DECODING OF CYCLIC CODES OVER THE RING $\frac{F_p[u]}{\langle u^k \rangle}$

Mohammad Reza Alimoradi[1]

AbuAlrub et al in (Des Codes Crypt 42:273-287, 2007) proposed an open problem in decoding of cyclic codes over the rings $F_2 + uF_2$ with $u^2 = 0$. In this paper we resolve this open problem and extend this decoding procedure for cyclic codes of arbitrary length over the ring $\frac{F_p[u]}{\langle u^k \rangle}$, where p is a prime number and $u^k = 0$. Note that the ring $\frac{F_p[u]}{\langle u^k \rangle} = F_p + uF_p + \cdots + u^{k-1}F_p$ may be of interest in coding theory, which have already been used in the construction of optimal frequency-hopping sequence.

Keywords: Cyclic codes, Hamming distance, Decoding, Torsion codes, frequency-hopping sequence.
MSC2000: 94B15, 94B35.

1. Introduction

A landmark paper [5] has shown that certain non-linear binary codes with excellent error-correcting capabilities and some optimal codes can be identified as images of linear codes over Z_4 under the Gray map. This has motivated the study of codes over finite rings. We will say that a code is optimal for a given source if its average length is at least as small as that of any other uniquely-decodable code. Since some binary codes with good parameters and some optimal codes are Gray images of cyclic codes over finite rings, apart from Z_4 ([13]), the study of cyclic codes over finite rings is significant. So far, a few papers have been published about the decoding of codes over finite rings (see [2], [8] and [13]). Codes over $F_2 + uF_2$ have been discussed by a number of authors (see [1], [13]). Note that cyclic codes over this ring have applied in DNA computing [9]. In this paper we present a method for decoding cyclic codes over the ring $\frac{F_p[u]}{\langle u^k \rangle} = F_p + uF_p + \cdots + u^{k-1}F_p$ by using the torsion codes, which are codes over the residue field associated to a chain ring. Note that some sequences over this ring having optimal Hamming correlation properties. These sequences are useful in frequency-hopping multiple-access spread-spectrum communication systems [14]. So the ring $= F_p + uF_p + \cdots + u^{k-1}F_p$ is significant in information theory and coding theory. A linear code C of length n over ring R is an R-submodule of R^n. A code is called cyclic if it is linear and invariant with respect to cyclic shift. Note that each $(c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in R^n$ is identified

[1]Assistant Professor, Department of Mathematics, Faculty of Mathematical Sciences, University of Malayer, Malayer, Iran, E-mail: malimoradisharif@yahoo.com

with the polynomial $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \frac{R[x]}{\langle x^n-1\rangle}$. So we can consider a cyclic code C of length n as an ideal in $R_n = \frac{R[x]}{\langle x^n-1\rangle}$. In this paper we denote $\frac{F_p[u]}{\langle u^k\rangle}$ by $R_{k,p}$ and $\frac{R_{k,p}[x]}{\langle x^n-1\rangle}$ by $R_{k,p,n}$. A ring R is called a von Neumann regular ring if for each a in R, there exists b in R such that $a = a^2b$ and is called reduced ring if its nilradical be zero. Clearly von Neumann regular rings are reduced. Let R be a ring. By a chain of prime ideals, we mean a nested sequence $p_0 \subsetneq p_1 \subsetneq \ldots \subsetneq p_n$ of distinct primes. The primes p_i are called the members of the chain, and n is called its length. The Krull dimension of R is defined to be the largest length of any chain of prim ideals. Clearly an Artinian ring is of dimension zero [7]. It is clear that a finite ring is an Artinian ring, thus its dimension is zero.

2. Application of $\frac{F_p[u]}{\langle u^k\rangle}$ in the construction of optimal frequency-hopping sequence

In modern radar and communication systems, frequency-hopping spread-spectrum techniques have become very popular. The hopping sequences are used to specify which frequency will be used for transmission at any given time. Fuji-Hara et al. investigated frequency-hopping multiple-access systems with a single optimal frequency-hopping sequence from a combinatorial approach [4]. Let $F = \{f_0, f_1, \ldots, f_{m-1}\}$ be a set of available frequencies with alphabet size m and $\chi(v, F)$ be the set of all sequences of length v over F. Any element of $\chi(v, F)$ is called a frequency hopping sequence of length v over F. In multiple-access spread spectrum communication systems, mutual interference occurs when two or more transmitters transmit on the same frequency at the same time. Frequency hopping sequences are required to have good Hamming correlations, and large linear span, where the linear span is defined to be the length of the shortest linear feedback shift register that can produce the sequence. In [14] Udaya et.al constructed a sequences over finite rings with optimal Hamming correlation properties. They constructed new sequences over the residue class ring $R = \frac{F_p[u]}{\langle w(u)^k\rangle}$, where $w(u)$ is an irreducible polynomial over F_p. Note that the ring $\frac{F_p[u]}{\langle u^k\rangle}$ is a particular case of polynomial residue class rings introduced in [14], when $w(u) = u$. It is generally desired that the family S of frequency hopping sequences has the following properties:
(i) The Hamming correlation $H_{XX}(w), w \neq 0$ for all frequency-hopping sequences X should be as small as possible.
(ii) The Hamming correlation between any sequence in a set with all phase shifts of other sequences in the set should be as small as possible.
(iii) The sequences should be of large period and linear complexity.

Definition 2.1. *For two sequences,* $X = (x_0, x_1, \ldots, x_{v-1})$ *and* $Y = (y_0, y_1, \ldots, y_{v-1}) \in \chi(v, F)$*, the Hamming correlation* $H_{XY}(w)$ *is defined by*

$$H_{XY}(w) = \sum_{t=0}^{v-1} h[x_i, y_{i+w}]$$

where $0 \leq w < v$ *if* $X = Y$ *and* $0 < w < v$ *if* $X = Y$ *and also* $h[x, y] = 1$ *if* $x = y$ *and* 0 *otherwise. Also all operations among position indices are performed modulo* v*. For any single frequency hopping sequence* $X \in \chi(v, F)$*, let* $H(X) = \max\limits_{0<t<v-1}\{H_{XX}(t)\}$*, be the maximum out-of-phase value of* $H_{XX}(t)$*. If* $H(X^*) \leq H(X)$ *for all* $X \in \chi(v, F)$*, then the sequence* X^* *is called an optimal frequency-hopping sequence.*

Definition 2.2. *A m-sequences (maximal length sequences) over the field* F_p *of length* $N = p^r - 1$ *is generated by a degree* r *primitive polynomial over* F_p*. Let* $s_0 s_1 s_2 \ldots$ *be a m sequences over* F_p *and* $f(x) = x^r - a_{r-1}x^{r-1} - \cdots - a_1 x - a_0$ *be the primitive polynomial over* F_p*, then the m-sequence* $s_0 s_1 s_2 \ldots$ *satisfies the recursion relationship*

$$s_{n+r} = a_{r-1}s_{n+r-1} + a_{r-2}s_{n+r-2} + \cdots + a_0 s_n, n = 0, 1, 2, \ldots$$

Associated with every m-sequence S^v can be constructed a family of sequences , which can be used to construct frequency hopping patterns. The number of sequences in a family depends on the number of distinct elements of R occurring in S^v. Families are optimal in the sense that they meet Lempel and Greenberger bound.

Lemma 2.1. ([11], *Lemma* 4, *Lempel and Greenberger bound*) *For every sequence* $S = \{s_i\}$ *of length* $p^l - 1$ *over a set of size* p^t*, we have* $H(S) \geq p^{l-t} - 1$.

Definition 2.3. *Let* R *be a local ring with maximal ideal* m *and residue field* $F = \frac{R}{m}$*, the Galois ring of* R *denoted as* $GR(R, r)$ *is defined as* $\frac{R[x]}{\langle f(x) \rangle}$*, where* $f(x)$ *is a basic monic irreducible polynomial of degree* r *over* R*. If* α *is a root of irreducible polynomial* $f(x)$ *in* $GR(R, r)$*, then each* $\beta \in GR(R, r)$ *can be uniquely written as*

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{r-1}\alpha^{r-1},\ a_0, a_1, \ldots, a_{r-1} \in R$$

Definition 2.4. *Let* R *be a local ring with residue field* F_{p^s} *(finite field with* p^s *element) and* $f(x)$ *be a basic monic irreducible polynomial of degree* r *over* R*, then trace functions which map elements of* $GR(R, r)$ *to* R *is defined as* $Tr_1{}^r(\beta) = a_0 \sum_{i=0}^{r-1} \alpha^{p^{si}} + a_1 \sum_{i=0}^{r-1} \alpha^{2p^{si}} + \cdots + a_{r-1} \sum_{i=0}^{r-1} \alpha^{(r-1)p^{si}}$*, where* $\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{r-1}\alpha^{r-1},\ a_0, a_1, \ldots, a_{r-1} \in R$.

Theorem 2.1. ([14], *Theorem* 1) *Every m-sequence over* R *has a unique trace representation given by* $S_i{}^v = Tr_1{}^r(v\alpha^i)$*, where* $v \in GR(R, r)$ *and* α *is a primitive root of* $f(x)$ *of degree* r.

Note that $R_{k,p}$ is a local ring with maximal ideal $\langle u \rangle$ and residue field F_p. Now, select a primitive basic monic irreducible polynomial $f(x)$ of degree r over $R_{k,p}$ (Since F_p is a subring of $R_{k,p}$, any irreducible polynomial over F_p is obviously irreducible over $R_{k,p}$). Then $\frac{R_{k,p}[x]}{\langle f(x) \rangle}$ is a Galois ring with residue field F_{p^r}. As $f(x)$ is a irreducible polynomial of degree r over F_p, then $f(x) \mid x^{p^r-1} - 1$. Now, if $\alpha \in GR(R_{k,p}, r)$ is a primitive element of F_{P^r}, then $\alpha^{p^r-1} = 1$. Therefore from the trace description in Theorem 2.1, it follows that all m-sequences over the ring $R_{k,p}$ are periodic with period $L = p^r - 1$ (Note that $S^v_{i+p^r-1} = Tr_1{}^r(v\alpha^{i+p^r-1}) = Tr_1{}^r(v\alpha^i) = S_i{}^v$).

Example 2.1. *In the following we give a m-sequences over the ring $R_{3,2}$. Let $f(x) = x^3 + x + 1$ and $\alpha \in GR(R_{3,2}, r)$ be a primitive element of F_{2^3}. So $\alpha^3 = \alpha + 1$ and the following Table implies that α is a primitive element of F_{2^3}.*

i	α^i
0	1
1	α
2	α^2
3	$\alpha + 1$
4	$\alpha^2 + \alpha$
5	$\alpha^2 + \alpha + 1$
6	$\alpha^2 + 1$
7	1

Now, let $v = u^2 + u\alpha + \alpha^2 \in GR(R_{3,2})$, then $s_0 = {S_0}^v = {Tr_1}^r(v) = u^2{Tr_1}^r(1) + u{Tr_1}^r(\alpha) + {Tr_1}^r(\alpha^2)$. Since ${Tr_1}^r(1) = 1$, and ${Tr_1}^r(\alpha) = {Tr_1}^r(\alpha^2) = 0$, then $s_0 = u^2$. Similarly, we obtain $s_1 = 1, s_2 = u, s_3 = u^2 + 1, s_4 = u + 1, s_5 = u^2 + u + 1$ and $s_6 = u^2 + u$. So, the m-sequences S^v is equal to the set $\{u^2, 1, u, u^2 + 1, u + 1, u^2 + u + 1, u^2 + u\}$.

Definition 2.5. *Let $\beta = b_0 + b_1u + \cdots + b_{k-1}u^{k-1} \in GR(R_{k,p}, r)$, where $b_0, b_1, \ldots, b_{k-1} \in F_{p^r}$. Now, let M_β be a matrix over F_p of dimension $r \times k$ formed by placing together k elements $b_0, b_1, \ldots, b_{k-1}$ as columns of M_β. So, the rank number of $\kappa(\beta)$ is defined as the rank of matrix M_β over F_p. Also the Trace Image of an m-sequence, S^v is defined as the set of distinct elements in S^v.*
Suppose $v \in GR(R_{k,p}, r)$ with $\kappa(v) = \rho$, then from definition we have the cardinality of Trace Image of S^v is p^ρ. Now for any m-sequence, $S^v = \{s_i\}$ and for every γ belonging to Trace Image of S^v a sequence $S^v(\gamma)$ is defined as $\{s_i + \gamma : i \in Z_{p^r-1}\}$. Since the cardinality of Trace Image of S^v is p^ρ, there exists p^ρ such sequence. So a family of p^ρ sequences associated with S^v is given by the set of sequences $\{S^v(\gamma), \gamma \in$ Trace Image of $S^v\}$ is denoted by $M(v)$. So corresponding to each m-sequence S^v, a family of hopping patterns derived from $M(v)$.

Theorem 2.2. ([14], *Theorem* 3) *Let S^v be a m-sequence over the ring $R_{k,p}$ with $\kappa(v) = \rho$. Then Hamming correlation between any two sequences $S^v(\gamma_1)$ and $S^v(\gamma_2)$ belonging to the family, $M(v)$ is given by*

$$H_{\gamma_1\gamma_2}(0) = \begin{cases} p^r - 1 & \gamma_1 = \gamma_2 \\ 0 & \gamma_1 \neq \gamma_2 \end{cases}$$

and for $w \neq 0$, we have

$$H_{\gamma_1\gamma_2}(w) = \begin{cases} p^{r-\rho} - 1 & \gamma_1 = \gamma_2 \\ p^{r-\rho} & \gamma_1 \neq \gamma_2 \end{cases}$$

In the following we give an example of application the ring $R_{3,2}$ in the construction of optimal frequency-hopping sequence

Example 2.2. *A family of frequency hopping patterns of length* 7 *derived from m-sequences over* $R_{3,2}$. *Such sequences are generated by* $\alpha \in GR(R_{3,2}, 3)$ *such that* $\alpha^3 = \alpha+1$. *Let* $v = u^2+\alpha+(u^2+u+1)\alpha^2 \in GR(R_{3,2}, 3)$. *Than* $M_v = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. *So* $\kappa(v) = 3$. *Also* $S^v = \{u^2+u+1, 1, u+1, u^2+u, u, u^2+1, u^2\}$. *In the following table we give patterns of the family* $M(v)$. *Note that pattern symbols are represented by decimal numbers in the range* $(0-7)$ *and* $h(u) \in R_{3,2}$ *is represented by* $h(2)$.

γ	$S^v(\gamma)$
0	(7 1 3 6 2 5 4)
1	(6 0 2 7 3 4 5)
u	(5 3 1 4 0 7 6)
$u+1$	(4 2 0 5 1 6 7)
u^2	(3 5 7 2 6 1 0)
u^2+1	(2 4 6 3 7 0 1)
u^2+u	(1 7 5 0 4 3 2)
u^2+u+1	(0 6 4 1 5 2 3)

Note that in above table $H_{\gamma_1\gamma_2}(w) = 2^{r-\rho} = 1$. *For example if* $\gamma_1 = u$, $\gamma_2 = u+1$, *then* $H_{\gamma_1\gamma_2}(3) = \sum_{i=0}^{6} h[a_i, b_{i+3}] = h[5,5] = 1$. *Now we show that the m-sequences* S^v *is an optimal frequency-hopping sequence. From Theorem* 2.2, *we have* $H(S^v) = 0$. *As* S^v *is a m-sequences of length* $N = 2^3-1$ *over* $R_{3,2}$ *with size* 2^3. *So from Lempel and Greenberger bound, we obtain* $H(S^v) = 2^{3-3}-1$. *So the m-sequences* S^v *meet Lempel and Greenberger bound and therefore is an optimal frequency-hopping sequence.*

3. Decoding of cyclic codes over $F_p + uF_p$

Udaya et al. in [13] introduced a decoding procedure for cyclic codes over the ring F_2+uF_2 by using of a Gray map and $\langle u, u+v\rangle$ construction codes. They showed that a cyclic code C of length n over this ring has structure $C = \langle fh, ufg\rangle$, where $fgh = x^n - 1$ and Gray image C is equivalent to a $\langle u, u+v\rangle$ constructed code with binary codes $C_1 = Res(C) = \langle fh\rangle$ and $C_2 = Tor_1(C) = \langle f\rangle$, where the residue code C_1 is defined as $C_1 = \{x \in {F_2}^n \,|\, \exists\, y \in {F_2}^n,\, x + uy \in C\}$ and the torsion code C_2 is defined as $C_2 = \{x \in {F_2}^n \,|\, ux \in C\}$. Also the decoding procedure is done in Galois extension of $F_2 + uF_2$. In this section we present a decoding procedure for cyclic codes over the ring $F_p + uF_p$. Since the ring $F_p + uF_p$ is a chain ring with unique maximal ideal $m = \langle u\rangle$ and the residue field F_p, we can use the torsion codes associated to a code over the chain ring. i.e, let C_2 be a linear code of length n over the ring $R_{2,p}$, then we associate to the code C_2 two codes $C^{2,u}$ and $Tor_1(C_2)$, which are defined as:

$$Tor_1(C_2) = \{k(x) \in \frac{F_p[x]}{\langle x^n - 1\rangle} \,|\, uk(x) \in C_2\}$$

and $C^{2,u} = \{b(x) \in \frac{F_p[x]}{\langle x^n-1\rangle} \mid \exists\, a(x),\, a(x)+ub(x) \in C_2\}$. Clear that $C^{2,u}$ and $Tor_1(C_2)$ are linear codes over the residue field F_p.

For proving Theorem 3.3 we use the two following theorem.

Theorem 3.1. ([12], *Theorem* 3.3) *Let C_k be a cyclic code of length n over $R_{k,p}$, then C_k is an ideal in $R_{k,p,n}$ that can be generated by $C_k = \langle g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x), ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x), u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x)+u^{k-1}t_1(x), u^{k-1}a_{k-1}(x)\rangle$ with $a_{k-1}(x) \mid a_{k-2}(x) \mid \ldots \mid a_1(x) \mid g(x) \mid (x^n-1) \bmod p$, and $a_{k-2}(x) \mid p_1(x)(\frac{x^n-1}{g(x)}), \ldots, a_{k-1}(x) \mid t_1(x)(\frac{x^n-1}{a_{k-2}(x)}), \ldots, a_{k-1}(x) \mid p_{k-1}(x)(\frac{x^n-1}{g(x)}) \ldots (\frac{x^n-1}{a_{k-2}(x)})$. Moreover $\deg p_{k-1} < \deg a_{k-1}, \ldots, \deg t_1 < \deg a_{k-1}$, and $\deg p_1 < \deg a_{k-2}$.*

Theorem 3.2. [7] *For a reduced ring R, the following conditions are equivalent:*
(1) *R is a von Neumann regular ring.*
(2) *The ring R is of dimension zero.*
(3) *Each finitely generated ideal of R is principal and is generated by an idempotent.*

Theorem 3.3. *Let C_k be a cyclic code of length n over the ring $R_{k,p}$ and n is relatively prime to p. Then $C_k = \langle g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle$.*

Proof. We know that if R is a finite chain ring and n is relatively prime to the characteristic of R, then $\frac{R[x]}{x^n-1}$ is a principal ideal ring (see [3], Theorem 3.6). So it is enough to show that $C_k = \langle g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x)\rangle$. Since n is relatively prime to p, the polynomial $x^n - 1$ can be uniquely written as the product of distinct irreducible factors and hence

$$GCD(a_{k-2}(x), \frac{x^n-1}{g(x)}) = 1. \tag{1}$$

From Theorem 3.1, we know that $a_{k-2}(x) \mid p_1(x)(\frac{x^n-1}{g(x)})$, which means $a_{k-2}(x) \mid p_1(x)$ by (1). But $\deg p_1(x) < \deg a_{k-2}(x)$ implis that $p_1(x) = 0$. Similarly we can prove that $p_2(x) = \cdots = p_{k-1}(x) = q_1(x) = \cdots = q_{k-2}(x) = t_1(x) = 0$. So

$$C_k = \langle g(x), ua_1(x), u^2a_2(x), \ldots, u^{k-1}a_{k-1}(x)\rangle.$$

Now let $h(x) = g(x)+ua_1(x)+\cdots+u^{k-1}a_{k-1}(x)$. Since n is relatively prime to p, the ring $R_{k,p,n}$ is a reduced and its dimension is zero. So $\langle g(x)\rangle = \langle e(x)\rangle$ for some idempotent $e(x)$ in $R_{k,p,n}$ by Theorem 3.2. Now, there exists a polynomial $r(x) \in R_{k,p,n}$ such that $e(x) = r(x)g(x)$. Let $m = LCM(k,p)$. Then $e(x) = r^m(x)g^m(x)$. Since $h^m(x) = g^m(x)$, we have $e(x) \in \langle h(x)\rangle$. This implies that $g(x) \in \langle h(x)\rangle$. Similarly we can show that $a_1(x), a_2(x), \ldots, a_{k-1}(x) \in \langle h(x)\rangle$ and so $\langle g(x), ua_1(x), u^2a_2(x), \ldots, u^{k-1}a_{k-1}(x)\rangle = \langle h(x)\rangle$. □

Lemma 3.1. *If $C_2 = \langle g(x)+up(x), ua(x)\rangle$ is a cyclic code of length n over the ring $R_{2,p}$, then $Tor_1(C_2) = \langle a(x)\rangle$ and $d_H(C_2) = d_H(Tor_1(C_2))$.*

Proof. Let $k(x) \in Tor_1(C_2)$. Then $uk(x) \in C_2$. So, there exist polynomials $r_0(x) + ur_1(x), s_0(x) + us_1(x) \in R_{2,p,n}$, such that

$$uk(x) = (r_0(x) + ur_1(x))(g(x) + up(x)) + (s_0(x) + us_1(x))ua(x).$$

Thus $uk(x) = ur_1(x)g(x) + us_0(x)a(x)$. But we know that $a(x) \mid g(x)$, so, we obtain $k(x) \in \langle a(x)\rangle$. Conversely if $ua(x) \in C_2$, then $a(x) \in Tor_1(C_2)$. Now, Theorem 4.2 in [10] implies that $d_H(C_2) = d_H(Tor_1(C_2))$. □

Lemma 3.2. *Let C_2 be a cyclic code of length n over the ring $R_{2,p}$, where n is relatively prime to p. Then $C^{2,u} = Tor_1(C_2)$.*

Proof. If $c_2(x) \in C^{2,u}$, then there exists $c_1(x) \in \frac{F_p[x]}{\langle x^n-1\rangle}$ such that $c_1(x) + uc_2(x) \in C_2$. As by Theorem 3.3, we have $C_2 = \langle g(x) + ua(x)\rangle$. So

$$c_1(x) + uc_2(x) = (h_1(x) + uh_2(x))(g(x) + ua(x)).$$

Since $a(x) \mid g(x)$, we must have $c_2(x) \in \langle a(x)\rangle$. So $C^{2,u} \subseteq Tor_1(C_2)$. Conversely, if $c(x) \in Tor_1(C_2)$, then $uc(x) \in C_2$, which means that $c(x) \in C^{2,u}$. So $C^{2,u} = Tor_1(C_2)$. □

The main purpose of this section is to prove the following theorem.

Theorem 3.4. *Let C_2 be a cyclic code of length n over the ring $R_{2,p}$, $w(x) = w_1(x) + uw_2(x)$ be a received word with an error polynomial $e(x) = e_1(x) + ue_2(x)$ and $w_H(e_i(x)) \leq \lfloor \frac{(d_H(Tor_1(C_2))-1)}{2} \rfloor$, for $i = 1, 2$. Then $w_1(x)$ and $w_2(x)$ can be decoded in the code $Tor_1(C_2)$.*

Proof. We have two cases
Case(i): Suppose n is relatively prime to p. Now, let $w(x) = c(x) + e(x)$, where $c(x) = c_1(x) + uc_2(x)$ is a codeword in C_2. Since $uc(x) = uc_1(x) \in C_2$ and $uc_1(x) = u(w_1(x) - e_1(x))$, we see that $w_1(x) - e_1(x) \in Tor_1(C_2)$. Now, we know $Tor_1(C_2)$ is a cyclic code over the finite field F_p. So, we can determine $e_1(x)$ by using the decoding algorithms for cyclic codes over the field F_p. Since $c_2(x) \in C^{2,u}$, also $C^{2,u} = Tor_1(C_2)$ by Lemma 3.2 and $d_H(w_2, c_2) \leq \lfloor \frac{(d_H(Tor_1(C_2))-1)}{2} \rfloor$, we see that w_2 will be uniquely decoded to c_2.
Case(ii): Suppose n is not relatively prime to p. Let $c_1(x) + uc_2(x)$ be a codeword in C_2. Then by Theorem 3.1, we have

$$c_1(x) + uc_2(x) = (r_1(x) + ur_2(x))(g(x) + up(x)) + s(x)ua(x).$$

Similar to case (i) we can determine $e_1(x)$, then the word $w_1(x)$ will be uniquely decoded to $c_1(x)$. Let $w_2'(x) = w_2(x) - r_1(x)p(x)$. Now, we know that $a(x) \mid g(x)$, so $w_2'(x) - e_2(x) \in \langle a(x)\rangle = Tor_1(C_2)$. Then we can determine $e_2(x)$ with using of the decoding algorithm for cyclic codes over the field F_p. □

Decoding Procedure:
1) Calculation of $d_H(Tor_1(C_2))$.
2) Let $d_H(C_2) = d_H(Tor_1(C_2))$.
3) Decode $w_1(x)$ to $c_1(x)$ in $Tor_1(C_2)$, where $w_1(x) + uw_2(x)$ is a received word.

4) if $GCD(n,p)=1$, then $w_2(x)$ decode to $c_2(x)$ in $Tor_1(C_2)$, else go to 5.
5) Let $w_2'(x) = w_2(x) - r_1(x)p(x)$.
6) Decode $w_2'(x)$ to $c_2'(x)$ in $Tor_1(C_2)$.
7) Let $c_2(x) = c_2'(x) + r_1(x)p(x)$.

We give an example in order to illustrate our results.

Example 3.1. *Let $C_2 = \langle (x+2)a(x), ua(x)\rangle$ be a cyclic code of length 8 over the ring $R_{2,3}$, where $a(x) = x^5+2x^4+x^3+x^2+2$. We know that the polynomial x^8-1 is uniquely decomposed to $(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$ over $R_{2,3}$. Then $d_H(C_2) = d_H(Tor_1(C_2)) = w_H(\langle a(x)\rangle)$. Let $\alpha \in GF(3^2) = \frac{F_3(x)}{\langle x^2+x+2\rangle}$ be a root of the primitive polynomial $x^2+x+2 \in F_3[x]$. Clearly $x^2+x+2 = (x-\alpha)(x-\alpha^3)$ over the Galois field $GF(3^2)$. Also $x+1$ and x^2+1 are minimal polynomials of α^4 and α^2, respectively. This implies that $a(x)$ has roots $\{\alpha, \alpha^2, \alpha^3, \alpha^4\}$ in the Galois field $GF(3^2)$. So $Tor_1(C_2)$ is a ternary 2-error-correcting cyclic code. Let*

$$w(x) = x^7+2x^6+x^3+x^2+1+u(2x^6+2x^5+x^3+2x^2+2)$$

be a received word with an error pattern $e(x)$. We can decode $w_1(x)$ in the ternary code $Tor_1(C_2)$ by using of the Peterson-Gorenstein-Zierler algorithm ([6] *Section* 5.4.1). *Suppose that $e_1(x) = E_1x^{t_1} + E_2x^{t_2}$, where $E_1, E_2 \in F_3$. Since*

$$S_1 = w_1(\alpha) = \alpha, S_2 = \alpha^3, S_3 = \alpha^3, S_4 = \alpha^4$$

and $M_2 = \begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} = \begin{pmatrix} \alpha & \alpha^3 \\ \alpha^3 & \alpha^3 \end{pmatrix}$ is a non-singular matrix with inverse ${M_2}^{-1} = \begin{pmatrix} \alpha^6 & \alpha^4 \\ \alpha^2 & \alpha^4 \end{pmatrix}$, we conclude that exactly two errors have been made. So,

$$\begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} \alpha^6 & \alpha^4 \\ \alpha^2 & \alpha^4 \end{pmatrix} \begin{pmatrix} \alpha^7 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha^7 \\ \alpha^6 \end{pmatrix}.$$

Thus the error locator polynomial is $\sigma(x) = 1+\alpha^6x+\alpha^7x^2$. It is easy to see that the error locator polynomial has roots α^4 and α^5. So, the error location numbers are $X_1 = \alpha^4$ and $X_2 = \alpha^3$. As the code is ternary, we must determine the error magnitudes E_1 and E_2. Since $S_1 = E_1\alpha^4 + E_2\alpha^3$ and $S_2 = E_1 + E_2\alpha^6$, we must solve the matrix equation

$$\begin{pmatrix} \alpha^4 & \alpha^3 \\ 1 & \alpha^6 \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha^3 \end{pmatrix}.$$

Solution of this matrix equation implies that $E_1 = 1$ and $E_2 = 2$. Therefore $e_1(x) = x^4+2x^3$.
Similarly we must decode $w_2(x) = 2x^6+2x^5+x^3+2x^2+2$ in the ternary code $Tor_1(C_2)$. Decoding of $w_2(x)$ implies that $e_2(x) = 2x^7+2x^2$. If we correct these errors in the received polynomial, then the vector $w(x)$ will be decoded to the code polynomial $c(x) = x^7+2x^6+2x^4+2x^3+x^2+1+u(x^7+2x^6+2x^5+x^3+2)$.□

4. Decoding of cyclic codes over the ring $\frac{F_p[u]}{\langle u^k\rangle}$

In this section, we extend the previous decoding procedure for cyclic codes over the ring $\frac{F_p[u]}{\langle u^k\rangle} = F_p + uF_p + u^2F_p + \cdots + u^{k-1}F_p$, where $u^k = 0$.

Lemma 4.1. *Let $C_3 = \langle g(x) + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x)\rangle$ be a cyclic code of length n over the ring $R_{3,p}$, then $Tor_2(C_3) = \langle a_2(x)\rangle$ and $d_H(C_3) = d_H(Tor_2(C_3))$, where $Tor_2(C_3) = \{k(x) \in \frac{F_p[x]}{\langle x^n-1\rangle} \mid u^2k(x) \in C_3\}$.*

Proof. Theorem 4.2 in [10], implies that $d_H(C_3) = d_H(Tor_2(C_3))$. Since $u^2a_2(x) \in C_3$, we have $a_2(x) \in Tor_2(C)$. So, $\langle a_2(x)\rangle \subseteq Tor_2(C_3)$. Conversely let $k(x) \in Tor_2(C_3)$, then $u^2k(x) \in C_3$. So by the structure of the code C_3, there exist polynomials $r_2(x), s_1(x), t_o(x) \in \frac{F_p[x]}{\langle x^n-1\rangle}$ such that $k(x) = r_2(x)g(x)+s_1(x)a_1(x)+t_0(x)a_2(x)$. But, we know that $a_2(x) \mid a_1(x) \mid g(x)$. Then $k(x) \in \langle a_2(x)\rangle$. □

Definition 4.1. *Let n be a positive integer relatively prime to p and s be an integer with $0 \le s < n$. If $GF(p^t)$ is an extension field of F_p and α be a primitive element of $GF(p^t)$ with minimal polynomial $M_\alpha(x)$ in $F_p(x)$, then the p-cyclotomic coset of s modulo n is defined the set $C_s = \{sp^i(mod\, n) : i = 0, 1, 2, \ldots\}$. A subset $\{i_1, i_2, \ldots, i_t\}$ of Z_n is called a set of representatives of the p-cyclotomic cosets of s modulo n if $C_{i_1}, C_{i_2}, \ldots, C_{i_t}$ are distinct and $\cup_{j=1}^{t} C_{i_j} = Z_n$.*

Theorem 4.1. ([6], *Theorem* 4.1.1) *Let n be a positive integer relatively prime to p, $t = ord_n(p)$ and α be a primitive n-th root of unity in Galois field $GF(p^t)$. So*
(i) For each integer s with $0 \le s < n$, the minimal polynomial of α^s over F_p is $M_{\alpha^s}(x) = \Pi_{i\in C_s}(x - \alpha^i)$.
(ii) $x^n - 1 = \Pi_s M_{\alpha^s}(x)$ is the factorization of $x^n - 1$ into irreducible factors over F_p, where s runs through a set of representatives of the p-cyclotomic cosets modulo n.

Definition 4.2. *Let C_3 be a cyclic code of length n over the ring $R_{3,p}$, then we associate to the code C_3 two codes*

$$C^{3,u^2} = \{c_2(x) \in \frac{F_p[x]}{\langle x^n - 1\rangle} \mid \exists\, c_0, c_1\ , c_0 + uc_1 + u^2c_2\ \in C_3\}$$

and

$$C^{3,u} = \{c_1 \in \frac{F_p[x]}{\langle x^n - 1\rangle} \mid \exists\, c_0, c_2\ ,\ c_0 + uc_1 + u^2c_2 \in C_3\}.$$

Lemma 4.2. *Let C_3 be a cyclic code of length n over the ring $R_{3,p}$, where n is a positive integer relatively prime to p. Then $C^{3,u} = Tor_1(C_3)$.*

Proof. At first, we show that $Tor_1(C_3) = \langle a_1(x)\rangle$, where $C_3 = \langle g(x) + ua_1(x) + u^2a_2(x)\rangle$. Clearly

$$Tor_1(C_3) = \{k(x) \in \frac{F_p[x]}{\langle x^n - 1\rangle} \mid \exists\, t(x),\ uk(x) + u^2t(x) \in C_3\}.$$

Since $ua_1(x) \in C_3$, we must have $a_1(x) \in Tor_1(C_3)$. Conversely if $k(x) \in Tor_1(C_3)$, then $uk(x) + u^2t(x) \in C_3$, for some $t(x) \in \frac{F_p[x]}{\langle x^n-1\rangle}$. So,

$$uk(x) + u^2t(x) = (h_0(x) + uh_1(x) + u^2h_2(x))(g(x) + ua_1(x) + u^2a_2(x)).$$

Now, we know that $a_1(x) \mid g(x)$, then $k(x) \in \langle a_1(x)\rangle$.
Since $ua_1(x) \in C_3$, we have $a_1(x) \in C^{3,u}$. So $Tor_1(C_3) \subseteq C^{3,u}$. Let $c_1(x) \in C^{3,u}$, then there exist polynomials $c_0(x), c_2(x) \in \frac{F_p[x]}{\langle x^n-1\rangle}$ such that $c_0(x) + uc_1(x) + u^2c_2(x) \in C_3$. Now, by the structure of the code C_3, we have

$$c_0(x) + uc_1(x) + u^2c_2(x) = (h_0(x) + uh_1(x) + u^2h_2(x))(g(x) + ua_1(x) + u^2a_2(x))$$

Since $a_1(x) \mid g(x)$, we must have $c_1(x) \in \langle a_1(x)\rangle = Tor_1(C_3)$. □

Lemma 4.3. *Let C_3 be a cyclic code of length n over the ring $R_{3,p}$, where n is relatively prime to p, then $C^{3,u^2} = Tor_2(C_3)$.*

Proof. Let $c_2(x) \in C^{3,u^2}$, then $c_0(x) + uc_1(x) + u^2c_2(x) \in C_3$, for some polynomials $c_0(x), c_1(x) \in \frac{F_p[x]}{\langle x^n-1\rangle}$. So,

$$c_0(x) + uc_1(x) + u^2c_2(x) = (h_0(x) + uh_1(x) + u^2h_2(x))(g(x) + ua_1(x) + u^2a_2(x)).$$

But, we know that $a_2(x) \mid a_1(x) \mid g(x)$, thus $c_2(x) \in \langle a_2(x)\rangle$. So $C^{3,u^2} \subseteq Tor_2(C_3)$. Conversely if $c(x) \in Tor_2(C_3)$, then $u^2c(x) \in C_3$. This implies that $c(x) \in C^{3,u^2}$. So, $C^{3,u^2} = Tor_2(C_3)$. □

Theorem 4.2. *Let C_3 be a cyclic code of length n over the ring $R_{3,p}$. If $w(x) = w_0(x) + uw_1(x) + u^2w_2(x)$ be a received word with an error pattern $e(x) = e_0(x) + ue_1(x) + u^2e_2(x), w_H(e_i(x)) \leq \lfloor \frac{(d_H(Tor_2(C_3))-1)}{2} \rfloor$, for $i = 0, 2$ and $w_H(e_1(x)) \leq \lfloor \frac{(d_H(Tor_1(C_3))-1)}{2} \rfloor$, then $w_0(x), w_2(x)$ can be decoded in the code $Tor_2(C_3)$ and $w_1(x)$ can be decoded in the code $Tor_1(C_3)$.*

Proof. Case(i): Suppose n is relatively prime to p. Let $w(x) = c(x) + e(x)$, where $c(x) = c_0(x) + uc_1(x) + u^2c_2(x)$ is a codeword in C_3. As $u^2c(x) = u^2c_0(x) \in C_3$ and $u^2c_0(x) = u^2(w_0(x) - e_0(x))$, then $w_0(x) - e_0(x) \in Tor_2(C_3)$. Since $Tor_2(C_3)$ is a cyclic code over the finite fieldF_p, the word w_0 can be decoded in the code $Tor_2(C_3)$. As $c_0(x) + uc_1(x) + u^2c_2(x) \in C_3$, then $c_1(x) \in C^{3,u} = Tor_1(C_3)$. So we can decode $w_1(x)$ in the code $Tor_1(C_3)$. Similarly we will decode $w_2(x)$ in the code $Tor_2(C_3)$.
Case(ii): Suppose n is not relatively prime to p. Similar to case (i) we can decode $w_0(x)$ in the code $Tor_2(C_3)$. Let $c(x) = c_0(x) + uc_1(x) + u^2c_2(x) \in C_3$, then $c(x) = (r_0(x)+ur_1(x)+u^2r_2(x))(g(x)+up_1(x)+u^2p_2(x))+(s_0(x)+us_1(x))(ua_1(x)+u^2q_1(x))+u^2t_0(x)a_2(x)$. Let $w_1'(x) = w_1(x)-r_0(x)p_1(x)$. Now, we know that $a_1(x) \mid g(x)$, then $w_1'(x)-e_1(x) \in \langle a_1(x)\rangle = Tor_1(C_3)$. So, $w_1'(x)$ can be decoded in $Tor_1(C_3)$. Then $w_1'(x) = d_1(x)a_1(x) + e_1(x)$ for some polynomial $d_1(x) \in F_p(x)$. So, $r_1(x), s_0(x)$ can be determined by dividing the polynomial $d_1(x)$ to $b_1(x)$. Let

$$w_2'(x) = w_2(x) - r_0(x)p_2(x) - r_1(x)p_1(x) - s_0(x)q_1(x).$$

But, we know that $a_2(x) \mid a_1(x) \mid g(x)$, so $w_2'(x) - e_2(x) \in \langle a_2(x)\rangle = Tor_2(C_3)$. Hence we can decode $w_2'(x)$ in the code $Tor_2(C_3)$. □

We work an example of this decoding procedure.

Example 4.1. *Let $\alpha \in GF(3^3)$ be a root of the irreducible polynomial $2x^3+x^2+x+1 \in F_3[x]$. In the following table we see that $2x^3+x^2+x+1$ is a primitive polynomial over the finite field F_3.*

i	α^i	i	α^i
1	010	7	121
2	001	8	120
3	111	9	012
4	122	10	220
5	201	11	022
6	101	12	221

Clearly $M_\alpha(x) = \Pi_{i\in C_1}(x-\alpha^i) = (x-\alpha)(x-\alpha^3)(x-\alpha^9) = 2x^3+x^2+x+1$ over the Galois field $GF(3^3)$. Also $M_{\alpha^2}(x) = 2x^3+x+1, M_{\alpha^4}(x) = 2x^3+2x^2+2x+1$ and $M_{\alpha^7}(x) = 2x^3+2x^2+1$. But $\{C_0, C_1, C_2, C_4, C_7\}$ is a set of representatives of the 3-cyclotomic cosets modulo 13, then $x^{13}-1 = (x+2)(2x^3+x^2+x+1)(2x^3+x+1)(2x^3+2x^2+2x+1)(2x^3+2x^2+1)$ over F_3 and $R_{3,3}$. Let

$$C_3 = \langle M_\alpha(x)M_{\alpha^2}(x)M_{\alpha^4}(x)M_{\alpha^7}(x) + uM_\alpha(x)M_{\alpha^2}(x)M_{\alpha^4}(x) + u^2M_\alpha(x)M_{\alpha^2}(x)\rangle$$

be a cyclic code of length 13 over the ring $R_{3,3}$. Since

$$Tor_2(C_3) = \langle M_\alpha(x)M_{\alpha^2}(x)\rangle,$$

the code $Tor_2(C_3)$ has roots $\{\alpha, \alpha^2, \alpha^3\}$ in the Galois field $GF(3^3)$. So, $Tor_2(C_3)$ is a ternary 1-error-correcting cyclic code. Also $Tor_1(C_3) = \langle M_\alpha(x)M_{\alpha^2}(x)M_{\alpha^4}(x)\rangle$, has roots $\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ in the Galois field $GF(3^3)$. So, $Tor_1(C_3)$ is a ternary 3-error-correcting cyclic code. Let $w(x) = 2x^{12}+2x^{10}+2x^9+2x^8+2x^7+2x^6+2x^5+2x^4+2x^3+2x^2+2x+2+u(x^{11}+2x^5+2x^4+2x^2+2)+u^2(2x^{12}+2x^{11}+x^{10}+2x^9+2x^7+2x^6+2x^4+2x^3+x^2+2)$ be a received word with an error polynomial $e(x) = e_0(x)+ue_1(x)+u^2e_2(x)$. Let $e_0(x) = ux^j$, where $u \in F_3$ and $0 \le j \le 12$. Since

$$S_1 = w_0(\alpha) = 022 = \alpha^{11} = e_0(\alpha) = u\alpha^j,$$

then $e_0(x) = x^{11}$. By using of the Sugiyama decoding algorithm ([6], Section 5.4.3) and the following table we can decode $w_1(x)$ in the code $Tor_1(C_3)$. Now, we know that at most three errors have been occuring and the syndromes are

$$S_1' = w_1(\alpha) = 2, S_2' = 2\alpha^9, S_3' = 2, S_4' = \alpha^{11}, S_5' = 2\alpha^3, S_6' = 2\alpha.$$

Now, we summarizes the results in the following table.

i	$r_i(x)$	$h_i(x)$	$b_i(x)$
-1	x^6		0
0	$2\alpha x^5 + 2\alpha^3 x^4 + \alpha^{11} x^3 + 2x^2 + 2\alpha^9 x + 2$		1
1	$\alpha^9 x^4 + \alpha^{12} x^3 + \alpha^{10} x^2 + 2\alpha^2 x + \alpha$	$2\alpha^{12} x + \alpha$	$\alpha^{12} x + 2\alpha$
2	$2\alpha^{11}$	$2\alpha^5 x + 2\alpha^2$	$\alpha^4 x^2 + 2\alpha^7 x + \alpha^{11}$

This implies that exactly two errors have been occuring. Hence $\sigma(x)$ is a multiple of $b_2(x) = \alpha^4 x^2 + 2\alpha^7 x + \alpha^{11}$. So $\sigma(x) = \alpha^2 b_2(x) = \alpha^6 x^2 + 2\alpha^9 x + 1$. It is easy to check that $\sigma(x)$ has roots α and α^6. Then the error location numbers are $X_1 = \alpha^{12}$ and $X_2 = \alpha^7$. As the code is ternary, we must determine the error magnitudes E_1 and E_2, where $e_1(x) = E_1 x^{12} + E_2 x^7$. Then we must solve the matrix equation

$$\begin{pmatrix} \alpha^{12} & \alpha^7 \\ \alpha^{11} & \alpha \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2\alpha^9 \end{pmatrix}.$$

Solution of this matrix equation implies that $E_1 = 2$ and $E_2 = 1$. Therefore $e_1(x) = 2x^{12} + x^7$. Similarly $w_2(\alpha) = 2\alpha^8$, then $e_2(x) = 2x^8$.□

In continue let C_k be a cyclic code of length n over the ring $R_{k,p}$, then for $i = 1, 2, \ldots, k-1$ the code $Tor_{k-1}(C_k)$ is defined as:

$$Tor_{k-1}(C_k) = \{t(x) \in \frac{F_p[x]}{\langle x^n - 1\rangle} \,|\, u^{k-1} t(x) \in C_k\}$$

It is clear that $Tor_{k-1}(C_k)$ is a cyclic code over the finite field F_p. Also for $i = 1, 2, \ldots, k-1$ the code C^{k,u^i} is defined as $C^{k,u^i} = \{c_i(x) \in \frac{F_p[x]}{\langle x^n-1\rangle} \,|\, c_0(x) + uc_1(x) + \cdots + u^{i-1}c_{i-1}(x) + u^{i+1}c_{i+1}(x) + \cdots + u^{k-1}c_{k-1}(x) \in C_k\}$, for some $c_0(x), c_1(x), \ldots, c_{k-1}(x) \in \frac{F_p[x]}{\langle x^n-1\rangle}$. It is clear that $Tor_i(C)$ and C^{k,u^i} are cyclic codes over the finite field F_p, for $i = 1, 2, \ldots, k-1$.

Lemma 4.4. *Let $C_k = \langle g + up_1 + \cdots + u^{k-1}p_{k-1}, ua_1 + \cdots + u^{k-1}q_{k-2}, u^2 a_2 + \cdots + u^{k-1}r_{k-3}, \ldots, u^{k-2}a_{k-2} + u^{k-1}s_1, u^{k-1}a_{k-1}\rangle$ be a cyclic code of length n over the ring $R_{k,p}$, then $Tor_i(C) = \langle a_i(x)\rangle$ for $i = 1, 2, \ldots, k-1$, and $d_H(C_k) = d_H(Tor_{k-1}(C_k))$.*

Proof. The proof is similar to proof of Lemma 3.1. □

Lemma 4.5. *Let $C_k = \langle g + ua_1 + u^2 a_2 + u^{k-2}a_{k-2} + u^{k-1}a_{k-1}\rangle$ be a cyclic code of length n over the ring $R_{p,n}$, and n is relatively prime to p, then for $i = 1, 2, \ldots, k-1$, the relation $C^{k,u^i} = Tor_i(C_k) = \langle a_i(x)\rangle$ does hold.*

Proof. Let $t(x) \in Tor_i(C_k)$, then $u^i t(x) \in C_k$. So $t(x) \in C^{k,u^i}$. Conversely let $c_i(x) \in C^{k,u^i}$, then $c_0(x) + uc_1(x) + \cdots + u^{k-1}c_{k-1}(x) \in C_k$ for some polynomials $c_0(x), c_1(x), \ldots, c_{k-1}(x)$. So, by Theorem 3.3, $c_0(x) + uc_1(x) + \cdots + u^{k-1}c_{k-1}(x) = (r_0(x) + ur_1(x) + \cdots + u^{k-1}r_{k-1)}(x))(g(x) + ua_1(x) + u^2 a_2(x) + u^{k-2}a_{k-2}(x) + u^{k-1}a_{k-1}(x))$. Then $c_i(x) = g(x)r_i(x) + a_1(x)r_{i-1}(x) + \cdots + a_i(x)r_0(x)$ for $i = 1, 2, \ldots, t-1$. Since $a_i(x) \,|\, a_{i-1}(x) \,|\, \ldots \,|\, a_2(x) \,|\, a_1(x) \,|\, g(x)$, we must have $c_i(x) \in \langle a_i(x)\rangle = Tor_i(C)$. □

Theorem 4.3. *Let C_k be a cyclic code of length n over the ring $R_{k,p}$. If $w(x) = w_0(x) + uw_1(x) + \cdots + u^{k-1}w_{k-1}(x)$ is a received word with an error polynomial $e(x) = e_0(x) + ue_1(x) + \cdots + u^{t-1}e_{t-1}(x)$,*

$$w_H(e_0(x)) \leq \lfloor \frac{(d_H(Tor_{k-1}(C_k) - 1)}{2} \rfloor$$

and for $i = 1, 2, \ldots, k-1$,

$$w_H(e_i(x)) \leq \lfloor \frac{(d_H(Tor_i(C_k) - 1)}{2} \rfloor,$$

then $w_0(x)$ can be decoded in the code $Tor_{k-1}(C_k)$ and for $i = 1, 2, \ldots, k-1$, $w_i(x)$ can be decoded in the code $Tor_i(C_k)$.

Proof. The proof is similar to proof of Theorem 4.2. □

5. Conclusions

We have described a decoding method for cyclic codes over the ring $\frac{F_p[u]}{\langle u^k\rangle}$, when the code length is an arbitrary number. A natural open problem is to extend this work for cyclic codes over chain rings, which residue field of chain ring is of characteristic prime number p. Another useful direction for further study would be to present a decoding algorithm for cyclic codes over the ring $\frac{F_p[u]}{\langle u^k\rangle}$ with considering the Lee weight.

Acknowledgments. The author would like to thank the anonymous reviewers for their valuable comments and suggestions which lead to improvement of this paper.

REFERENCES

[1] *T. Abualrub and I. Saip*, Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$, Des. Codes Crypt **42** (2007), 273-287.

[2] *E. Byrne, M. Greferath, J. Pernas, J. Zumbrgel*, Algebraic decoding of negacyclic codes over Z_4, Des. Codes Crypt **66** (2012) No.1-3, 3-16.

[3] *H. Q. Dinh, S. R. Lpez-Permouth*, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inf. Theory **50** (2004) No. 8, 1728-1744.

[4] *R. Fuji-Hara, Y.Miao, M. Mishima*, Optimal frequency hopping sequences: A combinatorial approach, IEEE Trans. Inform. Theory **50** (2004), 2408-2420.

[5] *A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Sole*, The Z_4-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inf. Theory **40** (1994), 301-319.

[6] *W. C. Huffman, V. Pless*, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2003.

[7] *J. A. Hunkaba*, Commutative ring with zero divisors, Pure and Applied Mathematics, Marcel Dekker, NewYork, 1988.

[8] *J. C. Interlando, R. Palazzo, M. Elia*, On the Decoding of Reed-Solomon and BCH Codes over Integer Residue Rings, IEEE Trans. Inform. Theory **43** (1997) No.3, 1012-1021.

[9] *J. Liang, L. Wang*, On cyclic DNA codes over $F_2 + uF_2$ J. Appl. Math. Comput. **51** (2016) No.1, 81-91.

[10] *G. H. Norton, A. Salagean*, On the Hamming distance of linear codes over a finite chain ring, IEEE Trans. Inform. Theory **46** (2000) No.3, 1060-1067.

[11] *A. Lempel, H. Greenberger*, Families of sequences with optimal Hamming correlation properties, IEEE Trans. Inform. Theory **IT-20** (1974), 90-94.

[12] *A. K. Singh, P. K. Kewat*, On cyclic codes over the ring $\frac{Z_p[u]}{\langle u^k \rangle}$, Des. Codes Crypt **74** (2013), 1-13.

[13] *P. Udaya, A. Bonnecaze*, Decoding of cyclic codes over $F_2 + uF_2$. IEEE Trans. Inf. Theory **45** (1999), 2148-2157.

[14] *P. Udaya, M.U. Siddiqi*, Optimal large linear complexity frequency hopping patterns derived from polynomials residue class rings, IEEE Trans. Inform. Theory **44** (1998), 1492-1503