

$\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)$ – linear skew constacyclic codes

Research Article

Ahlem Melakhessou, Nuh Aydin, Zineb Hebbache, Kenza Guenda

Abstract: In this paper, we study skew constacyclic codes over the ring \mathbb{Z}_qR where $R = \mathbb{Z}_q + u\mathbb{Z}_q$, $q = p^s$ for a prime p and $u^2 = 0$. We give the definition of these codes as subsets of the ring $\mathbb{Z}_q^\alpha R^\beta$. Some structural properties of the skew polynomial ring $R[x, \Theta]$ are discussed, where Θ is an automorphism of R . We describe the generator polynomials of skew constacyclic codes over \mathbb{Z}_qR , also we determine their minimal spanning sets and their sizes. Further, by using the Gray images of skew constacyclic codes over \mathbb{Z}_qR we obtained some new linear codes over \mathbb{Z}_4 . Finally, we have generalized these codes to double skew constacyclic codes over \mathbb{Z}_qR .

2010 MSC: 94B15, 94B60

Keywords: Linear codes, Skew constacyclic codes, $\mathbb{Z}_q\mathbb{Z}_q[u]$ – linear skew constacyclic codes, Bounds

1. Introduction

Codes over finite rings have been known for several decades, but interest in these codes increased substantially after the discovery that good non-linear binary codes can be constructed from codes over rings. Several methods have been introduced to produce certain types of linear codes with good algebraic structures and parameters. Cyclic codes and their various generalizations such as constacyclic codes and quasi-cyclic (QC) codes have played a key role in this quest. One particularly useful generalization of cyclic codes has been the class of quasi-twisted (QT) codes that produced hundreds of new codes with best known parameters [4, 8, 9, 11, 12, 16, 17] recorded in the database [25]. Yet another generalization of cyclic codes, called skew cyclic codes, were introduced in [15] and they have been the subject of an increasing research activity over the past decade. This is due to their algebraic structure and their applications to DNA codes and quantum codes [14, 19, 20]. Skew constacyclic codes over various rings

Ahlem Melakhessou; Department of Mathematics, Mostefa Ben Boulaïd University (Batna2), Batna, Algeria (email: a.melakhessou@univ-batna2.dz).

Nuh Aydin; Department of Mathematics and Statistics, Kenyon College, USA (email: aydinn@kenyon.edu).

Zineb Hebbache, Kenza Guenda (Corresponding Author); Faculty of Mathematics, USTHB, Laboratory of Algebra and Number Theory, BP 32 El Alia, Bab Ezzouar, Algeria (email: zinebhebbache@gmail.com, ken.guenda@gmail.com).

have been studied in [1, 2, 5, 13, 21, 23, 26, 30, 32, 33] as a generalization of skew cyclic codes over finite fields. Recently, P. Li et al. [28] gave the structure of $(1 + u)$ -constacyclic codes over the ring $\mathbb{Z}_2\mathbb{Z}_2[u]$ and Aydogdu et al. [6] studied $\mathbb{Z}_2\mathbb{Z}_2[u]$ -cyclic and constacyclic codes. Further, Jitman et al. [27] considered the structure of skew constacyclic codes over finite chain rings. More recently A. Sharma and M. Bhaintwal studied skew cyclic codes over ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$.

The aim of this paper is to introduce and study skew constacyclic codes over the ring $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)$, where q is a prime power and $u^2 = 0$. Some structural properties of the skew polynomial ring $R[x, \Theta]$ are discussed, where Θ is an automorphism of R . We describe the generator polynomials of skew constacyclic codes over R and \mathbb{Z}_qR . Using Gray images of skew constacyclic codes over \mathbb{Z}_qR we obtained some new linear codes over \mathbb{Z}_4 . Further, we generalize these codes to double skew constacyclic codes over \mathbb{Z}_qR .

The paper is organized as follows. We first give some basic results about the ring $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where $q = p^s$, p is a prime and $u^2 = 0$, and linear codes over \mathbb{Z}_qR , we construct the non-commutative ring $R[x, \Theta]$, where the structure of this ring depends on the elements of the commutative ring R and an automorphism Θ of R . We give some results on skew constacyclic codes over the ring R . In Section 3, we study the algebraic structure of skew constacyclic codes over the ring \mathbb{Z}_qR , section 4 includes the work on the generator polynomials of these codes, their minimal spanning sets and their sizes. In section 5, we determine the Gray images of skew constacyclic codes over R and \mathbb{Z}_qR . These codes are then further generalized to double skew constacyclic codes in the next section. Finally. In section 7, we use the Gray images of skew constacyclic codes over \mathbb{Z}_qR to obtain some new linear codes over \mathbb{Z}_4 .

2. Preliminaries

Let (α, β) denote $n = \alpha + 2\beta$ where α and β are positive integers. Consider the ring $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where $q = p^s$, p is a prime and $u^2 = 0$. The ring R is isomorphic to the quotient ring $\mathbb{Z}_q[u]/\langle u^2 \rangle$. The ring R is not a chain ring, whereas it is a local ring with the maximal ideal $\langle u, p \rangle$. Each element r of R can be expressed uniquely as

$$r = a + ub, \text{ where } a, b \in \mathbb{Z}_q.$$

2.1. Skew polynomial ring over R

In this subsection we construct the non-commutative ring $R[x, \Theta]$. The structure of this ring depends on the elements of the commutative ring R and an automorphism Θ of R . Note that an automorphism Θ in R must fix every element of \mathbb{Z}_q , hence it satisfies $\Theta(a + ub) = a + \delta(u)b$. Therefore, it is determined by its action on u . Let $\delta(u) = k + ud$, where k is a non-unit in \mathbb{Z}_q , $k^2 \equiv 0 \pmod q$ and $2kd \equiv 0 \pmod q$. Then,

$$\Theta(a + ub) = a + \delta(u)b = (a + kb) + udb, \tag{1}$$

for all $a + ub \in R$. Further, let Θ an automorphism of R and let m be its order. The skew polynomial ring $R[x, \Theta]$ is the set of polynomials over R in which the addition is defined as the usual addition of polynomials and the multiplication is defined by the rule

$$xa = \Theta(a)x.$$

The multiplication is extended to all elements in $R[x, \Theta]$ by associativity and distributivity. The ring $R[x, \Theta]$ is called a skew polynomial ring over R and an element in $R[x, \Theta]$ is called a skew polynomial. Further, an element $g(x) \in R[x, \Theta]$ is said to be a right divisor (resp. left divisor) of $f(x)$ if there exists $q(x) \in R[x, \Theta]$ such that

$$f(x) = q(x)g(x) \quad (\text{resp. } f(x) = g(x)q(x)).$$

In this case, $f(x)$ is called a left multiple (resp. right multiple) of $g(x)$.

Lemma 2.1. [31, Lemma 1] Let $f(x), g(x) \in R[x, \Theta]$ be such that the leading coefficient of $g(x)$ is a unit. Then there exist $q(x), r(x) \in R[x, \Theta]$ such that

$$f(x) = q(x)g(x) + r(x), \text{ where } r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)).$$

Definition 2.2. [31, Definition 3.2] A polynomial $f(x) \in R[x, \Theta]$ is said to be a central polynomial if

$$f(x)r(x) = r(x)f(x)$$

for all $r(x) \in R[x, \Theta]$.

Theorem 2.3. The center $Z(R[x, \Theta])$ of $R[x, \Theta]$ is $R^\Theta[x^m]$, where m is the order of Θ and R^Θ is the subring of R fixed by Θ .

Proof. We know $R = \mathbb{Z}_q + u\mathbb{Z}_q$ is the fixed ring of Θ . Since order of Θ is m , for any non-negative integer i , we have

$$x^{mi}a = (\Theta^m)^i(a)x^{mi} = ax^{mi}$$

for all $a \in R$. It gives $x^{mi} \in Z(R[x, \Theta])$, and hence all polynomials of the form

$$f = a_0 + a_1x^m + a_2x^{2m} + \dots + a_lx^{lm}$$

with $a_i \in R$ are in the center.

Conversely, let $f = f_0 + f_1x + f_2x^2 + \dots + f_kx^k \in Z(R[x, \Theta])$ we have $fx = xf$ which gives that all f_i are fixed by Θ , so that $f_i \in R$. Further, choose $a \in R$ such that $\Theta(a) \neq a$. Then it follows from the relation $af = fa$ that $f_i = 0$ for all indices i not divides m . Thus

$$f(x) = a_0 + a_1x^m + a_2x^{2m} + \dots + a_lx^{lm} \in R^\Theta[x^m].$$

□

Corollary 2.4. Let $f(x) = x^\beta - 1$. Then $f(x) \in Z(R[x, \Theta])$ if and only if $m \mid \beta$. Further, $x^\beta - \lambda \in Z(R[x, \Theta])$ if and only if $m \mid \beta$ and λ is fixed by Θ .

2.2. Skew constacyclic codes over R

In this section we generalize the structure and properties from [31] to codes over $\mathbb{Z}_q + u\mathbb{Z}_q$. Hence the proofs of many of the theorems will be omitted.

We start with some structural properties of $R[x, \Theta]/\langle x^\beta - \lambda \rangle$. The Corollary 2.4, shows that the polynomial $(x^\beta - \lambda)$ is in the center $Z(R[x, \Theta])$ of the ring $R[x, \Theta]$, hence generates a two-sided ideal if and only if $m \mid \beta$ and λ is fixed by Θ . Therefore, in this case $R[x, \Theta]/\langle x^\beta - \lambda \rangle$ is a well-defined residue class ring. If $m \nmid \beta$, then the quotient space $R[x, \Theta]/\langle x^\beta - \lambda \rangle$ which is not necessarily a ring is a left $R[x, \Theta]$ -module with multiplication defined by

$$r(x)(f(x) + (x^\beta - \lambda)) = r(x)f(x) + (x^\beta - \lambda),$$

for any $r(x), f(x) \in R[x, \Theta]$.

Next we define the skew λ -constacyclic codes over the ring R . A code of length β over R is a nonempty subset of R^β . A code C is said to be linear if it is a submodule of the R -module R^β . In this paper, all codes are assumed to be linear unless otherwise stated.

Given an automorphism Θ of R and a unit λ in R , a code C is said to be skew constacyclic, or specifically, $\Theta - \lambda$ -constacyclic if C is closed under the $\Theta - \lambda$ -constacyclic shift:

$$\rho_{\Theta, \lambda} : R^\beta \rightarrow R^\beta$$

defined by

$$\rho_{\Theta, \lambda}((a_0, a_1, \dots, a_{\beta-1})) = (\lambda\Theta(a_{\beta-1}), \Theta(a_0), \dots, \Theta(a_{\beta-2})). \tag{2}$$

In particular, such codes are called skew cyclic and skew negacyclic codes when λ is 1 and -1 , respectively. When Θ is the identity automorphism, he become classical constacyclic and we denote ρ_λ the constacyclic shift.

In the rest of paper, we restrict our study to the case where the length β of codes is a multiple of the order of Θ and λ is a unit in R^Θ , where R^Θ denotes the subring of R fixed by Θ .

The proofs of the next theorems are analogous to the proofs of [31] given for the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, therefore we omit them.

Theorem 2.5. [31, Theorem 3] *A code C_β of length β in $R_\beta = R[x, \Theta]/\langle x^\beta - \lambda \rangle$ is a $\Theta - \lambda$ -constacyclic code if and only if C_β is a left $R[x, \Theta]$ -submodule of the left $R[x, \Theta]$ -module R_β .*

Corollary 2.6. [31, Corollary 2] *A code C of length β over R is $\Theta - \lambda$ -constacyclic code if and only if the skew polynomial representation of C is a left ideal in $R[x, \Theta]/\langle x^\beta - \lambda \rangle$.*

The following theorem is the generalization of the Theorems 4 and 5 of [31].

Theorem 2.7. *Let C_β be a skew constacyclic code of length β over R . Then, C_β is a free principally generated skew constacyclic code if and only if there exists a minimal degree polynomial $g_\beta(x) \in C_\beta$ having its leading coefficient a unit such that $C_\beta = \langle g_\beta(x) \rangle$ and $g_\beta(x) \mid x^\beta - \lambda$. Moreover, C_β has a basis $\{g_\beta(x), xg_\beta(x), \dots, x^{\beta-\deg(g_\beta(x))-1}\}$ and $|C_\beta| = |R|^{\beta-\deg(g_\beta(x))}$.*

In this next, we study duals of $\Theta - \lambda$ -constacyclic codes over R . Further, the Euclidean inner product defined by

$$\langle v', w' \rangle = \sum_{i=0}^{\beta-1} v'_i w'_i,$$

for $v' = (v'_0, v'_1, \dots, v'_{\beta-1})$ and $w' = (w'_0, w'_1, \dots, w'_{\beta-1})$ in R^β .

Definition 2.8. *Let C_β be a $\Theta - \lambda$ -constacyclic code of length β over R . Then its dual C_β^\perp is defined as*

$$C_\beta^\perp = \{v' \in R^\beta; \langle v', w' \rangle = 0 \text{ for all } w' \in C_\beta\}$$

Lemma 2.9. *Let C_β be a code of length β over R , where β is a multiple of the order of the automorphism Θ and λ is fixed by Θ . Then C_β is $\Theta - \lambda$ -constacyclic if and only if C_β^\perp is $\Theta - \lambda^{-1}$ -constacyclic. In particular, if $\lambda^2 = 1$, then C_β is $\Theta - \lambda$ -constacyclic if and only if C_β^\perp is $\Theta - \lambda$ -constacyclic.*

Proof. Note that, for each unit λ in $R, \lambda \in R^\Theta$ if and only if $\lambda^{-1} \in R^\Theta$, since $\lambda \in R^\Theta$, so is λ^{-1} . Let $v' = (v'_0, v'_1, \dots, v'_{\beta-1}) \in C_\beta$ and $w' = (w'_0, w'_1, \dots, w'_{\beta-1}) \in C_\beta^\perp$ be two arbitrary elements. Since C_β is $\Theta - \lambda$ -constacyclic code,

$$\rho_{\Theta, \lambda}^{\beta-1}(v') = (\Theta^{\beta-1}(\lambda v'_1), \Theta^{\beta-1}(\lambda v'_2), \dots, \Theta^{\beta-1}(\lambda v'_{\beta-1}), \Theta^{\beta-1}(v'_0)) \in C_\beta.$$

Then, we have

$$\begin{aligned} 0 &= \langle \rho_{\Theta, \lambda}^{\beta-1}(v'), w' \rangle \\ &= \langle (\Theta^{\beta-1}(\lambda v'_1), \Theta^{\beta-1}(\lambda v'_2), \dots, \Theta^{\beta-1}(\lambda v'_{\beta-1}), \Theta^{\beta-1}(v'_0)), (w'_0, \dots, w'_{\beta-1}) \rangle \\ &= \lambda \langle (\Theta^{\beta-1}(v'_1), \Theta^{\beta-1}(v'_2), \dots, \Theta^{\beta-1}(v'_{\beta-1}), \Theta^{\beta-1}(\lambda^{-1} v'_0)), (w'_0, \dots, w'_{\beta-1}) \rangle \\ &= \lambda \left(\Theta^{\beta-1}(\lambda^{-1} v'_0) w'_{\beta-1} + \sum_{j=1}^{\beta-1} \Theta^{\beta-1}(v'_j) w'_{j-1} \right). \end{aligned}$$

As β is a multiple of the order of Θ and λ^{-1} is fixed by Θ , it follows that

$$\begin{aligned} 0 = \Theta(0) &= \Theta(\lambda\Theta^{\beta-1}(\lambda^{-1}v'_0)w'_{\beta-1} + \sum_{j=1}^{\beta-1} \Theta^{\beta-1}(v'_j)w'_{j-1}) \\ &= \lambda(v'_0\Theta(\lambda^{-1}w'_{\beta-1}) + \sum_{j=1}^{\beta-1} v'_j\Theta(w'_{j-1})) \\ &= \lambda\langle \rho_{\Theta, \lambda^{-1}}(w'), v' \rangle. \end{aligned}$$

This implies that, $\rho_{\Theta, \lambda^{-1}}(w') \in C_{\beta}^{\perp}$. In addition, assume that $\lambda^2 = 1$. Then $\lambda = \lambda^{-1}$. Therefore C_{β} is a $\Theta - \lambda$ -constacyclic code.

The converse follows from the fact that $(C_{\beta}^{\perp})^{\perp} = C_{\beta}$. □

3. $\mathbb{Z}_q R$ -linear skew constacyclic codes

In this section, we study skew λ -constacyclic codes over the ring $\mathbb{Z}_q R$.

We know that the ring \mathbb{Z}_q is a subring of the ring R . We construct the ring

$$\mathbb{Z}_q R = \{(e, r); e \in \mathbb{Z}_q, r \in R\}.$$

The ring $\mathbb{Z}_q R$ is not an R -module under the operation of standard multiplication. To make $\mathbb{Z}_q R$ an R -module, we follow the approach in [2] and define the map

$$\begin{aligned} \eta : R &\rightarrow \mathbb{Z}_q \\ a + ub &\mapsto a. \end{aligned}$$

It is clear that the mapping η is a ring homomorphism. Now, for any $d \in R$, we define the multiplication $*$ by

$$d * (e, r) = (\eta(d)e, dr).$$

This multiplication can be naturally generalized to the ring $\mathbb{Z}_q^{\alpha} R^{\beta}$ as follows.

For any $d \in R$ and $v = (e_0, e_1, \dots, e_{\alpha-1}, r_0, r_1, \dots, r_{\beta-1}) \in \mathbb{Z}_q^{\alpha} R^{\beta}$ define

$$dv = (\eta(d)e_0, \eta(d)e_1, \dots, \eta(d)e_{\alpha-1}, dr_0, dr_1, \dots, dr_{\beta-1}),$$

where $(e_0, e_1, \dots, e_{\alpha-1}) \in \mathbb{Z}_q^{\alpha}$ and $(r_0, r_1, \dots, r_{\beta-1}) \in R^{\beta}$.

The following results are analogous to the ones obtained in [2, 5] for the ring $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$.

Lemma 3.1. *The ring $\mathbb{Z}_q^{\alpha} R^{\beta}$ is an R -module under the above definition.*

The above Lemma allows us to give the next definition.

Definition 3.2. *A non-empty subset C of $\mathbb{Z}_q^{\alpha} R^{\beta}$ is called a $\mathbb{Z}_q R$ -linear code if it is an R -submodule of $\mathbb{Z}_q^{\alpha} R^{\beta}$.*

We note that the ring R is isomorphic to \mathbb{Z}_q as an additive group. Hence, for some positive integers k_0, k_1 and k_2 , any $\mathbb{Z}_q R$ -linear code C is isomorphic to a group of the form

$$\mathbb{Z}_q^{k_0} \times \mathbb{Z}_q^{2k_1} \times \mathbb{Z}_q^{k_2}.$$

Definition 3.3. *If $C \subseteq \mathbb{Z}_q^{\alpha} R^{\beta}$ is a $\mathbb{Z}_q R$ -linear code, group isomorphic to $\mathbb{Z}_q^{k_0} \times \mathbb{Z}_q^{2k_1} \times \mathbb{Z}_q^{k_2}$, then C is called a $\mathbb{Z}_q R$ -additive code of type $(\alpha, \beta, k_0, k_1, k_2)$, where k_0, k_1 , and k_2 are as defined above.*

The following results and definitions are analogous to the ones obtained in [6].

Let C be a $\mathbb{Z}_q R$ -linear code and let C_α (respectively C_β) be the canonical projection of C on the first α (respectively on the last β) coordinates. Since the canonical projection is a linear map, C_α and C_β are linear codes over \mathbb{Z}_q and over R of length α and β , respectively. A code C is called separable if C is the direct product of C_α and C_β , i.e.,

$$C = C_\alpha \times C_\beta.$$

We introduce an inner product on $\mathbb{Z}_q^\alpha R^\beta$. For any two vectors

$$v = (v_0, \dots, v_{\alpha-1}, v'_0, \dots, v'_{\beta-1}), w = (w_0, \dots, w_{\alpha-1}, w'_0, \dots, w'_{\beta-1}) \in \mathbb{Z}_q^\alpha \times R^\beta$$

let

$$\langle v, w \rangle = u \sum_{i=0}^{\alpha-1} v_i w_i + \sum_{j=0}^{\beta-1} v'_j w'_j.$$

Let C be a $\mathbb{Z}_q R$ -linear code. The dual of C is defined by

$$C^\perp = \{w \in \mathbb{Z}_q^\alpha \times R^\beta, \langle v, w \rangle = 0, \forall v \in C\}.$$

If $C = C_\alpha \times C_\beta$ is separable, then

$$C^\perp = C_\alpha^\perp \times C_\beta^\perp. \tag{3}$$

Now we are ready to define the skew constacyclic codes over $\mathbb{Z}_q^\alpha R^\beta$. We start by the following Lemma.

Lemma 3.4. *Let $R = \mathbb{Z}_q + u\mathbb{Z}_q$, where \mathbb{Z}_q is a subring of R . Then an element λ is unit in R if and only if $\eta(\lambda)$ is unit in \mathbb{Z}_q .*

Proof. Assume that λ is unit in R ; where $\lambda = \lambda_1 + u\lambda_2$ and $\lambda_1, \lambda_2 \in \mathbb{Z}_q$, then we have $\lambda.v = v.\lambda = 1$ and since η is a ring homomorphism, then we have $\eta(\lambda.v) = \eta(v.\lambda) = \eta(1)$ thus $\eta(\lambda).v' = v'.\eta(\lambda) = 1$ which means that $\eta(\lambda)$ is unit in \mathbb{Z}_q , where $v' = \eta(v) \in \mathbb{Z}_q$.

Conversely, suppose that $\eta(\lambda) = \lambda_1$ is unit in \mathbb{Z}_q we should prove that $\lambda = \lambda_1 + u\lambda_2$ is unit in R . The fact that λ is unit in R means that $\lambda.\lambda^{-1} = 1$, therefore $\lambda.\lambda^{-1} = (\lambda_1 + u\lambda_2)(\lambda_1 + u\lambda_2)^{-1} = (\lambda_1 + u\lambda_2)(\lambda_1^{-1} + u\lambda_3) = \lambda_1\lambda_1^{-1} + u(\lambda_2\lambda_1^{-1} + \lambda_1\lambda_3)$, then we denote $\lambda_3 = \frac{-\lambda_2\lambda_1^{-1}}{\lambda_1} = -\lambda_2(\lambda_1^{-1})^2$ and since λ_1 is unit in \mathbb{Z}_q , then $\lambda_1\lambda_1^{-1} = 1$ which implies that $\lambda.\lambda^{-1} = 1$, so λ is unit in R . \square

Definition 3.5. *Let Θ be an automorphism of R . A linear code C over $\mathbb{Z}_q^\alpha R^\beta$ is called skew constacyclic code if C satisfies the following two conditions.*

(i) C is an R -submodule of $\mathbb{Z}_q^\alpha R^\beta$,

(ii)

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \dots, \Theta(e_{\alpha-2}), \lambda\Theta(r_{\beta-1}), \Theta(r_0), \dots, \Theta(r_{\beta-2})) \in C$$

whenever

$$(e_0, e_1, \dots, e_{\alpha-1}, r_0, r_1, \dots, r_{\beta-1}) \in C$$

Remark 3.6. $\Theta(e_i) = e_i$ for $0 \leq i \leq \alpha - 1$, as $e_i \in \mathbb{Z}_q$ (the fixed ring of Θ).

In polynomial representation, each codeword $c = (e_0, e_1, \dots, e_{\alpha-1}, r_0, r_1, \dots, r_{\beta-1})$ of a skew constacyclic code can be represented by a pair of polynomials

$$\begin{aligned} c(x) &= (e_0 + e_1x + \dots + e_{\alpha-1}x^{\alpha-1}, r_0 + r_1x + \dots + r_{\beta-1}x^{\beta-1}) \\ &= (e(x), r(x)) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle. \end{aligned}$$

Let $h(x) = h_0 + h_1x + \dots + h_t x^t \in R[x, \Theta]$ and let $(f(x), g(x)) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$. The multiplication is defined by the basic rule

$$h(x)(f(x), g(x)) = (\eta(h(x))f(x), h(x)g(x)),$$

where $\eta(h(x)) = \eta(h_0) + \eta(h_1)x + \dots + \eta(h_t)x^t$.

Lemma 3.7. *A code C of length (α, β) over \mathbb{Z}_qR is a $\Theta - \lambda$ -constacyclic code if and only if C is left $R[x, \Theta]$ -submodule of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$.*

Proof. Assume that C is a skew constacyclic code and let $c \in C$. We denote by $c(x) = (e(x), r(x))$ the associated polynomial of c . As $xc(x)$ is a skew constacyclic shift of c , $xc(x) \in C$. Then, by linearity of C , $r(x)c(x) \in C$ for any $r(x) \in R[x, \Theta]$. Thus C is left $R[x, \Theta]$ -submodule of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$. Conversely, suppose that C is a left $R[x, \Theta]$ -submodule of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$, then we have that $xc(x) \in C$. Thus, C is a $\Theta - \lambda$ -constacyclic code.

The converse is straightforward. □

Theorem 3.8. *Let C be a linear code over \mathbb{Z}_qR of length (α, β) , and let $C = C_\alpha \times C_\beta$, where C_α is linear code over \mathbb{Z}_q of length α and C_β is linear code over R of length β . Then C is a skew λ -constacyclic code if and only if C_α is a $\eta(\lambda)$ -constacyclic code over \mathbb{Z}_q and C_β is a skew λ -constacyclic code over R .*

Proof. Let $(e_0, e_1, \dots, e_{\alpha-1}) \in C_\alpha$ and let $(r_0, r_1, \dots, r_{\beta-1}) \in C_\beta$. If $C = C_\alpha \times C_\beta$ is a skew constacyclic code, then

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \dots, \Theta(e_{\alpha-2}), \lambda\Theta(r_{\beta-1}), \Theta(r_0), \dots, \Theta(r_{\beta-2})) \in C,$$

which implies that

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \dots, \Theta(e_{\alpha-2})) \in C_\alpha$$

as Θ is fixed by \mathbb{Z}_q , then

$$(\eta(\lambda)e_{\alpha-1}, e_0, \dots, e_{\alpha-2}) \in C_\alpha$$

and

$$(\lambda\Theta(r_{\beta-1}), \Theta(r_0), \dots, \Theta(r_{\beta-2})) \in C_\beta.$$

Hence, C_α is a constacyclic code over \mathbb{Z}_q and C_β is a $\Theta - \lambda$ -constacyclic code over R .

On the other hand, suppose that C_α is a constacyclic code over \mathbb{Z}_q and C_β is a $\Theta - \lambda$ -constacyclic code over R . Note that

$$(\eta(\lambda)e_{\alpha-1}, e_0, \dots, e_{\alpha-2}) \in C_\alpha$$

and

$$(\lambda\Theta(r_{\beta-1}), \Theta(r_0), \dots, \Theta(r_{\beta-2})) \in C_\beta.$$

Since $C = C_\alpha \times C_\beta$ and $\Theta(e_i) = e_i$, then

$$(\eta(\lambda)\Theta(e_{\alpha-1}), \Theta(e_0), \dots, \Theta(e_{\alpha-2}), \lambda\Theta(r_{\beta-1}), \Theta(r_0), \dots, \Theta(r_{\beta-2})) \in C,$$

so C is a skew constacyclic code over \mathbb{Z}_qR . □

Corollary 3.9. *Let $C = C_\alpha \times C_\beta$ be a skew λ -constacyclic code over \mathbb{Z}_qR , where β is a multiple of the order Θ and λ^{-1} is fixed by Θ . Then the dual code $C^\perp = C_\alpha^\perp \times C_\beta^\perp$ of C is a skew λ^{-1} -constacyclic code over \mathbb{Z}_qR .*

Proof. From Equation (3), we have $C^\perp = C_\alpha^\perp \times C_\beta^\perp$. Clearly, if C_α is a constacyclic code over \mathbb{Z}_q then C_α^\perp is also a constacyclic code over \mathbb{Z}_q . Moreover, from Lemma (2.9), we have C_β^\perp is a skew λ -constacyclic code over R . Hence the dual code C^\perp is skew λ^{-1} -constacyclic over \mathbb{Z}_qR . \square

4. The generators and the spanning sets for \mathbb{Z}_qR -skew constacyclic codes

In this section, we find a set of generators for \mathbb{Z}_qR -skew constacyclic codes as a left $R[x, \Theta]$ -submodules of $\mathbb{Z}_q[x] \langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta] / \langle x^\beta - \lambda \rangle$. Let C be a \mathbb{Z}_qR -skew constacyclic codes, C and $R[x, \Theta] / \langle x^\beta - \lambda \rangle$ are $R[x, \Theta]$ -modules and we define the following mapping:

$$\Psi : C \rightarrow R[x, \Theta] / \langle x^\beta - \lambda \rangle$$

where

$$\Psi(f_1(x), f_2(x)) = f_2(x).$$

It is clear that Ψ is a module homomorphism whose image is a $R[x, \Theta]$ -submodule of $R[x, \Theta] / \langle x^\beta - \lambda \rangle$ and $\ker(\Psi)$ is a submodule of C .

Proposition 4.1. *Let C be a skew constacyclic code of length n over \mathbb{Z}_qR . Then*

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle,$$

where $f(x) \mid (x^\alpha - \eta(\lambda))$ and $g(x) \mid a(x) \mid (x^\beta - \lambda)$.

Proof. Assume that β is a positive integer coprime to the characteristic of R , by similarly theory of cyclic codes over $\mathbb{Z}_2\mathbb{Z}_4$ (see. [3]) we have that

$$\Psi(C) = (a(x) + ug(x)) \text{ with } a(x), g(x) \in R[x, \Theta] \text{ and } g(x) \mid a(x) \mid (x^\beta - \lambda).$$

Note that:

$$\ker(\Psi) = \{ (f(x), 0) \in C : f(x) \in \mathbb{Z}_q[x] / \langle x^\alpha - \eta(\lambda) \rangle \}.$$

Define the set I to be

$$I = \{ f(x) \in \mathbb{Z}_q[x] / \langle x^\alpha - \eta(\lambda) \rangle : (f(x), 0) \in \ker(\Psi) \}.$$

Clearly, I is an ideal of $\mathbb{Z}_q[x] / \langle x^\alpha - \eta(\lambda) \rangle$. Therefore, there exist a polynomial $f(x) \in \mathbb{Z}_q[x] / \langle x^\alpha - \eta(\lambda) \rangle$, such that $I = \langle f(x) \rangle$. Now, for any element $(c_1(x), 0) \in \ker(\Psi)$, we have $c_1(x) \in I = \langle f(x) \rangle$ and there exists some polynomials $m(x) \in \mathbb{Z}_q[x] / \langle x^\alpha - \eta(\lambda) \rangle$ such that $c_1(x) = m(x)f(x)$. Thus $(c_1(x), 0) = m(x) * (f(x), 0)$, which implies that $\ker(\Psi)$ is a left submodule of C generated by one element of the form $(f(x), 0)$ where $f(x) \mid (x^\alpha - \eta(\lambda))$. Thus, by the first isomorphism theorem, we have

$$C / \ker(\Psi) \cong \langle a(x) + ug(x) \rangle.$$

Let $(l(x), a(x) + ug(x)) \in C$, with

$$\Psi(l(x), a(x) + ug(x)) = \langle a(x) + ug(x) \rangle.$$

Then any \mathbb{Z}_qR -skew constacyclic code of length (α, β) can be generated as left $R[x, \Theta]$ -submodule of $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$ by two elements of the form $(f(x), 0)$ and $(l(x), a(x) + ug(x))$, in other word, any element in the code C can be described as

$$d_1(x) * (f(x), 0) + d_2(x) * (l(x), a(x) + ug(x)),$$

where $d_1(x)$ and $d_2(x)$ are polynomials in the ring $R[x, \Theta]$. In fact, the element $d_1(x)$ can be restricted to be an element in the ring $\mathbb{Z}_q[x]$. We will write this as:

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle,$$

where, $f(x) \mid (x^\alpha - \eta(\lambda))$ and $g(x) \mid a(x) \mid (x^\beta - \lambda)$. □

Lemma 4.2. *If $C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle$ is a \mathbb{Z}_qR -skew constacyclic code, then we may assume that $\deg(l(x)) \leq \deg(f(x))$.*

Proof. Suppose that $\deg(l(x)) \geq \deg(f(x))$ with $\deg(l(x)) = i$. Consider an other \mathbb{Z}_qR -skew constacyclic code of length (α, β) with generators of the form

$$D = \langle (f(x), 0), (l(x), a(x) + ug(x)) + x^i * (f(x), 0) \rangle \\ = \langle (f(x), 0), (l(x) + x^i f(x), a(x) + ug(x)) \rangle.$$

Clearly, $D \subseteq C$. However, we also have that:

$$(l(x), a(x) + ug(x)) = (l(x) + x^i f(x), a(x) + ug(x)) - x^i * (f(x), 0),$$

which implies that $(l(x), a(x) + ug(x)) \in C$. Therefore, $C \subseteq D$ implying $C = D$. □

Lemma 4.3. *If $C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle$ is a \mathbb{Z}_qR -skew constacyclic code, then we may assume that $f(x) \mid \frac{x^\beta - \lambda}{g(x)} l(x)$.*

Proof. Since $\frac{x^\beta - \lambda}{g(x)} * (l(x), a(x) + ug(x)) = (\frac{x^\beta - \lambda}{g(x)} l(x), 0)$, it follow that $\Psi(\frac{x^\beta - \lambda}{g(x)} * (l(x), a(x) + ug(x))) = 0$. Therefore, $(\frac{x^\beta - \lambda}{g(x)} l(x), 0) \in \ker(\Psi) \subseteq C$ and $f(x) \mid (\frac{x^\beta - \lambda}{g(x)} l(x))$. □

The above Lemma shows that if the \mathbb{Z}_qR -skew constacyclic code C has only one generator of the form $C = \langle l(x), a(x) + ug(x) \rangle$ then, $(x^\alpha - \eta(\lambda)) \mid \frac{x^\beta - \lambda}{g(x)} l(x)$ with $g(x) \mid a(x) \mid (x^\beta - \lambda)$. Thus from this discussion and Lemma 4.2 and 4.3, we have the following results.

Theorem 4.4. *Let C be a skew constacyclic code of length n over \mathbb{Z}_qR . Then C can be identified uniquely as*

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle,$$

where $f(x) \mid (x^\alpha - \eta(\lambda))$ and $g(x) \mid a(x) \mid (x^\beta - \lambda)$. and $l(x)$ is a skew polynomial satisfying $\deg(l(x)) \leq \deg(f(x))$ and $f(x) \mid \frac{x^\beta - \lambda}{g(x)} l(x)$.

Proof. Following from Proposition 4.1, Lemma 4.2 and 4.3, we can easily see that $C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle$, where the polynomials $f(x), l(x), a(x)$ and $g(x)$ are stated in the theorem. Now, we will prove the uniqueness of the generators. Since $\langle f(x) \rangle$ and $\langle a(x) + ug(x) \rangle$ are skew constacyclic codes over \mathbb{Z}_q and R respectively, then, the skew polynomials $f(x), a(x)$ and $g(x)$ are unique. Now, suppose that

$$C = \langle (f(x), 0), (l_1(x), a(x) + ug(x)) \rangle \\ = \langle (f(x), 0), (l_2(x), a(x) + ug(x)) \rangle,$$

then, we have

$$((l_1(x) - l_2(x)), 0) \in \ker(\Psi) = \langle f(x), 0 \rangle,$$

which implies that

$$l_1(x) - l_2(x) = f(x)j(x),$$

for some skew polynomial $j(x)$, and since $\deg(l_1(x) - l_2(x)) \leq \deg(l_1(x)) \leq \deg(f(x))$ then $j(x) = 0$ and $l_1(x) = l_2(x)$. \square

Definition 4.5. Let A be an R -module. A linearly independent subset B of A that spans A is called a basis of A . If an R -module has a basis, then it is called a free R -module.

Note that if C is a $\mathbb{Z}_q R$ -skew constacyclic code of the form

$$C = \langle (f(x), 0), (l(x), a(x) + ug(x)) \rangle,$$

with $g(x) \neq 0$, then C is a free R -module. If C is not of this form then it is not a free R -module. But we still present a minimal spanning set for the code. The following theorem gives us a spanning minimal set for $\mathbb{Z}_q R$ -skew constacyclic codes.

Theorem 4.6. Let C be a skew constacyclic code of length n over $\mathbb{Z}_q R$, where $f(x), l(x), a(x)$ and $g(x)$ are as in Theorem 4.4 and $f(x)h_f(x) = x^\alpha - \eta(\lambda)$, $a(x)h_a(x) = x^\beta - \lambda$, $a(x) = g(x)m(x)$. Let

$$S_1 = \bigcup_{i=0}^{\deg(h_f)-1} \{x^i * (f(x), 0)\},$$

$$S_2 = \bigcup_{i=0}^{\deg(h_a)-1} \{x^i * (l(x), a(x) + ug(x))\},$$

and

$$S_3 = \bigcup_{i=0}^{\deg(m)-1} \{x^i * (\eta(h_a(x))l(x), uh_a(x)g(x))\}.$$

Then

$$S = S_1 \cup S_2 \cup S_3,$$

forms a minimal spanning set for C and C has $q^{\deg(h_f)} q^{2\deg(h_a)} q^{\deg(m)}$ codewords.

Proof. Let $C(x) = \eta(d(x))(f(x), 0) + e(x)(l(x), a(x) + ug(x)) \in \mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$ be a codeword in C where $d(x)$ and $e(x)$ are skew polynomials in $R[x, \Theta]$. Now, if $\deg(\eta(d(x))) \leq \deg(h_f(x)) - 1$, then $\eta(d(x))(f(x), 0) \in \text{Span}(S_1)$. Otherwise, by using right division algorithm we have

$$\eta(d(x)) = h_f(x)\eta(q_1(x)) + \eta(r_1(x)),$$

where $q_1(x), r_1(x) \in R[x, \Theta]$ and $\eta(r_1(x)) = 0$ or $\deg(\eta(r_1(x))) \leq \deg(h_f(x)) - 1$. Therefore,

$$\eta(d(x))(f(x), 0) = (h_f(x)\eta(q_1(x)) + \eta(r_1(x)))(f(x), 0)$$

$$= \eta(r_1(x))(f(x), 0).$$

Hence, we can assume that $\eta(d(x))(f(x), 0) \in \text{Span}(S_1)$.

Now, if $\deg(\eta(e(x))) \leq \deg(h_a(x)) - 1$, then $\eta(e(x))(l(x), a(x) + ug(x)) \in \text{Span}(S_2)$. Otherwise, again by the right division algorithm, we get polynomials $q_2(x)$ and $r_2(x)$ such that:

$$e(x) = q_2(x)h_a(x) + r_2(x),$$

where $r_2(x) = 0$ or $\deg(r_2(x)) \leq \deg(h_a(x)) - 1$. So, we have

$$\begin{aligned} e(x)(l(x), a(x) + ug(x)) &= (q_2(x)h_a(x) + r_2(x))(l(x), a(x) + ug(x)) \\ &= q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) + r_2(x)(l(x), a(x) + ug(x)). \end{aligned}$$

Since $r_2(x) = 0$ or $\deg(r_2(x)) \leq \deg(h_a(x)) - 1$, then $r_2(x)(l(x), a(x) + ug(x)) \in \text{Span}(S_2)$. Let us consider

$$q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \in \text{Span}(S),$$

we know that $x^\beta - \lambda = a(x)h_a(x) = g(x)m(x)h_a(x)$ and also we have $f(x) \mid \frac{x^\beta - \lambda}{g(x)}l(x)$. Therefore, $\frac{x^\beta - \lambda}{g(x)}l(x) = f(x)k(x)$. Again, if $\deg(q_2(x)) \leq \deg(m(x)) - 1$ then $q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \in \text{Span}(S_3)$. Otherwise, $q_2(x) = \frac{x^\beta - \lambda}{h_a(x)g(x)}q_3(x) + r_3(x)$ with $r_3(x) = 0$ or $\deg(r_3(x)) \leq \deg(m(x)) - 1$. So,

$$\begin{aligned} & q_2(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \\ &= \left(\frac{x^\beta - \lambda}{h_a(x)g(x)}q_3(x)\eta(h_a(x))l(x), \frac{x^\beta - \lambda}{h_a(x)g(x)}q_3(x)uh_a(x)g(x) \right) \\ & \quad + r_3(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \\ &= \left(\frac{x^\beta - \lambda}{h_a(x)g(x)}q_3(x)\eta(h_a(x))l(x), 0 \right) + r_3(x)(\eta(h_a(x))l(x), uh_a(x)g(x)). \end{aligned}$$

Since $\frac{x^\beta - \lambda}{g(x)}l(x) = f(x)k(x)$, then $\left(\frac{x^\beta - \lambda}{h_a(x)g(x)}q_3(x)\eta(h_a(x))l(x), 0 \right) \in \text{Span}(S_1)$ and hence $r_3(x)(\eta(h_a(x))l(x), uh_a(x)g(x)) \in \text{Span}(S_3)$.

Consequently, $S = S_1 \cup S_2 \cup S_3$ forms a minimal spanning set for C . □

5. Gray images of skew constacyclic codes over \mathbb{Z}_qR

In this section, we define a Gray map on \mathbb{Z}_qR , and then extend it to $\mathbb{Z}_q^\alpha R^\beta$. We discuss the Gray images of \mathbb{Z}_qR -skew constacyclic codes where λ is fixed by Θ . We start by recall some results which we will need its in the next.

From [24, Definition 2] we have the following definition

Definition 5.1. Let C_β be a linear code over R of length $\beta = N\ell$ and let λ be unit in R . If for any codeword

$$\left(\begin{array}{c} c_{0,0}, c_{0,1}, \dots, c_{0,\ell-1}, c_{1,0}, c_{1,1}, \dots, c_{1,\ell-1}, \dots, \\ c_{N-1,0}, c_{N-1,1}, \dots, c_{N-1,\ell-1} \end{array} \right) \in C_\beta,$$

then

$$\left(\begin{array}{c} \lambda\Theta(c_{N-1,0}), \lambda\Theta(c_{N-1,1}), \dots, \lambda\Theta(c_{N-1,\ell-1}), \Theta(c_{0,0}), \Theta(c_{0,1}), \dots, \Theta(c_{0,\ell-1}), \dots, \\ \Theta(c_{N-2,0}), \Theta(c_{N-2,1}), \dots, \Theta(c_{N-2,\ell-1}) \end{array} \right) \in C_\beta.$$

Then we say that C_β is a $\Theta - \lambda$ -quasi-twisted code of length β . If ℓ is the least positive integer satisfies that $\beta = N\ell$, then C_β is said to be a $\Theta - \lambda$ -quasi-twisted code with index ℓ . Furthermore, if Θ is the identity map, we call C_β a quasi-twisted code of index ℓ over R .

According to [31], we define a Gray map ϕ over R by

$$\begin{aligned} \phi : R^\beta &\rightarrow \mathbb{Z}_q^{2\beta} \\ \phi(a + ub) &= (b, a + b), \end{aligned}$$

where $a, b \in \mathbb{Z}_q^\beta$

Furthermore, for $r = a + ub \in R$, we define a map

$$\Phi : \mathbb{Z}_q R \mapsto \mathbb{Z}_q^3$$

by

$$\Phi(e, r) = (e, \phi(r)) = (e, b, a + b)$$

and it can be extended componentwise $\mathbb{Z}_q^\alpha R^\beta$ to \mathbb{Z}_q^n as

$$\Phi(e_0, e_1, \dots, e_{\alpha-1}, r_0, r_1, \dots, r_{\beta-1}) = (e_0, e_1, \dots, e_{\alpha-1}, \phi(r_0), \phi(r_1), \dots, \phi(r_{\beta-1})),$$

for all $(e_0, e_1, \dots, e_{\alpha-1}) \in \mathbb{Z}_q^\alpha$ and $(r_0, r_1, \dots, r_{\beta-1}) \in R^\beta$, where $n = \alpha + 2\beta$. Φ is known as the Gray map on $\mathbb{Z}_q^\alpha R^\beta$.

Let $a \in \mathbb{Z}_q^{2\beta}$ with $a = (a_0, a_1) = (a^{(0)} \mid a^{(1)})$, $a^{(i)} \in \mathbb{Z}_q^\beta$, for $i = 0, 1$. Let $\sigma^{\otimes 2}$ be a map from $\mathbb{Z}_q^{2\beta}$ to $\mathbb{Z}_q^{2\beta}$ given by

$$\sigma^{\otimes 2}(a) = (\sigma_\lambda(a^{(0)}) \mid \sigma_\lambda(a^{(1)})),$$

where σ_λ is a constacyclic shift from \mathbb{Z}_q^β to \mathbb{Z}_q^β given by

$$\sigma_\lambda(a^{(i)}) = (\lambda a^{i, \beta-1}, a^{(i, 0)}, \dots, a^{(i, \beta-2)}),$$

for every $a^{(i)} = (a^{(i, 0)}, a^{(i, 1)}, \dots, a^{(i, \beta-1)})$ where $a^{(i, j)} \in \mathbb{Z}_q$, for $j = 0, 1, \dots, \beta - 1$. A linear code C_β of length 2β over \mathbb{Z}_q is said to be a quasi-twisted of index 2 if $\sigma^{\otimes 2}(C_\beta) = C_\beta$.

In addition, for each $\Theta \in \text{Aut}(R)$, let $T_\Theta : R^\beta \mapsto R^\beta$ be a linear transformation given by

$$T_\Theta(a_0, a_1, \dots, a_{\beta-1}) = (\Theta(a_0), \Theta(a_1), \dots, \Theta(a_{\beta-1})).$$

Remark 5.2. C_β is a skew constacyclic code if and only if $T_\Theta \circ \rho_\lambda(C_\beta) = C_\beta$.

Proposition 5.3. With the previous notation, we have $T_\Theta \circ \phi \circ \rho_\lambda = \sigma^{\otimes 2} \circ \phi$.

Proof. Let $r_i = a_i + ub_i$ be the elements of R for $i = 0, 1, \dots, \beta - 1$, we have $\rho_\lambda(r_0, r_1, \dots, r_{\beta-1}) = (\lambda r_{\beta-1}, r_0, r_1, \dots, r_{\beta-2})$. If we apply ϕ , we have

$$\begin{aligned} \phi(\rho_\lambda(r)) &= \phi(\lambda r_{\beta-1}, r_0, \dots, r_{\beta-2}) \\ &= (\lambda b_{\beta-1}, b_0, \dots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), a_0 + b_0, \dots, a_{\beta-2} + b_{\beta-2}). \end{aligned}$$

where $\phi_i(r) = (b_i, a_i + ub_i)$, now we apply T_Θ in the above equation we get,

$$\begin{aligned} T_\Theta \circ \phi(\rho_\lambda(r)) &= T_\Theta(\lambda b_{\beta-1}, b_0, \dots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), a_0 + b_0, \dots, a_{\beta-2} + b_{\beta-2}) \\ &= \left(\begin{array}{c} \Theta(\lambda b_{\beta-1}), \Theta(b_0), \dots, \Theta(b_{\beta-2}), \lambda\Theta(a_{\beta-1} + b_{\beta-1}), \\ \Theta(a_0 + b_0), \dots, \Theta(a_{\beta-2} + b_{\beta-2}) \end{array} \right), \end{aligned}$$

since λ is fixed by Θ and by (1), for any $a \in \mathbb{Z}_q$, we have $\Theta(a) = a$. So, we have

$$T_\Theta \circ \phi \circ \rho_\lambda(r) = \left(\begin{array}{c} \lambda b_{\beta-1}, b_0, \dots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), \\ (a_0 + b_0), \dots, (a_{\beta-2} + b_{\beta-2}) \end{array} \right).$$

For the other direction,

$$\begin{aligned} \sigma^{\otimes 2}(\phi(r)) &= \sigma^{\otimes 2}(b_0, b_1, \dots, b_{\beta-1}, a_0 + b_0, a_1 + b_1, \dots, a_{\beta-1} + b_{\beta-1}) \\ &= \left(\begin{array}{c} \lambda b_{\beta-1}, b_0, \dots, b_{\beta-2}, \lambda(a_{\beta-1} + b_{\beta-1}), \\ (a_0 + b_0), \dots, (a_{\beta-2} + b_{\beta-2}) \end{array} \right), \end{aligned}$$

and the result follows. □

As a consequence of the above Proposition, we have the following theorem.

Theorem 5.4. *Let C_β be a code of length β over R . Then C_β is a skew λ -constacyclic code of length β over R if and only if $\phi(C_\beta)$ is a quasi-twisted code of length 2β over \mathbb{Z}_q of index 2.*

Proof. The necessary part follows from Proposition 5.3, i.e.,

$$\sigma^{\otimes 2} \circ \phi(C_\beta) = T_\Theta \circ \phi \circ \rho_\lambda(C_\beta) = \phi(C_\beta).$$

For the sufficient part, assume that $\phi(C_\beta)$ is a quasi-twisted code of index 2, then

$$\phi(C_\beta) = \sigma^{\otimes 2} \circ \phi(C_\beta) = T_\Theta \circ \phi \circ \rho_\lambda(C_\beta).$$

The injectivity of ϕ implies that $T_\Theta(\rho_\lambda(C_\beta)) = C_\beta$, i.e., C_β is a skew constacyclic code over R . □

Theorem 5.5. *Let $C = C_\alpha \times C_\beta$ be $\Theta - \lambda$ -constacyclic code of length $n = \alpha + 2\beta$ over $\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle$.*

(i) *If $\alpha = \beta$, then $\Phi(C)$ is a quasi-twisted code of index 3 and length 3α .*

(ii) *If $\alpha \neq \beta$ and $\lambda = 1$, then $\Phi(C)$ is a generalized quasi cyclic code of index 3.*

Proof. Assume that $C = C_\alpha \times C_\beta$ is a skew λ -constacyclic code over $\mathbb{Z}_q R$ then by Theorem 3.8, we have that C_α is a constacyclic codes over \mathbb{Z}_q and C_β is skew constacyclic codes over R . Further, from Theorem 5.4, we have that, if C_β is skew constacyclic code over R then $\phi(C_\beta)$ is a quasi twisted code of length 2β over \mathbb{Z}_q of index 2. Which implies that

$$\Phi(e, r) = \left(\begin{array}{c} \lambda e_{\alpha-1}, e_0, \dots, e_{\alpha-2}, \lambda b_{\beta-1}, b_0, \dots, b_{\beta-2}, \\ \lambda(a_{\beta-1} + b_{\beta-1}), (a_0 + b_0), \dots, (a_{\beta-2} + b_{\beta-2}) \end{array} \right),$$

for any $(e_0, e_1, \dots, e_{\alpha-1}, r_0, r_1, \dots, r_{\beta-1}) \in C$. Therefore,

1. if $\alpha = \beta$, then $\Phi(C)$ is a quasi-twisted code of length 3α over \mathbb{Z}_q of index 3.
2. if $\alpha \neq \beta$ and $\lambda = 1$, then according to [22], $\Phi(C)$ is a generalized quasi-cyclic code of index 3.

□

6. Double skew constacyclic codes over $\mathbb{Z}_q R$

In this subsection, we study double skew constacyclic codes over $\mathbb{Z}_q R$. Let $\acute{n} = \acute{\alpha} + 2\acute{\beta}$ and $\acute{\acute{n}} = \acute{\alpha} + 2\acute{\acute{\beta}}$ be integers such that $n = \acute{n} + \acute{\acute{n}}$. We consider a partition of the set of the n coordinates into two subsets of \acute{n} and $\acute{\acute{n}}$ coordinates, respectively, so that C is a subset of $\mathbb{Z}_q^\acute{\alpha} R^\acute{\beta} \times \mathbb{Z}_q^\acute{\alpha} R^\acute{\acute{\beta}}$.

Definition 6.1. *A linear code C of length n over $\mathbb{Z}_q R$ is called a double skew constacyclic code if C satisfies the following conditions.*

(i) C is an R -submodule of $\mathbb{Z}_q^{\alpha+\acute{\alpha}}R^{\beta+\acute{\beta}}$.

$$(ii) (\eta(\lambda)\Theta(\acute{e}_{\alpha-1}), \Theta(\acute{e}_0), \dots, \Theta(\acute{e}_{\alpha-2}), \lambda\Theta(\acute{r}_{\beta-1}), \Theta(\acute{r}_0), \dots, \Theta(\acute{r}_{\beta-2}) \mid \eta(\lambda)\Theta(\acute{e}_{\acute{\alpha}-1}), \Theta(\acute{e}_{\acute{0}}), \dots, \Theta(\acute{e}_{\acute{\alpha}-2}), \lambda\Theta(\acute{r}_{\acute{\beta}-1}), \Theta(\acute{r}_{\acute{0}}), \dots, \Theta(\acute{r}_{\acute{\beta}-2})) \in C.$$

whenever

$$(\acute{e}_0, \dots, \acute{e}_{\alpha-1}, \acute{r}_0, \dots, \acute{r}_{\beta-1} \mid \acute{e}_{\acute{0}}, \dots, \acute{e}_{\acute{\alpha}-1}, \acute{r}_{\acute{0}}, \dots, \acute{r}_{\acute{\beta}-1}) \in C.$$

Remark 6.2. $\Theta(\acute{e}_i) = \acute{e}_i$ and $\Theta(\acute{e}_{\acute{i}}) = \acute{e}_{\acute{i}}$ for $0 \leq i \leq \alpha - 1$, as $\acute{e}_i, \acute{e}_{\acute{i}} \in \mathbb{Z}_q$ (the fixed ring of Θ).

Denote by $\mathfrak{R}_{\acute{\alpha}, \acute{\beta}, \acute{\alpha}, \acute{\beta}}$ the ring:

$$\mathbb{Z}_q[x]/\langle x^\alpha - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^\beta - \lambda \rangle \times \mathbb{Z}_q[x]/\langle x^{\acute{\alpha}} - \eta(\lambda) \rangle \times R[x, \Theta]/\langle x^{\acute{\beta}} - \lambda \rangle.$$

In polynomial representation, each codeword

$$c = (\acute{e}_0, \acute{e}_1, \dots, \acute{e}_{\alpha-1}, \acute{r}_0, \dots, \acute{r}_{\beta-1} \mid \acute{e}_{\acute{0}}, \acute{e}_{\acute{1}}, \dots, \acute{e}_{\acute{\alpha}-1}, \acute{r}_{\acute{0}}, \dots, \acute{r}_{\acute{\beta}-1})$$

of a skew constacyclic code can be represented by four polynomials

$$c(x) = \left(\begin{array}{l} \acute{e}_0 + \acute{e}_1x + \dots + \acute{e}_{\alpha-1}x^{\alpha-1}, \\ \acute{r}_0 + \acute{r}_1x + \dots + \acute{r}_{\beta-1}x^{\beta-1}, \\ \acute{e}_{\acute{0}} + \acute{e}_{\acute{1}}x + \dots + \acute{e}_{\acute{\alpha}-1}x^{\acute{\alpha}-1}, \\ \acute{r}_{\acute{0}} + \acute{r}_{\acute{1}}x + \dots + \acute{r}_{\acute{\beta}-1}x^{\acute{\beta}-1} \end{array} \right) = (\acute{e}(x), \acute{r}(x) \mid \acute{e}(x), \acute{r}(x)) \in \mathfrak{R}_{\acute{\alpha}, \acute{\beta}, \acute{\alpha}, \acute{\beta}}.$$

Let

$$h(x) = h_0 + h_1x + \dots + h_tx^t \in R[x, \Theta]$$

and let

$$(\acute{f}(x), \acute{g}(x) \mid \acute{f}(x), \acute{g}(x)) \in \mathfrak{R}_{\acute{\alpha}, \acute{\beta}, \acute{\alpha}, \acute{\beta}}.$$

We define the multiplication of $h(x)$ and $(\acute{f}(x), \acute{g}(x) \mid \acute{f}(x), \acute{g}(x))$ by

$$h(x)(\acute{f}(x), \acute{g}(x) \mid \acute{f}(x), \acute{g}(x)) = (\eta(h(x))\acute{f}(x), h(x)\acute{g}(x) \mid \eta(h(x))\acute{f}(x), h(x)\acute{g}(x)),$$

where $\eta(h(x)) = \eta(h_0) + \eta(h_1)x + \dots + \eta(h_t)x^t$. This gives us the following Theorem. But before that, we need to give the following Remark.

Remark 6.3. If $c(x) = (\acute{e}(x), \acute{r}(x) \mid \acute{e}(x), \acute{r}(x))$ represents the code word c , then $xc(x)$ represents the $\acute{n}\acute{n}$ -skew constacyclic shift of c .

Theorem 6.4. A linear code C is a double skew constacyclic code if and only if it is a left $R[x, \Theta]$ -submodule of the left-module $\mathfrak{R}_{\acute{\alpha}, \acute{\beta}, \acute{\alpha}, \acute{\beta}}$.

Proof. Assume that C is a double skew constacyclic code. Let $c \in C$, and let the associated polynomial of c be $c(x) = (\acute{e}(x), \acute{r}(x) \mid \acute{e}(x), \acute{r}(x))$. Since $xc(x)$ is an $\acute{n}\acute{n}$ -skew constacyclic shift of c . (See Remark 6.3), then $xc(x) \in C$. Further, by the linearity of C , it follows that $h(x)c(x) \in C$, for any $h(x) \in R[x, \Theta]$. Therefore C is a left $R[x, \Theta]$ -submodule of $\mathfrak{R}_{\acute{\alpha}, \acute{\beta}, \acute{\alpha}, \acute{\beta}}$. Converse is straightforward. \square

7. New linear codes over \mathbb{Z}_4

Codes over \mathbb{Z}_4 , sometimes called quaternary codes as well, have a special place in coding theory. Due to their importance, a database of quaternary codes was introduced in [7] and it is available online [18]. Hence we consider the case $q = 4$ to possibly obtain quaternary codes with good parameters. We conducted a computer search using Magma software [29] to find skew cyclic codes over $\mathbb{Z}_4(\mathbb{Z}_4 + u\mathbb{Z}_4)$ whose Gray images are quaternary linear codes with better parameters than the currently best known codes. We have found ten such codes which are listed in the table below.

The automorphism of $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ that we used is $\Theta(a + bu) = a + 3bu = a - bu$. In addition to the Gray map given in Section 4.1, there are many other possible linear maps from $\mathbb{Z}_4 + u\mathbb{Z}_4$ to \mathbb{Z}_4^ℓ for various values of ℓ . For example, the following map was used in [10] $a + bu \rightarrow (b, 2a + 3b, a + 3b)$ which triples the length of the code. We used both of these Gray maps in our computations, and obtained new codes from each map.

We first chose a cyclic code C_α over \mathbb{Z}_4 generated by $g_\alpha(x)$. The coefficients of this polynomial is given in ascending order of the terms in the table. Therefore, the entry 31212201, for example, represents the polynomial $3 + x + 2x^2 + x^3 + 2x^4 + 2x^5 + x^7$. Then we searched for divisors of $x^\beta - 1$ in the skew polynomial ring $R[x, \Theta]$ where $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ and $\Theta(a + bu) = a - bu$. For each such divisor $g_\beta(x)$ we constructed the skew cyclic code over \mathbb{Z}_4R generated by $(g_\alpha(x), g_\beta(x))$ and its \mathbb{Z}_4 -images under each Gray map described above. As a result of the search, we obtained ten new linear codes over \mathbb{Z}_4 . They are now added to the database ([18]) of quaternary codes. In the table below, which Gray map is used to obtain each new code is not explicitly stated, but it can be inferred from the values of α, β and n , the length of the \mathbb{Z}_4 image. If $n = \alpha + 2\beta$, then it is the map given in section 4.1 and if $n = \alpha + 3\beta$ it is the map described in this section. For example, the second code in the table has length $57 = 15 + 3 \cdot 14$. This means that the Gray map that triples the length of a code over R is used to obtain this code.

When $x^\beta - 1 = g(x)h(x)$ we can use either the generator polynomial $g(x)$ or the parity check polynomial $h(x)$ to define the skew cyclic code over R . For the codes given in the table below we used the parity check polynomial because it has smaller degree. In general a linear code C over \mathbb{Z}_4 has parameters $[n, 4^{k_1}2^{k_2}]$, and when $k_2 = 0$, C is a free code. In this case C has a basis with k vectors just like a linear code over a field. All of the codes in the table below are free codes, hence we will simply denote their parameters by $[n, k, d]$ where d is the Lee weight over \mathbb{Z}_4 .

Our computational results suggest that considering skew cyclic and skew constacyclic codes over $\mathbb{Z}_q(\mathbb{Z}_q + u\mathbb{Z}_q)$ is promising to obtain codes with good parameters over \mathbb{Z}_q .

Table 1. New quaternary codes

α	β	\mathbf{g}_α	\mathbf{g}_β	\mathbb{Z}_4 Parameters
15	14	31212201	$x^4 + (u + 1)x^3 + x^2 + (3u + 2)x + 3u + 3$	[43, 8, 26]
15	14	31212201	$x^4 + (u + 1)x^3 + x^2 + (3u + 2)x + 3u + 3$	[57, 8, 38]
15	14	3021310231	$x^3 + 2ux^2 + (3u + 3)x + 2u + 3$	[43, 6, 30]
15	14	3021310231	$x^3 + 3x^2 + (3u + 2)x + 1$	[57, 6, 42]
7	14	3121	$x^4 + (3u + 3)x^3 + 3x^2 + (u + 2)x + 3u + 3$	[35, 8, 20]
7	14	3121	$x^4 + (u + 3)x^3 + (u + 1)x^2 + (u + 2)x + 3u + 3$	[49, 8, 32]
7	14	12311	$x^3 + (2u + 1)x^2 + 3ux + 3u + 3$	[35, 6, 22]
7	14	12311	$x^3 + (2u + 1)x^2 + ux + u + 1$	[35, 6, 24]
7	14	12311	$x^3 + ux^2 + (3u + 3)x + 1$	[49, 6, 35]
7	14	12311	$x^3 + (u + 2)x^2 + x + 1$	[49, 6, 36]

Acknowledgment: The authors wish to express their thanks to the anonymous reviewers for their careful checking and valuable remarks that improved the presentation and the content of the paper.

References

- [1] T. Abualrub, I. Siap, Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, *Designs, Codes and Cryptography*, 42(3) (2007) 273–287.
- [2] T. Abualrub, I. Siap and I. Aydogdu, $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$ -Linear cyclic codes, *Proceedings of the IMECS 2014, Hong Kong* (2) (2014).
- [3] T. Abualrub, I. Siap, and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, *IEEE. Trans. Inf. Theory* 60(3) (2014) 1508–1514.
- [4] R. Ackerman, N. Aydin, New quinary linear codes from quasi-twisted codes and their duals, *Appl. Math. Lett.* 24(4) (2011) 512–515.
- [5] J. Borges, C. F. Córdoba, R. T. Valls, $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, generator polynomials and dual codes, *IEEE Transactions on Information Theory* 62(11) (2016) 6348–6354.
- [6] I. Aydogdu, T. Abualrub, I. Siap, $\mathbb{Z}_2\mathbb{Z}_2[u]$ -cyclic and constacyclic codes, *IEEE Transactions on Information Theory*, 63(8) (2016) 4883–4893.
- [7] N. Aydin, T. Asamov, A database of \mathbb{Z}_4 codes, *Journal of Combinatorics, Information & System Sciences* 34(1-4) (2009) 1–12.
- [8] N. Aydin, N. Connolly, M. Grassl, Some results on the structure of constacyclic codes and new linear codes over $GF(7)$ from quasi-twisted codes, *Adv. Math. of Commun.* 11(1) (2017) 245–258.
- [9] N. Aydin, N. Connolly, J. Murphree, New binary linear codes from QC codes and an augmentation algorithm, *Appl. Algebra Eng. Commun. Comput.* 28(4) (2017) 339–350.
- [10] N. Aydin, Y. Cengellenmis and A. Dertli, On some constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1 \rangle$, their \mathbb{Z}_4 images, and new codes, *Designs, Codes and Cryptography* 86(6) (2018) 1249–1255.
- [11] N. Aydin, I. Siap, D. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, *Designs, Codes and Cryptography* 24(3) (2001) 313–326.
- [12] N. Aydin, I. Siap, New quasi-cyclic codes over \mathbb{F}_5 , *Appl. Math. Lett.* 15(7) (2002) 833–836.
- [13] R. K. Bandi, M. Bhaintwal, A note on cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, *Discrete Mathematics Algorithms and Applications* 8(1) (2016) 1–17.
- [14] N. Bennenni, K. Guenda, S. Mesnager, DNA cyclic codes over rings, *Adv. in Math. of Comm.* 11(1) (2017) 83–98.
- [15] D. Boucher, W. Geiselmann, F. Ulmer, Skew-cyclic codes, *Appl. Algebra Engrg. Comm. Comput.* 18(4) (2007) 379–389.
- [16] R. Daskalov, P. Hristov, New binary one-generator quasi-cyclic codes, *IEEE Trans. Inf. Theory* 49(11) (2003) 3001–3005.
- [17] R. Daskalov, P. Hristov, E. Metodieva, New minimum distance bounds for linear codes over $GF(5)$ *Discrete Math.* 275(1–3) (2004) 97–110.
- [18] Database of \mathbb{Z}_4 Codes, online, <http://www.asamov.com/Z4Codes/CODES/ShowCODESTablePage.aspx> (Accessed March, 2019).
- [19] H. Q. Dinh, A. K. Singh, S. Pattanayak, S. Sriboonchitta, Cyclic DNA codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + v^2\mathbb{F}_2 + uv^2\mathbb{F}_2$, *Designs Codes and Cryptography* 86(7) (2018) 1451–1467.
- [20] M. F. Ezerman, S. Ling, P. Solé, O. Yemen, From skew-cyclic codes to asymmetric quantum code, *Adv. in Math. of Comm.* 5(1) (2011) 41–57.
- [21] J. Gao., Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, *J. Appl. Math. Inform.* 31(3–4) (2013) 337–342.
- [22] I. Siap, N. Kulhan, The structure of generalized quasi cyclic codes, *Appl. Math. E-Notes* 5 (2005) 24–30.
- [23] J. Gao, F. W. Fu, L. Xiao, R. K. Bandi, Some results on cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$, *Discrete Mathematics Algorithms and Applications* 7(4) (2015) 1–9.
- [24] J. Gao, F. Ma, F. Fu, Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$, *Appl. Comput. Math.* 6(3)

- (2017) 286–295.
- [25] M. Grassl, Code Tables: Bounds on the parameters of codes, online, <http://www.codetables.de/>.
 - [26] F. Gursoy, I. Siap, B. Yildiz, Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$, *Advances in Mathematics of Communications* 8(3) (2014) 313–322.
 - [27] S. Jitman, S. Ling, P. Udomkavanich, Skew constacyclic over finite chain rings, *Adv. Math. Commun.* 6(1) (2012) 39–63.
 - [28] P. Li, W. Dai, X. Kai, On $\mathbb{Z}_2\mathbb{Z}_2[u] - (1 + u)$ -additive constacyclic, arXiv:1611.03169v1 (2016).
 - [29] Magma computer algebra system, online, <http://magma.maths.usyd.edu.au/>
 - [30] J. F. Qian, L. N. Zhang, S. X. Zhu, $(1 + u)$ -Constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *Applied Mathematics Letters* 19(8) (2006) 820–823.
 - [31] A. Sharma, M. Bhaintwal, A class of skew-constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, *Int. J. Information and Coding Theory* 4(4) (2017) 289–303.
 - [32] I. Siap, T. Abualrub, N. Aydin, P. Seneviratne, Skew cyclic codes of arbitrary length, *Int. J. Information and Coding Theory* 2(1) (2011) 10–20.
 - [33] B. Yildiz, N. Aydin, Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and their \mathbb{Z}_4 -images, *Int. J. Information and coding Theory* 2(4) (2014) 226–237.