

DNA code from cyclic and skew cyclic codes over F 4 [v]/ v 3

Om Prakash, Ashutosh Singh, Ram Krishna Verma, Patrick Solé, Wei Cheng

▶ **To cite this version:**

Om Prakash, Ashutosh Singh, Ram Krishna Verma, Patrick Solé, Wei Cheng. DNA code from cyclic and skew cyclic codes over F 4 [v]/ v 3 . Entropy, 2023. hal-03946495

HAL Id: hal-03946495
https://hal.science/hal-03946495

Submitted on 19 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MDPI

Article

DNA code from cyclic and skew cyclic codes over $\mathbb{F}_4[v]/\langle v^3\rangle$

Om Prakash[1]*, Ashutosh Singh[1], Ram Krishna Verma[2], Patrick Solé[3] and Wei Cheng[4]

[1] Department of Mathematics, Indian Institute of Technology Patna
[2] SRM Institute of Science and Technology, Delhi-NCR Campus, Ghaziabad-201204, Uttar Pradesh, India
[3] I2M, (CNRS, Aix-Marseille University, Centrale Marseille), Marseilles, France
[4] LTCI, Télécom Paris (IP Paris); Secure-IC S.A.S., 104 Boulevard du Montparnasse, 75014 Paris, France
* Correspondence: sole@enst.fr

Abstract: The main motivation of this work is to study and obtain some reversible and DNA codes of length n with better parameters. Here, we first investigate the structure of cyclic and skew cyclic codes over the chain ring $\mathcal{R} := \mathbb{F}_4[v]/\langle v^3\rangle$. We show an association between the codons and the elements of $\mathcal{R}$ using a Gray map. Under this Gray map, we study reversible and DNA codes of length n. Finally, several new DNA codes are obtained that have improved parameters than previously known codes. We also determine the Hamming and the Edit distances of these codes.

Keywords: Reversible code, Gray map, DNA codes.

1. Introduction

DNA is a nucleic acid used for carrying genetic information in living organisms. It is a double-strand molecule formed from two possible nitrogenous bases-Purines (**A**denine & **G**uanine) and Pyrimidines (**C**ytosine & **T**hymine) and two chemically polar ends, namely, $5'$ and $3'$. The Watson-Crick complementary (WCC) relation, which is characterized as $\mathbf{A}^c = \mathbf{T}$, $\mathbf{G}^c = \mathbf{C}$, and vice-versa, is used to bind the bases of DNA. In 1994, Adleman [2] discussed the Hamiltonian path problem using DNA molecules. This (NP-complete) problem is solved by encoding a small graph in DNA molecules where all operations were carried out using standard protocols such as WCC relation. Due to massive parallelism, DNA computing emerged as a powerful tool among researchers to solve computationally difficult problems. Further, experiments are performed on synthesized DNA and RNA molecules to control their combinatorial constraints such as constant $GC-$content and Hamming distance.

Linear codes over finite fields have been explored for almost three decades, but this research area experienced an astonishing rate after the remarkable work of Hammons et al. [21] when they established a relation between linear codes over $\mathbb{Z}_4$ with other non-linear binary codes. Afterwards, many authors considered alphabets endowed with a ring structure and found many good linear codes over finite fields via specific Gray maps. Within the class of linear codes, cyclic codes are the pivotal and the most studied codes due to their theoretical richness and practical implementation. Recently, many authors [4,5,14,20] constructed DNA codes using cyclic codes over rings. For instance, Yildiz and Siap [20] and Bayram et al. [4] explored DNA codes over the rings $\mathbb{F}_2[v]/\langle v^4-1\rangle$ and $\mathbb{F}_4 + v\mathbb{F}_4$, $v^2 = v$, respectively. In 2019, Mostafanasab and Darani [14] discussed the structure of cyclic DNA codes over the chain ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Liu et al. [13] worked on cyclic DNA codes of an odd length over $\mathbb{F}_4[u]/\langle u^3\rangle$. Meanwhile, Gursoy et al. [10] studied reversible DNA codes by using skew cyclic codes. Recently, Cengellenmis et al [7] and Yildilz [20] studied DNA codes from skew cyclic codes over the rings $F_2[u,v,w]$, where $u^2 = v^2 + v = w^2 + w = uv + vu = uw + wu = vw + wv = 0$ and $\mathbb{F}_2[u]/(u^4-1)$, respectively.

Motivated by the above works, we consider cyclic as well as skew cyclic codes over the finite chain ring $\mathcal{R} = \mathbb{F}_4[v]/\langle v^3\rangle$ to construct DNA codes of arbitrary lengths. Hamming

Citation: Prakash, O.; Singh, A.; Verma, R.K.; Solé, P.; and Cheng, W. DNA code from cyclic and skew cyclic codes over $\mathbb{F}_4[v]/\langle v^3\rangle$. *Journal Not Specified* **2022**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2023 by the authors. Submitted to *Journal Not Specified* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

and edit distances are also calculated for the obtained codes. Interestingly, we obtain several new codes with better parameters than known codes [13].

The article is structured as follows: The Gray map, together with the correspondence of the codons and other basic results of cyclic codes, are contained in Section 2. Reversible cyclic codes over the ring $\mathcal{R}$ are covered in Section 3, whereas reversible skew cyclic codes are studied in Section 4. Some results related to the complement and reverse complement of obtained codes are presented in Section 5. Based on our established results from previous Sections, we provide a few examples of DNA codes of arbitrary lengths in Section 6. In the end, we conclude our work in Section 7.

2. Preliminaries

Let $\mathbb{F}_4 = \{0, 1, \mathfrak{t}, \mathfrak{t}^2\}$, where $\mathfrak{t}^2 = \mathfrak{t} + 1$ be a finite field. Then $\mathcal{R} := \mathbb{F}_4[v]/\langle v^3 \rangle$ is a finite chain ring with characteristic 2 and every element r of $\mathcal{R}$ can be represented as $r = \mathfrak{b}_1 + \mathfrak{b}_2 v + \mathfrak{b}_3 v^2$ where $\mathfrak{b}_i \in \mathbb{F}_4$, for $i = 0, 1, 2$ and $v^3 = 0$. It is easy to show that $\mathcal{R}$ is a principal ideal ring with unique maximal ideal $\langle v \rangle$ and $\mathcal{R}/\langle v \rangle$ is isomorphic to $\mathbb{F}_4$. Recall that the ring $\mathcal{R}$ has 48 invertible elements of the form $r = \mathfrak{b}_1 + \mathfrak{b}_2 v + \mathfrak{b}_3 v^2$, where $\mathfrak{b}_1$ is invertible in $\mathbb{F}_4$.

A linear code $\mathcal{C}$ of length n and alphabets from $\mathcal{R}$ is a submodule of an $\mathcal{R}$-module $\mathcal{R}^n$. The elements of $\mathcal{C}$ are called the codewords. The Hamming weight of an element $\mathfrak{b} = (\mathfrak{b}_0, \mathfrak{b}_1, \ldots, \mathfrak{b}_n) \in \mathcal{C}$ is defined as $w_H(\mathfrak{b}) = |\{i \mid \mathfrak{b}_i \neq 0\}|$ and Hamming distance $d_H(\mathfrak{b}, \mathfrak{k})$ between any two elements $\mathfrak{b} = (\mathfrak{b}_0, \mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ and $\mathfrak{k} = (\mathfrak{k}_0, \mathfrak{k}_1, \ldots, \mathfrak{k}_n)$ in $\mathcal{C}$ is defined as $d_H(\mathfrak{b}, \mathfrak{k}) = w_H(\mathfrak{b} - \mathfrak{k})$. Additionally, the lowest value in the set $\{d_H(\mathfrak{b}, \mathfrak{k}) \mid \mathfrak{b} \neq \mathfrak{k}, \forall\, \mathfrak{b}, \mathfrak{k} \in \mathcal{C}\}$ is considered as the the Hamming distance $d_H(\mathcal{C})$ of the code $\mathcal{C}$.

Now, we describe a Gray map $\Phi : \mathcal{R} \longrightarrow \mathbb{F}_4^3$ as

$$\Phi(\mathfrak{b}_0 + \mathfrak{b}_1 v + \mathfrak{b}_2 v^2) = (\mathfrak{b}_0 + \mathfrak{b}_1 + \mathfrak{b}_2, \mathfrak{b}_1 + \mathfrak{b}_2, \mathfrak{b}_2), \tag{1}$$

where $\mathfrak{b}_i \in \mathbb{F}_4$ for $i = 0, 1, 2$. It is easy to see that the function Φ is a distance-preserving map and is extendable to $\mathcal{R}^n$ component-wise. In the table 1, we establish the connection between the ring elements and the codons by using the Gray map (1).

Definition 1. *For a given polynomial $\mathfrak{g}(z) = \mathfrak{g}_0 + \mathfrak{g}_1 z + \ldots + \mathfrak{g}_m z^m \in \mathbb{F}_4[z]$, the reciprocal polynomial is denoted by $\mathfrak{g}^*(z)$ and defined as $\mathfrak{g}^*(z) = \sum_{i=0}^{m} \mathfrak{g}_{m-i} z^i$. A polynomial $\mathfrak{g}(z)$ is said to be self-reciprocal if and only if $\mathfrak{g}^*(z) = b\mathfrak{g}(z)$ for some non-zero element b in $\mathbb{F}_4$.*

Now, we present some useful lemmas that appeared in [8][9][13].

Lemma 1. *Let $\mathfrak{g}(z)$ and $\mathfrak{h}(z)$ be polynomials over $\mathcal{R}$ of degrees r and s, respectively with $r \geq s$. Then*

1. $[\mathfrak{g}(z)\mathfrak{h}(z)]^* = \mathfrak{g}^*(z)\mathfrak{h}^*(z)$
2. $[\mathfrak{g}(z) + \mathfrak{h}(z)]^* = \mathfrak{g}^*(z) + z^{(r-s)}\mathfrak{h}^*(z)$.

Lemma 2. *Let $\mathfrak{f}(z)$, $\mathfrak{g}(z)$ and $\mathfrak{h}(z)$ be polynomials over $\mathcal{R}$ of degrees r, s and t, respectively where $r \geq s, t$.Then*

1. $[\mathfrak{f}(z)\mathfrak{g}(z)\mathfrak{h}(z)]^* = \mathfrak{f}^*(z)\mathfrak{g}^*(z)\mathfrak{h}^*(z)$
2. $[\mathfrak{f}(z) + \mathfrak{g}(z) + \mathfrak{h}(z)]^* = \mathfrak{f}^*(z) + z^{(r-s)}\mathfrak{g}^*(z) + z^{(r-t)}\mathfrak{h}^*(z)$.

Using the Watson-Crick complementary relation, we define the reverse (**R**) and the reverse complement (**RC**) of a DNA codeword $\mathfrak{b} = (\mathfrak{b}_0, \mathfrak{b}_1, \ldots, \mathfrak{b}_{n-1})$ by $\mathfrak{b}^r = (\mathfrak{b}_{n-1}, \ldots, \mathfrak{b}_1, \mathfrak{b}_0)$ and $\mathfrak{b}^{rc} = (\mathfrak{b}_{n-1}^c, \ldots, \mathfrak{b}_1^c, \mathfrak{b}_0^c)$ respectively. For example, given $\mathfrak{b} = ATCCGT$, we get $\mathfrak{b}^r = TGCCTA$ and $\mathfrak{b}^{rc} = ACGGAT$.

We have the following observations based on the Gray map given in equation (1).

0	AAA	v^2	TTT	tv^2	GGG	t^2v^2	CCC
1	TAA	v^2+1	ATT	tv^2+1	CGG	t^2v^2+1	GCC
t	GAA	v^2+t	CTT	tv^2+t	AGG	t^2v^2+t	TCC
t^2	CAA	v^2+t^2	GTT	tv^2+t^2	TGG	$t^2v^2+t^2$	ACC
v	TTA	v^2+v	AAT	tv^2+v	CCG	t^2v^2+v	GGC
$v+1$	ATA	v^2+v+1	TAT	tv^2+v+1	GCG	t^2v^2+v+t	AGC
$v+t$	CTA	v^2+v+t	GAT	tv^2+v+t	TCG	t^2v^2+v+1	CGC
$v+t^2$	GTA	v^2+v+t^2	CAT	tv^2+v+t^2	ACG	$t^2v^2+v+t^2$	TGC
tv	GGA	v^2+tv	CCT	tv^2+tv	AAG	t^2v^2+tv	TTC
$tv+1$	CGA	v^2+tv+1	GCT	tv^2+tv+1	TAG	t^2v^2+tv+1	ATC
$tv+t$	AGA	v^2+tv+t	TCT	tv^2+tv+t	GAG	t^2v^2+tv+t	CTC
$tv+t^2$	TGA	v^2+tv+t^2	ACT	tv^2+tv+t^2	CAG	$t^2v^2+tv+t^2$	GTC
t^2v	CCA	v^2+t^2v	GGT	tv^2+t^2v	TTG	$t^2v^2+t^2v$	AAC
t^2v+1	GCA	v^2+t^2v+1	CGT	tv^2+t^2v+1	ATG	$t^2v^2+t^2v+1$	TAC
t^2v+t	TCA	v^2+t^2v+t	AGT	tv^2+t^2v+t	CTG	$t^2v^2+t^2v+t$	GAC
t^2v+t^2	ACA	$v^2+t^2v+t^2$	TGT	$tv^2+t^2v+t^2$	GTG	$t^2v^2+t^2v+t^2$	CAC

Table 1. Codons correspondence with the elements of $\mathcal{R}$

Lemma 3. *1. For any $a=(\mathfrak{b}_0+\mathfrak{b}_1v+\mathfrak{b}_2v^2)\in\mathcal{R}$, we have*
$\Phi(\mathfrak{b}_0+\mathfrak{b}_1v+\mathfrak{b}_2v^2)^r=\mathfrak{b}_1+\mathfrak{b}_0v+(\mathfrak{b}_0+\mathfrak{b}_1+\mathfrak{b}_2)v^2$, *where* $\mathfrak{b}_0,\mathfrak{b}_1,\mathfrak{b}_2\in\mathbb{F}_4$.
2. $\Phi(\mathfrak{b}_0+\mathfrak{b}_1)^r=\Phi(\mathfrak{b}_0)^r+\Phi(\mathfrak{b}_1)^r$, *where* $\mathfrak{b}_0,\mathfrak{b}_1\in\mathbb{F}_4$.

3. Reversible cyclic codes over $\mathcal{R}$

In the present section, we investigate the structure of cyclic codes and prove reversible conditions on these codes. Cyclic codes of odd lengths are given in [13] and a detailed discussion on cyclic codes of arbitrary length with alphabets from $\mathbb{Z}_2[u]/\langle v^3\rangle$ is explored in [1]. Now, in the subsequent theorems, we describe the structure of cyclic code. We omit the proof due to its similarity to the proof given in [1].

Theorem 1. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{R}$. Then the code $\mathcal{C}$ is given by*

$$\mathcal{C}=\langle \mathfrak{g}_0(z)+v\mathfrak{g}_1(z)+v^2\mathfrak{g}_2(z), va_1(z)+v^2p(z), v^2a_2(z)\rangle$$

where $a_2(z)|a_1(z)|\mathfrak{g}_0(z)|(z^n-1)$ over $\mathbb{F}_4$, $a_1(z)|\mathfrak{g}_1(z)(\frac{z^n-1}{\mathfrak{g}_0(z)})$, $a_2(z)|p(z)(\frac{z^n-1}{a_1(z)})$ and $a_2(z)|\mathfrak{g}_2(z)(\frac{z^n-1}{\mathfrak{g}_0(z)})(\frac{z^n-1}{a_1(z)})$ over $\mathbb{F}_4$. Moreover, $deg(\mathfrak{g}_2(z))<deg(a_2(z))$, $deg(p(z))<deg(a_2(z))$, and $deg(\mathfrak{g}_1(z))<deg(a_1(z))$.

Corollary 1. *If the length of a cyclic code $\mathcal{C}$ is odd and $\mathfrak{g}_1(z)=\mathfrak{g}_2(z)=p(z)=0$, then $\mathcal{C}=\langle \mathfrak{g}_0(z), va_1(z), v^2a_2(z)\rangle=\langle \mathfrak{g}_0(z)+va_1(z)+v^2a_2(z)\rangle$.*

A similar result is also possible when n is not odd. In this case, we assume that $\gcd(\frac{z^n-1}{a_2(z)},\mathfrak{g}_0(z))=1$ and consequently get the following result.

Corollary 2. *If a cyclic code $\mathcal{C}$ is of even length n and $\gcd(\frac{z^n-1}{a_2(z)},\mathfrak{g}_0(z))=1$, then $\mathfrak{g}_1(z)=\mathfrak{g}_2(z)=p(z)=0$.*

When $a_2(z) = \mathfrak{g}_0(z)$, then $a_2(z) = a_1(z) = \mathfrak{g}_0(z)$ and $\mathcal{C}$ as a subset of $\langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)\rangle$. Since other containment is true by the definition of $\mathcal{C}$, therefore, we get the following corollary.

Corollary 3. *For a cyclic code* $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), va_1 + v^2p(z), v^2a_2(z)\rangle$, *if* $a_2(z) = \mathfrak{g}_0(z)$, *then* $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)\rangle$.

Definition 2. *Given a code* $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), va_1(z) + v^2p(z), v^2a_2(z)\rangle$ *over* $\mathcal{R}$, *we define* $\mathcal{C}_{v^2}$ *by* $\{q(z) \in \mathbb{F}_4[z] \mid v^2q(z) \in \mathcal{C}\}$. *Particularly, since* $a_2(z)|a_1(z)|\mathfrak{g}_0(z)$, $\mathcal{C}_{v^2} = \langle a_2(z)\rangle$.

In the next result, we determine the Hamming distance of the code $\mathcal{C}$ by using the above definition in terms of the Hamming distance of $\mathcal{C}_{v^2}$.

Theorem 2. *Let* $\mathcal{C}$ *be a code given by* $\mathcal{C} = \langle \mathfrak{g}(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), va_1(z) + v^2p(z), v^2a_2(z)\rangle$. *Then Hamming distance of* $\mathcal{C}$ *and* $\mathcal{C}_{v^2}$ *are equal, i.e.,* $d_H(\mathcal{C}) = d_H(\mathcal{C}_{v^2})$.

Proof. It can be obtained from [15]. □

Remark 1. *For the sake of brevity, we use b for polynomial* $b(z)$ *whenever* $b(z)$ *belongs to the field* $\mathbb{F}_4$.

Lemma 4. *Let* $\mathfrak{g}_0(z), \mathfrak{g}_1(z)$ *and* $\mathfrak{g}_2(z) \in \mathbb{F}_4[z]$ *of degrees* r, s *and* t, *respectively. Then* $(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z))^* = \mathfrak{g}_0^*(z) + vz^{r-s}\mathfrak{g}_2^*(z) + v^2z^{r-t}\mathfrak{g}_2^*(z)$.

Theorem 3. *Let* $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)\rangle$ *be a cyclic code of even length over* $\mathcal{R}$ *with monic polynomials* $\mathfrak{g}_0(z)$, $\mathfrak{g}_1(z)$ *and* $\mathfrak{g}_2(z)$ *of degrees* r, s *and* t, *respectively. Then the code* $\mathcal{C}$ *is reversible if and only if*

(1) $\mathfrak{g}_0(z)$ *is a self-reciprocal polynomial;*
(2) $z^{r-s}\mathfrak{g}_1^*(z) = b_0\mathfrak{g}_1(z) + b_1\mathfrak{g}_0(z)$ *and* $z^{r-s}\mathfrak{g}_2^*(z) = b_0\mathfrak{g}_2(z) + b_1\mathfrak{g}_1(z) + b_2\mathfrak{g}_0(z)$, *where* $b_0 \in \mathbb{F}_4 \setminus \{0\}$ *and* $b_1, b_2 \in \mathbb{F}_4$.

Proof. Let $\mathcal{C}$ be a reversible cyclic code. Then

$$
\begin{aligned}
(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z))^* &= \mathfrak{g}_0^*(z) + vz^{r-s}\mathfrak{g}_2^*(z) + v^2z^{r-t}\mathfrak{g}_2^*(z) \text{ and} \\
(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z))^* &= b(z)(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)) \in \mathcal{C} \\
&= (b_0(z) + vb_1(z) + v^2b_2(z))(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)) \\
&= b_0(z)\mathfrak{g}_0(z) + v(b_0(z)\mathfrak{g}_1(z) + b_1(z)\mathfrak{g}_0(z)) \\
&\quad + v^2(b_0(z)\mathfrak{g}_2(z) + b_1(z)\mathfrak{g}_1(z) + b_2(z)\mathfrak{g}_0(z)).
\end{aligned}
$$

Comparing right side of two equations, we get $\mathfrak{g}_0^*(z) = b_0(z)\mathfrak{g}_0(z)$, $z^{r-s}\mathfrak{g}_1^*(z) = b_0(z)\mathfrak{g}_1(z) + b_1(z)\mathfrak{g}_0(z)$, and $z^{r-t}\mathfrak{g}_2^*(z) = b_0(z)\mathfrak{g}_2(z) + b_1(z)\mathfrak{g}_1(z) + b_2(z)\mathfrak{g}_0(z)$. Now, using $\deg \mathfrak{f}^*(z) \leq \deg \mathfrak{f}(z)$, we get $b_0(z) \neq 0$ in $\mathbb{F}_4$ and this implies that the polynomial $\mathfrak{g}_0(z)$ is self-reciprocal. Therefore, $z^{r-s}\mathfrak{g}_1^*(z) = b_0\mathfrak{g}_1(z) + b_1(z)\mathfrak{g}_0(z)$ where $b_0 = b_0(z)$ is a non-zero element in $\mathbb{F}_4$. Now comparing the degrees of both sides, we get a constant polynomial $b_1(z) \in \mathbb{F}_4$, say, b_1. We have $z^{r-t}\mathfrak{g}_2^*(z) = b_0\mathfrak{g}_2(z) + b_1\mathfrak{g}_1(z) + b_2(z)\mathfrak{g}_0(z)$. Again, comparing the degrees of both sides, we get $b_2(z)$ in $\mathbb{F}_4$, say b_2. Thus, $z^{r-s}\mathfrak{g}_1^*(z) = b_0\mathfrak{g}_1(z) + b_1\mathfrak{g}_0(z)$

and $z^{r-t}\mathfrak{g}_2^*(z) = b_0\mathfrak{g}_2 + b_1\mathfrak{g}_1(z) + b_2\mathfrak{g}_0(z)$ where $b_0 \in \mathbb{F}_4 \setminus \{0\}$ and $b_1, b_2 \in \mathbb{F}_4$.
Conversely, assume (1) and (2) hold. Then

$$\begin{aligned}(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z))^* =& \mathfrak{g}_0^*(z) + vz^{r-s}\mathfrak{g}_1^*(z) + v^2z^{r-t}\mathfrak{g}_2^*(z)\\ =& b_0\mathfrak{g}_0(z) + vb_0\mathfrak{g}_1(z) + vb_1\mathfrak{g}_0(z) + v^2b_0\mathfrak{g}_2(z)\\ &+ v^2b_1\mathfrak{g}_1(z) + v^2b_2\mathfrak{g}_0(z)\\ =& b_0(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)) + b_1(v\mathfrak{g}_0 + v^2\mathfrak{g}_1)\\ &+ b_2(v^2\mathfrak{g}_0(z)) \in \mathcal{C}\end{aligned}$$

Thus, the code $\mathcal{C}$ is reversible. □

Theorem 4. *Let $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), v^2a_2(z)\rangle$ be a cyclic code of even length n over $\mathcal{R}$ with polynomials $\mathfrak{g}_0(z)$, $\mathfrak{g}_1(z)$ and $\mathfrak{g}_2(z)$ of degrees r, s and t, respectively and $r > \max\{s, t\}$. Also, assume that $a_2(z)|\mathfrak{g}_0(z)|(z^n - 1)$. Then the code $\mathcal{C}$ is reversible if and only if*

(1) $\mathfrak{g}_0(z)$ and $a_2(z)$ are self-reversible;
(2) $z^{r-s}\mathfrak{g}_1^*(z) = b_0\mathfrak{g}_1(z) + b_1\mathfrak{g}_0(z)$, and $a_2(z)|(z^{r-t}\mathfrak{g}_2^*(z) + b_0\mathfrak{g}_2(z) + b_1\mathfrak{g}_1(z)$, where $b_0 \in \mathbb{F}_4 \setminus \{0\}$ and $b_1 \in \mathbb{F}_4$.

Proof. Let $\mathcal{C}$ be a reversible code. Then

$$(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z))^* = \mathfrak{g}_0^*(z) + vz^{r-s}\mathfrak{g}_1^*(z) + v^2z^{r-t}\mathfrak{g}_2^*(z).$$

Also,

$$\begin{aligned}(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z))^* &= b(z)(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)) + v^2c(z)a_2(z)\\ &= (b_0(z) + vb_1(z) + v^2b_2(z))(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) +\\ &v^2\mathfrak{g}_2(z)) + v^2c(z)a_2(z) \text{ where } b_i(z),\ c(z) \in \mathbb{F}_4[z]\\ &= b_0(z)\mathfrak{g}_0(z) + v(b_0(z)\mathfrak{g}_1(z) + b_1(z)\mathfrak{g}_0(z)) + v^2\\ &(b_0(z)\mathfrak{g}_2(z) + b_1(z)\mathfrak{g}_1(z) + b_2(z)\mathfrak{g}_0(z) + c(z)a_2(z)).\end{aligned}$$

Comparing both equations, we get $b_0(z) \in \mathbb{F}_4 \setminus \{0\}$, say b_0, this implies that $\mathfrak{g}_0(z)$ is self-reciprocal. Therefore, $z^{r-s}\mathfrak{g}_1^*(z) = b_0\mathfrak{g}_1(z) + b_1\mathfrak{g}_0(z)$, and $z^{r-t}\mathfrak{g}_2^*(z) = b_0\mathfrak{g}_2(z) + b_1\mathfrak{g}_1(z) + b_2(z)\mathfrak{g}_0(z) + c(z)a_2(z)$, and this implies that $a_2(z)$ divides $z^{r-t}\mathfrak{g}_2^*(z) + b_0\mathfrak{g}_2(z) + b_1\mathfrak{g}_1(z)$. Again, $v^2a_2^*(z) \in \mathcal{C}$ and hence $a_2(z)|\mathfrak{g}_0(z)$ implies that $a_2(z)$ is self-reversible.

Conversely, suppose conditions (1) and (2) hold. Then

$$\begin{aligned}(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z))^* &= \mathfrak{g}_0^*(z) + vz^{r-s}\mathfrak{g}_1^*(z) + v^2z^{r-t}\mathfrak{g}_2^*(z)\\ &= b_0\mathfrak{g}_0(z) + v(b_0\mathfrak{g}_1(z) + b_1\mathfrak{g}_0(z)) + v^2(b_0\mathfrak{g}_2(z)\\ &+ b_1\mathfrak{g}_1(z) + c(z)a_2(z))\ for\ some\ c(z) \in \mathbb{F}_4[z]\\ &= b_0(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)) + vb_1(\mathfrak{g}_0(z)\\ &+ v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)) + c(z)v^2a_2(z) \in \mathcal{C}.\end{aligned}$$

Therefore, $\mathcal{C}$ is reversible. □

The following theorem states the reversible condition of odd length codes or a code satisfying Corollary 2.

Theorem 5. *Let $\mathcal{C} = \langle \mathfrak{g}_0(z), va_1(z), v^2a_2(z)\rangle$ be a cyclic code over $\mathcal{R}$ with $a_2(z)|a_1(z)|\mathfrak{g}_0(z)|(z^n - 1)$. Then code $\mathcal{C}$ is reversible if and only if polynomials $\mathfrak{g}_0(z)$, $a_1(z)$ and $a_2(z)$ are self-reversible.*

Proof. Let $\mathcal{C}$ be a reversible code. Then for some polynomials $b_0(z)$, $b_1(z)$ and $b_2(z)$ in $\mathbb{F}_4[z]$, we have $(\mathfrak{g}_0(z))^* = b_0(z)\mathfrak{g}_0(z) + vb_1(z)a_1(z) + v^2b_2(z)a_2(z)$.

Comparing both sides, we get $b_0(z) \in \mathbb{F}_4 \setminus \{0\}$, say b_0, since $deg\mathfrak{f}^*(z) \leq deg\mathfrak{f}(z)$, then $\mathfrak{g}_0(z)$ is self-reciprocal. Similarly, $a_1(z)$ and $a_2(z)$ are self-reciprocal polynomials.
Conversely, let the polynomials $\mathfrak{g}_0(z)$, $a_1(z)$ and $a_2(z)$ be self-reciprocal. Then elements of $\mathcal{C}$ are given by the polynomial $b_0(z)\mathfrak{g}_0(z) + vb_1(z)a_1(z) + v^2b_2(z)a_2(z)$, therefore by Lemma [4] we have

$$\begin{aligned}(b_0(z)\mathfrak{g}_0(z) + vb_1(z)a_1(z) + v^2b_2(z)a_2(z))^* &= (b_0(z)\mathfrak{g}_0(z))^* + v(b_1(z)a_1(z))^*z^{r-s} \\ &\quad + v^2(b_2(z)a_2(z))^*z^{r-t}. \\ &= b_0^*(z)\mathfrak{g}_0^*(z) + vz^{r-s}b_1^*(z)a_1^*(z) \\ &\quad + v^2z^{r-t}b_2^*(z)a_2^*(z) \in \mathcal{C}.\end{aligned}$$

Thus, $\mathcal{C}$ is reversible. □

Now, in the following result, we determine the rank of a code $\mathcal{C}$. The proof is followed by similar arguments as in Theorem [3] of [1].

Theorem 6. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathcal{R}$ such that*

$$\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), va_1(z) + vp(z), v^2a_2(z)\rangle,$$

where $\mathfrak{g}_0(z)$, $\mathfrak{g}_1(z)$, $\mathfrak{g}_2(z)$ and $a_2(z)$ are polynomials in $\mathbb{F}_4[z]$ and $de\mathfrak{g}(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)) = r$, $de\mathfrak{g}(a_1(z)) = s$ and $de\mathfrak{g}(a_2(z)) = t$. Then $\mathcal{C}$ is a free module and $rank(\mathcal{C}) = n - t$. Moreover, basis of $\mathcal{C}$ is given by the set S, where

$$\begin{aligned}S =&\{(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)), x(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z)), \ldots, z^{n-r-1}(\mathfrak{g}_0(z) + v\mathfrak{g}_1(z) \\ &+ v^2\mathfrak{g}_2(z)), (va_1(z) + v^2p(z)), x(va_1(z) + v^2p(z)), \ldots, z^{r-s-1}(va_1(z) + v^2p(z)), \\ &v^2a_2(z), v^2xa_2(z), \ldots, v^2z^{s-t-1}a_2(z))\}.\end{aligned}$$

4. Reversible skew cyclic codes over $\mathcal{R}$

In this part, we focus on the structure of skew cyclic codes over $\mathcal{R}$ and establish a necessary and sufficient condition for these codes to be reversible. We first define the skew polynomial ring over $\mathcal{R}$ and give some definitions which will be used in this section.
Let $\theta \in Aut(\mathbb{F}_4)$ be defined by $\theta(a) = a^2$. Now, consider a map $\sigma : \mathcal{R} \longrightarrow \mathcal{R}$ defined by

$$\sigma(a_0 + a_1v + a_2v^2) = \theta(a_0) + \theta(a_1)v + \theta(a_2)v^2,$$

where $a_0, a_1, a_2 \in \mathbb{F}_4$. Since σ is an extension of θ, σ is an automorphism of $\mathcal{R}$. Let us consider the set

$$\mathcal{R}[z;\sigma] = \{a_0 + a_1z + \ldots + a_nz^n \mid a_i \in \mathcal{R}\ \forall\ i, n \in \mathbb{N}\}.$$

Define addition on $\mathcal{R}[z;\sigma]$ as usual addition of polynomials and multiplication under the rule $(a_iz^i)(a_jz^j) = a_i\sigma^i(a_j)z^{i+j}$. Then it is easy to show that $\mathcal{R}[z;\sigma]$ forms a ring under the above binary operations, known as a skew polynomial ring. Here, $(a_iz^i)(a_jz^j) \neq (a_jz^j)(a_iz^i)$ unless σ is identity automorphism.

Definition 3. *Let $\tau_\sigma : \mathcal{R}^n \longrightarrow \mathcal{R}^n$ be a skew cyclic shift operator defined by*

$$\tau_\sigma(a_0, a_1, \ldots, a_{n-1}) = (\sigma(a_{n-1}), \sigma(a_0), \ldots, \sigma(a_{n-2})), \forall\ (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n.$$

Then a linear code $\mathcal{C}$ of length n over $\mathcal{R}$ is said to be skew cyclic code if for any codeword $c \in \mathcal{C}$, their skew cyclic shift $\tau_\sigma(c)$ belongs to $\mathcal{C}$, that is, $\tau_\sigma(\mathcal{C}) = \mathcal{C}$.

Definition 4. *For skew polynomials, $a(z)$ and $b(z) \neq 0$, the polynomial $b(z)$ is said to be right divide $a(z)$ if and only if there exists a skew polynomial $q(z)$ such that $a(z) = q(z)b(z)$ and we denote it by $b(z)|_r a(z)$.*

Using similar arguments as in the commutative case, we give the structure of skew cyclic codes over $\mathcal{R}$ for automorphism σ.

Theorem 7. *Let $\mathcal{C}$ be a skew cyclic code in $\frac{\mathcal{R}[z;\sigma]}{\langle z^n-1\rangle}$. Then $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), va_1(z) + v^2p(z), v^2a_2(z)\rangle$ with $a_2(z)|_r a_1(z)|_r \mathfrak{g}_0(z)|_r(z^n-1)$ in $\mathbb{F}_4[z;\theta]$, $a_1(z)|_r \mathfrak{g}_1(z)(\frac{z^n-1}{\mathfrak{g}_0(z)})$ and $a_2(z)$ right divides $p(z)(\frac{z^n-1}{a_1(z)})$, and $\mathfrak{g}_2(z)(\frac{z^n-1}{\mathfrak{g}_0(z)})(\frac{z^n-1}{a_1(z)})$.*

Proof. Consider the ring $\mathcal{R}' = \frac{\mathbb{F}_4[v]}{\langle v^2\rangle}$ and $\sigma' \in Aut(\mathcal{R}')$. For a skew cyclic code $\mathcal{C}$ over $\mathcal{R}$, define a map $\psi_1 : \mathcal{R} \to \mathcal{R}'$ by $\psi_1(a + bv + cv^2) = a + bv$ where $a, b, c \in \mathbb{F}$. Then ψ_1 is a ring homomorphism that can be extended to a homomorphism $\phi : \mathcal{C} \to \frac{\mathcal{R}'[z;\sigma']}{\langle z^n-1\rangle}$ defined by

$$\phi(c_0 + c_1z + \ldots + c_{n-1}z^{n-1}) = \psi_1(c_0) + \psi_1(c_1)z + \ldots + \psi_1(c_{n-1})z^{n-1}.$$

Then $ker(\phi) = \{v^2r(z) : r(z) \in \mathbb{F}_4[z;\theta]/\langle z^n-1\rangle\}$.

In order to determine the generators of cyclic code in $\mathcal{R}_n = \mathcal{R}[z,\sigma]/\langle z^n-1\rangle$, we need to know the image of ϕ which is a skew cyclic code in $\mathcal{R}'_n = \mathcal{R}'[z,\sigma_2]/\langle z^n-1\rangle$.
Let D be a cyclic code in $\mathcal{R}'_n$. Now, define a map $\psi_2 : \mathcal{R}' \to \mathbb{F}_4$ by $\psi_2(a + ub) = a^2$. Then ψ_2 is a ring homomorphism. We extend ψ_2 to a ring homomorphism $\varphi : D \to \mathbb{F}_4[z;\theta]/\langle z^n-1\rangle$ defined by

$$\varphi(d_0 + d_1z + \ldots + d_{n-1}z^{n-1}) = \psi_2(d_0) + \psi_2(d_1)z + \ldots + \psi_2(d_{n-1})z^{n-1}$$

Then

$$\begin{aligned} ker(\varphi) &= \{vr'(z) : r'(z) \text{ is a skew polynomial in } \mathbb{F}_4[z;\theta]/\langle z^n-1\rangle\} \\ &= \langle va_1(z)\rangle \text{ with } a_1(z)|_r(z^n-1). \end{aligned}$$

Since the set image(φ) is also an ideal and hence a skew cyclic code generated by $\mathfrak{g}_0(z)$, where $\mathfrak{g}_0(z)$ right divides (z^n-1). Therefore, $D = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z), va_1(z)\rangle$ where $a_1(z)|_r\mathfrak{g}_0(z)$ and $a_1(z)|_r(\mathfrak{g}_1(z)\frac{z^n-1}{\mathfrak{g}_0(z)})$.
Similarly, the set image(ϕ) is an ideal over $\mathcal{R}'$. Therefore, skew cyclic code $\mathcal{C}$ over $\mathcal{R}$ is given by $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), va_1(z) + v^2p(z), v^2a_2(z)\rangle$ with $a_2(z)|_r a_1(z)|_r \mathfrak{g}_0(z)|_r(z^n - 1)$ and $a_1(z)|_r(\mathfrak{g}_1(z)\frac{z^n-1}{\mathfrak{g}_0(z)})$, $a_2(z)|_r(\mathfrak{g}_1(z)\frac{z^n-1}{\mathfrak{g}_0(z)})$. □

Definition 5. *Let $\mathfrak{g}(z) = \mathfrak{g}_0 + \mathfrak{g}_1z + \ldots + \mathfrak{g}_mz^m$ be a polynomial in $\mathbb{F}_4[z,\theta]$. Then $\mathfrak{g}(z)$ is said to be a palindromic polynomial if $\mathfrak{g}_i = \mathfrak{g}_{m-i}$ and θ-palindromic if $\mathfrak{g}_i = \theta(\mathfrak{g}_{m-i})$ where $i \in \{1, 2, \ldots, m\}$.*

Note that if the length of the code $\mathcal{C}$ is odd, then skew cyclic codes and cyclic codes are equivalent [18, Theorem 16]. Now, we give two lemmas to check the reversibility of even length skew cyclic codes over the field $\mathbb{F}_4$.

Lemma 5. *Let $\mathcal{C}$ be a skew cyclic code of even length generated by a monic polynomial $\mathfrak{f}(z) = 1 + \mathfrak{f}_1z + \ldots + \mathfrak{f}_{m-1}z^{m-1} + z^m$ of even degree, where $\mathfrak{f}(z)|_r(z^n-1)$ in $\mathbb{F}_4[z,\theta]$. Then the code $\mathcal{C}$ is reversible if and only if skew polynomial $\mathfrak{f}(z)$ is θ-palindromic.*

Proof. Let $\mathcal{C}$ be a skew cyclic code of even length generated by θ-palindromic polynomial $\mathfrak{f}(z)$ of even degree m over the ring $\mathbb{F}_4$. Then elements of the generated code are given by $\sum_{i=0}^{k-1} \alpha_i z^i \mathfrak{f}(z)$. By repetitive use of Lemma 3, for $c = \phi(\sum_{i=0}^{k-1} \alpha_i z^i \mathfrak{f}(z)) \in \mathcal{C}$, we get

$$(\phi(\sum_{i=0}^{k-1} \alpha_i z^i \mathfrak{f}(z)))^r = \phi(\sum_{i=0}^{k-1} \alpha_i z^{k-i-1} \mathfrak{f}(z)) \in \mathcal{C}.$$

Where $\alpha \in \mathbb{F}_4$ and $k = n - m$. Since c^r belongs to the code $\mathcal{C}$, $\mathcal{C}$ is a reversible code. Conversely, let $\mathcal{C}$ be a reversible code generated by $\mathfrak{f}(z) = 1 + \mathfrak{f}_1 z + \ldots + \mathfrak{f}_{m-1} z^{m-1} + z^m$. Then, because $n - m - 1$ is odd,

$$z^{n-m-1}\mathfrak{f}(z) = z^{n-m-1} + \theta(\mathfrak{f}_1) z^{n-m} + \ldots + \theta(\mathfrak{f}_{m-1}) z^{n-2} + z^{n-1}.$$

Since $\mathcal{C}$ is a skew cyclic and reversible code,

$$[z^{n-m-1}\mathfrak{f}(z)]^r = 1 + \theta(\mathfrak{f}_{m-1}) z + \theta(\mathfrak{f}_{m-2}) z^2 + \ldots + \theta(\mathfrak{f}_1) z^{m-1} + z^m \in \mathcal{C}.$$

Further, we get $deg(\mathfrak{f}(z) - [z^{n-m-1}\mathfrak{f}(z)]^r) < m$, which contradicts the fact that $\mathfrak{f}(z)$ is a minimal degree polynomial in $\mathcal{C}$ implies $\mathfrak{f}(z) - [z^{n-m-1}\mathfrak{f}(z)]^r = 0$. Comparing coefficients, we get

$$[\mathfrak{f}_i - \theta(\mathfrak{f}_{m-i})] = 0$$

for $i = 1, \ldots, m-1$. Thus, $\mathfrak{f}_i = \theta(\mathfrak{f}_{m-i})$ and the polynomial $\mathfrak{f}(z)$ is θ-palindromic. □

Lemma 6. *Let $\mathcal{C}$ be a skew cyclic code of even length generated by a monic polynomial $\mathfrak{f}(z) = 1 + \mathfrak{f}_1 z + \ldots + \mathfrak{f}_{m-1} z^{m-1} + z^m$ of odd degree, where $\mathfrak{f}(z)|_r(z^n - 1)$ in $\mathbb{F}_4[z, \theta]$. Then the code $\mathcal{C}$ is reversible if and only if the skew polynomial $\mathfrak{f}(z)$ is palindromic.*

Proof. Let $\mathcal{C}$ be a skew cyclic code of even length generated by a palindromic polynomial $\mathfrak{f}(z)$ of odd degree m over the ring $\mathbb{F}_4$. Then elements of the generated code are given by $\sum_{j=0}^{k-1} \alpha_j z^j \mathfrak{f}(z)$. By repetitive use of Lemma 3 and using property of palindromic polynomial, for $\mathcal{C} = \phi(\sum_{j=0}^{k-1} \alpha_j z^j \mathfrak{f}(z)) \in \mathcal{C}$, we get

$$(\phi(\sum_{j=0}^{k-1} \alpha_j z^j \mathfrak{f}(z)))^r = \phi(\sum_{j=0}^{k-1} \alpha_j z^{k-j-1} \mathfrak{f}(z)) \in \mathcal{C}.$$

Where $\alpha \in \mathbb{F}_4$ and $k = n - m$. Since the reverse of $\mathcal{C}$ belongs to $\mathcal{C}$, the code $\mathcal{C}$ is reversible. Conversely, Let $\mathcal{C}$ be a reversible code generated by $\mathfrak{f}(z) = 1 + \mathfrak{f}_1 z + \ldots + \mathfrak{f}_{m-1} z^{m-1} + z^m$. Since $n - m - 1$ is even,

$$z^{n-m-1}\mathfrak{f}(z) = z^{n-m-1} + \mathfrak{f}_1 z^{n-m} + \ldots + \mathfrak{f}_{m-1} z^{n-2} + z^{n-1}.$$

Also, the code $\mathcal{C}$ is a skew cyclic as well as reversible code; therefore, $[z^{n-m-1}\mathfrak{f}(z)]^r \in \mathcal{C}$ and

$$[z^{n-m-1}\mathfrak{f}(z)]^r = [1 + \mathfrak{f}_{m-1} z + \mathfrak{f}_{m-2} z^2 + \ldots + \mathfrak{f}_1 z^{m-1} + z^m] \in \mathcal{C}.$$

This implies that $deg(\mathfrak{f}(z) - [z^{n-m-1}\mathfrak{f}(z)]^r) < m$, which contradicts the fact that $\mathfrak{f}(z)$ is a minimal degree polynomial in $\mathcal{C}$. Hence, $\mathfrak{f}(z) - [z^{n-m-1}\mathfrak{f}(z)]^r = 0$. By comparing the coefficients, we get

$$[\mathfrak{f}_i - \mathfrak{f}_{m-i}] = 0 \text{ and } \mathfrak{f}_i = \mathfrak{f}_{m-i},$$

for $i = 1, \ldots, m-1$. Thus, the given polynomial $\mathfrak{f}(z)$ is palindromic. □

Now, in the next theorem, we provide necessary and sufficient conditions for a skew cyclic code $\mathcal{C}$ to be reversible in terms of palindromic and θ-palindromic polynomials. These conditions depend on the degree of generator polynomials of $\mathcal{C}$.

Theorem 8. *Let $\mathcal{C} = \langle \mathfrak{g}_0(z), v\mathfrak{g}_1(z), v^2\mathfrak{g}_2(z)\rangle$ be a skew cyclic code of even length, where $\mathfrak{g}_i(z)$ right divides (z^n-1) in $\mathbb{F}_4[z,\theta]$ and $deg(\mathfrak{g}_i(z))$ is even(odd), for $i = 0,1,2$. Then, the code $\mathcal{C}$ is reversible if and only if skew polynomials $\mathfrak{g}_i(z)$ are θ-palindromic (palindromic) for $i = 0,1,2$.*

5. DNA codes over $\mathcal{R}$

In this section, we discuss the complementary condition of the codes obtained from previous sections to get DNA codes. For a DNA code, reversible and complement conditions are essential.

Definition 6. *Let $\mathcal{C}$ be a code of length n over $\mathcal{R}$. If $\Phi(\mathcal{C})^{rc} \in \Phi(\mathcal{C})$ for all $c \in \mathcal{C}$, then $\mathcal{C}$ or equivalently $\Phi(\mathcal{C})$ is called a DNA code.*

In the following lemma, we give some relations on ring elements and their complement using the Gray map given in equation 1.

Lemma 7. *For given cyclic code in Section 3, the following conditions hold:*

(1) For any $r \in \mathcal{R}$, $r + r^c = v^2$.

(2) For any $r_1, r_2 \in \mathcal{R}$, $r_1^c + r_2^c = (r_1 + r_2)^c + v^2$.

Proof. This lemma can easily be proved by observing Table 1. □

Remark 2. *We identify $\mathfrak{i}(z)$ by the polynomial $1 + z + z^2 + \cdots + z^{n-1}$.*

Theorem 9. *Given a polynomial $\mathfrak{a}(z)$ in $\mathcal{R}[z]$. We have $\mathfrak{a}(z)^{rc} = \mathfrak{a}(z)^r + v^2\mathfrak{i}(z)$.*

Proof. Let $\mathcal{C}$ be a reversible-complement code. Then by definition $\mathcal{C}$ is reversible and $0 \in \mathcal{C}$ implies that $(0 + 0z + \ldots + 0z^{n-1})^c \in \mathcal{C}$. That is, $\mathcal{C}$ is reversible and $v^2 + v^2z + \ldots + v^2z^{n-1} \in \mathcal{C}$.
Conversely, let $\mathfrak{a}(z) = \mathfrak{a}_0 + \mathfrak{a}_1 z + \ldots + \mathfrak{a}_{n-1}z^{n-1} + \mathfrak{a}_n z^n$ be a polynomial in $\mathcal{R}[z]$. Then

$$\begin{aligned}\mathfrak{a}(z)^{rc} &= \mathfrak{a}_n^c + \mathfrak{a}_{n-1}^c z + \ldots + \mathfrak{a}_1^c z^{n-1} + \mathfrak{a}_0^c z^n \\ &= \mathfrak{a}_n + v^2 + (\mathfrak{a}_{n-1} + v^2)z + (\mathfrak{a}_{n-2} + v^2)z^2 + \ldots \\ &+ (\mathfrak{a}_1 + v^2)z^{n-1} + (\mathfrak{a}_0 + v^2)z^n \\ &= v^2\mathfrak{i}(z) + \mathfrak{a}(z)^r \in \mathcal{C}.\end{aligned}$$

Thus, cyclic code $\mathcal{C}$ is a reversible-complement code. □

Corollary 4. *Let $\mathcal{C}$ be a cyclic code of even length over $\mathcal{R}$. Then $\mathcal{C}$ is a DNA code if and only if $\mathcal{C}$ is reversible and $v^2\mathfrak{i}(z)$ is in $\mathcal{C}$.*

Proof. It is obvious from above theorem. □

6. Computational Results

Now, we provide some examples of DNA codes satisfying above mentioned constraints. We consider DNA code of any length (even or odd). All the computational works are performed by using Magma software [6].

Example 1. *In $\mathbb{F}_4[z]$, we have*

$$z^6 - 1 = (z+1)^2(z+\mathfrak{t})^2(z+\mathfrak{t}^2)^2.$$

Length	$\mathfrak{g}_0(z)$	Type of code	Gray image
5	$1\mathfrak{t}1$	$(5,3,3)$	$(15,4^9,3)$
5	11111	$(5,1,5)$	$(15,4^3,5)$
6	10101	$(6,2,3)$	$(18,4^6,3)$
10	101010101	$(10,2,5)$	$(30,4^6,5)$
13	$1\mathfrak{t}0(1+\mathfrak{t})0\mathfrak{t}1$	$(13,7,5)$	$(39,4^{21},5)$
14	1010101010101	$(14,2,7)$	$(42,4^6,7)$
17	$11\mathfrak{t}11$	$(17,13,4)$	$(51,4^{39},4)$
17	$1(1+\mathfrak{t})11\mathfrak{t}11(1+\mathfrak{t})1$	$(17,9,7)$	$(51,4^{27},7)$
29	$1\mathfrak{t}0\mathfrak{t}(1+\mathfrak{t})1(1+\mathfrak{t})\mathfrak{t}(1+\mathfrak{t})1(1+\mathfrak{t})\mathfrak{t}0\mathfrak{t}1$	$(10,1,5)$	$(30,4^3,5)$

Table 2. DNA codes of different lengths.

Code	Type of code	Gray image	DNA code [13]
$\langle \mathfrak{g}_2\mathfrak{g}_3, v\mathfrak{g}_2\mathfrak{g}_3, v^2\mathfrak{g}_2\mathfrak{g}_3\rangle$	$(15,13,2)$	$(45,4^{39},2)$	$(45,4^{26},2)$
$\langle \mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_6, v\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_6, v^2\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_6\rangle$	$(15,11,4)$	$(45,4^{33},4)$	$(45,4^{24},3)$
$\langle \mathfrak{g}_4\mathfrak{g}_8\mathfrak{g}_9, v\mathfrak{g}_4\mathfrak{g}_8\mathfrak{g}_9, v^2\mathfrak{g}_4\mathfrak{g}_8\mathfrak{g}_9\rangle$	$(15,9,5)$	$(45,4^{27},5)$	$(45,4^{18},5)$
$\langle \mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7, v\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7, v^2\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7\rangle$	$(15,7,7)$	$(45,4^{21},7)$	$(45,4^{14},7)$
$\langle \mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7\mathfrak{g}_9, v\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7\mathfrak{g}_9, v^2\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7\mathfrak{g}_9\rangle$	$(15,3,9)$	$(45,4^9,9)$	$(45,4^6,9)$

Table 3. Codes of length 45.

Let $\mathcal{C}$ be a cyclic code of length $n = 6$ over $\mathcal{R}$ given by

$$\mathcal{C} = \langle z^4+z^2+1, v(z^4+z^2+1), v^2(z^4+z^2+1)\rangle.$$

Then by Theorem [2], we get $d(\mathcal{C}) = 3$. Also, $(x-1)$ does not divide (z^4+z^2+1) and polynomial (z^4+z^2+1) is self reciprocal. Thus, we get a DNA code $\mathcal{C}$ of parameters $(18,4^6,3)$.

In the next example, we give some DNA codes of arbitrary lengths which are generated from cyclic codes over $\mathcal{R}$.

Example 2. *Suppose $\mathcal{C}$ is a cyclic code of the form $\mathcal{C} = \langle \mathfrak{g}_0(z) + v\mathfrak{g}_1(z) + v^2\mathfrak{g}_2(z), va_1(z) + v^2p(z), v^2a_2(z)\rangle$, where $\gcd(\frac{z^n-1}{a_2(z)}, \mathfrak{g}_0(z)) = 1$. If $\mathfrak{g}_0(z) = a_1(z) = a_2(z)$, then we list several DNA codes in Table 2 which are obtained from cyclic code $\mathcal{C}$. Since $\mathfrak{g}_0(z)$, $a_1(z)$ and $a_2(z)$ are equal, therefore in Table 2, we mention only $\mathfrak{g}_0(z)$. For the brevity, polynomial $z^2+\mathfrak{b}_1z+\mathfrak{b}_0$ is represented as $\mathfrak{b}_0\mathfrak{b}_1 1$.*

Sr No	Generator of Code	Type of code	Gray image	DNA code [13]
1	$\langle \mathfrak{g}_2\mathfrak{g}_3, v\mathfrak{g}_2\mathfrak{g}_3, v^2\mathfrak{g}_2\mathfrak{g}_3\rangle$	$(9,7,2)$	$(27,4^{21},2)$	$(27,4^{14},2)$
2	$\langle \mathfrak{g}_4\mathfrak{g}_5, v\mathfrak{g}_4\mathfrak{g}_5, v^2\mathfrak{g}_4\mathfrak{g}_5\rangle$	$(9,3,3)$	$(27,4^9,3)$	$(27,4^6,3)$
3	$\langle \mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5, v\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5, v^2\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5\rangle$	$(9,1,9)$	$(27,4^3,9)$	$(27,4^2,9)$

Table 4. Codes of length 27.

AAAAAAAAAAAAAAAAAAAAAAAAA	TAATAATAATAATAATAATAATAA
GAAGAAGAAGAAGAAGAAGAAGAAA	CAACAACAACAACAACAACAACAACAA
TTATTATTATTATTATTATTATTA	ATAATAATAATAATAATAATAATA
CTACTACTACTACTACTACTACTA	GTAGTAGTAGTAGTAGTAGTAGTA
GGAGGAGGAGGAGGAGGAGGAGGA	CGACGACGACGACGACGACGACGACGA
AGAAGAAGAAGAAGAAGAAGAAGA	TGATGATGATGATGATGATGATGA
CCACCACCACCACCACCACCACCA	GCAGCAGCAGCAGCAGCAGCAGCA
TCATCATCATCATCATCATCATCA	ACAACAACAACAACAACAACAACA
TTTTTTTTTTTTTTTTTTTTTTTTT	ATTATTATTATTATTATTATTATT
CTTCTTCTTCTTCTTCTTCTTCTT	GTTGTTGTTGTTGTTGTTGTTGTT
AATAATAATAATAATAATAATAAT	TATTATTATTATTATTATTATTAT
GATGATGATGATGATGATGATGAT	CATCATCATCATCATCATCATCAT
CCTCCTCCTCCTCCTCCTCCTCCT	GCTGCTGCTGCTGCTGCTGCTGCT
TCTTCTTCTTCTTCTTCTTCTTCT	ACTACTACTACTACTACTACTACT
GGTGGTGGTGGTGGTGGTGGTGGT	CGTCGTCGTCGTCGTCGTCGTCGT
AGTAGTAGTAGTAGTAGTAGTAGT	TGTTGTTGTTGTTGTTGTTGTTGT
GGGGGGGGGGGGGGGGGGGGGGGG	CGGCGGCGGCGGCGGCGGCGGCGG
AGGAGGAGGAGGAGGAGGAGGAGG	TGGTGGTGGTGGTGGTGGTGGTGG
CCGCCGCCGCCGCCGCCGCCGCCG	GCGGCGGCGGCGGCGGCGGCGGCG
TCGTCGTCGTCGTCGTCGTCGTCG	ACGACGACGACGACGACGACGACG
AAGAAGAAGAAGAAGAAGAAGAAG	TAGTAGTAGTAGTAGTAGTAGTAG
GAGGAGGAGGAGGAGGAGGAGGAG	CAGCAGCAGCAGCAGCAGCAGCAG
TTGTTGTTGTTGTTGTTGTTGTTG	ATGATGATGATGATGATGATGATG
CTGCTGCTGCTGCTGCTGCTGCTG	GTGGTGGTGGTGGTGGTGGTGGTG
CCCCCCCCCCCCCCCCCCCCCCCC	GCCGCCGCCGCCGCCGCCGCCGCC
TCCTCCTCCTCCTCCTCCTCCTCC	ACCACCACCACCACCACCACCACC
GGCGGCGGCGGCGGCGGCGGCGGC	AGCAGCAGCAGCAGCAGCAGCAGC
CGCCGCCGCCGCCGCCGCCGCCGC	TGCTGCTGCTGCTGCTGCTGCTGC
TTCTTCTTCTTCTTCTTCTTCTTC	ATCATCATCATCATCATCATCATC
CTCCTCCTCCTCCTCCTCCTCCTC	GTCGTCGTCGTCGTCGTCGTCGTC
AACAACAACAACAACAACAACAAC	CACCACCACCACCACCACCACCAC
TACTACTACTACTACTACTACTAC	GACGACGACGACGACGACGACGAC

Table 5. Codewords of length 45 and dimension 3.

Example 3. *Consider a cyclic code $\mathcal{C}$ of length $n = 9$ over ring $\mathcal{R}$. In $\mathbb{F}_4[z]$, we have*

$$z^9 - 1 = (z+1)(z+\mathfrak{t})(z+\mathfrak{t}^2)(z^3+\mathfrak{t})(z^3+\mathfrak{t}^2).$$

To write briefly, we identify factors by $\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3, \mathfrak{g}_4$ and $\mathfrak{g}_5$, respectively. Codes for $n = 9$ are given in Table 4. All codes are better than codes that appeared in [13].

Example 4. *Consider a cyclic code $\mathcal{C}$ of length $n = 15$ over ring $\mathcal{R}$. In $\mathbb{F}_4[z]$, we have*

$$\begin{aligned} z^{15} - 1 =& (z+1)(z+\mathfrak{t})(z+\mathfrak{t}^2)(z^2+z+\mathfrak{t})(z^2+z+\mathfrak{t}^2)(z^2+\mathfrak{t}z+1) \\ & (z^2+\mathfrak{t}z+\mathfrak{t})(z^2+\mathfrak{t}^2z+1)(z^2+\mathfrak{t}^2z+\mathfrak{t}^2). \end{aligned}$$

For brevity, we identify factors by $\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3, \mathfrak{g}_5, \mathfrak{g}_6, \mathfrak{g}_7, \mathfrak{g}_8$, and $\mathfrak{g}_9$, respectively. DNA codes for $n = 15$ are given in Table 3. All obtained DNA codes are better than the codes given in [13]. In particular, if $\mathcal{C} = \langle \mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7\mathfrak{g}_8\mathfrak{g}_9,\ v\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7\mathfrak{g}_8\mathfrak{g}_9,\ v^2\mathfrak{g}_2\mathfrak{g}_3\mathfrak{g}_4\mathfrak{g}_5\mathfrak{g}_6\mathfrak{g}_7\mathfrak{g}_8\mathfrak{g}_9 \rangle$, then we obtained a DNA code with parameters $[45, 4^3, 15]$. Further, we list all DNA codewords of obtained DNA code in table 5.

7. Conclusions

In this paper, we have studied reversible and DNA codes using the chain ring $\mathcal{R} = \mathbb{F}_4[v]/\langle v^3 \rangle$. We have defined a Gray map on $\mathcal{R}$ and found codons corresponding to the elements of $\mathcal{R}$. In this way, we have obtained good DNA and reversible codes with the

Hamming distances. In the future one can work on DNA codes over a generalized structure of $\mathcal{R}$ as well as DNA codes by using skew polynomial rings.

Author Contributions: This work is initiated by the second and third authors under the supervision of the first author. Then we discussed it with the fourth and fifth authors to reach to the final version.

Funding:

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: The first and second authors are thankful to the DST and the CSIR, Govt. of India, for financial support under CRG/2020/005927, vide Diary No. SERB/F/6780/ 2020-2021 dated 31 December 2020 and under File No. 09/1023(0027)/2019- EMR-1, respectively. Also, we thank the Indian Institute of Technology Patna for providing research facilities.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Abualrub, T.; Siap, I. Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$. *Des. Codes Cryptogr.*, **2007**, 42(3), 273-287.
2. Adleman, L.M. Molecular computation of solutions to combinatorial problems. *Science*. **1994**, 266(5187), 1021-1024.
3. Akutsu, T. Tree edit distance problems: Algorithms and applications to bioinformatics. *IEICE transactions on information and systems*. **2010**, 93(2), 208-218.
4. Bayram, A.; Oztas, E.S.; Siap, I. Codes over $F_4 + vF_4$ and some DNA applications. *Des. Codes Cryptogr.* **2016**, 80, 379-393. https://doi.org/10.1007/s10623-015-0100-8.
5. Bennenni, N.; Guenda, K.; Mesnager, S. DNA cyclic codes over rings. *Advances in Mathematics of Communications*, **2017**, 11(1), 83.
6. Bosma, W.; Cannon, W.J.; Playoust, C. The Magma algebra system I: The user language. *J. Symbolic Comput.* **1997**, 24(3-4), 235-265.
7. Cengellenmis, Y.; Aydin, N.; Dertli, A. Reversible DNA codes from skew cyclic codes over a ring of order 256, *Journal of Algebra Combinatorics Discrete Structures and Applications*. **2021**, 8(1), 1-8.
8. 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. *Theoret. Comput. Sci.* **2019**, 773, 27-42.
9. Guenda, K.; Gulliver, T.A. Construction of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ for DNA computing. *Appl. Algebra Engrg. Comm. Comput.* **2013**, 24(6), 445-459.
10. Gursoy, F.; Oztas, E.S.; Siap, I. Reversible DNA codes using skew polynomial rings. *Appl. Algebra Engrg. Comm. Comput.* **2017**, 28(4), 311-320.
11. Limbachiya, D.; Rao, B.; Gupta, M.K. The art of DNA strings: Sixteen years of DNA coding theory. arXiv preprint arXiv:1607.00266, **2016**.
12. Ling, S. Xing, C. Coding theory: a first course. *Cambridge University Press*. **2004**.
13. Liu, J.; Liu, H. DNA Codes Over the Ring $\mathbb{F}_4[u]/\langle u^3\rangle$. IEEE Access. **2020**, 8, 77528-77534.
14. Mostafanasab H.; Darani, A. Y. On Cyclic DNA Codes Over $F_2 + uF_2 + u^2F_2$. *Commun. Math. Stat.* **2019**, 1-14.
15. Norton, G. H.; Sălăgean, A. On the Hamming distance of linear codes over a finite chain ring. *IEEE Trans. Inform. Theory*, **2000**, 46(3), 1060-1067.
16. Norton, G. H.; Sălăgean, A. On the structure of linear and cyclic codes over a finite chain ring. *Appl. Algebra Engrg. Comm. Comput.* **2000**, 10(6), 489-506.
17. Ristad E. S.; Yianilos, P. N. Learning string-edit distance. *IEEE Trans. Pattern Anal. Mach. Intell.* **1998**, 20(5), 522-532.
18. Siap, I.; Abualrub, T.; Aydin N.; Seneviratne, P. Skew cyclic codes of arbitrary length. *Int. J. Inf. Coding Theory*. **2011**, 2(1), 10-20.
19. Jitman, S.; Ling, S.; Udomkavanich, P. Skew constacyclic codes over finite chain rings. *arXiv preprint arXiv:1008.0327*. **2010**.
20. Yildiz, B.; Siap, I. Cyclic codes over $F_2[u]/(u^4 - 1)$ and applications to DNA codes. *Comput. Math. Appl*. **2012**, 63(7), 1169-1176.
21. Hammons, A. R.; Kumar, P. V.; Calderbank, A. R.; Sloane, N. J.; Solé, P. The $Z/sub4/-$linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inf. Theory*. **1994**, 40(2), 301-319.