The structure of duals of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and some DNA codes

Srinivasulu Bathala* and
Maheshanand Bhaintwal

Department of Mathematics,
Indian Institute of Technology Roorkee,
Roorkee, India
Email: bslu1981@gmail.com
Email: mahesfma@iitr.ac.in
*Corresponding author

Abstract: In this paper, we study the structure of duals of cyclic codes over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2,\ u^2 = v^2 = 0,\ uv = vu$. We determine a unique set of generators for these codes. We also determine a minimal spanning set for a class of cyclic codes of odd length over R. A sufficient condition for a cyclic code of odd length over R to contain its dual is presented. We give a necessary and sufficient condition for a cyclic code of odd lengths over R to be reversible complement. Further, we construct DNA codes as images of reversible complement cyclic codes of odd length over R.

Keywords: DNA codes; duals of cyclic codes; reversible codes; reversible complement codes.

Reference to this paper should be made as follows: Srinivasulu, B. and Bhaintwal, M. (2017) 'The structure of duals of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and some DNA codes', *Int. J. Information and Coding Theory*, Vol. 4, No. 1, pp.79–100.

Biographical notes: Srinivasulu Bathala is pursuing PhD at the Department of Mathematics, Indian Institute of Technology Roorkee. He is currently working in the area of algebraic coding theory.

Maheshanand Bhaintwal is an Associate Professor at the Department of Mathematics, Indian Institute of Technology Roorkee. His research interests include codes over finite rings, skew codes and Boolean functions in coding theory and cryptography.

1 Introduction

Cyclic codes are an important class of linear codes because of their richness in algebraic structure and ease in practical usage. Cyclic codes over finite fields are well studied (MacWilliams and Sloane, 1997). Though cyclic codes over finite rings were introduced in early 1970s, they have received much attention after a breakthrough paper by Hammons et al. (1994), where certain good non-linear binary codes are shown as Gray images of linear codes over $\mathbb{Z}_4$. Since then, the structure of cyclic codes has been studied over various finite rings (Abualrub and Siap, 2007; Batoul, Guenda and Gulliver, 2014;

Bonnecaze and Udaya, 1999; Dinh and Lopez-Permouth, 2004; Pless and Qian, 1996; Zhu, Wang and Shi, 2010). Most of this study is over finite chain rings (Batoul, Guenda and Gulliver, 2014; Dinh and Lopez-Permouth, 2004). Recently, Yildiz and Karadeniz (2010, 2011) have studied codes over a non-chain ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2,\ u^2 = v^2 = 0$. They have determined the generator polynomials of cyclic codes over R and obtained some good binary codes as Gray images of these codes.

The structure of duals of cyclic codes over finite fields and more generally over finite chain rings is well known (Batoul, Guenda and Gulliver, 2014; Dinh and Lopez-Permouth, 2004; MacWilliams and Sloane, 1997). Zhu, Wang and Shi (2010) have investigated the structural properties of cyclic codes over the semi-local ring $\mathbb{F}_2 + v\mathbb{F}_2,\ v^2 = v$. They have shown that these codes are principally generated. They have also determined their duals. For odd length, Bonnecaze and Udaya (1999) have determined the generator polynomials of cyclic codes as well as their duals over the ring $\mathbb{F}_2 + u\mathbb{F}_2,\ u^2 = 0$. Recently, Abualrub and Siap (2007) have determined the generator polynomials of duals of cyclic codes of even length over the rings $\mathbb{F}_2 + u\mathbb{F}_2,\ u^2 = 0$ and $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2,\ u^3 = 0$. Motivated by the study of Abualrub and Siap (2007), in this paper, we study the structure of duals of cyclic codes of arbitrary length over the ring R.

In addition, we also construct some Deoxyribonucleic acid (DNA) codes over R. DNA codes are a class of algebraic codes possessing properties similar to DNA structure. DNA is a complex molecule that contains all the genetic information called genes, which is necessary to build the structure of a living organism and to its functioning. DNA contains two long polymers called strands which consist of four simple units called nucleotides, namely Adenine (A), Guanine (G), Thymine (T) and Cytosine (C). These two strands are twisted in the shape of a double helix, running in opposite directions to each other and are connected to each other by the Watson–Crick rule. According to this rule, A and G from one strand are connected, respectively, to T and C from the other strand. The connected nucleotides are called complements of each other. If $\bar{x}$ denotes the complement of a base nucleotide x, then we have $\bar{A} = T,\ \bar{T} = A,\ \bar{C} = G$ and $\bar{G} = C$. According to Watson–Crick complement (WCC), a DNA strand $x = x_1x_2\cdots x_k$ will be paired up with its reverse-complement $\bar{x}_k\bar{x}_{k-1}\cdots\bar{x}_1$. For example, a DNA strand $5' - AGATT - 3'$ will be paired up with $3' - AATCT - 5'$ strand.

DNA computing techniques address many combinatorial problems (Adleman, 1994; Lipton, 1995). DNA codes that satisfy certain combinatorial constraints have applications in reliable communication systems (Mansuripur et al., 2003). The complicated structure of DNA facilitates an excellent error-correcting capability of these codes. A DNA code is a cyclic code with some or all of the constraints: Hamming constraint, the reverse constraint, the reverse-complement constraint and the fixed GC-content. Gaborit and King (2005) studied DNA codes over the finite field $\mathbb{F}_4$ for the first time. Later Abualrub, Ghrayeb and Zeng (2006) developed the theory for construction of additive cyclic codes of odd length over $\mathbb{F}_4$ which are suitable for DNA computing. The study of DNA codes over finite fields has been extended to finite commutative rings (Bayram, Oztas and Siap, 2016; Liang and Wan, 2016; Siap, Abualrub and Ghrayeb, 2009; Yildiz and Siap, 2012). Yildiz and Siap studied DNA codes as reversible complement cyclic codes of odd length over the finite chain ring $\mathbb{F}_2[u]/\langle u^4 - 1\rangle$ by identifying the 16 elements of the ring with DNA double pairs (Yildiz and Siap, 2012). Similarly, Bennenni, Guenda and Mesnager (2015) studied DNA codes over the finite chain ring $\mathbb{F}_2[u]/\langle u^6\rangle$. The authors defined a new Gray map

and showed that the Gray images of these DNA codes of length n are quasi-cyclic codes of index six and of length $6n$ over the alphabet $\{A, G, C, T\}$. Recently Zhu and Chen (2015) have studied DNA codes over the semi-local ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2,\ u^2 = 0, v^2 = v$. They have constructed DNA codes as direct sum of reversible complement cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2,\ u^2 = 0$. Motivated from the constructions of DNA codes (Bennenni, Guenda and Mesnager, 2015; Yildiz and Siap, 2012; Zhu and Chen, 2015) over finite commutative rings, in this paper, we construct DNA codes through reversible cyclic codes of odd length over the non-chain local ring $\mathbb{F}_2[u, v]/\langle u^2, v^2\rangle$. There exists a one-one correspondence between the elements of *R* and the set of DNA double pairs $S_{D_{16}} = \{AA, AT, AG, AC, TT, TA, TG, TC, GG, GA, GC, GT, CC, CA, CG, CT\}$ such that the image of a reversible complement cyclic code over *R* is a DNA code satisfying the WCC property.

The paper is organised as follows. In Section 2, basic notations and definitions are given. In Section 3, we determine the generator polynomials of duals of cyclic codes over *R* and present a minimal spanning set for a class of cyclic codes of odd length over *R*. In Section 4, reversible cyclic codes over *R* are studied. In Section 5, we give a necessary and sufficient conditions for a cyclic code over *R* to be reversible complement. In Section 6, we construct DNA codes over *R*.

2 Cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$

Let *R* denote the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 = \{a + ub + vc + uvd \mid a, b, c, d \in \mathbb{F}_2\}$ with $u^2 = 0 = v^2$ and $uv = vu$. *R* is a commutative ring with identity and of characteristic two. More information about the ring can be found in Yildiz and Karadeniz (2010). A linear code $\mathcal{C}$ of length n over *R* is an *R*-submodule of R^n. $\mathcal{C}$ is called a cyclic code if it is closed with respect to cyclic shift, i.e. $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. Let $R_n = \frac{R[x]}{\langle x^n - 1\rangle}$. Identifying each n-tuple $(c_0, c_1, \ldots, c_{n-1})$ in R^n with the polynomial $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in R_n$, we see that $\mathcal{C}$ is a cyclic code of length n over *R* if and only if $\mathcal{C}$ is an ideal of R_n. A polynomial $f(x) \in R[x]$ is said to be regular if it is not a zero-divisor. The structure of cyclic codes of length n over *R* is given in Yildiz and Karadeniz (2011). In this section, we further simplify the structure of cyclic codes of odd length over *R* and give the generators for their duals. Hence we recall the basic notations and definitions that are given in Yildiz and Karadeniz (2011). The following theorem presents the structure of a cyclic code of length n over *R*.

Theorem 1: *Let $\mathcal{C}$ be a cyclic code of length n over the ring R. Then $\mathcal{C}$ is one of the followings:*

1 *(Yildiz and Karadeniz, 2011, Theorem 3.2) If n is odd, then* $\mathcal{C} = \langle g_1(x) + ua_1(x) + uvr_1(x),\ va_2(x) + uva_3(x)\rangle$, *where* $g_1(x), a_1(x), a_2(x), a_3(x), r_1(x)$ *are polynomials in* $\mathbb{Z}_2[x]/\langle x^n - 1\rangle$ *such that* $a_1(x)|g_1(x)|x^n - 1$, $a_3(x)|a_2(x)|x^n - 1$ *and* $a_2(x)|g_1(x)|x^n - 1$. *Or*

2 *(Yildiz and Karadeniz, 2011, Theorem 3.1) If n is even, then* $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x),\ ua_1(x) + vq_2(x) + uvr_2(x),\ va_1(x) + uvr_3(x),\ uva_3(x)\rangle$, *where* $g_1(x), p_1(x), a_1(x), a_2(x), a_3(x), q_1(x), q_2(x), r_1(x), r_2(x)$ *are polynomials*

in $\mathbb{Z}_2[x]/\langle x^n-1\rangle$ *such that* $a_1(x)|g_1(x)|(x^n-1)$, $a_3(x)|a_2(x)|g_1(x)|(x^n-1)$, $a_1(x)|p_1(x)\frac{x^n-1}{g_1(x)}$ *and* $a_3(x)|r_3(x)\frac{x^n-1}{a_2(x)}$. *Or*

3 *(Kewat, Ghosh and Pattanayak, 2015, Proposition 3.3). If* n *is even and* $a_3(x)=g_1(x)$, *then* $\mathcal{C}=\langle g_1(x)+up_1(x)+vq_1(x)+uvr_1(x)\rangle$ *with* $g_1(x)+up_1(x)+vq_1(x)+uvr_1(x)|(x^n-1)$ *in* R_n. *Further,* $\mathcal{C}$ *is a free cyclic code over R.*

The following result gives more details about the relationships between the generators of the cyclic code $\mathcal{C}$ of length n over R and the factorisation of x^n-1.

Theorem 2: *Let* $\mathcal{C}=\langle g_1(x)+up_1(x)+vq_1(x)+uvr_1(x),\ ua_1(x)+vq_2(x)+uvr_2(x),\ va_2(x)+uvr_3(x),\ uva_3(x)\rangle$ *be a cyclic code of length* n *over R. Then*

1 $a_2(x)$ *divides* $\frac{x^n-1}{a_1(x)}q_2(x)$;

2 $a_2(x)$ *divides* $\frac{x^n-1}{g_1(x)}\left[q_1(x)+\frac{p_1(x)}{a_1(x)}q_2(x)\right]$;

3 $a_2(x)$ *divides* $\frac{g_1(x)}{a_1(x)}q_2(x)$;

4 $a_3(x)$ *divides* $q_2(x)$;

5 $a_3(x)$ *divides* $\frac{x^n-1}{a_1(x)}\left[r_2(x)+\frac{q_2(x)}{a_2(x)}r_3(x)\right]$;

6 $a_3(x)$ *divides* $q_1(x)+\frac{g_1(x)}{a_1(x)}r_2(x)+\frac{g_1(x)}{a_1(x)a_2(x)}r_3(x)q_2(x)$;

7 $a_3(x)$ *divides* $\frac{x^n-1}{g_1(x)}\left[r_1(x)+\frac{p_1(x)}{a_1(x)}r_2(x)+\frac{q_1(x)+\frac{p_1(x)}{a_1(x)}q_2(x)}{a_2(x)}r_3(x)\right]$ *and,*

8 $a_3(x)$ *divides* $p_1(x)+\frac{g_1(x)}{a_2(x)}r_3(x)$.

Proof: The results directly follow from (Kewat, Ghosh and Pattanayak, 2015, Proposition 3.2) for $p=2$. □

The dual $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ of length n over R is defined as $\mathcal{C}^\perp=\{y\in R^n \mid c\cdot y=0 \text{ for every } c\in\mathcal{C}\}$, where the dot product is the usual Euclidian inner product over R. Obviously $\mathcal{C}^\perp$ is a linear code of length n over R. $\mathcal{C}$ is self-orthogonal if $\mathcal{C}\subseteq\mathcal{C}^\perp$ and self-dual if $\mathcal{C}=\mathcal{C}^\perp$.

The Hamming weight $w_H(c)$ of any $c\in R^n$ is the number of non-zero coordinates in c. The Hamming distance between any two elements c_1 and c_2 in R^n is defined as $d(c_1,c_2)=w_H(c_1-c_2)$, and it satisfies all metric axioms. The minimum Hamming distance of a linear code $\mathcal{C}$, denoted by $d_H(\mathcal{C})$, is defined as the minimum of the Hamming weights of non-zero codewords in $\mathcal{C}$. The Gray map ϕ from R to $\mathbb{Z}_2^4$ is given by $\phi(a+ub+vc+uvd)=(a+b+c+d,c+d,b+d,d)$, which can be extended to R^n in a natural way. The Lee weight of any $c\in R^n$ is defined as $w_L(c)=w_H(\phi(c))$. The Gray map ϕ is a linear isometry from $(R^n,\ d_L)$ to $(\mathbb{F}_2^{4n},\ d_H)$. Therefore, if $\mathcal{C}$ is a linear code of length n over R with 2^k codewords and minimum Lee distance d, then $\phi(\mathcal{C})$ is a binary $[4n,k,d]$-linear code (Yildiz and Karadeniz, 2011).

For a polynomial $f(x)=f_0+f_1x+\cdots+f_mx^m\in R[x]$ of degree m, the reciprocal of $f(x)$ is defined to be the polynomial $f^*(x)=x^mf(1/x)=f_m+f_{m-1}x+\cdots+$

$f_0 x^m$. We note that $\deg(f^*(x)) \leq \deg(f(x))$, and if $f_0 \neq 0$, then $\deg(f^*(x)) = \deg(f(x))$. $f(x)$ is called self-reciprocal if $f^*(x) = f(x)$.

Lemma 3: *Abualrub, Ghrayeb and Zeng (2006) Let* $f(x),\ g(x)$ *be any two polynomials in* $R[x]$ *with* $\deg(f(x)) \geq \deg(g(x))$. *Then*

1 $[f(x)g(x)]^* = f^*(x)g^*(x)$;

2 $[f(x) + g(x)]^* = f^*(x) + x^i g^*(x)$, *where* $i = deg(f(x)) - deg(g(x))$.

Now we present a simplified structure of cyclic codes of odd length n over the ring R.

Lemma 4: *Let* $\mathcal{C} = \langle g_1(x) + ua_1(x) + uvr_1(x),\ \ va_2(x) + uva_3(x)\rangle$ *be a cyclic code of odd length* n *over R, where* $g_1(x), a_1(x), a_2(x), a_3(x), r_1(x) \in \mathbb{Z}_2[x]$ *with* $a_1(x)|g_1(x)|(x^n - 1)$ *and* $a_3(x)|a_2(x)|g_1(x)|(x^n - 1)$ *over* $\mathbb{Z}_2$. *Then* $va_2(x) \in \mathcal{C}$ *and* $deg(r_1(x)) < deg(a_3(x))$.

Proof: We have $u(va_2(x) + uva_3(x)) = uva_2(x) \in \mathcal{C}$ and $\frac{x^n-1}{a_2(x)}(va_2(x) + uva_3(x)) = uv\frac{x^n-1}{a_2(x)}a_3(x) \in \mathcal{C}$. Since n is odd, $a_2(x)$ and $\frac{x^n-1}{a_2(x)}$ are relatively prime. Therefore there exist $p_1(x), p_2(x) \in \mathbb{Z}_2[x]$ such that $p_1(x)a_2(x) + p_2(x)\frac{x^n-1}{a_2(x)} = 1$, which implies that $uva_3(x) = p_1(x)a_3(x)[uva_2(x)] + p_2(x)\left[uv\frac{x^n-1}{a_2(x)}a_3(x)\right] \in \mathcal{C}$. Therefore $[va_2(x) + uva_3(x)] + [uva_3(x)] = va_2(x) \in \mathcal{C}$. For the second part, assume $\deg(r_1(x)) \geq \deg(a_3(x))$. Since $a_3(x)$ is monic, we can apply division algorithm. To that end, there exist polynomials $q(x)$ and $r(x)$ in $\mathbb{Z}_2[x]$ such that $r_1(x) = a_3(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(a_3(x))$. Since $uva_3(x) \in \mathcal{C}$, we have

$$\begin{aligned}
&\langle g_1(x) + ua_1(x) + uvr_1(x), va_2(x) + uva_3(x)\rangle \\
&\quad = \langle g_1(x) + ua_1(x) + uvr(x) + uvq(x)a_3(x), \\
&\qquad va_2(x) + uva_3(x)\rangle \\
&\quad = \langle g_1(x) + ua_1(x) + uvr(x), va_2(x) + uva_3(x)\rangle.
\end{aligned}$$

Hence, we may assume that $\deg(r_1(x)) < \deg(a_3(x))$. □

Theorem 5: *Let* $\mathcal{C} = \langle g_1(x) + ua_1(x) + uvr_1,\ \ va_2(x) + uva_3(x)\rangle$ *be a cyclic code of odd length* n *over R, where* $g_1(x), g_2(x), a_1(x)$ *and* $a_2(x)$ *are binary polynomials such that* $a_1(x)|g_1(x)|(x^n - 1)$ *and* $a_3(x)|a_2(x)|g_1(x)|(x^n - 1)$. *Then* $\mathcal{C} = \langle g_1(x) + ua_1(x),\ va_2(x) + uva_3(x)\rangle = \langle g_1(x),\ ua_1(x),\ va_2(x),\ uva_3(x)\rangle$.

Proof: Consider $v[g_1(x) + ua_1(x) + uvr_1(x)] + \frac{g_1(x)}{a_2(x)}[va_2(x))] = uva_1(x) \in \mathcal{C}$. This implies that $a_3(x)|a_1(x)$. Also, $\frac{x^n-1}{a_3(x)}[g_1(x) + ua_1(x) + uvr_1(x)] = uvr_1(x)\frac{x^n-1}{a_3(x)} \mod (x^n - 1)$, which implies that $a_3(x)|r_1(x)\frac{x^n-1}{a_3(x)}$. But since n is odd, we get $a_3(x)|r_1(x)$. Also, since $\deg(r_1(x)) < \deg(a_3(x))$, we must have $r_1(x) = 0$. From Lemma 4, we have $va_2(x), uva_3(x) \in \mathcal{C}$. As $r_1(x) = 0$, we can easily show that $g_1(x), ua_1(x) \in \mathcal{C}$. Therefore $\langle g_1(x),\ ua_1(x),\ va_2(x),\ uva_3(x)\rangle \subseteq \mathcal{C}$. The reverse inclusion is trivial. □

3 Duals of cyclic codes over R

Let I be an ideal of R_n. Then the annihilator $A(I)$ of I in R_n is defined as

$$A(I) = \{f(x) \in R_n \mid f(x)g(x) = 0 \text{ for all } g(x) \in I\}.$$

It is easy to see that if $\mathcal{C}$ is a cyclic code of length n over R with the associated ideal I, then the associated ideal of $\mathcal{C}^\perp$ is $A^*(I) = \{f^*(x) \mid f(x) \in A(I)\}$. In this section, we derive the duals of cyclic codes over R described in Theorem 1. We first give the duals of cyclic codes of odd lengths over R. Since the annihilator of a cyclic code is also a cyclic code, we have the following result.

Theorem 6: *Let $\mathcal{C} = \langle g_1(x), ua_1(x), va_2(x), uva_3(x)\rangle$ be a cyclic code of odd length n over R, where $a_1(x)|g_1(x)|(x^n-1)$ and $a_3(x)|a_2(x)|g_1(x)|(x^n-1)$ over $\mathbb{Z}_2$. Then $A(\mathcal{C}) = \left\langle \frac{x^n-1}{a_3(x)},\ u\frac{x^n-1}{a_2(x)}, v\frac{x^n-1}{a_1(x)}, uv\frac{x^n-1}{g_1(x)} \right\rangle$.*

Proof: Let $J = \left\langle \frac{x^n-1}{a_3(x)},\ u\frac{x^n-1}{a_2(x)}, v\frac{x^n-1}{a_1(x)}, uv\frac{x^n-1}{g_1(x)} \right\rangle$. Then clearly $J \subseteq A(\mathcal{C})$. Let $A(\mathcal{C}) = \langle h_1(x), uk_1(x), vh_2(x), uvk_2(x)\rangle$, where $k_1(x)|h_1(x)|(x^n-1)$ and $k_2(x)|h_2(x)|h_1(x)|(x^n-1)$ over $\mathbb{Z}_2$. As $uva_3(x) \in \mathcal{C}$ and $h_1(x) \in A(\mathcal{C})$, we have $uva_3(x) \cdot h_1(x) = 0 \pmod{x^n-1}$. This implies that $h_1(x) = \frac{x^n-1}{a_3(x)}s(x)$ for some $s(x) \in \mathbb{Z}_2[x]$, and so $h_1(x) \in \left\langle \frac{x^n-1}{a_3(x)} \right\rangle$. Similarly, we can see that $k_1(x) \in \left\langle \frac{x^n-1}{a_2(x)} \right\rangle$, $h_2(x) \in \left\langle \frac{x^n-1}{a_1(x)} \right\rangle$ and $k_2(x) \in \left\langle \frac{x^n-1}{g_1(x)} \right\rangle$. Therefore $A(\mathcal{C}) \subseteq J$, and the result follows. □

Corollary 7: *Let $\mathcal{C} = \langle g(x),\ ua(x)\rangle,\ a(x) \mid g(x) \mid (x^n-1)$ be a cyclic code of odd length over the ring $\mathbb{Z}_2 + u\mathbb{Z}_2,\ u^2 = 0$. Then the annihilator of $\mathcal{C}$ is $A(\mathcal{C}) = \left\langle \frac{x^n-1}{a(x)},\ u\frac{x^n-1}{g(x)} \right\rangle$.*

Proof: The proof follows from similar arguments as in Theorem 6. □

Example 1: *Let $\mathcal{C} = \langle x^2+x+1,\ uv\rangle$. Then $\mathcal{C}$ is a cyclic code of length 3 over R. The Gray image of $\mathcal{C}$ under ϕ, i.e. $\phi(\mathcal{C})$ is a $[12, 6, 3]$-binary linear code. Also, from Theorem 6, we get $\mathcal{C}^\perp = \langle u(x+1),\ v(x+1)\rangle$. Further, $\phi(\mathcal{C}^\perp)$ is an optimal $[12, 6, 4]$-binary linear code.*

Example 2: *Let $n = 7$, and $x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1) = f_1f_2f_3$. Let $\mathcal{C} = \langle uf_1f_3,\ vf_1f_2,\ uvf_1\rangle$. Then $\mathcal{C}$ is a cyclic code of length 7 over R. The Gray image of $\mathcal{C}$ under ϕ is an optimal $[28, 12, 8]$-binary linear code. Also, from Theorem 6, we get $\mathcal{C}^\perp = \langle f_2f_3,\ uf_2, vf_3, uv\rangle$. Further, $\phi(\mathcal{C}^\perp)$ is a $[28, 16, 4]$-binary linear code.*

In Table 1, we give examples of some good binary codes obtained as the Gray images of cyclic codes of odd length n over R and their corresponding duals. The binary codes whose parameters are marked with $*$ denote the optimal codes Grassl.

Now we give the generator polynomials of the duals of cyclic codes of even lengths over the ring R. The following result follows from Theorems 1 and 2.

Table 1 Binary images of some cyclic codes of length n over the ring R

Length	Generators of $\mathcal{C}$	The dual code $\mathcal{C}^{\perp}$	$\phi(\mathcal{C})$	$\phi(\mathcal{C}^{\perp})$
3	$\langle uv(x^2+x+1)\rangle$	$\langle x+1,\ u,\ v\rangle$	$[12,1,12]^*$	$[12,11,2]^*$
3	$\langle u(x^2+x+1),\ v(x+1),\ uv\rangle$	$\langle u(x^2+x+1),\ v(x+1),\ uv\rangle$	$[12,6,4]^*$	$[12,6,4]^*$
3	$\langle v(x+1),\ uv\rangle$	$\langle u(x^2+x+1),\ v\rangle$	$[12,5,4]^*$	$[12,7,2]$
3	$\langle x+1,\ uv\rangle$	$\langle u(x^2+x+1),\ v(x^2+x+1)\rangle$	$[12,9,2]^*$	$[12,3,6]^*$
3	$\langle u(x+1),\ v(x+1),\ uv\rangle$	$\langle u(x^2+x+1),\ v(x^2+x+1),\ uv\rangle$	$[12,7,4]^*$	$[12,5,4]^*$
7	$\langle uv(x+1)(x^3+x^2+1)\rangle$	$\langle x^3+x^2+1,\ u,\ v\rangle$	$[28,3,16]^*$	$[28,25,2]^*$

Lemma 8: *Let* $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x),\ ua_1(x) + vq_2(x) + uvr_2(x),\ va_2(x) + uvr_3(x),\ uva_3(x)\rangle$ *be a cyclic code of length* n *over* R*, where* $a_1(x)|g_1(x)|(x^n-1)$ *and* $a_3(x)|a_2(x)|g_1(x)|(x^n-1)$ *over* $\mathbb{Z}_2$*. Then there exist polynomials* $m_1(x),\ m_2(x),\ m_3(x),\ m_4(x), m_5(x)$ *and* $m_6(x)$ *in* $\mathbb{Z}_2[x]$ *such that*

1 $\frac{x^n-1}{g_1(x)}p_1(x) = m_1(x)a_1(x)$;

2 $\frac{x^n-1}{a_1(x)}q_2(x) = m_2(x)a_2(x)$;

3 $\frac{x^n-1}{g_1(x)}\left[q_1(x) + \frac{p_1(x)}{a_1(x)}q_2(x)\right] = m_3(x)a_2(x)$;

4 $\frac{x^n-1}{a_2(x)}r_3(x) = m_4(x)a_3(x)$;

5 $\frac{x^n-1}{a_1(x)}\left[r_2(x) + \frac{q_2(x)}{a_2(x)}r_3(x)\right] = m_5(x)a_3(x)$ *and*

6 $\frac{x^n-1}{g_1(x)}\left[r_1(x) + \frac{p_1(x)}{a_1(x)}r_2(x) + \frac{q_1(x)+\frac{p_1(x)}{a_1(x)}q_2(x)}{a_2(x)}r_3(x)\right] = m_6(x)a_3(x)$.

Lemma 9: *Let* $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x),\ ua_1(x) + vq_2(x) + uvr_2(x),\ va_2(x) + uvr_3(x),\ uva_3(x)\rangle$ *be a cyclic code of length* n *over* R*, where* $a_1(x)|g_1(x)|(x^n-1)$ *and* $a_3(x)|a_2(x)|g_1(x)|(x^n-1)$ *over* $\mathbb{Z}_2$*. Then* $m_2(x)g_1(x) = 0$.

Proof: Since $m_2(x)g_1(x) = \frac{x^n-1}{a_2(x)}\left[\frac{g_1(x)}{a_1(x)}q_2(x)\right]$ and $a_2(x)|\frac{g_1(x)}{a_1(x)}q_2(x)$, the result follows. □

Theorem 10: *Let* $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x),\ ua_1(x) + vq_2(x) + uvr_2(x),\ va_2(x) + uvr_3(x),\ uva_3(x)\rangle$ *be a cyclic code of even length* n *over* R*, where* $a_1(x)|g_1(x)|(x^n-1)$ *and* $a_3(x)|a_2(x)|g_1(x)|(x^n-1)$ *over* $\mathbb{Z}_2$*. Then* $A(\mathcal{C}) = \left\langle \frac{x^n-1}{a_3(x)} + um_4(x) + vm_5(x) + uvm_6(x), u\frac{x^n-1}{a_2(x)} + vm_2(x) + uvm_3(x), v\frac{x^n-1}{a_1(x)} + uvm_1(x), uv\frac{x^n-1}{g_1(x)}\right\rangle$*, where* $m_i(x),\ i = 1,2,\ldots,6$ *are as defined in Lemma 8.*

Proof: Let $J = \left\langle \frac{x^n-1}{a_3} + um_4 + vm_5 + uvm_6, u\frac{x^n-1}{a_2} + vm_2 + uvm_3, v\frac{x^n-1}{a_1} + uvm_1, uv\frac{x^n-1}{g_1}\right\rangle$. First we show that $J \subseteq A(\mathcal{C})$. We have the following identities:

(i) $\left(uv\frac{x^n-1}{g_1}\right)(g_1 + up_1 + vq_1 + uvr_1) = uv\frac{x^n-1}{g_1}g_1 = 0.$

$$(ii)\quad \left(v\frac{x^n-1}{a_1}+uvm_1\right)(ua_1+vq_2+uvr_2)=uv\frac{x^n-1}{a_1}a_1=0.$$

$$(iii)\quad \left(v\frac{x^n-1}{a_1}+uvm_1\right)(g_1+up_1+vq_1+uvr_1)=v\frac{x^n-1}{a_1}g_1+uv\frac{x^n-1}{a_1}p_1+uvm_1g_1$$
$$=0+uvm_1g_1+uvm_1g_1=0.$$

$$(iv)\quad \left(u\frac{x^n-1}{a_2}+vm_2+uvm_3\right)(va_2+uvr_3)=uv\frac{x^n-1}{a_2}a_2=0.$$

$$(v)\quad \left(u\frac{x^n-1}{a_2}+vm_2+uvm_3\right)(ua_1+vq_2+uvr_2)=uv\frac{x^n-1}{a_2}q_2+uva_1m_2$$
$$=uva_1m_2+uva_1m_2$$
$$=0.$$

Since $m_2g_1=0$, we have

$$(vi)\quad \left(u\frac{x^n-1}{a_2}+vm_2+uvm_3\right)(g_1+up_1+vq_1+uvr_1)$$
$$=u\frac{x^n-1}{a_2}g_1+uv\frac{x^n-1}{a_2}q_1+vm_2g_1+uvm_2p_1+uvm_3g_1$$
$$=uv\frac{x^n-1}{a_2}\left[q_1+\frac{p_1}{a_1}q_2\right]+uv\frac{x^n-1}{a_2}\frac{p_1}{a_1}q_2+uv\frac{x^n-1}{a_2}\frac{p_1}{a_1}q_2+uvm_3g_1$$
$$=uvm_3g_1+uvm_3g_1$$
$$=0.$$

$$(vii)\quad \left(\frac{x^n-1}{a_3}+um_4(x)+vm_5(x)+uvm_6(x)\right)(uva_3)=u\frac{x^n-1}{a_3}a_3=0.$$

$$(viii)\quad \left(\frac{x^n-1}{a_3}+um_4+vm_5+uvm_6\right)(va_2+uvr_3)$$
$$=v\frac{x^n-1}{a_3}a_2+uv\frac{x^n-1}{a_3}r_3+uvm_4a_2$$
$$=uvm_4a_2+uvm_4a_2$$
$$=0.$$

$$(ix)\quad \left(\frac{x^n-1}{a_3}+um_4+vm_5+uvm_6\right)(ua_1+vq_2+uvr_2)$$
$$=u\frac{x^n-1}{a_3}a_1+v\frac{x^n-1}{a_3}q_2+uv\frac{x^n-1}{a_3}r_2+uvm_4q_2+uvm_5a_1$$
$$=uv\frac{x^n-1}{a_3}r_2+uv\frac{x^n-1}{a_2a_3}r_3q_2+uvm_5a_1$$
$$=uv\frac{x^n-1}{a_3}\left[r_2+\frac{q_2}{a_2}r_3\right]+uvm_5a_1$$
$$=uvm_5a_1+uvm_5a_1=0.$$

From Lemma 8, we have

$$
\begin{aligned}
(x)\quad & \left(\frac{x^n-1}{a_3} + um_4 + vm_5 + uvm_6\right)(g_1 + up_1 + vq_1 + uvr_1) \\
&= \frac{x^n-1}{a_3}g_1 + u\frac{x^n-1}{a_3}p_1 + v\frac{x^n-1}{a_3}q_1 + uv\frac{x^n-1}{a_3}r_1 + um_4g_1 \\
&\quad + uvm_4q_1 + vm_5g_1 + uvm_5p_1 + uvm_6g_1 \\
&= u\left[\frac{x^n-1}{a_3}p_1 + \frac{x^n-1}{a_2a_3}r_3g_1\right] + v\left[\frac{x^n-1}{a_3}q_1 + \frac{x^n-1}{a_1a_3}\left(r_2 + \frac{q_2}{a_2}r_3\right)g_1\right] \\
&\quad + uv\left[\frac{x^n-1}{a_3}r_1 + m_4q_1 + m_5p_1\right] + uvm_6g_1 \\
&= u\frac{x^n-1}{a_3}\left[p_1 + \frac{g_1}{a_2}r_3\right] + v\frac{x^n-1}{a_3}\left[q_1 + \frac{r_2}{a_1}g_1 + \frac{q_2}{a_1a_2}r_3g_1\right] \\
&\quad + uv\frac{x^n-1}{a_3}\left[r_1(x) + \frac{p_1}{a_1}r_2 + \frac{q_1 + \frac{p_1}{a_1}q_2}{a_2}r_3\right] + uvm_6g_1 \\
&= 0 + 0 + uvm_6g_1 + uvm_6g_1 = 0.
\end{aligned}
$$

It follows from (i) to (x) above that $J \subseteq A(\mathcal{C})$.

On the other hand, to prove $A(\mathcal{C}) \subseteq J$, we let $A(\mathcal{C}) = \langle \hat{g}_1 + u\hat{p}_1 + v\hat{q}_1 + uv\hat{r}_1,\ u\hat{a}_1 + v\hat{q}_2 + uv\hat{r}_2,\ v\hat{a}_2 + uv\hat{r}_3,\ uv\hat{a}_3\rangle$ such that $\hat{a}_3|\hat{a}_2|\hat{g}_1|x^n-1$ and $\hat{a}_3|\hat{a}_1|\hat{g}_1|x^n-1$ over $\mathbb{Z}_2$. Since $(uv\hat{a}_3)(g_1 + up_1 + vq_1 + uvr_1) = 0 \pmod{x^n-1}$, we get $\hat{a}_3g_1 = 0 \pmod{x^n-1}$ and therefore $\hat{a}_3 = \frac{x^n-1}{g_1}t_1$ for some $t_1 \in \mathbb{Z}_2[x]$. Moreover, since $uv\frac{x^n-1}{g_1} \in J$, we have

$$uv\hat{a}_3 = t_1\left[uv\frac{x^n-1}{g_1}\right] \in J \tag{1}$$

Similarly, as $(v\hat{a}_2 + uv\hat{r}_3)(ua_1 + vq_2 + uvr_2) = 0 \pmod{x^n-1}$, so $uv\hat{a}_2a_1 = 0 \pmod{x^n-1}$ and therefore $\hat{a}_2 = \frac{x^n-1}{a_1}t_2$ for some $t_2 \in \mathbb{Z}_2[x]$. Again, as $(v\hat{a}_2 + uv\hat{r}_3)(g_1 + up_1 + vq_1 + uvr_1) = 0 \pmod{x^n-1}$, we have $v\frac{x^n-1}{a_1}t_2g_1 + uvt_2\frac{x^n-1}{a_1}p_1 + uv\hat{r}_3g_1 = 0 \pmod{x^n-1}$. This implies that $m_1g_1t_2 + \hat{r}_3g_1 = 0 \pmod{x^n-1}$. Therefore, $\hat{r}_3 = \frac{x^n-1}{g_1}t_3 + m_1t_2$ for some $t_3 \in \mathbb{Z}_2[x]$. Also, we have

$$
\begin{aligned}
v\hat{a}_2 + uv\hat{r}_3 &= v\frac{x^n-1}{a_1}t_2 + uv\frac{x^n-1}{g_1}t_3 + uvm_1t_2 \\
&= t_2\left[v\frac{x^n-1}{a_1} + uvm_1\right] + t_3\left[uv\frac{x^n-1}{g_1}\right] \in J.
\end{aligned} \tag{2}
$$

Now since $(u\hat{a}_1 + v\hat{q}_2 + uv\hat{r}_2)(va_2 + uvr_3) = 0 \pmod{x^n-1}$, we have $uv\hat{a}_1a_2 = 0 \pmod{x^n-1}$ and therefore $\hat{a}_1 = \frac{x^n-1}{a_2}t_4$ for some $t_4 \in \mathbb{Z}_2[x]$. Again, $(u\hat{a}_1 + v\hat{q}_2 + uv\hat{r}_2)(ua_1 + vq_2 + uvr_2) = 0 \pmod{x^n-1}$, which implies that $uv\hat{a}_1q_2 + uv\hat{q}_2a_1 = 0 \pmod{x^n-1}$. This further implies that $\frac{x^n-1}{a_2}q_2t_4 + \hat{q}_2a_1 = 0 \pmod{x^n-1}$.

Therefore, $t_4 m_2 a_1 + \hat{q}_2 a_1 = 0 \pmod{x^n - 1}$. Hence $\hat{q}_2 = \frac{x^n-1}{a_1} t_5 + m_2 t_4$ for some $t_5 \in \mathbb{Z}_2[x]$. Further, we have

$$\begin{aligned}
0 &= (u\hat{a}_1 + v\hat{q}_2 + uv\hat{r}_2)(g_1 + up_1 + vq_1 + uvr_1) \\
&= ut_4 \frac{x^n-1}{a_2} g_1 + uvt_4 \frac{x^n-1}{a_2} q_1 + vt_5 \frac{x^n-1}{a_1} g_1 + vm_2 g_1 t_4 + uvt_5 \frac{x^n-1}{a_1} p_1 \\
&\quad + uvm_2 p_1 t_4 + uv\hat{r}_2 g_1 \\
&= 0 + uvt_4 \frac{x^n-1}{a_2} q_1 + 0 + t_4 \frac{x^n-1}{a_2} \left(\frac{g_1}{a_1} q_2 \right) + uvt_5 \frac{x^n-1}{a_1} p_1 \\
&\quad + uv \frac{x^n-1}{a_1 a_2} q_2 p_1 t_4 + uv\hat{r}_2 g_1 \\
&= uvt_4 \frac{x^n-1}{a_2} \left[q_1 + \frac{p_1}{a_1} q_2 \right] + uvt_5 m_1 g_1 + uv\hat{r}_2 g_1 \\
&= uvt_4 m_3 g_1 + uvt_5 m_1 g_1 + uv\hat{r}_2 g_1.
\end{aligned}$$

Therefore, $uvt_4 m_3 g_1 + uvt_5 m_1 g_1 + uv\hat{r}_2 g_1 = 0 \pmod{x^n - 1}$. Hence $\hat{r}_2 = \frac{x^n-1}{g_1} t_6 + m_3 t_4 + m_1 t_5$ for some $t_6 \in \mathbb{Z}_2[x]$. Now we show $u\hat{a}_1 + v\hat{q}_2 + uv\hat{r}_2 \in J$. We have

$$\begin{aligned}
u\hat{a}_1 + v\hat{q}_2 + uv\hat{r}_2 &= u \frac{x^n-1}{a_2} t_4 + v \frac{x^n-1}{a_1} t_5 + vm_2 t_4 \\
&\quad + uv \frac{x^n-1}{g_1} t_6 + uvm_3 t_4 + uvm_1 t_5 \\
&= t_4 \left[u \frac{x^n-1}{a_1} + vm_2 + uvm_3 \right] + t_5 \left[v \frac{x^n-1}{a_1} + uvm_1 \right] \\
&\quad + t_6 \left[uv \frac{x^n-1}{g_1} \right] \in J. \qquad (3)
\end{aligned}$$

Finally, as $(\hat{g}_1 + u\hat{p}_1 + v\hat{q}_1 + uv\hat{r}_1)(uva_3) = 0 \pmod{x^n - 1}$, so $uv\hat{g}_1 a_3 = 0 \pmod{x^n - 1}$ and therefore $\hat{g}_1 = \frac{x^n-1}{a_3} t_7$ for some $t_7 \in \mathbb{Z}_2[x]$. Also, $(\hat{g}_1 + u\hat{p}_1 + v\hat{q}_1 + uv\hat{r}_1)(va_2 + uvr_3) = 0 \pmod{x^n - 1}$ implies that $\frac{x^n-1}{a_a} r_3 t_7 + \hat{p}_1 a_2 = 0 \pmod{x^n - 1}$. Therefore, $t_7 m_4 a_2 + \hat{p}_1 a_2 = 0 \pmod{x^n - 1}$, and so $\hat{p}_1 = \frac{x^n-1}{a_2} t_8 + m_4 t_7$ for some $t_8 \in \mathbb{Z}_2[x]$. Now we have

$$\begin{aligned}
0 &= (\hat{g}_1 + u\hat{p}_1 + v\hat{q}_1 + uv\hat{r}_1)(ua_1 + vq_2 + uvr_2) \\
&= uvt_7 \frac{x^n-1}{a_3} r_2 + uvt_8 \frac{x^n-1}{a_2} q_2 + uvt_7 \frac{x^n-1}{a_2 a_3} r_3 q_2 + uva_1 \hat{q}_1 \\
&= uvt_7 \frac{x^n-1}{a_3} \left[r_2 + \frac{q_2}{a_2} r_3 \right] + uvt_8 \frac{x^n-1}{a_2} q_2 + uva_1 \hat{q}_1 \\
&= uvt_7 m_5 a_1 + uvt_8 m_2 a_1 + uva_1 \hat{q}_1.
\end{aligned}$$

Therefore $\hat{q}_1 = \frac{x^n-1}{a_1} t_9 + t_8 m_2 + t_7 m_5$ for some $t_9 \in \mathbb{Z}_2[x]$. Again we have

$$\begin{aligned}
0 &= (\hat{g}_1 + u\hat{p}_1 + v\hat{q}_1 + uv\hat{r}_1)(g_1 + up_1 + vq_1 + uvr_1) \\
&= \hat{g}_1 g_1 + u\left[p_1 \hat{g}_1 + \hat{p}_1 g_1\right] + v\left[q_1 \hat{g}_1 + \hat{q}_1 g_1\right] + uvr_1 \hat{g}_1 + uv\hat{p}_1 q_1 + uv\hat{q}_1 p_1 + uv\hat{r}_1 g_1
\end{aligned}$$

$$
\begin{aligned}
&= 0 + u\left[t_7\frac{x^n-1}{a_3}p_1 + t_8\frac{x^n-1}{a_2}g_1 + t_7\frac{x^n-1}{a_2a_3}r_3g_1\right] + v\left[q_1\hat{g}_1 + \hat{q}_1g_1\right]\\
&\quad + uvr_1\hat{g}_1 + uv\hat{p}_1q_1 + uv\hat{q}_1p_1 + uv\hat{r}_1g_1\\
&= ut_7\frac{x^n-1}{a_3}\left[p_1 + \frac{r_3}{a_2}g_1\right] + v\left[q_1\hat{g}_1 + \hat{q}_1g_1\right] + uvr_1\hat{g}_1 + uv\hat{p}_1q_1\\
&\quad + uv\hat{q}_1p_1 + uv\hat{r}_1g_1\\
&= 0 + v\left[t_7\frac{x^n-1}{a_3}q_1 + t_9\frac{x^n-1}{a_1}g_1 + t_8\frac{x^n-1}{a_1a_2}q_2g_1\right.\\
&\qquad\qquad \left. + t_7\frac{x^n-1}{a_3}g_1\left(r_2 + \frac{q_2}{a_2}r_3\right)\right]\\
&\quad + uvr_1\hat{g}_1 + uv\hat{p}_1q_1 + uv\hat{q}_1p_1 + uv\hat{r}_1g_1\\
&= vt_7\frac{x^n-1}{a_3}\left[q_1 + \frac{g_1}{a_1}r_2 + \frac{g_1}{a_1a_2}q_2r_3\right] + uvr_1\hat{g}_1 + uv\hat{p}_1q_1 + uv\hat{q}_1p_1 + uv\hat{r}_1g_1\\
&= 0 + uvr_1\hat{g}_1 + uv\hat{p}_1q_1 + uv\hat{q}_1p_1 + uv\hat{r}_1g_1\\
&= uvt_7\frac{x^n-1}{a_3}r_1 + uvt_8\frac{x^n-1}{a_2}q_1 + uvt_7\frac{x^n-1}{a_2a_3}r_3q_1\\
&\quad + uvt_9\frac{x^n-1}{a_1}p_1 + uvt_8\frac{x^n-1}{a_1a_2}q_2p_1\\
&\quad + uvt_7\frac{x^n-1}{a_1a_3}\left(r_2 + \frac{q_2}{a_2}r_3\right)p_1 + uv\hat{r}_1g_1\\
&= uvt_7\frac{x^n-1}{a_3}\left[r_1(x) + \frac{p_1(x)}{a_1(x)}r_2(x) + \frac{q_1(x) + \frac{p_1(x)}{a_1(x)}q_2(x)}{a_2(x)}r_3(x)\right]\\
&\quad + uvt_8\frac{x^n-1}{a_2}\left[q_1 + \frac{p_1}{a_1}q_2\right] + uvt_9\frac{x^n-1}{a_1}p_1 + uv\hat{r}_1g_1\\
&= uvt_7m_6g_1 + uvt_8m_3g_1 + uvt_9m_1g_1 + uv\hat{r}_1g_1.
\end{aligned}
$$

Therefore $\hat{r}_1 = \frac{x^n-1}{g_1}t_{10} + t_7m_6 + t_8m_3 + t_9m_1$ for some $t_{10} \in \mathbb{Z}_2[x]$. Finally we show that $\hat{g}_1 + u\hat{p}_1 + v\hat{q}_1 + uv\hat{r}_1 \in J$. For that consider

$$
\begin{aligned}
\hat{g}_1 + u\hat{p}_1 + v\hat{q}_1 + uv\hat{r}_1 &= \frac{x^n-1}{a_3}t_7 + u\frac{x^n-1}{a_2}t_8 + um_4t_7\\
&\quad + v\frac{x^n-1}{a_1}t_9 + vm_2t_8 + vm_5t_7\\
&\quad + uv\frac{x^n-1}{g_1}t_{10} + uvm_6t_7 + uvm_3t_8 + uvvm_1t_9\\
&= t_7\left[\frac{x^n-1}{a_3} + um_4 + vm_5 + uvm_6\right]\\
&\quad + t_8\left[u\frac{x^n-1}{a_2} + vm_2 + uvm_3\right]\\
&\quad + t_9\left[v\frac{x^n-1}{a_1} + uvm_1\right] + t_{10}\left[uv\frac{x^n-1}{g_1}\right] \in J. \qquad (4)
\end{aligned}
$$

Hence from (1), (2), (3) and (4), we get $A(\mathcal{C}) \subseteq J$. Thus $A(\mathcal{C}) = J$. □

Corollary 11: *Let* $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x)\rangle$ *be a free cyclic code of even length* n *over* R *such that* $(g_1(x) + up_1(x) + vq_1(x) + uvr_1(x))|(x^n - 1)$. *Then* $A(\mathcal{C}) = \left\langle \frac{x^n-1}{g_1(x)} + um_4(x) + vm_5(x) + uvm_6(x)\right\rangle$, *where* $\frac{x^n-1}{g_1(x)}p_1(x) = m_4(x)g_1(x)$, $\frac{x^n-1}{g_1(x)}q_1(x) = m_5(x)g_1(x)$ *and* $\frac{x^n-1}{g_1(x)}\left[r_1(x) + \frac{p_1(x)}{g_1(x)}q_1(x) + \frac{q_1(x)}{g_1(x)}p_1(x)\right] = m_6(x)g_1(x)$.

Proof: Let $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x)\rangle$ be a free cyclic code of even length n over R. Then $\mathcal{C}$ can also be written as $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x),\ ug_1(x) + uvq_1(x),\ vg_1(x) + uvp_1(x),\ uvg_1(x)\rangle$. Comparing $\mathcal{C}$ with the cyclic code given in Theorem 10, we get $a_1(x) = a_2(x) = a_3(x) = g_1(x),\ q_2(x) = 0$, $r_2(x) = q_1(x)$ and $r_3(x) = p_1(x)$. Therefore, the annihilator of $\mathcal{C}$ is of the form $A(\mathcal{C}) = \left\langle \frac{x^n-1}{g_1(x)} + um_4(x) + vm_5(x) + uvm_6(x), u\frac{x^n-1}{g_1(x)} + vm_2(x) + uvm_3(x), v\frac{x^n-1}{g_1(x)} + uvm_1(x), uv\frac{x^n-1}{g_1(x)}\right\rangle$, where $\frac{x^n-1}{g_1(x)}p_1(x) = m_1(x)g_1(x),\ m_2(x) = 0,\ \frac{x^n-1}{g_1(x)}q_1(x) = m_3(x)g_1(x)$, $\frac{x^n-1}{g_1(x)}p_1(x) = m_4(x)g_1(x),\ \frac{x^n-1}{g_1(x)}q_1(x) = m_5(x)g_1(x)$ and $\frac{x^n-1}{g_1(x)}\left[r_1(x) + \frac{p_1(x)}{g_1(x)}q_1(x) + \frac{q_1(x)}{g_1(x)}p_1(x)\right] = m_6(x)g_1(x)$. This implies that $m_1(x) = m_4(x)$ and $m_3(x) = m_5(x)$. Therefore,

$$\begin{aligned} A(\mathcal{C}) &= \left\langle \frac{x^n-1}{g_1(x)} + um_4(x) + vm_5(x) + uvm_6(x),\ u\frac{x^n-1}{g_1(x)} + vm_2(x)\right. \\ &\quad \left. + uvm_3(x),\ v\frac{x^n-1}{g_1(x)} + uvm_1(x),\ uv\frac{x^n-1}{g_1(x)}\right\rangle \\ &= \left\langle \frac{x^n-1}{g_1(x)} + um_4(x) + vm_5(x) + uvm_6(x),\ u\frac{x^n-1}{g_1(x)} + 0 + uvm_5(x),\right. \\ &\quad \left. v\frac{x^n-1}{g_1(x)} + uvm_4(x),\ uv\frac{x^n-1}{g_1(x)}\right\rangle \\ &= \left\langle \frac{x^n-1}{g_1(x)} + um_4(x) + vm_5(x) + uvm_6(x)\right\rangle. \end{aligned}$$

Hence the result. □

Example 3: *Let* $n = 4$ *and* $\mathcal{C} = \langle (x^2+1) + u(x+1) + v(x+1) + uv\rangle$ *be a cyclic code of length* 4 *over* R. *Clearly* $(x^2+1) + u(x+1) + v(x+1) + uv$ *divides* $x^4 - 1$. *Therefore,* $\mathcal{C}$ *is a free cyclic code. Further from Corollary 11, we get* $A(\mathcal{C}) = \langle (x^2+1) + u(x+1) + v(x+1) + uv\rangle$. *This implies that* $\mathcal{C}^\perp = \langle (x^2+1) + u(x+1) + v(x+1) + uv\rangle$, *and so* $\mathcal{C}$ *a self-dual code. The Gray image of* $\mathcal{C}$, *i.e.* $\phi(\mathcal{C})$ *is a binary* $[16, 8, 4]$*-linear code.*

Example 4: *Let* $n = 4$. *We have* $x^4 - 1 = (x-1)^4$. *Let* $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x),\ ua_1(x) + vq_2(x) + uvr_2(x),\ va_2(x) + uvr_3(x),\ uva_3(x)\rangle$, *where* $g_1(x) = (x+1)^2$, $a_1(x) = a_2(x) = x + 1$, $a_3(x) = 1$, $p_1(x) = q_1(x) = q_2(x) = 1$ *and* $r_1(x) = r_2(x) = r_3(x) = 0$. *The generators of* $\mathcal{C}$ *satisfy all the conditions that are given in Theorem 2. Therefore,* $\mathcal{C}$ *is a cyclic code of length* 4 *over* R. *The Gray image of* $\mathcal{C}$ *is an optimal binary code with the parameters* $[16, 12, 2]$. *Further, from Lemma 8*

and Theorem 10, we get $m_1(x) = x+1$, $m_2(x) = (x+1)^2$, $m_3(x) = x$, $m_4(x) = m_5(x) = m_6(x) = 0$, *and* $A(\mathcal{C}) = \langle u(x+1)^3 + v(x+1)^2 + uvx,\ v(x+1)^3 + uv(x+1),\ uv(x+1)^2\rangle$. *This implies that* $\mathcal{C}^\perp = \langle u(x+1)^3 + vx(x+1)^2 + uvx^2,\ v(x+1)^3 + uvx^2(x+1),\ uv(x+1)^2\rangle$, $\phi(\mathcal{C}^\perp)$ *is a* $[16, 4, 8]$*-binary linear code, which is an optimal code.*

Example 5: *Let* $\mathcal{C} = \langle g_1(x) + up_1(x) + vq_1(x) + uvr_1(x),\ ua_1(x) + vq_2(x) + uvr_2(x),\ va_2(x) + uvr_3(x),\ uva_3(x)\rangle$, *where* $g_1(x) = (x+1)^3$, $a_1(x) = (x+1)^2$, $a_2(x) = (x+1)^2$, $a_3(x) = x+1$, $p_1(x) = q_1(x) = q_2(x) = r_1(x) = r_2(x) = r_3(x) = 0$. *The generators of* $\mathcal{C}$ *satisfy all the conditions of Theorem 2. Therefore,* $\mathcal{C}$ *is a cyclic code of length* 4 *over R. The Gray image of* $\mathcal{C}$ *is a binary code with the parameters* $[16, 8, 4]$. *From Lemma 8 and Theorem 10, we get* $m_1(x) = m_2(x) = m_3(x) = m_4(x) = m_5(x) = m_6(x) = 0$, *and* $A(\mathcal{C}) = \langle (x+1)^3, u(x+1)^2, v(x+1)^2, uv(x+1)\rangle$. *Then* $\mathcal{C}^\perp = \langle (x+1)^3, u(x+1)^2, v(x+1)^2, uv(x+1)\rangle$ *and* $\phi(\mathcal{C}^\perp)$ *is a* $[16, 8, 4]$*-binary linear code.*

In Table 2, we give the duals of some principal and non-principal cyclic code of even length over *R*. We also see that the Gray images of these codes are binary linear codes with good parameters.

Table 2 Binary images of some cyclic codes of length n over the ring *R*

Length	Generators of $\mathcal{C}$	The dual code $\mathcal{C}^\perp$	$\phi(\mathcal{C})$	$\phi(\mathcal{C}^\perp)$	Remarks
2	$\langle x+1+u\rangle$	$\langle x+1+u\rangle$	$[8,4,2]$	$[8,4,2]$	Self-dual
2	$\langle x+1+u, u, v\rangle$	$\langle uv(x+1)\rangle$	$[8,7,2]^*$	$[8,1,8]^*$	$\mathcal{C}^\perp \subset \mathcal{C}$
2	$\langle u(x+1), v(x+1), uv\rangle$	$\langle u(x+1), v(x+1), uv\rangle$	$[8,4,4]^*$	$[8,4,4]^*$	Self-dual
2	$\langle x+1, u\rangle$	$\langle u(x+1)\rangle$	$[8,6,2]^*$	$[8,2,4]$	$\mathcal{C}^\perp \subset \mathcal{C}$

Theorem 12: *Let* $\mathcal{C} = \langle g_1(x),\ ua_1(x),\ va_2(x),\ uva_3(x)\rangle$ *be a cyclic code of odd length* n *over R, where* $a_1(x)|g_1(x)|(x^n-1)$ *and* $a_3(x)|a_2(x)|g_1(x)|(x^n-1)$ *over* $\mathbb{Z}_2$. *If* $x^n - 1 = 0 \pmod{g_1 g_1^*}$, *then* $\mathcal{C}^\perp \subseteq \mathcal{C}$.

Proof: Suppose $x^n - 1 = 0 \pmod{g_1(x)g_1^*(x)}$. Then $g_1(x)|\frac{x^n-1}{g_1^*(x)}$. Since $a_3(x)|g_1(x)|\frac{x^n-1}{g_1^*(x)}$, we have $uv\frac{x^n-1}{g_1^*(x)} = uvf_1(x)a_3(x) \in \langle uva_3\rangle \subseteq \mathcal{C}$, for some $f_1(x) \in \mathbb{Z}_2[x]$. Again, as $a_2(x)|g_1(x)|\frac{x^n-1}{g_1^*(x)}|\frac{x^n-1}{a_1^*(x)}$, so $v\frac{x^n-1}{a_1^*(x)} = vf_2(x)a_2(x) \in \langle va_2(x)\rangle \subseteq \mathcal{C}$ for some $f_2(x) \in \mathbb{Z}_2[x]$. Similarly, $a_1(x)|g_1(x)|\frac{x^n-1}{g_1^*(x)}|\frac{x^n-1}{a_2^*(x)}$ implies that $u\frac{x^n-1}{a_2^*(x)} \in \mathcal{C}$, and $g_1(x)|\frac{x^n-1}{g_1^*(x)}|\frac{x^n-1}{a_3^*(x)}$ implies that $\frac{x^n-1}{a_3^*(x)} \in \mathcal{C}$. Therefore $\mathcal{C}^\perp = \left\langle \frac{x^n-1}{a_3^*(x)}, u\frac{x^n-1}{a_2^*(x)}, v\frac{x^n-1}{a_1^*(x)}, uv\frac{x^n-1}{g_1^*(x)}\right\rangle \subseteq \mathcal{C}$. Hence the result. □

Example 6: *Let* $n = 21$. *We have* $x^{21} - 1 = (x+1)(x^2+x+1)(x^3+x^2+1)(x^3+x+1)(x^6+x^4+x^2+x+1)(x^6+x^5+x^4+x^2+1) = f_1f_2f_3f_4f_5f_6$ *over R. It is easy to see that* $f_4^* = f_3, f_3^* = f_4, f_5^* = f_6$ *and* $f_6^* = f_5$. *Therefore, the cyclic code* $\mathcal{C} = \langle f_3f_5,\ uf_3,\ vf_5,\ uv\rangle$ *of length* 21 *over R contains its dual, as*

$(f_3f_5)^* = f_3^*f_5^* = f_4f_6$ *and* $x^{21} - 1 = 0 \pmod{f_3f_5f_4f_6}$. *From Theorem 6, we get* $C^\perp = \langle uf_1f_2f_3f_4f_5,\ vf_1f_2f_3f_5f_6,\ uvf_1f_2f_3f_5\rangle$.

The converse of Theorem 12 need not hold in general. For example, the dual of the cyclic code $\mathcal{C} = \langle x^2 + x + 1,\ u,\ v\rangle$ of length 3 over R is $\mathcal{C}^\perp = \langle uv(x+1)\rangle$. Clearly $\mathcal{C}^\perp \subseteq \mathcal{C}$ but $x^3 - 1 \neq 0 \pmod{(x^2+x+1)^2}$. However, if $\mathcal{C}$ is a free cyclic code of odd length n, then $\mathcal{C} = \langle g_1(x)\rangle$ with $g_1(x)|x^n - 1$ over $\mathbb{Z}_2$, and $\mathcal{C}^\perp \subseteq \mathcal{C}$ if and only if $x^n - 1 = 0 \pmod{g(x)g^*(x)}$.

Now we determine a spanning set for the cyclic code $\mathcal{C}$ of odd length n over R. Consider the cyclic code $\mathcal{C}$ of odd length as given in Theorem 5. Let $\gcd(a_1(x), a_2(x)) = a'(x)$ over $\mathbb{Z}_2$. Then there exists $p(x), p'(x) \in \mathbb{Z}_2[x]$ such that $p(x)a_1(x) + p'(x)a_2(x) = a'(x)$. Since $uva_1(x), uva_2(x) \in \mathcal{C}$, we get $uv[p(x)a_1(x) + p'(x)a_2(x)] = uva'(x) \in \mathcal{C}$. Clearly, $a'(x)$ is monic over $\mathbb{Z}_2$, $a_3(x)|a'(x)$, $\deg(a'(x)) \leq \deg(a_1(x))$ and $\deg(a'(x)) \leq \deg(a_2(x))$. With these notations, we have the following result.

Theorem 13: *Let* $\mathcal{C} = \langle g_1(x),\ ua_1(x),\ va_2(x),\ uva_3(x)\rangle$ *be a cyclic code of odd length* n *over* R *such that* $a_3(x)|a_1(x)|g_1(x)|x^n - 1$, $a_3(x)|a_2(x)|g_1(x)|x^n - 1$ *over* $\mathbb{Z}_2$. *Let* $deg(g_1(x)) = t_1$, $\deg(a_1(x)) = t_2$, $deg(a_2(x)) = t_3$ *and* $deg(a_3(x)) = t_4$. *If* $\gcd(a_1(x), a_2(x)) = a'(x)$ *over* $\mathbb{Z}_2$ *with* $deg(a'(x)) = t$, *then* $\mathcal{C}$ *is spanned by the set* $S = \{g_1(x), xg_1(x), \ldots, x^{n-t_1-1}g_1(x), ua_1(x), uxa_1(x), \ldots, ux^{t_1-t_2-1}a_1(x), va_2(x), vxa_2(x), \ldots, vx^{t_1-t_3-1}a_2(x), uva_3(x), uvxa_3(x), \ldots, uvx^{t-t_4-1}a_3(x)\}$.

Proof: First we show that $uvx^{t-t_4}a_3(x) \in span(S)$. Since $a'(x)$ is a monic polynomial of degree t, there exists $m(x) \in \mathbb{Z}_2[x]$ such that $uvx^{t-t_4}a_3(x) = uva'(x) + uvm(x)$, where $m = 0$ or $\deg(m) < \deg(a') = t$. Also since $uvx^{t-t_4}a_3(x), uva'(x) \in \mathcal{C}$, we have $uvx^{t-t_4}a_3(x) + uva'(x) = uvm(x) \in \mathcal{C}$. This implies that $\deg(m(x)) \geq t_4$, because $a_3(x)$ is a polynomial of minimum degree in $\mathcal{C}$. Therefore $t_4 \leq \deg(m(x)) < t$ and $uvm(x) = \alpha_0 uva_3(x) + \alpha_1 uvxa_3(x) + \cdots + \alpha_{t-t_4-1}uvx^{t-t_4-1}a_3(x)$, where $\alpha_0 + \alpha_1 x + \cdots + \alpha_{t-t_4-1}x^{t-t_4-1}$ is a binary polynomial of degree at most $t - t_4 - 1$. This gives $uvx^{t-t_4}a_3(x) \in span(S)$. Similarly, we can show that $x^{n-t_1}g_1(x), ux^{t_1-t_2}a_1(x), vx^{t_1-t_3}a_2(x) \in span(S)$. Hence the result. □

Example 7: *Let* $n = 7$ *and* $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1) = f_1f_2f_3$. *Let* $\mathcal{C} = \langle f_2f_3,\ uf_2,\ vf_3,\ uv\rangle$. *Clearly* $\mathcal{C}$ *is a cyclic code of length* 7 *over* R *with* $t_1 = 6, t_2 = 3, t_3 = 3, t_4 = 0$. *Also,* $\gcd(f_2, f_3) = 1$ *implies that* $uv \in \langle uf_2, vf_3\rangle$. *Therefore, the set* $S = \{f_2f_3, uf_2, uxf_2, ux^2f_2, vf_3, vxf_3, vx^2f_3\}$ *spans the cyclic code* $\mathcal{C}$.

The spanning set given Theorem 13 need not be minimal in general. However, in the following result, we present a minimal spanning set for a class of cyclic codes of odd length over R.

Corollary 14: *Let* $\mathcal{C} = \langle g_1(x),\ ua_1(x),\ uva_3(x)\rangle$ *be a cyclic code of odd length* n *over* R *such that* $a_3(x)|a_1(x)|g_1(x)|x^n - 1$ *over* $\mathbb{Z}_2$. *Let* $deg(g_1(x)) = t_1$, $deg(a_1(x)) = t_2$ *and* $deg(a_3(x)) = t_4$. *Then a minimal spanning set of* $\mathcal{C}$ *is* $S = \{g_1(x), xg_1(x), \ldots, x^{n-t_1-1}g_1(x), ua_1(x), uxa_1(x), \ldots, ux^{t_1-t_2-1}a_1(x), uva_3(x), uvxa_3(x), \ldots, uvx^{t_2-t_4-1}a_3(x)\}$. *Further, the cardinality of* $\mathcal{C}$ *is* $16^{n-t_1}4^{t_1-t_2}2^{t_2-t_4}$.

Proof: As S is linearly independent over the ring R, the result follows. □

Example 8: *Let* $n = 3$. *We have* $x^3 - 1 = (x-1)(x^2+x+1)$. *Let* $\mathcal{C} = \langle x^2 + x + 1,\ uv\rangle$. *Then* $\mathcal{C}$ *is a cyclic code of length* 3 *over R.* $\mathcal{C}$ *is spanned by the set* $S = \{x^2 + x + 1, uv, uvx\}$ *and contains* $16^{3-2}2^{2-0} = 2^6$ *codewords. Further,* $\phi(\mathcal{C})$ *is a* $[12, 6, 3]$*-binary linear code.*

Remark 1: Similarly we can give minimal spanning sets for the cyclic codes $\mathcal{C} = \langle g_1(x),\ va_2(x),\ uva_3(x)\rangle$ of odd length over *R*.

Now we construct DNA codes as reversible complement cyclic codes over *R*. Because of the complexity of the structure of cyclic codes of arbitrary length over *R*, we construct DNA codes from the cyclic codes of odd length over *R*.

4 The reverse constraint

In this section, we find the necessary and sufficient conditions for a cyclic code $\mathcal{C}$ over *R* to be reversible. We recall that the polynomials $g_1(x), g_2(x), a_1(x)$ and $a_2(x)$ given in Theorem 1 are monic over $\mathbb{Z}_2$.

Definition 4.1: The reverse of a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, denoted by c^r, is defined as $c^r = (c_{n-1}, c_{n-2}, \ldots, c_0)$.

Definition 4.2: A linear code $\mathcal{C}$ of length n over *R* is said to be *reversible* if $c^r \in \mathcal{C}$ for all $c \in \mathcal{C}$.

The following theorem presents a condition for a cyclic code over finite fields to be reversible.

Theorem 15: *(Massey, 1964, Theorem 1) The cyclic code over* $\mathbb{F}_q$ *generated by a monic polynomial* $g(x)$ *is reversible if and only if* $g(x)$ *is self-reciprocal.*

Theorem 16: *(Guenda and Aaron Gulliver, 2013, Theorem 4.6) Let* $\mathcal{C} = \langle g(x),\ ua(x)\rangle$ *be a linear cyclic code of odd length* n *over* $R = \mathbb{Z}_2 + u\mathbb{Z}_2, u^2 = 0$, *where* $a(x)|g(x)|x^n - 1$ *and* $g(x), a(x) \in \mathbb{Z}_2[x]$. *Then* $\mathcal{C}$ *is a reversible cyclic code if and only if both* $g(x)$ *and* $a(x)$ *are self-reciprocal.*

The following theorem gives a necessary and sufficient condition for a cyclic code of odd length over *R* to be reversible.

Lemma 17: *Let* $\mathcal{C} = \langle g_1(x), ua_1(x), va_2(x), uva_3(x)\rangle$ *be a reversible cyclic code of odd length* n *over R, where* $a_3(x)|a_1(x)|g_1(x)|(x^n - 1)$ *and* $a_3(x)|a_2(x)|g_1(x)|(x^n - 1)$ *over* $\mathbb{Z}_2$. *Then for any polynomial* $f(x) = f_0 + f_1x + \cdots + f_{m-1}x^{m-1} + f_mx^m \in \mathcal{C}$ *of degree* m, *we have* $f^*(x) \in \mathcal{C}$.

Proof: First we see that

$$\begin{aligned} f^r(x) &= x^{n-m-1}f_m + f_{m-1}x^{n-m} + \cdots + f_0x^{n-1} \\ &= x^{n-m-1}[f_m + f_{m-1}x + \cdots + f_0x^m \\ &= x^{n-m-1}f^*(x) \in \mathcal{C}. \end{aligned}$$

Therefore $x^{m+1}\left[x^{n-m-1}f^*(x)\right] = f^*(x) \in \mathcal{C}$. □

Theorem 18: *Let $\mathcal{C} = \langle g_1(x), ua_1(x), va_2(x), uva_3(x)\rangle$ be a cyclic code of odd length n over R, where $a_3(x)|a_1(x)|g_1(x)|(x^n-1)$ and $a_3(x)|a_2(x)|g_1(x)|(x^n-1)$ over $\mathbb{Z}_2$. Then $\mathcal{C}$ is reversible if and only if $a_1(x), a_2(x), a_3(x)$ and $g_1(x)$ are self-reciprocal polynomials over $\mathbb{Z}_2$.*

Proof: Suppose that $\mathcal{C}$ is a reversible code over R. We have $\mathcal{C} \pmod u = \langle g_1(x), va_2(x)\rangle$. In view of Theorem 16, for the ring $\mathbb{Z}_2 + v\mathbb{Z}_2,\ v^2 = 0$, we have both $g_1(x)$ and $a_2(x)$ are self-reciprocal. Now to show that $a_1(x)$ is a self-reciprocal polynomial in $R[x]$, assume $a_1(x) \neq a_1^*(x)$. Since $a_1(x)$ is a monic polynomial with a non-zero constant term, we have $\deg(a_1) = \deg(a_1^*)$. Also since $\mathcal{C}$ is a reversible cyclic code, $ua_1^*(x) \in \mathcal{C}$. Let $a(x) = \gcd(a_1(x),\ a_1^*(x))$. Then there exists $l_1(x),\ l_2(x) \in R[x]$ such that $l_1(x)[ua_1(x)] + l_2(x)[ua_1^*(x)] = ua(x) \in \mathcal{C}$. Also it is easy to see that $\deg(a(x)) < \deg(a_1(x))$. Thus we get $a(x) \in \mathbb{Z}_2[x]$ such that $ua(x) \in \mathcal{C}$ and $\deg(a(x)) < \deg(a_1(x))$. But this contradicts the fact that $a_1(x)$ is a minimal degree polynomial such that $ua_1(x) \in \mathcal{C}$. Hence $a_1(x)$ is self-reciprocal polynomial. Similarly we get $a_3(x) = a_3^*(x)$.

Conversely, assume that $g_1(x), a_1(x), a_2(x)$ and $a_3(x)$ are self-reciprocal polynomials over $\mathbb{Z}_2$. Let $c \in \mathcal{C}$. Then $c = l_1(x)g_1(x) + ul_2(x)a_1(x) + vl_3(x)a_2(x) + uvl_4(x)a_3(x)$ for some polynomials $l_1(x), l_2(x), l_3(x)$,
$l_4(x) \in \mathbb{F}_2[x]$. Now

$$\begin{aligned} c^* &= [l_1(x)g_1(x) + ul_2(x)a_1(x) + vl_3(x)a_2(x) + uvl_4(x)a_3(x)]^* \\ &= [l_1(x)g_1(x) + ul_2(x)a_1(x)]^* + vx^i[l_3(x)a_2(x) + ul_4(x)a_3(x)]^* \\ &= l_1^*(x)g_1^*(x) + ux^{i_1}l_2^*(x)a_1^*(x) + x^ivl_3^*(x)a_2^*(x) + uvx^{i_2}l_4^*(x)a_3^*(x) \\ &= l_1^*(x)g_1(x) + ux^{i_1}l_2^*(x)a_1(x) + vx^il_3^*(x)a_2(x) + uvx^{i_2}l_4^*(x)a_3(x) \ \in \mathcal{C}, \end{aligned}$$

where i, i_1, i_2 are defined as in Lemma 3. This implies that $c^* \in \langle g_1(x), ua_1(x), va_2(x), uaa_3(x)\rangle$. Therefore, $\mathcal{C}$ is a reversible code over R. □

5 DNA codes over *R*

In this section, we construct DNA codes from cyclic codes of odd length over R. We identify the elements of the ring R with nucleotide base pairs $S_{D_{16}} = \{AA,\ AT,\ AG,\ AC,\ TT,\ TA,\ TG,\ TC,\ GG,\ GA, GC,\ GT,\ CC,\ CA,\ CG,\ CT\}$. Table 3 below gives a one-to-one correspondence Φ between R and $S_{D_{16}}$.

Table 3 Correspondence of DNA double pairs with elements of the ring R under Φ

AA	0	TT	$v + uv$
AG	u	AC	$1 + uv$
TG	$1 + v$	TC	$u + v + uv$
GC	$1 + u + uv$	CG	$1 + u + v$
GT	1	CA	$1 + v + uv$
CC	v	GG	uv
GA	$u + uv$	CT	$u + v$
AT	$1 + u$	TA	$1 + u + v + uv$

We recall that the Watson–Crick complement (WCC) for nucleotides given by $\bar{A} = T$, $\bar{T} = A$, $\bar{G} = C$ and $\bar{C} = G$. Similarly the WCC for DNA double bases is taken as $\overline{AA} = \bar{A}\bar{A} = TT$, $\overline{AT} = \bar{A}\bar{T} = TA, \cdots \overline{TC} = \bar{T}\bar{C} = AG$. From Table 3, we see that if XY is the DNA double pair corresponding to an element $a \in R$, then the complement of XY corresponds to $a + v + uv$. We also note that when an element of R is multiplied by $1 + v$, the corresponding DNA pair will be reversed. Therefore, if $d_1 d_2 \cdots d_{2n}$ is the DNA sequence of an n-tuple c in R^n, then the DNA sequence of $(1 + v)c^r$ is $d_{2n} d_{2n-1} \cdots d_1$. For example, the DNA sequence corresponding to the polynomial $x + x^2 = 0 + 1 \cdot x + 1 \cdot x^2 = (0, 1, 1)$ is $AAGTGT$, and the DNA sequence corresponding to the polynomial $(1 + v)(x + x^2)^r = (1 + v)(1, 1, 0) = (1 + v, 1 + v, 0)$ is $TGTGAA$ which is reverse of the string $AAGTGT$.

We define the complement of any $a \in R$ to be $\bar{a} = a + (v + uv)$. Extending this definition, we have the complement of any $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{n-1} x^{n-1} \in R_n$ as $f^c(x) = \bar{f}_0 + \bar{f}_1 x + \bar{f}_2 x^2 + \cdots + \bar{f}_{n-1} x^{n-1}$. The reversible complement of $f(x) \in R^n$ is denoted by $f^{rc}(x)$ and is defined as $f^{rc}(x) = \bar{f}_{n-1} + \bar{f}_{n-2} x + \cdots + \bar{f}_0 x^{n-1}$.

Lemma 19: *For any $a, b \in R$, we have*

1 $a + \bar{a} = v + uv$;

2 $\overline{a + b} = \bar{a} + \bar{b} + v + uv$;

3 $(v + uv) + \overline{(v + uv)a} = (v + uv)a$.

Definition 5.1: A cyclic code $\mathcal{C}$ of length n over R is said to be reversible complement if $f^{rc}(x) \in \mathcal{C}$ for every $f(x) \in \mathcal{C}$.

Definition 5.2: A linear code $\mathcal{C}$ of length n is called cyclic DNA code over R if

1 $\mathcal{C}$ is cyclic code, i.e. $\mathcal{C}$ is an ideal of $R[x]/\langle x^n - 1\rangle$

2 $f^{rc}(x) \in \mathcal{C}$, for every codeword $f(x) \in \mathcal{C}$.

The following theorem gives a necessary and sufficient condition for a cyclic code of odd length n over R to be reversible complement.

Theorem 20: *Let $\mathcal{C} = \langle g_1(x), ua_1(x), va_2(x), uva_3(x)\rangle$ be a cyclic code of odd length n over R, where $a_1(x)|g_1(x)|(x^n - 1)$, $a_3(x)|a_2(x)|g_1(x)|(x^n - 1)$ over $\mathbb{Z}_2$. Then $\mathcal{C}$ is a reversible complement cyclic code if and only if*

1 $(v + uv)\frac{x^n - 1}{x - 1} \in \mathcal{C}$.

2 $g_1(x), a_1(x), a_2(x)$ *and* $a_3(x)$ *are self-reciprocal over* $\mathbb{Z}_2$.

Proof: Let $\mathcal{C}$ be reversible complement over R. Then, as $\mathbf{0} = (0, 0, \ldots, 0) \in \mathcal{C}$, so $\mathbf{0}^{rc} \in \mathcal{C}$. This implies that

$$\begin{aligned}\overline{(0, 0, \ldots, 0)} &= (v + uv, v + uv, \ldots, v + uv)\\ &= (v + uv)(1, 1, \ldots, 1) \in \mathcal{C}.\end{aligned}$$

Hence $(v+uv)\frac{x^n-1}{x-1} \in \mathcal{C}$. Now we show that $g_1(x)$ is self-reciprocal. Let $g_1(x) = 1 + g_1x + g_2x^2 + \cdots + g_{r-1}x^{r-1} + x^r$. Then

$$\begin{aligned} g_1^{rc}(x) &= \bar{0} + \bar{0}x + \cdots + \bar{0}x^{n-r-2} + \bar{1}x^{n-r-1} + \bar{g}_{r-1}x^{n-r} + \cdots \\ &\quad + \bar{g}_1x^{n-2} + \bar{1}x^{n-1} \\ &= (v+uv) + (v+uv)x + \cdots + (v+uv)x^{n-r-2} + \bar{g}_{r-1}x^{n-r} + \cdots \\ &\quad + \bar{g}_1x^{n-2} \in \mathcal{C}. \end{aligned}$$

Now as $(v+uv)\frac{x^n-1}{x-1} \in \mathcal{C}$, so $g_1^{rc}(x) + (v+uv)\frac{x^n-1}{x-1} \in \mathcal{C}$. Therefore,

$$\begin{aligned} g_1^{rc}(x) + (v+uv)\frac{x^n-1}{x-1} &= x^{n-r-1} + [(v+uv) + \bar{g}_{r-1}]x^{n-r} + \cdots \\ &\quad + [(v+uv) + \bar{g}_1]x + x^r \\ &= x^{n-r-1}[1 + g_{r-1}x + \cdots + g_1x + x^r] \\ &= x^{n-r-1}g_1^*(x) \ \in \mathcal{C}. \end{aligned}$$

This implies that $g_1^*(x) \in \mathcal{C}$, and therefore there exist $l_1(x), l_2(x), l_3(x), l_4(x) \in R[x]$ such that $g_1^*(x) = g_1(x)l_1(x) + ua_1(x)l_2(x) + va_2(x)l_3(x) + uva_3(x)l_4(x)$. Since $g_1(x) \in \mathbb{Z}_2[x]$, comparing the degrees of $g_1(x)$ on both sides, we get $l_2(x) = l_3(x) = l_4(x) = 0$, and since $g_1(x)$ is monic, we get $l_1(x) = 1$. Hence $g(x)$ is self-reciprocal over $\mathbb{Z}_2$. Using similar arguments, we can show that $a_1(x), a_2(x)$ and $a_3(x)$ are also self-reciprocal.

Conversely assume that conditions (1) and (2) hold. First we prove that $c^*(x) \in \mathcal{C}$ for any $c(x) \in \mathcal{C}$. Let $c(x) \in \mathcal{C}$. Then $c(x) = g_1(x)k_1(x) + ua_1(x)k_2(x) + va_2(x)k_3(x) + uva_3(x)k_4(x)$ for some $k_1(x), k_2(x), k_3(x)$ and $k_4(x)$ in $R[x]$. Then $c^*(x) = g_1^*(x)k_1^*(x) + ux^{j_1}a_1^*(x)k_2^*(x) + vx^{j_2}a_2^*(x)k_3^*(x) + uvx^{j_3}a_3^*(x)k_4^*(x)$, where j_1, j_2, j_3 are defined as in Lemma 3. This implies that $c^*(x) = g_1(x)k_1^*(x) + ux^{j_1}a_1(x)k_2^*(x) + vx^{j_2}a_2(x)k_3^*(x) + uvx^{j_3}a_3(x)k_4^*(x) \in \mathcal{C}$. Let $c(x) = c_0 + c_1x + \cdots + c_kx^k$. Since $\mathcal{C}$ is linear, we have $(v+uv)\frac{x^n-1}{x-1} + x^{n-k-1}c(x) \in \mathcal{C}$. Now

$$\begin{aligned} (v+uv)\frac{x^n-1}{x-1} + x^{n-k-1}c(x) &= (v+uv) + (v+uv)x + \cdots + (v+uv)x^{n-k-2} \\ &\quad + ((v+uv) + c_0)x^{n-k-1} \\ &\quad + ((v+uv) + c_1)x^{n-k-1} + \cdots \\ &\quad + ((v+uv) + c_{k-1})x + ((v+uv) + c_k) \\ &= \bar{c}_0x^{n-k-1} + \cdots + \bar{c}_{k-1}x + \bar{c}_k \\ &= (c^*(x))^{rc}. \end{aligned}$$

Thus $(c^*(x))^{rc} \in \mathcal{C}$. Therefore $[(c^*(x))^{rc}]^* = c^{rc}(x) \ \in \mathcal{C}$. Hence the result. □

We note that if a cyclic code $\mathcal{C}$ is a reversible complement cyclic code of odd length over R, then it is reversible over R as $\bar{0} + a^{rc} = a^r \in \mathcal{C}$ for all $a \in \mathcal{C}$. Now we construct DNA codes from codes over $S_{D_{16}}$. Let $\mathcal{C}$ be a linear code over R. Define $\Phi : \mathcal{C} \to S_{D_{16}}$ such that

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto (\Phi(c_0), \Phi(c_1), \ldots, \Phi(c_{n-1})). \tag{5}$$

Let $\mathcal{C}$ be a reversible complement cyclic code of odd length n over R with minimum Hamming distance d. Let $f(x) \in \mathcal{C}$ and $\Phi(f(x)) = d_0 d_1 \cdots d_{2n-1}$ be the corresponding DNA sequence in $\Phi(\mathcal{C}) \subseteq S^n_{D_{16}}$. Then we have

1 $f^c(x) \in \mathcal{C}$ implies that $\Phi(f^c(x)) = \bar{d}_0 \bar{d}_1 \cdots \bar{d}_{2n-1} \in \Phi(\mathcal{C})$

2 $(1+v)f^r(x) \in \mathcal{C}$ implies that $\Phi((1+v)f^r(x)) = d_{2n-1} d_{2n-2} \cdots d_1 \in \Phi(\mathcal{C})$

3 $(1+v)f^{rc}(x) \in \mathcal{C}$ implies that $\Phi((1+v)f^{rc}(x)) = \bar{d}_{2n-1} \bar{d}_{2n-2} \cdots \bar{d}_1 \in \Phi(\mathcal{C})$, which is the WCC property.

Thus $\Phi(\mathcal{C})$ is a DNA code over $S_{D_{16}}$ of length n. Now we discuss the GC-content of a DNA code over $S_{D_{16}}$. The WCC pairs A and T, C and G are chemically joined to each other by two and three hydrogen bonds, respectively, and the total number of such bonds in a DNA determines its stability. In order to avoid undesirable hybridisation, we may assume that all strings in $\Phi(\mathcal{C})$ have the same melting points which can be explained by the GC-content. A DNA with high GC-content is more stable.

The following result gives the minimum Hamming distance of a cyclic code $\mathcal{C}$ over R.

Theorem 21: *(Kewat, Ghosh and Pattanayak, 2015, Theorem 5.1) Let* $\mathcal{C} = \langle g_1(x), ua_1(x), va_2(x), uva_3(x) \rangle$ *be a cyclic code of odd length* n*, where* $a_1(x)|g_1(x)|(x^n-1)$*,* $a_3(x)|a_2(x)|(x^n-1)$ *over* $\mathbb{Z}_2$*. Then* $d_H(\mathcal{C}) = d_H(\mathcal{C}_{uv})$*, where* $\mathcal{C}_{uv} = \{f \in R_n \mid uvf \in \mathcal{C}\}$ *and* $d_H(\mathcal{C})$ *is minimum Hamming distance of the code* $\mathcal{C}$*.*

In view of Theorem 21, if $\mathcal{C}$ is a reversible complementary cyclic code of length n over the ring R with minimum distance d, then $\Phi(\mathcal{C})$ is DNA code of length $2n$ over S_{D_4} with minimum Hamming distance at least d. Now consider the ideal generated by v over R, $vR = \{0, v, uv, v+uv\}$. The image of vR under Φ is $\Phi(vR) = \{AA, CC, GG, TT\}$. This implies that if $\mathcal{C} = \langle vg(x) \rangle$, $g(x)|x^n - 1$ is a reversible complement cyclic code of length n over R, then $\Phi(\mathcal{C})$ is a DNA code of length n over the alphabet $\{AA, CC, GG, TT\}$. Further, if two codewords in $\mathcal{C}$ differ at a coordinate, then their images differ at the two coordinate positions corresponding to the image of the coordinate. Therefore, we have the following result.

Theorem 22: *If* $\mathcal{C} = \langle vg(x) \rangle$*,* $g(x)|x^n - 1$ *is a reversible complement cyclic code of length* n *over* R *with minimum Hamming distance* d*, then* $\Phi(\mathcal{C})$ *is a DNA code of length* $2n$ *over the alphabet* $\{AA, CC, GG, TT\}$ *with the minimum Hamming distance* $2d$*.*

From Theorem 22, we note that if $\mathcal{C}$ is a DNA cyclic code with minimum Hamming distance d, then $\Phi(\mathcal{C})$ has a subcode with minimum Hamming distance $2d$.

6 Examples

We can construct cyclic DNA codes as follows. First we note that the ring R contains the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$, $u^2 = 0$ and $\mathbb{Z}_2$ properly, so the factorisation of a polynomial over these rings is still valid over R. Let $\mathcal{C} = \langle g_1(x), ua_1(x), va_2(x), uva_3(x) \rangle$ be a cyclic code of odd length n over R such that $a_1(x)|g_1(x)|(x^n-1)$, $a_3(x)|a_2(x)|(x^n-1)$ over $\mathbb{Z}_2$. If

each of $g_1(x), a_1(x), a_2(x), a_3(x)$ is self-reciprocal, and not divisible by $x-1$, then $\mathcal{C}$ is a cyclic DNA code.

Example 9: *For* $n = 3$*, we have* $x^3 - 1 = (x-1)(x^2+x+1) \in \mathbb{Z}_2[x]$. *Let* $g(x) = x^2 + x + 1$. *As* $(v+uv)\frac{x^n-1}{x-1} \notin \langle ug(x)\rangle$ *and* $(v+uv)\frac{x^n-1}{x-1} \notin \langle uvg(x)\rangle$, *the only possible non-trivial cyclic DNA codes of length* 3 *over R are* $\mathcal{C}_1 = \langle g(x)\rangle$ *and* $\mathcal{C}_2 = \langle vg(x)\rangle$. *The following Table 4 gives Hamming distance and size of each cyclic DNA code of length* 3 *over R. We can easily see that the cyclic DNA code* $\mathcal{C}_1 = \langle g(x)\rangle$ *is a repetition code of length* 3 *over R. The image of* $\mathcal{C}_1$ *under* Φ *is a DNA code of length* 6 *and size* 16 *such that* $\Phi(\mathcal{C}_1) = \{AAAAAA, AGAGAG, TGTGTG, GCGCGC, GTGTGT, CCCCCC, GAGAGA, ATATAT, TTTTTT, ACACAC, TCTCTC, CGCGCG, CACACA, GGGGGG, CTCTCT, TATATA\}$. *Similarly, we have* $\Phi(\mathcal{C}_2) = \{AAAAAA, CCCCCC, TTTTTT, GGGGGG\}$.

Table 4 $g(x) = x^2 + x + 1$. The DNA cyclic codes of length 3 over *R* and its image under Φ

No.	Generators	Length	Size	$d_H(\mathcal{C})$	$d_H(\Phi(\mathcal{C}))$
1.	$\langle g(x)\rangle$	3	16^1	3	3
2.	$\langle vg(x)\rangle$	3	4^1	3	6

In the similar way, we have only two cyclic DNA codes of length 5 as well as of length 7 over *R*. Now we see some cyclic DNA codes of length 9. For $n = 9$, we have $x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1) \in \mathbb{Z}_2[x]$. Let $g_1(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $g_2(x) = x^6 + x^3 + 1$ and $g_3(x) = x^2 + x + 1$. In Table 5, we have listed some non-trivial DNA codes of length 9 over *R*.

Table 5 List of DNA cyclic codes of length 9 over *R*

Sl. No.	Generators	Size
1.	$\langle g_1\rangle$	16^1
2.	$\langle g_2\rangle$	16^3
3.	$\langle g_3\rangle$	16^7
4.	$\langle vg_1\rangle$	4^1
5.	$\langle vg_2\rangle$	4^3
6.	$\langle vg_3\rangle$	4^7
7.	$\langle g_1, ug_2\rangle$	$16^1.4^2$
8.	$\langle g_1, vg_2\rangle$	$16^1.4^2$
9.	$\langle g_1, uvg_2\rangle$	$16^1.2^2$
10.	$\langle g_1, ug_3\rangle$	$16^1.4^6$
11.	$\langle g_1, vg_3\rangle$	$16^1.4^6$
12.	$\langle g_1, uvg_3\rangle$	$16^1.2^6$
13.	$\langle vg_1, uvg_2\rangle$	$4^1.4^2$
14.	$\langle vg_1, uvg_3\rangle$	$4^1.2^6$

Example 10: *Let* $\mathcal{C} = \langle vg_2(x) \rangle$ *be a cyclic DNA code of length* 9 *over R. It is easy to check that* $g_2(x)$ *is a self-reciprocal polynomial over* $\mathbb{Z}_2$*. Therefore,* $\mathcal{C}$ *is a DNA code with Hamming distance* 3 *and size* 64*. The image of* $\mathcal{C}$ *under* Φ*, i.e.* $\Phi(\mathcal{C})$ *is a DNA code of length* 18 *with minimum distance* 6*. The codewords of* $\Phi(\mathcal{C})$ *are given in Table 6.*

Table 6 The DNA code of length 9 obtained from $\mathcal{C} = \langle v(x^6 + x^3 + 1) \rangle$ over *R*

AAAACCAAAACCAAAACC	AAAAGGAAAAGGAAAAGG	AAAATTAAAATTAAAATT	AACCAAAACCAAAACCAA
AAGGAAAAGGAAAAGGAA	AATTAAAATTAAAATTAA	CCAAAACCAAAACCAAAA	GGAAAAGGAAAAGGAAAA
TTAAAATTAAAATTAAAA	CCCCAACCCCAACCCCAA	CCGGAACCGGAACCGGAA	CCTTAACCTTAACCTTAA
GGCCAAGGCCAAGGCCAA	GGGGAAGGGGAAGGGGAA	GGTTAAGGTTAAGGTTAA	TTCCAATTCCAATTCCAA
TTGGAATTGGAATTGGAA	TTTTAATTTTAATTTTAA	CCAACCCCAACCCCAACC	CCAAGGCCAAGGCCAAGG
CCAATTCCAATTCCAATT	GGAACCGGAACCGGAACC	GGAAGGGGAAGGGGAAGG	GGAATTGGAATTGGAATT
TTAACCTTAACCTTAACC	TTAAGGTTAAGGTTAAGG	TTAATTTTAATTTTAATT	AACCCCAACCCCAACCCC
AACCGGAACCGGAACCGG	AACCTTAACCTTAACCTT	AAGGCCAAGGCCAAGGCC	AAGGGGAAGGGGAAGGGG
AAGGTTAAGGTTAAGGTT	AATTCCAATTCCAATTCC	AATTGGAATTGGAATTGG	AATTTTAATTTTAATTTT
CCCCCCCCCCCCCCCCCC	CCGGCCCCGGCCCCGGCC	CCTTCCCCTTCCCCTTCC	GGCCCCGGCCCCGGCCCC
GGGGCCGGGGCCGGGGCC	GGTTCCGGTTCCGGTTCC	TTCCCCTTCCCCTTCCCC	TTGGCCTTGGCCTTGGCC
TTTTCCTTTTCCTTTTCC	CCCCGGCCCCGGCCCCGG	CCGGGGCCGGGGCCGGGG	CCTTGGCCTTGGCCTTGG
GGCCGGGGCCGGGGCCGG	GGGGGGGGGGGGGGGGGG	GGTTGGGGTTGGGGTTGG	TTCCGGTTCCGGTTCCGG
TTGGGGTTGGGGTTGGGG	TTTTGGTTTTGGTTTTGG	CCCCTTCCCCTTCCCCTT	CCGGTTCCGGTTCCGGTT
CCTTTTCCTTTTCCTTTT	GGCCTTGGCCTTGGCCTT	GGGGTTGGGGTTGGGGTT	GGTTTTGGTTTTGGTTTT
TTCCTTTTCCTTTTCCTT	TTGGTTTTGGTTTTGGTT	TTTTTTTTTTTTTTTTTT	AAAAAAAAAAAAAAAAAA

7 Conclusion

In this paper, we have determined the generators of dual of a cyclic code over *R*. We have given a sufficient condition that a cyclic code of odd length over *R* to contain its dual. A minimal spanning set for cyclic codes of odd lengths over *R* is determined. We have also proved a necessary and sufficient conditions that a cyclic code over *R* to be reversible complement. Further, we have constructed cyclic DNA codes over nucleotide base pairs $S_{D_{16}}$ as images of reversible complement cyclic codes over *R*. Few examples with good minimum distances are presented to illustrate the results.

Acknowledgement

The first author would like to thank Ministry of Human Resource Development (MHRD), India, for providing financial support. The authors would like to thank the anonymous referees for their valuable comments and suggestions.

References

Abualrub, T., Ghrayeb, A. and Zeng, X.N. (2006) 'Construction of cyclic codes over $GF(4)$ for DNA computing', *Journal of the Franklin Institute*, Vol. 343, No. 4, pp.448–457.

Abualrub, T. and Siap, I. (2007) 'Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$', *Designs, Codes and Cryptography*, Vol. 42, No. 3, pp.273–287.

Adleman, L.M. (1994) 'Molecular computation of solutions to combinatorial problems', *Science*, Vol. 266, No. 5187, pp.1021–1024.

Batoul, A., Guenda, K. and Gulliver, T.A. (2014) 'On self-dual cyclic codes over finite chain rings', *Designs, Codes and Cryptography*, Vol. 70, No. 3, pp.347–358.

Bayram, A., Oztas, E.S. and Siap, I. (2016) 'Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications', *Designs, Codes and Cryptography*, Vol. 80, pp.379–393. doi:10.1007/s10623-015-0100-8.

Bennenni, N., Guenda, K. and Mesnager, S. (2015) 'New DNA cyclic codes over rings', arXiv preprint, arXiv:1505.06263.

Bonnecaze, A. and Udaya, P. (1999) 'Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$', *IEEE Transactions on Information Theory*, Vol. 45, No. 4, pp.1250–1255.

Dinh, H.Q. and Lopez-Permouth, S. (2004) 'Cyclic and negacyclic codes over finite chain rings', *IEEE Transactions on Information Theory*, Vol. 50, No. 8, pp. 1728–1744.

Gaborit, P. and King, O.D. (2005) 'Linear construction for DNA codes', *Theoretical Computer Science*, Vol. 334, No. 1, pp.99–113.

Grassl, M. *Bounds on the minimum distance of linear codes and quantum codes*, http://www.codetables.de (accessed on 3 October 2016).

Guenda, K. and Gulliver, T.A. (2013) 'Construction of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ for DNA computing', *Applicable Algebra in Engineering, Communication and Computing*, Vol. 24, No. 6, pp.445–459.

Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A. and Solé, P. (1994) 'The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes', *IEEE Transactions on Information Theory*, Vol. 40, No. 2, pp.301–319.

Kewat, P.K., Ghosh, B. and Pattanayak, S. (2015) 'Cyclic codes over the ring $\mathbb{Z}_p[u,v]/\langle u^2, v^2, uv - vu\rangle$', *Finite Fields and Their Applications*, Vol. 34, pp.161–175.

Liang, J. and Wan, L. (2016) 'On cyclic DNA codes over $\mathbb{F}_2 + u\mathbb{F}_2$', *Journal of Applied Mathematics and Computing*, Vol. 51, No. 1, pp.81–91.

Lipton, R.J. (1995) 'DNA solutions of hard computational problems', *Science*, Vol. 268, No. 5210, pp.542–545.

MacWilliams, F.J. and Sloane, N.J.A. (1977) *The Theory of Error Correcting Codes*, North Holland Publishing Co., Elsevier, New York.

Mansuripur, M., Khulbe, P., Kuebler, S., Perry, J., Giridhar, M. and Peyghambarian, N. (2003) 'Information storage and retrieval using macromolecules as storage media', *University of Arizona Technical Report*, Vol. 5069, pp.231–243.

Massey, J.L. (1964) 'Reversible codes', *Information and Control*, Vol. 7, No. 3, pp.369–380.

Pless, V.S. and Qian, Z. (1996) 'Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$', *IEEE Transactions on Information Theory*, Vol. 42, No. 5, pp.1594–1600.

Siap, I., Abualrub, T. and Ghrayeb, A. (2009) 'Cyclic DNA codes over the ring $\mathbb{F}_2[u]/(u^2 - 1)$ based on the deletion distance', *Journal of the Franklin Institute*, Vol. 346, No. 8, pp.731–740.

Yildiz, B. and Karadeniz S. (2010) 'Linear codes over $\mathbb{F}2 + u\mathbb{F}2 + v\mathbb{F}2 + uv\mathbb{F}2$', *Designs, Codes and Cryptography*, Vol. 54, No. 1, pp.61–81.

Yildiz, B. and Karadeniz, S. (2011) 'Cyclic codes over $\mathbb{F}2 + u\mathbb{F}2 + v\mathbb{F}2 + uv\mathbb{F}2$', *Designs, Codes and Cryptography*, Vol. 58, No. 3, pp.221–234.

Yildiz, B. and Siap, I. (2012) 'Cyclic codes over $\mathbb{F}_2[u]/\langle u^4 - 1\rangle$ and applications to DNA codes', *Computers & Mathematics with Applications*, Vol. 63, No. 7, pp.1169–1176.

Zhu, S. and Chen, X. (2015) 'Cyclic DNA codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$', arXiv preprint, arXiv:1508.07113.

Zhu, S., Wang, Y. and Shi, M. (2010) 'Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$', *IEEE Transactions on Information Theory*, Vol. 56, No. 4, pp.1680–1684.