On cyclic codes over finite chain rings

Monika$^1$, Sucheta Dutt$^2$ and Ranjeet Sehmi$^{3*}$

$^{1,2,3}$ Punjab Engineering College (Deemed to be University), Chandigarh, India

E-mail: rsehmi@pec.edu.in

Abstract. Recent studies involve various approaches to establish a generating set for cyclic codes of arbitrary length over the class of Galois rings. One such approach involves the use of polynomials with minimal degree corresponding to specific subsets of the code, defined progressively. In this paper, we extend this approach to obtain a set of generators of cyclic codes over finite chain rings. Further, we observe that this set acts as a minimal strong Gröbner basis (MSGB) for the code.

1. Introduction

One of the major goals of channel coding from mathematical perspective, is to construct codes in such a way that maximum information is transferred per unit time and it is also able to detect and correct maximum number of errors. To study both of these properties, we first need to know the structure of a code. Let $R$ be a commutative ring with identity. A linear code of arbitrary length $n$ over $R$ is defined as a subset $C$ of $R^n$, which is an $R$-submodule of $R^n$. A linear code of length $n$ is known as a cyclic code if for any codeword $s = (s_0, s_1, \cdots, s_{n-1})$ of $C$, all the cyclic shifts of $s$ also belong to $C$. For example, $\{(0, 0, 0), (0, 1, 1), (1, 1, 0), (1, 0, 1)\}$ is a cyclic code of length 3 over $\mathbb{Z}_2$. Further, by identifying the codeword $(s_0, s_1, \cdots, s_{n-1}) \in R^n$ with the polynomial $s_0 + s_1 z + \cdots + s_{n-1} z^{n-1} \in R[z]/<z^n-1>$, these codes can also be recognized as the ideals of $R_n$. Throughout this paper, $R$ is considered to be a finite chain ring. A ring whose ideals can be linearly ordered by inclusion is called a finite chain ring. It is a known fact that a finite chain ring is a local ring. A description of cyclic codes over the class of finite chain rings is well explored by Xiusheng LIU [2]. In his work, the requirements for a code over $R$ to be cyclic are transformed into those over its residue field. Another approach on structure of such codes is explored by Norton and Salagean([3],[4],[5],[6]). The structure and properties of these codes can be examined easily if their generators are known. Recent studies involve various approaches for finding the generators of cyclic codes over Galois rings. One such approach which involves the use of minimal degree polynomials is given by T. Abulrub and R. Oehmke in the study of cyclic codes over $\mathbb{Z}_4$([7],[8]). It is further extended by A. Garg and S. Dutt over the integer residue rings [9] and by J. Kaur et. al over the class of Galois rings [1].

In this paper, we extend this approach to establish a set of generators of cyclic codes of arbitrary length over finite chain rings. Further, we observe that these generators form a MSGB for the code.

2. Preliminaries

Let us state certain definitions [2].

Suppose $R$ is a finite chain ring. Let $M$ be its unique maximal ideal generated by $\gamma$, i.e. $M = \gamma R$.
\[ <\gamma> = R\gamma = \{\alpha\gamma : \alpha \in R\}. \]  

Then,  
\[ R = <\gamma^0 > \supset <\gamma^1 > \supset <\gamma^2 > \supset \ldots \supset <\gamma^i > \supset \ldots \]  
is a chain of ideals of \( R \) which terminates to the trivial ideal \( \{0\} \) of \( R \). So there is a smallest integer \( \nu \) for which \( \{\gamma^\nu\} = \{0\} \). This integer \( \nu \) denotes the nilpotency index of \( \gamma \). Also all the zero divisors of \( R \) along with its zero element make the maximal ideal \( M \) and all the units of \( R \) lie outside \( M \). We shall denote such a finite chain ring \( R \) by \( FR(\gamma, \nu) \). Suppose \( F = R/<\gamma> \) is the residue field of \( FR(\gamma, \nu) \) with a prime characteristic say \( p \). There is a canonical map from the ring \( R \) to its residue field \( F \) which can be naturally extended to a projection \( \phi : R[z] \to F[z] \), where \( R[z] \) and \( F[z] \) represent the polynomial rings over \( R \) and \( F \) respectively. For any \( I(z) \in R[z] \), let \( \hat{I}(z) = \phi(\{I(z)\}) \) and for \( C \subseteq R[z] \), let  
\[ \hat{C} = \{\hat{I}(z) | (z) \in C\}. \]  

A polynomial in \( R[z] \) is said to be a monic polynomial if coefficient of its leading term is 1. Also, \( I(z) \in R[z] \) is a unit in \( R[z] \) iff \( \hat{I}(z) \) is a unit in \( F[z] \). A basic irreducible polynomial over \( R \) is a non-unit \( I(z) \in R[z] \) such that \( \hat{I}(z) \) is an irreducible polynomial over \( F \).

Next, we introduce some basic results.

**Lemma 2.1** (Proposition 2.2, [5]). Consider the ring \( FR(\gamma, \nu) \).

(i) For any element \( a \in FR(\gamma, \nu) \), \( a \neq 0 \) there is a unit \( u \in FR(\gamma, \nu) \) and a unique \( i \leq \nu - 1 \), \( i \in \{0\} \cup Z^+ \) such that \( a = u\gamma^i \) and \( u \) is unique modulo \( \gamma^{\nu-i} \);  
(ii) \( Ann(\gamma^i) = <\gamma^{\nu-i}> \).

The following lemma gives a unique representation of every element in a finite chain ring.

**Lemma 2.2** (Proposition 2.2, [10]). Consider the ring \( FR(\gamma, \nu) \).

(i) There exists an element \( \beta \in FR(\gamma, \nu) \) with multiplicative order \( p^{m-1} \). Also, it is possible to express any element \( s \in FR(\gamma, \nu) \) uniquely as \( s = s_0 + s_1\gamma + s_2\gamma^2 + \ldots + s_{\nu-1}\gamma^{\nu-1} \), where \( s_i \in T = \{0, 1, \beta, \ldots, \beta^{p^{m-2}} \} \) for \( 0 \leq i \leq \nu - 1 \). (Here, \( T = \{0, 1, \beta, \ldots, \beta^{p^{m-2}} \} \) is known as the Teichmuller set of \( FR(\gamma, \nu) \));  
(ii) Let \( s = s_0 + s_1\gamma + s_2\gamma^2 + \ldots + s_{\nu-1}\gamma^{\nu-1} \), where \( s_i \in T \) for \( 0 \leq i \leq \nu - 1 \). Then \( s \) is a unit in \( FR(\gamma, \nu) \) iff \( s_0 \neq 0 \). Moreover, there exists \( a_0 \in T \) satisfying \( a_0^\nu = s_0 \).

**Lemma 2.3** (Theorem 3.2, [4]). A subset \( G \) of \( FR(\gamma, \nu)[z] \) is said to be a MSGB iff \( G = \{s_0q_0, s_1q_1, \ldots, s_rq_r \} \) for some \( r \leq \nu - 1 \), where  
(i) \( s_i = \gamma^i \) for \( 0 \leq i_0 \leq \cdots \leq i_r \leq \nu - 1 \) and \( lc(q_i(z)) \) is a unit in \( FR(\gamma, \nu) \) for \( i \leq r \);  
(ii) \( deg(q_i) > deg(q_{i+1}) \) for \( i \leq r - 1 \);  
(iii) \( s_{i+1}q_i \in <s_{i+1}q_{i+1}, \cdots, s_rq_r> \) for \( i \leq r - 1 \).

3. Generators

Consider a cyclic code \( C \) over \( R = FR(\gamma, \nu) \). It is an ideal of \( R_m \). Consider the subset of \( C \) containing all those polynomials which have minimum degree in \( C \). Denote this set by \( S_0 \). Choose the polynomial in \( S_0 \) which has least power of \( \gamma \) in its leading coefficient \( (lc) \). Denote this polynomial by \( f_0(z) \). Suppose \( lc(f_0(z)) = \gamma^{i_0}u_0 \), where \( u_0 \) is some unit in \( R \) and \( 0 \leq i_0 \leq \nu - 1 \). If
\( i_0 = 0 \) then \( f_0(z) \) is a monic polynomial. Otherwise, define \( S_1 \) to be the subset of \( C \) containing all those polynomials whose leading coefficients contain a power of \( \gamma \) less than \( i_0 \). First, select all the least degree polynomials of \( S_1 \) and then out of these choose the one with smallest power of \( \gamma \) in its leading coefficient. Denote this polynomial by \( f_1(z) \) and let the power of \( \gamma \) in \( \text{lc}(f_1(z)) \) be \( i_1 \). Clearly, \( \text{deg}(f_1(z)) > \text{deg}(f_0(z)) \) and \( i_1 < i_0 \). Now, successively define \( S_k \) for \( k = 2, 3, \cdots \) to be the subset of \( C \) containing all those polynomials whose leading coefficients contain a power of \( \gamma \) which is less than \( i_{k-1} \), where \( i_{k-1} \) is the power of \( \gamma \) in \( \text{lc}(f_{k-1}(z)) \). Here, the method of choosing \( f_{k-1}(z) \) remains the same as that of \( f_1(z) \), which means that \( f_{k-1}(z) \) is the polynomial of \( S_{k-1} \) having smallest power of \( \gamma \) in its leading coefficient among all the least degree polynomials in \( S_{k-1} \). Clearly, \( i_0 > i_1 > \cdots \) is a sequence of non negative integers. So, there will exist a positive integer \( m \) such that \( i_m \) becomes the smallest power of \( \gamma \) among the leading coefficient of all the polynomials in \( S_m \) and the sequence terminates. Let \( t_k \) be the degree of \( f_k(z) \) for \( k = 0, 1, \cdots, m \). Clearly, \( t_0 < t_1 < \cdots < t_m \).

**Remark 1**: It is easy to observe that \( i_m \), the power of \( \gamma \) in \( \text{lc}(f_m(z)) \) is the smallest among those in leading coefficients of all the polynomials in \( C \).

**Remark 2**: Let \( k(z) \) be a polynomial in \( C \). Let \( i \) be the power of \( \gamma \) in its leading coefficient. It is easy to see that there is a largest integer \( j \) with \( 0 \leq j \leq m \) such that \( \text{deg}(k(z)) \geq t_j \) and \( i \geq i_j \). The polynomial

\[
c(z) = k(z) - \gamma^{i-i_j} f_j(z) u z^{\text{deg}(k(z))-t_j}
\]

either vanishes or \( \text{deg}(c(z)) < \text{deg}(k(z)) \) for some unit \( u \) in \( R \). Clearly, \( c(z) \in C \) and for some polynomial \( b(z) \in R_n \),

\[
c(z) = k(z) - b(z)f_j(z).
\]

In the next theorem we obtain generators for a cyclic code over \( FR(\gamma, \nu) \).

**Theorem 3.1**: Consider a cyclic code \( C \) over \( FR(\gamma, \nu) \). Let \( f_i(z), \ 0 \leq i \leq m \), be the polynomials as described above. Then \( C \) is generated by the set \( \{ f_i(z); \ i = 0, 1, \cdots, m \} \).

**Proof**: Let \( g(z) \) be an arbitrary polynomial in \( C \). Then, Remark 2 supports the existence of a largest integer \( j \) such that \( \text{deg}(g(z)) \geq t_j \), \( 0 \leq j \leq m \) and a polynomial \( q_1(z) \in R_n \) such that the polynomial

\[
r_1(z) = g(z) - q_1(z)f_j(z)
\]

remains in \( C \). Moreover, either \( r_1(z) \) is zero or \( \text{deg}(r_1(z)) \) is less than \( \text{deg}(g(z)) \).

If \( r_1(z) = 0 \), then \( g(z) = q_1(z)f_j(z) \), i.e. \( g(z) \in \langle f_j(z) \rangle \).

Otherwise, if \( \text{deg}(r_1(z)) < \text{deg}(g(z)) \), then again there exists a largest integer \( k \) such that \( \text{deg}(r_1(z)) \geq t_k \), \( 0 \leq k \leq j \leq m \) and a polynomial \( q_2(z) \in R_n \) such that the polynomial

\[
r_2(z) = r_1(z) - q_2(z)f_k(z)
\]

remains in \( C \). Moreover, \( r_2(z) \) is zero or \( \text{deg}(r_2(z)) \) is less than \( \text{deg}(r_1(z)) \). If \( r_2(z) = 0 \),

\[
g(z) = q_2(z)f_k(z) + q_1(z)f_j(z).
\]

Therefore, in this case \( g(z) \in \langle f_k(z), f_j(z) \rangle \). Otherwise, if \( \text{deg}(r_2(z)) < \text{deg}(r_1(z)) \), then by applying the above argument a limited number of times, and using the minimality of \( \text{deg}(f_0(z)) \)
in $C$, the remainder vanishes ultimately. Filling in for the remainders backwards, we can easily conclude that
\[ g(z) \in < f_j(z), f_k(z), \cdots, f_m(z) >. \]
Hence, we have
\[ C \subseteq < f_0(z), f_1(z), \cdots, f_m(z) > \]
which proves that
\[ C = < f_0(z), f_1(z), \cdots, f_m(z) >. \]
\[ \square \]

**Corollary 3.2** : An arbitrary length cyclic code over $FR(\gamma, \nu)$ can have at most $\min\{\nu, t_m + 1\}$ generators, where $t_m = \deg(f_m(z))$.

The result that a cyclic code over a field is principally generated follows from Corollary 3.2 as a special case for $\nu = 1$.

**Theorem 3.3** : Let $f_0(z)$ be the polynomial as described earlier. Then $f_0(z) = \gamma^i\nu h_0(z)$, where $h_0(z)$ is monic in $R^0[z]/ < z^n - 1 >$, $R^0 = FR(\gamma, \nu - i_0)$ and $i_0$ is the power of $\gamma$ in $lc(f_0(z))$.

**Proof** : Let $f_0(z) = \gamma^i\nu u_0 z^k + b_{t_0 - 1} z^{t_0 - 1} + \cdots + b_1 x + b_0$, where $b_j \in R$ for $0 \leq j \leq t_0 - 1$. If possible, suppose $b_j \neq 0$ (mod $\gamma^i\nu$) for some $j$. Now $\gamma^{j - t_0} f_0(z)$ is a polynomial in $C$ with degree lesser than $t_0$ which is a negation to the fact that $\deg(f_0(z))$ is minimum in $C$. Hence, $b_j \equiv 0$ (mod $\gamma^i\nu$) for every $j$. Thus, $f_0(z) = \gamma^i\nu h_0(z)$, where $h_0(z)$ is monic in $R^0[z]/ < z^n - 1 >$ and $R^0 = FR(\gamma, \nu - i_0)$.

**Theorem 3.4** : Let $f_j(z)$ be polynomials as described previously. Then

(i) $\gamma^{j-1-i} f_j(z) \in < f_0(z), f_1(z), \cdots, f_{j-1}(z) >$;
(ii) $f_j(z) = \gamma^i h_j(z)$, where $h_j(z)$ is monic in $R^j[z]/ < z^n - 1 >$ and $R^j = FR(\gamma, \nu - i_j)$, for $0 \leq j \leq m$;
(iii) $h_{j-1}(z)|h_j(z) (\bmod \gamma^{j-2-i_{j-1}})$, for $2 \leq j \leq m$;
(iv) $h_0(z)|h_1(z) (\bmod \gamma^i)$;
(v) $h_m(z)|(z^n - 1) (\bmod \gamma^{m-1-i_m})$.

**Proof**:

(i) The polynomial $\gamma^{j-1-i} f_j(z) - z^{t_j - t_{j-1}} f_{j-1}(z)$ is in $C$ and has degree less than $t_j$. Proceeding as in Theorem 3.1, we have an integer $k < j$ so that $\gamma^{j-1-i} f_j(z) - z^{t_j - t_{j-1}} f_{j-1}(z) \in < f_0(z), f_1(z), \cdots, f_k(z) >$ implying that
\[ \gamma^{j-1-i} f_j(z) \in < f_0(z), f_1(z), \cdots, f_{j-1}(z) >. \]

(ii) We shall proceed by mathematical induction to prove this part. The result holds for $j = 0$ from the previous theorem. Suppose it is true for the polynomials $f_k(z)$, $1 \leq k \leq j - 1$. Now using first part of this theorem, it can be easily grasped that there exist polynomials $A_k(z)$, $0 \leq k \leq j - 1$ in $R_n$ such that
\[ \gamma^{j-1-i} f_j(z) = \sum_{k=0}^{j-1} \gamma^i h_k(z) A_k(z), \]
\[ = \gamma^{j-1} \sum_{k=0}^{j-1} \gamma^{i-k-j-1} h_k(z) A_k(z). \]
Now, suppose there exists a coefficient $f_k$ of the polynomial $f_j(z)$ such that $f_k \neq 0 \pmod{\gamma^i}$. Multiplying the above equation by $\gamma^i z^{j-1}$ on both sides, we get $\gamma^i z^{j-1} f_j(z) = 0$, which is a contradiction. Therefore, $f_j(z) = \gamma^i h_j(z)$, where $h_j(z)$ is monic in $R[z]/<z^n - 1>$ and $R' = FR(\gamma, \nu - i_j)$.

(iii) For $1 \leq k \leq \nu - 1$ consider the map $\Psi_k : FR(\gamma, \nu) \rightarrow FR(\gamma, k)$ defined as $c \mapsto c \pmod{\gamma^i}$. Clearly, $\Psi_k$ is a ring homomorphism for every $k$. We can extend it to a homomorphism

$$\Phi_k : FR(\gamma, \nu)[z]/<z^n - 1> \rightarrow FR(\gamma, k)[z]/<z^n - 1>$$

as $\Phi_k(c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}) = \Psi_k(c_0) + \Psi_k(c_1) z + \cdots + \Psi_k(c_{n-1}) z^{n-1}$. Now using part (i) and (ii) of this theorem, we have $\gamma^{j-1} h_j(z) \in <f_0(z), f_1(z), \cdots, f_{j-1}(z)>$ implying that

$$\gamma^{j-1} h_j(z) = \sum_{k=0}^{j-1} \gamma^k h_k(z) A_k(z),$$

where $A_k(z) \in R_n$ for $0 \leq k \leq j-1$. Therefore, $\gamma^{j-1}(h_j(z) - h_{j-1}(z) A_{j-1}(z)) = 0$, where $A(z) = \sum_{k=0}^{j-2} \gamma^k z^{-2} h_k(z) A_k(z)$. Consequently, either $h_j(z) = h_{j-1}(z) A_{j-1}(z) - \gamma^{j-2-i_j} A(z) = 0$ or the power of $\gamma$ in each of its coefficient is either equal to or greater than $\nu - i_j$. As $<\gamma^{j-1} h_j > \subset <\gamma^{j-2-i_j} >$ the coefficients of the polynomial $h_j(z) - h_{j-1}(z) A_{j-1}(z) - \gamma^{j-2-i_j} A(z)$ vanish modulo $\gamma^{j-2-i_j}$ in both the cases. Thus,

$$h_j(z) - h_{j-1}(z) A_{j-1}(z) \equiv h_j(z) - h_{j-1}(z) A_{j-1}(z) - \gamma^{j-2-i_j} A(z),$$

$$\equiv 0 \pmod{\gamma^{j-2-i_j}}.$$ 

Therefore, $\Phi_{j-2-i_j}(h_j(z) - h_{j-1}(z) A_{j-1}(z)) = 0$ which together with the fact that $\Phi_{j-2-i_j}$ is a homomorphism implies that $\Phi_{j-2-i_j}(h_j(z)) = \Phi_{j-2-i_j}(h_{j-1}(z) A_{j-1}(z))$. Hence, $h_{j-1}(z) | h_j(z) \pmod{\gamma^{j-2-i_j}}$. This proves the third part of the theorem.

(iv) Using first part of this theorem for $j = 1$, we have $\gamma^{i_0-i_0} f_1(z) \in <f_0(z)>$. So, $\gamma^{i_0-i_0} f_1(z) = f_0(z) g(z)$ for some $g(z) \in R_n$, i.e., $\gamma^{i_0} (h_1(z) - h_0(z) g(z)) = 0$. Consequently, either $h_1(z) - h_0(z) g(z) = 0$ or the power of $\gamma$ in each of its coefficient is either equal to or greater than $\nu - i_0$. Thus, $\Phi_{\nu-i_0}(h_1(z) - h_0(z) g(z)) = 0$ and it follows that $h_0(z)|h_1(z) \pmod{\gamma^{i_0-i_0}}$.

(v) Since $\gamma^m (z^n - 1) \in <f_0(z), f_1(z), \cdots, f_m(z)>$ there exist $B_k(z) \in R_n$, for $0 \leq k \leq m$ such that $\gamma^m (z^n - 1) = \gamma^m h_0(z) B_0(z) + \gamma^m h_1(z) B_1(z) + \cdots + \gamma^m h_m(z) B_m(z)$. Hence, $\gamma^m (z^n - 1 - \gamma^m h_0(z) B_0(z) - \gamma^m h_1(z) B_1(z) - \cdots - \gamma^m h_m(z) B_m(z)) = 0$, where $B(z) = \gamma^{i_0-i_m} h_0(z) B_0(z) + \gamma^{i_1-i_m} h_1(z) B_1(z) + \cdots + h_m(z) B_m(z) - 1$. It follows that $h_m(z)|(z^n - 1) \pmod{\gamma^{i_m-i_m}}$ by using a similar argument as in part (iii).

Given below is an illustration of theorem 3.4.

**Example 1**: Consider a cyclic code $<4, 2(z + 1), (z + 1)^2>$ of length 4 over the finite chain ring $Z_5$ as reported by A. Garg [9]. Here, $\gamma = 2$ and $\nu = 3$. Clearly, the generators are given in the required form i.e.

$\hat{f}_0(z) = 2^2 \ast 1$, $h_0(z) = 1$, $i_0 = 2$,

$\hat{f}_1(z) = 2^1 \ast (z + 1)$, $h_1(z) = (z + 1)$, $i_1 = 1$,

$\hat{f}_2(z) = 2^0 \ast (z + 1)^2$, $h_2(z) = (z + 1)^2$, $i_2 = 0$. 

5
(i) For $j = 1$, $\gamma^{i_0-i} f_1(z) = 4(z + 1) \in <f_0(z)>$. Next, for $j = 2$, $\gamma^{i_1-i} f_2(z) = 2(z + 1)^2 = 4 * 0 + 2(z + 1) * (z + 1) \in <f_0(z), f_1(z)>$.

(ii) For $j = 0$, $f_0(z) = 2^2$ and $h_0(z) = 1$ which is clearly a monic polynomial in $R^0[z]/<z^4 - 1>$. Next, for $j = 1$, $f_1(z) = 2(z + 1)$ and $h_1(z) = (z + 1)$ which is clearly a monic polynomial in the ring $R^1[z]/<z^4 - 1>$. Further, for $j = 2$, $f_2(z) = (z + 1)^2$ and $h_2(z) = (z + 1)^2$. It can be easily seen that $(z + 1)^2$ is a monic polynomial in the ring $R^2[z]/<z^4 - 1>$.

(iii), (iv) and (v) are obvious.

The following theorem is an immediate consequence of Lemma 2.3 and Theorem 3.4.

**Theorem 3.5**: Let $C$ be a cyclic code over $FR(\gamma, \nu)$ where $f_j(z)$, for $0 \leq j \leq m$ are polynomials as described before. Then $\{f_0(z), f_1(z), \cdots, f_m(z)\}$ is a MSGB for $C$.

4. Conclusion

In this paper, we have established a set of generators for cyclic codes of arbitrary length over $FR(\gamma, \nu)$ and it is observed that this set behaves as a MSGB for the code.

**References**

[1] Kaur J, Dutt S and Sehmi R 2018 On cyclic codes over Galois rings Discrete Applied Mathematics 280 156-161

[2] Liu X 2013 On the Characterization of cyclic codes over two classes of rings Acta Mathematica Scientia 33B(2) 413-22

[3] Norton and Salagean 2000 On the structure of linear and cyclic codes over finite chain rings Applicable algebra in engineering, communication and computing 10 489-506

[4] Norton G H and Salagean 2001 A cyclic codes and minimal strong Gröbner bases over a principal ideal ring Finite Fields And Their Applications 9 237-49

[5] Norton and Salagean 2001 Strong Gröbner bases for polynomials over a principal ideal ring Bull. Austral. Math. Soc. 64 505-28

[6] Salagean 2005 Repeated root cyclic and negacyclic codes over a finite chain ring Discrete Applied Mathematics 413-419

[7] Abualrub T, Ghrayeb A and Oehmke R 2004 A Mass Formula and Rank of $Z_4$ cyclic codes of length $2^n$ IEEE Transactions of Information Theory 50 3306-12

[8] Abualrub T and Oehmke R 2003 Cyclic codes of length $2^n$ over $Z_4$ Discrete Applied Mathematics 128 3-9

[9] Garg A and Dutt S cyclic codes finite rings 2017 PhD Thesis PEC University of Technology Chandigarh

[10] Sharma A and Sidana T 2017 Repeated root constacyclic codes over finite commutative chain rings and their distances Preprint 1706.06269v2[math.AC]