Indian J. Pure Appl. Math., **50**(1): 113-120, March 2019
 DOI: 10.1007/s13226-019-0310-2

DECODING OF CYCLIC CODES OVER THE RING $\frac{F_2[u]}{\langle u^t\rangle}$

Karim Samei* and Mohammad Reza Alimoradi**

**Department of Mathematics, Bu-Ali Sina university, Hamedan, Iran*

***Department of Mathematics, Faculty of Mathematical Sciences, University of Malayer, Malayer, Iran*

e-mails: samei@ipm.ir; malimoradisharif@yahoo.com

(*Received* 17 *October* 2016; *accepted* 14 *March* 2018)

In this paper we resolve an open problem about decoding cyclic codes over the ring F_2+uF_2 with $u^2=0$. This problem was first proposed by AbuAlrub *et al*. in (Des Codes Crypt **42**: 273-287, 2007). Also we extend this decoding procedure for cyclic codes of arbitrary length over the ringe $\frac{F_2[u]}{\langle u^t\rangle}=F_2+uF_2+u^2F_2+\cdots+u^{t-1}F_2$, where $u^t=0$.

Key words : Cyclic codes, Hamming distance, decoding, torsion codes.

1. INTRODUCTION

Codes over finite rings have received much attention recently after Hammons *et al*. [4] found that some of the best non-linear codes such as the Kerdock, Preparata and Goethal codes can be viewed as linear codes over Z_4 via the Gray map from ${Z_4}^n$ to F_2^{2n}. Note that codes over finite rings have been studied in different contexts by numerous authors [1, 2, 4, 6, 7, 10]. Among codes over finite rings the class of cyclic codes is a significant class from both theoretical and practical point of view. Also cyclic codes are the powerful error-correcting codes and can be efficiently encoded and decoded. Recall that rings Z_4, F_2+uF_2, with $u^2=0$ and $F_2\times F_2$ are three non-isomorphic ring of order four. Since some of the binary codes with good error-correcting capability are Gray images of cyclic codes over these rings [1, 2, 4, 10], then the study of codes over these rings is significant. Unlike the binary field, there is a little work in the literature on the decoding of codes over finite rings. Recently a few papers have been published, such as decoding of negacyclic codes over the ring Z_4, [3] and decoding of cyclic codes of odd-length over the ring F_2+uF_2, [9]. In this paper we suggest a simple procedure for decoding of cyclic codes of arbitrary length over the ring $\frac{F_2[u]}{\langle u^t\rangle}=F_2+uF_2+u^2F_2+\cdots+$

$u^{t-1}F_2$, with $u^t = 0$ by using of the torsion codes, which are codes over residue field associated to a chain ring. Also we consider Hamming distance in order to estimate the error correction capability of codes over this ring.

Let R be a commutative ring with identity, a linear code C of length n is a R-submodule of R^n. For any ring R, a cyclic shift on R^n is a permutation σ such that

$$\sigma(c_0, c_1, \ldots, c_{n-2}, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$$

A linear code C over the ring R that is invariant under the cyclic shift is called a cyclic code. Recall that with the following correspondence:

$$R^n \to \frac{R[x]}{\langle x^n - 1\rangle}$$

$$(c_0, c_1, \ldots, c_{n-1}) \to c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$$

a cyclic code C of length n over R is an ideal of $R_n = \frac{R[x]}{\langle x^n-1\rangle}$. The Hamming weight of a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is defined by $w_H(c) = |\{i : c_i \neq 0\}|$ and the minimum Hamming distance of a code C is defined by $d_H(C) = min\{w_H(c) : 0 \neq c \in C\}$. We denote $\frac{F_2[u]}{\langle u^t\rangle}$ by R_t and $\frac{R_t[x]}{\langle x^n-1\rangle}$ by $R_{t,n}$. A finite ring R is called a chain ring if its ideals ordered by inclusion. Clearly a finite chain ring is a local ring. Also a finite ring is a finite chain ring if and only if it is a local ring and its maximal ideal is a principal ideal (see proposition 2.1 in [7]). Let $\langle a\rangle$ be a unique maximal ideal of the finite chain ring R, where a is a nilpotent element of R with nilpotency index e and let denote by k the field $\frac{R}{\langle a\rangle}$. Now assume that C is a code of length n over the chain ring R. For $i = 1, 2, \ldots, e-1$ the projections of $(C : a^i)$ over the field k are denoted by $\overline{(C : a^i)}$ and are called the torsion codes associated to the code C, where $(C : a^i)$ is defined as $(C : a^i) = \{x \in R^n : xa^i \in C\}$.

2. Main Results

Udaya and Bonnecaze [9] gave a decoding algorithm for cyclic codes of odd-length over the ring $F_2 + uF_2$ by using a suitable Gray map and a $\langle \boldsymbol{u}, \boldsymbol{u} + \boldsymbol{v}\rangle$ construction. They associated to each code C over the ring $F_2 + uF_2$ two binary codes

$$Res(C) = \{a(x) \in \frac{F_2[x]}{\langle x^n - 1\rangle} \,|\, \exists\, b(x)\,, a(x) + ub(x) \in C\}$$

and

$$Tor_1(C) = \{k(x) \in \frac{F_2[x]}{\langle x^n - 1\rangle} \,|\, uk(x) \in C\}.$$

In addition the decoding procedure is done in Galois extension of F_2+uF_2. In this section we present a decoding procedure for cyclic code over the ring $\frac{F_2[u]}{\langle u^t\rangle}$ by using of torsion codes. At first we explain this procedure for cyclic codes over both rings F_2+uF_2 and $F_2+uF_2+u^2F_2$. Now let C be a code of length n over the ring F_2+uF_2. Note that F_2+uF_2 is a chain ring with maximal ideal $\langle u\rangle$, where u is a nilpotent element with nilpotency index two. Now we associate to the code C two binary codes. The torsion code $Tor_1(C)$ is defined as:

$$Tor_1(C)=\{k(x)\in F_{2,n}:\ uk(x)\in C\}$$

and the code C^u is defined as:

$$C^u=\{k(x)\in F_{2,n}:\ t(x)+uk(x)\in C,\ \text{for some},\ t(x)\in F_{2,n}\}.$$

Similarly the ring $F_2+uF_2+u^2F_2$ is a chain ring with unique maximal ideal $\langle u\rangle$ and residue field F_2. Now let C be a cyclic code of length n over $F_2+uF_2+u^2F_2$, we associate to the code C two binary codes $Tor_2(C)$ and C^{u^2}, which the code C^{u^2} is defined as:

$$C^{u^2}=\{c_2(x)\in F_{2,n}: c_0(x)+uc_1(x)+u^2c_2(x)\in C\,\text{for some}\,c_0(x),c_1(x)\in F_{2,n}\}.$$

$([1],\text{Theorem }1)$ Let C be a cyclic code of length n over the ring F_2+uF_2, then $C=\langle g(x)+up(x),ua(x)\rangle$, where $g(x),p(x),a(x)$ are binary polynomials with $a(x)\,|\,g(x)$ and $g(x)\,|\,(x^n-1)$ in F_2, and $a(x)\,|\,p(x)\frac{x^n-1}{g(x)}$ and $deg(p(x))<deg(a(x))$. $([7],\text{Theorem }3.6)$. Let C be a cyclic code over R_t, then C is an ideal in $R_{t,n}$ that can be generated by $C=\langle g+up_1+\cdots+u^{t-1}p_{t-1},ua_1+u^2q_1+\cdots+u^{t-1}q_{t-2},u^2a_2+u^3r_1+\cdots+u^{t-1}r_{t-3},\ldots,u^{t-2}a_{t-2}+u^{t-1}s_1,u^{t-1}a_{t-1}\rangle$, with $a_{t-1}(x)\,|\,a_{t-2}(x)\,|\,\ldots,\,|\,a_2(x)\,|\,a_1(x)\,|\,g(x)\,|\,(x^n-1)$ in F_2. When n is an odd number, then $C=\langle g(x)+ua_1(x)+\cdots+u^{t-1}a_{t-1}(x)\rangle$. C be a cyclic code of odd-length n over the ring F_2+uF_2, then $C=\langle g(x)+ua(x)\rangle$.

PROOF : Since n is an odd number, then x^n-1 factors uniquely into a product of distinct irreducible polynomials. Then $\gcd(a(x),\frac{x^n-1}{g(x)})=1$, so $a(x)\,|\,p(x)$. Now we know that $deg\,p(x)<deg\,a(x)$, then $p(x)=0$. So $C=\langle g(x),ua(x)\rangle$. Let $h(x)=g(x)+ua(x)$. Since n is relatively prime to two, then $R_{2,n}$ is a reduced and 0-dimensional ring. So by Lemma 1 in [5], there exist an idempotent $e(x)$ in $R_{2,n}$ such that $\langle g(x)\rangle=\langle e(x)\rangle$. Thus $e(x)=r(x)g(x)$ for some polynomial $r(x)\in R_{2,n}$. Then $e(x)=r^2(x)g^2(x)$. As $h^2(x)=g^2(x)$, then $e(x)\in\langle h(x)\rangle$. This implies that $g(x)\in\langle e(x)\rangle\subseteq\langle h(x)\rangle$. So $\langle g(x),ua(x)\rangle=\langle h(x)\rangle$.

Lemma 1 — Let $C=\langle g(x)+up(x),ua(x)\rangle$ be a cyclic code of length n over the ring R_2, then $Tor_1(C)=\langle a(x)\rangle$ and $d_H(C)=d_H(Tor_1(C))$.

PROOF : Let $k(x) \in Tor_1(C)$, then $uk(x) \in C$. So there exist $r_0(x) + ur_1(x), s_0(x) + us_1(x) \in R_{2,n}$ such that

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

But we know that $a(x) \mid g(x)$, then $k(x) \in \langle a(x) \rangle$. Conversely $ua(x) \in C$, implies that $a(x) \in Tor_1(C)$. Now Theorem 4.2 of [6] implies that $d_H(C) = d_H(Tor_1(C))$.

Lemma 2 — Let C be a cyclic code of odd-length n over $F_2 + uF_2$, then $C^u = Tor_1(C)$.

PROOF : Let $c_2(x) \in Tor_1(C)$, then there exist $c_1(x) \in R_{2,n}$ such that $c_1(x) + uc_2(x) \in C = \langle g(x) + ua(x) \rangle$. So $c_1(x) + uc_2(x) = (h_1(x) + uh_2(x))(g(x) + ua(x))$, for some polynomials $h_1(x), h_2(x) \in F_{2,n}$. This implies that $c_2(x) = h_1(x)a(x) + h_2(x)g(x)$. As we know that $a(x) \mid g(x)$, then $c_2(x) \in \langle a(x) \rangle$, so $C^u \subseteq Tor_1(C)$. Conversely if $c(x) \in Tor_1(C)$, then $uc(x) \in C$, this implies that $c(x) \in C^u$. So $C^u = Tor_1(C)$.

***Theorem* 1** — *Let $C = \langle g(x) + up(x), ua(x) \rangle$ be a cyclic code of length n over $F_2 + uF_2$, $w(x) = w_1(x) + uw_2(x)$ be a received word with an error polynomial $e(x) = e_1(x) + ue_2(x)$ and $w_H(e_i(x)) \leq \lfloor \frac{d_H(Tor_1(C)-1)}{2} \rfloor$, for $i = 1, 2$. Then $w_i(x)$ will be decoded in binary code $Tor_1(C)$.*

PROOF : Case(i) Let n be an odd number and $w(x) = c(x) + e(x)$, where $c(x) = c_1(x) + uc_2(x)$ is a codeword in C. Since $uc(x) = uc_1(x) \in C$, then $c_1(x) \in Tor_1(C)$. As $uc_1(x) = u(w_1(x) - e_1(x))$ and $Tor_1(C)$ is a binary cyclic code, then we can determine $e_1(x)$ with using of decoding algorithms in F_2. Since $d_H(w_1, c_1) = w_H(e_1) \leq \lfloor \frac{d_H(Tor_1(C)-1)}{2} \rfloor$, then the word $w_1(x)$ will be decoded uniquely to $c_1(x)$. Similarly $w_2(x) = c_2(x) + e_2(x)$. Since $c_2(x) \in C^u = Tor_1(C)$ and $d_H(w_2, c_2) = w_H(e_2) \leq \lfloor \frac{d_H(Tor_1(C)-1)}{2} \rfloor$, then $w_2(x)$ will be decoded uniquely to $c_2(x)$.

Case (ii) : Let n be an even number and $w(x) = c(x) + e(x)$, where $c(x) = c_1(x) + uc_2(x)$ is a codeword in C. Since $uc(x) = uc_1(x) \in C$, then $c_1(x) \in Tor_1(C)$. Similar to case i we can determine $e_1(x)$ in binary code $Tor_1(C)$ and $w_1(x)$ will be decoded to $c_1(x)$. Also by the structure of code C there exist binary polynomials $r_1(x), r_2(x), s(x) \in F_{2,n}$ such that $c_2(x) = r_1(x)p(x) + r_2(x)g(x) + s(x)a(x)$. Now we know that $a(x) \mid g(x)$. So $w_2(x) - r_1(x)p(x) - e_2(x) \in \langle a(x) \rangle$. Let $w_2'(x) = w_2(x) - r_1(x)p(x)$, then $w_2'(x) - e_2(x) = \langle a(x) \rangle = Tor_1(C)$. So we can determine $e_2(x)$ in binary code $Tor_1(C)$ with using of decoding algorithms in F_2.

Lemma 3 — Let $C = \langle g(x) + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x) \rangle$ be a cyclic code of length n over $F_2 + uF_2 + u^2F_2$, then $Tor_2(C) = \langle a_2(x) \rangle$ and also $d_H(C) = d_H(Tor_2(C))$.

PROOF : At first we show that $Tor_2(C) = \{k(x) \in F_{2,n} | u^2k(x) \in C\}$. Let $k(x) \in Tor_2(C)$, then $k(x) = \overline{h(x)}$, where $\overline{h(x)}$ denote image of $h(x)$ in $F_{2,n}$. So $u^2h(x) \in C$. Let $h(x) = h_0(x) +$

$uh_1(x) + u^2h_2(x)$, where $h_0(x), h_1(x), h_2(x)$ are binary polynomials. Then $u^2h(x) = u^2h_0(x) = u^2k(x)$. So $Tor_2(C) = \{k(x) \in F_{2,n} : u^2k(x) \in C\}$. Then by theorem 4.2 of [6], we have $d_H(C) = d_H(Tor_2(C))$. Since $u^2a_2(x) \in C$, then $a_2(x) \in Tor_2(C)$. So $\langle a_2(x)\rangle \subseteq Tor_2(C)$.

Conversely let $k(x) \in Tor_2(C)$, then $u^2k(x) \in C$, therefore $u^2k(x) = (r_0(x) + ur_1(x) + u^2r_2(x))(g(x) + up_1(x) + u^2p_2(x)) + (s_0(x) + us_1(x) + u^2s_2(x))(ua_1(x) + u^2q_1(x)) + (t_0(x) + ut_1(x) + u^2t_2(x))(u^2a_2(x))$. So $k(x) = r_2(x)g(x) + s_1(x)a_1(x) + t_0(x)a_2(x)$. But we know that $a_2(x) \,|\, a_1(x) \,|\, g(x)$, then $k(x) \in \langle a_2(x)\rangle$.

Lemma 4 — Let C be a cyclic code of odd-length n over the ring $F_2 + uF_2 + u^2F_2$, then $C^{u^2} = Tor_2(C)$.

PROOF : Let $c_2 \in C^{u^2}$, then there exist $c_0, c_1 \in F_{2,n}$ such that

$$c_0(x) + uc_1(x) + u^2c_2(x) \in C = \langle g(x) + ua_1(x) + u^2a_2(x)\rangle$$

So $c_0(x) + uc_1(x) + u^2c_2(x) = (h_0(x) + uh_1(x) + u^2h_2(x))(g(x) + ua_1(x) + u^2a_2(x))$. Then $c_2(x) = h_0(x)a_2(x) + h_1(x)a_1(x) + h_2(x)g(x)$. Now, we know that $a_2(x) \,|\, a_1(x) \,|\, g(x)$, then $c_2(x) \in \langle a_2(x)\rangle$. So $C^{u^2} \subseteq Tor_2(C)$. Conversely if $c(x) \in Tor_2(C)$, then $u^2c(x) \in C$. This implies that $c(x) \in C^{u^2}$. So $C^{u^2} = Tor_2(C)$.

For any cyclic code C of length n over $F_2 + uF_2 + u^2F_2$, we define binary code C^u as following:

$$C^u = \{c_1 \in F_{2,n} : c_0 + uc_1 + u^2c_2 \in C \,\text{for some}\, c_0, c_2 \in F_{2,n}\}.$$

Lemma 5 — Let C be a cyclic code of odd-length n over the ring $F_2 + uF_2 + u^2$, then $C^u = Tor_1(C)$.

PROOF : At first we show that $Tor_1(C) = \langle a_1(x)\rangle$, where $C = \langle g(x) + ua_1(x) + u^2a_2(x)\rangle$. Clearly $Tor_1(C) = \{k(x) \in F_{2,n} : uk(x) + u^2t(x) \in C, \exists\, t(x) \in F_{2,n}\}$. Since $ua_1(x) \in C$, then $a_1(x) \in Tor_1(C)$. Conversely if $k(x) \in Tor_1(C)$, then $uk(x) + u^2t(x) \in C$, for some $t(x) \in F_{2,n}$.

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

So $k(x) = h_0(x)a_1(x) + h_1(x)g(x)$. Then $k(x) \in \langle a_1(x)\rangle$. Since $ua_1(x) \in C$, then $a_1(x) \in C^u$. So $\langle a_1(x)\rangle \subseteq C^u$. Let $c_1(x) \in C^u$, then there exist $c_0(x), c_2(x) \in F_{2,n}$, such that $c_0(x) + uc_1(x) + u^2c_2(x) \in C$. So

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

Therefore $c_1(x) = h_0(x)a_1(x) + h_1(x)g(x)$. As we know that $a_1(x) | g(x)$, thus $c_1(x) \in \langle a_1(x)\rangle$.

Theorem 2 *— Let $C = \langle g(x) + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x)\rangle$ be a cyclic code of length n over the ring $F_2+uF_2+u^2F_2$. If $w(x) = w_0(x)+uw_1(x)+u^2w_2(x)$ be a received word with an error polynomials $e(x) = e_0(x)+ue_1(x)+u^2e_2(x)$. Also $w_H(e_i(x)) \leq \lfloor \frac{(d_H(Tor_2(C)-1)}{2} \rfloor$ for $i = 0, 2$. and $w_H(e_1(x)) \leq \lfloor \frac{(d_H(Tor_1(C)-1)}{2} \rfloor$, then $w_0(x), w_2(x)$ will be decoded in code $Tor_2(C)$ and $w_1(x)$ will be decoded in code $Tor_1(C)$.*

PROOF : *Case* (i). Suppose n is an odd number and $w(x) = c(x) + e(x)$, where $c(x) = c_0(x) + uc_1(x) + u^2c_2(x)$ is a code-word in C. Since $u^2c(x) = u^2c_0(x) \in C$ and $u^2c_0(x) = u^2(w_0(x) - e_0(x))$, this implies that $w_0(x) - e_0(x) \in Tor_2(C)$. Since $Tor_2(C)$ is a binary code, we can decode w_0 in $Tor_2(C)$. Since $c_1(x) \in C^u = Tor_1(C)$ and $c_1(x) = (w_1(x) - e_1(x))$. As $Tor_1(C)$ is a binary code, then we can decode w_1 in $Tor_1(C)$. In this approach we can decode $w_2(x)$ in binary code $C^{u^2} = Tor_2(C)$.

Case (ii). Let n be an even number and $w(x) = c(x) + e(x)$, where $c(x) = c_0(x) + uc_1(x) + u^2c_2(x)$ is a codeword in C. Similar to case i, we can decode $w_0(x)$ in binary code $Tor_2(C)$. By using of the structure of code C, there exist binary polynomials $r_0, r_1, r_2, s_0, s_1, t_0$ such that $c_1(x) = r_0(x)p_1(x) + r_1(x)g(x) + s_0(x)a_1(x)$ and

$$c_2(x) = r_0(x)p_2(x) + r_1(x)p_1(x) + s_0(x)q_1(x) + r_2(x)g(x) + s_1(x)a_1(x) + t_0(x)a_2(x)$$

Let $w_1'(x) = w_1(x)-r_0(x)p_1(x)$, now we know that $a_1(x) \mid g(x)$. So $w_1'(x)-e_1(x) \in \langle a_1(x)\rangle = Tor_1(C)$. So $w_1'(x)$ will be decoded in binary code $Tor_1(C)$. Then $w_1'(x) = d_1(x)a_1(x) + e_1(x)$ for some binary polynomial $d_1(x)$. Therefore $r_1(x), s_0(x)$ completly determined by dividing binary polynomials $d_1(x)$ to $b_1(x)$. Let $w_2'(x) = w_2(x) - r_0(x)p_2(x) - r_1(x)p_1(x) - s_0(x)q_1(x)$ As $a_2(x) \mid a_1(x) \mid g(x)$, then $w_2'(x) - e_2(x) \in \langle a_2(x)\rangle = Tor_2(C)$. So $w_2'(x)$ and therefore $w_2(x)$ will be decoded in binary code $Tor_2(C)$.

We work an example of this decoding procedure.

Let $C = \langle (x-1)^7 + u(x-1)^5 + u^2(x-1)^4, u(x-1)^6 + u^2(x-1)^3, u^2(x-1)^5\rangle$ be a cyclic code of length 8 over $F_2 + uF_2 + u^2F_2$. Now we know that $d_H(C) = d_H(Tor_2(C))$ and $Tor_2(C) = \langle a_2(x)\rangle = \langle (x-1)^5\rangle$, we must compute $d_H(Tor_2(C))$. Since 5 has a 2-adic length 1 nonzero expansion, then $d_H(C) = 4$. (see Lemma 10 in [1]). So C is a 1-error-correcting code. If $w(x) = x^6+x^5+x^4+x^3+x^2+x+1+u(x^7+x^6+x^5+x^2+x)+u^2(x^7+x^6+x^5+x^2+1)$ be a received word, then $w_0(x) = xa_2(x) + (x^4 + x^3 + 1)$. So by using of decoding algorithm for cyclic codes over binary field (see Page 148 in [8]), we obtain $e_0(x) = x^7$. Therefore $c_0(x) = (x-1)^7 = g(x)$. So $r_0(x) = 1$, then $w_1'(x) = (x+1)a_1(x)+x^5+x^3+x$. Similarly using of decoding algorithm for cyclic codes over binary field implies that $e_1(x) = x^7$. So $w_1'(x) - e_1(x) = a_1(x)$, therefore $d_1(x) = x^8$.

So $r_1(x) = (x-1)^7, s_0(x) = 1$. Therefore we obtain $w_2'(x) - e_2(x) = x^2a_2(x) + x^4 + x^2 + 1$, then $e_2(x) = x^6$. If we correct these errors in the received polynomial, then the vector $w(x)$ will be decoded to $c(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 + u(x^6 + x^4 + x^2 + 1) + u^2(x^7 + x^5 + x^4 + x^3 + x + 1)$. In continue of this section we will describe decoding procedure for cyclic codes over $\frac{F_2[u]}{\langle u^t\rangle}$ for $t \geq 3$. Now let C be a cyclic code over the ring R_t, for any $i = 1, 2, \ldots, t-1$ we define codes C^{u^i} as $C^{u^i} = \{c_i(x) \in F_{2,n} : c_0(x) + uc_1(x) + \cdots + u^{t-1}c_{t-1}(x) \in C\}$, for some $c_0(x), c_1(x), \ldots, c_{i-1}(x), c_{i+1}(x), \ldots, c_{t-1}(x) \in F_{2,n}$.

Clearly $Tor_i(C) = \{k(x) \in F_{2,n} : u^ik(x) \in C\}$ and C^{u^i} are binary cyclic codes for $i = 1, 2, \ldots, t-1$.

Lemma 6 — Let $C = \langle g+up_1+\cdots+u^{t-1}p_{t-1}, ua_1+\cdots+u^{t-1}q_{t-2}, u^2a_2+\cdots+u^{t-1}r_{t-3}, \ldots, u^{t-2}a_{t-2} + u^{t-1}s_1, u^{t-1}a_{t-1}\rangle$ be a cyclic code of length n over R_t, then $Tor_i(C) = \langle a_i(x)\rangle$ for $i = 1, 2, \ldots, t-1$ and $d_H(C) = d_H(Tor_{t-1}(C))$.

PROOF : Similar to Lemma 4.

Lemma 7 — Let $C = \langle g + ua_1 + u^2a_2 + u^{t-2}a_{t-2} + u^{t-1}a_{t-1}\rangle$ be a cyclic code of odd-length n over the ring R_t, then for $i = 1, 2, \ldots, t-1$, the relation $C^{u^i} = Tor_i(C) = \langle a_i(x)\rangle$ does hold.

Proof : Let $k(x) \in Tor_i(C)$, then $u^ik(x) \in C$. So $k(x) \in C^{u^i}$. Conversely let $c_i(x) \in C^{u^i}$, then $c_0(x) + uc_1(x) + \cdots + u^{t-1}c_{t-1}(x) \in C$ for some polynomials $c_0(x), c_1(x), \ldots, c_{t-1}(x)$. So $c_0(x) + uc_1(x) + \cdots + u^{t-1}c_{t-1}(x) = (r_0(x) + ur_1(x) + \cdots + u^{t-1}r_{t-1}(x))(g(x) + ua_1(x) + u^2a_2(x) + u^{t-2}a_{t-2}(x) + u^{t-1}a_{t-1}(x))$. Then $c_i(x) = g(x)r_i(x) + a_1(x)r_{i-1}(x) + \cdots + a_i(x)r_0(x)$ for any $i = 1, 2, \ldots, t-1$. But we know that $a_i(x) \mid a_{i-1}(x) \mid \ldots \mid a_2(x) \mid a_1(x) \mid g(x)$, then $c_i(x) \in \langle a_i(x)\rangle = Tor_i(C)$.

***Theorem* 3** — *Let* $C\langle g+up_1+\cdots+u^{t-1}p_{t-1}, ua_1+\cdots+u^{t-1}q_{t-2}, u^2a_2+\cdots+u^{t-1}r_{t-3}, \ldots, u^{t-2}a_{t-2} + u^{t-1}s_1, u^{t-1}a_{t-1}\rangle$ *be a cyclic code of length* n *over the ring* R_t. *If* $w(x) = w_0(x) + uw_1(x) + \cdots + u^{t-1}w_{t-1}(x)$ *be a received word with an error polynomials* $e(x) = e_0(x) + ue_1(x) + \cdots + u^{t-1}e_{t-1}(x), w_H(e_0(x)) \leq \lfloor(\frac{d_H(Tor_{t-1}(C)-1)}{2}\rfloor$ *and* $w_H(e_i(x)) \leq \lfloor(\frac{d_H(Tor_i(C)-1)}{2}\rfloor$ *for* $i = 1, 2, \ldots, t-1$. *Then* $w_0(x)$ *will be decoded in binary code* $Tor_{t-1}(C)$ *and* $w_i(x)$ *will be decoded in binary codes* $Tor_i(C)$. *for* $i = 1, 2, \ldots, t-1$.

PROOF : Similar to Theorem 2.

3. CONCLUSION

We have described a decoding procedure for cyclic codes over the ring $\frac{F_2[u]}{\langle u^t\rangle}$, when the code length

is an arbitrary number with using of torsion codes associated to code, which these codes are binary codes. A natural open problem is to extend this work to cyclic codes over chain rings, which residue field of chain ring is of characteristic two. We also expect to present a decoding algorithm for cyclic codes over this ring with considering the Lee weight.

ACKNOWLEDGEMENT

The authors are thankful to the anonymous referees for their careful reading of the paper and valuable comments.

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**(3) (2013), 273-287.
2. A. Bonnecaze and P. Udaya, Cyclic codes and self-dual codes over F_2+uF_2, *IEEE Trans. Inf. Theory*, **45** (1999), 1250-1255.
3. E. Byrne, M. Greferath, J. Pernas, and J. Zumbrgel, Algebraic decoding of negacyclic codes over Z_4, *Des. Codes. Crypt*., **66**(1-3) (2007), 3-16.
4. A. R. Jr. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, The $Z4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, **40**(2) (1994), 301-319.
5. J. A. Huckaba, *Commutative ring with zero divisors*, Pure and Applied Mathematics, Marcel Dekker, New York (1988).
6. G. H. Norton and A. Salagean, On the Hamming distance of linear codes over a finite chain ring, *IEEE Trans. Inform. Theory*, **46**(3) (2000), 1060-1067.
7. H. Quang Dinh and S. R. Lpez-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory*, **50**(8) (2004), 1728-1744.
8. S. Ling and C. Xing, *Coding theory a first course*, Cambridge University Press (2004).
9. P. Udaya and A. Bonnecaze, Decoding of cyclic codes over F_2+uF_2, *IEEE Trans. Inform. Theory*, **45** (1999), 2148-2157.
10. S. Zhu, Y. Wang, and M. Shi, Some results on cyclic codes over F_2+vF_2, *IEEE Trans. Inform. Theory*, **56**(4) (2010), 1680-1684.