Reversible complement cyclic codes over finite chain rings

Monika Dalal[1], Sucheta Dutt[1*] and Ranjeet Sehmi[1]
[1]Department of Applied Sciences,Punjab Engineering College
(Deemed to be University), Chandigarh, India, 160012
[*]Corresponding author(s). E-mail(s): *rsehmi@pec.edu.in* ;
Contributing authors : *monika.phdappsc@pec.edu.in*;
sucheta@pec.edu.in;

Abstract

Let k be an arbitrary element of a finite commutative chain ring R and u be a unit in R. In this work, we present necessary conditions which are sufficient as well for a cyclic code to be a (u, k) reversible complement code over R. Using these conditions, all principally generated cyclic codes over the ring $Z_2 + vZ_2 + v^2Z_2, v^3 = 0$ of length 4 have been checked to find whether they are $(1, 1)$ reversible complement or not.

Keywords : Code, Cyclic, Reversible, Complement

1 Introduction

The class of cyclic codes is a crucial class of linear block codes where cyclic shifts of every codeword belong to the code itself. Reversible and reversible complement cyclic codes are important subclasses of cyclic codes which find applications in DNA data storage, molecular computation, quantum computing, cryptography and communication networks. A vast literature is available on reversible cyclic codes over fields, Galois rings and finite chain rings [**?**, **?**, **?**, **?**, **?**]. Reversible complement cyclic codes over different rings have also been explored by various researchers [?, ?, ?, ?, ?, ?, ?, ?]. J. Kaur et al. have defined a generalized notion for complement of an element of a finite commutative ring in [**?**]. They have used this notion to derive necessary conditions for a cyclic code over a Galois ring to be a reversible complement, which are sufficient as well.

In this work, we present necessary conditions which are sufficient as well for a cyclic code to be a (u, k) reversible complement code over R, thereby extending the results of [?]. Using these conditions, all principally generated cyclic codes over the ring $Z_2 + vZ_2 + v^2Z_2, v^3 = 0$ of length 4 have been checked to find whether they are $(1, 1)$ reversible complement or not.

2 Preliminaries

Let R be a finite commutative ring having unity. If all the ideals of R form a chain under inclusion, then it is said to be a finite commutative chain ring. Let k be an arbitrary element in R and u be a unit in R such that $u^2 = 1$ and $uk = k$. J. Kaur et al. have shown that for every r belonging to R, an element $\overline{r}$ belonging to R can be found such that $r + u\overline{r} = k$ [?]. It is easily seen that $\overline{(\overline{r})} = r$. This elememt $\overline{r}$ of R is defined as the complement of r with respect to u and k, by J. Kaur et al. Henceforth, we shall denote $\overline{r}$ by $(r)^c_{(u,k)}$ to emphasize its dependency on u and k and call it the (u, k) complement of r. A linear code C over R is said to be a cyclic code if for every codeword in C, all of its cyclic shifts also belong to C. A cyclic code C having length n over a ring R is said to be a reversible cyclic code if $(a_{n-1}, a_{n-2}, \cdots, a_0) \in C$ for every $(a_0, a_1, \cdots, a_{n-1}) \in C$. Let $a(z)$ be equal to $a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}$ be the polynomial representation of the codeword $(a_0, a_1, \cdots, a_{n-1})$. The reciprocal polynomial of a polynomial $a(z)$ in C is denoted by $a^*(z)$ and is equal to $z^{deg\left(a(z)\right)} a(1/z)$. The (u, k) reverse complement of $a(z)$ is defined by $(a_{n-1})^c_{(u,k)} + (a_{n-2})^c_{(u,k)} z + \cdots + (a_0)^c_{(u,k)} z^{n-1}$ and is denoted by $\big(a(z)\big)^{RC}_{(u,k)}$. A cyclic code C is called a (u, k) reversible complement code if $\big(a(z)\big)^{RC}_{(u,k)} \in C$ for every $a(z) \in C$.

3 Reversible complement cyclic codes

In this section, let R denote a finite chain ring and C denote a cyclic code having arbitrary length n over R. We obtain necessary conditions which are sufficient as well for C to be a (u, k) reversible complement code using the reversiblity conditions established by Monika et al. in [?]. We also present some examples of reversible complement cyclic codes over such rings. For the sake of completeness, we recall the structure of C over R [?] and the conditions for reversibility of C given by Monika et al. [?].

Let $S = \{f_0(z), f_1(z), \cdots, f_m(z)\}$ be a set of minimal degree polynomials of certain subsets of C with leading coefficient of $f_j(z)$ equal to $\gamma^{i_j} u_j$, where u_j is some unit in R, $deg\big(f_j(z)\big) < deg\big(f_{j+1}(z)\big)$, $i_j > i_{j+1}$ and i_j is the smallest such power. If $i_0 = 0$, then $f_0(z)$ is monic and we have $m = 0$.

Theorem 3.1. *([?]) Suppose C is a cyclic code over R and $S = \{f_0(z), f_1(z), \cdots, f_m(z)\}$, where $f_j(z)$ are polynomials of C as defined above. Then*

(i) S is a generating set for C.

(ii) For every j, $0 \leq j \leq m$, $f_j(z) = \gamma^{i_j} h_j(z)$ such that $h_j(z)$ is a monic polynomial over the finite chain ring having nilpotency index $\nu - i_j$ and maximal ideal $\langle\gamma\rangle$.

Theorem 3.2. *([?]) Let C be a cyclic code over R generated by S as defined earlier. Then C is reversible if and only if* (*i*) $f_{_0}^*(z) = u_{_0} f_{_0}(z)$ *for some unit* $u_{_0} \in R$,

(*ii*) $f_{_r}^*(z) - u_{_r} f_{_r}(z) \in \langle f_{_s}(z), f_{_{s-1}}(z), \cdots, f_{_0}(z)\rangle$ *for some* $s < r$ *and a unit* $u_{_r} \in R$, $0 < r \leq \nu - 1$.

We require the following lemma 3.1 to establish the main result of this article.

Lemma 3.1. *Let C be a cyclic code having length n over R generated by the set S. Let $a(z)$ be an arbitrary polynomial of degree s in C and $0(z)$ denote the zero polynomial in C. Then, the (u,k) reverse complement of $a(z)$ can be expressed as*

$$\big(a(z)\big)^{RC}_{_{(u,k)}} = \big(0(z)\big)^{RC}_{_{(u,k)}} - u^{-1} z^{n-s-1} a^*(z),$$

where $a^*(z)$ is the reciprocal polynomial of $a(z)$.

Proof. Let $0(z)$ be the zero polynomial of C and $a(z) = a_{_0} + a_{_1} z + \cdots + a_{_s} z^s$, for $a_{_i} \in R$, $0 \leq i \leq s < n$ be an arbitrary polynomial of degree s in C. Then $\big(0(z)\big)^{RC}_{_{(u,k)}} = u^{-1}k(z^{n-1} + z^{n-2} + \cdots + z + 1)$ and $\big(a(z)\big)^{RC}_{_{(u,k)}} = (a_{_0})^c_{_{(u,k)}} z^{n-1} + (a_{_1})^c_{_{(u,k)}} z^{n-2} + \cdots + (a_{_s})^c_{_{(u,k)}} z^{n-s-1} + u^{-1}k(z^{n-s-2} + \cdots + z + 1)$. Therefore, $\big(0(z)\big)^{RC}_{_{(u,k)}} - \big(a(z)\big)^{RC}_{_{(u,k)}} = \big(u^{-1}k - (a_{_0})^c_{_{(u,k)}}\big) z^{n-1} + \big(u^{-1}k - (a_{_1})^c_{_{(u,k)}}\big) z^{n-2} + \cdots + \big(u^{-1}k - (a_{_s})^c_{_{(u,k)}}\big) z^{n-s-1} = u^{-1}\big(a_{_0} z^{n-1} + a_{_1} z^{n-2} + \cdots + a_{_s} z^{n-s-1}\big) = u^{-1} z^{n-s-1} a^*(z)$. Thus, $\big(a(z)\big)^{RC}_{_{(u,k)}} = \big(0(z)\big)^{RC}_{_{(u,k)}} - u^{-1} z^{n-s-1} a^*(z)$. □

Theorem 3.3. *Consider a cyclic code C having length n over R, generated by S as defined earlier. Then, C is a (u,k) reversible complement code over R if and only if*

(*i*) $\big(0(z)\big)^{RC}_{_{(u,k)}} \in C$,

(*ii*) $f_{_0}^*(z) = u_{_0} f_{_0}(z)$ *for some unit* $u_{_0} \in R$,

(*iii*) $f_{_r}^*(z) - u_{_r} f_{_r}(z) \in \langle f_{_s}(z), f_{_{s-1}}(z), \cdots, f_{_0}(z)\rangle$ *for some* $s < r$ *and a unit* $u_{_r} \in R$, $0 < r \leq \nu - 1$.

Proof. Let C be a cyclic code having length n over R such that C is a (u,k) reversible complement code. Then $\big(a(z)\big)^{RC}_{_{(u,k)}} \in C$ for every $a(z)$ belonging to C. In particular, $\big(0(z)\big)^{RC}_{_{(u,k)}} \in C$. This proves (i). Using Lemma 3.1, we get that $u^{-1} z^{n-s-1} a^*(z) = \big(0(z)\big)^{RC}_{_{(u,k)}} - \big(a(z)\big)^{RC}_{_{(u,k)}} \in C$. Since C is cyclic, it follows that $a^*(z) \in C$ for every $a(z) \in C$. Thus, C is reversible. Conditions (ii) and (iii) now follow from Theorem 3.2.

Conversely, let C be a cyclic code having length n over R such that (i), (ii) and (iii) hold. Conditions (ii) and (iii) imply that C is reversible by Theorem 3.2 and therefore, $a^*(z)$ belongs to C for every $a(z)$ belonging to C. This together with condition (i) and Lemma 3.1 implies that $\big(a(z)\big)^{RC}_{_{(u,k)}} \in C$ for every $a(z)$ belonging to C. Thus, C is a (u,k) reversible complement code over R. □

Next, we provide some examples to support this result.

Example 3.1. *Let C be a cyclic code with length 4 over the ring $R = Z_2 + vZ_2 + v^2Z_2, v^3 = 0$ of characteristic 2. The following table classifies all principally generated cyclic codes of length 4 over R into $(1,1)$ reversible complement cyclic codes and not $(1,1)$ reversible complement cyclic codes. We shall denote $z+1$ by h in this table.*

S. No.	Cyclic code C	$(1,1)$ Reversible complement
1	$\langle 0 \rangle$	No
2	$\langle v^2 \rangle$	No
3	$\langle v^2 h \rangle$	No
4	$\langle v^2 h^2 \rangle$	No
5	$\langle v^2 h^3 \rangle$	No
6	$\langle v \rangle$	No
7	$\langle vh \rangle$	No
8	$\langle vh^2 \rangle$	No
9	$\langle vh^3 \rangle$	No
10	$\langle 1 \rangle$	Yes
11	$\langle h \rangle$	Yes
12	$\langle h^2 \rangle$	Yes
13	$\langle h^3 \rangle$	Yes
14	$\langle vh + v^2 \rangle$	No
15	$\langle vh^2 + v^2 \rangle$	No
16	$\langle vh^2 + v^2 h \rangle$	No
17	$\langle vh^2 + v^2(h+1) \rangle$	No
18	$\langle vh^3 + v^2 \rangle$	No
19	$\langle vh^3 + v^2 h(h+1) \rangle$	No
20	$\langle vh^3 + v^2 h \rangle$	No
21	$\langle h + v^2 \rangle$	Yes
22	$\langle h^2 + v^2 \rangle$	No
23	$\langle h^3 + v^2 \rangle$	No
24	$\langle h^3 + v^2 h \rangle$	No
25	$\langle h^3 + v^2(h+1) \rangle$	No