CYCLIC CODES OVER THE RING \( Z_{p^e} \) OF LENGTH \( p^e \)

Shi Minjia\(^*\)
Zhu Shixin\(^*\)

\(^*\)(Hefei University of Technology, School of Management, Hefei 230009, China)
\(^*\)(School of Mathematics Science, Anhui University, Hefei 230039, China)

Abstract The study of cyclic codes over rings has generated a lot of public interest. In this paper, we study cyclic codes and their dual codes over the ring \( Z_{p^e} \) of length \( p^e \), and find a set of generators for these codes. The ranks and minimal generator sets of these codes are studied as well, which play an important role in decoding and determining the distance distribution of codes.

Key words Cyclic code; Rank; Minimal generator set

CLC Index TN911.22

DOI 10.1007/s11767-007-0071-7

I. Introduction

Linear and cyclic codes over rings have recently aroused great interest because of their new roles in algebraic coding theory and their successful application in combined coding and modulation. A remarkable paper by Hammons, et al.\(^[3]\) has shown that certain binary nonlinear codes with good error correcting capabilities can be viewed through a Gray mapping as linear codes over \( \mathbb{Z}_p \)-module. The map \( \mu : R \to S \) defined by \( \mu(f(x)) = f(x) \mod p \) is an onto ring homomorphism.

Let \( u = (u_0, u_1, \ldots, u_{n-1}) \) and \( v = (v_0, v_1, \ldots, v_{n-1}) \) be any two vectors over a ring. We define their inner product as \( u \cdot v = u_0 v_0 + \cdots + u_{n-1} v_{n-1} \). If \( u \cdot v = 0 \), then \( u \) and \( v \) are said to be orthogonal.

We define the dual of a cyclic code \( C \) to be the set \( C^\perp = \{ u \in R, u \cdot v = 0, \forall v \in C \} \). It is clear that \( C^\perp \) is also a cyclic code. Following Ref.[2], we shall define the rank of a code \( C \) over \( R \) of type \( \{k_1, k_2\} \), denoted by \( \text{rank} (C) \), by the minimal number of generators of \( C \), and define the free rank of \( C \), denoted by \( f\text{-rank} (C) \), by the maximum of the ranks of \( R_i \)-free submodules of \( C \). A code of \( R_i \) of type \( \{k_1, k_2\} \) has the rank equal to \( k_1 + k_2 \) and the free rank equal to \( k_1 \). These definitions can be generalized to codes over \( R \).

Progress has been obtained in the direction of determining the structural properties of codes over large families of finite rings of odd length. The structure of cyclic codes over ring \( Z_{p^e} \) was obtained by Calderbank, et al.\(^[3]\), and later on, with a different proof, by Pramod Kanwar, et al.\(^[4]\). Authors of Refs.[5,6] studied the structure of cyclic codes over ring \( F_p + uF_p + \cdots + u^{k-1}F_p \) and so on. The case that the length of codes is even is relatively less studied. The cyclic codes of length \( 2^e \) over \( Z_4 \) are studied by Abualrub, et al.\(^[7]\). Blackford\(^[8]\) studied cyclic codes over \( Z_4 \) of oddly even length. Dougherty, et al.\(^[9]\) determined the structure of all cyclic codes over \( Z_4 \) of even length. In this paper, results are presented on the generators of cyclic codes and their dual codes over ring \( R_{p^e} \).

The ranks of these cyclic codes and their minimal generator sets are studied as well.

The remainder of the paper is organized as follows. In Section II, we study cyclic codes over \( R \), and we show that the structure of cyclic codes over

---

1 Manuscript received date: April 19, 2007; revised date: September 6, 2007.
The article is partly supported by the National Natural Science Foundation of China (No.60673074) and the Key Project of Ministry of Education Science and Technology’s Research (107065).
Communication author: Shi Minjia, born in 1980, male, Ph.D. School of Mathematics & Computational Science, Anhui University, Hefei 230030, China.
Email: shiminjia_219@tom.com.
$R$ depends on the cyclic codes over $S$. After identifying this relation, we find a unique set of generators for cyclic code over $R$. In section III, IV, we study the dual cyclic codes and their ranks of these cyclic codes respectively. Section V concludes the paper.

II. Generators for Cyclic Codes over Ring $R$

Through this paper, we will assume that $p$ is an odd prime, $e > 0$ is an integer and $n = p^e$. We can present a series of Lemmas that will help us in the computation of special generators of ideals in $R_n$.

Lemma 1 Let $n = p^e$, $p > 2$, then $(x + p - 1)$ is a nilpotent element whose nilindex is less than or equal to $n$ in $S_n$.

So, $(x + p - 1)$ is a nilpotent element whose nil-index is less than or equal to $n$ in $S_n$.

Lemma 2 Let $f(x) = \sum_{i=0}^{n-1} c_i (x + p - 1)^i$ be an element of $S_n$, then $f(x)$ has an inverse in $S_n$ if and only if $c_0 \neq 0$.

Proof According to Lemma 1, $(x + p - 1)$ is a nilpotent element in $S_n$; it is clear that $f(x)$ is invertible if and only if $c_0 \neq 0$.

Q.E.D.

Similarly, we have the following Lemma.

Lemma 3 Let $f(x) = \sum_{i=0}^{n-1} c_i (x + p - 1)^i$ be an element of $R_n$ with $c_0 = 0$ or $p$, then $f(x)$ is a unit in $R_n$.

Lemma 4[10] Ring $S_n$ and $R_n$ are local rings with maximal ideals $(x + p - 1)$ and $(x + p - 1)$.

Let $I$ be an ideal in $R_n$ containing no monic elements. Let $f(x)$ be an element of $I$ with minimal degree $t$. If $f(x) = \sum_{i=0}^{n-t} c_i (x + p - 1)^i$ and $c_0 \equiv 0 \pmod{p}$ for some $k < t$ then $p f(x)$ is a nonzero polynomial in $I$ of degree less than $t$. This is a contradiction to our choice of $t$. Hence, we can assume that $f(x)$ has content $p$, $\sum_{i=0}^{n-t} d_i (x + p - 1)^i$, $d_i \in S$, $0 \leq i < t$, $f(x) \in S[x]$. If $m$ is the smallest positive integer such that $d_m = 0$, then $f(x) = p (x + p - 1)^m [1 + \sum_{i=m+1}^{n-t} d_i (x + p - 1)^i]$. By Lemma 2, $[1 + \sum_{i=m+1}^{n-t} d_i (x + p - 1)^i]$ is a unit in $S$. It follows that $p (x + p - 1)^m \in I$, where $m$ is the unique smallest positive integer with this property. This yields the following result.

Theorem 1 If $I$ is an ideal containing no nonzero monic elements in $R_n$, then there is a unique nonnegative integer $m$ such that $I = \langle p (x + p - 1)^m \rangle$.

Theorem 1 establishes a one-to-one correspondence between the set of ideals containing no monic polynomials and the set of polynomials of the form $p(x + p - 1)^m$, where $0 \leq m < n$, which are generators of such ideals. In the next theorem of this section, we will extend this correspondence to the entire set of ideals of $R_n$ by establishing a unique set of generators for each ideal. Because of their uniqueness, we will refer to our selected generators as distinguished generators.

Theorem 2 Let $I = \langle f(x) \rangle$ be a principal ideal in $R_n$, where $f(x) = f_1(x) + p f_2(x)$, $f(x) \in S_n$, $i = 1, 2$. Assume also that $f_1(x) \neq 0$, then $I$ has a unique generator of the form $f(x) = (x + p - 1)^s + p \sum_{i=0}^{s-1} c_i (x + p - 1)^i$, where $s$ is the degree of the unique monic element of minimal degree in $I$ and $m$ is the smallest positive integer such that $p (x + p - 1)^m \in I$.

Proof Let $\mu(I) = \langle f(x) \rangle \pmod {p}$, then $\mu(I)$ is an ideal of $S_n$. According to Lemma 4, $S_n$ is a local ring with only maximal ideal $\langle x + p - 1 \rangle$, so we can assume that $\mu(I) = \langle x + p - 1 \rangle$. Then $f(x)$ can be written as $f(x) = (x + p - 1)^s + p \sum_{i=0}^{s-1} c_i (x + p - 1)^i$. Let $m$ be the smallest positive integer such that $p (x + p - 1)^m \in I$. Then $I = \langle x + p - 1 \rangle + p \sum_{i=0}^{m-1} c_i (x + p - 1)^i$. For uniqueness, suppose there exists a polynomial $g(x) \in R_n$ such that $I = \langle g(x) \rangle$, $g(x)$ can be written as $g(x) = (x + p - 1)^s + p \sum_{i=0}^{s-1} d_i (x + p - 1)^i$. Then $f(x) = g(x) = p \sum_{i=0}^{m-1} (c_i - d_i) (x + p - 1)^i$ if $pc_i \equiv pd_i \pmod {p}$ for some $i$, let $k$ be the smallest positive integer such that $pc_k \equiv pd_k \pmod {p}$. We can assume $c_k - d_k = 1$ and denote $f(x) - g(x)$ as $f(x) - g(x) = p (x + p - 1)^m + \sum_{i=0}^{m-1} e_i (x + p - 1)^i$ where $e_0 = 1$. According to Lemma 1, $\sum_{i=0}^{m-1} e_i (x + p - 1)^i$ is an invertible element, then $p (x + p - 1)^m \in I$. But $k \leq m - 1$, we have a contradiction to our choice of $m$. Therefore, we must have $f(x) = g(x)$ and the generator of $I$ in the theorem is unique.

Q.E.D.

Let $I$ be an ideal that is not principal. By Theorem 1, we see that $I$ must contain a monic polynomial. Let $f(x)$ be a monic polynomial of minimal degree $s$ in $I$. $f(x)$ must divide every monic polynomial in $I$ mod $p$ (Since $S_n$ is a principal ideal ring). Also, as in the proof of Theorem 1, any monomorphic polynomial in $I$ must be of the form $pg_i(x)$ for some monominal $g_i(x) \in S_n$. Therefore, nonprincipal ideals need only