Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 3** : 1–10.
ISSN-0037-8712
doi:10.5269/bspm.79100

On Skew Cyclic Reversible DNA Codes Over $\mathbb{F}_4[v]/\langle v^4 - v\rangle$

Joël Kabore* and Mohammed Elhassani Charkani

ABSTRACT: In this paper, we study a specific class of skew cyclic codes over the ring $\mathbb{F}_4[v]/\langle v^4 - v\rangle$ which is suitable for describing DNA codes over this ring. Using the Gray map between $\mathbb{F}_4[v]/\langle v^4 - v\rangle$ and $\mathbb{F}_4^4$ (or equivalently DNA 4-bases), we describe reversible DNA codes and reversible-complement DNA codes over this ring.

Key Words: Skew cyclic code, gray map, reversible code, DNA code.

Contents

1 Introduction **1**

2 Background **2**

3 Skew Cyclic Codes with a Particular Automorphism **3**

4 Skew Cyclic DNA Codes **5**

5 Conclusion **9**

1. Introduction

In recent years, numerous connections have been established between coding theory and biology, particularly in the study of genetics through DNA molecules. This intersection has drawn significant attention leading to the emergence of DNA coding as a vibrant research area within coding theory. DNA computing has become a subject of growing interest.

DNA is a molecule composed of two strands, each being a finite sequence made up of nucleotides: A(for Adenine), G(for Guanine), T(for Thymine), and C(for Cytosine). These strands are paired through the Watson-Crick complement where A pairs with T and G pairs with C. In genetics, a DNA molecule is represented as a pair of complementary strands twisted into a double helix. The process in which a strand binds with its Watson-Crick complement to form this structure is known as hybridization.

A nonempty subset of $\mathfrak{D}^n$, where $\mathfrak{D}$ is the set of nucleotides, is called DNA code of length n. It must satisfy several biological and combinatorial constraints. These criteria ensure stability, reliability and biological applications.

Adelman was the pioneer of DNA computing, having initiated this field in 1994 by using the Watson-Crick Complement to fix an NP-complete problem [3]. Since then, the study of DNA codes have been extended over various algebraic structures [2,3,4,8,9,10,15,16]. Much work on skew cyclic codes over finite rings have been done, see for example [7,13,17] for chain rings and [1,6,12,14] for over rings.

Abualrub et al. investigate the structure of θ- skew cyclic codes and their duals over the ring $\mathbb{F}_2[v]/\langle v^2 - v\rangle$ in [1]. Bhardwaj et al. further explore skew constacyclic codes within a broader class of non-chain rings in [6]. In [11], Gursoy et al. employ skew cyclic codes over finite fields to construct DNA codes. Several methods for constructing DNA codes using skew cyclic codes over $\mathbb{F}_4 + v\mathbb{F}_4$ are provided in [5,15]. This structural understanding enables us to effectively study skew cyclic codes over $\mathbb{F}_4[v]/\langle v^4 - v\rangle$ and to characterize DNA codes.

This study is structured as follows. Section 2 provides basic properties related to codes and DNA codes. Section 3 is dedicated to constructing skew cyclic codes over $\mathbb{F}_4[v]/\langle v^4 - v\rangle$, adapted for DNA codes study. Section 4 focuses on the reversibility of DNA codes over $\mathbb{F}_4[v]/\langle v^4 - v\rangle$.

* Corresponding author.
2020 *Mathematics Subject Classification:* 94B05, 94B60, 11T71.
Submitted September 22, 2025. Published January 22, 2026

2. Background

In this paper, we denote the ring $\frac{\mathbb{F}_4[v]}{\langle v^4-v\rangle}$ by $\mathfrak{R}_4$, and $\mathbb{F}_4$ is the finite field $\{0,1,\varpi,\varpi^2\}$, with $\varpi^2=\varpi+1$. The ring $\mathfrak{R}_4$ is a finite principal ring with maximal ideals: $\langle v\rangle,\ \langle v-1\rangle,\ \langle v-\varpi\rangle,\ \langle v-\varpi^2\rangle$. Let

$$\eta_0=v^3+1,\ \eta_1=v^3+v^2+v,\ \eta_2=v^3+\varpi v^2+\varpi^2 v,\ \eta_3=v^3+\varpi^2 v^2+\varpi v.$$

It is easy to see that $\eta_i^2=\eta_i,\ \eta_i\eta_j=0$ and $\sum_{i=0}^{3}\eta_i=1$, where $0\le i\neq j\le 4$. Then any element $\lambda=\lambda_0+\lambda_1 v+\lambda_2 v^2+\lambda_3 v^3$ of $\mathfrak{R}_4$ can be uniquely represented as (see [14]):

$$\lambda=\lambda_0\eta_0+(\lambda_0+\lambda_1+\lambda_2+\lambda_3)\eta_1+(\lambda_0+\varpi\lambda_1+\varpi^2\lambda_2+\lambda_3)\eta_2+(\lambda_0+\varpi^2\lambda_1+\varpi\lambda_2+\lambda_3)\eta_3.$$

Note that an element $\lambda=\lambda_0\eta_0+\lambda_1\eta_1+\lambda_2\eta_2+\lambda_3\eta_3$ is a unit if and only if $\lambda_i\neq 0,\quad \forall\ i\in\{0,1,2,3\}$. We defined the Gray map on $\mathfrak{R}_4$ by $\Psi:\mathfrak{R}_4\longrightarrow\mathbb{F}_4^4$, where

$$\Psi(\lambda_0\eta_0+\lambda_1\eta_1+\lambda_2\eta_2+\lambda_3\eta_3)=(\lambda_0,\lambda_1,\lambda_2,\lambda_3).$$

Any $\mathfrak{R}_4$-submodule of $\mathfrak{R}_4^n$ is called linear code of length n over $\mathfrak{R}_4$. Let $\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_n)$ be an element of $\mathfrak{R}_4^n$ and w_H be the function defined by $w_H(\lambda):=|\{i\mid \lambda_i\neq 0\}|$. Hamming distance between two codewords λ,β is defined as $d_H(\lambda,\beta)=w_H(\lambda-\beta)$. Using the Gray map Ψ, it is convenient to endowed $\mathbb{F}_4^{4n}$ with the Hamming distance and $\mathfrak{R}_4^n$ with the well-known Lee distance defined as $d_L(\lambda,\beta)=w_L(\lambda-\beta)$, where $w_L(\lambda)=w_H(\Psi(\lambda))$. It is easy to verify the following result.

Lemma 2.1 *The Gray map $\Psi:(\mathfrak{R}_4^n,d_L)\longrightarrow(\mathbb{F}_4^{4n},d_H)$ is a distance-preserving map.*

Let $\mathfrak{R}_4[y,\theta]:=\left\{\lambda_0+\lambda_1 y+\ldots+\lambda_{n-1}y^{n-1}\mid \lambda_i\in\mathfrak{R}_4, n\in\mathbb{N}\right\}$ be the skew polynomial ring defined over $\mathfrak{R}_4$, where θ is an automorphism over $\mathfrak{R}_4$. We recall that the addition in $\mathfrak{R}_4[y,\theta]$ is the usual addition of polynomials and the multiplication is defined by $(\lambda y^i)(\beta y^j)=\lambda\theta^i(\beta)y^{i+j}$. A linear code $\mathfrak{C}$ of length n over $\mathfrak{R}_4$ such that $\tau_\theta(\lambda)=(\theta(\lambda_{n-1}),\theta(\lambda_0),\cdots,\theta(\lambda_{n-2}))\in\mathfrak{C}$ whenever $\lambda=(\lambda_0,\lambda_1,\cdots,\lambda_{n-1})\in\mathfrak{C}$ is called θ-skew cyclic code of length n over $\mathfrak{R}_4$. By identifying the codeword $(\lambda_0,\lambda_1,\cdots,\lambda_{n-1})$ with the polynomial $\lambda_0+\lambda_1 y+\cdots+\lambda_{n-1}y^{n-1}$, we can consider a θ-skew cyclic code of length n over $\mathfrak{R}_4$ as a left submodule of the $\mathfrak{R}_4[y,\theta]$-module $\mathfrak{R}_n:=\mathfrak{R}_4[y,\theta]/\langle\, y^n-1,\rangle$, where the multiplication is defined as

$$\mathfrak{g}(y)\,(\mathfrak{h}(y)+\langle\, y^n-1\,\rangle)=\mathfrak{g}(y)\mathfrak{h}(y)+\langle\, y^n-1\,\rangle.$$

A code $\mathfrak{C}$ of length $4n$ over $\mathbb{F}_4$ is called a 4-quasi-cyclic code if

$$\tau_4(u)=(u_0^{(n-1)},u_1^{(n-1)},u_2^{(n-1)},u_3^{(n-1)},u_0^{(0)},u_1^{(0)},u_2^{(0)},u_3^{(0)},\cdots,u_0^{(n-2)},u_1^{(n-2)},u_2^{(n-2)},u_3^{(n-2)})\in\mathfrak{C}$$

whenever

$$u=(u_0^{(0)},u_1^{(0)},u_2^{(0)},u_3^{(0)},u_0^{(1)},u_1^{(1)},u_2^{(1)},u_3^{(1)},\cdots,u_0^{(n-1)},u_1^{(n-1)},u_2^{(n-1)},u_3^{(n-1)})\in\mathfrak{C},\ \forall\ u\in\mathfrak{C}.$$

In the sequel, we consider the automorphism θ defined on $\mathfrak{R}_4$ by

$$\theta(\lambda_0\eta_0+\lambda_1\eta_1+\lambda_2\eta_2+\lambda_3\eta_3)=\lambda_3\eta_0+\lambda_2\eta_1+\lambda_1\eta_2+\lambda_0\eta_3.$$

In [14], this automorphism corresponds to $\Theta_{Id,\tau}$, where τ is the permutation $(0\ 3)(1\ 2)$. The following result shows the connection between skew cyclic codes over $\mathfrak{R}_4$ and 4-quasi-cyclic codes over $\mathbb{F}_4$.

Theorem 2.1 *Let $\mathfrak{C}\subset\mathfrak{R}_4^n$. If $\mathfrak{C}$ is a skew cyclic code, then $\Psi(\mathfrak{C})(\subseteq\mathbb{F}_4^{4n})$ is similar to a 4-quasi-cyclic code.*

Proof: Suppose that $u=(u_0^{(0)}\eta_0+u_1^{(0)}\eta_1+u_2^{(0)}\eta_2+u_3^{(0)}\eta_3,u_0^{(1)}\eta_0+u_1^{(1)}\eta_1+u_2^{(1)}\eta_2+u_3^{(1)}\eta_3,\cdots,u_0^{(n-1)}\eta_0+u_1^{(n-1)}\eta_1+u_2^{(n-1)}\eta_2+u_3^{(n-1)}\eta_3)\in\mathfrak{C}$. We have

$$\begin{aligned}\tau_4(\Psi(u)) &= \tau_4((u_0^{(0)},u_1^{(0)},u_2^{(0)},u_3^{(0)},u_0^{(1)},u_1^{(1)},u_2^{(1)},u_3^{(1)}\cdots,u_0^{(n-1)},u_1^{(n-1)},u_2^{(n-1)},u_3^{(n-1)}))\\ &= (u_0^{(n-1)},u_1^{(n-1)},u_2^{(n-1)},u_3^{(n-1)},u_0^{(0)},u_1^{(0)},u_2^{(0)},u_3^{(0)},\cdots,u_0^{(n-2)},u_1^{(n-2)},u_2^{(n-2)},u_3^{(n-2)})\end{aligned}$$

and

$$\begin{aligned}
\Psi(\tau_\theta(u)) &= \Psi(\theta(u_0^{(n-1)}\eta_0 + u_1^{(n-1)}\eta_1 + u_2^{(n-1)}\eta_2 + u_3^{(n-1)}\eta_3), \theta(u_0^{(0)}\eta_0 + u_1^{(0)}\eta_1 + u_2^{(0)}\eta_2 + u_3^{(0)}\eta_3),\\
&\quad \cdots, \theta(u_0^{(n-2)}\eta_0 + u_1^{(n-2)}\eta_1 + u_2^{(n-2)}\eta_2 + u_3^{(n-2)}\eta_3))\\
&= \Psi(u_3^{(n-1)}\eta_0 + u_2^{(n-1)}\eta_1 + u_1^{(n-1)}\eta_2 + u_0^{(n-1)}\eta_3, u_3^{(0)}\eta_0 + u_2^{(0)}\eta_1 + u_1^{(0)}\eta_2 + u_0^{(0)}\eta_3,\\
&\quad \cdots, u_3^{(n-2)}\eta_0 + u_2^{(n-2)}\eta_1 + u_1^{(n-2)}\eta_2 + u_0^{(n-2)}\eta_3)\\
&= (u_3^{(n-1)}, u_2^{(n-1)}, u_1^{(n-1)}, u_0^{(n-1)}, u_3^{(0)}, u_2^{(0)}, u_1^{(0)}, u_0^{(0)}, \cdots, u_3^{(n-2)}, u_2^{(n-2)}, u_1^{(n-2)}, u_0^{(n-2)}).
\end{aligned}$$

□

We can associate $\mathbb{F}_4$ and nucleotides set $\mathfrak{D}$ by using the one-to-one map μ defined by $\mu(0) = A,\ \mu(1) = T,\ \mu(\varpi) = C,\ \mu(\varpi^2) = G$. It follows that $\overline{0} = 1,\ \overline{1} = 0,\ \overline{\varpi} = \varpi^2,\ \overline{\varpi^2} = \varpi$. This map naturally extends to $\mathfrak{R}_4$ by

$$\mu(\lambda_0\eta_0 + \lambda_1\eta_1 + \lambda_2\eta_2 + \lambda_3\eta_3) = \mu(\lambda_0)\eta_0 + \mu(\lambda_1)\eta_1 + \mu(\lambda_2)\eta_2 + \mu(\lambda_3)\eta_3.$$

A one-to-one map Φ between $\mathfrak{R}_4$ and $\mathfrak{D}_4 = \{AAAA, TTTT, GGGG, CCCC, \cdots\}$ is defined by

$$\begin{array}{cccc}
\Phi: & \mathfrak{R}_4 & \to & \mathfrak{D}_4\\
 & \lambda_0\eta_0 + \lambda_1\eta_1 + \lambda_2\eta_2 + \lambda_3\eta_3 & \mapsto & (\mu(\lambda_0), \mu(\lambda_1), \mu(\lambda_2), \mu(\lambda_3)).
\end{array}$$

Definition 2.1 *1. A code $\mathfrak{C}$ is called reversible code if $\lambda^r = (\lambda_{n-1}, \lambda_{n-2}, ..., \lambda_0) \in \mathfrak{C}$ whenever $\lambda = (\lambda_0, \lambda_1, ..., \lambda_{n-1}) \in \mathfrak{C}$ for all $\lambda \in \mathfrak{C}$; λ^r is called the reverse of λ.*

2. A code $\mathfrak{C}$ is called complement code if $\lambda^c = (\overline{\lambda}_0, \overline{\lambda}_1, ..., \overline{\lambda}_{n-1}) \in \mathfrak{C}$ whenever $\lambda = (\lambda_0, \lambda_1, ..., \lambda_{n-1}) \in \mathfrak{C}$ for all $\lambda \in \mathfrak{C}$; λ^c is called the complement of λ.

3. A code $\mathfrak{C}$ is called reversible-complement if $\lambda^{rc} = (\overline{\lambda}_{n-1}, \overline{\lambda}_{n-2}, ..., \overline{\lambda}_0) \in \mathfrak{C}$ whenever $\lambda = (\lambda_0, \lambda_1, ..., \lambda_{n-1}) \in \mathfrak{C}$ for all $\lambda \in \mathfrak{C}$; λ^{rc} is called the reverse-complement of λ.

Example 2.1 *Let $\mathfrak{C}$ be a code of length 3 over $\mathfrak{R}_4$ and $\lambda = (\varpi\eta_0 + \eta_1 + \varpi^2\eta_2, \eta_1 + \varpi^2\eta_3, \varpi\eta_0 + \varpi^2\eta_1 + \eta_2 + \eta_3)$ be a codeword. The codeword λ corresponds to the DNA codeword $\Phi(\lambda) = (CTGA, ATAG, CGTT)$. The reverse of λ is given by $\lambda^r = (\varpi\eta_0 + \varpi^2\eta_1 + \eta_2 + \eta_3, \eta_1 + \varpi^2\eta_3, \varpi\eta_0 + \eta_1 + \varpi^2\eta_2)$ and this corresponds to the DNA codeword $\Phi(\lambda^r) = (CGTT, ATAG, CTGA)$. However $\Phi(\lambda^r)$ is not the reverse of $\Phi(\lambda)$ which is given by*

$$\begin{aligned}
\Phi(\lambda)^r &= (TTGC, GATA, AGTC)\\
&= \Phi(\eta_0 + \eta_1 + \varpi^2\eta_2 + \varpi\eta_3, \varpi^2\eta_0 + \eta_2, \varpi^2\eta_1 + \eta_2 + \varpi\eta_3)\\
&= \Phi((\theta(\lambda))^r).
\end{aligned}$$

The above example shows that the automorphism θ is a suitable tool to characterize the reversibility of DNA codes since $\Phi(\lambda)^r = \Phi((\theta(\lambda))^r)$.

3. Skew Cyclic Codes with a Particular Automorphism

In the sequel, we simply designate a θ-skew cyclic code by skew cyclic code and denote it by $\mathfrak{C}$. Note that an element $\lambda = \lambda_0\eta_0 + \lambda_1\eta_1 + \lambda_2\eta_2 + \lambda_3\eta_3 \in \mathfrak{R}_4$ is a unit if and only if $\lambda_i \neq 0$, for all $i \in \{0, 1, 2, 3\}$. This implies that λ is not a unit if and only if λ can be represented as $\lambda_{i_1}\eta_{i_1} + \lambda_{i_2}\eta_{i_2} + \lambda_{i_3}\eta_{i_3}$, where $\lambda_{i_1}, \lambda_{i_2}, \lambda_{i_3} \in \mathbb{F}_4$ and $i_1, i_2, i_3 \in \{0, 1, 2, 3\}$.

Remark 3.1 *The lemma below is given in [6, Lemma 3] in an incorrect form.*

Lemma 3.1 *Let $\mathfrak{g}(y) = \lambda_t y^t + \lambda_{t-1}y^{t-1} + \cdots + \lambda_0 \in \mathfrak{C}$, where t is the minimal degree in $\mathfrak{C}$ and $\lambda_t = \lambda_{i_1}\eta_{i_1} + \lambda_{i_2}\eta_{i_2} + \lambda_{i_3}\eta_{i_3}$ with $\lambda_{i_1}, \lambda_{i_2}, \lambda_{i_3} \in \mathbb{F}_4 \setminus \{0\}$. Then all coefficients of $\mathfrak{g}$ are represented as $\beta_{i_1}\eta_{i_1} + \beta_{i_2}\eta_{i_2} + \beta_{i_3}\eta_{i_3}$.*

Proof: Let $\mathfrak{g}(y) = \lambda_t y^t + \lambda_{t-1}y^{t-1} + \cdots + \lambda_0$, where $\lambda_t = \lambda_{i_1}\eta_{i_1} + \lambda_{i_2}\eta_{i_2} + \lambda_{i_3}\eta_{i_3}$. If η_{i_4} is an other idempotent that does not appear in the representation of λ_t, then $\eta_{i_4}\lambda_t = 0$. It follows that $\deg(\eta_{i_4}\mathfrak{g}(y)) < t$. Then, according to the minimality of $\deg(\mathfrak{g})$, we obtain $\eta_{i_4}\mathfrak{g}(y) = 0$. □

Theorem 3.1 *Let $\mathfrak{g}(y) = \lambda_t y^t + \lambda_{t-1} y^{t-1} + \cdots + \lambda_0 \in \mathfrak{C}$, where t is the minimal degree in $\mathfrak{C}$ and λ_t is a unit. Then $\mathfrak{C} = \langle \mathfrak{g} \rangle$ and $\mathfrak{g}$ is a right divisor of $y^n - 1$.*

Proof: Let $\mathfrak{h}(y)$ be a polynomial in $\mathfrak{C}$. Using the left division algorithm, there exist two polynomials $q_1(y),\ r_1(y) \in \mathfrak{R}_4[y,\theta]$ such that $\mathfrak{h}(y) = q_1(y)\mathfrak{g}(y) + r_1(y)$, where $\deg r_1 < \deg \mathfrak{g}$.
The fact that $\mathfrak{C}$ is a left submodule of $\mathfrak{R}_n$ ensures that $r_1(y) = \mathfrak{h}(y) - q_1(y)\mathfrak{g}(y) \in \mathfrak{C}$. Since $t = \deg(\mathfrak{g}$ is minimal, we obtain $r_1(y) = 0$.
Likewise, using the left division algorithm, it is easy to deduce that $\mathfrak{g}$ is a right divisor of $y^n - 1$. □

The following result is similar to [1, Lemma 3].

Lemma 3.2 *Let $\mathfrak{g}(y) = \lambda_t y^t + \lambda_{t-1} y^{t-1} + \cdots + \lambda_0 \in \mathfrak{C}$, where t is the minimal degree in $\mathfrak{C}$ and $\lambda_t = \lambda_{i_1}\eta_{i_1} + \lambda_{i_2}\eta_{i_2} + \lambda_{i_3}\eta_{i_3}$ with $\lambda_{i_1}, \lambda_{i_2}, \lambda_{i_3} \in \mathbb{F}_4 \setminus \{0\}$. Let $\mathfrak{f} \in \mathfrak{R}_4[y,\theta]$ such that $\deg \mathfrak{f} > \deg \mathfrak{g}$. Then there exist two polynomials $q_1(y),\ r_1(y) \in \mathfrak{R}_4[y,\theta]$ such that $\mathfrak{f}(y) = q_1(y)\mathfrak{g}(y) + r_1(y)$, where $\deg r_1(y) \leq \deg \mathfrak{g}(y)$ or $r_1(y)$ is a polynomial with a unit leading coefficient that satisfies $\deg r_1(y) \leq \deg \mathfrak{f}(y)$.*

Proof: Suppose $\mathfrak{f} = \varpi$ is a constant term, then $\mathfrak{g} = \lambda_{i_1}\eta_{i_1} + \lambda_{i_2}\eta_{i_2} + \lambda_{i_3}\eta_{i_3}$. We denote the other idempotent by η_{i_4}.

- If $\mathfrak{f}$ is unit then $\mathfrak{f} = 0\mathfrak{g} + \mathfrak{f}$
- If $\mathfrak{f}$ is not a unit, then $\mathfrak{f} = \beta_{j_1}\eta_{j_1}$ or $\mathfrak{f} = \beta_{j_1}\eta_{j_1} + \beta_{j_2}\eta_{j_2}$ or $\mathfrak{f} = \beta_{j_1}\eta_{j_1} + \beta_{j_2}\eta_{j_2} + \beta_{j_3}\eta_{j_3}$.
  Case 1: $\mathfrak{f} = \beta_{j_1}\eta_{j_1}$.
  Subcase 1: If $\mathfrak{f} = \beta_{i_1}\eta_{i_1}$, then $\mathfrak{f} = (\beta_{i_1}\lambda_{i_1}^{-1}\eta_{i_1})\mathfrak{g}$. It is similar for indices $i_2; i_3$.
  Subcase 2: If $\mathfrak{f} = \beta_{i_4}\eta_{i_4}$, then $\mathfrak{f} = \beta_{i_4}(\lambda_{i_1}^{-1}\eta_{i_1} + \lambda_{i_2}^{-1}\eta_{i_2} + \lambda_{i_3}^{-1}\eta_{i_3})\mathfrak{g} + \beta_{i_4}$.
  Case 2: $\mathfrak{f} = \beta_{j_1}\eta_{j_1} + \beta_{j_2}\eta_{j_2}$.
  Subcase 1: If $\mathfrak{f} = \beta_{i_1}\eta_{i_1} + \beta_{i_2}\eta_{i_2}$, then $\mathfrak{f} = (\beta_{i_1}\lambda_{i_1}^{-1}\eta_{i_1} + \beta_{i_2}\lambda_{i_2}^{-1}\eta_{i_2})\mathfrak{g}$. It is similar for the couple of indices $(i_1, i_3); (i_2, i_3)$.
  Subcase 2: If $\mathfrak{f} = \beta_{i_1}\eta_{i_1} + \beta_{i_4}\eta_{i_4}$, then $\mathfrak{f} = (\beta_{i_1}\lambda_{i_1}^{-1}\eta_{i_1})\mathfrak{g} + \beta_{i_4}\eta_{i_4}$. But from Case 1, we have $\beta_{i_4}\eta_{i_4} = q\mathfrak{g} + \beta_{i_4}$, where $q = \beta_{i_4}(\lambda_{i_1}^{-1}\eta_{i_1} + \lambda_{i_2}^{-1}\eta_{i_2} + \lambda_{i_3}^{-1}\eta_{i_3})$. It follows that $\mathfrak{f} = (\beta_{i_1}\lambda_{i_1}^{-1}\eta_{i_1} + q)\mathfrak{g} + \beta_{i_4}$. It is similar for the pairs $(i_2, i_4); (i_3, i_4)$.
  Case 3: $\mathfrak{f} = \beta_{j_1}\eta_{j_1} + \beta_{j_2}\eta_{j_2} + \beta_{j_3}\eta_{j_3}$.
  Subcase 1: If $\mathfrak{f} = \beta_{i_1}\eta_{i_1} + \beta_{i_2}\eta_{i_2} + \beta_{i_3}\eta_{i_3}$, then $\mathfrak{f} = (\beta_{i_1}\lambda_{i_1}^{-1}\eta_{i_1} + \beta_{i_2}\lambda_{i_2}^{-1}\eta_{i_2} + \beta_{i_3}\lambda_{i_3}^{-1}\eta_{i_3})\mathfrak{g}$.
  Subcase 2: If $\mathfrak{f} = \beta_{i_1}\eta_{i_1} + \beta_{i_2}\eta_{i_2} + \beta_{i_4}\eta_{i_4}$, then $\mathfrak{f} = (\beta_{i_1}\lambda_{i_1}^{-1}\eta_{i_1} + \beta_{i_2}\lambda_{i_2}^{-1}\eta_{i_2})\mathfrak{g} + \beta_{i_4}\eta_{i_4}$. From Case 1, $\beta_{i_4}\eta_{i_4} = q\mathfrak{g} + \beta_{i_4}$, this implies that $\mathfrak{f} = (\beta_{i_1}\lambda_{i_1}^{-1}\eta_{i_1} + \beta_{i_2}\lambda_{i_2}^{-1}\eta_{i_2} + q)\mathfrak{g} + \beta_{i_4}$. It is similar for triplets $(i_1, i_3, i_4); (i_2, i_3, i_4)$.

The proof is completed using induction on the degree of $\mathfrak{f}$. □

Theorem 3.2 *Let $\mathfrak{C}$ be a skew cyclic code of length n over $\mathfrak{R}_4$ which does not contain any polynomial with a unit leading coefficient. Suppose that $\mathfrak{g}$ is a polynomial in $\mathfrak{C}$ of minimal degree whose its leading coefficient is represented as $\lambda_{i_1}\eta_{i_1} + \lambda_{i_2}\eta_{i_2} + \lambda_{i_3}\eta_{i_3}$, where $\lambda_{i_1}, \lambda_{i_2}, \lambda_{i_3}$ are non zero elements in $\mathbb{F}_4$. Then $\mathfrak{C} = \langle \mathfrak{g}(y) \rangle$.*
Moreover, $\mathfrak{g}(y) = \eta_{i_1} g_0(y) + \eta_{i_2} g_1(y) + \eta_{i_3} g_2(y)$, where $g_0(y),\ g_1(y),\ g_2(y)$ are divisors of $y^n - 1$ in $\mathbb{F}_4[y]$.

Proof: Without loss of generality, let us consider that the leading coefficient of $\mathfrak{g}$ is represented as $\lambda_0\eta_0 + \lambda_1\eta_1 + \lambda_1\eta_2$, where $\lambda_0, \lambda_1, \lambda_2$ are non zero elements in $\mathbb{F}_4$. Let $\mathfrak{h}(y) \in \mathfrak{C}$, from Lemma 3.2, there exist two polynomials $q_1(y),\ r_1(y) \in \mathfrak{R}_4[y,\theta]$ such that $\mathfrak{h}(y) = q_1(y)\mathfrak{g}(y) + r_1(y)$, where $\deg r_1(y) \leq \deg \mathfrak{g}(y)$ or $r_1(y)$ is a polynomial with a unit leading coefficient that satisfies $\deg r_1(y) \leq \deg \mathfrak{h}(y)$. Since $\mathfrak{C}$ does not contain any polynomial with a unit leading coefficient, then $r_1(y) = 0$, by minimality of degree of $\mathfrak{g}$. Hence $\mathfrak{C} = \langle \mathfrak{g}(y) \rangle$. Using Lemma 3.1, we find that $\mathfrak{g}(y)$ can be represented as $\mathfrak{g}(y) = \eta_0 g_0 + \eta_1 g_1 + \eta_2 g_2$, where $g_0, g_1, g_2 \in \mathbb{F}_4[y]$. Using the division algorithm over $\mathbb{F}_4[y]$, there exist $q_2(y),\ r_2(y) \in \mathbb{F}_4[y]$ such that $y^n - 1 = q_2(y)g_0(y) + r_2(y)$, where $\deg r_2(y) < \deg g_0(y)$. We have

$$\begin{aligned}(\eta_0+\eta_3)(y^n-1) &= (\eta_0+\eta_3)q_2(y)g_0(y) + (\eta_0+\eta_3)r_2(y)\\ &= q_2(y)(\eta_0+\eta_3)g_0(y) + (\eta_0+\eta_3)r_2(y)\\ &= q_2(y)\eta_0 g_0(y) + q_2(y)\eta_3 g_0(y) + (\eta_0+\eta_3)r_2(y)\\ &= q_2(y)\eta_0 \mathfrak{g}(y) + q_2(y)\eta_3 g_0(y) + (\eta_0+\eta_3)r_2(y).\end{aligned}$$

Since $q_2(y)\eta_1\mathfrak{g}(y) = q_2(y)\eta_1 g_1(y)$ and $q_2(y)\eta_2\mathfrak{g}(y) = q_2(y)\eta_2 g_2(y) \in \mathfrak{C}$, then

$$q_2(y)\eta_1 g_1(y) + q_2(y)\eta_2 g_2(y) + q_2(y)\eta_0 g_0(y) + q_2(y)\eta_3 g_0(y) + (\eta_0+\eta_3)r_2(y) \in \mathfrak{C}.$$

Since $\deg(g_1) = \deg(g_2) = \deg(g_0)$ and $\deg(r_2(y)) < \deg(g_0(y))$, then the leading coefficient of $q_2(y)\eta_1 g_1(y) + q_2(y)\eta_2 g_2(y) + q_2(y)\eta_0 g_0(y) + q_2(y)\eta_3 g_0(y) + (\eta_0+\eta_3)r_2(y)$ is a unit. Moreover, $\mathfrak{C}$ does not contain any polynomial with a unit leading coefficient, then $q_2(y)\eta_1 g_1(y) + q_2(y)\eta_2 g_2(y) + q_2(y)\eta_0 g_0(y) + q_2(y)\eta_3 g_0(y) + (\eta_0+\eta_3)r_2(y) = 0$. We get $r_2(y) = 0$. Thus g_0 divides $y^n - 1$. It is the same case for g_1 and g_2. □

Theorem 3.3 *[6, Theorem 7] Suppose that $\mathfrak{C}$ contains some polynomials with a unit leading coefficient such that none of them is of minimal degree. Let $\mathfrak{g}(y)$ be a polynomial in $\mathfrak{C}$ of minimal degree with a non-unit leading coefficient and $\mathfrak{f}(y)$ be a polynomial of minimal degree among polynomials in $\mathfrak{C}$ with a unit leading coefficient. Then $\mathfrak{C} = \langle \mathfrak{g}(y), \mathfrak{f}(y)\rangle$.*

4. Skew Cyclic DNA Codes

In this section, we focus on the properties of skew DNA cyclic codes over $\mathfrak{R}_4$.

Definition 4.1 *[11, Definition 4] Let θ be an automorphism of $\mathfrak{R}_4$.*

1. *A palindromic polynomial $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_t y^t$ of degree t over $\mathfrak{R}_4$ is a polynomial that satisfies $\lambda_j = \lambda_{t-j}\ \forall\ j \in \{0, 1 \cdots, t\}$.*
2. *A θ-palindromic polynomial $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_t y^t$ of degree t over $\mathfrak{R}_4$ is a polynomial that satisfies $\lambda_j = \theta(\lambda_{t-j})\ \forall\ j \in \{0, 1 \cdots, t\}$.*

If λ is a codeword, we easyly find that $\Psi(\lambda)^r = \Psi(\theta(\lambda)^r)$.

Definition 4.2 *A linear code $\mathfrak{C}$ over $\mathfrak{R}_4$ is said to be a reversible DNA code if $\Psi(\lambda)^r \in \Psi(\mathfrak{C})$ for all $\lambda \in \mathfrak{C}$. It is said to be a reversible-complement DNA code if $\Psi(\lambda)^{rc} \in \Psi(\mathfrak{C})\ \forall\ \lambda \in \mathfrak{C}$.*

Theorem 4.1 *Let $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_{t-1}y^{t-1} + \lambda_t y^t$ be a right divisor of $y^n - 1$ in $\mathfrak{R}_4[y, \theta]$. Suppose that λ_t is a unit and $n,\ t$ are even. Then the skew cyclic code $\mathfrak{C} = \langle \mathfrak{g}(y)\rangle$ of length n is a reversible DNA code if and only if $\mathfrak{g}(y)$ is a palindromic polynomial.*

Proof: Suppose that $\mathfrak{g}$ is a palindromic polynomial, then $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_1 y^{t-1} + \lambda_0 y^t$. For a codeword λ, we have $(\Psi(\lambda))^r = \Psi((\theta(\lambda))^r)$. Therefore

$$(\Psi(\sum_{j=0}^{l} \gamma_j x^j \mathfrak{g}(y)))^r = \Psi(\sum_{j=0}^{l} \theta(\gamma_j) x^{l-j}\mathfrak{g}(y)) \tag{4.1}$$

where $l = n - t - 1$ and $\gamma_j \in \mathfrak{R}_4$. The result is clear since $\mathfrak{C}$ is skew cyclic.
Reciprocally, assume that $\mathfrak{C}$ is a reversible DNA code of length n. Since λ_t is a unit, we can consider that $\mathfrak{g}$ is monic. Let $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_{t-1}y^{t-1} + y^t$. Furthermore, as $\mathfrak{g}$ divides $y^n - 1$, then λ_0 is a unit. We have

$$\mathfrak{g}^r(y) = y^{n-t-1} + \theta(\lambda_{t-1})y^{n-t} + \cdots + \theta(\lambda_1)y^{n-2} + \theta(\lambda_0)y^{n-1} \in \mathfrak{C}$$

and

$$y^{t+1}\mathfrak{g}^r(y) = 1 + \lambda_{t-1}y + \cdots + \lambda_1 y^{t-1} + \lambda_0 y^t \in \mathfrak{C}.$$

Then

$$\mathfrak{g}(y) - \lambda_0^{-1}x^{t+1}\mathfrak{g}^r(y) = (\lambda_0 - \lambda_0^{-1}) + (\lambda_1 - \lambda_0^{-1}\lambda_{t-1})y + \cdots + (\lambda_{t-1} - \lambda_0^{-1}\lambda_1)y^{t-1} \in \mathfrak{C}.$$

Since $\deg(\mathfrak{g})$ is minimal, we get $\mathfrak{g}(y) - \lambda_0^{-1}y^{t+1}\mathfrak{g}^r(y) = 0$. That is to say

$$(\lambda_0 - \lambda_0^{-1}) = (\lambda_1 - \lambda_0^{-1}\lambda_{t-1}) = \cdots = 0.$$

Therefore $\lambda_0 = 1,\ \lambda_j = \lambda_{t-j}$ for all $j \in \{0, 1, \cdots, t\}$. □

Theorem 4.2 *Let $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_{t-1}y^{t-1} + \lambda_t y^t$ be a right divisor of $y^n - 1$ in $\mathfrak{R}_4[y, \theta]$. Suppose that λ_t is a unit, n is even and t is odd. Then the skew cyclic code $\mathfrak{C} = \langle \mathfrak{g}(y) \rangle$ of length n is a reversible DNA code if and only if there exists a θ-palindromic polynomial $\mathfrak{h}$ such that $\mathfrak{C} = \langle \mathfrak{h}(y) \rangle$.*

Proof: Suppose that $\mathfrak{g}$ is a θ-palindromic polynomial. As λ_t is a unit, we can assume that $\mathfrak{g}$ is monic and $\mathfrak{g}(y) = 1 + \lambda_1 y + \cdots + \theta(\lambda_1)y^{t-1} + y^t$. For a codeword λ, we have $(\Psi(\lambda))^r = \Psi((\theta(\lambda))^r)$. Therefore

$$(\Psi(\sum_{j=0}^{l} \gamma_j x^j \mathfrak{g}(y)))^r = \Psi(\sum_{j=0}^{l} \theta(\gamma_j) x^{l-j} \mathfrak{g}(y)) \tag{4.2}$$

where $l = n - t - 1$ and $\lambda_j \in \mathfrak{R}_4$. We conclude by using the fact that $\mathfrak{C}$ is skew cyclic.
Reciprocally, assume that $\mathfrak{C}$ is a reversible DNA code of length n. Since λ_t is a unit, we can consider that $\mathfrak{g}$ is monic. Let $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_{t-1}y^{t-1} + y^t$. Furthermore, as $\mathfrak{g}$ divides $y^n - 1$, then λ_0 is a unit. We have

$$\mathfrak{g}^r(y) = y^{n-t-1} + \theta(\lambda_{t-1})y^{n-t} + \cdots + \theta(\lambda_1)y^{n-2} + \theta(\lambda_0)y^{n-1} \in \mathfrak{C}$$

and

$$y^{t+1}\mathfrak{g}^r(y) = 1 + \theta(\lambda_{t-1})y + \cdots + \theta(\lambda_1)y^{t-1} + \theta(\lambda_0)y^t \in \mathfrak{C}.$$

Then

$$\mathfrak{g}(y) - \theta(\lambda_0^{-1})y^{t+1}\mathfrak{g}^r(y) = (\lambda_0 - \theta(\lambda_0^{-1})) + (\lambda_1 - \theta(\lambda_0^{-1})\theta(\lambda_{t-1}))y + \cdots + (\lambda_{t-1} - \theta(\lambda_0^{-1})\theta(\lambda_1))y^{t-1} \in \mathfrak{C}.$$

Since $\deg(\mathfrak{g})$ is minimal, we get $\mathfrak{g}(y) - \theta(\lambda_0^{-1})y^{t+1}\mathfrak{g}^r(y) = 0$. That is to say

$$(\lambda_0 - \theta(\lambda_0^{-1})) = (\lambda_1 - \theta(\lambda_0^{-1})\theta(\lambda_{t-1})) = \cdots = 0.$$

Since $\lambda_0 = \theta(\lambda_0^{-1})$, we have $\lambda_0^2 = \theta(\lambda_0)$.
Then $\mathfrak{g}(y) = \sum_{j=0}^{\frac{t-1}{2}} (\lambda_j y^j + \lambda_0\theta(\lambda_j)y^{t-j})$ and $\lambda_0\mathfrak{g}(y) = \sum_{j=0}^{\frac{t-1}{2}} (\lambda_0\lambda_j y^j + \theta(\lambda_0 a_j)y^{t-j}) \in \mathfrak{C}$. The result follows by the fact that $\mathfrak{C} = \langle \mathfrak{g}(y) \rangle = \langle \lambda_0\mathfrak{g}(y) \rangle$. □

Theorem 4.3 *Let $\mathfrak{g}(y) = \eta_{i_0}g_0 + \eta_{i_1}g_1 + \eta_{i_2}g_2$ be a polynomial of degree t, where $g_0(y), g_1(y), g_2(y)$ are of the same degree t and divide $y^n - 1$ in $\mathbb{F}_4[y]$. Suppose n and t are even. Then the skew cyclic code $\mathfrak{C} = \langle \mathfrak{g}(y) \rangle$ of length n is a reversible DNA code if and only if $\mathfrak{g}(y)$ is a palindromic polynomial.*

Proof: Suppose that $\mathfrak{g}(y)$ is a palindromic polynomial, then $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_1 y^{t-1} + \lambda_0 y^t$. For a codeword λ, we have $(\Psi(\lambda))^r = \Psi((\theta(\lambda))^r)$. Therefore

$$(\Psi(\sum_{j=0}^{l} \gamma_j x^j \mathfrak{g}(y)))^r = \Psi(\sum_{j=0}^{l} \theta(\gamma_j) y^{l-j} \mathfrak{g}(y)),$$

where $l = n - t - 1$ and $\gamma_j \in \mathfrak{R}_4$. We conclude by using the fact that $\mathfrak{C}$ is skew cyclic.
Reciprocally, assume that $\mathfrak{C} = \langle \mathfrak{g}(y) \rangle$ is a reversible skew cyclic code of length n. Without loss of generality, suppose that $\mathfrak{g}(y) = \eta_0 g_0 + \eta_1 g_1 + \eta_2 g_2$. Since $g_0(y),\ g_1(y),\ g_2(y)$ divide $y^n - 1$ in $\mathbb{F}_4[y]$, we can assume that $\mathfrak{g} = \lambda_0 + \lambda_1 y + \cdots + \lambda_{t-1} y^{t-1} + \lambda_t y^t$, where $\lambda_0 = \eta_0 b_0 + \eta_1 b_1 + \eta_2 b_2;\ \lambda_t = \eta_0 a_0 + \eta_1 a_1 + \eta_2 a_2$ and $b_0, b_1, b_2, a_0, a_1, a_2$ are non zero elements of $\mathbb{F}_4$. We have

$$\mathfrak{g}^r(y) = \theta(\lambda_t) y^{n-t-1} + \theta(\lambda_{t-1}) y^{n-t} + \cdots + \theta(\lambda_1) y^{n-2} + \theta(\lambda_0) y^{n-1} \in \mathfrak{C}$$

and

$$y^{t+1} \mathfrak{g}^r(y) = \lambda_t + \lambda_{t-1} y + \cdots + \lambda_1 y^{t-1} + \lambda_0 y^t \in \mathfrak{C}.$$

Let $\tilde{\lambda}_0 = \eta_0 b_0^{-1} + \eta_1 b_1^{-1} + \eta_2 b_2^{-1}$ and $\tilde{\lambda}_t = \eta_0 a_0^{-1} + \eta_1 a_1^{-1} + \eta_2 a_2^{-1}$. We get

$$\tilde{\lambda}_t \mathfrak{g} - \tilde{\lambda}_0 y^{t+1} \mathfrak{g}^r(y) = (\tilde{\lambda}_t \lambda_0 - \tilde{\lambda}_0 \lambda_t) + (\tilde{\lambda}_t \lambda_1 - \tilde{\lambda}_0 \lambda_{t-1}) y + \cdots + (\tilde{\lambda}_t \lambda_{t-1} - \tilde{\lambda}_0 \lambda_1) y^{t-1} \in \mathfrak{C}.$$

According to the minimality of $\deg(\mathfrak{g})$, we obtain $\tilde{\lambda}_t \mathfrak{g} - \tilde{\lambda}_0 x^{t+1} \mathfrak{g}^r(y) = 0$. Therefore

$$(\tilde{\lambda}_t \lambda_0 - \tilde{\lambda}_0 \lambda_t) = (\tilde{\lambda}_t \lambda_1 - \tilde{\lambda}_0 \lambda_{t-1}) = \cdots = 0.$$

We have

$$\begin{aligned} \tilde{\lambda}_t \lambda_0 - \tilde{\lambda}_0 \lambda_t &= (\eta_0 a_0^{-1} b_0 + \eta_1 a_1^{-1} b_1 + \eta_2 a_2^{-1} b_2) - (\eta_0 a_0 b_0^{-1} + \eta_1 a_1 b_1^{-1} + \eta_2 a_2 b_2^{-1}) \\ &= \eta_0 (a_0^{-1} b_0 - a_0 b_0^{-1}) + \eta_1 (a_1^{-1} b_1 - a_1 b_1^{-1}) + \eta_2 (a_2^{-1} b_2 - a_2 b_2^{-1}). \end{aligned}$$

Then $\tilde{\lambda}_t \mathfrak{g} - \tilde{\lambda}_0 x^{t+1} \mathfrak{g}^r(y) = 0$ implies that $(a_0^{-1} b_0 - a_0 b_0^{-1}) = (a_1^{-1} b_1 - a_1 b_1^{-1}) = (a_2^{-1} b_2 - a_2 b_2^{-1}) = 0$. Then $a_i^2 = b_i^2$. Therefore $a_i = b_i,\ \forall\ i \in \{0, 1, 2\}$ and $\lambda_0 = \lambda_t$.
From Lemma 3.1, we deduce that $\lambda_j = \lambda_{t-j}$ for all $j \in \{0, 1, \cdots, t\}$. □

Theorem 4.4 *Let $\mathfrak{g}(y) = \eta_{i_0} g_0 + \eta_{i_1} g_1 + \eta_{i_2} g_2$ be a polynomial of degree t, where $g_0(y), g_1(y), g_2(y)$ are of the same degree t and divide $y^n - 1$ in $\mathbb{F}_4[y]$. If n is odd or (n is even and t is odd). Then the skew cyclic code $\mathfrak{C} = \langle \mathfrak{g}(y) \rangle$ of length n cannot be a reversible DNA code.*

Proof: Assume that $\mathfrak{g}(y) = \eta_0 g_0 + \eta_1 g_1 + \eta_2 g_2$. Since $g_0(y),\ g_1(y),\ g_2(y)$ divide $y^n - 1$ in $\mathbb{F}_4[y]$, we can assume that $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_{t-1} y^{t-1} + \lambda_t y^t$, where $\lambda_0 = \eta_0 b_0 + \eta_1 b_1 + \eta_2 b_2;\ \lambda_t = \eta_0 a_0 + \eta_1 a_1 + \eta_2 a_2$ and $b_0, b_1, b_2, a_0, a_1, a_2$ are non zero elements of $\mathbb{F}_4$. We have

$$\mathfrak{g}^r(y) = \theta(\lambda_t) y^{n-t-1} + \theta(\lambda_{t-1}) y^{n-t} + \cdots + \theta(\lambda_1) y^{n-2} + \theta(\lambda_0) y^{n-1} \in \mathfrak{C},$$

and

$$y^{t+1} \mathfrak{g}^r(y) = \theta(\lambda_t) + \theta(\lambda_{t-1}) y + \cdots + \theta(\lambda_1) y^{t-1} + \theta(\lambda_0) y^t \in \mathfrak{C}.$$

Therefore

$$\mathfrak{g}(y) + \eta_3 y^{t+1} g^r(y) = (\eta_0 a_0 + \eta_1 a_1 + \eta_2 a_2 + \eta_3 a_0) y^t + (\lambda_{t-1} + \eta_3 \theta(\lambda_1)) y^{t-1} + \cdots + (\lambda_0 + \eta_3 \theta(\lambda_t)) \in \mathfrak{C}.$$

Since a_0, a_1, a_2 are units in $\mathbb{F}_4$, then the leading coefficient of $\mathfrak{g}(y) + \eta_3 y^{t+1} \mathfrak{g}^r(y)$ is a unit, which is a contradiction. □

If $\lambda = (\lambda_0, \lambda_1, \cdots, \lambda_{n-1})$ is an element of a skew cyclic code of odd length n over $\mathfrak{R}_4$, then it is easy to see that $(\lambda_{n-1}, \lambda_0, \cdots, \lambda_{n-2})$ is also a codeword. Hence it is a cyclic code.

Theorem 4.5 *Assume that $\mathfrak{C}$ is generated by a right divisor $\mathfrak{g}$ of $y^n - 1$ in $\mathfrak{R}_4[y, \theta]$ and n is odd.*

(*a*) *Suppose that $\mathfrak{g}$ is palindromic or θ-palindromic. Then $\mathfrak{C}$ is a reversible DNA code.*

(*b*) *Suppose that $\mathfrak{C}$ is a reversible DNA code. Then there exists a monic polynomial $\mathfrak{h}(y) \in \mathfrak{R}_4[y]$ that is both palindromic and θ-palindromic such that $\mathfrak{C} = \langle \mathfrak{h}(y) \rangle$.*

Proof: We can assume that $\mathfrak{g}$ is monic. Let $\mathfrak{g}(y) = \lambda_0 + \lambda_1 y + \cdots + \lambda_{t-1}y^{t-1} + y^t$, where t is odd. Since the length of $\mathfrak{C}$ is odd, we get

$$\mathfrak{g}_\theta(y) := y^n \mathfrak{g}(y) = \theta(\lambda_0) + \theta(\lambda_1)y + \cdots + \theta(\lambda_{t-1})y^{t-1} + y^t \in \mathfrak{C}.$$

(a) Assume that $\mathfrak{g}$ is palindromic, then

$$(\Psi(\sum_{j=0}^{l} \gamma_j y^j \mathfrak{g}(y)))^r = \Psi(\sum_{j=0}^{l} \theta(\gamma_j) y^{l-j} \mathfrak{g}(y)),$$

where $l = n - t - 1$ and $\gamma_j \in \mathfrak{R}_4$.

Assume that $\mathfrak{g}$ is θ-palindromic, then

$$(\Psi(\sum_{j=0}^{l} \gamma_j x^j \mathfrak{g}(y)))^r = \Psi(\sum_{j=0}^{l} \theta(\gamma_j) x^{l-j} \mathfrak{g}_\theta(y)),$$

where $l = n - t - 1$ and $\gamma_j \in \mathfrak{R}_4$. Since $\mathfrak{C}$ is a skew cyclic code, the result follows.

(b) Now suppose that $\mathfrak{C}$ is a reversible DNA code. We have

$$\mathfrak{g}^r(y) = y^{n-t-1} + \theta(\lambda_{t-1})y^{n-t} + \cdots + \theta(\lambda_1)y^{n-2} + \theta(\lambda_0)y^{n-1} \in \mathfrak{C}$$

and

$$y^{t+1}\mathfrak{g}^r(y) = 1 + \theta(\lambda_{t-1})y + \cdots + \theta(\lambda_1)y^{t-1} + \theta(\lambda_0)y^t \in \mathfrak{C}.$$

From Theorem 4.2, we know that there exists a θ-palindromic polynomial $\mathfrak{h}(y) = \lambda_0\mathfrak{g}(y) = \beta_0 + \beta_1 y + \cdots + \theta(\beta_1)y^{t-1} + \theta(\beta_0)y^t \in \mathfrak{R}_4[y,\theta]$ such that $\mathfrak{C} = \langle \mathfrak{h}(y) \rangle$, where $\beta_0 = \lambda_0^2 = \theta(\lambda_0)$. As n is odd, we obtain

$$\mathfrak{h}_\theta(y) = \theta(\beta_0) + \theta(\beta_1)y + \cdots + \beta_1 y^{t-1} + \beta_0 y^t \in \mathfrak{C}.$$

Therefore, according to the minimality of $\deg(\mathfrak{h})$, we get

$$\theta(\beta_0^{-1})\mathfrak{h}(y) - \beta_0^{-1}\mathfrak{h}_\theta(y) = (\theta(\beta_0^{-1})\beta_0 - \beta_0^{-1}\theta(\beta_0)) + (\theta(\beta_0^{-1})\beta_1 - \beta_0^{-1}\theta(\beta_1))y + \cdots + (\theta(\beta_0^{-1})\theta(\beta_1) - \beta_0^{-1}\beta_1)y^{t-1} = 0.$$

Then

$$(\theta(\beta_0^{-1})\beta_0 - \beta_0^{-1}\theta(\beta_0)) = (\theta(\beta_0^{-1})\beta_1 - \beta_0^{-1}\theta(\beta_1)) = \cdots = (\theta(\beta_0^{-1})\theta(\beta_1) - \beta_0^{-1}\beta_1) = 0.$$

We deduce that $\theta(\beta_0^{-1})\beta_0 - \beta_0^{-1}\theta(\beta_0) = 0$, hence $\theta(\beta_0^{-1})\beta_0 = 1$. Therefore $\beta_0 = \theta(\beta_0)$. Since $\beta_0 = \lambda_0^2 = \theta(\lambda_0)$, we get $\beta_0 = 1$. It follows that $\beta_j = \theta(\beta_j)$ for all $j \in \{1, \cdots t\}$.

If t is even, the approach is similar to the case where t is odd. □

Recall that a standard DNA molecule is made up of two strands. For hybridization to occur, one strand must meet its corresponding reverse-complement strand. Therefore, it is important to characterize reversible-complement codes.

Proposition 4.1 *Assume that $\mathfrak{C}$ is generated by a right divisor $\mathfrak{g}$ of $y^n - 1$ in $\mathfrak{R}_4[y,\theta]$.*

(a) *Suppose that n and the degree of g are both even. Then $\mathfrak{C}$ is a reversible-complement DNA code if and only if $\mathfrak{g}$ is a palindromic polynomial and $1 + y + \cdots + y^{n-1} \in \mathfrak{C}$.*

(b) *Suppose that n is even and the degree of $\mathfrak{g}$ is odd. Then $\mathfrak{C}$ is a reversible-complement DNA code if and only if $\mathfrak{C}$ there exists a θ-palindromic polynomial $\mathfrak{h}$ such that $\mathfrak{C} = \langle \mathfrak{h}(y) \rangle$ and $1+y+\cdots+y^{n-1} \in \mathfrak{C}$.*

(c) *Suppose n is odd. Then $\mathfrak{C}$ is a reversible-complement DNA code if and only if there exists a monic polynomial $\mathfrak{h}(y) \in \mathfrak{R}_4[y]$ that is both palindromic and θ-palindromic such that $\mathfrak{C} = \langle \mathfrak{h}(y) \rangle$ and $1 + y + \cdots + y^{n-1} \in \mathfrak{C}$.*

Proof: Using the Watson-Crick complement and the correspondence Φ between $\mathfrak{R}_4$ and $\mathfrak{D}_4$, we easily find that $\beta+\overline{\beta}=1$, $\forall\,\beta\in\mathfrak{R}_4$. Let $\mathfrak{l}(y)=\beta_0+\beta_1 y+\cdots+\beta_{n-1}y^{n-1}\in\mathfrak{C}$, since $\mathfrak{C}$ is skew cyclic, it is a complement code if and only if $\mathfrak{l}(y)+\mathfrak{l}^c(y)=(\beta_0+\overline{\beta_0})+(\beta_1+\overline{\beta_1})y+\cdots+(\beta_{n-1}+\overline{\beta_{n-1}})y^{n-1}=1+y+\cdots+y^{n-1}\in\mathfrak{C}$. We conclude by considering Theorems 4.1, 4.2 and 4.5. □

Proposition 4.2 *Let $\mathfrak{g}(y)=\eta_{i_0}g_0+\eta_{i_1}g_1+\eta_{i_2}g_2\in R[y,\theta]$, where $g_0(y),g_1(y),g_2(y)$ are of the same degree and divide y^n-1 in $\mathbb{F}_4[y]$. Then $\mathfrak{C}=\langle\mathfrak{g}(y)\rangle$ cannot be a complement DNA code.*

Proof: Suppose $\mathfrak{C}$ is a complement code, then as in the above proof, we have $1+y+\cdots+y^{n-1}\in\mathfrak{C}$. Since $\mathfrak{C}=\langle\mathfrak{g}(y)\rangle$ cannot contain monic polynomials, the result follows. □

5. Conclusion

In this work, we explore the structure of skew cyclic codes over $\mathfrak{R}_4$ with respect to the automorphism θ defined on $\mathfrak{R}_4$ by $\theta(\lambda_0\eta_0+\lambda_1\eta_1+\lambda_2\eta_2+\lambda_3\eta_3)=\lambda_3\eta_0+\lambda_2\eta_1+\lambda_1\eta_2+\lambda_0\eta_3$. We establish a divisibility relation for particular polynomials in $\mathfrak{R}_4[y]$ and we derive generators polynomials of skew cyclic codes. This enables to characterize skew reversible DNA codes using palindromic and θ-palindromic polynomials.

References

1. T. Abualrub, N. Aydin, P. Seneviratne, *On θ-cyclic over $\mathbb{F}_2+v\mathbb{F}_2$*. Australas. J. Combin. 54, 115-126, (2012).
2. T. Abualrub, A. Ghrayeb, X. N. Zeng, *Construction of cyclic codes over $GF(4)$ for DNA computing*. J. Franklin Inst. 343, 448-457, (2006).
3. L. M. Adleman, *Molecular computation of solutions to combinatorial problems*. Science 266, 1021-1024, (1994).
4. D. Boneh, C. Dunworth, R. J. Lipton, *Breaking DES using a molecular computer*. In DNA Based Computer, eds. R. J. Lipton and E. B. Baum, Ser. Discr. Math. Theor. Comp. Sci. 27 (DIMACS Workshop, Princeton), 37-66, (1996).
5. A. Bayram, E. S. Oztas, I. Siap, *Codes over $\mathbb{F}_4+v\mathbb{F}_4$ and some DNA applications*. Des. Codes Cryptogr. 80, 379-393, (2016).
6. S. Bhardwaj, M. Raka, *Skew constacyclic codes over a non-chain ring over $\mathbb{F}_q[u,v]/\langle f(u),g(v),uv-vu\rangle$*. Appl. Algebra Engrg. Comm. Comput. 31, 173-194, (2020).
7. D. Boucher, W. Geiselmann, F. Ulmer, *Skew-cyclic codes*. Appl. Algebra Engrg. Comm. Comput. 18, 379-389, (2007).
8. Y. Cengellenmis, A. Dertli, *On the Skew cyclic codes and the reversibility problem for DNA 4-Bases*. Math. Comput. Sci. 14, 431-435, (2020).
9. A. G. D'yachkov, P. A. Vilenkin, I. K. Ismagilov, R. S. Sarbaev, A. Macula, D. Torney, and S. White, *On DNA Codes*. Probl. Inf. Transm. 41, 349-367, (2005).
10. K. Guenda, T. A. Gulliver, *Construction of cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ for DNA computing*. Appl. Algebra Engrg. Comm. Comput. 24, 445-459, (2013).
11. F. Gursoy, E. S. Oztas, I. Siap, *Reversible DNA codes using skew polynomial rings*. Appl. Algebra Engrg. Comm. Comput. 28, 311-320, (2017).
12. F. Gursoy, I. Siap, B. Yildiz, *Construction of skew cyclic codes over $\mathbb{F}_q+v\mathbb{F}_q$*. Adv. Math. Commun. 8, 313-322, (2014).
13. S. Jitman, S. Ling, P. Udomkavanich, *Skew Constacyclic codes over finite chain rings*. Adv. Math. Commun. 6, 39-63, (2012).
14. J. Kabore, A. Fotue-Tabue, K. Guenda, M. E. Charkani, *Skew constacyclic codes over $\frac{\mathbb{F}_q[v]}{\langle v^q-v\rangle}$*. Advances and Applications in Discrete Mathematics 25, 173-199, (2020).
15. J. Kabore, M. E. Charkani, *Construction of DNA codes using θ-skew cyclic codes over $\mathbb{F}_4+v\mathbb{F}_4$*. Advances and Applications in Discrete Mathematics 42, 737-755, (2025).
16. O. Prakash, A. Singh, R. K. Verma, P. Solé, W. Cheng, *DNA code from cyclic and skew cyclic codes over $\mathbb{F}_4[v]/\langle v^3\rangle$*. Entropy 25, 1-12, (2023).
17. I. Siap, T. Abualrub, N. Aydin, P. Seneviratne, *Skew cyclic codes of arbitrary length*. Int. J. Inf. Coding Theory 2, 10-20, (2011).

Joël Kabore,
Department of Mathematics,
Joseph Ki-Zerbo University,
Burkina-Faso.
E-mail address: jokabore@yahoo.fr

and

Mohammed Elhassani Charkani,
Department of Mathematics,
Faculty of Sciences Dhar EL Mahraz,
Sidi Mohamed Ben Abdellah University,
Morocco.
E-mail address: mcharkani@gmail.com