H_3 in C_n. Similarly, let $H_2 = \langle g^{st}\rangle$ and $H_1 = \langle g^{stw}\rangle$. Let T (resp. W) be an ordered transversal of H_2 in H_3 (resp. H_1 in H_2). We may take

$$T = \left\{1, g^s, g^{2s}, \dots, g^{s(t-1)}\right\}. \tag{2.2}$$

As we show in the following diagram, $|T| = \frac{|H_3|}{|H_2|} = \frac{n/s}{n/(st)} = t > 1$ and $|W| = \frac{|H_2|}{|H_1|} = \frac{n/(st)}{n/(stw)} = w > 1$. In particular, stw is a divisor of $|C_n| = n$.

$$\begin{tikzcd} H_1 \arrow[r, "W"] & H_2 \arrow[r, "T"] & H_3 \arrow[r, "S"] & C_n \end{tikzcd}.$$

Let $\mathcal{R} = \mathbb{F}_{2^m}C_n$ be the semi-simple group algebra of C_n over $\mathbb{F}_{2^m}$. For any subgroup H of C_n, $H^\dagger = \sum_{h\in H} h$ is an idempotent of $\mathcal{R}$. The aim of this note is to determine the weight distribution of the cyclic code $\mathcal{C}$ generated by $H_1^\dagger + H_2^\dagger + H_3^\dagger$, i.e.,

$$\mathcal{C} = \left\{r\left(H_1^\dagger + H_2^\dagger + H_3^\dagger\right) \,\middle|\, r \in \mathcal{R}\right\}.$$

Clearly,

$$\left(H_1^\dagger + H_2^\dagger + H_3^\dagger\right)^2 = H_1^\dagger + H_2^\dagger + H_3^\dagger.$$

Thus, $H_1^\dagger + H_2^\dagger + H_3^\dagger$ is indeed an idempotent of $\mathcal{R}$. For any element r of $\mathcal{R}$, $r \in \mathcal{C}$ if and only if $r(H_1^\dagger + H_2^\dagger + H_3^\dagger) = r$. Considering $\mathcal{R}H_1^\dagger = \{rH_1^\dagger \mid r \in \mathcal{R}\}$ as a vector space over $\mathbb{F}_{2^m}$, it is easy to see that

$$\left\{\alpha\beta\gamma H_1^\dagger \,\middle|\, \alpha \in S, \beta \in T, \gamma \in W\right\}$$

is a basis for $\mathcal{R}H_1^\dagger$ over $\mathbb{F}_{2^m}$. Hence, any element $r \in \mathcal{R}H_1^\dagger$ can be uniquely expressed as

$$r = \sum_{\alpha\in S}\sum_{\beta\in T}\sum_{\gamma\in W} a_{\alpha,\beta}^{(\gamma)}\alpha\beta\gamma H_1^\dagger \in \mathcal{R}H_1^\dagger, \quad a_{\alpha,\beta}^{(\gamma)} \in \mathbb{F}_{2^m}. \tag{2.3}$$

Observe that $H_1^\dagger H_2^\dagger = H_2^\dagger$ and $H_1^\dagger H_3^\dagger = H_3^\dagger$ since $H_1 \subset H_2$ and $H_1 \subset H_3$, which implies

$$(H_1^\dagger + H_2^\dagger + H_3^\dagger)H_1^\dagger = \left(H_1^\dagger\right)^2 + H_1^\dagger H_2^\dagger + H_1^\dagger H_3^\dagger = H_1^\dagger + H_2^\dagger + H_3^\dagger.$$

This shows that

$$\mathcal{C} = \mathcal{R}\left(H_1^\dagger + H_2^\dagger + H_3^\dagger\right) \subseteq \mathcal{R}H_1^\dagger = \left\{rH_1^\dagger \,\middle|\, r \in \mathcal{R}\right\}.$$

We want to determine which elements of $\mathcal{R}H_1^\dagger$ are, in fact, belonging to $\mathcal{C}$. For this purpose, assume that $r(H_1^\dagger + H_2^\dagger + H_3^\dagger) = r$, where r is an element of $\mathcal{R}H_1^\dagger$ given as in (2.3). Expanding this equation, we have

$$\begin{aligned} r &= \sum_{\alpha\in S}\sum_{\beta\in T}\sum_{\gamma\in W} a_{\alpha,\beta}^{(\gamma)}\alpha\beta\gamma H_1^\dagger = r(H_1^\dagger + H_2^\dagger + H_3^\dagger) \\ &= \sum_{\alpha\in S}\sum_{\beta\in T}\sum_{\gamma\in W} a_{\alpha,\beta}^{(\gamma)}\alpha\beta\gamma H_1^\dagger + \sum_{\alpha\in S}\sum_{\beta\in T}\sum_{\gamma\in W} a_{\alpha,\beta}^{(\gamma)}\alpha\beta\gamma H_2^\dagger + \sum_{\alpha\in S}\sum_{\beta\in T}\sum_{\gamma\in W} a_{\alpha,\beta}^{(\gamma)}\alpha\beta\gamma H_3^\dagger. \end{aligned}$$