ISSN 0974 - 9373

Vol. 19 No. 2 (2015) **Journal of International Academy of Physical Sciences** pp. 117-121

# Reversible and Reversible Complement Cyclic Codes over Galois Rings

**Jasbir Kaur*, Sucheta Dutt and Ranjeet Sehmi**

Department of Applied Sciences
PEC University of Technology, Chandigarh-160012, INDIA
Email: kjasbir03@gmail.com, suchetapec@yahoo.co.in, rksehmi2003@yahoo.co.in

(Received May 02, 2015)

**Abstract:** Let $\Re$ be a Galois ring of characteristic $p^{\alpha}$ where $p$ is a prime and $a$ is a natural number. In this paper a relation between reversible cyclic codes and reversible complement cyclic codes has been determined. The reversible complement cyclic codes have applications in DNA-based computations.

**MSC:** 94B15, 94B05, 94B60.

**Keywords:** Cyclic codes, Reversible cyclic codes, Complement.

## 1. Introduction

The Galois ring $\Re = GR(p^a, m)$ is a Galois extension of $Z_{p^a}$ of degree $m$, where $p$ is a prime and $a$ is a natural number. The Galois ring of characteristic $p^a$ and cardinality $p^{am}$, where $m$ is a natural number, is isomorphic to the ring $Z_{p^a}[u]/f(u)$ where $f(u)$ is a monic basic irreducible polynomial of degree $m$ in $Z_{p^a}[u]$ [1, 2].

A cyclic code over a ring $R$ is a linear code which is invariant under cyclic shifts. The cyclic codes of length $n$ over a ring $R$ under a linear map can be considered as ideals of $R[x]/<x^n - 1>$. Thus the tuple $c = (c_0, c_1, ..., c_{n-1})$ can be identified with the polynomial $c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$. Moreover, the reversible complement cyclic codes have wide applications in the field of DNA-based computations. For reference see [3-8].

This paper is organized as follows. In Section 2, a necessary and sufficient condition for a reversible cyclic code to be a reversible complement cyclic code has been obtained, thereby extending a result of

Bennenni[3] to Galois rings. In Section 3, examples are given to illustrate the result obtained in Section 2. We have identified reversible complement cyclic codes in the list given by Abualrub[9] for single generator reversible cyclic codes of length 4 over $Z_4$.

## 2. Reversible and Reversible Complement Cyclic Codes

Let $\Re = GR(p^a, m) \cong Z_{p^a}[u]/<f(u)>$ be a Galois ring and $\Re_n = \Re[x]/<x^n - 1>$.

*Remark 1:* It can be easily seen that for every element *e* in $\Re$ there exists an element $\overline{e}$ such that $e + \overline{e} = 1 + u + u^2 + ... + u^{m-1}$. We shall call $\overline{e}$ the complement of *e*. Clearly $\overline{(\overline{e})} = e$.

**Definition 1:** *A cyclic code C of length n over a ring R is called reversible if* $(c_{n-1}, ..., c_1, c_0)$ *belongs to C whenever* $(c_0, c_1, ..., c_{n-1}) \in C$.

**Definition 2:** A cyclic code C of length n over a ring R is called reversible complement code if $(\overline{c}_{n-1}, ..., \overline{c}_1, \overline{c}_0) \in C$ whenever $(c_0, c_1, ..., c_{n-1}) \in C$.

The element $(\overline{c}_{n-1}, ..., \overline{c}_1, \overline{c}_0)$, represented as a polynomial $(c(x))^{RC}$, is called reversible complement of $c(x)$.

**Definition 3:** The reciprocal polynomial of $f(x) \in R[x]$ denoted as $f^*(x)$ is defined as $f^*(x) = x^{\deg(f(x))} f(1/x)$.

*Remark 2:* It is easy to prove that $((c^*(x))^{RC})^* = (c(x))^{RC}$ for $c(x)$ in *C*.

**Lemma 1:** *Let C be a reversible complement cyclic code over* $\Re$ *of length n. Then C is reversible.*

*Proof:* Let $g(u) = 1 + u + u^2 + ... + u^{m-1}$ and $0(x)$ be the zero polynomial in $\Re_n$. Then $0(x) \in C$ and hence $(0(x))^{RC} \in C$.

i.e. $g(u)(1 + ... + x^{n-2} + x^{n-1}) \in C$.

Let $c(x) = c_0 + c_1 x + ... + c_t x^t$, $0 \le t < n$, be a polynomial in *C*. Then

$$(c(x))^{RC} = g(u)(1 + x + ... + x^{n-t-2}) + (\overline{c}_t x^{n-t-1} + ... + \overline{c}_1 x^{n-2} + \overline{c}_0 x^{n-1})$$

belongs to $C$. Therefore, $g(u)(1+x+...+x^{n-1})-(c(x))^{RC} \in C$.
Moreover,

$$\begin{aligned} g(u)(1+x+...+x^{n-1})-(c(x))^{RC} &= (c_t x^{n-t-1}+...+c_1 x^{n-2}+c_0 x^{n-1}) \\ &= x^{n-t-1}(c_t+...+c_1 x^{t-1}+c_0 x^t) \end{aligned}$$

Therefore, $x^{n-t-1}(c_t+...+c_1 x^{t-1}+c_0 x^t) \in C$.

As $C$ is cyclic, $(c_t+...+c_1 x^{t-1}+c_0 x^t) \in C$.

So, $c^*(x) \in C$. Hence $C$ is a reversible cyclic code.

**Lemma 2:** *Let C be a reversible cyclic code over $\Re$ of length n such that* $(1+u+u^2+...+u^{m-1})(1+x+x^2+...+x^{n-2}+x^{n-1}) \in C$. *Then C is a reversible complement cyclic code.*

***Proof:*** Let $c(x)=c_0+c_1x+...+c_tx^t$, $0 \le t < n$, be a polynomial in $C$. As $C$ is cyclic,

$$x^{n-t-1}(c(x))=c_0x^{n-t-1}+...+c_{t-1}x^{n-2}+c_tx^{n-1} \in C.$$

Moreover, $g(u)(1+x+...+x^{n-2}+x^{n-1}) \in C$

where $g(u)=1+u+u^2+...+u^{m-1}$.

Therefore, $g(u)(1+x+...+x^{n-2}+x^{n-1})-(c_0x^{n-t-1}+...+c_{t-1}x^{n-2}+c_tx^{n-1}) \in C$.

i.e. $\quad g(u)(1+x+...+x^{n-t-2})+(\overline{c}_0x^{n-t-1}+...+\overline{c}_tx^{n-1})=(c^*(x))^{RC} \in C$.

As $C$ is reversible, $((c^*(x))^{RC})^* \in C$. This together with Remark 2 implies that $(c(x))^{RC} \in C$. Hence $C$ is a reversible complement cyclic code.
Lemmas 1 and 2 combine to give the following theorem:

**Theorem 1:** *A cyclic code C is a reversible complement cyclic code of length n over $\Re$ if and only if C is a reversible cyclic code of length n over $\Re$ and* $(1+u+u^2+...+u^{m-1})(1+x+...+x^{n-1}) \in C$.

## 3. Illustration

The single generator reversible cyclic codes over $Z_4 = GR(2^2,1)$ of length 4 as ideals of $\Re_4 = GR(2^2,1)/<x^4-1>$ have been obtained by Abualrub[1]. With the help of following examples, we illustrate that the class of reversible complement cyclic codes over $Z_4$ of length 4 is a proper subset of the class of reversible cyclic codes over $Z_4$ of length 4.

**Example 1:** *The reversible cyclic code* $C = < x^2 + 2x + 3 >$ *of length 4 over* $GR(2^2,1)$ *is reversible complement and* $(x^3 + x^2 + x + 1) \in C$.

**Example 2:** *The reversible cyclic code* $C = < x^2 + 3 >$ *of length 4 over* $GR(2^2,1)$ *is not reversible complement cyclic code and* $(x^3 + x^2 + x + 1) \notin C$.

In Table 1, we provide the complete list of single generator reversible cyclic codes and reversible complement cyclic codes of length 4 over $GR(2^2,1)$.

**Table 1:** Single generator reversible and reversible complement cyclic codes of length over $GR(2^2,1)$**.**

| Sr. No | Reversible | Reversible Complement |
|---|---|---|
| 1. | $< 1 >$ | Yes |
| 2. | $< x + 1 >$ | Yes |
| 3. | $< x + 3 >$ | Yes |
| 4. | $< x^2 + 1 >$ | Yes |
| 5. | $< x^2 + 3 >$ | No |
| 6. | $< x^2 + 2x + 1 >$ | No |
| 7. | $< x^2 + 2x + 3 >$ | Yes |
| 8. | $< x^3 + x^2 + x + 1 >$ | Yes |
| 9. | $< x^3 + 3x^2 + x + 3 >$ | No |
| 10. | $< 2x^3 + 2x^2 + 2x + 2 >$ | No |
| 11. | $< 2x^2 + 2 >$ | No |
| 12. | $< 2x + 2 >$ | No |
| 13. | $< 2 >$ | No |

## 4. Conclusion

In this paper a necessary and sufficient condition for a reversible cyclic code to be a reversible complement cyclic code has been obtained.

## Acknowledgements

The author (Jasbir Kaur) gratefully acknowledges the World Bank funded TEQIP II for financial support.

## References

**1.** B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

**2.** Z. X. Wan, *Finite fields and Galois rings*, World Scientific Publishing Company, 2011.

**3.** T. Abualrub, A. Ghrayeb and X. N. Zeng, Construction of cyclic codes over $GF(4)$ for DNA computing, *J. Franklin Inst.*, **343** (2006) 448-457.

**4.** A. Bayram, E. S. Oztas and I. Siap, Codes over $F_4+vF_4$ and some DNA applications, *Des. Codes Cryptogr.*, (2015) DOI: 10.1007/s10623-015-0100-8.

**5.** N. Bennenni, K. Guenda and S. Mesnager, New DNA cyclic codes over rings, *arXiv.org,* arXiv:1505.06263[cs.IT], (2015).

**6.** K. Guenda and T. A. Gulliver, Construction of cyclic codes over $F_2+uF_2$ for DNA computing, *Appl. Algebra Engrg. Comm. Comput.*, **24(6)** (2013) 445-459.

**7.** I. Siap, T. Abualrub and A. Ghrayeb, Cyclic DNA codes over the ring $F_2[u]/<u^2-1>$ based on the deletion distance, *J. Franklin Inst.*, **346** (2009) 731-740.

**8.** B. Yildiz and I. Siap, Cyclic codes over $F_2[u]/<u^4-1>$ and applications to DNA codes, *Comput. Math Appl.,* **63** (2012) 1169-1176.

**9.** T. Abualrub, Reversible cyclic codes over $Z_4$, *Australasian J. Combinatorics*, **38** (2007) 195-205.

**10.** J. L. Massey, Reversible codes, *Inform. Control,* **7(3)** (1964) 369-380.