DOI: 10.2478/auom-2024-0029
An. Şt. Univ. Ovidius Constanţa **Vol. 32(3),2024, 75–87**

Two-dimensional cyclic codes over a finite chain ring

Disha Garg and Sucheta Dutt

Abstract

In this paper, we have determined the generators and rank of a 2D cyclic code of length mn over a finite chain ring $\mathfrak{R}$ with residue field $\mathbb{F}_q$, where m is arbitrary and $q \equiv 1(mod\ n)$. Further, we have obtained a necessary and sufficient condition for a 2D cyclic code over a finite chain ring $\mathfrak{R}$ to be MHDR. Some examples of 2D cyclic codes have been constructed and ranks of these 2D cyclic codes have been calculated by us. We have also given a few examples of 2D cyclic codes over some finite chain rings, which are MHDR.

1 Introduction

The class of two-dimensional (2D) cyclic codes is an important class of error-correcting codes. These codes have been extensively studied over the past few decades due to their wide applications in various digital communication systems where reliable transformation of information is critical.

The basic theory of 2D cyclic codes was introduced by H. Imai [8] in 1977. Later, the relation between 2D cyclic codes and quasi-cyclic codes was established by C. Gneri and F. zbudak [7]. In 2016, 2D cyclic codes of length $n = s2^k$ over the finite field $\mathbb{F}_{p^m}$ were characterized as ideals of the quotient ring $\mathbb{F}_{p^m}[x, y]/\langle x^s - 1, y^{2^k} - 1\rangle$ for an odd prime p by Z. Sepasdar and K. Khashyarmanesh [11]. Using a similar approach, the algebraic structure of repeated root 2D constacyclic codes of length $2p^s2^k$ over a finite field $\mathbb{F}_{p^m}$

Key Words: Cyclic codes, 2D codes, Finite chain ring, Hamming distance.
2010 Mathematics Subject Classification: Primary 94B15; Secondary 94B05.
Received: 18.08.2023
Accepted: 24.12.2023

was characterized by Z. Rajabai and K. Khashyarmanesh [10]. The generator matrix of a 2D cyclic code of arbitrary length was determined by Z. Sepasdar [12] using another approach. Recently, using the concept of central primitive idempotents, a new form of generator polynomials of two-dimensional (α, β)-constacyclic codes of arbitrary length sl has been established by S. Bhardwaj and M. Raka [2].

The class of MHDR (Maximum Hamming distance with respect to rank) cyclic codes is an important subclass of cyclic codes. These codes have been studied extensively in literature [1, 4, 5, 6, 13].

This paper is organized as follows: In Section 2, we state some basic definitions and preliminary results on cyclic codes and 2D cyclic codes over finite chain rings. In section 3, we obtain the generators and the rank of a 2D cyclic code of length mn over a finite chain ring, where m is arbitrary and n is co-prime to the cardinality of the residue field of the finite chain ring. We also provide some examples of such 2D cyclic codes. In section 4, we give a condition for a 2D cyclic code to be MHDR over the finite chain ring. We also provide some examples of 2D cyclic codes over some finite chain rings, which are MHDR.

2 Preliminaries

Let R be a finite commutative ring. A code C of length t over R is called a linear code if it is a submodule of R^t over R. A linear code C of length t over R is known to be cyclic if $\tau(b) \in C$ for every $b \in C$, where τ is the usual cyclic shift operator over R^t defined by $\tau(r_0, r_1, \dots, r_{t-1}) = (r_{t-1}, r_0, r_1, \dots, r_{t-2})$. It is well established that a cyclic code C of length t over R can be viewed as an ideal of $R[x]/\langle x^t - 1\rangle$. Let $c = \left[r_{ij}\right],\ 0 \le i \le m-1,\ 0 \le j \le n-1,\ r_{ij} \in R$ be a $m \times n$ array over R. Then, the row cyclic shift of c, denoted by τ_r is defined by $\tau_r \begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{m-1} \end{pmatrix} = \begin{pmatrix} r_{m-1} \\ r_0 \\ \vdots \\ r_{m-2} \end{pmatrix}$, where r_i denotes the i^{th} row of c for $0 \le i \le m-1$. Further, the column shift of c, denoted by τ_c is defined by $\tau_c(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, \dots, c_{n-2})$,where c_j denotes the j^{th} column of c for $0 \le j \le n-1$. A linear code $\mathcal{C}$ of length mn over R is called a 2D cyclic code if its codewords, viewed as $m \times n$ arrays of the form $c = \left[r_{ij}\right],\ 0 \le i \le m-1,\ 0 \le j \le n-1,\ r_{ij} \in R$, are closed under both row and column cyclic shifts. It is easy to check that a 2D cyclic code $\mathcal{C}$ of length mn over R can be viewed as an ideal of the ring $R[x, y]/\langle x^m - 1, y^n - 1\rangle$.

For any two codewords, $c = \left[c_{ij}\right], c' = \left[c'_{ij}\right],\ 0 \le i \le m-1,\ 0 \le j \le n-1$

in a 2D cyclic code $\mathcal{C}$, the Hamming distance between c and c' is given by $d_H(c,c') = \sum_{j=0}^{n-1}\sum_{i=0}^{m-1} d_H(c_{ij},c'_{ij})$, where $d_H(c_{ij},c'_{ij}) = \begin{cases} 0 & \text{if } c_{ij}=c'_{ij} \\ 1 & \text{if } c_{ij}\neq c'_{ij} \end{cases}$. The minimum Hamming distance of $\mathcal{C}$ is given by $d_H(\mathcal{C}) = \min_{c\neq c'} d_H(c,c')$. Also, the Hamming weight of a codeword $c = \left[c_{ij}\right] \in \mathcal{C}$, denoted by $w_H(c)$, is number of non zero c_{ij} and the minimum Hamming weight of $\mathcal{C}$ is given by $w_H(\mathcal{C}) = \min_{c\in\mathcal{C}} w_H(c)$. Clearly, $d_H(\mathcal{C}) = w_H(\mathcal{C})$. The rank of $\mathcal{C}$ is defined to be the cardinality of the minimal spanning set of $\mathcal{C}$. The code $\mathcal{C}$ is called MHDR if $d_H(\mathcal{C}) = mn - Rank(\mathcal{C}) + 1$.

An element $\omega \in R$ is called primitive n^{th} root of unity if n is the smallest positive integer such that $\omega^n = 1$. An element $x \in R$ is called an idempotent element if $x^2 = x$. Moreover, the idempotents of a commutative ring R with unity are called primitive idempotents if and only if they are pairwise orthogonal and their sum is equal to the unity of the ring.

If all ideals of a finite commutative ring R form a chain under inclusion operation, then R is said to be a finite chain ring. All ideals of a finite chain ring are principally generated. Moreover, there exists a unique maximal ideal in a finite chain ring. Let $\mathfrak{R}$ be a finite chain ring and $\langle\gamma\rangle$ be its maximal ideal. Let ν be the nilpotency index of γ and $\mathfrak{R}/\langle\gamma\rangle = \mathbb{F}_q$, where $q = p^r$. The set $T = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$, where $\xi \in \mathfrak{R}$ is an element such that $\xi^{p^r-1} = 1$, is called the Teichmuller set of $\mathfrak{R}$. The map $^- : \mathfrak{R} \longrightarrow \mathbb{F}_q$ defined as $\bar{r} = r(mod\,\gamma)$ is an onto-ring homomorphism which can be naturally extended as a map from the polynomial ring $\mathfrak{R}[x]$ to $\mathbb{F}_q[x]$.
We state below some well-established results which are required for later use.

Theorem 1. *[9] Let $g(x) \in \mathfrak{R}[x]$ be a monic polynomial such that $\bar{g}(x) = f_1(x)f_2(x)\ldots f_m(x)$, where $f_i(x) \in \mathbb{F}_q[x]$ are pairwise coprime monic polynomials for $1 \leq i \leq m$. Then there exist monic, pairwise coprime polynomials $g_i(x) \in \mathfrak{R}[x]$ such that $g(x) = g_1(x)g_2(x)\ldots g_m(x)$.*

Theorem 2. *[9] Let $\mathfrak{R}$ be a finite chain ring and $g(x) \in \mathfrak{R}[x]$ be a monic polynomial. Then $g(x)$ factors uniquely in $\mathfrak{R}[x]$ if $\bar{g}(x)$ is square free.*

The structure of a cyclic code C over a finite chain ring $\mathfrak{R}$ has been determined by Monika et al. [3, 4]. We reproduce below the relevant results from [3, 4], which we shall require for determining the structure of a 2D cyclic code over $\mathfrak{R}$.

Theorem 3. *[3, 4] Let $\mathcal{C}$ be a cyclic code of length n over a finite chain ring $\mathfrak{R}$. Then, there exists a positive integer r such that $\mathcal{C} = \langle p_0(x),\ p_1(x), \ldots,\ p_r(x)\rangle$, where $p_j(x) = \gamma^{s_j} q_j(x)$ is the minimal degree polynomial among all the polynomials in $\mathcal{C}$ whose leading coefficient is γ^{s_j} for $0 \leq j \leq r$. Also, $q_j(x)$*

is a monic polynomial in $\mathfrak{R}^j[x]/\langle x^n - 1\rangle$*, where* $\mathfrak{R}^j$ *is the finite chain ring* $\mathbb{F}_q + \gamma\mathbb{F}_q + \gamma^2\mathbb{F}_q + \cdots + \gamma^{\nu-s_j-1}\mathbb{F}_q$ *for* $0 \leq j \leq r$*,* $s_0 > s_1 > \cdots > s_r$ *and* $t_0 < t_1 < \cdots < t_r$*, where* $t_j = deg(p_j(x))$*. Moreover, the polynomials* $p_j(x)$ *can be uniquely expressed as* $p_j(x) = \gamma^{s_j}\sum_{k=0}^{\nu-s_j-1}\gamma^k h_{j,k}(x)$*, where* $h_{j,k}(x) \in T(x)$*,* $h_{j,0}(x) = \overline{q_j(x)}$ *and* $deg(h_{j,0}(x)) = t_j$*.*

Corollary 1. *[3] A cyclic code of arbitrary length over* $\mathfrak{R}$ *is generated by at most* $k = min\{\nu, t_r + 1\}$ *elements.*

Theorem 4. *[4] Let* $\mathcal{C} = \langle p_0(x),\ p_1(x), \ldots,\ p_r(x)\rangle$ *be a cyclic code of length* n *over a finite chain ring* $\mathfrak{R}$ *where,* $p_j(x) = \gamma^{s_j}q_j(x)$ *such that* $\nu - 1 \geq s_0 > s_1 > \cdots > s_r$ *and* $t_0 < t_1 < \cdots < t_r$*, where* $t_j = deg(p_j(x))$*. Then the rank of* $\mathcal{C}$ *is* $n - t_0$ *and the minimal spanning set is given by* $S = \{p_0(x), xp_0(x), \ldots x^{t_1-t_0-1}p_0(x), p_1(x), xp_1(x), \ldots x^{t_2-t_1-1}p_1(x), \ldots, p_r(x), xp_r(x), \ldots x^{n-t_r-1}p_r(x)\}$*.*

The generators and the dimension of a 2D (α, β)-constacyclic codes of arbitrary length $s.l$ over a finite field $\mathbb{F}_q$ have been determined by S. Bhardwaj and M.Raka [2]. We replicate below the appropriate result from [2], which we shall require for further use.

Lemma 1. *[2] Let* C *be a 2D* (α, β)*-constacyclic codes of length* sl *over a finite field* $\mathbb{F}_q$*, where* s *is arbitrary and* $l \equiv 1(mod\ q)$*. Then,* C *is generated by* $\langle \eta_0(y)p_0(x), \eta_1(y)p_1(x), \ldots, \eta_{l-1}(y)p_{l-1}(x)\rangle$*, where* $\eta_i(y)$ *are primitive central idempotents in* $\mathbb{F}_q[y]/\langle y^l - \beta\rangle$ *and* $deg(p_i(x)) = a_i$*. Also, the dimension of* C *is* $sl - a_0 - a_1 - \cdots - a_{l-1}$*.*

3 Structure and rank of a 2D cyclic code over a finite chain ring

In this section, we obtain the generators of a 2D cyclic code of length mn over a finite chain ring $\mathfrak{R}$ with residue field $\mathbb{F}_q$, where m is arbitrary and $q \equiv 1(mod\ n)$. We also determine the rank of such 2D cyclic codes over $\mathfrak{R}$.

Lemma 2. *Let* $\mathfrak{R}$ *be a finite chain ring. Then,*

(1) There exists an element $\zeta \in \mathfrak{R}$ *which is a primitive* n^{th} *root of unity.*

(2) The elements $\theta_i(y) = \frac{1}{n}(1 + \zeta^{n-i}y + (\zeta^{n-i}y)^2 + \cdots + (\zeta^{n-i}y)^{n-1})$ *for* $0 \leq i \leq n-1$ *are primitive idempotents of* $\mathfrak{R}[y]/\langle y^n - 1\rangle$*. Moreover,* $\theta_i(y)y^j = (\zeta^i)^j\theta_i(y)$ *for* $0 \leq i,\ j \leq n-1$*.*

Proof. Consider the ring $\mathbb{F}_q[y]/\langle y^n - 1\rangle$; where $\mathbb{F}_q$ is the residue field of $\mathfrak{R}$ and $q \equiv 1(mod n)$. Let $\omega \in \mathbb{F}_q$ be a primitive n^{th} root of unity. Then

$$y^n - 1 = (y-1)(y-\omega)(y-\omega^2)\dots(y-\omega^{n-1}) \text{ in } \mathbb{F}_q(y)$$

Let $\bar{\zeta} = \omega$ for some $\zeta \in \mathfrak{R}$. By Theorem 1 and Theorem 2, it is easy to see that $y^n - 1 = (y-1)(y-\zeta)(y-\zeta^2)\dots(y-\zeta^{n-1})$ in $\mathfrak{R}_q(y)$, so that ζ is a primitive n^{th} root of unity in $\mathfrak{R}$. This proves (1).
It can be easily proved that $\theta_i(y) = \frac{1}{n}(1+\zeta^{n-i}y+(\zeta^{n-i}y)^2+\cdots+(\zeta^{n-i}y)^{n-1}) = \prod_{j\neq i}\frac{(y-\zeta^j)}{(\zeta^i-\zeta^j)}$ for $0 \le i \le n-1$ and $\theta_i(y)\theta_j(y) = 0$ in $\mathfrak{R}[y]/\langle y^n - 1\rangle$ for $i \neq j$. Further, $\prod_{j\neq i}(y-\zeta^j)$ divides $\theta_i(y)$ and $\theta_i(\zeta^i) = 1$ which implies that $y - \zeta^i$ divides $\theta_i(y) - 1$. It follows that $\theta_i(y)(\theta_i(y) - 1) = 0$ in $\mathfrak{R}[y]/\langle y^n - 1\rangle$, so that $\theta_i^2(y) = \theta_i(y)$. Also, $\theta_i(\zeta^j) = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$ implies that $\theta_0(\zeta^i) + \theta_1(\zeta^i) + \cdots + \theta_{n-1}(\zeta^i) = 1$ for $0 \le i \le n-1$, which further implies that $(y-\zeta^i) \mid \theta_0(y) + \theta_1(y) + \cdots + \theta_{n-1}(y) - 1$ for $0 \le i \le n-1$. Hence $\theta_0(y) + \theta_1(y) + \cdots + \theta_{n-1}(y) = 1$ in $\mathfrak{R}[y]/\langle y^n - 1\rangle$. Therefore, $\theta_i(y),\ 0 \le i \le n-1$, are primitive idempotents in $\mathfrak{R}[y]/\langle y^n - 1\rangle$. Also, $\theta_i(y)y = \frac{1}{n}(y + \zeta^{n-i}y^2 + \zeta^{2(n-i)}y^3 + \cdots + \zeta^{(n-1)(n-i)}y^n) = \frac{1}{n}(\zeta^i + y + \zeta^{n-i}y^2 + \cdots + \zeta^{(n-2)(n-i)}y^{n-1}) = \frac{\zeta^i}{n}(1+\zeta^{n-i}y+(\zeta^{n-i}y)^2+\cdots+(\zeta^{n-i}y)^{n-1}) = \zeta^i\theta_i(y)$. It follows that $\theta_i(y)y^j = (\theta_i(y)y)y^{j-1} = (\zeta^i\theta_i(y))y^{j-1} = \cdots = (\zeta^i)^j\theta_i(y)$ for $0 \le i,\ j \le n-1$. This proves (2).

□

Remark 1. *In the proof of the Lemma 2 above, we have used Theorem 1 and Theorem 2 to establish the existence of a primitive n^{th} root of unity ζ in $\mathfrak{R}$. However, it can be easily checked that if ω is primitive n^{th} root of unity in the residue field $\mathbb{F}_q$ of $\mathfrak{R}$, then $\zeta = \omega^{\gamma^{\nu-1}}$ is primitive n^{th} root of unity in $\mathfrak{R}$.*

Let $\theta_j(y) = \frac{1}{n}(1+\zeta^{n-j}y+(\zeta^{n-j}y)^2+\cdots+(\zeta^{n-j}y)^{n-1}),\ 0 \le j \le n-1$ be the primitive idempotents in the ring $\mathfrak{R}[y]/\langle y^n - 1\rangle$. Define the sets $C_j = \{g_j(x) \in \mathfrak{R}[x]/\langle x^m - 1\rangle \mid g_j(x)\theta_j(y) \in \mathcal{C}\};\ 0 \le j \le n-1$. It can be easily verified that each C_j is an ideal of the ring $\mathfrak{R}[x]/\langle x^m - 1\rangle$ for $0 \le j \le n-1$ and therefore a cyclic code of length m over $\mathfrak{R}$. By Theorem 3, there exist polynomials $p_i^{(j)}(x) = \gamma^{s_i^{(j)}} q_i^{(j)}(x) = \gamma^{s_i^{(j)}} \sum_{k=0}^{\nu-s_i^{(j)}-1} \gamma^k h_{i,k}^{(j)}(x) \in \mathfrak{R}[x]/\langle x^m - 1\rangle$, where $p_i^{(j)}(x)$ is the minimal degree polynomial among all the polynomials in C_j whose leading coefficient is $\gamma^{s_i^{(j)}}$ for $0 \le i \le r_j$ and $\nu - 1 \ge s_0^{(j)} > s_1^{(j)} > \cdots > s_{r_j}^{(j)}$ such that $C_j = \langle p_0^{(j)}(x),\ p_1^{(j)}(x)\dots,\ p_{r_j}^{(j)}(x)\rangle;\ 0 \le j \le n-1$.

Let $f(x,y) \in \mathcal{C}$, where $\mathcal{C}$ is a 2D cyclic code of length mn over a finite chain ring $\mathfrak{R}$. Clearly, $f(x,y)$ can be written as $\sum_{i=0}^{n-1} f_i(x)y^i$, where $f_i(x) \in$

$\mathfrak{R}[x]/\langle x^m-1\rangle$ for $0\le i\le n-1$. Now, $\theta_j(y)f(x,y)=\theta_j(y)\sum_{i=0}^{n-1}f_i(x)y^i=\sum_{i=0}^{n-1}f_i(x)y^i\theta_j(y)=\sum_{i=0}^{n-1}f_i(x)(\zeta^j)^i\theta_j(y)=\theta_j(y)f(x,\zeta^j)$ (by Lemma 2).

It follows by definition of C_j that $f(x,\zeta^j)\in C_j,\ 0\le j\le n-1$. Therefore, $f(x,\zeta^j)=p_0^{(j)}(x)t_0^{(j)}(x)+p_1^{(j)}(x)t_1^{(j)}(x)+\cdots+p_{r_j}^{(j)}(x)t_{r_j}^{(j)}(x)$ for some $t_i^{(j)}(x)\in\mathfrak{R}[x]/\langle x^m-1\rangle$. Also, we have $f(x,y)=f(x,y)\sum_{j=0}^{n-1}\theta_j(y)=\sum_{j=0}^{n-1}\theta_j(y)f(x,\ \zeta^j)=\sum_{j=0}^{n-1}\theta_j(y)[p_0^{(j)}(x)t_0^{(j)}(x)+p_1^{(j)}(x)t_1^{(j)}(x)+\cdots+p_{r_j}^{(j)}(x)t_{r_j}^{(j)}(x)]$. Thus, the set $\{\theta_j(y)p_i^{(j)}(x)\mid 0\le i\le r_j,\ 0\le j\le n-1\}$ generates $\mathcal{C}$.

We record these observations below in the form of a theorem.

Theorem 5. *Let $\mathcal{C}$ be a 2D cyclic code of length mn over a finite chain ring $\mathfrak{R}$ with residue field $\mathbb{F}_q$, where m is arbitrary and $q\equiv 1(mod\ n)$. Then the set $\{\theta_j(y)p_i^{(j)}(x)\mid 0\le i\le r_j,\ 0\le j\le n-1\}$ generates $\mathcal{C}$ where, $\theta_j(y)$ are primitive idempotents of $\mathfrak{R}[y]/\langle y^n-1\rangle$ and $p_i^{(j)}(x),\ 0\le i\le r_j$ are the generators of the cyclic code $C_j=\{g_j(x)\in\mathfrak{R}[x]/\langle x^m-1\rangle\mid g_j(x)\theta_j(y)\in\mathcal{C}\},\ 0\le j\le n-1$.*

The following result is an immediate consequence of Theorem 5 and Corollary 1.

Corollary 2. *The number of generators of a 2D cyclic code $\mathcal{C}$ over $\mathfrak{R}$ is at most kn where $k=\sum_{j=0}^{n-1}(r_j+1)$, where $r_j+1\le min(\nu,\ t_{r_j})$ for each j, $0\le j\le n-1$ and $t_{r_j}^{(j)}=deg(p_{r_j}^{(j)}(x))$.*

Theorem 6. *Let $\mathcal{C}$ be a 2D cyclic code of length mn over a finite chain ring $\mathfrak{R}$ generated by the set $\{\theta_j(y)p_i^{(j)}(x)\mid 0\le i\le r_j,\ 0\le j\le n-1\}$ as given in Theorem 5. Then, the minimal spanning set of $\mathcal{C}$ is given by $A=\bigcup_{j=0}^{n-1}\bigcup_{i=0}^{r_j}A_{i,j}$, where $A_{i,j}=\{p_i^{(j)}(x)\theta_j(y),xp_i^{(j)}(x)\theta_j(y),\dots x^{t_{i+1}^{(j)}-t_i^{(j)}-1}p_i^{(j)}(x)\theta_j(y)\}$. Further, $Rank(\mathcal{C})=mn-\sum_{j=0}^{n-1}t_0^{(j)}$, where $t_i^{(j)}=deg(p_i^{(j)}(x))$ and $t_{r_j+1}=m$.*

Proof. Let $f(x,y)\in\mathcal{C}$ be any element. Proceeding as in the proof of Theorem 5, we have $f(x,y)=\sum_{j=0}^{n-1}f(x,\zeta^j)\theta_j(y)$, where $f(x,\zeta^j)\in C_j$. By Theorem 4, the set, $S_j=\{p_0^{(j)}(x),\ xp_0^{(j)}(x),\dots,x^{t_1^{(j)}-t_0^{(j)}-1}p_0^{(j)}(x),\ p_1^{(j)}(x),\ xp_1^{(j)}(x),\dots,x^{t_2^{(j)}-t_1^{(j)}-1}p_1^{(j)}(x),\dots,p_{r_j}^{(j)}(x),\ xp_{r_j}^{(j)}(x),\dots x^{m-t_r^{(j)}-1}p_{r_j}^{(j)}(x)\}$ is the minimal spanning set of C_j. Therefore $f(x,\zeta^j)\in Span(S_j)$ and hence $f(x,y)\in Span(A)$. Now, we will prove that no element of the set A can be written as a linear combination of other elements of A . If possible, let there exists $c_{i,k}^{(j)}\in\mathfrak{R}$ such that $x^{m-t_{r_j}^{(j)}-1}p_{r_j}^{(j)}(x)\theta_j(y)=\sum_{j=0}^{n-1}\big(\sum_{i=0}^{r_j-1}(c_{i,0}^{(j)}p_i^{(j)}(x)\theta_j(y)+$

$c_{i,1}^{(j)} x p_i^{(j)}(x)\theta_j(y) + \cdots + c_{i,t_{i+1}^{(j)}-t_i-1}^{(j)} x^{t_{i+1}^{(j)}-t_i^{(j)}-1} p_i^{(j)}(x)\theta_j(y)) + c_{r_j,0}^{(j)} p_{r_j}^{(j)}(x)\theta_j(y) + c_{r_j,1}^{(j)} x p_{r_j}^{(j)}(x)\theta_j(y) + \cdots + c_{r_j,m-t_{r_j}^{(j)}-2}^{(j)} x^{m-t_{r_j}^{(j)}-2} p_{r_j}^{(j)}(x)\theta_j(y))$
$= \sum_{j=0}^{n-1}\sum_{i=0}^{r_j} c_i^{(j)}(x) p_i^{(j)}(x)\theta_j(y)$, where $c_i^{(j)}(x) = c_{i,0} + c_{i,1}x + \cdots + c_{i,t_{i+1}^{(j)}-t_i^{(j)}-1} x^{t_{i+1}^{(j)}-t_i^{(j)}-1}$, $0 \le i \le r_j - 1$ and $c_{r_j}^{(j)}(x) = c_{r_j,0} + c_{r_j,1}x + \cdots + c_{r_j,m-t_{r_j}^{(j)}-2} x^{m-t_{r_j}^{(j)}-2}$. Substituting $y = \zeta^j,\ 0 \le j \le n-1$ and using $\theta_j(\zeta^j) = 1,\ \theta_j(\zeta^k) = 0$ for $k \ne j$, we get $x^{m-t_{r_j}^{(j)}-1} p_{r_j}^{(j)}(x) = \sum_{i=0}^{r_j} c_i^{(j)}(x) p_i^{(j)}(x)$. Multiplying by $\gamma^{\nu - s_{r_j-1}^{(j)}}$, we get $x^{m-t_{r_j}^{(j)}-1}\gamma^{\nu-s_{r_j-1}^{(j)}} p_{r_j}^{(j)}(x) = c_{r_j}^{(j)}(x)\gamma^{\nu-s_{r_j-1}^{(j)}} p_{r_j}^{(j)}(x)$. Which is not possible, as the degree of L.H.S of the last equation is $m-1$ whereas the degree of R.H.S is at most $m-2$. Therefore, $x^{m-t_{r_j}^{(j)}-1} p_{r_j}^{(j)}(x)$ can not be written as a linear combination of other elements of A. Using the similar arguments $x^{t_{i+1}^{(j)}-t_i^{(j)}-1} p_i^{(j)}(x),\ 0 \le i \le r_j - 1$ can not be written as a linear combination of other elements of A. Therefore, set A is minimal spanning set of $\mathcal{C}$ and hence $Rank(\mathcal{C}) = mn - \sum_{j=0}^{n-1} t_0^{(j)}$. □

Following are some examples of 2D cyclic codes over some finite chain rings.

Example 1. *Consider the finite chain ring $\mathfrak{R} = \mathbb{Z}_{25}$ with residue field $\mathbb{F}_5$ and nilpotency index 2. Let $\mathcal{C}$ be 2D cyclic code of length mn over $\mathfrak{R}$, where $m = 5$ and $n = 4$. Then $\mathcal{C}$ can be viewed as an ideal of $R = \mathfrak{R}[x,y]/\langle x^5 - 1,\ y^4 - 1\rangle$. It can be easily seen that 7 is primitive 4^{th} root of unity in $\mathbb{Z}_{25}$. Therefore, by Lemma 2, $\theta_0(y) = 19(1 + y + y^2 + y^3), \theta_1(y) = 19(1 + 18y - y^2 + 7y^3), \theta_2(y) = 19(1 - y + y^2 - y^3), \theta_3(y) = 19(1 + 7y - y^2 + 18y^3)$ are primitive idempotents of $\mathfrak{R}[y]/\langle y^4 - 1\rangle$. Consider the following cyclic codes of length 5 over $\mathfrak{R}$*

$$C_0 = C_2 = \langle p_0^{(0)}(x),\ p_1^{(0)}(x)\rangle = \langle 5, x^4 + x^3 + x^2 + x + 1\rangle$$
$$C_1 = C_3 = \langle p_0^{(1)}(x)\rangle = \langle x - 1\rangle$$

By Theorem 5, the set $\{\theta_0(y)p_0^{(0)}(x),\ \theta_0(y)p_1^{(0)}(x),\ \theta_1(y)p_0^{(1)}(x),\ \theta_2(y)p_0^{(0)}(x),\ \theta_2(y)p_1^{(0)}(x),\ \theta_3(y)p_0^{(1)}(x)\}$ generates a 2D cyclic code of length mn over $\mathfrak{R}$, where $m = 5$ and $n = 4$ and by Theorem 6, $Rank(\mathcal{C}) = 18$.

Example 2. *Consider the finite chain ring $\mathfrak{R} = \mathbb{Z}_{169}$ with residue field $\mathbb{F}_{13}$ and nilpotency index 2. Let $\mathcal{C}$ be 2D cyclic code of length mn over $\mathfrak{R}$, where $m = 169$ and $n = 12$. Then $\mathcal{C}$ can be viewed as an ideal of $R = \mathfrak{R}[x,y]/\langle x^{169} - 1,\ y^{12} - 1\rangle$. It can be easily seen that $2^{13} \equiv 80 (mod\ 169)$ is primitive 12^{th} root of unity in $\mathfrak{R}$. Therefore, by Lemma 2, $\theta_j(y) = \frac{1}{12}(1 + 80^{(12-j)}y + (80^{(12-j)}y)^2 + \cdots + (80^{(12-j)}y)^{11})$ are primitive idempotents of $\mathfrak{R}[y]/\langle y^{12} - 1\rangle;\ 0 \le j \le 11$.*

Consider the following cyclic codes of length 169 *over* $\mathfrak{R}$

$$\begin{aligned}
C_0 = C_1 &= \langle p_0^{(0)}(x)\rangle = \langle x-1\rangle \\
C_2 &= \langle p_0^{(2)}(x)\rangle = \langle x^{13}-1\rangle \\
C_3 &= \langle p_0^{(3)}(x)\rangle \\
&= \langle x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\rangle \\
C_4 &= \langle p_0^{(4)}(x)\rangle = \langle 13(x-1)\rangle \\
C_5 = C_6 &= \langle p_0^{(5)}(x),\ p_1^{(5)}(x)\rangle = \langle 13(x-1), x^{13}-1\rangle \\
C_7 = C_8 &= \langle p_0^{(7)}(x)\rangle = \langle x^{13}+1\rangle \\
C_9 = C_{10} &= \langle p_0^{(9)}(x)\rangle = \langle 13(x^{13}-1)\rangle \\
C_{11} &= \langle p_0^{(11)}(x),\ p_1^{(11)}(x)\rangle = \langle 13, (x-1)\rangle
\end{aligned}$$

By Theorem 5, the set $\{\theta_0(y)p_0^{(0)}(x), \theta_1(y)p_0^{(0)}(x), \theta_2(y)p_0^{(2)}(x), \theta_3(y)$ $p_0^{(3)}(x), \theta_4(y)p_0^{(4)}(x),\ \theta_5(y)p_0^{(5)}(x),\ \theta_5(y)p_1^{(5)}(x),\ \theta_6(y)p_0^{(5)}(x),\ \theta_6(y)p_1^{(5)}(x),$ $\theta_7(y)p_0^{(7)}(x)),\ \theta_8(y)p_0^{(7)}(x),\ \theta_9(y)p_0^{(9)}(x),\ \theta_{10}(y)p_0^{(9)}(x),\ \theta_{11}(y)p_0^{(11)}(x),$ $\theta_{11}(y)p_1^{(11)}(x)\}$ *generates a 2D cyclic code of length* mn *over* $\mathfrak{R}$, *where* $m = 169$ *and* $n = 12$ *and by Theorem 6,* $Rank(\mathcal{C}) = 1946$.

4 MHDR 2D cyclic codes over a finite chain ring

In this section, we obtain a necessary and sufficient condition for a 2D cyclic code to be MHDR over a finite chain ring $\mathfrak{R}$. We also provide some examples of 2D cyclic codes which are MHDR over $\mathfrak{R}$.

Theorem 7. *Let* $\mathcal{C}$ *be a 2D cyclic code of length* mn *over a finite chain ring* $\mathfrak{R}$ *generated by the set* $\{\theta_j(y)p_i^{(j)}(x) \mid 0 \le i \le r_j,\ 0 \le j \le n-1\}$ *as given in Theorem 5. Then, the set* $\mathcal{C}_{\nu-1} = \{f(x,y) \in \mathbb{F}_q[x,y]/\langle x^m-1, y^n-1\rangle$ *such that* $\gamma^{\nu-1}\underline{f(x,y) \in \mathcal{C}}\}$ *is a 2D cyclic code of length* mn *over* $\mathbb{F}_q$ *generated by the set* $\{q_0^{(j)}(x)\theta_j(y) \mid\ 0 \le j \le n-1\}$.

Proof. Clearly, $\mathcal{C}_{\nu-1}$ is an ideal of the ring $\mathbb{F}_q[x,y]/\langle x^m-1, y^n-1\rangle$ and hence a 2D cyclic code of length mn over $\mathbb{F}_q$. Let $f(x,y) \in \mathcal{C}_{\nu-1}$ be any element. Then, $f(x,y)\overline{\theta_j(y)} = \sum_{i=0}^{n-1} f_i(x)(\zeta^j)^i\overline{\theta_j(y)} = f(x,\zeta^j)\overline{\theta_j(y)} \in \mathcal{C}_{\nu-1},\ 0 \le j \le n-1$. By definition of $\mathcal{C}_{\nu-1}$, $\gamma^{\nu-1}f(x,\zeta^j)\overline{\theta_j(y)} = \gamma^{\nu-1}f(x,\zeta^j)\theta_j(y) \in \mathcal{C}$. Therefore, $\gamma^{\nu-1}f(x,\zeta^j) \in C_j$ which implies that $deg(f(x,\zeta^j)) \ge t_0^{(j)}$ for $0 \le j \le n-1$, since $\gamma^k q_0^{(j)}(x)$ is the minimal degree polynomial in C_j, where $k \ge s_0^{(j)}$. Now,

$deg(q_0^{(j)}(x)) = deg(\overline{q_0^{(j)}(x)})$ as $q_0^{(j)}(x)$ is a monic polynomial. By division algorithm, there exists unique polynomials $m_0^{(j)}(x),\ r_0^{(j)}(x) \in \mathbb{F}_q[x]/\langle x^m - 1\rangle$ such that $r_0^{(j)}(x) = f(x, \zeta^j) - \overline{q_0^{(j)}(x)}m_0^{(j)}(x)$, where $r_0^{(j)}(x) = 0$ or $deg(r_0^{(j)}(x)) < deg(\overline{q_0^{(j)}(x)})$. As $\gamma^{\nu-1}r_0^{(j)}(x) \in C_j$ and $deg(\gamma^{\nu-1}q_0^{(j)}(x)) = deg(\gamma^{\nu-1}\overline{q_0^{(j)}(x)})$ is minimal in C_j, $r_0^{(j)}(x) = 0$. Therefore, $f(x,y) = f(x,y)\sum_{j=0}^{n-1}\overline{\theta_j(y)} = \sum_{j=0}^{n-1} f(x,\ \zeta^j)\overline{\theta_j(y)} = \sum_{j=0}^{n-1}\overline{q_0^{(j)}(x)}m_0^{(j)}(x)\overline{\theta_j(y)}$. Hence the set $\{\overline{q_0^{(j)}(x)\theta_j(y)} \mid 0 \le j \le n-1\}$ generates $\mathcal{C}_{\nu-1}$.

□

Theorem 8. *Let $\mathcal{C}$ be a 2D cyclic code of length mn over $\mathfrak{R}$. Then $w_H(\mathcal{C}) = w_H(\mathcal{C}_{\nu-1})$.*

Proof. Let $f(x,y) \in \mathcal{C}_{\nu-1}$ be such that $w_H(\mathcal{C}_{\nu-1}) = w_H(f(x,y))$. Now, $w_H(f(x,y)) = w_H(\gamma^{\nu-1}f(x,y))$ since $f(x,y) \in \mathbb{F}_q[x,y]$. As $\gamma^{\nu-1}f(x,y) \in \mathcal{C}$, we have $w_H(\mathcal{C}_{\nu-1}) = w_H(f(x,y)) = w_H(\gamma^{\nu-1}f(x,y)) \ge w_H(\mathcal{C})$. Conversely, let $c(x,y) = c_0(x,y) + \gamma c_1(x,y) + \cdots + \gamma^{\nu-1}c_{\nu-1} \in \mathcal{C}$ be such that $w_H(\mathcal{C}) = w_H(c(x,y))$. Since $\gamma^{\nu-1}c(x,y) \in \mathcal{C}$, then $c_0(x,y) \in \mathcal{C}_{\nu-1}$. Therefore, $w_H(\mathcal{C}) = w_H(c(x,y)) \ge w_H(c_0(x,y)) \ge w_H(\mathcal{C}_{\nu-1})$. Hence, $w_H(\mathcal{C}) = w_H(\mathcal{C}_{\nu-1})$. □

Corollary 3. *The 2D cyclic code $\mathcal{C}$ over $\mathfrak{R}$ is MHDR if and only if the 2D cyclic code $\mathcal{C}_{\nu-1}$ over $\mathbb{F}_q$ is MHDR.*

Proof. Since the set $\{\overline{q_0^{(j)}(x)\theta_j(y)} \mid 0 \le j \le n-1\}$ generates $\mathcal{C}_{\nu-1}$, By Lemma 1, $Dim(\mathcal{C}_{\nu-1}) = mn - \sum_{j=0}^{n-1} t_0^{(j)}$ and by Theorem 6 $Rank(\mathcal{C}) = mn - \sum_{j=0}^{n-1} t_0^{(j)}$. Therefore, $Dim(\mathcal{C}_{\nu-1}) = Rank(\mathcal{C})$. Also, by Theorem 8, $d_H(\mathcal{C}) = d_H(\mathcal{C}_{\nu-1})$. Therefore, $\mathcal{C}$ is MHDR if and only if $\mathcal{C}_{\nu-1}$ is MHDR. □

We give below some examples of 2D cyclic codes, which are MHDR over $\mathfrak{R}$, where the minimum hamming distance of the codes is calculated with the help of the MAGMA software.

Example 3. *Consider the finite chain ring $\mathfrak{R} = \mathbb{Z}_{27}$ with residue field $\mathbb{F}_3$ and nilpotency index 3. Let $\mathcal{C}$ be 2D cyclic code of length $mn = 18$ over $\mathfrak{R}$, where $m = 9$ and $n = 2$. Then $\mathcal{C}$ can be viewed as an ideal of $R = \mathfrak{R}[x,y]/\langle x^9 - 1,\ y^2 - 1\rangle$. It can be easily seen that $2^9 \equiv 26(mod\ 27)$ is primitive 2^{nd} root of unity in $\mathbb{Z}_{27}$. Therefore, $\theta_0(y) = 14 + 14y, \theta_1(y) = 14 + 13y$ are primitive idempotents of $\mathfrak{R}[y]/\langle y^2 - 1\rangle$. Consider the following cyclic codes of length 9 over $\mathfrak{R}$*

$$C_0 = \langle 3, (x-1)^2\rangle$$
$$C_1 = \langle 3(x-1)\rangle$$

By Theorem 5, the set $\{3(14+14y), (x-1)^2(14+14y), 3(x-1)(14+13y)\}$ *generates* $\mathcal{C}$. *Therefore,* $Rank(\mathcal{C}) = 17$. *Also, by Theorem 7 , the set* $\{(2+2y), (x-1)(2+y)\}$ *generates a 2D cyclic code over* $\mathbb{F}_3$ *whose generator matrix is given by,*

$$G = \begin{pmatrix}
2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\
1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1
\end{pmatrix}$$

The minimum hamming distance of this code is 2. Therefore, $\mathcal{C}$ *is a 2D cyclic code of length* 18*, which is MHDR over* $\mathbb{Z}_{27}$.

Example 4. *Consider the finite chain ring* $\mathfrak{R} = \mathbb{Z}_{49}$ *with residue field* $\mathbb{F}_7$ *and nilpotency index 2. Let* $\mathcal{C}$ *be 2D cyclic code of length* $mn = 6$ *over* $\mathfrak{R}$*, where* $m = 2$ *and* $n = 3$*. Then* $\mathcal{C}$ *can be viewed as an ideal of* $R = \mathfrak{R}[x, y]/\langle x^2-1,\ y^3-1\rangle$. *It can be easily seen that* $2^7 \equiv 30(mod\ 49)$ *is primitive* 3^{rd} *root of unity in* $\mathbb{Z}_{49}$. *Therefore,* $\theta_0(y) = 33+33y+33y^2, \theta_1(y) = 33+6y+10y^2, \theta_2(y) = 33+10y+6y^2$ *are primitive idempotents of* $\mathfrak{R}[y]/\langle y^3-1\rangle$. *Consider the following cyclic codes of length* 2 *over* $\mathfrak{R}$

$$C_0 = \langle 7(x+1)\rangle$$
$$C_1 = \langle x-1\rangle$$
$$C_2 = \langle 7(x-1)\rangle$$

By Theorem 5, the set $\{7(x+1)(33+33y+33y^2), (x-1)(33+6y+10y^2), 7(x-1)(33+10y+6y^2)\}$ *generates* $\mathcal{C}$. *Therefore,* $Rank(\mathcal{C}) = 3$. *Also, by Theorem 7 , the set* $\{(x+1)(5+5y+5y^2), (x-1)(5+6y+3y^2), (x-1)(35+3y+6y^2)\}$

generates a 2D cyclic code over $\mathbb{F}_7$ whose generator matrix is given by,

$$G = \begin{pmatrix} 5 & 5 & 5 & 5 & 5 & 5 \\ 2 & 1 & 4 & 5 & 6 & 3 \\ 2 & 4 & 1 & 5 & 3 & 6 \end{pmatrix}$$

The minimum hamming distance of this code is 4. Therefore, $\mathcal{C}$ is a 2D cyclic code of length 6, which is MHDR over $\mathbb{Z}_{49}$.

Example 5. *Consider the finite chain ring $\mathfrak{R} = \mathbb{Z}_{121}$ with residue field $\mathbb{F}_{11}$ and nilpotency index 2. Let $\mathcal{C}$ be 2D cyclic code of length $mn = 10$ over $\mathfrak{R}$, where $m = 5$ and $n = 2$. Then $\mathcal{C}$ can be viewed as an ideal of $R = \mathfrak{R}[x,y]/\langle x^5 - 1,\ y^2 - 1\rangle$. It can be easily seen that $10^{11} \equiv 120 (mod\ 121)$ is primitive 2^{nd} root of unity in $\mathfrak{R}$. Therefore, $\theta_0(y) = 61+61y, \theta_1(y) = 61+60y$ are primitive idempotents of $\mathfrak{R}[y]/\langle y^2-1\rangle$. Consider the following cyclic codes of length 5 over $\mathfrak{R}$*

$$C_0 = \langle 11, (x+1)\rangle$$
$$C_1 = \langle x-1\rangle$$

By Theorem 5, the set $\{11(61+61y), (x+1)(61+61y), (x-1)(61+60y)\}$ generates $\mathcal{C}$. Therefore, $Rank(\mathcal{C}) = 9$. Also, by Theorem 7 , the set $\{(6+6y), (x-1)(6+5y)\}$ generates a 2D cyclic code over $\mathbb{F}_{11}$ whose generator matrix is given by,

$$G = \begin{pmatrix} 6 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 6 \\ 5 & 6 & 6 & 5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 6 & 6 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 6 & 6 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 5 & 6 & 6 & 5 \end{pmatrix}$$

The minimum hamming distance of this code is 2. Therefore, $\mathcal{C}$ is a 2D cyclic code of length 10, which is MHDR over $\mathfrak{R}$.

Example 6. *Consider the finite chain ring $\mathfrak{R} = \mathbb{Z}_{25}$ with residue field $\mathbb{F}_5$ and nilpotency index 2. Let $\mathcal{C}$ be 2D cyclic code of length $mn = 6$ over $\mathfrak{R}$, where $m = 3$ and $n = 2$. Then $\mathcal{C}$ can be viewed as an ideal of $R = \mathfrak{R}[x,y]/\langle x^3 - 1,\ y^2 - 1\rangle$. It can be easily seen that 24 is primitive 2^{nd} root of unity in $\mathbb{Z}_{25}$. Therefore, $\theta_0(y) = 13+13y, \theta_1(y) = 13+12y$ are primitive idempotents of*

$\mathfrak{R}[y]/\langle y^2-1\rangle$. Consider the following cyclic codes of length 3 over $\mathfrak{R}$

$$C_0 = \langle 5(x^2+x+1)\rangle$$
$$C_1 = \langle (x-1)\rangle$$

By Theorem 5, the set $\{5(x^2+x+1)(13+13y),(x-1)(13+12y)\}$ generates $\mathcal{C}$. Therefore, $Rank(\mathcal{C})=3$. Also, by Theorem 7 , the set $\{(x^2+x+1)(3+3y),(x-1)(3+2y)\}$ generates a 2D cyclic code over $\mathbb{F}_5$ whose generator matrix is given by,

$$G = \begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 3 \\ 2 & 3 & 3 & 2 & 0 & 0 \\ 0 & 0 & 2 & 3 & 3 & 2 \end{pmatrix}$$

The minimum hamming distance of this code is 4. Therefore, $\mathcal{C}$ is a 2D cyclic code of length 6, which is MHDR over $\mathbb{Z}_{25}$.

5 Conclusion

In this paper, the generators and rank of a 2D cyclic code of length mn over a finite chain ring $\mathfrak{R}$ with residue field $\mathbb{F}_q$ have been determined, where m is arbitrary and $q \equiv 1(mod\ n)$. Further, a condition for a 2D cyclic code to be MHDR has been obtained, and a few examples of 2D cyclic codes over some finite chain rings which are MHDR, have been provided.

References

[1] Abualrub, T., Ghrayeb, A. and Oehmke, R.H.: A mass formula and rank of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inf. Theory, 50(12), (2004), 3306-3312.

[2] Bhardwaj, S. and Raka, M.: Two dimensional constacyclic codes of arbitrary length over finite fields, Indian J. Pure Appl. Math., 53(1), (2022), 49-61.

[3] Monika, Dutt, S. and Sehmi, R.: On cyclic codes over finite chain rings, J. Phys. Conf. Ser., (2021).

[4] Dalal, M., Dutt, S. and Sehmi, R.: MDS and MHDR cyclic codes over finite chain rings, arXiv preprint arXiv:2303.15819.

[5] Garg, A. and Dutt, S.: On Rank and MDR Cyclic Codes of Length 2^k Over Z_8, In Algorithms and Discrete Applied Mathematics: Third International Conference, CALDAM 2017, Sancoale, Goa, India, February

16-18, (2017), Proceedings (pp. 177-186). Cham: Springer International Publishing.

[6] Garg, A. and Dutt, S.: On rank and MDR cyclic and negacyclic codes of length p^k over Z_{p^m}, Discrete Applied Mathematics, 285, (2020), 581-590.

[7] Gneri, C. and zbudak, F.: A relation between quasi-cyclic codes and 2D cyclic codes, Finite Fields their Appl., 18, (2012), 123132. https://doi.org/10.1016/j.ffa.2011.07.004.

[8] Imai, H.: A theory of two-dimensional cyclic codes, Inf. Control, 34, (1977), 121. https://doi.org/10.1016/S0019-9958(77)90232-7.

[9] Norton, G.H. and Slgean A.: On the structure of linear and cyclic codes over a finite chain ring, Appl. Algebr. Eng. Commun. Comput., 10, (2000), 489506. https://doi.org/10.1007/PL00012382

[10] Rajabi, Z. and Khashyarmanesh, K.: Repeated-root two-dimensional constacyclic codes of length $2p^s.2^k$, Finite Fields their Appl., 50, (2018), 122137. https://doi.org/10.1016/j.ffa.2017.11.008.

[11] Sepasdar, Z. and Khashyarmanesh, K.: Characterizations of some two-dimensional cyclic codes correspond to the ideals of $F[x,y]/<x^s-1, y^{2^k}-1>$, Finite Fields their Appl., 41, (2016), 97112.

[12] Sepasdar, Z.: Generator matrix for two-dimensional cyclic codes of arbitrary length, (2017), 16. http://arxiv.org/abs/1704.08070.

[13] Shiromoto, K.: A basic exact sequence for the Lee and Euclidean weights of linear codes over Z_l, Linear Algebra Appl., 295, (1999), 191200. https://doi.org/10.1016/S0024-3795(99)00125-1.

Disha Garg,
Department of Mathematics,
Punjab Engineering College (Deemed to be University),
Sector 12, Chandigarh, 160012, India.
Email: disha.phd21appsc@pec.edu.in

Sucheta Dutt,
Department of Mathematics,
Punjab Engineering College (Deemed to be University),
Sector 12, Chandigarh, 160012, India.
Email: sucheta@pec.edu.in