Hindawi
Journal of Mathematics
Volume 2024, Article ID 4540992, 8 pages
https://doi.org/10.1155/2024/4540992

Research Article

MDS and MHDR Cyclic Codes over Finite Chain Rings

Monika Dalal, Sucheta Dutt, and Ranjeet Sehmi

Department of Applied Sciences, Punjab Engineering College (Deemed to be University), Chandigarh 160012, India

Correspondence should be addressed to Sucheta Dutt; sucheta@pec.edu.in

Received 18 April 2023; Revised 17 November 2023; Accepted 20 November 2023; Published 25 January 2024

Academic Editor: Xiaogang Liu

This work establishes a unique set of generators for a cyclic code over a finite chain ring. Towards this, we first determine the minimal spanning set and rank of the code. Furthermore, sufficient as well as necessary conditions for a cyclic code to be an MDS code and for a cyclic code to be an MHDR code are obtained. Finally, to support our results, some examples of optimal cyclic codes are presented.

1. Introduction

Coding theory aims to provide optimal codes for detecting and correcting a maximum number of errors during data transmission through noisy channels. Cyclic codes have been in focus due to their rich algebraic structure which enables easy encoding and decoding of data through the process of channel coding. Cyclic codes over rings have gained a lot of importance after the remarkable breakthrough given by Hammons et al. in reference [1]. A vast literature is available on the structure of cyclic codes over fields, integer residue rings, Galois rings, finite chain rings, and some finite nonchain rings [2–29]. Cyclic codes over finite chain rings with length coprime to the characteristic of residue field have been investigated in references [2, 16, 22]. Islam and Prakash have established a unique set of generators for cyclic codes over Z_{p^k} in reference [4] and for cyclic codes over $F_q + uF_q, u^2 = 0$ in reference [5]. A. Sharma and T. Sidana have studied cyclic codes of p^s length over finite chain rings in reference [15], thereby extending the results of Kiah et al. on cyclic codes over Galois rings [14]. Dinh explored the structure and properties of cyclic codes of length p^s over finite chain rings with nilpotency index 2 [13]. However, in most of the studies, there have been some limitations on either the length of code or the nilpotency index of the ring. We do not impose any such restriction in this paper. Salagean made use of the existence of a Grobner basis for an ideal of a polynomial ring to establish a unique set of generators for a cyclic code over a finite chain ring with arbitrary parameters [18]. Al-Ashker et al. have also worked in the same direction in the paper [28] by extending the novel approach given by Siap and Abualrub [12] which pulls back the generators of a cyclic code over Z_2 to establish the structure of cyclic codes over the ring $Z_2 + uZ_2 + \cdots + u^{k-1}Z_{k-1}, u^k = 0$. They have also extended this approach over the finite chain ring $F_q + uF_q + \cdots + u^{k-1}F_{q-1}, \ u^k = 0$ [24]. Monika and Sehmi have given a constructive approach to establish a generating set for a cyclic code over a finite chain ring by making use of minimal degree polynomials of certain subsets of the code [20]. We make some advancements to this study by establishing a unique set of generators for a cyclic code over a finite chain ring with arbitrary parameters. It is noted that this unique set of generators retains all the properties of generators obtained in reference [20].

The paper is organised as follows: In Section 2, we state some preliminary results. In Section 3, we establish a unique set of generators for a cyclic code over a finite chain ring. In Section 4, we establish a minimal spanning set and rank of the cyclic code. We give sufficient as well as necessary conditions for a cyclic code to be an MDS code. We establish sufficient as well as necessary conditions for a cyclic code of length which is not coprime to the characteristic of residue field of the ring to be an MHDR code. Finally, we provide a few examples of MDS and MHDR cyclic codes over some finite chain rings.

2. Preliminaries

Let R be a finite commutative chain ring. Let $\langle\gamma\rangle$ be the unique maximal ideal of R and ν be the nilpotency index of γ. Let $F_q = R/\langle\gamma\rangle$ be the residue field of R, where $q = p^s$ for a prime p and a positive integer s.

The following is a well-known result (for reference, see [15]).

Proposition 1. *Let R be a finite commutative chain ring. Then, we have the following:*

(i) $charR = p^a$, where $1 \le a \le \nu$ and $|R| = |F_q|^\nu = p^{s\nu}$

(ii) There exists an element $\zeta \in R$ with multiplicative order $p^s - 1$. The set $\top = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^s-2}\}$ is called the Teichmüller set of R

(iii) Every $r \in R$ can be uniquely expressed as $r = r_0 + r_1\gamma + \cdots + r_{\nu-1}\gamma^{\nu-1}$, where $r_i \in \top$ for $0 \le i \le \nu - 1$. Also, r is a unit in R if and only if $r_0 \neq 0$

Remark 2. Let $k(z) = k_0 + k_1 z + \cdots + k_t z^t$, where $k_j \in R$ for $j = 0, 1, \ldots, t$ is a polynomial of degree t in $R[z]$. By using Proposition 1(iii), $k(z)$ can be expressed as

$$k(z) = a_0(z) + \gamma a_1(z) + \cdots + \gamma^{\nu-1} a_{\nu-1}(z), \tag{1}$$

where $a_j(z) \in \top[z]$ for $j = 0, 1, \ldots, \nu - 1$.

We define a map ϕ: $R \longrightarrow \top$ by $\phi(r) = r \pmod{\gamma} = \overline{r}$ for $r \in R$. Clearly, ϕ is a natural onto homomorphism, and therefore, $\overline{R} = \top$, where $\overline{R}$ denotes the image of R under ϕ. This map can be naturally extended from $R[z]$ to $\top[z]$ by $\sum_{i=0}^{k} a_i z^i \mapsto \sum_{i=0}^{k} \overline{a_i} z^i$, where $a_i \in R$ for $0 \le i \le k$.

Let us now recall some basic definitions and known results.

A linear code C with length n over a finite commutative chain ring R is said to be a cyclic code if $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ for every $(c_0, c_1, \ldots, c_{n-1}) \in C$. It is well established that C can be viewed as an ideal of $R[z]/\langle z^n - 1\rangle$. The Hamming weight $w_H(c)$ of $c = (c_0, c_1 \cdots c_{n-1}) \in C$ is defined as the number of integers i such that $c_i \neq 0$ for $0 \le i \le n - 1$. The Hamming distance $d_H(C)$ of a code C over R is given by $d_H(C) = \min\{w_H(c)$: c is a nontrivial element of $C\}$. C is said to be an MDS (maximum distance separable) code with respect to the Hamming metric if $|C| = |R|^{n - d_H(C) + 1}$. The rank of C is defined as the total number of elements in the minimal spanning set of C. C is said to be an MHDR (maximum Hamming distance with respect to rank) code if $d_H(C) = n - \mathrm{rank}(C) + 1$. The i^{th} torsion code of C is defined as $\mathrm{Tor}_i(C) = \{\phi(k(z)) \in \overline{R}[z]$: $\gamma^i k(z) \in C\}$, where $0 \le i \le \nu - 1$. Then, $\mathrm{Tor}_i(C)$ for all i, $0 \le i \le \nu - 1$ is a principally generated cyclic code over the residue field of R. The degree of the generator polynomial of $\mathrm{Tor}_i(C)$ is called the i^{th} torsional degree of C. A polynomial in $R[z]$ is said to be monic if its leading coefficient, i.e., the coefficient of its leading term is a unit in R. The leading coefficient of a polynomial $k(z)$ in $R[z]$ is denoted by $\mathrm{lc}(k(z))$.

3. Unique Set of Generators

In this section, a unique set of generators for a cyclic code C of arbitrary length n over R has been established. For this, let us first recall the construction given by Monika et al. to obtain a generating set for a cyclic code C over a finite chain ring R [20]. Let $f_0(z), f_1(z), \ldots, f_m(z)$ be minimal degree polynomials of certain subsets of C such that $\deg(f_j(z)) = t_j < n$ and the leading coefficient of $f_j(z)$ is equal to $\gamma^{i_j} u_j$, where u_j is some unit in R, $t_j < t_{j+1}$, $i_j > i_{j+1}$, and i_j is the smallest of such power. If $i_0 = 0$, then $f_0(z)$ is a monic polynomial and we have $m = 0$.

Lemma 3 (see [20]). *Let C be a cyclic code having a length n over R and $f_j(z)$, $0 \le j \le m$, be polynomials as defined above. Then, we have the following:*

(i) C is generated by the set $\{f_j(z); j = 0, 1, \ldots, m\}$

(ii) For $0 \le j \le m$, $f_j(z) = \gamma^{i_j} h_j(z)$, where $h_j(z)$ is a monic polynomial over the finite commutative chain ring having nilpotency index $\nu - i_j$ and maximal ideal $\langle\gamma\rangle$

(iii) $\{f_j(z); j = 0, 1, \ldots, m\}$ forms a Grobner basis for C

The following results are straightforward generalisations of reference [19] for cyclic codes over the class of Galois rings to finite chain rings and have been communicated in reference [21]. These results are required to proceed further.

Lemma 4 (see [21]). *We consider a cyclic code C of arbitrary length n over R generated by $\{f_0(z), f_1(z), \ldots, f_m(z)\}$ as defined above. Then, for every $(z) \in \mathrm{Tor}_{i_j}(C)$, $\deg(a(z)) \ge t_j$. Also, $\mathrm{Tor}_{i_j}(C) = \langle\overline{h_j(z)}\rangle$ and t_j is the i_j^{th} torsional degree of C.*

Remark 5 (see [21]). Let $C = \langle f_0(z), f_1(z), \ldots, f_m(z)\rangle$ be a cyclic code having a length n over R, where $f_j(z)$ for $j = 0, 1, \ldots, m$ are polynomials as defined above. Then, we have

(i) $\mathrm{Tor}_0(C) = \mathrm{Tor}_1(C) = \cdots = \mathrm{Tor}_{i_m - 1}(C) = \{0\}$

(ii) $\mathrm{Tor}_{i_j}(C) = \mathrm{Tor}_{i_j+1}(C) = \cdots = \mathrm{Tor}_{i_{j-1}-1}(C) \subset \mathrm{Tor}_{i_{j-1}}(C)$ for $j = 1, 2, \ldots, m$

(iii) $\mathrm{Tor}_{i_0}(C) = \mathrm{Tor}_{i_0+1}(C) = \cdots = \mathrm{Tor}_{\nu-2}(C) = \mathrm{Tor}_{\nu-1}(C)$

Remark 6. For a cyclic code C with a generating set as defined above, the abovementioned remark implies that

(i) for $i_0 \le i \le \nu - 1$, the i^{th} torsional degree of C is t_0

(ii) for $1 \le j \le m$ and $i_j \le i \le i_{j-1} - 1$, the i^{th} torsional degree of C is t_j

Theorem 7 (see [21]). *Let C be a cyclic code having an arbitrary length n over R generated by polynomials $f_0(z), f_1(z), \ldots, f_m(z)$ as defined earlier. If $|\top| = p^s$, then we have*

$$|C| = p^{s\left(n\nu-\left(ni_m+t_0k_0+t_1k_1+\cdots+t_mk_m\right)\right)}, \tag{2}$$

where t_j *for* $j = 0, 1, \ldots, m$ *are the torsional degrees of* $Tor_{i_j}(C)$, $k_0 = \nu - i_0$, *and* $k_j = i_{j-1} - i_j$ *for* $j = 1, 2, \ldots, m$.

Theorem 8 (see [21]). *Let* $C = \langle f_0(z), f_1(z), \ldots, f_m(z)\rangle$ *be a cyclic code as defined above. Then,* $d_H(C) = d_H(Tor_{i_0}(C)) = d_H(\langle \overline{h_0(z)}\rangle)$.

Remark 9. Let $\gamma^i k(z), \gamma^j w(z) \in R[z]$ such that $i \geq j$, $\deg(k(z)) \geq \deg(w(z))$, and $w(z)$ is monic. Let $a, b \in R$ be the leading coefficient of $k(z)$ and $w(z)$, respectively. Then, we have

$$\gamma^i k(z) - \gamma^{i-j} ab^{-1} z^{\deg(k(z)) - \deg(w(z))} \gamma^j w(z) = \gamma^i s_1(z), \tag{3}$$

for some $s_1(z) \in R[z]$ such that $\deg(s_1(z)) < \deg(k(z))$. If $\deg(s_1(z)) \geq \deg(w(z))$, then by applying a similar argument as mentioned above on $\gamma^i s_1(z)$, we have

$$\gamma^i s_1(z) - \gamma^{i-j} \mathrm{lc}(s_1(z)) b^{-1} z^{\deg(s_1(z)) - \deg(w(z))} \gamma^j w(z) = \gamma^i s_2(z), \tag{4}$$

for some $s_2(z) \in R[z]$ such that $\deg(s_2(z)) < \deg(s_1(z))$. Again, if $\deg(s_2(z)) \geq \deg(w(z))$, then repeatedly apply the abovementioned argument a finite number of times to obtain polynomials $s_3(z), s_4(z), \ldots, s_l(z)$ in $R[z]$ with $\deg(s_2(z)) > \deg(s_3(z)) > \cdots > \deg(s_l(z)) \geq \deg(w(z))$ such that

$$\gamma^i s_l(z) - \gamma^{i-j} \mathrm{lc}(s_l(z)) b^{-1} z^{\deg(s_l(z)) - \deg(w(z))} \gamma^j w(z) = \gamma^i s(z), \tag{5}$$

where $s(z) \in R[z]$ and $\deg(s(z)) < \deg(w(z))$. Now, by back substituting all these values of $\gamma^i s_l(z), \gamma^i s_{l-1}(z), \ldots, \gamma^i s_1(z)$ one by one, we finally get

$$\gamma^i k(z) - q(z)\gamma^j w(z) = \gamma^i s(z), \tag{6}$$

for $q(z), s(z) \in R[z]$, $\deg(q(z)) \leq \deg(k(z)) - \deg(w(z))$, and $\deg(s(z)) < \deg(w(z))$.

In the following theorem, a unique set of generators for a cyclic code C over a finite chain ring R has been obtained, which retains all the properties as that of the generating set obtained in reference [20].

For a positive integer t, define $\mathfrak{B}_t = \{a(z) \in \top[z], \text{such that} \quad \deg(a(z)) < t\}$.

Theorem 10. *Let* $C = \langle f_0(z), f_1(z), \ldots, f_m(z)\rangle$ *be a cyclic code having an arbitrary length over R as defined above. Then, there exist polynomials* $\mathfrak{u}_0(z), \mathfrak{u}_1(z), \ldots, \mathfrak{u}_m(z)$ *in C such that for* $0 \leq j \leq m$, *we have*

$$\mathfrak{u}_j(z) = \sum_{l=i_j}^{\nu-1} \gamma^l b_{j,l}(z), \tag{7}$$

where $b_{j,l}(z) \in \top[z]$ *for* $i_j \leq l \leq \nu - 1$, $b_{j,i_j}(z) = \overline{h_j(z)}$, *such that* $\overline{h_j(z)}$ *is the generator polynomial of* i_j^{th} *torsion code of C and* $\deg(b_{j,i_j}(z)) = t_j$. *Furthermore,* $b_{j,l}(z) \in \mathfrak{B}_{t_j}$ *for* $i_j < l < i_{j-1}$, $b_{j,l}(z) \in \mathfrak{B}_{t_r}$ *for* $i_r \leq l < i_{r-1}$ *and* $j - 1 \geq r \geq 1$, *and* $b_{j,l}(z) \in \mathfrak{B}_{t_0}$ *for* $i_0 \leq l \leq \nu - 1$. *Also, C is generated by the set* $\{\mathfrak{u}_0(z), \mathfrak{u}_1(z), \ldots, \mathfrak{u}_m(z)\}$ *which retains all the properties as that of the generating set* $\{f_0(z), f_1(z), \ldots, f_m(z)\}$ *and* $\mathfrak{u}_j(z)$ *are unique in this form.*

Proof. Let $C = \langle f_0(z), f_1(z), \ldots, f_m(z)\rangle$ be a cyclic code over R such that $f_j(z)$ are polynomials as defined above. By construction, it is clear that $f_0(z)$ is unique in C. Therefore, $f_0(z) = \mathfrak{u}_0(z)$. Now, we consider that

$$f_1(z) = \sum_{l=i_1}^{\nu-1} a_{1,l}(z), \tag{8}$$

where $a_{1,l}(z) \in \top[z]$ for $i_1 \leq l \leq \nu - 1$, $a_{1,i_1}(z) = \overline{h_1(z)}$ such that $\overline{h_1(z)}$ is the generator polynomial of i_1^{th} torsion code of C, and $\deg(a_{1,i_1}(z)) = t_1$ and $a_{1,l}(z) \in \mathfrak{B}_{t_1}$ for $i_1 < l \leq \nu - 1$. If $a_{1,l}(z) \in \mathfrak{B}_{t_0}$ for $i_0 \leq l \leq \nu - 1$, then $f_1(z)$ is of the desired form. Otherwise, suppose $k \leq \nu - i_0 - 1$ to be the least nonnegative integer such that $a_{1,i_0+k}(z) \notin \mathfrak{B}_{t_0}$. Then, $\deg(a_{1,i_0+k}(z)) \geq t_0$. By Remark 9, we have

$$\gamma^{i_0+k} a_{1,i_0+k}(z) = \gamma^{i_0} h_0(z) q_k^{(1)}(z) + \gamma^{i_0+k} s_k^{(1)}(z), \tag{9}$$

for some polynomials $q_k^{(1)}(z), s_k^{(1)}(z) \in R[z]$ such that $\deg(s_k^{(1)}(z)) < t_0$. Let $\gamma^{i_0+k} s_k^{(1)}(z) = \sum_{l=i_0+k}^{\nu-1} \gamma^l s_{k,l}^{(1)}(z)$, where $s_{k,l}^{(1)}(z) \in \mathfrak{B}_{t_0}$ for $i_0 + k \leq l \leq \nu - 1$. We substitute this in equation (9) and then back substitute the value of $\gamma^{i_0+k} a_{1,i_0+k}(z)$ in equation (8) to get

$$\begin{aligned} f_1(z) = &\sum_{l=i_1, l\neq i_0+k}^{\nu-1} \gamma^l a_{1,l}(z) + \gamma^{i_0} h_0(z) q_k^{(1)}(z) \\ &+ \sum_{l=i_0+k}^{\nu-1} \gamma^l s_{k,l}^{(1)}(z). \end{aligned} \tag{10}$$

This implies that

$$f_1(z) - \gamma^{i_0} h_0(z) q_k^{(1)}(z) = \sum_{l=i_1}^{i_0+k-1} \gamma^l a_{1,l}(z) + \gamma^{i_0+k} s_{k,i_0+k}^{(1)}(z) + \sum_{l=i_0+k+1}^{\nu-1} \gamma^l \left(a_{1,l}(z) + s_{k,l}^{(1)}(z)\right). \tag{11}$$

Clearly, the term with content γ^{i_0+k} on the right-hand side of the abovementioned equation now belongs to $\mathfrak{B}_{t_0}$. Following the same arguments as mentioned above for every $a_{1,i_0+k'}(z) \notin \mathfrak{B}_{t_0}$, where $k < k' \leq \nu - i_0 - 1$, we can obtain a polynomial say $\mathfrak{u}_1(z) = \sum_{l=i_1}^{\nu-1} b_{1,l}(z)$ in C by subtracting a suitable multiple of $f_0(z)$ from $f_1(z)$ which will satisfy all the desired properties, i.e., $b_{1,l}(z) \in \top[z]$, $b_{1,i_1}(z) = \overline{h_1(z)}$, $b_{1,l}(z) \in \mathfrak{B}_{t_1}$ for $i_1 < l < i_0$ and $b_{1,l}(z) \in \mathfrak{B}_{t_0}$ for $i_0 \leq l \leq \nu - 1$ such that $C = \langle \mathfrak{u}_0(z), \mathfrak{u}_1(z), f_2(z), \ldots, f_m(z) \rangle$.

Now consider the following polynomial:

$$f_2(z) = \sum_{l=i_2}^{\nu-1} a_{2,l}(z), \tag{12}$$

where $a_{2,l}(z) \in \top[z]$ for $i_1 \leq l \leq \nu - 1$, $a_{2,i_2}(z) = \overline{h_2(z)}$, and $\deg(a_{2,i_2}(z)) = t_2$ and $a_{2,l} \in \mathfrak{B}_{t_2}$ for $i_2 < l \leq \nu - 1$. Furthermore, if $a_{2,l}(z) \in \mathfrak{B}_{t_1}$ for $i_1 \leq l < i_0$ and $a_{2,l}(z) \in \mathfrak{B}_{t_0}$ for $i_0 \leq l \leq \nu - 1$, then $f_2(z)$ is of the desired form. Otherwise, let there exist least positive integers $k \leq \nu - i_0 - 1$ and $r \leq i_0 - i_1 - 1$ such that $a_{2,i_0+k}(z) \notin \mathfrak{B}_{t_0}$ and $a_{2,i_1+r}(z) \notin \mathfrak{B}_{t_1}$. By using Remark 9 for $a_{2,i_0+k}(z)$ and $a_{2,i_1+r}(z)$, we have

$$\begin{aligned} \gamma^{i_0+k} a_{2,i_0+k}(z) - \gamma^{i_0} h_0(z) q_k^{(2)}(z) &= \gamma^{i_0+k} s_k^{(2)}(z), \\ \gamma^{i_1+r} a_{2,i_1+r}(z) - \gamma^{i_1} h_1(z) q_r^{(2)}(z) &= \gamma^{i_1+r} s_r^{(2)}(z), \end{aligned} \tag{13}$$

such that $q_k^{(2)}(z), s_k^{(2)}(z), q_r^{(2)}(z), s_r^{(2)}(z) \in R[z]$ and the degrees of $s_k^{(2)}(z)$ and $s_r^{(2)}(z)$ are strictly less than that of t_0 and t_1, respectively. Let $s_k^{(2)}(z) = \sum_{l=i_0+k}^{\nu-1} \gamma^l s_{k,l}^{(2)}(z)$ and $s_r^{(2)}(z) = \sum_{l=i_1+r}^{\nu-1} \gamma^l s_{r,l}^{(2)}(z)$ for every $s_{k,l}^{(2)}(z), s_{r,l}^{(2)}(z)$ in $\top[z]$. Then, $s_{k,l}^{(2)}(z) \in \mathfrak{B}_{t_0}$ for $i_0 \leq l \leq \nu - 1$ and $s_{r,l}^{(2)}(z) \in \mathfrak{B}_{t_1}$ for $i_1 + r \leq l \leq \nu - 1$. Using this to obtain the value of $a_{2,i_0+k}(z)$ and $a_{2,i_1+r}(z)$ and then back substituting these values in the summand for $f_2(z)$, we get $f_2(z) - \gamma^{i_1} h_1(z) q_r^{(2)}(z) - \gamma^{i_0} h_0(z) q_k^{(2)}(z) \sum_{l=i_2}^{i_1+r-1} \gamma^l a_{2,l}(z) + \gamma^{i_1+r} s_{r,i_1+r}^{(2)}(z) + \sum_{l=i_1+r+1}^{i_0+k-1} \gamma^l (a_{2,l}(z) s_{r,l}^{(2)}(z)) + \gamma^{i_0+k} s_{k,i_0+k}^{(2)}(z) \sum_{l=i_0+k+1}^{\nu-1} \gamma^l (a_{2,l}(z) + s_{r,l}^{(2)}(z) + s_{k,l}^{(2)}(z))$. Clearly, on the right-hand side of this equation, the term with content γ^{i_1+r} now has a degree that is strictly less than that of t_1 and the term with content γ^{i_0+k} has a degree that is strictly less than that of t_0. Following the similar arguments as mentioned above for every $k < k' \leq \nu - i_0 - 1$ and $r < r' \leq i_0 - i_1 - 1$, we can finally obtain a polynomial $\mathfrak{u}_2(z) = \sum_{l=i_2}^{\nu-1} \gamma^l b_{2,l}(z)$ in C by subtracting a suitable multiple of $f_0(z)$ and $f_1(z)$ from $f_2(z)$ and $\mathfrak{u}_2(z)$ satisfies all the desired properties. Similarly, for every $3 \leq j \leq m$, we can obtain a polynomial $\mathfrak{u}_j(z) = \sum_{l=i_j}^{\nu-1} b_{j,l}(z)$ in C by subtracting suitable multiples of $f_{j-1}(z), f_{j-2}(z), \ldots, f_0(z)$ from $f_j(z)$, such that $\mathfrak{u}_j(z)$ is of the desired form and $C = \langle \mathfrak{u}_0(z), \mathfrak{u}_1(z), \ldots, \mathfrak{u}_m(z) \rangle$. It is clear from the abovementioned arguments that these $\mathfrak{u}_j(z)$ have the same structural properties as those of $f_j(z)$, for every $0 \leq j \leq m$.

Then, we show that the polynomials $\mathfrak{u}_j(z)$, $0 \leq j \leq m$ obtained above are unique in this form. Let $C = \langle \mathfrak{u}_0(z), \mathfrak{u}_1(z), \ldots, \mathfrak{u}_m(z) \rangle = \langle w_0(z), w_1(z), \ldots, w_m(z) \rangle$, where $\mathfrak{u}_j(z) = \sum_{l=i_j}^{\nu-1} \gamma^l b_{j,l}(z)$ and $w_j(z) = \sum_{l=i_j}^{\nu-1} \gamma^l d_{j,l}(z)$, such that $b_{j,l}(z), d_{j,l}(z) \in \top[z]$ for $i_j \leq l \leq \nu - 1$, $b_{j,i_j}(z) = d_{j,i_j}(z) = \overline{h_j(z)}$ for the generator polynomial $\overline{h_j(z)}$ of the i_j^{th} torsion code of C, and $\deg(b_{j,i_j}(z)) = \deg(d_{j,i_j}(z)) = t_j$. Furthermore, $b_{j,l}(z), d_{j,l}(z) \in \mathfrak{B}_{t_j}$ for $i_j < l < i_{j-1}$, $b_{j,l}(z), d_{j,l}(z) \in \mathfrak{B}_{t_r}$ for $i_r \leq l < i_{r-1}$ and $j - 1 \geq r \geq 1$, and $b_{j,l}(z), d_{j,l}(z) \in \mathfrak{B}_{t_0}$ for $i_0 \leq l \leq \nu - 1$. Clearly, $w_0(z) = f_0(z) = \mathfrak{u}_0(z)$ by the abovementioned construction. For $1 \leq j \leq m$, we consider the following polynomial:

$$w_j(z) - \mathfrak{u}_j(z) = \sum_{l=i_j}^{\nu-1} \gamma^l \left(d_{j,l}(z) - b_{j,l}(z)\right). \tag{14}$$

Let us denote the polynomials $d_{j,l}(z) - b_{j,l}(z)$ by $e_{j,l}(z)$ for $i_j \leq l \leq \nu - 1$. Then, we have

$$w_j(z) - \mathfrak{u}_j(z) = \gamma^{i_j+1} \sum_{l=i_j+1}^{\nu-1} \gamma^{l-i_j-1} e_{j,l}(z), \tag{15}$$

since $d_{j,i_j}(z) = b_{j,i_j}(z) = \overline{h_j(z)}$, i.e., $e_{j,i_j}(z) = 0$. We have that $\phi(\sum_{l=i_j+1}^{\nu-1} \gamma^{l-i_j-1} e_{j,l}(z)) = e_{j,i_j+1}(z) \in Tor_{i_j+1}(C)$. From Remark 5 and Lemma 4, we have that $\mathrm{Tor}_{i_j+1}(C) = \mathrm{Tor}_{i_j}(C) = \langle \overline{h_j(z)} \rangle$ for $i_j + 1 < i_{j-1}$. Therefore, $e_{j,i_j+1}(z) \in \langle \overline{h_j(z)} \rangle$ but $\deg(e_{j,i_j+1}(z)) < t_j$ which implies that $e_{j,i_j+1}(z) = 0$. By substituting this in equation (15) and applying the same arguments a finite number of times, we get $e_{j,l}(z) = 0$ for $i_j \leq l < i_{j-1}$. By substituting this in equation (15), we have

$$w_j(z) - \mathfrak{u}_j(z) = \gamma^{i_{j-1}} \sum_{l=i_{j-1}}^{\nu-1} \gamma^{l-i_{j-1}} e_{j,l}(z). \tag{16}$$

We have $\phi(\sum_{l=i_{j-1}}^{\nu-1} \gamma^{l-i_{j-1}} e_{j,l}(z)) = e_{j,i_{j-1}}(z) \in Tor_{i_{j-1}}(C)$. By using Lemma 4, we get that $e_{j,i_{j-1}}(z) \in \langle \overline{h_{j-1}(z)} \rangle$. Then, $e_{j,i_{j-1}}(z) = 0$, since $\deg(e_{j,i_{j-1}}(z)) < t_{j-1}$. By using this in equation (15), we get

$$w_j(z) - \mathfrak{u}_j(z) = \gamma^{i_{j-1}+1} \sum_{l=i_{j-1}+1}^{\nu-1} \gamma^{l-i_{j-1}+1} e_{j,l}(z). \tag{17}$$

Again, we have $\phi(\sum_{l=i_{j-1}+1}^{\nu-1} \gamma^{l-i_{j-1}+1} e_{j,l}(z)) = e_{j,i_{j-1}+1}(z) \in Tor_{i_{j-1}+1}(C)$. By using Remark 5 and Lemma 4, we get that $e_{j,i_{j-1}+1}(z) \in Tor_{i_{j-1}+1}(C) = Tor_{i_{j-1}}(C) = \langle \overline{h_{j-1}(z)} \rangle$ for

$i_{j-1}+1<i_{j-2}$. Then, $e_{j,i_{j-1}+1}(z)=0$, since $\deg(e_{j,i_{j-1}+1}(z))<t_{j-1}$. By substituting this in equation (15) and repeatedly applying the same argument a finite number of times, we get $e_{j,l}(z)=0$ for $i_{j-1}\le l<i_{j-2}$. Working in a similar manner for every $l\le \nu-1$, we can finally conclude that $w_j(z)-\mathfrak{u}_j(z)=0$. Hence, the generator polynomials $\mathfrak{u}_j(z)$ for $0\le j\le m$ are unique in C. □

Remark 11. It is observed that the unique set of generators obtained in Theorem 7 forms a Grobner basis for C over R.

4. MDS and MHDR Cyclic Codes over a Finite Chain Ring

In this section, the minimal spanning set and rank of a cyclic code C over a finite chain ring R have been established. Sufficient as well as necessary conditions for a cyclic code to be an MDS code and for a cyclic code to be an MHDR code have been obtained. Finally, to support our results, some examples of optimal cyclic codes have been presented.

Theorem 12. *Let C be a cyclic code having an arbitrary length n over a finite chain ring R. Then, rank$(C)=n-t_0$, where t_0 is the degree of minimal degree polynomial in C.*

Proof. Let C be a cyclic code having an arbitrary length n over R. Let $\{\mathfrak{u}_0(z),\mathfrak{u}_1(z),\ldots,\mathfrak{u}_m(z)\}$ be a unique set of generators for C as obtained above. Clearly, the set $S=\{\mathfrak{u}_m(z), z\mathfrak{u}_m(z),\ldots,z^{n-t_m-1}\mathfrak{u}_m(z),\mathfrak{u}_{m-1}(z),z\mathfrak{u}_{m-1}(z),\ldots, z^{n-t_{m-1}-1}\mathfrak{u}_{m-1}(z),\ldots,\mathfrak{u}_1(z), z\mathfrak{u}_1(z),\ldots,z^{n-t_1-1}\mathfrak{u}_1(z),\mathfrak{u}_0(z),z\mathfrak{u}_0(z),\ldots,z^{n-t_0-1}\mathfrak{u}_0(z)\}$ spans C. Now, we shall prove that $S'=\{\mathfrak{u}_m(z),z\mathfrak{u}_m(z),\ldots,z^{n-t_m-1}\mathfrak{u}_m(z),\mathfrak{u}_{m-1}(z),z\mathfrak{u}_{m-1}(z),\ldots,z^{t_m-t_{m-1}-1}\mathfrak{u}_{m-1}(z),\ldots,\mathfrak{u}_1(z),z\mathfrak{u}_1(z),\ldots,z^{t_2-t_1-1}\mathfrak{u}_1(z),\mathfrak{u}_0(z),z\mathfrak{u}_0(z),\ldots,z^{t_1-t_0-1}\mathfrak{u}_0(z)\}$ also spans C. For this, we need to prove that $z^{t_{j+1}-t_j}\mathfrak{u}_j(z)$ for $0\le j\le m-1$ are in span S'. We shall show this by induction on j. First, we prove that $z^{t_1-t_0}\mathfrak{u}_0(z)\in$ span S'. Clearly, $z^{t_1-t_0}\mathfrak{u}_0(z)$ is a polynomial of degree t_1 in C. Then, we have $z^{t_1-t_0}\mathfrak{u}_0(z)-\gamma^{i_0-i_1}\mathfrak{u}_1(z)=q_0(z)\mathfrak{u}_0(z)$ for some $q_0(z)\in R[z]$ with a degree less than t_1-t_0 which implies that $z^{t_1-t_0}\mathfrak{u}_0(z)-\gamma^{i_0-i_1}\mathfrak{u}_1(z)\in$ span S'. Therefore, we have $z^{t_1-t_0}\mathfrak{u}_0(z)\in$ span S'. We suppose that $z^{t_2-t_1}\mathfrak{u}_1(z)$, $z^{t_3-t_2}\mathfrak{u}_2(z),\ldots,z^{t_j-t_{j-1}}\mathfrak{u}_{j-1}(z)\in$ span S' for $1\le j\le m-1$. Now, we will show that $z^{t_{j+1}-t_j}\mathfrak{u}_j(z)\in$ span S'. Clearly, $z^{t_{j+1}-t_j}\mathfrak{u}_j(z)$ is a polynomial of degree t_{j+1} in C. Then, we have $z^{t_{j+1}-t_j}\mathfrak{u}_j(z)-\gamma^{i_j-i_{j+1}}\mathfrak{u}_{j+1}(z)\in\langle\mathfrak{u}_0(z),\mathfrak{u}_1(z),\ldots,\mathfrak{u}_j(z)\rangle$; and $z^{t_{j+1}-t_j}\mathfrak{u}_j(z)=\gamma^{i_j-i_{j+1}}\mathfrak{u}_{j+1}(z)+m_0(z)\mathfrak{u}_0(z)+m_1\mathfrak{u}_1(z)+\cdots+m_j\mathfrak{u}_j(z)$, where $m_i(z)\in R[z]$ and $\deg(m_i(z))<t_{i+1}-t_i$ for all i, $0\le i\le j$. This implies that $m_i\mathfrak{u}_i(z)\in$ span S' for $0\le i\le j$, which further implies that $z^{t_{j+1}-t_j}\mathfrak{u}_j(z)\in$ span S'. Therefore, we have $z^{t_{j+1}-t_j}\mathfrak{u}_j(z)\in$ span S' for all j, $0\le j\le m-1$.

Then, we prove the linear independence of S'. Let if possible, there exist $\alpha_{j,r}\in R$ such that

$$\begin{aligned}z^{n-t_m-1}\mathfrak{u}_m(z)=&\alpha_{m,0}\mathfrak{u}_m(z)+\alpha_{m,1}z\mathfrak{u}_m(z)+\cdots+\alpha_{m,n-t_m-2}z^{n-t_m-2}\mathfrak{u}_m(z)\\&+\alpha_{m-1,0}\mathfrak{u}_{m-1}(z)+\alpha_{m-1,1}z\mathfrak{u}_{m-1}(z)+\cdots\\&+\alpha_{m-1,t_m-t_{m-1}-1}z^{t_m-t_{m-1}-1}\mathfrak{u}_{m-1}(z)+\cdots\\&+\alpha_{1,0}\mathfrak{u}_1(z)+\alpha_{1,1}z\mathfrak{u}_1(z)+\cdots+\alpha_{1,t_2-t_1-1}z^{t_2-t_1-1}\mathfrak{u}_1(z)\\&+\alpha_{0,0}\mathfrak{u}_0(z)+\alpha_{0,1}z\mathfrak{u}_0(z)+\cdots+\alpha_{0,t_1-t_0-1}z^{t_1-t_0-1}\mathfrak{u}_0(z).\end{aligned}\tag{18}$$

This implies that $z^{n-t_m-1}\mathfrak{u}_m(z)=\alpha_m(z)\,\mathfrak{u}_m(z)+\alpha_{m-1}(z)\mathfrak{u}_{m-1}(z)+\cdots+\alpha_0(z)\mathfrak{u}_0(z)$, where $\alpha_m(z)=\alpha_{m,0}+\alpha_{m,1}z+\cdots+\alpha_{m,n-t_m-2}z^{n-t_m-2}$ and $\alpha_i(z)=\alpha_{i,0}+\alpha_{i,1}z+\cdots+\alpha_{i,t_{i+1}-t_i-1}z^{t_{i+1}-t_i-1}$ for $0\le i\le m-1$. Clearly, $\deg(\alpha_m(z))\le n-2$ and $\deg(\alpha_i(z))\le t_{i+1}-1$ for all i, $0\le i\le m-1$. Then, by multiplying equation (18) by $\gamma^{\nu-i_{m-1}}$, we get

$$z^{\nu-t_m-1}\gamma^{\nu-i_{m-1}}\mathfrak{u}_m(z)=\alpha_m(z)\gamma^{\nu-i_{m-1}}\mathfrak{u}_m(z).\tag{19}$$

Then, the degree of LHS of equation (19) is $n-1$ but that of RHS is atmost $n-2$ which is a contradiction. Therefore, $z^{n-t_m-1}\mathfrak{u}_m(z)$ cannot be expressed as a linear combination of elements of S'. We can apply similar arguments to prove that none of $z^{t_m-t_{m-1}-1}\mathfrak{u}_{m-1}(z)$, $z^{t_{m-1}-t_{m-2}-1}\mathfrak{u}_{m-2}(z),\ldots,z^{t_1-t_0-1}\mathfrak{u}_0(z)$ can be expressed as a linear combination of elements of S'. Therefore, we get that S' is linearly independent, and hence, it is a minimal spanning set for C. It follows that rank$(C)=n-t_0$.

The following theorem determines all the MDS cyclic codes of arbitrary length over a finite chain ring R. □

Theorem 13. *A cyclic code C having a length n over R is an MDS if and only if it is principally generated by a monic polynomial and $Tor_0(C)$ is an MDS cyclic code having a length n over $\top$ with respect to Hamming metric.*

Proof. Let $C=\langle\mathfrak{u}_0(z),\mathfrak{u}_1(z),\ldots,\mathfrak{u}_m(z)\rangle$ be an MDS cyclic code having a length n over R such that $\mathfrak{u}_j(z)$, $0\le j\le m$ are polynomials as in Theorem 10. Since C is an MDS, therefore, $|C|=|R|^{n-d_H(C)+1}$. By using Theorem 7, we have $p^{s(n\nu-ni_m-t_0k_0-t_1k_1-\cdots-t_mk_m)}=p^{s\nu(n-d_H(C)+1)}$ which implies that $ni_m+t_0k_0+t_1k_1+\cdots+t_mk_m=\nu(d_H(C)-1)$. Thus, we can

conclude that $t_j = 0$ for $1 \le j \le m$ and $i_m = 0$ because $i_m + k_0 + k_1 + \cdots + k_m = \nu$ and $t_m > t_{m-1} > \cdots > t_0 \ge d_H(C) - 1$. This implies that C is principally generated by a monic polynomial and $t_0 = d_H(C) - 1$. By using Theorems 7 and 8, we have $|\top|^{(n - d_H(Tor_0(C))+1)} = p^{s(n - d_H(Tor_0(C))+1)} = p^{s(n-d_H(C)+1)} = p^{s(n-t_0)} = |Tor_0(C)|$. Thus, $Tor_0(C)$ is an MDS cyclic code over the residue field $\top$.

Conversely, suppose a cyclic code C having a length n over R is principally generated by a monic polynomial, say $\mathbf{u}_0(z)$ as obtained in Theorem 10 and $Tor_0(C)$ is an MDS code over $\top$. Then, this means that $i_0 = 0$ and $|Tor_0(C)| = |\top|^{(n - d_H(Tor_0(C))+1)}$. By using Theorems 7 and 8, we can conclude that $|R|^{n-d_H(C)+1} = p^{s\nu(n - d_H(Tor_0(C))+1)} = p^{s\nu(n-t_0)} = |C|$, i.e., C is an MDS cyclic code over R.

The following lemma by Sharma and Sidana determines the Hamming distance of a cyclic code C of length $n' p^r$, $(n', p) = 1$, and $r \ge 1$ over a finite chain ring R as given in reference [27]. □

Lemma 14 (see [27]). *Let C be a cyclic code having a length $n = n' p^r$ for $(n', p) = 1$ and $r \ge 1$ over R. Then, we have*

$$d_H(C) = \begin{cases} 1, & if\ t_0 = 0, \\ l + 2, & if\ lp^{r-1} + 1 \le t_0 \le (l+1)p^{r-1}, \\ & \text{with } 0 \le l \le p - 2, \\ (i+1)p^k, & if\ p^r - p^{r-k} + (i-1)p^{r-k-1} + 1 \le t_0 \le p^r - p^{r-k} + ip^{r-k-1}, \\ & \text{with } 1 \le i \le p-1 \text{ and } 1 \le k \le r-1. \end{cases} \tag{20}$$

We use Lemma 14 mentioned above to determine all MHDR cyclic codes of length $n' p^r$, $(n', p) = 1$ and $r \ge 1$ over R in Theorems 15 and 16.

Theorem 15. *A cyclic code C of length $n' p$, $(n', p) = 1$ over a finite chain ring R is an MHDR code.*

Proof. Let C be a cyclic code of length $n' p$, $(n', p) = 1$ over R. By Lemma 14, we have

$$d_H(C) = \begin{cases} 1, & \text{if } t_0 = 0, \\ t_0 + 1, & \text{if } 1 \le t_0 \le p - 1, \end{cases} \tag{21}$$

which implies that $d_H(C) = t_0 + 1 = n - \text{rank}(C) + 1$ for $0 \le t_0 \le p - 1$ by using Theorem 12. Hence, a cyclic code of length $n' p$, $(n', p) = 1$ over R is always an MHDR code. □

Theorem 16. *Let C be a cyclic code having a length $n = n' p^r, r > 1$ over R. Then, C is an MHDR if and only if $t_0 \in \{0, 1, p^r - 1\}$.*

Proof. By Lemma 14, we have the following:

(i) for $t_0 = 0$, the Hamming distance of C is 1, which is the same as $n - \text{rank}(C) + 1$ by using Theorem 12. So, C is an MHDR code.

(ii) for $lp^{r-1} + 1 \le t_0 \le (l+1)p^{r-1}$ with $0 \le l \le p - 2$, the Hamming distance of C is $l + 2$. Here, C is an MHDR if and only if $d_H(C) = n - \text{rank}(C) + 1$, i.e., $l + 1 = t_0$ by using Theorem 12. Then, $lp^{r-1} + 1 \le t_0$ would imply $lp^{r-1} + 1 \le l + 1$, i.e., $l(p^{r-1} - 1) \le 0$. It follows that $l(p^{r-1} - 1) = 0$, which implies $l = 0$, since $p^{r-1} \ne 1$. Then, C is an MHDR if and only if $t_0 = 1$.

(iii) for $k = r - 1$, $t_0 = p^r - p + i, 1 \le i \le p - 1$, the Hamming distance of C is $(i+1)p^{r-1}$. C is an MHDR code if and only if $(i+1)p^{r-1} = n - \text{rank}(C) + 1 = t_0 + 1$ by using Theorem 12. Then, we have $p^r - p + i = t_0 = (i+1)p^{r-1} - 1$. It follows that $p(p^{r-1} - 1) = (i+1)(p^{r-1} - 1)$, which implies that $i = p - 1$, since $p^{r-1} \ne 1$. Then, C is an MHDR for $t_0 = p^r - 1$. It can be easily seen that for other values of t_0, C is not an MHDR code. □

Theorem 17. *Let C be an MDS cyclic code having an arbitrary length over R. Then, C is also an MHDR code over R.*

Proof. Let C be an MDS cyclic code having an arbitrary length n over R. By Theorem 13, C is principally generated by a monic polynomial over R say $\mathbf{u}_0(z)$ with degrees t_0 and $i_0 = 0$ and Tor $_0(C)$ is also an MDS code over $\top$. Then, we have

$$|Tor_0(C)| = p^{s(n - d_H(C)+1)}. \tag{22}$$

Also, from Theorem 7, we have

$$|Tor_0(C)| = p^{s(n-t_0)}. \tag{23}$$

Equations (22) and (23) together with Theorem 12 imply that $d_H(C) = t_0 + 1 = n - \text{rank}(C) + 1$. Therefore, C is an MHDR cyclic code over R. □

However, Example 1 shows that the converse of the abovementioned statement is not true.

Example 1. Let $R = Z_5 + 5Z_5$. Let $C = \langle 5, (z-1)^{24} \rangle$ be a cyclic code having a length $n = 25$ over R. Here, $i_0 = 1, i_1 = 0, t_0 = 0$, $t_1 = 24$, $\text{rank}(C) = 25$, and $d_H(C) = 1$.

By using Theorem 16, we see that C is an MHDR cyclic code over R. However, C is not an MDS code, since it is not principally generated (using Theorem 17).

Example 2. Let $R = Z_5 + 5Z_5$. Let $C = \langle (z-1)^{24} \rangle$ be a cyclic code having a length $n = 25$ over R. Here, $i_0 = 0$, $t_0 = 24$, $\text{rank}(C) = 1$, and $d_H(C) = 24$. By using Theorem 16, we see that C is an MHDR cyclic code over R. Also, C is an MDS code, since it is principally generated by a monic polynomial and $|Tor_0(C)| = 5 = |Z_5|^{n-d_H(Tor_0(C))+1}$ (using Theorem 13).

Example 3. Let $R = Z_2 + \gamma Z_2 + \gamma^2 Z_2 + \gamma^3 Z_2$. Let $C = \langle (z^2 - 1) + \gamma(z-1) + \gamma^2(z-1) + \gamma^3 \rangle$ be a cyclic code having a length $n = 6$ over R. Here, $i_0 = 0$, $t_0 = 2$, $\text{rank}(C) = 4$, and $d_H(C) = 3$. It is principally generated by a monic polynomial and $|Tor_0(C)| = 2^4 = |Z_2|^{n-d_H(Tor_0(C))+1} = 2^{6-3+1} = 2^4$, so we see that C is an MDS code over R by using Theorem 13. Also, from Theorem 15, we see that C is also an MHDR code.

Example 4. Let $R = Z_2 + \gamma Z_2 + \gamma^2 Z_2 + \gamma^3 Z_2$. Let $C = \langle \gamma^2 (z^3 - 1) + \gamma^3 (z^2 - 1) \rangle$ be a cyclic code having a length $n = 6$ over R. Here, $i_0 = 2$, $t_0 = 3$, $\text{rank}(C) = 3$, and $d_H(C) = 2$. It is not generated by a monic polynomial, so by Theorem 13, C is not an MDS code. Also, from Theorem 15, we see that C is not an MHDR code.

Example 5. Let $R = Z_3 + \gamma Z_3 + \gamma^2 Z_3$. Let $C = \langle \gamma^2 (z^2 - 1), \gamma (z^2 - 1)^3 + \gamma^2 (z-1) \rangle$ be a cyclic code having a length $n = 18$ over R. Here, $i_0 = 2$, $i_1 = 1\, t_0 = 2$, $t_1 = 6$, $\text{rank}(C) = 16$, and $d_H(C) = 2$. Since C is not generated by a monic polynomial, so by Theorem 13, it is not an MDS code. Also, from Theorem 16, we see that C is not an MHDR code.

5. Conclusion

In this work, a unique set of generators for a cyclic code having an arbitrary length over a finite chain ring with an arbitrary nilpotency index has been established. The minimal spanning set and rank of the code have also been determined. Furthermore, sufficient as well as necessary conditions for a cyclic code having an arbitrary length to be an MDS code and for a cyclic code having a length which is not coprime to the characteristic of the residue field of the ring to be an MHDR code have been obtained. Some examples of optimal cyclic codes have also been presented.

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Disclosure

A preprint has previously been published [30].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Monika Dalal and Ranjeet Sehmi equally contributed to this work.

Acknowledgments

This research was supported by the Council of Scientific and Industrial Research (CSIR), India, in the form of research fellowship to the first author.

References

[1] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The Z_4-linearity of kerdock, preparata, goethals, and related codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[2] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic codes," *Designs, Codes and Cryptography*, vol. 6, pp. 21–35, 1995.

[3] J. L. Massey, "Reversible codes," *Information and Control*, vol. 7, pp. 369–380, 1964.

[4] H. Islam and O. Prakash, "Construction of reversible cyclic codes over Z_p^k," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 6, pp. 1817–1830, 2022.

[5] O. Prakash, S. Patel, and S. Yadav, "Reversible cyclic codes over some finite rings and their application to DNA codes," *Computational and Applied Mathematics*, vol. 40, no. 7, p. 17, 2021.

[6] H. Islam, O. Prakash, and D. K. Bhunia, "On the structure of cyclic codes over $M_2(F_p+uF_p)$," *Indian Journal of Pure and Applied Mathematics*, vol. 53, no. 1, pp. 153–161, 2022.

[7] H. Islam, O. Prakash, and P. Sol´e, "Z_4Z_4 [u]-additive cyclic and constacyclic codes," *Advances in Mathematics of Communications*, vol. 15, no. 4, pp. 737–755, 2021.

[8] H. Islam and O. Prakash, "A study of cyclic and constacyclic codes over $Z_4+uZ_4+vZ_4$," *International Journal of Information and Coding Theory*, vol. 5, no. 2, pp. 155–168, 2018.

[9] A. Garg and S. Dutt, "Determining minimal degree polynomials of a cyclic code of length 2^kover Z_8," *CALDAM*, vol. 10743, pp. 118–130, 2018.

[10] T. Abualrub and I. Siap, "Reversible cyclic codes over Z_4," *Australian Journal of Combinatorics*, vol. 38, pp. 196–205, 2007.

[11] T. Abualrub and R. Oehmke, "On Generators of Z_4cyclic codes of length 2^e," *IEEE Transactions on Information Theory*, vol. 49, no. 9, pp. 2126–2133, 2003.

[12] T. Abualrub and I. Siap, "Cyclic codes over the rings Z_2+u Z_2 and $Z_2+u\,Z_2+u^2\,Z_2$," *Designs, Codes and Cryptography*, vol. 42, pp. 273–287, 2007.

[13] H. Q. Dinh, "Constacyclic codes of length psover $F_p^m+u\,F_p^m$," *Journal of Algebra*, vol. 324, no. 5, pp. 940–950, 2010.

[14] H. M. Kiah, K. H. Leung, and S. Ling, "Cyclic codes over GR(p^2,m)of length p^k," *Finite Fields and Their Applications*, vol. 14, pp. 834–846, 2008.

[15] A. Sharma and T. Sidana, "On the structure and distances of repeated-root constacyclic codes of prime power lengths over finite commutative chain rings," *IEEE Transactions on Information Theory*, vol. 65, pp. 1072–1084, 2018.

[16] G. H. Norton and A. Salagean, "On the structure of linear and cyclic codes over a finite chain ring," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, pp. 489–506, 2000.

[17] G. H. Norton and A. Salagean, "Cyclic codes and minimal strong Grobner bases over a principal ideal ring," *Finite Fields and Their Applications*, vol. 9, pp. 237–249, 2003.

[18] A. Salagean, "Repeated-root cyclic and negacyclic codes over a finite chain ring," *Discrete Applied Mathematics*, vol. 154, pp. 413–419, 2006.
[19] J. Kaur, S. Dutt, and R. Sehmi, "On cyclic codes over Galois rings," *Discrete Applied Mathematics*, vol. 280, pp. 156–161, 2020.
[20] Monika, S. Dutt, and R. Sehmi, "On cyclic codes over finite chain rings," *Journal of Physics: Conference Series*, vol. 1850, pp. 1–6, 2021.
[21] M. Dalal, S. Dutt, and R. Sehmi, "Reversible cyclic codes over finite chain rings," https://arxiv.org/abs/2307.09156.
[22] H. Q. Dinh and S. R. L. Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1728–1744, 2004.
[23] T. Sidana and A. Sharma, "Repeated-root constacyclic codes over the chain ring $F_p{}^m[u]/<u^3>$," *IEEE Transactions on Information Theory*, vol. 8, 2017.
[24] M. M. Al-Ashker and J. Chen, "Cyclic codes of arbitrary length over $F_q+uF_q+...+U^{K-1}F_q$," *Palestine Journal of Mathematics*, vol. 2, no. 1, pp. 72–80, 2013.
[25] S. T. Dougherty and S. Ling, "Cyclic codes over Z_4 of even length," *Designs, Codes and Cryptography*, vol. 39, pp. 127–153, 2006.
[26] H. Q. Dinh, A. Singh, P. Kumar, and S. Sriboonchitta, "Cyclic codes over $GR(p^e,m)[u]/<u^k>$," *Discrete Mathematics*, vol. 343, 2020.
[27] A. Sharma and T. Sidana, "Repeated-root constacyclic codes over finite commutative chain rings and their distances," 2017, http://arxiv.org/abs/1706.06269v2.
[28] M. Al-Ashker and M. Hamoudeh, "Cyclic codes over $Z_2+u Z_2+...+u^{k-1} Z_2$," *Turkish Journal of Mathematics*, vol. 35, pp. 737–749, 2011.
[29] T. Abualrub and R. Oehmke, "Cyclic codes of length 2^e over Z_4," *Discrete Applied Mathematics*, 2003.
[30] M. Dalal, S. Dutt, and R. Sehmi, "MDS and MHDR cyclic codes over finite chain rings," 2023, https://arxiv.org/abs/2303.15819.