

Construction of Dual Cyclic Codes over $\mathbb{F}_2[u, v]/\langle u^2, v^2 - v, uv - vu \rangle$ for DNA Computation

Abhay Kumar Singh[#], Narendra Kumar[#], Pooja Mishra[#], Indivar Gupta[@], and Manoj Kumar Singh^{@,*}

[#]Indian Institute of Technology (ISM), Dhanbad – 826 004, India

[@]DRDO-Scientific Analysis Group, Delhi – 110 054, India

^{*}E-mail: manojksingh@sag.drdo.in

ABSTRACT

Here, we assume the construction of cyclic codes over $\mathfrak{R} = \mathbb{F}_2[u, v]/\langle u^2, v^2 - v, uv - vu \rangle$. In particular, dual cyclic codes over $\mathfrak{R}_1 = \mathbb{F}_2[u]/\langle u^2 \rangle$ with respect to Euclidean inner product are discussed. The cyclic dual codes over \mathfrak{R} are studied with respect to DNA codes (reverse and reverse complement). Many interesting results are obtained. Some examples are also provided, which explain the main results. The GC-Content and DNA codes over \mathfrak{R} are discussed. We summarise the article by giving a special DNA table.

Keywords: Dual cyclic codes; DNA cyclic codes; Reverse constraint codes; Reverse constraint complement codes; The GC content

1. INTRODUCTION

Since last 30 years, cyclic codes have been well studied due to their rich algebraic structures. Cyclic codes also have practical implementations in DNA computing. The cyclic codes constructions over of 16 element have great interest and these are an extension of cyclic codes over the rings of 4 element. Due to which, many authors attracted to study the rings of 16 element in a series of papers¹⁻³. In particular, Yildiz², *et al.* assumed the ring \mathfrak{R} with $u^2 = u$ and $v^2 = v$ of 16 elements, where they studied the cyclic codes over such ring. Recently, Gao⁴, *et al.* discussed various categories of linear codes over the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$ of 16 elements.

In 1987, Tom Haed introduced the computing by DNA and Adleman first time used the DNA computation to discuss the Hamiltonian path problem⁵. DNA computing is better than silicon-based computing because of their storage capacity, which attracted several authors to study the cyclic DNA codes over some rings. In particular, Guenda⁶, *et al.* considered the structure of \mathfrak{R}_1 of 4 element. They discussed the construction of cyclic codes over such ring for DNA computing. Benneni⁷, *et al.* discussed the new DNA cyclic codes over ring. Later, Zhu⁸, *et al.* discussed the cyclic DNA codes over \mathfrak{R} and explored the application in DNA computing. Recently, ring $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$ of 16 element is considered⁹, where they stabilised the theory for DNA construction. They also explained the GC-content of these codes on the basis of deletion distance. The cyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ and its DNA computing were also studied. Further,

Dinh¹⁰, *et al.* considered the ring of 64 element and discussed the DNA codes by applying the Chinese Remainder Theorem. These works encourage us to study the DNA dual cyclic codes for our purpose.

2. PRELIMINARIES

Here, we remind some basic facts and results, which will be used throughout the paper. Let η be the gray map, which maps the elements of \mathfrak{R} to the elements of \mathfrak{R}_1 and is given as,

$$\eta(a + bv) = (a, a + b),$$

where $a, b \in \mathfrak{R}_1$.

Let two n-tuples h and $k \in \mathfrak{R}^n$. The Euclidean inner product is given as $h.k = h_0k_0 + h_1k_1 + \dots + h_{n-1}k_{n-1}$. For the code C over \mathfrak{R} of length n , the dual code of C is as given by $C^\perp = \{h \in \mathfrak{R}^n \mid h.k = 0, \forall k \in C\}$.

The set $S_{D_4} = \{A, T, G, C\}$ represents the DNA alphabet. The elements of the ring \mathfrak{R}_1 are given as $0, 1, u, 1+u$. Here, we can easily see that the elements of S_{D_4} and \mathfrak{R}_1 are related by 0 to A , 1 to G , u to T , and $1+u$ to C . By WCC rule, $\bar{A} = T$, $\bar{T} = A$, $\bar{G} = C$ and $\bar{C} = G$. The set $S_{D_{16}}$ is given below, which is taken from¹.

$$S_{D_{16}} = \left\{ \begin{array}{l} AA, AT, AC, AG, TT, TA, TC, TG, \\ CC, CA, CT, CG, GG, GA, GT, GC \end{array} \right\}$$

The elements of the set $S_{D_{16}}$ are known as DNA double pairs. We define a map $\psi: C \rightarrow S_{D_{16}}^{2^n}$, such that

$$\begin{aligned} &(a_0 + b_0v, a_1 + b_1v, \dots, a_{n-1} + b_{n-1}v) \\ &\rightarrow (a_0, a_1, \dots, a_{n-1}, a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1}), \end{aligned}$$

where $a_i, b_i \in \mathfrak{R}_1$. Let $x = (x_0, x_1, \dots, x_{n-2}, x_{n-1}) \in \mathfrak{R}^n$. We define the reverse of x to be $x^r = (x_{n-1}, x_{n-2}, \dots, x_1, x_0)$, the complement of x to be $x^c = (\bar{x}_0, \bar{x}_1, \dots, \bar{x}_{n-2}, \bar{x}_{n-1})$ and the reverse-complement of x to be $x^c = \bar{x}_0, \bar{x}_1, \dots, \bar{x}_{n-2}, \bar{x}_{n-1}$. A code C is reversible, if each codeword $x \in C$, x^r is also in C and C is called reversible complement if $x^{rc} \in C, \forall x \in C$. The reciprocal of a polynomial $c(x) = c_0 + c_1x + \dots + c_{r-2}x^{r-1} + c_r x^r$ with $c_r \neq 0$ is defined as polynomial $c^*(x) = c_r + c_{r-1}x + \dots + c_1x^{r-1} + c_0x^r$. If $c^*(x) = c(x)$, then $c(x)$ is known as self-reciprocal polynomial. The number of places in which the DNA codeword has coordinate C or G is known as GC-content.

3. DUAL CODES OVER \mathfrak{R}_1

Here, we study the generator polynomials for the dual cyclic codes over \mathfrak{R}_1 .

Theorem 3.1¹¹ Let C be a cyclic code in $\mathfrak{R}_{1,n} = \mathfrak{R}_1[x]/(x^n-1)$. Then

(i). If n be an odd no, then $c = (g, ua) = (g+ua)$, where g and a is polynomials over \mathbb{F}_2 . Then dual of code C is

$$C^\perp = (\tilde{u}\tilde{h}), \text{ and } \tilde{h} \mid (x^n-1).$$

(ii). If n is even, then, let $g = a$, then, $c = (g+ua)$ where $g \mid (x^n-1) \pmod 2$ and $(g+up) \mid (x^n-1)$ in \mathfrak{R} and $g \mid p\hat{g}$

. Then the dual of C is $C^\perp = \left(\left(\frac{x^n-1}{g} \right)^* + ux^i(m_2)^* \right)$ with $p \left(\frac{x^n-1}{g} \right) = gm_2$ and

$$i = \deg \left(\frac{x^n-1}{g} \right) - \deg(m_2) \text{ where } \left(\frac{x^n-1}{g} \right) \mid (x^n-1) \pmod 2 \text{ and}$$

$$\left(\left(\frac{x^n-1}{g} \right)^* + ux^i(m_2)^* \right) \mid (x^n-1) \text{ in } \mathfrak{R} \text{ and } \left(\frac{x^n-1}{g} \right) \mid (x^i(m_2)^*) \left(\frac{x^n-1}{g} \right)^*.$$

(iii). Let $g \neq a$, then $C = (g + up, ua)$, where g, a, p are polynomials over \mathbb{F}_2 with $a \mid g \mid (x^n-1) \pmod 2$, $a \mid p\hat{g}$, where $\hat{g} = \left(\frac{x^n-1}{g} \right)$ and $\deg p \leq \deg a$. Then the dual of C ,

$$C^\perp = \left(\left(\frac{x^n-1}{a} \right)^* + ux^i(m_2)^*, u \left(\frac{x^n-1}{g} \right)^* \right) \text{ with } p \left(\frac{x^n-1}{g} \right) = gm_2,$$

$$i = \deg \left(\frac{x^n-1}{g} \right) - \deg(m_2), \text{ where } \left(\frac{x^n-1}{g} \right)^*, \left(\frac{x^n-1}{a} \right)^*, \text{ and}$$

$x^i(m_2)^*$ are polynomials over \mathbb{F}_2 with

$$\left(\frac{x^n-1}{g} \right)^* \mid \left(\frac{x^n-1}{a} \right)^* \mid (x^n-1) \pmod 2, \left(\frac{x^n-1}{g} \right)^* \mid x^i(m_2)^* \left(\frac{x^n-1}{a} \right)^*$$

$$\text{and } \deg(x^i(m_2)^*) \leq \deg \left(\frac{x^n-1}{g} \right)^*.$$

Proof: Proof is similar to paper¹³ [Theorem 4].

4. DNA CODES

We mainly study the dual DNA cyclic codes over \mathfrak{R} by using the generators of dual cyclic codes over \mathfrak{R}_1 in the present section. First discuss the reverse constraint codes over \mathfrak{R} . For this purpose, some useful lemmas are as given, which are easily verified by examples.

Lemma 4.1¹⁰ Let h, k be any two polynomials over with $\deg h \leq \deg k$. Then

$$(i) (h.k)^* = h^* k^*$$

$$(ii) (h + k)^* = h^* + x^{\deg h - \deg k} k^*.$$

Lemma 4.2¹² Let $C = (f)$ be a cyclic code over \mathbb{F}_2 , where f is a monic polynomial. Then C is a reversible if and only if f is a self-reciprocal polynomial over \mathbb{F}_2 .

Lemma 4.3 For odd length n , let $C^\perp = (\tilde{u}\tilde{h})$ be a cyclic code over \mathfrak{R}_1 , where $\tilde{h} = \left(\frac{x^n-1}{g} \right)^*$. Then necessary and sufficient

for reversible of C^\perp is \tilde{h} is self-reciprocal polynomial.

Example 4.1 Let $g = (x-1)(x^3+x+1)$ and hence $\tilde{h} = (x^3+x^2+1)$ be a polynomial in x^7-1 over \mathbb{F}_2 . It is easy to see that \tilde{h} is self-reciprocal. Since $C^\perp = (\tilde{u}\tilde{h})$, therefore C^\perp is reversible code.

Lemma 4.4 For even length n , let $C^\perp = \left(\left(\frac{x^n-1}{g} \right)^* + ux^i(m_2)^* \right)$ be a cyclic code over \mathfrak{R}_1 . Then necessary and sufficient conditions for reversible of C^\perp are

$$(1). \left(\frac{x^n-1}{g} \right)^* \text{ is self-reciprocal.}$$

$$(2). (i). x^i(x^i(m_2)^*)^* = x^i(m_2)^* \text{ or}$$

$$(ii). \left(\frac{x^n-1}{g} \right)^* = x^j(x^i(m_2)^*)^* + x^i(m_2)^*, \text{ where}$$

$$j = \deg \left(\frac{x^n-1}{g} \right)^* - \deg(x^i(m_2)^*).$$

Example 4.2 Let $x^{10}-1 = g_1^2 g_2^2 = (x+1)^2(x^4+x^3+x^2+x+1)^2$ over \mathbb{F}_2 . Let cyclic code $C = (g_1 g_2^2 + u g_2^2 C_0)$

and $C^\perp = \left(\left(\frac{x^n-1}{g} \right)^* + ux^i(m_2)^* \right)$. Hence, we

have $\left(\frac{x^n-1}{g} \right)^* = g_1, m_2 = C_0$ and $x^i(m_2)^* = x C_0$.

$$x^j(x^i(m_2)^*)^* = x^i(m_2)^*, \text{ where } j = \deg \left(\frac{x^n-1}{g} \right)^* - \deg(x^i(m_2)^*) = 0.$$

Hence, C^\perp is reversible.

Lemma 4.5 For even length n ,

Let $C^\perp = \left(\left(\frac{x^n - 1}{a} \right)^* + ux^i(m_2)^*, u \left(\frac{x^n - 1}{g} \right)^* \right)$ be a cyclic code over \mathfrak{R}_1 . Then necessary and sufficient conditions for reversible of C^\perp are

(1). $\left(\frac{x^n - 1}{g} \right)^*, \left(\frac{x^n - 1}{a} \right)^*$ are self-reciprocal.

(2). $\left(\frac{x^n - 1}{g} \right)^* \mid \left[x^j \left(x^i(m_2)^* \right)^* + x^i(m_2)^* \right]$,

where $j = \deg \left(\frac{x^n - 1}{g} \right)^* - \deg \left(x^i(m_2)^* \right)$.

Example 4.3 Let $x^{10} - 1 = g_1^2 g_2^2 = (x + 1)^2 (x^4 + x^3 + x^2 + x + 1)^2$ over \mathbb{F}_2 . Let cyclic code and $C^\perp = \left(\left(\frac{x^n - 1}{a} \right)^* + ux^i(m_2)^*, u \left(\frac{x^n - 1}{g} \right)^* \right)$. We have

$\left(\frac{x^n - 1}{a} \right)^* = g_1 g_2, \left(\frac{x^n - 1}{g} \right)^* = g_1, m_2 = 1$ and $x^i(m_2)^* = x$. We

can easily check that $\left(\frac{x^n - 1}{g} \right)^*, \left(\frac{x^n - 1}{a} \right)^*$ are self-

reciprocal and $\left(\frac{x^n - 1}{g} \right)^* \mid \left[x^j \left(x^i(m_2)^* \right)^* + x^i(m_2)^* \right]$, where

$j = \deg \left(\frac{x^n - 1}{g} \right)^* - \deg \left(x^i(m_2)^* \right) = 4$, hence, follows the result.

Theorem 4.6 For general length n , let $C^\perp = vC_1^\perp \oplus (1 + v)C_2^\perp$, be a cyclic code over \mathfrak{R} , where C_1^\perp and C_2^\perp are cyclic codes over \mathfrak{R}_1 . Then C^\perp is reversible if and only if C_1^\perp and C_2^\perp are reversible cyclic codes respectively

Proof First, we consider C_1^\perp and C_2^\perp are reversible, which means $(C_1^\perp)^r \in C_1^\perp$ and $(C_2^\perp)^r \in C_2^\perp$ and $d = vd_1 + (1 + v)d_2$. Hence, $d^r = vd_1^r + (1 + v)d_2^r \in C^\perp$ where $d_1 \in C_1^\perp$ and $d_2 \in C_2^\perp$.. It is easy to see that $d_1^r \in C_1^\perp$ and $d_2^r \in C_2^\perp$, thus $d^r = vd_1^r + (1 + v)d_2^r \in C^\perp$. Therefore the dual of cyclic code C^\perp is reversible.

Conversely, if C^\perp is reversible, then for any $b_1 \in C_1^\perp, b_2 \in C_2^\perp$, we have $b = vb_1 + (1 + v)b_2 \in C^\perp$ Therefore $b^r = vb_1^r + (1 + v)b_2^r \in C^\perp$. Let, where $e_1 \in C_1^\perp$ and $e_2 \in C_2^\perp$. Then, . Thus, we get $b_1^r = e_1 \in C_1^\perp$ and $b_2^r = e_2 \in C_2^\perp$. Hence, both C_1^\perp and C_2^\perp are reversible.

Example 4.4 Let $\tilde{h}_1 = (x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1)$, $\tilde{h}_2 = (x^{11} + x^{10} + x^6 + x^5 + x + 1)$ be self-

reciprocal polynomials in $x^{15} - 1$.

Since $C^\perp = \langle g \rangle = (v\tilde{h}_1 + (1 + v)\tilde{h}_2) = vx^{13} + vx^{12} + (1 + v)x^{11} + x^{10} + vx^9 + vx^7 + x^6 + (1 + v)x^5 + vx^4 + vx^3 + x + 1$, and $g^r = x^{13} + x^{12} + vx^{10} + vx^9 + (1 + v)x^8 + x^7 + vx^6 + vx^4 + x^3 + (1 + v)x^2 + vx + v$.

On the other hand

$(v + (1 + v)x^2)g = x^{13} + x^{12} + vx^{10} + vx^9 + (1 + v)x^8 + x^7 + vx^6 + vx^4 + x^3 + (1 + v)x^2 + vx + v = g^r$ in C^\perp . Which means the cyclic code C^\perp is reversible.

Example 4.5 Let $\tilde{h}_1 = (x^6 + x^3 + 1)$ and $\tilde{h}_2 = (x^3 + 1)$ be two self-reciprocal polynomials in $x^9 - 1$. As $C^\perp = \langle g \rangle = (v\tilde{h}_1 + (1 + v)\tilde{h}_2) = 1 + x^3 + vx^6$, and $g^r = x^6 + x^3 + v$. An another way we can obtain as $(v + (1 + v)x^3)g = x^6 + x^3 + v = g^r \in C^\perp$. Therefore, C^\perp is reversible cyclic code.

Next, the reverse-complement codes over \mathfrak{R} are discussed. Some lemmas are taken from paper⁸, which are given below.

Lemma 4.7 $d + \bar{d} = u, d \in \mathfrak{R}$.

Lemma 4.8 Let $d, e \in \mathfrak{R}$, then $\overline{d + e} = \bar{d} + \bar{e} + u$.

Lemma 4.9 If $d \in \mathbb{F}_2$, then we get $u + \bar{u}d = ud$.

Using all these Lemmas, we describe the next result.

Theorem 4.10 Let $C^\perp = vC_1^\perp + (1 + v)C_2^\perp$ be a cyclic code over \mathfrak{R} . Then, c^\perp is reversible-compliment if and only if c^\perp is reversible and $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C^\perp$.

Proof Suppose that C^\perp is a cyclic code over.

For any $c = (c_{n-1}, c_{n-2}, \dots, c_1, c_0) \in C^\perp, c^r = (\bar{c}_{n-1}, \bar{c}_{n-2}, \dots, \bar{c}_1, \bar{c}_0) \in C^\perp$ as C^\perp is reverse compliment. It is well known that $0 \in C^\perp$, its compliment is also in c^\perp , then $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C^\perp$. Whence

$$\begin{aligned} c^r &= (c_0, c_1, \dots, c_{n-2}, c_{n-1}) \\ &= (\bar{c}_0, \bar{c}_1, \dots, \bar{c}_{n-2}, \bar{c}_{n-1}) \\ &+ (\bar{0}, \bar{0}, \dots, \bar{0}, \bar{0}) \in C^\perp \end{aligned}$$

On the other side, the cyclic code c^\perp is reversible, which means for any $c \in C^\perp$, then c^r is in C^\perp . Since, $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C^\perp$, thus $c^r = (\bar{c}_{n-1}, \bar{c}_{n-2}, \dots, \bar{c}_1, \bar{c}_0) = (c_{n-1}, c_{n-2}, \dots, c_1, c_0) + (\bar{0}, \bar{0}, \dots, \bar{0}, \bar{0}) \in C^\perp$. Then, cyclic code c^\perp is reversible-complement.

5. THE GC WEIGHT

In present section, we discuss the construction of GC weight over \mathfrak{R} . Therefore, some results are given below, which will be used in main result.

Lemma 5.1 Let n be an odd number, and C be a cyclic codes over \mathfrak{R}_1 , then $c = (g, ua) = (g + ua)$, where g and a are polynomials over \mathbb{F}_2 . Then dual of code C is

$C^\perp = (u\tilde{h})$, with rank $n - \text{deg}(\tilde{h})$ and \mathbb{F}_2 -basis is given by $\{u\tilde{h}, u x \tilde{h}, \dots, u x^{n - \text{deg} \tilde{h} - 1} \tilde{h}\}$.

Lemma 5.2 Let C be a cyclic codes of even length over \mathfrak{R}_1 .

(1). If $g = a$, then $C = (g + up)$, with $p\left(\frac{x^n - 1}{g}\right) = gm_2$,

we have, $C^\perp = \left(\left(\frac{x^n - 1}{g}\right)^* + ux^i(m_2)^*\right)$ with $p\left(\frac{x^n - 1}{a}\right) = gm_2$

and $i = \text{deg}\left(\frac{x^n - 1}{g}\right) - \text{deg}(m_2)$. Let $\left(\frac{x^n - 1}{g}\right) = \tilde{h}$, then

$C^\perp = (\tilde{h} + ux^i(m_2)^*)$ has the rank $n - \text{deg}(\tilde{h})$ and \mathbb{F}_2 -

basis is given as $\{(\tilde{h} + ux^i(m_2)^*) x (\tilde{h} + ux^i(m_2)^*), \dots,$

$x^{n - \text{deg} \tilde{h} - 1} (\tilde{h} + ux^i(m_2)^*) u\tilde{h}, ux\tilde{h}, \dots, ux^{n - \text{deg} \tilde{h} - 1} \tilde{h}\}$.

(2) Let $C = (g + up, ua)$, with $p\left(\frac{x^n - 1}{g}\right) = gm_2$,

$p\left(\frac{x^n - 1}{a}\right) = gm_2, C^\perp = \left(\left(\frac{x^n - 1}{a}\right)^* + ux^i(m_2)^*, u\left(\frac{x^n - 1}{g}\right)^*\right)$

where $i = \text{deg}\left(\frac{x^n - 1}{g}\right) - \text{deg}(m_2)$. Let $\left(\frac{x^n - 1}{a}\right) = \tilde{h}$ and

$\left(\frac{x^n - 1}{g}\right) = \tilde{r}$, then $C^\perp = (\tilde{h} + ux^i(m_2)^*, u\tilde{r})$ is

of the rank $n - \text{deg} \tilde{r}$ and \mathbb{F}_2 -basis is $\{(\tilde{h} + ux^i(m_2)^*) x$

$(\tilde{h} + ux^i(m_2)^*), \dots, x^{n - \text{deg} \tilde{h} - 1} (\tilde{h} + ux^i(m_2)^*) u\tilde{h}, ux\tilde{h}, \dots,$

$ux^{n - \text{deg} \tilde{h} - 1} \tilde{h}, u\tilde{r}, ux\tilde{r}, \dots, ux^{\text{deg} \tilde{h} - \text{deg} \tilde{r} - 1} \tilde{r}\}$.

Next, we discuss the minimally generating set of C^\perp with the help of all \mathbb{F}_2 -basis.

Theorem 5.3 Suppose $C^\perp = vC_1^\perp + (1 + v)C_2^\perp$ is a cyclic code of over \mathfrak{R} . Then C^\perp has a minimally generating set $\Delta = v\pi + (1 + v)\theta$, where π and θ are minimally generating set of C_1^\perp and C_2^\perp , respectively.

Let $\psi(\Delta) = x^n\pi + \theta$, where π and θ are minimally generating set of C_1^\perp and C_2^\perp , respectively. Next, result explains the GC-content.

Theorem 5.4 For general length n , let $C^\perp = vC_1^\perp + (1 + v)C_2^\perp$ be a cyclic code of over \mathfrak{R} and $C_1^\perp = (\tilde{h}_1 + ux^i(m_{12})^*, u\tilde{r}_1), C_2^\perp = (\tilde{h}_2 + ux^i(m_{22})^*, u\tilde{r}_2)$, with

$\tilde{r}_1 | \bar{h}_1 | (x^n - 1), \tilde{r}_2 | \bar{h}_2 | (x^n - 1)$ and we have

$\text{deg}(m_{12}) \leq \tilde{r}_1, \text{deg}(m_{22}) \leq \tilde{r}_2$. Then hamming weight

calculator of $\chi = x^n \{ \tilde{h}_1, x \tilde{h}_1, \dots, x^{n - \text{deg} \tilde{h}_1 - 1} \tilde{h}_1 \} + \{ \tilde{h}_2, x \tilde{h}_2, \dots,$

$x^{n - \text{deg} \tilde{h}_2 - 1} \tilde{h}_2 \}$ gives the GC weight over \mathfrak{R} .

Proof Using the fact that the GC-content of C^\perp is the u times of $\psi(\chi)$. Using above Theorem,

$$u\psi(x) = u x^n \{ \tilde{h}_1, x \tilde{h}_1, \dots, x^{n - \text{deg} \tilde{h}_1 - 1} \tilde{h}_1 \} + u \{ \tilde{h}_2, x \tilde{h}_2, \dots, x^{n - \text{deg} \tilde{h}_2 - 1} \tilde{h}_2 \}$$

Hence GC weight is obtained as the Hamming weight of

$$\chi = x^n \{ \tilde{h}_1, x \tilde{h}_1, \dots, x^{n - \text{deg} \tilde{h}_1 - 1} \tilde{h}_1 \} + \{ \tilde{h}_2, x \tilde{h}_2, \dots, x^{n - \text{deg} \tilde{h}_2 - 1} \tilde{h}_2 \}$$

6. DNA CODES OVER \mathfrak{R}

Definition Let $\tilde{h}_1(x), \tilde{h}_2(x)$ be two polynomials, where $\tilde{h}_i = ((x^n - 1)/f_i)^*$ and $f_i \in \mathfrak{R}_1$ with $i = 1, 2$ and both dividing $x^n - 1$ over \mathfrak{R}_1 . Let

$\text{deg} \tilde{h}_1(x) = t_1, \text{deg} \tilde{h}_2(x) = t_2, k = \min\{n - t_1, n - t_2\}$

and we have $g = v\tilde{h}_1(x) + (1 + v)\tilde{h}_2(x)$. $L(g)$ is said to be ρ -set and defined as $L(g) = \{\epsilon_0, \epsilon_1, \dots, \epsilon_{k-1}, \xi_0, \xi_1, \dots, \xi_{k-1}\}$,

where $\epsilon(i) = x^i g, \xi(i) = x^i \rho(h), 0 \leq i \leq k-1$ and

$h = vx^{t_2 - t_1} \tilde{h}_1 + (1 + v)\tilde{h}_2$, if $t_1 \leq t_2, h = v\tilde{h}_1 + (1 + v)x^{t_1 - t_2} \tilde{h}_2$,

otherwise. Let $C^\perp = \langle g \rangle_{\mathfrak{R}}$ be the linear code over \mathfrak{R} .

Note that $\langle L(g) \rangle$ or $\langle g \rangle_{\mathfrak{R}}$ is the \mathfrak{R} -module.

Let $g = \alpha_0 + \alpha_1 x + \dots + \alpha_t x^t$ over \mathfrak{R} ,

$\rho(h) = \beta_0 + \beta_1 x + \dots + \beta_s x^s$ and the set $L(g)$ is obtained by

generator matrix

$$L(g) = \begin{bmatrix} \epsilon_0 \\ \xi_0 \\ \epsilon_1 \\ \xi_1 \\ \vdots \\ \vdots \\ \vdots \end{bmatrix} = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_t & \dots & 0 & \dots & \dots & 0 \\ \beta_0 & \beta_1 & \beta_2 & \dots & \dots & \dots & \beta_s & \dots & \dots & 0 \\ 0 & \alpha_0 & \alpha_1 & \dots & \dots & \alpha_t & \dots & \dots & \dots & 0 \\ 0 & \beta_0 & \beta_1 & \dots & \dots & \dots & \dots & \beta_s & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

Theorem 6.1 Let \tilde{h}_1 and \tilde{h}_2 be self-reciprocal polynomials dividing $x^n - 1$ over \mathfrak{R}_1 with degree t_1 and t_2 .

If $\tilde{h}_1 \neq \tilde{h}_2$, then $g = v\tilde{h}_1 + (1 + v)\tilde{h}_2$ and $|\langle L(g) \rangle| = 16^k$ where,

$k = \min\{n - t_1, n - t_2\}$. Also, $C^\perp = \langle L(g) \rangle$ is linear code over \mathfrak{R} and $\psi(C^\perp)$ is reversible DNA code.

Proof Already, we have discussed algebraic structures, which make proof complete. Here, we notice that the reverse of $C^\perp = \langle L(g) \rangle$ is given as $(\psi(\sum \theta_i \epsilon_i + \sum \gamma_i \xi_i)) = \psi(\sum \rho(\theta_i) \xi_{k-1-i} + \sum \rho(\gamma_i) \xi_{k-1-i})$, where $\theta_i, \gamma_i \in \mathfrak{R}$ and $0 \leq i \leq k-1$.

Example 6.1 Let $\tilde{h}_1 = x^4 + x^3 + x^2 + x + 1, \tilde{h}_2 = x + 1$, where both divides $x^5 - 1$ over \mathbb{F}_2 . Hence, $g = v\tilde{h}_1 + (1 + v)\tilde{h}_2 = vx^4 + vx^3 + vx^2 + x + 1, h = x^4 + x^3 + vx^2 + vx + v$ and we get $\rho(h) = x^4 + x^3 + (1 + v)x^2 + (1 + v)x + (1 + v)$. Thus, $C^\perp = \langle L(g) \rangle$ and $\psi(C^\perp)$ satisfy the reverse constraint. The generator matrix is defined as,

$$L(g) = \begin{bmatrix} \varepsilon_0 \\ \xi_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & v & v & v \\ 1+v & 1+v & 1+v & 1 & 1 \end{bmatrix}$$

Let $\theta_0 = v$ and $\gamma_0 = v + u$, and $\theta_0\varepsilon_0 + \gamma_0\xi_0 = (v + u + uv) + (v + u + uv)x + (v + u + uv)x^2 + ux^3 + ux^4$
 $C^\perp = (v + u + uv, v + u + uv, v + u + uv, u, u)$. Hence,

$\psi(C^\perp) = (TTTTGGGT)$. Again, $\psi(\theta_0)\xi_0 + \psi(\gamma_0)\varepsilon_0 = u + ux + (1 + v + uv)x^2 + (1 + v + uv)x^3 + (1 + v + uv)x^4$ and $C_2^\perp = (u, u, 1 + v + uv, 1 + v + uv, 1 + v + uv)$ and $\psi(C_2^\perp) = (TTGGTTT)$. Hence, we have $(\psi(C_1^\perp))^\vee = \psi(C_2^\perp)$. Therefore, $\psi(C^\perp)$ is reversible.

Corollary 6.2 Consider the code $C^\perp = vC_1^\perp \oplus (1 + v)C_2^\perp$, where C_1^\perp and C_2^\perp are reversible code and $C^\perp = \langle L(g) \rangle$ be a linear code over \mathfrak{R} . If $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C^\perp$, then $\psi(C^\perp)$ gives reversible-compliment code.

Example 6.2 Let the polynomial \tilde{h}_1 and \tilde{h}_2 , where both divide $x^7 - 1$ over \mathbb{F}_2 . Thus we have the polynomial $g = v\tilde{h}_1 + (1 + v)\tilde{h}_2 = \langle 1 + x + vx^2 + vx^3 + vx^4 + vx^5 + vx^6 \rangle$. Here, we can see that $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C^\perp$, thus follows the result.

Corollary 6.3 Let $C^\perp = vC_1^\perp \oplus (1 + v)C_2^\perp$ is a cyclic code over \mathfrak{R} , C_1^\perp and C_2^\perp are reversible code and $C^\perp = \langle L(g) \rangle$ be a linear code over \mathfrak{R} and $\psi(C^\perp)$ is a reversible-DNA code. If we add compliment of 0 vector to $L(g)$ then $\psi(C^\perp)$ satisfies the reversible-compliment constraint.

Corollary 6.4 Let C_1^\perp be a reversible and $g = v\tilde{h}_1 + (1 + v)\tilde{h}_2$ over \mathfrak{R} . Then $C^\perp = \langle g \rangle$ is a reversible cyclic code over \mathfrak{R} and $\psi(C^\perp)$ is a reversible DNA code. If $x - 1$ does not divide g , then $\psi(C^\perp)$ follows the reversible-compliment constraint.

Proof Rows of generator matrix of C^\perp are given as $g, xg, \dots, x^{t-1}g$, where t is dimension of C^\perp . Using the ρ -set $\langle L(g) \rangle$, we get $\left(\psi \left(\sum_i \theta_i x^i g \right) \right)^\vee = \psi \left(\sum_i \rho(\theta_i) x^{t-1-i} g \right)$ with $\theta_i \in \mathfrak{R}$ and $0 \leq i \leq t - 1$, thus C^\perp is reversible code. Since \tilde{h} does not affect the coefficients, so, we can use ρ -set $\langle L(g) \rangle$ as linear code. Dual code C^\perp contains $1 + x + x^2 + \dots + x^{n-1}$ as $x - 1$ does not divide g . Thus reversible-complement DNA code of $\psi(C^\perp)$ is obtained from corollary 6.2.

Example 6.3 Let $\tilde{h}_1 = 1 + x + x^3 + x^4 = \tilde{h}_2$ be polynomial, then $C^\perp = \langle g \rangle$ is reversible code over \mathfrak{R} . Using the paper¹³ [Theorem, 2.6], we get parameter [6, 2, 4]. In this example, we get 256 DNA code words in the decimal form in Table 1. For example, 985685 represent CCAAGGTTTT.

Table 1. DNA Correspondence of $C^\perp = \langle g \rangle$ explained in Example 6.3

| | | | | | | |
|----------|----------|----------|----------|----------|----------|----------|
| 0 | 325 | 650 | 975 | 131200 | 1331525 | 1331850 |
| 1332175 | 2662400 | 2663050 | 2662725 | 2663375 | 3993600 | 3993925 |
| 3994250 | 3994575 | 1300 | 1105 | 1950 | 1755 | 1332500 |
| 1332305 | 1333150 | 1334125 | 2663700 | 2663505 | 2664350 | 2664155 |
| 3994900 | 3994705 | 3995550 | 3995355 | 2600 | 2925 | 2210 |
| 2535 | 1333800 | 1334125 | 1333410 | 1333735 | 2665000 | 2665325 |
| 2664610 | 2664935 | 3996200 | 3996525 | 3995810 | 3996135 | 3900 |
| 3705 | 3510 | 3315 | 1335100 | 1334905 | 1334710 | 1334515 |
| 2666300 | 2666105 | 2665910 | 2665715 | 3997305 | 3997110 | 3996915 |
| 3997500 | 5324800 | 5325125 | 5325450 | 5325775 | 4526080 | 4526405 |
| 4526730 | 4527055 | 7987200 | 7987525 | 7987850 | 7988175 | 7188480 |
| 7188805 | 7189130 | 7189455 | 5326100 | 5325905 | 5326750 | 5326555 |
| 4527380 | 4527185 | 4528030 | 4527835 | 7988500 | 7988305 | 7989150 |
| 7988955 | 7189780 | 7189585 | 7190430 | 7190235 | 5327400 | 5327725 |
| 5327010 | 5327335 | 4528680 | 4529005 | 4528290 | 4528615 | 7989800 |
| 7990125 | 7989410 | 7989735 | 7191080 | 7191405 | 7190690 | 7191015 |
| 5328700 | 5328505 | 5328310 | 5328115 | 4529980 | 4529785 | 4529590 |
| 4529395 | 7991100 | 7990905 | 7990710 | 7990515 | 7192380 | 7192185 |
| 7191990 | 7191795 | 5324800 | 5325125 | 5325450 | 5325775 | 11980800 |
| 11981125 | 11981450 | 11981775 | 9052160 | 9052485 | 9052810 | 9053135 |
| 10383360 | 10383685 | 10384010 | 10384335 | 10650900 | 10650705 | 10651550 |
| 10651355 | 11982100 | 11981905 | 11982750 | 11982555 | 9053460 | 9053265 |
| 9054110 | 9053915 | 10384660 | 10384465 | 10385310 | 10385115 | 10652200 |
| 10652525 | 10651810 | 10652135 | 11983400 | 11983725 | 11983010 | 11983335 |
| 9054760 | 9055085 | 9054370 | 9054695 | 10385960 | 10386285 | 10385570 |
| 10385895 | 10653500 | 10653305 | 10653110 | 10652915 | 11984700 | 11984505 |
| 11984310 | 11984115 | 9056060 | 9055865 | 9055670 | 9055475 | 10387260 |
| 10387065 | 10386870 | 10386675 | 15974400 | 15974725 | 15975050 | 15975375 |
| 15175680 | 15176005 | 15176330 | 15176655 | 14376960 | 14377285 | 14377610 |
| 14377935 | 13578240 | 13578565 | 13578890 | 13579215 | 15975700 | 15975505 |
| 15976350 | 15976155 | 15176980 | 15176785 | 15177630 | 15177435 | 14378260 |
| 14378065 | 14378910 | 14378715 | 13579540 | 13579345 | 13580190 | 13579995 |
| 15977000 | 15977325 | 15976610 | 15976935 | 15178280 | 15178605 | 15177890 |
| 15178215 | 14379560 | 14379885 | 14379170 | 14379495 | 13580840 | 13581165 |
| 13580450 | 13580775 | 15978300 | 15978105 | 15977910 | 15977715 | 15179580 |
| 15179385 | 15179190 | 15178995 | 14380860 | 14380665 | 14380470 | 14380275 |
| 13582140 | 13581945 | 13581750 | 13581555 | | | |

7. CONCLUSIONS

In this article, the algebraic structures of dual cyclic codes over \mathfrak{R} are discussed. The necessary and sufficient condition of DNA codes properties over \mathfrak{R} have been discussed. The GC-content and DNA codes over \mathfrak{R} are also discussed with help of examples and a special DNA Table. The discussion on DNA dual cyclic codes over the generalised ring may be an open problem.

REFERENCES

- Oztas, E. S. & Siap, I. Lifted polynomials over \mathbb{F}_{16} and their applications to DNA codes. *Filomat*, 2013, **27**(3), 459-466.
doi: 10.2298/FIL13033459O.
- Yildiz, B. & Karadeniz, S. Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, *Designs, Codes and Cryptography*. 2011, **58**, 221-234.
doi: 10.1007/s10623-010-9399-3
- Bayram, A.; Oztas, E.S. & Siap, I. Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications. *Designs, Codes and Cryptography*, 2016, **80**, 379-393.
doi: 10.1007/s10623-015-0100-8, (2015).
- Gao, J.; Fu, F.W. & Gao, Y. Some classes of linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ and their applications to construct good and new Z4-linear codes. *Appl. Algebr. Eng. Comm.*, 2016, 131-53.
doi: 10.1007/s00200-016-0300-0.
- Adleman, L. Molecular computation of solutions to combinatorial problems. *Science*, 1994, **266**(5187), 1021-1024.
doi: 10.1126/science.7973651.
- Guenda, K. & Gulliver, T. A. Construction of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ for DNA computing. *Appl. Algebr. Eng. Comm.*, 2013, **24**(6), 445-459.
doi: 10.1007/s00200-0138-0188-x.
- Bennenni, Guenda K. & Mesnager S. New DNA cyclic codes over rings, arXiv preprint arXiv.1505.06263 (2015).
- Zhu, S. & Chen, X. Cyclic DNA codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and their applications. *J. Appl. Math. Comput.*, 2017, **55**(1-2), 479-93.
doi: 10.1007/s12190-016-1046-3.
- Dinh, H.Q.; Singh, A.K.; Pattanayak, S. & Sriboonchitta, S. Construction of cyclic DNA codes over the ring $\mathbb{Z}_4[u] / \langle u^2 - 1 \rangle$ based on the deletion distance. *Theoretical Comput. Sci.*, 2018.
doi: 10.1016/j.tcs.2018.06.002.
- Dinh, H.Q.; Singh, A.K.; Pattanayak, S. & Sriboonchitta, S. Cyclic DNA codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + v^2\mathbb{F}_2 + uv^2\mathbb{F}_2$. *Designs Code Cryptogr.*, 2017, **86**(7), 1451-1467.
doi: 10.1007/s10623-017-0405-x.
- Abualrub, T. & Siap, I. Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. *Designs Code Cryptogr.*, 2007, **42**(3), 273-287.
doi: 10.1007/s10623-006-9034-5.
- Massey, J.L. Reversible codes. *Information and Control*, 1964, **7**(3), 369-380.
doi: 10.1016/s0019-9958(64)90438-3.
- Shiromoto, K. & Storme, L. A Griesmer bound for linear codes over finite quasi-Fresenius rings. *Discrete Appl Math.*, 2003, **128**(1), 263-274.
doi: 10.1016/s166-218x(02)00450-x.

CONTRIBUTORS

Dr Abhay Kumar Singh received his MSc in (Mathematics) from Institute of Science, Banaras Hindu University, Varanasi, India, in 2002, and a PhD in Algebra from IIT (BHU) Varanasi, India, in 2007. Currently working as a Senior Assistant Professor, at Indian Institute of Technology (ISM) Dhanbad, India. He has been working on the areas of theory of rings and modules, algebraic coding theory, code base cryptography, etc. In the current study he has provided over all necessary guidance and support to carry out this work successfully.

Mr. Narendra kumar received his MSc in (Mathematics) from Institute of Science, Banaras Hindu University, Varanasi, India, in 2013. Presently he is working as a senior research scholar in the Department of Applied Mathematics at IIT(ISM), Dhanbad, India. His current research area is Algebraic Coding theory. In the current work, he has been written the whole paper and provided all results and examples.

Mrs Pooja Mishra received her MSc from Rewa University in 2003. Later on she received MTech from Amity University in 2013. Presently, she is pursuing her PhD from Indian Institute of Technology (ISM), Dhanbad. Her research interest is in information theory, cloud computing and image processing. In the current work she has involved to improve the work.

Dr Indivar Gupta received his MSc (Mathematics) from Jiwaji University Gwalior. He obtained his PhD from Indian Institute of Technology Delhi. Presently he is working as Scientist 'F' at SAG DRDO, Delhi. He has published more than 20 research paper in various international journals and conferences. His area of research includes cryptology and information security, finite field and number theory. In the paper, he has given valuable inputs for the development in computing a special DNA Table.

Mr Manoj Kumar Singh received his MSc (Mathematics) from CSJM University Kanpur. Presently, he is working as Scientist 'D' at SAG DRDO, Delhi. His area of research includes: Cryptology, coding theory and finite field. In the current paper, he has carried out exhaustive literature survey on Dual Cycle Codes over Rings for DNA computation. He has also provided all the support in preparing the manuscript for publication.