

Structure of skew cyclic codes over $\mathbb{F}_p[u]/\langle u^k \rangle$

Habibul Islam [†]

Om Prakash ^{*}

Department of Mathematics

Indian Institute of Technology Patna

Patna 801106

Bihar

India

Abstract

In this paper, for any integer $k > 1$, we study skew cyclic codes of length n over $R_k = \mathbb{F}_p + u\mathbb{F}_p + \dots + u^{k-1}\mathbb{F}_p$, where $u^k = 0$ and p is an odd prime. It is noted that the ring R_k is isomorphic to the quotient ring $\mathbb{F}_p[u]/\langle u^k \rangle$. We characterize skew cyclic codes of length n over R_k as free left $R_k[x; \theta]$ -submodules of $R_k[x; \theta]/\langle x^n - 1 \rangle$ and construct their generators and minimal generating sets. Also, an algorithm of encoding and decoding of these codes has been provided. Finally, some examples of optimal linear codes are given from Gray images of skew cyclic codes over R_k .

Subject Classification: (2010) 94B05, 94B15, 94B35, 94B60.

Keywords: Skew polynomial ring, Skew cyclic code, Generating set, Syndrome decoding, Optimal code, Gray map.

1. Introduction

Over the last few decades, many new error-correcting codes have been explored by using cyclic codes due to their advancement in algebraic structures. Recall that a cyclic code of length n over a field $\mathbb{F}_q$ is defined to be an ideal of the quotient ring $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ and also the ideal is principally generated by a factor of $x^n - 1$. But for the case of finite rings, analogously we cannot identify a cyclic code with a principally generated ideal of a quotient ring. Hence, the task of finding generators of cyclic

[†] E-mail: habibul.pma17@iitp.ac.in

^{*} E-mail: om@iitp.ac.in (Corresponding Author)

codes over a finite ring is challenging. In 2007, Abualrub and Siap [1] studied cyclic codes over chain rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + \mathbb{Z}_2 + u^2\mathbb{Z}_2$. They obtained their generators over these two rings explicitly. Later, in 2015, Singh and Kewat [29] generalized the concept of [1] over the chain ring $\mathbb{Z}_p[u]/\langle u^k \rangle$ and discussed their generators as well as minimal spanning set. In 2021, Prakash et al. [26] determined the generators and minimal spanning sets for cyclic codes over $\mathbb{Z}_{p^k}$. Recently, cyclic codes over finite commutative rings and their useful application to construct reversible codes in [20] and LCD (linear complementary dual) codes in [19] have been carried out. Further, cyclic codes in the form of their generalized classes, namely, constacyclic codes over finite commutative rings have received major attention for exploring new parameters both in classical and quantum codes [12, 14, 16–18]. Again, cyclic codes by using the concept of generalized cyclotomic classes have appeared in [23, 24, 27].

On the other hand, in 2007, Boucher et al. [5] used the concept of skew polynomial rings in coding theory. They characterized skew cyclic code of length n as an ideal of the quotient ring $\mathbb{F}_q[x; \theta]/\langle x^n - 1 \rangle$, where θ is an automorphism on $\mathbb{F}_q$. Further, Boucher and Ulmer [6] explored some new codes from skew cyclic codes whose minimum distances are larger than the distances of previously best-known codes. Later, Siap et al. [28] considered skew cyclic codes of length n as left $\mathbb{F}[x; \theta]$ -submodules of $\mathbb{F}_q[x; \theta]/\langle x^n - 1 \rangle$ and also constructed generators for these codes. Abualrub et al. [2] gave the structure of skew cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. In 2012, Jitman et al. [21] considered skew constacyclic codes over finite chain rings, in particular, over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. After that, Gao [8] studied skew cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$, while Gursoy et al. [10] considered these codes over $\mathbb{F}_q + u\mathbb{F}_q$. Recently, Dastbasteh et al. [7] studied skew cyclic codes over the ring $\mathbb{F}_p + u\mathbb{F}_p$ and obtained their generators. Apart from these, there are many other important studies on these codes over different finite commutative rings, particularly, over non-chain rings, we refer [11, 13, 15, 25]. For any odd prime p , let $\mathbb{F}_p$ be the field of size p and $R_k = \mathbb{F}_p + u\mathbb{F}_p + \dots + u^{k-1}\mathbb{F}_p$ where $u^k = 0$ and $k > 1$ is an integer. Note that $R_1 = \mathbb{F}_p$. In this paper, we study skew cyclic codes of length n over R_k and construct their generators explicitly. The main motive of the study is to obtain complete structures of skew cyclic codes by using their generators and show their encoding and decoding process over R_k . Note that the ring R_k is isomorphic to the quotient ring $\mathbb{F}_p[u]/\langle u^k \rangle$. Any element w of R_k can be written as $w = a_0 + ua_1 + \dots + u^{k-1}a_{k-1}$ where $a_i \in \mathbb{F}_p$ for $0 \leq i \leq k-1$. Also, the units of R_k can be obtained by the result that w is a unit in R_k if and only if a_0 is a unit in $\mathbb{F}_p$. Let θ be an element of the Galois group

$\text{Aut}(R_k)$ and $\theta(u) = a_0 + ua_1 + \dots + u^{k-1}a_{k-1}$. Since θ is an automorphism on R_k and $u^k = 0$, $k > 1$, $\theta(u^k) = 0$ and hence $a_0 = 0$. Particularly, we choose the automorphism θ on R_k for $k > 1$ as $\theta(1) = 1, \theta(0) = 0$ and $\theta(u) = su$, for some $1 \neq s \in \mathbb{F}_p^*$. For this automorphism θ , the set $R_k[x; \theta] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in R_k\}$ forms a noncommutative ring under the usual addition of polynomials and multiplication of polynomials with respect to the condition $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$. The ring $R_k[x; \theta]$ is known as a skew polynomial ring. Let the order of θ be m , i.e., $\theta^m(a) = a$ for all $a \in R_k$. Then one can easily check that the center of $R_k[x; \theta]$ is $\mathbb{F}_p[x^m]$ and hence $R_{k,n} = R_k[x; \theta] / \langle x^n - 1 \rangle$ is a ring when $m \mid n$ where skew cyclic codes of length n over R_k are nothing but ideals of $R_{k,n}$. On the other side, if m does not divide n , $R_{k,n}$ is a left $R_k[x; \theta]$ -module and skew cyclic codes of length n over R_k are left $R_k[x; \theta]$ -submodules of $R_{k,n}$. Since we are especially interested to skew cyclic codes of length n over R_k , for $k > 1$, where m does not divide n , we focus on the module structure of $R_{k,n}$ throughout.

2. Basic definitions and results

Definition 2.1: A code C of length n over R_k is said to be a skew cyclic code if

- (1) C is an R_k -submodule of R_k^n and
- (2) for any $c = (c_0, c_1, \dots, c_{n-1}) \in C$, we have $\tau(c) := (\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$.

Note that if θ is the identity automorphism in the above definition, then it is a cyclic code over R_k . For any codeword $c = (c_0, c_1, \dots, c_{n-1}) \in R_k^n$, we can find a polynomial $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ in $R_{k,n} = R_k[x; \theta] / \langle x^n - 1 \rangle$. With this identification, one can easily find the following result.

Theorem 2.2 : A linear code C of length n over R_k is a skew cyclic code if and only if the polynomial representation of C is a left $R_k[x; \theta]$ -submodule of $R_{k,n} = R_k[x; \theta] / \langle x^n - 1 \rangle$.

Theorem 2.3 : [22] Let $f(x), g(x) \in R_k[x; \theta]$ where the leading coefficient of $g(x)$ is a unit. Then there exist two unique polynomials $q(x), r(x) \in R_k[x; \theta]$ such that $f(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $\deg(g(x)) > \deg(r(x))$.

Now, we discuss some important results which help to develop our main results in the subsequent sections. Their proofs are easy to derive and therefore we omitted some of them.

Proposition 2.4 : For any polynomial $f(x) \in R_k[x; \theta]$, where $k > 1$, there exist polynomials $f_i(x) \in R_{k-i}[x; \theta]$ such that $f(x)u^i = u^i f_i(x)$ for $1 \leq i \leq k-1$.

Proposition 2.5 : The set of units of $R_i[x; \theta]$ is $U(R_i[x; \theta]) = \{a + uh_1(x) + u^2h_2(x) + \dots + u^{i-1}h_{i-1}(x) \mid a \in \mathbb{F}_p^* \text{ and } h_i(x) \in \mathbb{F}_p[x]\}$, where $1 \leq i \leq k$.

Proof : We can prove the result by induction on i where it is true for $i = 2$, see [[7], Lemma 13]. □

Proposition 2.6 : For $k \geq 2$, the polynomial $x^n - 1$ factories in $R_{k-1}[x; \theta]$ as $x^n - 1 = g_1(x)g_2(x)$ if and only if there exist polynomials $f_1(x), f_2(x) \in R_k[x; \theta]$ such that $x^n - 1 = f_1(x)f_2(x)$ where $f_i(x) = g_i(x) + u^{k-1}k_i(x)$, $k_i(x) \in \mathbb{F}_p[x]$, for $i = 1, 2$.

Corollary 2.7 : The polynomial $x^n - 1$ factories in $\mathbb{F}_p[x]$ as $x^n - 1 = g_1(x)g_2(x)$ if and only if there exist polynomials $f_1(x), f_2(x) \in R_k[x; \theta]$ such that $x^n - 1 = f_1(x)f_2(x)$ where $f_i(x) = g_i(x) + ul_{1i}(x) + u^2l_{2i}(x) + \dots + u^{k-1}l_{k-1i}(x)$, $l_{ji} \in \mathbb{F}_p[x]$, for $i = 1, 2$ and $1 \leq j \leq k-1$.

3. Generators of skew cyclic codes over R_k

In this section, we are interested to find the generators of skew cyclic codes of arbitrary length n over R_k . Note that if $f(x) \in R_k[x; \theta]$ and the leading coefficient d of $f(x)$ is unit, then $d^{-1}f(x)$ is a monic polynomial. But an arbitrary element of R_k not necessarily be a unit. Therefore, a skew cyclic code C over R_k may or may not contain any monic polynomials. By applying Theorem 2.3, we can find the generator polynomials if C contains any monic polynomial of minimal degree. However, the task becomes difficult if C does not contain any monic polynomial or contains some monic polynomials which are not of a minimal degree in C . Based on this distinction, we would be able to find the generators of skew cyclic codes for all possible cases in the next four theorems.

Theorem 3.1 : Let $f(x)$ be a non-monic polynomial of minimal degree in C . Then $f(x) = u^i a^i(x)$ where $a^i(x) \in R_{k-i}[x; \theta]$ for some positive integer i .

Proof : Let $f(x)$ be a non-monic polynomial of minimal degree in C . Let $f(x) = a_0 + a_1x + \dots + ua_r x^r$ where $a_i \in R_k$ and $a_r \in R_{k-1}$. Suppose $a_r = t_1 + ut_2 + \dots + u^{k-2}t_{k-1}$ where $t_i \in \mathbb{F}_p$. Let i be the least

positive integer such that $t_i \neq 0$. Then $f(x) = a_0 + a_1x + \dots + ua_r x^r$ with $a_r = u^{i-1}(t_i + ut_{i+1} + \dots + u^{k-i-1}t_{k-i})$. Therefore, $u^{k-1}f(x), u^{k-2}f(x), \dots, u^{k-i}f(x)$ are in C with degree less than r . Since $f(x)$ is the polynomial in C with minimal degree r , $u^{k-1}f(x) = 0, u^{k-2}f(x) = 0, \dots, u^{k-i}f(x) = 0$. Hence, $f(x) = u^i a^i(x)$ where $a^i(x) \in R_{k-i}[x; \theta]$ with unit leading coefficient.

Theorem 3.2 : Let C be a non-zero skew cyclic code of length n over R_k for $k > 1$. Suppose C does not contain any monic polynomial and $a(x) = ua^1(x)$ is the minimal degree polynomial in C , then $C = \langle ua^1(x) \rangle$ with $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$.

Proof : Let $c(x) \in C$ be a codeword. Then $c(x)$ is not a monic polynomial. Let $c(x) = c_0 + c_1x + \dots + uc_t x^t$ where $c_i \in R_k$ and $c_t \in R_{k-1}$. Assume that $c_t = e_1 + ue_2 + \dots + u^{k-2}e_{k-1} \in R_{k-1}$. Let j be the least positive integer such that $e_j \neq 0$. Then $c(x) = c_0 + c_1x + \dots + u^j c_j x^j$ where $c_i \in R_k$ and $c_j \in R_{k-j}^*$. Let $a(x) = ua^1(x)$ be the polynomial of minimal degree r in C with $a^1(x) = a_0 + a_1x + \dots + a_r x^r$ where $a_i \in R_{k-1}$ and $a_r \in R_{k-1}^*$. Let $c(x) = c_1(x) + c_2(x)$ where $c_1(x)$ contains all terms of degree up to $r-1$ and $c_2(x)$ contains all rest terms (with degree r and above). If possible, let c_{t-1} be a unit. Since $a_r \in R_{k-1}^*$, $\alpha = \theta(a_r) \in R_{k-1}^*$. Also, by definition, $\theta^i(u) = s^i u$ and let $d = s^{t-r} \in \mathbb{F}_p^*$. Now,

$$\begin{aligned} d_1(x) &= u^{j-1} d^{-1} \alpha^{-1} x^{t-r} a(x) \\ &= u^{j-1} d^{-1} \alpha^{-1} \theta^{t-r}(ua_0)x^{t-r} + u^{j-1} d^{-1} \alpha^{-1} \theta^{t-r}(ua_1)x^{t-r+1} + \dots + \\ &\quad u^{j-1} d^{-1} \alpha^{-1} \theta^{t-r}(ua_{r-1})x^{t-1} + u^{j-1} \alpha^{-1} d^{-1} \theta^{t-r}(ua_r)x^t \\ &= u^{j-1} d^{-1} \alpha^{-1} \theta^{t-r}(ua_0)x^{t-r} + u^{j-1} d^{-1} \alpha^{-1} \theta^{t-r}(ua_1)x^{t-r+1} + \dots + \\ &\quad u^{j-1} d^{-1} \alpha^{-1} \theta^{t-r}(ua_{r-1})x^{t-1} + u^j x^t \in C. \end{aligned}$$

Also,

$$\begin{aligned} d_2(x) &= (c_t)^{-1} c(x) \\ &= (c_t)^{-1} c_0 + (c_t)^{-1} c_1 x + \dots + (c_t)^{-1} c_{t-1} x^{t-1} + u^j x^t \in C. \end{aligned}$$

Then $d(x) = d_2(x) - d_1(x) \in C$ is a polynomial of degree $(t-1)$. Hence, the leading coefficient of $d(x)$, i.e., d_{t-1} is a unit. This contradicts the fact that C does not contain any monic polynomial. Thus, c_{t-1} can not be a unit. By a similar argument, we can conclude that none of the coefficients of $c_2(x)$ is a unit. If possible, let coefficient c_i of the polynomial $c_1(x)$ be a unit for some integer i . Then $u^{k-1}c(x) = u^{k-1}c_1(x) \in C$ where $\deg(u^{k-1}c_1(x)) < r = \deg(a(x))$. This contradicts the fact that $a(x)$ is the minimal degree polynomial

in C . Consequently, $c(x) = uc^1(x)$ where $c^1(x) \in R_{k-1}[x; \theta]$. Now, by division algorithm, we have two polynomials $q(x), r(x) \in R_{k-1}[x; \theta]$ such that $c^1(x) = q(x)a^1(x) + r(x)$, where $\deg(r(x)) < \deg(a^1(x))$ or $r(x) = 0$. Then $uc^1(x) = uq(x)a^1(x) + ur(x) = q'(x)ua^1(x) + ur(x)$. Hence, $ur(x) = uc^1(x) - q'(x)ua^1(x) \in C$. As $\deg(ur(x)) = \deg(r(x)) < \deg(a^1(x)) = r$, $ur(x) = 0$. Since $r(x) \in R_{k-1}[x; \theta]$, $r(x) = 0$. Then $c(x) = uc^1(x) = q'(x)ua^1(x) \in \langle ua^1(x) \rangle$. Hence, $C = \langle ua^1(x) \rangle$.

Again, by division algorithm, we get two polynomials $b^1(x), r^1(x)$ in $R_{k-1}[x; \theta]$ such that $x^n - 1 = b^1(x)a^1(x) + r^1(x)$, where $\deg(r^1(x)) < \deg(a^1(x))$ or $r^1(x) = 0$. By Proposition 2.4, we have $u(x^n - 1) = b_1^1(x)ua^1(x) + ur^1(x)$. Thus, we have $ur^1(x) = -b_1^1(x)ua^1(x) \in C$. As $\deg(ur^1(x)) = \deg(r^1(x)) < \deg(a^1(x)) = r$, $ur^1(x) = 0$. Since $r^1(x) \in R_{k-1}[x; \theta]$, $r^1(x) = 0$. Therefore, $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$. $\square$

Theorem 3.3 : Let C be a non-zero skew cyclic code of length n over R_k for $k > 1$ in which $g(x)$ be the minimal degree monic polynomial. Then $C = \langle g(x) \rangle$ and $x^n - 1 = k(x)g(x)$ in $R_k[x; \theta]$.

Proof : It is easy to verify by using Theorem 2.3. $\square$

Theorem 3.4 : Let C be a non-zero skew cyclic code of length n containing at least one monic polynomial over R_k for $k > 1$. Suppose C does not contain any monic polynomial of minimal degree and $a(x) = ua^1(x)$ is the polynomial of minimal degree in C . Let $g(x)$ be the polynomial of minimal degree among the monic polynomials in C . Then $C = \langle g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x), ua^1(x) \rangle$ where $x^n - 1 = k(x)g(x)$ in $R_k[x; \theta]$ and $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$.

Proof : Similar to Theorem 3.2, it is verified. $\square$

Proposition 3.5 : Let $C = \langle g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x), ua^1(x) \rangle$ be a non-zero skew cyclic code as given in Theorem 3.4. Then $a^1(x) | (g(x) + up_1(x) + \dots + u^{k-2}p_{k-2}(x)) \bmod u^{k-1}$ and $\frac{x^n - 1}{g(x)}[up_1(x) + \dots + u^{k-1}p_{k-1}(x)] \in \langle ua^1(x) \rangle$.

Proof : Let $ut(x) \in C = \langle g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x), ua^1(x) \rangle$ where $t(x) \in R_{k-1}[x; \theta]$. By division algorithm, we have $t(x) = q(x)a^1(x) + r(x)$ where $\deg(r(x)) < \deg(a^1(x))$ or $r(x) = 0$. Then $ut(x) = q'(x)ua^1(x) + ur(x)$ and hence $ur(x) \in C$. This is a contradiction unless $ur(x) = 0$, i.e., $r(x) = 0$. Therefore, $ut(x) = q'(x)ua^1(x) \in \langle ua^1(x) \rangle$. As a result, for any $ut(x) \in C$, we get $t(x) = q(x)a^1(x)$ and $ut(x) \in \langle ua^1(x) \rangle$. Note that $u(g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x)) = u(g(x) + up_1(x) + \dots + u^{k-2}p_{k-2}(x)) \in C$.

Hence, from the above discussion we conclude that $a^1(x) | (g(x) + up_1(x) + \dots + u^{k-2}p_{k-2}(x)) \bmod u^{k-1}$. Further,

$$\begin{aligned} & \frac{x^n - 1}{g(x)} [g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x)] \\ &= u \left[\left(\frac{x^n - 1}{g(x)} \right) p_1(x) + \dots + \left(\frac{x^n - 1}{g(x)} \right) u^{k-2}p_{k-1}(x) \right] \in C. \end{aligned}$$

Thus, $\frac{x^n - 1}{g(x)} [up_1(x) + \dots + u^{k-1}p_{k-1}(x)] \in \langle ua^1(x) \rangle$. $\square$

4. Minimal spanning set

In this section, we discuss the minimal spanning set of skew cyclic codes of length n for different cases as given in Theorem 3.2, 3.3 and 3.4, respectively. These sets will help to find the generator matrices and sizes of skew cyclic codes over R_k .

Theorem 4.1 : Let $C = \langle ua^1(x) \rangle$ be a non-zero skew cyclic code of length n over R_k where $a(x) = ua^1(x)$ is the polynomial of minimal degree r in C with $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$. Then $\Gamma = \{ua^1(x), xua^1(x), \dots, x^{n-r-1}ua^1(x)\}$ is a minimal generating set for C and $|C| = (p^{k-1})^{n-r}$.

Proof: Let $C = \langle ua^1(x) \rangle$ where $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$. Let $c(x) \in C$. Then $c(x) = j(x)ua^1(x)$. Let $j(x) = j_1(x) + u^{k-1}j_2(x)$ where $j_1(x) \in R_{k-1}[x; \theta]$, $j_2(x) \in \mathbb{F}_p[x]$. Then $c(x) = j(x)ua^1(x) = (j_1(x) + u^{k-1}j_2(x))ua^1(x) = uj_3(x)a^1(x)$, where $j_1(x)u = uj_3(x)$. If $\deg(j_3(x)) \leq (n-r-1)$, then $c(x) \in \text{span}(\Gamma)$. Otherwise, by division algorithm, we have $j_3(x) = q_1(x)\frac{x^n-1}{a^1(x)} + r_1(x)$, where $\deg(r_1(x)) < \deg(a^1(x)) = (n-r)$ or $r_1(x) = 0$. Therefore,

$$c(x) = uj_3(x)a^1(x) = u \left(q_1(x)\frac{x^n-1}{a^1(x)} + r_1(x) \right) a^1(x) = ur_1(x)a^1(x).$$

Since $\deg(r_1(x)) \leq (n-r-1)$, therefore, $c(x) \in \text{span}(\Gamma)$ and Γ generates C . Clearly none of the element of Γ is a linear combination of preceding elements. Therefore, Γ is the minimal generating set for C . Since $r_1(x) \in R_{k-1}$, $|C| = (p^{k-1})^{n-r}$. $\square$

Theorem 4.2 : Let $C = \langle g(x) \rangle$ be a non-zero skew cyclic code of length n where $g(x)$ is the monic polynomial of minimal degree r in C and $x^n - 1 = k(x)g(x)$ in $R_k[x; \theta]$. Then $\Gamma = \{g(x), xg(x), \dots, x^{n-r-1}g(x)\}$ is a minimal generating set for C and $|C| = (p^k)^{n-r}$.

Proof : Similar to the proof of Theorem 4.1. $\square$

Theorem 4.3: Let $C = \langle g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x), ua^1(x) \rangle$ be a non-zero skew cyclic code of length n over R_k where $a(x) = ua^1(x)$ is the polynomial of minimal degree t in C which is not monic, $g(x)$ is the polynomial of minimal degree r among all monic polynomials in C , $x^n - 1 = k(x)g(x)$ in $R_k[x; \theta]$ and $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$. Then $\Gamma = \{h(x), xh(x), \dots, x^{n-r-1}h(x), ua^1(x), xua^1(x), \dots, x^{r-t-1}ua^1(x)\}$ is a minimal generating set for C and $|C| = (p^k)^{n-r} (p^{k-1})^{r-t}$, where $h(x) = g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x)$.

Proof : Similar to the proof of Theorem 4.1, it is verified. $\square$

5. Encoding of skew cyclic codes over R_k

Now, we propose an encoding algorithm for skew cyclic codes of arbitrary length n over R_k as an application of Theorems 4.1, 4.2 and 4.3, respectively.

Theorem 5.1 : Let C be a skew cyclic code of length n over R_k .

Case I : If $C = \langle ua^1(x) \rangle$ where $a(x) = ua^1(x)$ is the polynomial of minimal degree r in C and $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$, then any codeword $c(x) \in C$ can be encoded as $c(x) = [t_0(x) + ut_1(x) + \dots + u^{k-2}t_{k-2}(x)]ua^1(x)$, where $t_0(x) + ut_1(x) + \dots + u^{k-2}t_{k-2}(x)$ is a polynomial of degree $\leq (n - r - 1)$ in $R_{k-1}[x; \theta]$.

Case II : If $C = \langle g(x) \rangle$ where $g(x)$ is the monic polynomial of minimal degree r in C and $x^n - 1 = k(x)g(x)$ in $R_k[x; \theta]$, then any codeword $c(x) \in C$ can be encoded as $c(x) = [t_0(x) + ut_1(x) + \dots + u^{k-1}t_{k-1}(x)]g(x)$, where $t_0(x) + ut_1(x) + \dots + u^{k-1}t_{k-1}(x)$ is a polynomial of degree $\leq (n - r - 1)$ in $R_k[x; \theta]$.

Case III : If $C = \langle g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x), ua^1(x) \rangle$ where $g(x)$ is the polynomial of minimal degree r among all monic polynomials in C , $a(x) = ua^1(x)$ is the polynomial of minimal degree τ in C , $x^n - 1 = b^1(x)a^1(x)$ in $R_{k-1}[x; \theta]$, $x^n - 1 = k(x)g(x)$ in $R_k[x; \theta]$, $a^1(x) | (g(x) + up_1(x) + \dots + u^{k-2}p_{k-2}(x)) \bmod u^{k-1}$ and $\frac{x^n - 1}{g(x)}[up_1(x) + \dots + u^{k-1}p_{k-1}(x)] \in \langle ua^1(x) \rangle$, then any codeword $c(x) \in C$ can be encoded as

$$c(x) = [t_0(x) + ut_1(x) + \dots + u^{k-1}t_{k-1}(x)](g(x) + up_1(x) + \dots + u^{k-1}p_{k-1}(x)) \\ + [j_0(x) + uj_1(x) + \dots + u^{k-2}j_{k-2}(x)]ua^1(x),$$

where $t_0(x) + ut_1(x) + \dots + u^{k-1}t_{k-1}(x)$ is a polynomial of degree $\leq (n-r-1)$ in $R_k[x; \theta]$ and $j_0(x) + uj_1(x) + \dots + u^{k-2}j_{k-2}(x)$ is a polynomial of degree $\leq (r-\tau-1)$ in $R_{k-1}[x; \theta]$.

Note that if a skew cyclic code C is in the form given in Theorem 3.4, we follow the encoding process, Case III of Theorem 5.1 and syndrome decoding process for decoding. Through an example, we validate the encoding and decoding algorithm for Case III of Theorem 5.1.

Example 5.2 : Let $k=3$ and $p=3$, $R_3 = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, $R_2 = \mathbb{F}_3 + u\mathbb{F}_3$ and automorphism θ on R_3 define by $\theta(u) = -u, \theta(1) = 1, \theta(0) = 0$. Take $n=6, r=4, \tau=2$ and $C = \langle x^4 + (1+u+u^2)x^2 - (u+u^2)x + (1+u+u^2), u(x^2-x+1) \rangle$. Suppose the sender wishes to transmit two strings $I = (1+u+2u^2, 2u+u^2) \in R_3^2$ and $J = (2+u, u) \in R_2^2$. Following Case III of Theorem 5.1, the sender encodes two strings I, J as

$$\text{Encode}(I, J) = ((1+u+2u^2)x + 2u+u^2)(x^4 + (1+u+u^2)x^2 - (u+u^2)x + \\ (1+u+u^2)) + u((2+u)x + u)(x^2 - x + 1) \\ = (1+u+2u^2)x^5 + (2u+u^2)x^4 + (1+2u)x^3 + ux^2 + (1+2u)x \\ + 2u+u^2.$$

Then the sender sends the encoded string $(1+u+2u^2, 2u+u^2, 1+2u, u, 1+2u, 2u+u^2)$ though an open channel. Due to noises appeared in the channel, suppose receiver received the string as $(1+u+2u^2, 2u+2u^2, 1+2u, u, 1+2u, 2u+u^2)$ (messages with some errors). Note that the number of symbols in input is 10 whereas in output is 18. Also, the receiver follows the syndrome decoding algorithm to retrieve the actual string (messages) which was sent by sender. Thus, a receiver should follow the following process.

$$t_1(x) + ut_2(x) + u^2t_3(x) = (1+u+2u^2)x^5 + (2u+2u^2)x^4 + (1+2u)x^3 + ux^2 \\ + (1+2u)x + 2u+u^2.$$

which gives $t_1(x) = x^5 + x^3 + x$, $t_2(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2$ and $t_3(x) = 2x^5 + 2x^4 + 1$. Therefore, syndromes are given by

$$e_1(x) = t_1(x)(x^2 - 1) = 0; e_2(x) = t_2(x)(x^4 + x^3 - x - 1) = 0; \\ e_3(x) = t_3(x)(x^4 + x^3 - x - 1) = x + x^2 - x - x^5.$$

Moreover, $x^4(x^4 + x^3 - x - 1) = x + x^2 - x - x^5$. Thus, $e_3(x)$ is the syndrome of x^4 . Consequently, the receiver can detect the error term u^2x^4 . By applying division algorithm, receiver obtains the strings I and J as follows:

$$\begin{aligned} & (1+u+2u^2)x^5 + (2u+u^2)x^4 + (1+2u)x^3 + ux^2 + (1+2u)x + 2u + u^2 \\ &= ((1+u+2u^2)x + 2u + u^2)(x^4 + (1+u+u^2)x^2 - (u+u^2)x + (1+u+u^2)) \quad (1) \\ &+ u((2+u)x + u)(x^2 - x + 1). \end{aligned}$$

Hence, the receiver can extract I and J from equation (1).

6. Gray map and optimal linear codes

We consider the Gray map $\phi: R_t \rightarrow \mathbb{F}_p^t$ from [3] defined by

$$\begin{aligned} & \phi(a_0 + ua_1 + \dots + u^{t-1}a_{t-1}) \\ &= (a_0 + a_1 + \dots + a_{t-1}, a_1 + \dots + a_{t-2} + a_{t-1}, \dots, a_{t-2} + a_{t-1}, a_{t-1}) \end{aligned}$$

where $a_i \in \mathbb{F}_p$ for $i = 0, 1, \dots, t-1$. In [3], it is proved that ϕ is a distance preserving $\mathbb{F}_p$ -linear map from $(R_t, \text{Lee weight})$ to $(\mathbb{F}_p^t, \text{Hamming Weight})$. For $t > 1$, clearly ϕ is a one-to-one map. Moreover, if C is a linear code over R_t with parameters $[n, M, d]$, then $\phi(C)$ is a linear code over $\mathbb{F}_p$ with parameters $[nt, M, d]$. Further, if C is a free code with dimension k , then $\phi(C)$ is also free with dimension tk over $\mathbb{F}_p$. In the present section, we consider principally generated free skew cyclic codes over R_t as given in Theorem 3.3. Further, to obtain p -ary optimal codes, we take Gray images of these codes. The calculations are carried out by using the Magma software [4]. According to the online database [9], here we obtain some optimal linear codes.

Example 6.1 : Let $R_2 = \mathbb{F}_3 + u\mathbb{F}_3$ where $u^2 = 0$. The automorphism θ on R_2 is define by $\theta(a+ub) = a-ub$ for $a, b \in \mathbb{F}_3$. Now, the polynomial $g(x) = x^3 + (1+u)x^2 + x + 1 + u$ is a right divisor of $x^4 - 1$ in $R_2[x; \theta]$. Then $C = \langle g(x) \rangle$ is a free skew linear code of length 4 and dimension 1 over R_2 . Therefore, $\phi(C)$ is a linear code with parameters $[8, 2, 6]$ over $\mathbb{F}_3$ and it is an optimal linear code as per the database [9].

Example 6.2 : Let $R_2 = \mathbb{F}_5 + u\mathbb{F}_5$ where $u^2 = 0$. The automorphism θ on R_2 is define by $\theta(a+ub) = a-ub$ for $a, b \in \mathbb{F}_5$. Now, the polynomial $g(x) = x + 1 + 3u$ is a right divisor of $x^2 - 1$ in $R_2[x; \theta]$. Then $C = \langle g(x) \rangle$ is a free skew linear code of length 2 and dimension 1 over R_2 . Therefore,

$\phi(C)$ is a linear code with parameters $[4, 2, 3]$ over $\mathbb{F}_5$ which is an optimal linear code as per the database [9].

References

- [1] T. Abualrub and I. Siap, Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, *Des. Codes Cryptogr.* 42(3) (2007), pp. 271-287.
- [2] T. Abualrub, N. Aydin and P. Seneviratne, On θ -cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, *Austr. J. Combin.* 54 (2012), pp. 115-126.
- [3] A. Alahmadi, A. Alkenani, R. Alomari, N. Muthana, P. Sole and B. Yildiz, Comparison of the Lee and homogenous weights over a family of chain rings, *Bull. Korean Math. Soc.* 55(2) (2018), pp. 633-647.
- [4] W. Bosma and J. Cannon, Handbook of Magma Functions, Univ. of Sydney, (1995).
- [5] D. Boucher, W. Geiselmann and F. Ulmer, Skew cyclic codes, *Appl. Algebra Eng. Comm.* 18(4) (2007), pp. 379-389.
- [6] D. Boucher and F. Ulmer, Coding with skew polynomial rings, *J. Symb. Comput.* 44(12) (2009), pp. 1644-1656.
- [7] R. Dastbasteh, H. Mousavi, T. Abualrub, N. Aydin and J. Haghighat, Skew cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$, *Int. J. Inf. Coding Theory* 5(1) (2018), pp. 81-99.
- [8] J. Gao, Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, *J. Appl. Math. Inform.* 31(3-4) (2013), pp. 337-342.
- [9] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at <http://www.codetables.de>, Accessed on 2021-08-02.
- [10] F. Gursoy, I. Siap and B. Yildiz, Construction of skew cyclic codes over $F_q + vF_q$, *Adv. Math. Commun.* 8(3) (2014), pp. 313-322.
- [11] H. Islam and O. Prakash, Skew cyclic and skew $(\alpha_1 + u\alpha_2 + v\alpha_3 + uv\alpha_4)$ -constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, *Int. J. Inf. Coding Theory* 5(2) (2018), pp. 101-116.
- [12] H. Islam and O. Prakash, A study of cyclic and constacyclic codes over $\mathbb{Z}_4 + \mathbb{Z}_4 + v\mathbb{Z}_4$, *Int. J. Inf. Coding Theory* 5(2) (2018), pp. 155-168.
- [13] H. Islam and O. Prakash, A note on skew constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, *Discrete Math. Algorithms Appl.* 11(03) (2019), 1950030.

- [14] H. Islam and O. Prakash, A class of constacyclic codes over the ring $\mathbb{Z}_4[u, v] / \langle u^2, v^2, uv - vu \rangle$ and their Gray images, *Filomat* 33(8) (2019), pp. 2237-2248.
- [15] H. Islam, O. Prakash and R. K. Verma, A family of constacyclic codes over $\mathbb{F}_{p^m}[v, w] / \langle v^2 - 1, w^2 - 1, vw - wv \rangle$. *Int. J. Inf. Coding Theory* 5(3-4) (2020), pp. 198-210.
- [16] H. Islam, O. Prakash and R. K. Verma, New quantum codes from constacyclic codes over the ring $R_{k,m}$, *Adv. Math. Commun.* (2020), doi: 10.3934/amc.2020097.
- [17] H. Islam and O. Prakash, New quantum codes from constacyclic and additive constacyclic codes, *Quantum Inf. Process.* 19(9) (2020), pp. 1-17.
- [18] H. Islam and O. Prakash, New $\mathbb{Z}_4$ codes from constacyclic codes over a non-chain ring, *Comp. Appl. Math.* 40(12) (2021), <https://doi.org/10.1007/s40314-020-01398-y>.
- [19] H. Islam, E. Martínez-Moro and O. Prakash, Cyclic codes over a non-chain ring $R_{e,q}$ and their application to LCD codes, *Discrete Math.* 344(10) (2021), <https://doi.org/10.1016/j.disc.2021.112545>.
- [20] H. Islam and O. Prakash, Construction of reversible cyclic codes over $\mathbb{Z}_{p^k}$, *J. Discrete Math. Sci. Cryptogr.* (2021), doi : 10.1080/09720529.2020.1815341.
- [21] S. Jitman, S. Ling and P. Udomkavanich, Skew constacyclic codes over finite chain ring, *Adv. Math. Commun.* 6 (2012), pp. 39-63.
- [22] B. R. McDonald, *Finite Rings With Identity*, Marcel Dekker Inc., New York (1974).
- [23] Pankaj and M. Pruthi, Cyclic codes from Whiteman's generalized cyclotomic sequences of order $2^r, r \geq 2$, *J. Inf. Optim. Sci.* 38(3-4) (2017), pp. 621-646.
- [24] Pankaj and M. Pruthi, Cyclic codes of prime power length from generalized cyclotomic classes of order 2^r , *J. Inf. Optim. Sci.* 39(4) (2018), pp. 965-971.
- [25] O. Prakash, H. Islam, S. Patel and P. Solé, New Quantum Codes from Skew Constacyclic Codes Over a Class Of Non-Chain Rings $R_{e,q}$, *Internat. J. Theoret. Phys.* (2021), <https://doi.org/10.1007/s10773-021-04910-0>.

- [26] O. Prakash, H. Islam and S. Das, On cyclic codes with minimal generating sets over the ring $\mathbb{Z}_{p^k}$, *Southeast Asian Bull. Math.* 45(4) (2021), pp. 521-532.
- [27] M. Pruthi and S. Kumar, Cyclic codes with generalized cyclotomic cubic classes, *J. Discrete Math. Sci. Cryptogr.* 22(6) (2019), 923-933.
- [28] I. Siap, T. Abualrub, N. Aydin and P. Seneviratne, Skew cyclic codes of arbitrary length, *Int. J. Inf. Coding Theory* 2(1) (2011), pp.10-20.
- [29] A. K. Singh and P. K. Kewat, On cyclic codes over the ring $\mathbb{Z}_p[u]/\langle u^k \rangle$, *Des. Codes Cryptogr.* 74(1) (2015), pp. 1-13.

Received April, 2021

Revised October, 2021