Skew cyclic codes over F_4R

Benbelkacem, Nasreddin; Ezerman, Martians Frederic; Abualrub, Taher; Aydin, Nuh;
Batoul, Aicha

2020

Benbelkacem, N., Ezerman, M. F., Abualrub, T., Aydin, N., & Batoul, A. (2020). Skew cyclic codes over F_4R . Journal of Algebra and its Applications, 2250065-.
doi:10.1142/S0219498822500657

<https://hdl.handle.net/10356/146375>

<https://doi.org/10.1142/S0219498822500657>

Electronic version of an article published as Journal of Algebra and its Applications, 2250065-. <https://doi.org/10.1142/S0219498822500657> @ copyright World Scientific Publishing Company [<https://www.worldscientific.com/worldscinet/jaa>].

Downloaded on 26 Apr 2023 18:24:44 SGT

SKEW CYCLIC CODES OVER $\mathbb{F}_4R$

NASREDDINE BENBELKACEM

*Faculty of Mathematics, University of Science and Technology Houari Boumediene
BP 32 El Alia, Bab Ezzouar, 16111 Algiers, Algeria
benbelkacem213@gmail.com*

MARTIANUS FREDERIC EZERMAN

*School of Physical and Mathematical Sciences, Nanyang Technological University
21 Nanyang Link, Singapore 637371
fredezerman@ntu.edu.sg*

TAHER ABUALRUB

*Department of Mathematics and Statistics, College of Arts and Sciences,
American University of Sharjah, P.O. Box 26666 Sharjah, United Arab Emirates
abualrub@aus.edu*

NUH AYDIN

*Department of Mathematics and Statistics,
Kenyon College, Gambier, Ohio OH 43022, United States of America
aydinn@kenyon.edu*

AICHA BATOUL

*Faculty of Mathematics, University of Science and Technology Houari Boumediene
BP 32 El Alia, Bab Ezzouar, 16111 Algiers, Algeria
a.batoul@hotmail.fr*

Received (Day Month Year)

Revised (Day Month Year)

Accepted (Day Month Year)

Communicated by (xxxxxxxxx)

This paper considers a new alphabet set, which is a ring that we call $\mathbb{F}_4R$, to construct linear error-control codes. Skew cyclic codes over this ring are then investigated in details. We define a nondegenerate inner product and provide a criteria to test for self-orthogonality. Results on the algebraic structures lead us to characterize $\mathbb{F}_4R$ -skew cyclic codes. Interesting connections between the image of such codes under the Gray map to linear cyclic and skew-cyclic codes over $\mathbb{F}_4$ are shown. These allow us to learn about the relative dimension and distance profile of the resulting codes. Our setup provides a natural connection to DNA codes where additional biomolecular constraints must be incorporated into the design. We present a characterization of R -skew cyclic codes which are reversible complement.

Keywords: Linear codes; Skew cyclic codes; Mixed alphabets

1. Introduction

The use of noncommutative rings to construct error control codes has recently been an active research area, initiated by the seminal works of Boucher *et al.* in [7] and [8] as well as that of Abualrub *et al.* in [2]. In the first two, Boucher and collaborators generalized the notion of cyclic codes by using generator polynomials in a noncommutative polynomial ring called the skew polynomial ring. They supplied examples of skew cyclic codes with Hamming distances larger than previously best-known linear codes of the same length and dimension. In [2], Abualrub *et al.* generalized the concept of skew cyclic codes to skew quasi-cyclic codes. They then constructed several new codes with Hamming distances exceeding the Hamming distances of the previously best-known linear codes with comparable parameters.

Another emerging topic in the studies of error correcting codes is additive codes over mixed alphabets. Borges *et al.* introduced the class of $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes in [6]. This class generalizes binary and quaternary linear codes. A $\mathbb{Z}_2\mathbb{Z}_4$ -additive code is defined to be a subgroup of $\mathbb{Z}_2^s\mathbb{Z}_4^s$. Abualrub *et al.* studied the structure of $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes in [4]. They determined the generator polynomials and the minimal generating sets for these codes. Despite the fact that $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes constitute a new type of codes that emerged only in the last decade, they have been shown to have some applications, *e.g.*, in steganography [14]. Codes over the mixed alphabet $\mathbb{Z}_2\mathbb{Z}_3$, with applications in *football pool problem*, were constructed by Abualrub and Aydin in [1].

In this paper, we merge the topic of skew cyclic codes with that of codes over mixed alphabets. In particular, we study the structure of linear skew cyclic codes over the ring $\mathbb{F}_4R$, where $\mathbb{F}_4 := \{0, 1, w, w^2 = w + 1\}$ is the field of four elements and $R = \{a + vb \mid a, b \text{ in } \mathbb{F}_4\}$ is the commutative ring with 16 elements where $v^2 = v$.

It is well-known that R is a finite non-chain ring with two maximal ideals $\langle v \rangle$ and $\langle v + 1 \rangle$, making $R/\langle v \rangle$ and $R/\langle v + 1 \rangle$ isomorphic to $\mathbb{F}_4$. The Chinese Remainder Theorem then implies that $R = \langle v \rangle \times \langle v + 1 \rangle$. As was shown in [5], R can be uniquely expressed as $\{a + vb = (b + a)v + a(v + 1) \mid a, b \in \mathbb{F}_4\}$. Any codeword $\mathbf{c}$ in a skew cyclic code C over $\mathbb{F}_4R$ has the form $\mathbf{c} = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{F}_4^\alpha R^\beta$.

Initially, the length n of skew cyclic code over a field $\mathbb{F}_q$ was restricted to be a multiple of the order of the ring (field) automorphism θ because in this case the ideal $\langle X^n - 1 \rangle$ is a two-sided ideal of the skew polynomial ring $\mathbb{F}_q[X, \theta]$ and we obtain a ring structure on the quotient space. Moreover, skew cyclic codes are ideals of $\mathbb{F}_q[X]/\langle X^n - 1 \rangle$ in this case. Later, it was shown in [15] that the restriction on length can be lifted if skew cyclic codes are viewed as $\mathbb{F}_q[X, \theta]$ -modules rather than ideals. This applies to the case when the alphabet is a ring as well. We take this approach in this work.

Definition 1.1. Let S be any commutative ring and let θ be an automorphism of S . The skew polynomial ring $S[X, \theta]$ is defined by

$$S[X, \theta] = \{a_0 + a_1X + a_2X^2 + \dots + a_nX^n : a_i \in S \text{ for all } i = 0, 1, \dots, n\},$$

where addition of these polynomials is defined in the usual way while multiplication is defined using the distributive law and the rule

$$(aX^i) \cdot (bX^j) = a\theta^i(b)X^{i+j}$$

The ring $S[X, \theta]$ is not commutative even when S is. Therefore, when we talk about divisibility, we need to specify left or right divisibility, and when we discuss ideals we need to talk about left, right, or two-sided ideals. For example, we say that $f(X)$ is a left divisor of $g(X)$ in $S[X, \theta]$ if there exists $h(X) \in S[X, \theta]$ such that $g(X) = f(X) \cdot h(X)$ with skew multiplication of polynomials. Note that, given a ring S , the notation $S[X, \theta]/\langle X^\beta - 1 \rangle$ does not automatically imply that a quotient ring structure is defined. It denotes the quotient space, that is, the set of cosets of the additive group $\langle X^\beta - 1 \rangle$.

The following are our contributions.

- (1) We show that skew cyclic codes over $\mathbb{F}_4R$ are left $R[X, \theta]$ -submodules of $R_{\alpha, \beta} := \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle \times R[X, \theta]/\langle X^\beta - 1 \rangle$, and the dual of a skew cyclic code over $\mathbb{F}_4R$ for any even β is also a skew cyclic code.
- (2) We determine their generator polynomials and establish interesting results that relate these codes to cyclic and quasi-cyclic (QC) codes over $\mathbb{F}_4R$. First, we show that a skew cyclic code over $\mathbb{F}_4R$ is equivalent to an $\mathbb{F}_4R$ -cyclic code if α and β are both odd integers. Second, we establish that if α and β are both even integers, then an $\mathbb{F}_4R$ -skew cyclic code C is equivalent to an $\mathbb{F}_4R$ quasi-cyclic code of index 2.
- (3) Conditions for skew cyclic codes over $\mathbb{F}_4R$ to be self-orthogonal are studied.
- (4) We use the Gray mapping to associate these codes to codes over $\mathbb{F}_4$ of length $\alpha + 2\beta$ and exhibit a nice relationship between these codes and their images over $\mathbb{F}_4$. The Gray image of any skew cyclic code over $\mathbb{F}_4R$ is the product of a cyclic code over $\mathbb{F}_4$ of length α and two skew cyclic codes, each of length β , over $\mathbb{F}_4$. We supply examples of good skew cyclic codes over $\mathbb{F}_4R$ and their respective Gray images for different lengths.
- (5) We construct optimal linear codes over $\mathbb{F}_4$ as images of skew cyclic codes over $\mathbb{F}_4R$ under the Gray mapping.
- (6) Applications of these codes to DNA computing are included in our treatment.

2. Preliminaries

Let $A \oplus B = \{a + b \mid a \in A, b \in B\}$ and $A \otimes B = \{(a, b) \mid a \in A, b \in B\}$ as defined in [16]. An $\mathbb{F}_4$ -linear code of length n is a subspace of $\mathbb{F}_4^n$. A subset C of R^n is a

linear code over R if C is an R -submodule. Given a linear code C over R , let

$$\begin{aligned} C_1 &:= \{\mathbf{x} + \mathbf{y} \in \mathbb{F}_4^n \mid (\mathbf{x} + \mathbf{y})v + \mathbf{x}(v+1) \in C \text{ for some } \mathbf{x}, \mathbf{y} \in \mathbb{F}_4^n\} \text{ and} \\ C_2 &:= \{\mathbf{x} \in \mathbb{F}_4^n \mid (\mathbf{x} + \mathbf{y})v + \mathbf{x}(v+1) \in C \text{ for some } \mathbf{y} \in \mathbb{F}_4^n\}. \end{aligned}$$

One can quickly verify that C_1 and C_2 are linear codes over $\mathbb{F}_4$. In fact, any linear code C over R can be expressed as $C = vC_1 \oplus (v+1)C_2$. Let $r = a + vb \in R$ and $\mathbf{c} = (c_1, c_2, \dots, c_n) \in C$, i.e., $c_j = a_j + vb_j$ with $a_j, b_j \in \mathbb{F}_4$ for $1 \leq j \leq n$. The j -th entry of $r\mathbf{c}$ is

$$\begin{aligned} (a + vb)(a_j + vb_j) &= ((a + b)v + a(v+1))(a_j + vb_j) \\ &= \underbrace{aa_j}_x + v(\underbrace{ab_j + ba_j + bb_j}_y) = (x + y)v + x(v+1). \end{aligned}$$

Hence, $r\mathbf{c}$ can be written in terms of C_1 and C_2 with

$$\mathbf{x} = a(a_1, a_2, \dots, a_n) \text{ and } \mathbf{y} = (a + b)(b_1, b_2, \dots, b_n) + b(a_1, a_2, \dots, a_n).$$

Definition 2.1. Let an automorphism θ over R be defined by

$$\theta : R \mapsto R \text{ sending } a + vb \mapsto a^2 + (v+1)b^2. \quad (2.1)$$

Restricted to $\mathbb{F}_4$, it interchanges w and w^2 while keeping $\{0, 1\}$ fixed. Note that our θ here is equal to the composition of automorphisms $\varphi \circ \theta_1$ in [11]. A subset C of R^n is said to be an R -skew cyclic code of length n if two conditions are satisfied.

- (1) C is an R -submodule of R^n .
- (2) If $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C$ then the skew cyclic shift of $\mathbf{c}$ over R , denoted by $T_\theta(\mathbf{c}) := (\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2}))$, is also in C .

It is often convenient to associate a vector $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ with a polynomial $a(X) := a_0 + a_1X + \dots + a_{n-1}X^{n-1}$ in an indeterminate X . This allows for constructions of codes using results from the algebra of polynomial rings.

The next two theorems can be inferred by a slight modification on the corresponding theorems in [11], with q restricted to 4. The respective proof is therefore omitted for brevity.

Theorem 2.1. (From [11, Theorem 3]) Let $C = vC_1 \oplus (v+1)C_2$ be an R -linear code. Then C is an R -skew cyclic code if and only if C_1 and C_2 are skew cyclic codes over $\mathbb{F}_4$.

Theorem 2.2. (From [11, Theorem 5]) Let $C = vC_1 \oplus (v+1)C_2$ be an R -skew cyclic code of length n . Let $g_1(X)$ and $g_2(X)$ be the respective generator polynomials of C_1 and C_2 as $\mathbb{F}_4$ -skew cyclic codes. Then $C = \langle vg_1(X) + (v+1)g_2(X) \rangle$.

For any element in R , we introduce a new ring homomorphism

$$\eta : R \mapsto \mathbb{F}_4 \text{ sending } a + vb \text{ to } a. \quad (2.2)$$

Let $\mathbb{F}_4 R := \{(a, b) \mid a \in \mathbb{F}_4 \text{ and } b \in R\}$. It is straightforward to verify that $\mathbb{F}_4 R$ is an R -module under the multiplication

$$d * (a, b) = (\eta(d)a, db) \text{ with } d \in R \text{ and } (a, b) \in \mathbb{F}_4 R. \quad (2.3)$$

This extends naturally to $\mathbb{F}_4^\alpha R^\beta$. Let $\mathbf{x} = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{F}_4^\alpha R^\beta$, for α and $\beta \in \mathbb{N}$, and $d \in R$. Then

$$d * \mathbf{x} = (\eta(d)a_0, \eta(d)a_1, \dots, \eta(d)a_{\alpha-1}, db_0, db_1, \dots, db_{\beta-1}). \quad (2.4)$$

Definition 2.2. A nonempty subset C of $\mathbb{F}_4^\alpha R^\beta$ is called an $\mathbb{F}_4 R$ -linear code if it is an R -submodule of $\mathbb{F}_4^\alpha R^\beta$ with respect to the scalar multiplication in Equation (2.4).

A nondegenerate *inner product* between $\mathbf{x} = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1})$ and $\mathbf{y} = (d_0, d_1, \dots, d_{\alpha-1}, e_0, e_1, \dots, e_{\beta-1})$ in $\mathbb{F}_4^\alpha R^\beta$ is given by

$$\langle \mathbf{x}, \mathbf{y} \rangle = v \sum_{i=0}^{\alpha-1} a_i d_i + \sum_{j=0}^{\beta-1} b_j e_j \in R. \quad (2.5)$$

Note that if $\alpha = 0$, then the inner product is well-defined for elements $\mathbf{x}, \mathbf{y} \in R^\beta$. The dual code of an $\mathbb{F}_4 R$ -linear code C , denoted by $C^\perp$, is also $\mathbb{F}_4 R$ -linear and is defined in the usual way as

$$C^\perp := \{\mathbf{y} \in \mathbb{F}_4^\alpha R^\beta \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in C\}.$$

Let

$$\begin{aligned} a(X) &= a_0 + a_1 X + \dots + a_{\alpha-1} X^{\alpha-1} \in \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle \text{ and} \\ b(X) &= b_0 + b_1 X + \dots + b_{\beta-1} X^{\beta-1} \in R[X, \theta]/\langle X^\beta - 1 \rangle. \end{aligned}$$

Then any codeword $\mathbf{c} = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{F}_4^\alpha R^\beta$ can be identified with a module element consisting of two polynomials such that

$$c(X) = (a(X), b(X)). \quad (2.6)$$

This identification gives a one-to-one correspondence between $\mathbb{F}_4^\alpha R^\beta$ and

$$R_{\alpha, \beta} := \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle \times R[X, \theta]/\langle X^\beta - 1 \rangle. \quad (2.7)$$

The product of $r(X) = r_0 + r_1 X + \dots + r_t X^t \in R[X, \theta]$ and $(a(X), b(X)) \in R_{\alpha, \beta}$ is

$$r(X) * (a(X), b(X)) = (\eta(r(X))a(X), r(X)b(X)), \quad (2.8)$$

where $\eta(r(X)) = \eta(r_0) + \eta(r_1)X + \dots + \eta(r_t)X^t \in \mathbb{F}_4[X]$. Here, $\eta(r(X))a(X)$ is the usual polynomial multiplication in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ while $r(X)b(X)$ is the polynomial multiplication in $R[X, \theta]/\langle X^\beta - 1 \rangle$ where $X(a + vb) = (a^2 + (v+1)b^2)X$.

Theorem 2.3. $R_{\alpha, \beta}$ is a left $R[X, \theta]$ -module with respect to $*$ in Equation (2.8).

Proof. Verifying that the required properties are satisfied over $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ is easy since we do not have to deal with skewness. Verifying over $R[X, \theta]/\langle X^\beta - 1 \rangle$ is routine, albeit tedious. It suffices to use the fact that θ is a homomorphism with $\theta^{-1} = \theta$. $\square$

3. Generator Polynomials of $\mathbb{F}_4R$ -Skew Cyclic Codes

This section begins with a formal definition of an $\mathbb{F}_4R$ -skew cyclic code and, then, proposes a method to determine a generator polynomial of any $\mathbb{F}_4R$ -skew cyclic code C in $R_{\alpha,\beta}$. We use a general notion of equivalence to say that two codes are *equivalent* if one can be obtained from the other by a combination of the following operations: (a) some composition of a permutation of the first α positions, a permutation of the last β positions, (b) multiplication of the scalars appearing in a chosen position by a unit, and (c) applying a ring (or field) automorphism to elements in a chosen position.

Definition 3.1. An $\mathbb{F}_4R$ -linear code C of length $n = \alpha + \beta$ is said to be $\mathbb{F}_4R$ -skew cyclic if, for any codeword $\mathbf{c} = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in C$, its skew cyclic shift $T_\theta(\mathbf{c}) := (a_{\alpha-1}, a_0, \dots, a_{\alpha-2}, \theta(b_{\beta-1}), \theta(b_0), \dots, \theta(b_{\beta-2}))$ is also in C .

Theorem 3.1. Let C be an $\mathbb{F}_4R$ -skew cyclic code of length $n = \alpha + \beta$ such that β is an even integer. Then $C^\perp$ is also an $\mathbb{F}_4R$ -skew cyclic code of the same length.

Proof. It suffices to show that, for any $\mathbf{x} = (a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1}) \in C^\perp$, we have $T_\theta(\mathbf{x}) \in C^\perp$. Let $\mathbf{y} = (d_0, d_1, \dots, d_{\alpha-1}, e_0, e_1, \dots, e_{\beta-1})$ be any codeword in C . Then we write $\langle T_\theta(\mathbf{x}), \mathbf{y} \rangle$ as

$$\begin{aligned} & \langle (a_{\alpha-1}, a_0, \dots, a_{\alpha-2}, \theta(b_{\beta-1}), \theta(b_0), \dots, \theta(b_{\beta-2})), (d_0, d_1, \dots, d_{\alpha-1}, e_0, e_1, \dots, e_{\beta-1}) \rangle \\ &= v(a_{\alpha-1}d_0 + a_0d_1 + \dots + a_{\alpha-2}d_{\alpha-1}) + (\theta(b_{\beta-1})e_0 + \theta(b_0)e_1 + \dots + \theta(b_{\beta-2})e_{\beta-1}). \end{aligned}$$

Hence, one only needs to show that

$$a_{\alpha-1}d_0 + a_0d_1 + \dots + a_{\alpha-2}d_{\alpha-1} = 0 \text{ and } \theta(b_{\beta-1})e_0 + \theta(b_0)e_1 + \dots + \theta(b_{\beta-2})e_{\beta-1} = 0.$$

Now, let $\gamma := \text{lcm}(\alpha, \beta)$. Then γ is an even integer since β is an even integer. Since C is $\mathbb{F}_4R$ -skew cyclic, for any $\mathbf{y} \in C$ we have $T_\theta^\gamma(\mathbf{y}) = \mathbf{y}$ and $T_\theta^{\gamma-1}(\mathbf{y}) \in C$. Hence, $\langle \mathbf{x}, T_\theta^{\gamma-1}(\mathbf{y}) \rangle = 0$. Since $T_\theta^{\gamma-1}(\mathbf{y}) = (d_1, \dots, d_{\alpha-1}, d_0, \theta(e_1), \dots, \theta(e_{\beta-1}), \theta(e_0))$, we then obtain

$$v \sum_{j=0}^{\alpha-1} a_j d_{(j+1) \pmod{\alpha}} + \sum_{j=0}^{\beta-1} b_j \theta(e_{(j+1) \pmod{\beta}}) = 0.$$

This implies

$$\begin{aligned} 0 &= a_{\alpha-1}d_0 + a_0d_1 + a_1d_2 + \dots + a_{\alpha-2}d_{\alpha-1} \text{ and} \\ 0 &= b_{\beta-1}\theta(e_0) + b_0\theta(e_1) + b_1\theta(e_2) + \dots + b_{\beta-2}\theta(e_{\beta-1}). \end{aligned}$$

Applying θ to both sides of the last equation yields

$$\theta(0) = \theta(b_{\beta-1})e_0 + \theta(b_0)e_1 + \theta(b_1)e_2 + \dots + \theta(b_{\beta-2})e_{\beta-1} = 0,$$

completing the proof. $\square$

Theorem 3.2. A code C is $\mathbb{F}_4R$ -skew cyclic if and only if C is a left $R[X, \theta]$ -submodule of $R_{\alpha,\beta}$ under the multiplication $*$.

Proof. Let $c(X) = (a(X), b(X))$ be any codeword of an $\mathbb{F}_4 R$ -skew cyclic code C . Hence, $(a_0, a_1, \dots, a_{\alpha-1}, b_0, b_1, \dots, b_{\beta-1})$ and all of its T_θ -skew cyclic shifts are in C . We associate, for each $j \in \mathbb{N}$, the polynomial

$$X^j * c(X) = (a_{\alpha-j} + a_{\alpha-j+1}X + \dots + a_{\alpha-j-1}X^{\alpha-1}, \\ \theta^j(b_{\beta-j}) + \theta^j(b_{\beta-j+1})X + \dots + \theta^j(b_{\beta-j-1})X^{\beta-1})$$

with the vector

$$(a_{\alpha-j}, a_{\alpha-j+1}, \dots, a_{\alpha-j-1}, \theta^j(b_{\beta-j}), \theta^j(b_{\beta-j+1}), \dots, \theta^j(b_{\beta-j-1})).$$

The indices of the first block (of length α) are taken modulo α and those of the second block (of length β) are taken modulo β . By the $\mathbb{F}_4 R$ -linearity of C , we have $r(X) * c(X) \in C$ for any $r(X) \in R[X, \theta]$. Thus, C is a left $R[X, \theta]$ -submodule of $R_{\alpha, \beta}$.

Conversely, let C be a left $R[X, \theta]$ -submodule of the left $R[X, \theta]$ -module $R_{\alpha, \beta}$. Then, for any $c(X) \in C$, we have $X^j * c(X) \in C$ for any $j \in \mathbb{N}$. Thus, C is indeed an $\mathbb{F}_4 R$ -skew cyclic code. $\square$

Let C be an $\mathbb{F}_4 R$ -skew cyclic code. Let $c(X) = (a(X), b(X))$ be an element in C . Let $\ell(X)$ be an element in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$. We use $\mathbf{0}$ to denote either the zero vector $(0, 0, \dots, 0)$ or the zero polynomial. Let

$$I := \{b(X) \in R[X, \theta]/\langle X^\beta - 1 \rangle \mid (\ell(X), b(X)) \in C, \exists \ell(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle\} \text{ and} \\ J := \{a(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle \mid (a(X), \mathbf{0}) \in C\}.$$

The following results establish useful properties of the sets I and J

Lemma 3.1. J is an ideal in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ generated by a divisor of $X^\alpha - 1$.

Proof. If $a_1(X)$ and $a_2(X)$ are in J , then $(a_1(X), \mathbf{0})$ and $(a_2(X), \mathbf{0})$ are in C by definition. Hence, $(a_1(X), \mathbf{0}) + (a_2(X), \mathbf{0}) = (a_1(X) + a_2(X), \mathbf{0}) \in C$, ensuring that $a_1(X) + a_2(X) \in J$. Let $s(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ and $a(X) \in J$. Then $(a(X), \mathbf{0})$ is in C . Because C is a left $R[X, \theta]$ -module, we have

$$s(X) * (a(X), \mathbf{0}) = (s(X)a(X), \mathbf{0}) \in C \implies s(X)a(X) \text{ modulo } (X^\alpha - 1) \in J.$$

Thus, J is an ideal in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ generated by a divisor $f(X)$ of $X^\alpha - 1$. $\square$

Lemma 3.2. I is a principally generated left $R[X, \theta]$ -submodule of $R[X, \theta]/\langle X^\beta - 1 \rangle$.

Proof. Let $b_1(X)$ and $b_2(X)$ be elements in I . Then there exist polynomials $\ell_1(X)$ and $\ell_2(X)$ in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ such that $(\ell_1(X), b_1(X)), (\ell_2(X), b_2(X)) \in C$. Hence,

$$(\ell_1(X), b_1(X)) + (\ell_2(X), b_2(X)) = (\ell_1(X) + \ell_2(X), b_1(X) + b_2(X)) \in C,$$

implying $b_1(X) + b_2(X) \in I$. Let $r(X) \in R[X, \theta]/\langle X^\beta - 1 \rangle$ and $(\ell(X), b(X)) \in C$. Since C is a left $R[X, \theta]$ -submodule of $R_{\alpha, \beta}$, we have

$$r(X) * (\ell(X), b(X)) = (\eta(r(X))\ell(X) \text{ modulo } (X^\alpha - 1), r(X)b(X) \text{ modulo } (X^\beta - 1))$$

in C , making $r(X)b(X) \text{ modulo } (X^\beta - 1) \in I$. Thus, I is a left submodule in $R[X, \theta]/\langle X^\beta - 1 \rangle$ and, by Theorem 2.2, $I = \langle g(X) \rangle$ where

$$g(X) := vg_1(X) + (v+1)g_2(X). \quad (3.1)$$

Our proof is now complete. $\square$

The following result classifies all $\mathbb{F}_4R$ -skew cyclic codes.

Theorem 3.3. *Let $g(X)$ be as defined in Equation (3.1). Let C be an $\mathbb{F}_4R$ -skew cyclic code. Then C is generated as a left submodule of $R_{\alpha, \beta}$ by $(f(X), \mathbf{0})$ and $(\ell(X), g(X))$, where $\ell(X)$ is an element in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ and $f(X)$ divides $X^\alpha - 1$.*

Proof. Let $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$ with $\mathbf{c}_1 \in \mathbb{F}_4^\alpha$ and $\mathbf{c}_2 \in R^\beta$. Then $c_2(X) \in I$ and we write $c_2(X) = q(X)g(X)$ for some $q(X) \in R[X, \theta]/\langle X^\beta - 1 \rangle$. There exists $\ell(X) \in \mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ such that $(\ell(X), g(X)) \in C$, since $g(X) \in I$. We have

$$\begin{aligned} \mathbf{c} &= (\mathbf{c}_1, \mathbf{c}_2) = (c_1(X), \mathbf{0}) + (\mathbf{0}, q(X)g(X)) \\ &= (c_1(X), \mathbf{0}) + (\eta(q(X))\ell(X), q(X)g(X)) + (\eta(q(X))\ell(X), \mathbf{0}) \\ &= (c_1(X), \mathbf{0}) + q(X) * ((\ell(X), g(X)) + (\ell(X), \mathbf{0})). \end{aligned}$$

Hence, $(\eta(q(X))\ell(X) + c_1(X), \mathbf{0}) \in C$, making $\eta(q(X))\ell(X) + c_1(X) \in J$. By Lemma 3.1, there exists $p(X) \in J$ satisfying $\eta(q(X))\ell(X) + c_1(X) = p(X)f(X)$. Thus, $c(X) = q(X) * (\ell(X), g(X)) + (p(X)f(X), \mathbf{0})$. $\square$

Lemma 3.3. *Let C be an $\mathbb{F}_4R$ -skew cyclic code. Then, without loss of generality, we can assume $\deg(\ell(X)) < \deg(f(X))$, where $f(X)$ is the divisor of $X^\alpha - 1$ as in Theorem 3.3.*

Proof. Suppose that $\deg(\ell(X)) - \deg(f(X)) = k \geq 0$. Consider the code D generated by $\{(f(X), \mathbf{0}), (\ell(X), g(X)) + sX^k * (f(X), \mathbf{0})\} = \{(f(X), \mathbf{0}), (\ell_1(X), g(X))\}$, where $\ell_1(X) = \ell(X) + sX^k f(X)$ for some $s \in \mathbb{F}_4$. Hence, $D \subseteq C$. On the other hand, $(\ell(X), g(X)) = (\ell(X), g(X)) + sX^k * (f(X), \mathbf{0}) - sX^k * (f(X), \mathbf{0})$. Hence, $C \subseteq D$, making $C = D$. Notice here that $\deg(\ell_1(X)) < \deg(\ell(X))$. We repeat the same process on $\ell_1(X)$ until we obtain $\deg(\ell(X)) < \deg(f(X))$. $\square$

Theorem 3.4. *An $\mathbb{F}_4R$ -skew cyclic code is equivalent to an $\mathbb{F}_4R$ -cyclic code if both α and β are odd integers.*

Proof. Let C be an $\mathbb{F}_4R$ -skew cyclic code and $\gamma := \text{lcm}(\alpha, \beta)$. Then $\gcd(\gamma, 2) = 1$ since γ is odd. Then there exist integers k and j such that $\gamma k + 2j = 1$. Hence,

$2j = 1 - \gamma k = 1 + \gamma t$, for some $t > 0$ where $t \equiv -k \pmod{\gamma}$. As in Equation (2.6), let $c(X) = (a(X), b(X)) \in C$. Then

$$\begin{aligned} X^{2j} * c(X) &= X^{2j} * \left(\sum_{i=0}^{\alpha-1} a_i X^i, \sum_{i=0}^{\beta-1} b_i X^i \right) = \left(\sum_{i=0}^{\alpha-1} a_i X^{i+2j}, \sum_{i=0}^{\beta-1} \theta^{2j}(b_i) X^{i+2j} \right) \\ &= \left(\sum_{i=0}^{\alpha-1} a_i X^{i+1+\gamma t}, \sum_{i=0}^{\beta-1} \theta^{2j}(b_i) X^{i+1+\gamma t} \right) \\ &= \left(\sum_{i=0}^{\alpha-2} a_i X^{i+1+\gamma t} + a_{\alpha-1} X^{\alpha+\gamma t}, \sum_{i=0}^{\beta-2} b_i X^{i+1+\gamma t} + b_{\beta-1} X^{\beta+\gamma t} \right) \\ &= \left(\sum_{i=0}^{\alpha-2} a_i X^{i+1} + a_{\alpha-1}, \sum_{i=0}^{\beta-2} b_i X^{i+1} + b_{\beta-1} \right) \in C. \end{aligned}$$

The second to the last equation is due to $\theta^2(r) = r$ for all $r \in R$, while the last equation follows because $X^\alpha = X^\beta = X^\gamma = 1$. This shows that $X^{2j} * c(X)$ is the cyclic shift of $c(X)$ over $\mathbb{F}_4 R$. Thus, C is cyclic. $\square$

Theorem 3.5. *An $\mathbb{F}_4 R$ -skew cyclic code is equivalent to an $\mathbb{F}_4 R$ -quasi-cyclic code of index 2 if both α and β are even integers.*

Proof. Let C be an $\mathbb{F}_4 R$ -skew cyclic code, $\alpha = 2N$, and $\beta = 2M$ for some $N, M \in \mathbb{N}$. Then $\gamma = \text{lcm}(\alpha, \beta)$ is an even integer with $\text{gcd}(\gamma, 2) = 2$. For any

$$\mathbf{c} = (a_{0,0}, a_{0,1}, \dots, a_{N-1,0}, a_{N-1,1}, b_{0,0}, b_{0,1}, \dots, b_{M-1,0}, b_{M-1,1}) \in C$$

there exist integers $k \geq 0$ and j such that $2j = 2 + k\gamma$. Consider

$$\begin{aligned} T_{\theta^{2+k\gamma}}(a_{0,0}, a_{0,1}, \dots, a_{N-1,0}, a_{N-1,1}, b_{0,0}, b_{0,1}, \dots, b_{M-1,0}, b_{M-1,1}) &= \\ T_{\theta^{k\gamma}}(a_{N-1,0}, a_{N-1,1}, \dots, a_{N-2,0}, a_{N-2,1}, b_{M-1,0}, b_{M-1,1}, \dots, b_{M-2,0}, b_{M-2,1}) &= \\ (a_{N-1,0}, a_{N-1,1}, \dots, a_{N-2,0}, a_{N-2,1}, b_{M-1,0}, b_{M-1,1}, \dots, b_{M-2,0}, b_{M-2,1}) &\in C, \end{aligned}$$

since $T_{\theta^{k\gamma}}(\mathbf{c}) = \mathbf{c}$ for any $\mathbf{c} \in \mathbb{F}_4^\alpha R^\beta$. Thus, C is equivalent to an $\mathbb{F}_4 R$ -quasi cyclic code of length $n = \alpha + \beta$ and index 2. $\square$

4. The Gray Mapping

The classical Gray mapping $\phi^* : R \mapsto \mathbb{F}_4^2$ is defined by $\phi^*(a + vb) = (a + b, a)$ for any $a + vb \in R$. The *Lee weight* of any element in R is the Hamming weight of its image under ϕ^* . This map extends naturally to vectors in R^n . For any $\mathbf{x} = (x_0, x_1, \dots, x_{\alpha-1}) \in \mathbb{F}_4^\alpha$ and $\mathbf{y} = (y_0, y_1, \dots, y_{\beta-1}) \in R^\beta$, the *Gray map* over $\mathbb{F}_4 R$ is defined by

$$\phi : \mathbb{F}_4^\alpha R^\beta \mapsto \mathbb{F}_4^{\alpha+2\beta} \text{ sending } (\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x}, \phi^*(\mathbf{y})).$$

The map ϕ is an isometry which transforms the Lee distance in $\mathbb{F}_4^\alpha R^\beta$ to the Hamming distance in $\mathbb{F}_4^{\alpha+2\beta}$. For any $\mathbb{F}_4 R$ -linear code C , the code $\phi(C)$ is $\mathbb{F}_4$ -linear. Furthermore, we have

$$wt(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x}) + wt_L(\mathbf{y}) \quad (4.1)$$

where $wt_H(\mathbf{x})$ is the Hamming weight of $\mathbf{x}$ and $wt_L(\mathbf{y})$ is the Lee weight of $\mathbf{y}$.

Theorem 4.1. *Let C be a self-orthogonal $\mathbb{F}_4 R$ -linear code under the inner product defined in Equation (2.5). Then $\phi(C)$ is a Euclidean self-orthogonal code over $\mathbb{F}_4$.*

Proof. It suffices to show that the Gray images of codewords are Euclidean orthogonal whenever the codewords are orthogonal. Let C be a self-orthogonal $\mathbb{F}_4 R$ -linear code of length $\alpha + \beta$. Let $\mathbf{v} = (\mathbf{a}, \mathbf{b} + v\mathbf{c})$, $\mathbf{w} = (\mathbf{d}, \mathbf{u} + v\mathbf{s}) \in \mathbb{F}_4^\alpha \times R^\beta$ be codewords in C with $\mathbf{a}, \mathbf{d} \in \mathbb{F}_4^\alpha$ and $\mathbf{b}, \mathbf{c}, \mathbf{u}, \mathbf{s} \in R^\beta$. Then, by Equation (2.5),

$$\langle \mathbf{v}, \mathbf{w} \rangle = v(\mathbf{a} \cdot \mathbf{d}) + \mathbf{b} \cdot \mathbf{u} + v(\mathbf{b} \cdot \mathbf{s} + \mathbf{c} \cdot \mathbf{u} + \mathbf{c} \cdot \mathbf{s}) = 0 + v0 \in R.$$

Hence, $\mathbf{b} \cdot \mathbf{u} = 0$ and $\mathbf{a} \cdot \mathbf{d} + \mathbf{b} \cdot \mathbf{s} + \mathbf{c} \cdot \mathbf{u} + \mathbf{c} \cdot \mathbf{s} = 0$. Since $\phi(\mathbf{v}) = (\mathbf{a}, \mathbf{b} + \mathbf{c}, \mathbf{b})$ and $\phi(\mathbf{w}) = (\mathbf{d}, \mathbf{u} + \mathbf{s}, \mathbf{u})$, one gets

$$\phi(\mathbf{v}) \cdot \phi(\mathbf{w}) = \mathbf{a} \cdot \mathbf{d} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{s} + \mathbf{c} \cdot \mathbf{u} + \mathbf{c} \cdot \mathbf{s} + \mathbf{b} \cdot \mathbf{u} = 0.$$

Therefore, the code $\phi(C)$ is Euclidean self-orthogonal. $\square$

Theorem 4.2. *Let C be an $\mathbb{F}_4 R$ -skew cyclic code of length $n = \alpha + \beta$. Then, $\phi(C) = C_0 \otimes C_1 \otimes C_2$, where C_0 is a cyclic code of length α in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$ and both C_1 and C_2 are skew cyclic codes of length β in $R[X, \theta]/\langle X^\beta - 1 \rangle$. Moreover,*

$$|\phi(C)| = \prod_{i=0}^2 |C_i|.$$

Proof. From $\{\mathbf{x} = (a_0, a_1, \dots, a_{\alpha-1}, b_0 + vc_0, b_1 + vc_1, \dots, b_{\beta-1} + vc_{\beta-1}) : \mathbf{x} \in C\}$, we construct the codes

$$C_0 := \{(a_0, a_1, \dots, a_{\alpha-1})\}, C_1 := \{(b_0 + c_0, b_1 + c_1, \dots, b_{\beta-1} + c_{\beta-1})\},$$

$$\text{and } C_2 := \{(b_0, b_1, \dots, b_{\beta-1})\}.$$

A codeword $\mathbf{u} := (a_0, a_1, \dots, a_{\alpha-1}) \in C_0$ corresponds to a codeword

$$\mathbf{x} = (a_0, a_1, \dots, a_{\alpha-1}, b_0 + vc_0, b_1 + vc_1, \dots, b_{\beta-1} + vc_{\beta-1}) \in C.$$

Since C is an $\mathbb{F}_4 R$ -skew cyclic code, we know that $T_\theta(\mathbf{x})$ is given by

$$(a_{\alpha-1}, a_0, a_1, \dots, a_{\alpha-2}, \theta(b_{\beta-1} + vc_{\beta-1}), \theta(b_0 + vc_0), \dots, \theta(b_{\beta-2} + vc_{\beta-2})) \in C.$$

Hence, $(a_{\alpha-1}, a_0, a_1, \dots, a_{\alpha-2}) \in C_0$. This implies that C_0 is a cyclic code of length α in $\mathbb{F}_4[X]/\langle X^\alpha - 1 \rangle$.

The proof that C_1 and C_2 are skew cyclic codes of length β in $R[X]/\langle X^\beta - 1 \rangle$ follows the same line of argument. Thus, $\phi(C) = C_0 \otimes C_1 \otimes C_2$ and $|\phi(C)| = \prod_{i=0}^2 |C_i|$. $\square$

Lemma 4.1. *Let $C = \langle (f(X), \mathbf{0}), (\mathbf{0}, g(X)) \rangle$ be an $\mathbb{F}_4 R$ -skew cyclic code with $\ell(X) := \mathbf{0}$. Then $C = C_1 \otimes C_2$ where C_1 is a skew cyclic code over $\mathbb{F}_4$ and C_2 is a skew cyclic code over R .*

Proof. Note that $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$ if and only if $\mathbf{c}_1 = q_1 f(X)$ and $\mathbf{c}_2 = q_2 g(X)$ if and only if $\mathbf{c}_1 \in C_1 = (f(X))$ and $\mathbf{c}_2 \in C_2 = (g(X))$ if and only if $C = C_1 \otimes C_2$ where $C_1 = (f(X))$ and $C_2 = (g(X))$. $\square$

Lemma 4.2. *Let $C = C_1 \otimes C_2$ where C_1 is an $\mathbb{F}_4$ -skew cyclic Euclidean self-orthogonal code and C_2 is an R -skew cyclic self-orthogonal code over R . Then C is a self-orthogonal $\mathbb{F}_4 R$ -skew cyclic code.*

Proof. Suppose $C_1 \subseteq C_1^\perp$ and $C_2 \subseteq C_2^\perp$. Let $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$ and $\mathbf{u} = (\mathbf{c}_3, \mathbf{c}_4) \in C$. Then $\mathbf{c}_1, \mathbf{c}_3 \in C_1 = (f(X))$ and $\mathbf{c}_2, \mathbf{c}_4 \in C_2 = (g(X))$. This implies that $\mathbf{c}_1 \cdot \mathbf{c}_3 = 0 \in \mathbb{F}_4$ and $\langle \mathbf{c}_2, \mathbf{c}_4 \rangle = 0 \in R$. Hence,

$$\langle \mathbf{c}, \mathbf{u} \rangle = v(\mathbf{c}_1 \cdot \mathbf{c}_3) + \langle \mathbf{c}_2, \mathbf{c}_4 \rangle = v \cdot 0 + 0 = 0.$$

Therefore, $C \subseteq C^\perp$, i.e., the $\mathbb{F}_4 R$ -skew cyclic code C is self-orthogonal. $\square$

Note that the converse does not hold. In fact, $C^\perp \neq C_1^\perp \otimes C_2^\perp$ in general. For example, consider $C := C_1 \otimes C_2 \in \mathbb{F}_4^6 R^3$. Let C_1 be the $\mathbb{F}_4$ -skew cyclic codes with parameters $[6, 3, 4]_4$ generated by $w + w^2 X + w^2 X^2 + X^3$. This code is not self-dual although the dual, under the usual Euclidean inner product over $\mathbb{F}_4$, has the same parameters $[6, 3, 4]_4$. The standard generator and parity check matrices are, respectively,

$$G_{C_1} = \begin{pmatrix} 1 & 0 & 0 & w^2 & w & w \\ 0 & 1 & 0 & w & w^2 & w \\ 0 & 0 & 1 & w & w & w^2 \end{pmatrix} \text{ and } H_{C_1} = \begin{pmatrix} 1 & 0 & 0 & w & w^2 & w^2 \\ 0 & 1 & 0 & w^2 & w & w^2 \\ 0 & 0 & 1 & w^2 & w^2 & w \end{pmatrix}.$$

For C_2 we use the R -skew cyclic code generated by $X + (w + v)$. As an R -code, its standard generator and parity check matrices are, respectively,

$$G_{C_2} = \begin{pmatrix} 1 & 0 & w^2 + v \\ 0 & 1 & w + v \end{pmatrix} \text{ and } H_{C_2} = (w^2 + v \ w + v \ 1).$$

Notice that $x = (1, 0, 0, w^2, w, w, w^2 v, v, wv)$ is a codeword in $C_1^\perp \otimes C_2^\perp$ and $y = (w, w^2, w^2, 1, 0, 0, w + v, v, wv)$ is a codeword in C , but $\mathbf{x} \notin C^\perp$, since

$$\langle \mathbf{x}, \mathbf{y} \rangle = v \sum_{i=0}^5 x_i y_i + \sum_{j=0}^2 x_j y_j = v \neq 0.$$

5. $\mathbb{F}_4$ -Codes with Good Parameters from $\mathbb{F}_4 R$ -Skew Cyclic Codes

This section highlights several ways of obtaining $\mathbb{F}_4$ -linear codes with good parameters from $\mathbb{F}_4 R$ -skew cyclic codes.

First, we consider the case of $\alpha = 0$. This yields skew cyclic codes over R . We start by finding a divisor $g_\beta(X)$ of $X^\beta - 1$ in the skew polynomial ring $R[X, \theta]$. Then the skew cyclic code C_β over R has a generator matrix

$$G = \begin{pmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1}g(X) \end{pmatrix} = \begin{pmatrix} \mathbf{g} \\ T_\theta(\mathbf{g}) \\ \vdots \\ T_\theta^{k-1}(\mathbf{g}) \end{pmatrix}$$

where $k = \beta - \deg(g(X))$ is the dimension of C_β . Its Gray image is an $\mathbb{F}_4$ -linear code of length 2β and dimension $2k$ with a generator matrix

$$\phi(G) = \begin{pmatrix} \phi(\mathbf{g}) \\ \phi(T_\theta(\mathbf{g})) \\ \vdots \\ \phi(T_\theta^{k-1}(\mathbf{g})) \\ \hline \phi(v\mathbf{g}) \\ \phi(T_\theta(v\mathbf{g})) \\ \vdots \\ \phi(T_\theta^{k-1}(v\mathbf{g})) \end{pmatrix} = \begin{pmatrix} G_{up} \\ G_{lo} \end{pmatrix}. \quad (5.1)$$

Note that G_{up} and G_{lo} , individually, generate linear codes over $\mathbb{F}_4$ of length 2β . There are some optimal codes that can be obtained in this way.

Example 5.1. For $\beta = 6$, the polynomial $g(X) = X^3 + w^2X^2 + w^2X + w$ divides $X^\beta - 1$ in $R[X, \theta]$. The matrix G_{up} , obtained from $g(X)$, generates a $[12, 3, 8]_4$ quasi-cyclic code, which is optimal according to the Grassl table [10]. Moreover, checking the online database [9], we see that it is a new code among the class of quasi-cyclic codes. Table 1 includes a few more examples of optimal $\mathbb{F}_4$ codes of length 2β .

Table 1. Examples of Optimal $\mathbb{F}_4$ -Linear Codes from G_{up}

No.	Parameters	$g(X) \in R[X, \theta]$	Remark
1	$[6, 2, 4]_4$	$X + (v + w)$	
2	$[8, 2, 6]_4$	$X^2 + wX + w$	New as a QC code
3	$[10, 2, 8]_4$	$X^3 + (v + w)X^2 + (v + w)X + 1$	
4	$[10, 3, 6]_4$	$X^2 + (v + w^2)X + 1$	
5	$[12, 3, 8]_4$	$X^3 + w^2X^2 + w^2X + w$	New as a QC code

A number of high-rate optimal linear codes over $\mathbb{F}_4$ from skew cyclic codes over R (that is, $\alpha = 0$) can be constructed from the full matrix $\phi(G)$ in Equation (5.1).

Table 2 provides a representative subset of such codes, each of length 2β .

Table 2. Examples of Optimal $\mathbb{F}_4$ -Linear Codes from $\phi(G)$

No.	Parameter	$g(X) \in R[X, \theta]$	No.	Parameter	$g(X) \in R[X, \theta]$
1	$[8, 6, 2]_4$	$X + w^2$	5	$[16, 14, 2]_4$	$X + w^2$
2	$[10, 8, 2]_4$	$X + 1$	6	$[18, 16, 2]_4$	$X + v + w^2$
3	$[12, 10, 2]_4$	$X + w$	7	$[20, 18, 2]_4$	$X + w^2$
4	$[14, 12, 2]_4$	$X + 1$	8	$[30, 28, 2]_4$	$X + v + w^2$

Finally, for $\alpha \neq 0$ and $\beta \neq 0$, to maximize the minimum distance of the image of an $\mathbb{F}_4R$ skew cyclic code, one can consider codes with generators of the form $(g_\alpha(X), g_\beta(X))$ where $g_\alpha(X)$ divides $X^\alpha - 1$ over $\mathbb{F}_4$ and $g_\beta(X)$ divides $X^\beta - 1$ in $R[X, \theta]$ such that $\alpha - \deg g_\alpha(X) = 2(\beta - \deg g_\beta(X))$. This ensures that the dimension of the cyclic code over $\mathbb{F}_4$ generated by $g_\alpha(X)$ is equal to the dimension of the Gray $(\mathbb{F}_4)$ -image of the skew cyclic code over R generated by $g_\beta(X)$. A generator matrix of the Gray image is of the form

$$(G_{g_\alpha} | \phi(G))$$

where G_{g_α} is the circulant matrix obtained from $g_\alpha(X)$, *i.e.*, the standard generator of the cyclic code generated by $g_\alpha(X)$, and $\phi(G)$ is as in Equation (5.1). Moreover, the ranks of these two matrices are the same.

The main advantage of this construction is to enable us to find codes with minimum distances much higher than what we would have gotten from the direct sum construction in Theorem 4.2. The codes in Table 3 have minimum distances that are within 2 to 4 units of the minimum distances of the comparable best-known linear codes in [10]. We present the polynomials in a compact form by listing the coefficients in the decreasing order of exponents. In Entry 1, for example, $[1ww^2w^2w^2]$ stands for $X^4 + wX^3 + w^2X^2 + w^2X + w^2$. For brevity, since a cyclic code can also be defined by its check polynomial $h(X) := (X^n - 1)/g(X)$, we give the check polynomial $h_\alpha(X)$, instead of $g_\alpha(X)$, whenever $\deg(h_\alpha(X)) < \deg(g_\alpha(X))$.

We have thus shown that there are several possible ways to construct good quaternary codes via skew cyclic codes over $\mathbb{F}_4R$.

6. DNA Skew Cyclic Code over $\mathbb{F}_4R$

The encoding and decoding systems to store or transfer information or data by mimicking DNA sequences are known collectively as *DNA codes*. The strands, *i.e.*, DNA strings, are preferred to be short to make the synthesis easy and cheap. They must, however, satisfy numerous constraints to be useful for applications. The two most common applications are as basic tools for biomolecular computation and as biomolecular barcoding-tagging system to identify and manipulate individual molecules in complex libraries.

Table 3. Examples of $\mathbb{F}_4$ -Linear Codes with Good Parameters

No.	α	β	h_α	g_β	Parameters
1	10	5	$[1w1]$	$[1(v+w)(v+w)1]$	$[20, 4, 9]_4$
2	15	3	$[1ww^2w^2w^2]$	$[1(v+w^2)]$	$[21, 4, 12]_4$
3	17	3	$[11w11]$	$[1(v+w)]$	$[23, 4, 14]_4$
4	15	5	$[1ww^2w^2w^2]$	$[1(v+w)(v+w)1]$	$[25, 4, 14]_4$
5	30	3	$[1ww^2w^2w^2]$	$[1(v+w)]$	$[36, 4, 22]_4$
6	34	3	$[11w11]$	$[11]$	$[40, 4, 26]_4$
7	45	3	$[1ww^2w^2w^2]$	$[1(v+w)]$	$[51, 4, 32]_4$
8	51	3	$[11w11]$	$[1(v+w^2)]$	$[57, 4, 38]_4$
9	63	3	$[10w^21w^2]$	$[1(v+w)]$	$[69, 4, 49]_4$

Numerous approaches to DNA codes have been extensively investigated. A recent addition to several surveys that have appeared in the literature is the work of Limbachiya *et al.* in [12]. Tools from algebraic coding theory, both from finite fields as well as rings, have been fruitfully used since the inception. A relatively early work by Marathe *et al.* in [13] discussed important design criteria and bounds derived from error-correcting codes. We continue on this line of studies by constructing $\mathbb{F}_4R$ -DNA skew cyclic codes.

The *Watson-Crick complement* of a strand is the strand obtained by replacing each **A** by **T** and vice versa, and each **G** by **C** and vice versa. One writes $\bar{\mathbf{A}} = \mathbf{T}$, $\bar{\mathbf{T}} = \mathbf{A}$, $\bar{\mathbf{C}} = \mathbf{G}$, and $\bar{\mathbf{G}} = \mathbf{C}$. Let $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n)$ be distinct codewords in a DNA code $\mathcal{D}$. The *reverse* of $\mathbf{x}$ is $\mathbf{x}_{\text{rev}} = (x_n, x_{n-1}, \dots, x_1)$. The *complement* of $\mathbf{x}$ is $\mathbf{x}^c = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n)$. Hence, $\mathbf{x}_{\text{rev}}^c = (\bar{x}_n, \bar{x}_{n-1}, \dots, \bar{x}_1)$ is the *reverse complement* of $\mathbf{x}$.

The process in which a strand and its complement bound to form a double-helix is known as *hybridization*. Constraints on the codewords in a DNA code are imposed to avoid it. Let $\mathcal{D}$ be a DNA code of fixed length n , cardinality M , and minimum distance d . Then the constraints on the Hamming distances

$$\text{wt}_H(\mathbf{x}, \mathbf{y}) \geq d \text{ and } \text{wt}_H(\mathbf{x}^c, \mathbf{y}_{\text{rev}}) \geq d \text{ for all } \mathbf{x}, \mathbf{y} \in \mathcal{D} \quad (6.1)$$

are imposed to prevent hybridization between any two strands as well as between a strand and the reverse of any other strand. A *reverse-complement DNA code* $\mathcal{D}$ has parameters $(n, M, d)_4$ that satisfies Equation (6.1).

Abualrub *et al.* studied $\mathbb{F}_4$ -DNA codes of odd lengths in [3], using the bijection between the set of DNA alphabets $\{\mathbf{A}, \mathbf{T}, \mathbf{C}, \mathbf{G}\}$ and $\mathbb{F}_4 := \{0, 1, w, w^2\}$, in that respective ordering. They also established that any $\mathbb{F}_4$ -cyclic code with generator polynomial $f(X)$ is reverse-complement if and only if $f(X) \in \mathbb{F}_4[X]$ is a self-reciprocal polynomial, *i.e.*, $f(X) = X^{\deg(f(X))} \cdot f(X^{-1})$, which is not divisible by $X - 1$ in [3, Theorem 11].

We now extend their bijection to a bijection between the elements of R and

the 16 DNA codons in $\{\mathbf{A}, \mathbf{C}, \mathbf{G}, \mathbf{T}\}^2$. Let $a := a_1 + vb_1 \in R$, with $a_1, b_1 \in \mathbb{F}_4$. The complement $\bar{a}$ of a is given by

$$\bar{a} := a + v = a_1 + v(b_1 + 1). \quad (6.2)$$

The next lemma follows immediately from the definition.

Lemma 6.1. *For all $a, b \in R$, we have*

$$\overline{a + b} = \bar{a} + \bar{b} + v, \overline{(v + 1)a} = (v + 1)\bar{a} + v, \text{ and } \overline{va} = v\bar{a}.$$

The bijection that we use here can be explicitly given as a list.

$a \in R$	Codon	$\bar{a} \in R$	Codon	$a \in R$	Codon	$\bar{a} \in R$	Codon
0	AA	v	TT	$1 + vw^2$	CG	$1 + vw$	GC
1	TA	$1 + v$	AT	$w^2 + vw^2$	AG	$w^2 + vw$	TC
w	CA	$w + v$	GT	vw^2	GG	vw	CC
w^2	GA	$w^2 + v$	CT	$w + vw^2$	TG	$w + vw$	AC

Definition 6.1. An R -linear code C of length β is called DNA-skew cyclic if

- (1) The code C is R -skew cyclic of length β .
- (2) For any codeword $\mathbf{x} \in C$, $\mathbf{x} \neq \mathbf{x}_{\text{rev}}^c$ with $\mathbf{x}_{\text{rev}}^c \in C$.

We adopt the following definition of reciprocal polynomials.

Definition 6.2. Let $f(X) = \sum_{i=0}^{\alpha} a_i X^i$ be a polynomial in $R[X, \theta]$. The reciprocal polynomial of $f(X)$ is the polynomial $f^*(X)$ given by

$$f^*(X) := (f(X))^* = X^{\alpha} \cdot f(X^{-1}) = \sum_{i=0}^{\alpha} \theta^{\alpha}(a_i) X^{\alpha-i} = \sum_{i=0}^{\alpha} \theta^{\alpha}(a_{\alpha-i}) X^i. \quad (6.3)$$

If $f(X) = f^*(X)$, then $f(X)$ is *skew self-reciprocal*.

Lemma 6.2. *Let $f(X), g(X) \in R[X, \theta]$, with $\alpha = \deg(f(X)) \geq \deg(g(X)) = \beta$. Then the following assertions hold.*

- (1) *The reciprocal of $f(X) \cdot g(X)$ is given by*

$$(f(X) \cdot g(X))^* = \begin{cases} f^*(X) \cdot g^*(X) & \text{if } \beta \text{ is even,} \\ \Theta(f^*(X)) \cdot g^*(X) & \text{if } \beta \text{ is odd.} \end{cases} \quad (6.4)$$

- (2) $(f(X) + g(X))^* = f^*(X) + X^{\alpha-\beta} \cdot g^*(X)$.

Proof. Let $f(X) = \sum_{i=0}^{\alpha} a_i X^i$ and $g(X) = \sum_{j=0}^{\beta} b_j X^j$ be polynomials in $R[X, \theta]$ with $\alpha \geq \beta$. Then,

$$f(X) \cdot g(X) = \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} a_i \theta^i(b_j) X^{i+j}.$$

To prove the first assertion, we use Equation (6.3) to obtain

$$\begin{aligned} (f(X) \cdot g(X))^* &= \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \theta^{\alpha+\beta}(a_i) \theta^{\alpha+\beta-i}(b_j) X^{\alpha+\beta-i-j} \\ &= \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \theta^{\alpha+\beta}(a_{\alpha-i}) \theta^{\beta+i}(b_{\beta-j}) X^{i+j}. \end{aligned} \quad (6.5)$$

On the other hand, applying Equation (6.3) on $f(X)$ and $g(X)$, we get

$$\begin{aligned} f^*(X) \cdot g^*(X) &= \left(\sum_{i=0}^{\alpha} \theta^{\alpha}(a_{\alpha-i}) X^i \right) \left(\sum_{j=0}^{\beta} \theta^{\beta}(b_{\beta-j}) X^j \right) \\ &= \sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \theta^{\alpha}(a_{\alpha-i}) \theta^{\beta+i}(b_{\beta-j}) X^{i+j}. \end{aligned} \quad (6.6)$$

Since θ has order 2, the expression in Equations (6.5) and (6.6) are equal when β is even. When β is odd, we can write the expression in Equation (6.5) as

$$\sum_{i=0}^{\alpha} \sum_{j=0}^{\beta} \theta^{\alpha+1}(a_{\alpha-i}) \theta^{\beta+i}(b_{\beta-j}) X^{i+j} = \Theta(f^*(X)) \cdot g^*(X).$$

To prove the second assertion, we use Equation (6.3) to write

$$\begin{aligned} (f(X) + g(X))^* &= \sum_{j=0}^{\beta} \theta^{\alpha}(a_j + b_j) X^{\alpha-j} + \sum_{i=\beta}^{\alpha} \theta^{\alpha}(a_i) X^{\alpha-i} = \\ &= \sum_{i=0}^{\alpha} \theta^{\alpha}(a_{\alpha-i}) X^i + \sum_{j=0}^{\beta} \theta^{\alpha}(b_{\beta-j}) X^j = f^*(X) + X^{\alpha-\beta} \cdot g^*(X). \quad \square \end{aligned}$$

Example 6.1. Given $f(X) = X + 1$ and $g(X) = X + v$ in $R[X, \theta]$, we have

$$(f(X) \cdot g(X))^* = vX^2 + vX + 1 = \Theta(f^*(X)) \cdot g^*(X).$$

A code is *reversible complement* if $\mathbf{c}_{\text{rev}}^c \in C$ for any $\mathbf{c} \in C$. The next theorem characterizes reversible complement R -skew cyclic codes.

Theorem 6.1. *Let $g_1(X)$ and $g_2(X)$ divide $X^{\beta}-1$ in $\mathbb{F}_4[X]$. Let $C = \langle g(X) \rangle$ be R -skew cyclic of odd length β with $g(X) = vg_1(X) + (v+1)g_2(X)$. Then C is reversible complement if and only if $g(X)$ is skew self-reciprocal and $v(X^{\beta}-1)/(X-1) \in C$.*

Proof. Let $g(X) = vg_1(X) + (v+1)g_2(X)$ and $C = \langle g(X) \rangle$ be an R -skew cyclic code of odd length β . Suppose that C is reversible complement. Since $\mathbf{0} \in C$, we have $(\bar{0}, \bar{0}, \dots, \bar{0}) = (v, v, \dots, v) = v(X^{\beta}-1)/(X-1) \in C$. Let

$$\begin{aligned} g_1(X) &= g_0 + g_1X + \dots + g_{t-1}X^{t-1} + X^t \text{ and} \\ g_2(X) &= h_0 + h_1X + \dots + h_{k-1}X^{k-1} + X^k, \end{aligned}$$

where $t \leq k$. Then

$$\begin{aligned} g(X) &= vg_1(X) + (v+1)g_2(X) \\ &= (vg_0 + (v+1)h_0) + (vg_1 + (v+1)h_1)X + \dots \\ &\quad + (vg_{t-1} + (v+1)h_{t-1})X^{t-1} + (v + (v+1)h_t)X^t \\ &\quad + (v+1)h_{t+1}X^{t+1} + \dots + (v+1)h_{k-1}X^{k-1} + (v+1)X^k. \end{aligned}$$

Since C is reversible complement, it contains

$$\begin{aligned} g_{\text{rev}}^c(X) &= v(1 + X + \dots + X^{\beta-k-2}) + \overline{(v+1)}X^{\beta-k-1} + \overline{(v+1)h_{k-1}}X^{\beta-k} \\ &\quad + \dots + \overline{(v+1)h_{t+1}}X^{\beta-t-2} + \overline{(v + (v+1)h_t)}X^{\beta-t-1} \\ &\quad + \overline{(vg_{t-1} + (v+1)h_{t-1})}X^{\beta-t} + \dots + \overline{(vg_1 + (v+1)h_1)}X^{\beta-2} \\ &\quad + \overline{(vg_0 + (v+1)h_0)}X^{\beta-1}. \end{aligned}$$

Using Lemma 6.1 we can write

$$\begin{aligned} g_{\text{rev}}^c(X) &= v(1 + X + \dots + X^{\beta-k-2}) + \overline{(v+1)}X^{\beta-k-1} + \overline{(v+1)h_{k-1}}X^{\beta-k} \\ &\quad + \dots + \overline{(v+1)h_{t+1}}X^{\beta-t-2} + \overline{v}X^{\beta-t-1} + \overline{(v+1)h_t}X^{\beta-t-1} + vX^{\beta-t-1} \\ &\quad + \overline{vg_{t-1}}X^{\beta-t} + \overline{(v+1)h_{t-1}}X^{\beta-t} + vX^{\beta-t} + \dots + \overline{vg_1}X^{\beta-2} \\ &\quad + \overline{(v+1)h_1}X^{\beta-2} + vx^{\beta-2} + \overline{vg_0}X^{\beta-1} + \overline{(v+1)h_0}X^{\beta-1} + vX^{\beta-1}. \end{aligned}$$

Because C is R -linear, $g_{\text{rev}}^c(X) + v(X^\beta - 1)/(X - 1) \in C$. This implies

$$\begin{aligned} g_{\text{rev}}^c(X) + v(X^\beta - 1)/(X - 1) &= \\ &= ((v+1) + v)X^{\beta-k-1} + ((v+1)h_{k-1} + v)X^{\beta-k} + \dots + \\ &= ((v+1)h_{t+1} + v)X^{\beta-t-2} + (\overline{v} + v)X^{\beta-t-1} + ((v+1)h_t + v)X^{\beta-t-1} + \\ &= (\overline{vg_{t-1}} + v)X^{\beta-t} + ((v+1)h_{t-1} + v)X^{\beta-t} + \dots + (\overline{vg_1} + v)X^{\beta-2} + \\ &= ((v+1)h_1 + v)X^{\beta-2} + (\overline{vg_0} + v)X^{\beta-1} + ((v+1)h_0 + v)X^{\beta-1}. \end{aligned}$$

By Equation (6.2) we can write

$$\begin{aligned} &(v+1)X^{\beta-k-1} + (v+1)h_{k-1}X^{\beta-k} + \dots + (v+1)h_{t+1}X^{\beta-t-2} + \\ &vX^{\beta-t-1} + (v+1)h_tX^{\beta-t-1} + X^{\beta-t} + (v+1)h_{t-1}X^{\beta-t} + \dots + \\ &vg_1X^{\beta-2} + (v+1)h_1X^{\beta-2} + vg_0X^{\beta-1} + (v+1)h_0X^{\beta-1} \end{aligned}$$

as

$$\begin{aligned} &(v+1)X^{\beta-k-1} + (v+1)h_{k-1}X^{\beta-k} + \dots + (v+1)h_{t+1}X^{\beta-t-2} + \\ &(v + (v+1)h_t)X^{\beta-t-1} + (vg_{t-1} + (v+1)h_{t-1})X^{\beta-t} + \dots + \\ &(vg_1 + (v+1)h_1)X^{\beta-2} + (vg_0 + (v+1)h_0)X^{\beta-1}. \end{aligned}$$

Multiplying on the left by $X^{k+1-\beta}$, we obtain

$$\begin{aligned} &\theta^k(v+1) + \theta^k((v+1)h_{k-1})X + \dots + \theta^k((v+1)h_{t+1})X^{k-t-1} \\ &\quad + \theta^k(v + (v+1)h_t)X^{k-t} + \theta^k(vg_{t-1} + \theta^k(v+1)h_{t-1})X^{k-t+1} + \dots \\ &\quad + \theta^k(vg_1 + (v+1)h_1)X^{k-1} + \theta^k(vg_0 + (v+1)h_0)X^k. \end{aligned}$$

Hence, $g^*(X) \in C$. Since $C = \langle g(X) \rangle$, there exists $q(X) \in R[X, \theta]$ such that $g^*(X) = q(X) \cdot g(X)$, which implies $\deg(g^*(X)) = \deg(g(X))$ and $q(X) = 1$. Thus, $g^*(X) = g(X)$, as required.

Conversely, let $C = \langle g(X) \rangle$ be an R -skew cyclic code of length β generated by $g(X) = vg_1(X) + (v+1)g_2(X)$, where $g_1(X)$ and $g_2(X)$ are two divisors of $X^\beta - 1$ in $\mathbb{F}_4[X]$. Let $c(X) = c_0 + c_1X + \dots + c_kX^k \in C$, then there exists $q(X) \in R[X, \theta]$ such that $c(X) = q(X) \cdot g(X)$. By Lemma 6.2, $c^*(X) = q^*(X) \cdot g^*(X)$. Since C is skew self-reciprocal, $c^*(X) = q^*(X) \cdot g(X) \in C$ for any $c(X) \in C$. We have

$$c^*(X) = \theta^k(c_k) + \theta^k(c_{k-1})X + \dots + \theta^k(c_0)X^k \in C.$$

Hence,

$$v(X^\beta - 1)/(X - 1) = v(1 + \dots + X^{\beta-1}) \in C.$$

Since C is R -linear,

$$\begin{aligned} X^{\beta-k-1} \cdot c^*(X) + v(X^\beta - 1)/(X - 1) = \\ v + \dots + vX^{\beta-k-2} + (c_0 + v)X^{\beta-k-1} + \dots + (c_k + v)X^{\beta-1}. \end{aligned}$$

By Equation (6.2),

$$v + \dots + vX^{\beta-k-2} + \overline{c_0}X^{\beta-k-1} + \dots + \overline{c_k}X^{\beta-1} = (c^*(X))_{\text{rev}}^c \in C.$$

This concludes the proof. $\square$

The theorem that we have just proved leads us from R -skew cyclic codes to the definition and subsequent characterization of $\mathbb{F}_4R$ -skew cyclic codes in the context of DNA coding.

Definition 6.3. An $\mathbb{F}_4R$ -linear code C is DNA-skew cyclic if the following conditions hold.

- (1) C is an $\mathbb{F}_4R$ -skew cyclic code, i.e., C is an R -left submodule of

$$F[X]/\langle X^\alpha - 1 \rangle \times R[X, \theta]/\langle X^\beta - 1 \rangle.$$

- (2) Any codeword $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$ and its reverse complement

$$\mathbf{c}_{\text{rev}}^c = ((\mathbf{c}_1)_{\text{rev}}^c, (\mathbf{c}_2)_{\text{rev}}^c) \in C$$

are distinct.

The characterization of reverse complement codes over $\mathbb{F}_4R$ can now be established.

Theorem 6.2. Let $C = \langle (f(X), \mathbf{0}), (\mathbf{0}, g(X)) \rangle$ be an $\mathbb{F}_4R$ -skew cyclic code. Note that $\ell(X) := \mathbf{0}$ and $C = C_1 \otimes C_2$, with C_1 an $\mathbb{F}_4$ -cyclic code and C_2 an R -skew cyclic code. Then C is reversible complement if and only if C_1 and C_2 are reversible complement over $\mathbb{F}_4$ and R , respectively.

Proof. Let C be an $\mathbb{F}_4 R$ -skew cyclic code generated by $(f(X), \mathbf{0})$ and $(\mathbf{0}, g(X))$. Lemma 4.1 shows how to find $C = C_1 \otimes C_2$. Let $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C = C_1 \otimes C_2$ with $\mathbf{c}_1 \in C_1$ and $\mathbf{c}_2 \in C_2$. Suppose that C_1 and C_2 are reversible complement over $\mathbb{F}_4$ and R , respectively. Then we have $(\mathbf{c}_1)_{\text{rev}}^c \in C_1$ and $(\mathbf{c}_2)_{\text{rev}}^c \in C_2$. Thus,

$$((\mathbf{c}_1)_{\text{rev}}^c, (\mathbf{c}_2)_{\text{rev}}^c) = \mathbf{c}_{\text{rev}}^c \in C_1 \otimes C_2 = C.$$

Conversely, let $\mathbf{c}_1 \in C_1$ and $\mathbf{c}_2 \in C_2$. Then $\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2) \in C$. If C is reversible complement, then

$$\mathbf{c}_{\text{rev}}^c = ((\mathbf{c}_1)_{\text{rev}}^c, (\mathbf{c}_2)_{\text{rev}}^c) \in C = C_1 \otimes C_2.$$

This implies $\mathbf{c}_{1,\text{rev}}^c \in C_1$ and $\mathbf{c}_{2,\text{rev}}^c \in C_2$, as required. $\square$

7. Conclusion

We have presented our study on skew cyclic codes over the ring $\mathbb{F}_4 R$. Their algebraic structure as left submodules of a skew-polynomial ring is investigated, resulting in the identification of their generators. We have shown that, under some simple conditions on their length, they are equivalent to cyclic or 2-quasi-cyclic codes over the same ring. We supplied several ways of obtaining $\mathbb{F}_4$ -linear codes with good parameters as images of $\mathbb{F}_4 R$ -skew cyclic codes under the Gray mapping. Finally, we have demonstrated how this setup leads naturally to DNA codes and proved a condition on the associated generator polynomial of an $\mathbb{F}_4 R$ -skew cyclic code that guarantees the code to be reversible complement. One of the interesting questions to explore in this topic is to find out whether the class of codes that we propose here contains codes with better relative minimum distances or sizes than known DNA codes.

References

- [1] T. Abualrub and N. Aydin, Additive cyclic codes over mixed alphabets and the football pool problem, *Discrete Math., Algorithms and Appl.*, **9** (2017), <https://doi.org/10.1142/S1793830917500100>.
- [2] T. Abualrub, A. Ghayeb, N. Aydin and I. Siap, On the construction of skew quasi-cyclic codes, *IEEE Trans. Inform. Theory*, **56** (2010), 2081–2090.
- [3] T. Abualrub, A. Ghayeb and X. N. Zeng, Construction of cyclic codes over $GF(4)$ for DNA computing, *J. Franklin Inst.*, **343** (2006), 448–457.
- [4] T. Abualrub, I. Siap and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, *IEEE Trans. Inform. Theory*, **60** (2014), 1508–1514.
- [5] A. Bayram, E. Oztas and I. Siap, Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications, *Des. Codes Cryptogr.*, **80** (2016), 379–393.
- [6] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: Generator matrices and duality, *Des. Codes Cryptogr.*, **54** (2010), 167–179.
- [7] D. Boucher, W. Geiselmann and F. Ulmer, Skew-cyclic codes, *Appl. Algebra Engrg. Commun. Comput.*, **18** (2007), 379–389.
- [8] D. Boucher, P. Sole and F. Ulmer, Skew constacyclic codes over Galois rings, *Adv. Math. Commun.*, **2** (2008), 273–292.

- [9] Z. Chen, Online database of quasi-twisted codes <http://www.tec.hkr.se/~chen/research/codes/searchqc2.htm>. Accessed on April 26, 2019.
- [10] M. Grassl Bounds on the minimum distance of linear codes and quantum codes. Online at <http://www.codetables.de>. Accessed on May 12, 2019.
- [11] F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, *Adv. Math. Commun.*, **8** (2014), 313–322.
- [12] D. Limbachiya, B. Rao and M. K. Gupta, The art of DNA strings: Sixteen years of DNA coding theory. Online at <http://arxiv.org/abs/1607.00266>
- [13] A. Marathe, A. E. Condon and R. M. Corn, On combinatorial DNA word design, *J. Comput. Biology* **8** (2001), 201–219.
- [14] H. Rifá-Pous, J. Rifá, and L. Ronquillo, $\mathbb{Z}_2\mathbb{Z}_4$ -additive perfect codes in steganography, *Adv. Math. Commun.*, **5** (2011), 425–433.
- [15] I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne Skew cyclic codes of arbitrary length, *Int. J. Information and Coding Theory*, **2** (2011), 425–433.
- [16] S. Zhu, Y. Wang, and M. Shi, Some result on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, **56** (2010), 1680–1684.