Palestine Journal of Mathematics

Vol. 12(2)(2023) , 321–328

Decoding of cyclic codes over a class of finite rings

Mohammad Reza Alimoradi

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 94B05, 94B15; Secondary 94B05, 94B15.

Keywords and phrases: Decoding, Chain rings, Principal ideal rings, Chines Remainder Theorem, Torsion codes.

Abstract In this paper, a decoding procedure for cyclic codes of odd length over the ring $F_p + vF_p$ is presented. Also a decoding method for cyclic codes over ring R is proposed when $R \simeq R_1 \times R_2 \times \cdots \times R_t$ and decoding of cyclic codes over R_i is available. Since any finite principal ideal ring is isomorphic to a finite product of chain rings, we can decode cyclic codes over finite principal ideal ring, when decoding of cyclic codes over chain rings is given

1 Introduction

A class of constacyclic codes over $F_p + vF_p$, where p is a odd prime number, where studied by Zhu et al. in [7]. They introduced a Gray map from the ring $F_p + vF_p$ to F_p^2 and proved that the image of a $(1-2v)$-constacyclic code of length n over $F_p + vF_p$ under this Gray map is a distance-invariant linear cyclic code of length $2n$ over F_p. Recently quadratic residue codes over $F_p + vF_p$ have been considered by Kaya et al. in [6]. The main purpose of this article is presentation of a decoding procedure for cyclic codes over finite ring R, where R is isomorphic to a finite product of chain rings. Specially we present a method for decoding cyclic codes of odd length over the ring $F_p + vF_p$, with $v^2 = v$. The rest of this paper is organized as follows. Section 2 recalls some basic definitions and notations that are used in the sequel of this paper. A decoding procedure for cyclic codes over the ring $F_p + vF_p$ is presented in section 3. A decoding method for cyclic codes over finite ring R, when R is isomorphic to a finite product of local rings is proposed in section 4.

2 Preliminaries

In this paper, we assume that all rings are commutative with identity. A finite ring R is called a chain ring if its ideals ordered by inclusion. Examples of finite chain rings are Galois rings and the ring Z_{p^s} of integer modulo p^s. Obviously a finite chain ring is a local ring. It is easy to see that a ring is finite chain ring if and only if its maximal ideal is a principal ideal. Let $m = \langle a \rangle$ be a unique maximal ideal of finite chain ring R, where a is a nilpotent element of R. The smallest positive integer t such that $a^t = 0$ is called the nilpotency index of a. A ring R is called principal ideal ring if each ideal of R is a principal ideal.

Theorem 2.1. *(see [4], Proposition* 2.7*) Let R be a finite commutative ring. Then the following conditions are equivalent:*

(i) R is a principal ideal ring.

(ii) R is isomorphic to a finite product of chain rings

Moreover, the decomposition in (ii) is unique up to the order of factors. □

.

A linear code C of length n over a ring R is an R-submodule of R^n. Linear code C is said to be cyclic if for every codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ its cyclic-shift $\sigma(c) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, negacyclic if $\gamma(c) = (-c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ and λ-constacyclic if $\tau(c) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, where λ is a unite in R. Let $R \simeq R_1 \times R_2 \times \cdots R_t$, then $R \simeq e_1R_1 \oplus e_2R_2 \oplus \cdots \oplus e_tR_t$, where for $i = 1, 2, \ldots, t$ idempotent e_i is a t-tuple such that the i-th component is equal to 1 and all other components are zero. Let I be an ideal of the ring

R, the canonical homomorphism $\pi : R \to \frac{R}{I}$ is defined by $\pi(x) = x + I$. For each positive integer n this homomorphism can be extended to $\psi : R^n \to (\frac{R}{I})^n$ by

$$\psi(x_1, x_2, \ldots, x_n) = (x_1 + I, x_2 + I, \ldots, x_n + I)$$

Let R be a finite local ring with unique maximal ideal m. Since m is nilpotent, the smallest $s \geq 1$ such that $m^s = 0$ is called the index of nilpotency. Clear that each finite ring has finitely many maximal ideals. Suppose $m_1, m_2, \ldots, m_t$ are maximal ideals of finite ring R and for $i = 1, 2, \ldots, t$ the index of nilpotency of m_i is s_i. We denote the quotient ring $\frac{R}{{m_i}^{s_i}}$ by R_i. Since ${m_1}^{s_1}, {m_2}^{s_2}, \ldots {m_t}^{s_t}$ are relatively prime in pairs, we have

$$\Pi_{i=1}^{t} {m_i}^{s_i} = \cap_{i=1}^{t} {m_i}^{s_i} = 0$$

Therefore the Chinese Remainder Theorem implies that the canonical map

$$\psi : R \to \Pi_{i=1}^{t} R_i$$

is defined by:

$$\psi(x) = (x + {m_1}^{s_1}, x + {m_2}^{s_2}, \ldots, x + {m_t}^{s_t})$$

is a ring isomorphism. For $i = 1, 2, \ldots, t$, the canonical map $\psi_i : R^n \to {R_i}^n$ is a homomorphism. Let C be a code of length n over R. Then for $i = 1, 2, \ldots, t$, $\psi_i(C) \subset {R_i}^n$ is denoted by C_i. The extended map $\psi : R^n \to \Pi_{i=1} {R_i}^n$ is defined by $\psi(x) = (\psi_1(x), \psi_2(x), \ldots$ $, \psi_t(x))$ is a R-module isomorphism, then $C \simeq C_1 \times C_2 \times \cdots \times C_t$. Conversely for $i = 1, 2, \ldots, t$, let C_i be a code of length n over R_i. Then $C = CRT(C_1, C_2, \ldots, C_t)$ is defined by

$$C = \{\psi^{-1}(x_1, x_2, \ldots, x_t) : x_i \in C_i\,, i = 1, 2, \ldots, t\}$$

is a code over the ring R. With the above notation the code C is called Chinese product of codes $C_1, C_2, \ldots, C_t$.

3 Decoding of cyclic codes over $F_p + vF_p$

The main purpose of this section is to give a decoding algorithm for cyclic codes over the ring $F_p + vF_p$. Throughout this section R_p will denote the ring $F_p + vF_p$ and $R_{p,n}$ denote the ring $\frac{R_p[x]}{\langle x^n - 1\rangle}$. It is easy to see that both $\frac{R_p}{\langle v\rangle}$ and $\frac{R_p}{\langle 1-v\rangle}$ are isomorphic to F_p. From the Chinese Remainder Theorem, we have $R_p \simeq F_p \times F_p$. From the ideals of R_p, we can see that they do not form a chain. For instance, two ideals $\langle v\rangle$ and $\langle 1 - v\rangle$ are not comparable. Since R_p is a finite semi-local ring, the polynomial factorization over this ring is not unique. So Hensel Lemma is not valid. Instead of Hensel lift the Chinese Remainder Theorem has an essential role in the study of codes over this ring.

Let p be an odd prime number and $\lambda = 1 - 2v$ be a unit in R_p. We see that any element $c \in {R_p}^n$ can be written as:
$c = a + vb = (a + b)v + a(1 - v)$, where $a, b \in {F_p}^n$
So for each code C over R_p two codes C_{1-v} and C_v are defined as:

$$C_{1-v} = \{a \in {F_p}^n \mid \exists b \in {F_p}^n\ : va + (1 - v)b \in C\}$$

$$C_v = \{b \in {F_p}^n \mid \exists a \in {F_p}^n\ : va + (1 - v)b \in C\}.$$

From definition of C_{1-v} and C_v, we have $C = vC_{1-v} \oplus (1 - v)C_v$. In other word any code C over R_p can be characterized by its associated codes C_{1-v} and C_v.

Theorem 3.1. *(see [6], Proposition* 2.6*) Let $\psi : R_{p,n} \to S_{p,n}$ be defined as*

$$\psi(c(x)) = c((1 - 2v)x).$$

If n is odd, then ψ is a ring isomorphism, where $S_{p,n} = \frac{R_p[x]}{\langle x^n-(1-2v)\rangle}$. □

From now on we assume that the length of all codes over the ring R_p is an odd number. From Theorem 3.1, we have the following Theorem.

Theorem 3.2. *(see [7], Theorem 4.2, 4.3)Let $C = vC_{1-v} \oplus (1-v)C_v$ be a linear code of length n over R_p. Then C is a cyclic code of length n over R_p if and only if C_{1-v} and C_v are cyclic codes of length n over F_p. Also $C = \langle vg_1(x), (1-v)g_2(x)\rangle$, where $g_1(x), g_2(x)$ are the monic generator polynomials of C_{1-v} and C_v, respectively. Moreover for any cyclic code of length n over R_p, there is a unique polynomial $g(x)$ such that $C = \langle g(x)\rangle$ and $g(x) \mid x^n - 1$, where $g(x) = vg_1(x) + (1-v)g_2(x)$.* □

The Gray map $\varphi : R_p \to F_p^2$, is given in [7] as:

$$\varphi(a + vb) = (-b, 2a + b) = (-b, -b + 2(a + b)).$$

This map can be extended to ${R_p}^n$ in a natural way. From definition of Lee weight and Gray map φ, we have $w_L(c) = w_H(\varphi(c))$ for any $c \in {R_p}^n$. Now let C be a cyclic code of length n over R_p, $c = a + vb \in C$ and $\bar{C} = C_{1-v} \oplus C_v$. Then $b \in \bar{C}$. If $C_{1-v} \subseteq C_v$, then $\bar{C} = C_v$. So $|C| = |C_{1-v}||\bar{C}|$. Therefore the code $\varphi(C)$ can be seen as equivalent to a $\langle \mathbf{u}, \mathbf{u+v}\rangle$ code with codes $\bar{C}$ and C_{1-v}. Suppose $C_{1-v} \subseteq C_v$, from the definition of the Gray map φ, the vector space structure of R_p and $p > 2$ it is easy to see that any codeword in $\varphi(C)$ can be written as the interleaved version of c_1 and $c_1 + c_2$, where $c_1 \in \bar{C}$ and $c_2 \in C_{1-v}$. So code $\varphi(C)$ can be obtained from the $\bar{C}$ and C_{1-v} through a $\langle \mathbf{u}, \mathbf{u+v}\rangle$ construction.

Theorem 3.3. *Let $C = \langle vg_1(x), (1-v)g_2(x)\rangle$ be a cyclic code of length n over R_p, where $g_2(x) \mid g_1(x) \mid x^n - 1$. Let $Z_2 = \{\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+t_1-1}\}$ be t_1 consecutive roots of the polynomial $g_2(x)$ and let $Z_1 = \{\alpha^j, \alpha^{j+1}, \ldots, \alpha^{j+t_1+t_2-1}\}$ be $t_1 + t_2$ consecutive roots of the polynomial $g_1(x)$, where $\alpha \in GF(p^n)$ is a primitive element. Then the following inequality does hold.*

$$d_L(C) \geq min\{2(t_1 + 1), t_1 + t_2 + 1\}.$$

Proof. *Since the code $\varphi(C)$ is equivalent to $\langle \boldsymbol{u}, \boldsymbol{u+v}\rangle$ constructed code from two codes $\bar{C}$ and C_{1-v}. We have*

$$d_L(C) = d_H(\varphi(C)) = min\{2d_H(\bar{C}), d_H(C_{1-v})\}.$$

But $\bar{C} = \langle g_2(x)$ and $C_{1-v} = \langle g_1(x)\rangle$, thus $d_L(C) \geq min\{2(t_1 + 1), t_1 + t_2 + 1\}$. □

Now let $w(x) = w_1(x) + vw_2(x) = c(x) + e(x)$ be a received word, where $e(x)$ is the error polynomial which has Lee weight $\nu \leq t$, where $t = \lfloor \frac{d_L(C)-1}{2} \rfloor$. Suppose that the errors occur in the unknown coordinates $k_1, k_2, \ldots, k_l$. So $e(x) = e_{k_1}x^{k_1} + e_{k_2}x^{k_2} + \cdots + e_{k_l}x^{k_l}$, where $e_{k_i} \in R_p$ for $i = 1, 2, \ldots, l$. The error-locator polynomial $\sigma(z)$ corresponding to error in position $k_1, k_2, \ldots, k_l$ is defined as:
$\sigma(z) = 1 + \sigma_1 z + \sigma_2 z^2 + \cdots + \sigma_l z^l = (1 - \alpha^{k_1}z)(1 - \alpha^{k_2}z)\cdots(1 - \alpha^{k-l}z)$. Note that in contrast the binary case the degree of polynomial $\sigma(z)$ need not to be equal to the Lee weight of error. But the degree of polynomial $\sigma(z)$ depend on the type of error. By using of the vector representation of R_p over F_p, $e(x)$ can be written as follows:

$$e(x) = (e_{k_{1,0}} + ve_{k_{1,1}})x^{k_1} + \cdots + (e_{k_{l,0}} + ve_{k_{l,1}})x^{k_l} \tag{3.1}$$

where $e_{k_{i,j}} \in F_p$, for $i = 1, 2, \ldots, l; j = 0, 1$. In this case, apart from finding the component error locator polynomials we need to evaluate the component error magnitudes. *From equation* (3.1), we have $e(x) = e_1(x) + ve_2(x)$, where $e_1(x), e_2(x), \acute{e}(x)$ and $\acute{\acute{e}}(x)$ are defined as following:

$$e_1(x) = e_{k_{1,0}}x^{k_1} + e_{k_{2,0}}x^{k_2} + \cdots + e_{k_{l,0}}x^{k_l} \tag{3.2}$$

$$e_2(x) = e_{k_{1,1}}x^{k_1} + e_{k_{2,1}}x^{k_2} + \cdots + e_{k_{t,1}}x^{k_l} \tag{3.3}$$

$$\acute{e}(x) = (e_{k_{1,0}} + e_{k_{1,1}})x^{k_1} + (e_{k_{2,0}} + e_{k_{2,1}})x^{k_2} + \cdots + (e_{k_{t,0}} + e_{k_{t,1}})x^{k_l} \tag{3.4}$$

$$\acute{e}(x) = (2e_{k_{1,0}} + e_{k_{1,1}})x^{k_1} + \cdots + (2e_{k_{t,0}} + e_{k_{t,1}})x^{k_l} \tag{3.5}$$

The following two Theorems are essential for decoding procedure. The proof of this Theorem is based on the property of Gray map φ and triangle inequality for Hamming distance.

Theorem 3.4. *Let $e(x) = e_1(x) + ve_2(x)$ be an error polynomial. Let $w_L(e(x)) \leq t$, then we have*
(i) $w_H(\acute{e}(x)) \leq t$.
(ii) *Either* $w_H(e_2(x)) \leq \lfloor t/2 \rfloor$ *or* $w_H(\hat{e}(x)) \leq \lfloor t/2 \rfloor$. □

With assumption of Theorem 3.3 if $c(x) = c_1(x) + vc_2(x) \in C$, then $c_1(\alpha^h) = 0$, for $h = i, i+1, \ldots, i+t_1-1$ and $(c_1+c_2)(\alpha^r) = 0$, for $r = j, j+1, \ldots, j+t_1+t_2-1$. Then $w(\alpha^h) = e(\alpha^h)$, for $h = i, i+1, \ldots, i+t_1-1$. So

$$w_1(\alpha^h) = e_1(\alpha^h), w_2(\alpha^h) = e_2(\alpha^h)$$

also

$$(w_1 + w_2)(\alpha^r) = \acute{e}(\alpha^r), r = j, j+1, \ldots, j+t_1+t_2-1.$$

Now let $\acute{w}(x) = w_1(x) + w_2(x)$ and $\acute{S}_r = \acute{w}(\alpha^r), r = j, j+1, \ldots, j+t_1+t_2-1$. Also let

$$\hat{w}(x) = 2w_1(x) + w_2(x), \hat{S}_h = \hat{w}(\alpha^h) = \hat{e}(\alpha^h), h = i, i+1, \ldots, i+t_1-1$$

The decoding algorithm organized in four steps.

(i) **Calculating syndromes from the received vector:**
Compute $t_1 + t_2$ syndromes of $\acute{S} = \{\acute{S}_r : j \leq r \leq j+t_1+t_2-1\}$, t_1 syndromes of $S_2 = \{S_{2,h} : i \leq h \leq i+t_1-1\}$ and t_1 syndromes of $\hat{S} = \{\hat{S}_h : i \leq h \leq i+t_1-1\}$ by using of the following equations:

$$\acute{S}_r = \acute{w}(\alpha^r) = \acute{e}(\alpha^r), j \leq r \leq j+t_1+t_2-1. \tag{3.6}$$

$$S_{2,h} = w_2(\alpha^h) = e_2(\alpha^h), i \leq h \leq i+t_1-1. \tag{3.7}$$

$$\hat{S}_h = \hat{w}(\alpha^h) = \hat{e}(\alpha^h), i \leq h \leq i+t_1-1. \tag{3.8}$$

(ii) **Computation of error locator polynomials:**
Let $\acute{S}(z) = \sum_{r=j}^{j+t_1+t_2-1} \acute{S}_r z^r$. Let $\acute{\sigma}(z)$ be the error locator polynomial corresponding to $\acute{e}$. Similar to the procedure of Sugiama (see [5], Section 5.4) for decoding of cyclic codes over finite fields there exists a polynomial $\acute{\omega}(z)$ such that

$$\acute{S}(z)\acute{\sigma}(z) \equiv \acute{\omega}(z) \,(mod\, z^{t_1+t_2}),\ deg(\acute{\omega}(z)) < deg(\acute{\sigma}(z)). \tag{3.9}$$

So the error locator polynomial $\acute{\sigma}(z)$ can be obtained by solving above equation over $GF(p^n)$. Let $S_2(z) = \sum_{h=i}^{i+t_1-1} S_{2,h} z^h$, there is a polynomial $\omega_2(z)$ such that

$$S_2(z)\sigma_2(z) \equiv \omega_2(z)(\,mod\, z^{t_1}),\ deg(\omega_2(z)) < deg(\sigma_2(z)). \tag{3.10}$$

Also let $\hat{S}(z) = \sum_{h=i}^{i+t_1-1} \hat{S}_h z^h$, thus there exists a polynomial $\hat{\omega}(z)$ such that

$$\hat{S}(z)\hat{\sigma}(z) \equiv \hat{\omega}(z)(mod\, z^{t_1}),\ deg(\hat{\omega}(z)) < deg(\hat{\sigma}(z)), \tag{3.11}$$

where $\sigma_2(z)$ is the error locator polynomial corresponding to e_2 and $\hat{\sigma}(z)$ is the error locator polynomial corresponding to $\hat{e}$. The error locator polynomials $\sigma_2(z)$ and $\hat{\sigma}(z)$ can be obtained by solving above key equation over $GF(p^n)$ and help of Matlab software.

(iii) **Computation of error locations and the error magnitudes:**

Let $\acute{P}$ be the inverse of the roots of $\acute{\sigma}(z)$. As in the case of decoding of cyclic codes over finite fields let $\acute{E}$ be the set of error magnitudes corresponding to $\acute{e}$. Similarly P_2, $\hat{P}$, E_2 and $\hat{E}$ can be defined. Then, according to the determination of error locations we can obtain the error magnitudes.

(iv) **Computation of error polynomial:**

By using of *Theorem* 3.4, either the error polynomial $e_2(x)$ and or $\hat{e}(x)$ can be decoded in the code $\bar{C}$ and $\acute{e}$ can be decoded in the code C_{1-v}. Since at least any two of $e_2(x), \hat{e}(x)$, and $\acute{e}(x)$ will be determined, we can decode the error polynomial $e(x)$ by using of equation $e_2(x) = 2\acute{e}(x) - \hat{e}(x)$.

Theorem 3.5. *It is possible to completely decode an error* $e(x)$ *if* $w_L(e(x)) \leq t$, *where*

$$t = \begin{cases} \lfloor \frac{2t_1+1}{2} \rfloor & t_1 < t_2 \\ \lfloor \frac{t_1+t_2}{2} \rfloor & t_1 \geq t_2 \end{cases}$$

Proof. *If* $t_1 < t_2$, *then Theorem* 3.3 *implies that* $d_L(C) \geq 2(t_1 + 1)$. *Recall that the degree of syndrome polynomial* $\acute{S}(z)$ *is* $t_1 + t_2$ *and* $\acute{S}(z)$ *is a polynomial over field* F_p, *so the solution of* (3.9) *is guaranteed only if the degree of error locator polynomials* $\acute{\sigma}(z)$ *is less than or equal to* $\lfloor \frac{t_1+t_2}{2} \rfloor$. *Now from Theorem* 3.4, *we have*

$$w_H(\acute{e}(x)) \leq \lfloor \frac{2t_1+1}{2} \rfloor \leq \lfloor \frac{t_1+t_2}{2} \rfloor.$$

Thus $\acute{e}(x)$ *can be decoded in code* C_{1-v}, *which is a code over* F_p *with Hamming distance more than or equal to* $t_1 + t_2 + 1$. *Similarly the degree of syndrome polynomial* $S_2(z)$ *is* t_1, *so the solution of* (3.10) *is guaranteed only if the degree of error locator polynomials* $\sigma_2(z)$ *is less than or equal to* $\lfloor \frac{t_1}{2} \rfloor$. *From Theorem* 3.4, *we have* $w_H(e_2(x)) \leq \lfloor \frac{\lfloor \frac{2t_1+1}{2} \rfloor}{2} \rfloor \leq \lfloor \frac{t_1}{2} \rfloor$ *or* $w_H(\hat{e}(x)) \leq \lfloor \frac{t_1}{2} \rfloor$. *Hence* $e_2(x)$ *or* $\hat{e}(x)$ *can be decoded in code* $\bar{C}$, *which is a code over* F_p *with Hamming distance more than or equal to* $t_1 + 1$. *If* $t_1 \geq t_2$, *similar calculations show that it is possible to find error polynomial* $e(x)$. $\square$

Example 1: Let $C = \langle vg_1(x), (1-v)g_2(x) \rangle$ be a cyclic code of length 13 over the ring R_3 and α be a primitive element of order 13 in $GF(3^3) = \frac{F_3(x)}{\langle x^3+x^2+2 \rangle}$. Let $g_2 = f_1 f_2$ and $g_1 = f_1 f_2 f_4$, where $f_0(x) = x+2$, $f_1(x) = x^3+x^2+2$, $f_2(x) = x^3+2x^2+2x+2$, $f_4(x) = x^3+2x+2$ and $f_7(x) = x^3 + x^2 + x + 2$. The sets of consecutive roots of polynomials $g_2(x)$ and $g_1(x)$ are given as follows:
$Z_2 = \{\alpha, \alpha^2, \alpha^3\}$ and $Z_1 = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$.
Since $t_1 = 3$ and $t_1 + t_2 = 6$, Theorem 3.3 implies that the minimum Lee distance of the code is more than or equal to 7. In the following Table the decoding procedure is described. Note that $\acute{w}(x), \hat{w}(x)$ can be decoded in codes C_{1-v} and $\bar{C}$, respectively by using of Peterson-Gorenstein-Zierler algorithm (see,[5], Section 5.4.1).

Table 2

$w(x)$	$2x + 2vx^2$
$\hat{S}$	$\{2\alpha^7, 2\alpha, 2\alpha^8\}$
$\hat{\sigma}(x)$	$\alpha^5 x^3 + \alpha^7 x + 1$
$\acute{\sigma}(x)$	$\alpha^3 x + 1$
$\acute{P}$	$\{\alpha^{-7}\}$
$\acute{E}$	$\{2\}$
$\acute{e}(x)$	$2x^7$
$\acute{e}(x)$	$x^7 + 2x^2 + 2$
$e_2(x)$	$2x^2 + 2$

$\square$

4 Decoding of cyclic codes over principal ideal rings

In this section a decoding method for cyclic codes over a finite principal ideal ring with assumption that decoding of cyclic codes over its components is available is given. Let R be a finite principal ideal ring, from Theorem 1, $R \simeq R_1 \times R_2 \ldots \times R_t \simeq e_1R_1 \oplus e_2R_2 \oplus \ldots \oplus e_tR_t$, where each R_i is a chain ring. Let S be a finite chain ring with unique maximal ideal $m = \langle a \rangle$, where a is a nilpotent element with nilpotency index t. and k be the residue field $\frac{S}{m}$. Since every finite field has prime power order, then $|k| = p^l$ for some prime number p and a integer $l \geq 1$ and $|R| = p^{lt}$. Also n is a positive integer which is not divisible by p, then $x^n - 1$ factors uniquely into pairwise coprime monic irreducible polynomials in $S[x]$.

We assume that finite ring R is isomorphic to a finite product of local rings,i.e, $R \simeq R_1 \times R_2 \times \ldots \times R_t$, where each R_i is a local ring. Let n be a positive integer, the map $\psi : R^n \to {R_1}^n \times {R_2}^n \times \cdots \times {R_t}^n$ is defined as:

$$\psi(r_0, r_1, \ldots, r_{n-1}) = (s_1, s_2, \ldots, s_t),$$

where $r_j = (a_{j1}, a_{j2}, \ldots, a_{jt})$ for $j = 0, 1, \ldots, n-1$. Also $s_1 = (a_{01}, a_{11}, \ldots, a_{n-1,1}) \in {R_1}^n, s_2 = (a_{02}, a_{12}, \ldots, a_{n-1,2}) \in {R_2}^n, \ldots, s_t = (a_{0t}, a_{1t}, \ldots, a_{n-1,t}) \in {R_t}^n$. Clearly ψ is an isomorphism of abelian groups. Let C be a linear code of length n over R, then

$$\psi(C) = C_1 \times C_2 \times \cdots \times C_t,$$

where C_i is a linear code of length n over R_i for $i = 1, 2, \ldots t$. Let $c \in C$ be transmitted through a noisy channel and $w = c + e = (w_0, w_1, \ldots, w_{n-1}) \in R^n$ be a received word, then c_j can be written as $c_j = \sum_{i=1}^{t} e_i a_{ji}$ for $j = 0, 1, \ldots, n-1$. So

$$c(x) = \sum_{i=1}^{t} e_i a_{0i} + (\sum_{i=1}^{t} e_i a_{1i})x + \cdots + (\sum_{i=1}^{t} e_i a_{n-1,i})x^{n-1}$$

$$= e_1(\sum_{j=0}^{n-1} a_{j1}x^j) + e_2(\sum_{j=0}^{n-1} a_{j2}x^j) + \cdots + e_t(\sum_{j=0}^{n-1} a_{jt}x^j).$$

Let $\acute{c_i} = \sum_{j=0}^{n-1} a_{ji}x^j$ for $i = 1, 2, \ldots, t$. So $c(x) = (\acute{c_1}, \acute{c_2}, \ldots, \acute{c_t})$, then by linearity of each C_i, we have $\acute{c_i} \in C_i$. Let $w = (w_0, w_1, \ldots, w_{n-1})$, where $w_j = (b_{j1}, b_{j2}, \ldots, b_{jt})$ for $j = 0, 1, \ldots, n-1$. So

$$\psi(w) = (b_{01}, b_{11}, \ldots, b_{n-1,1}, b_{02}, b_{12}, \ldots, b_{n-1,2}, \ldots, b_{0t}, b_{1t}, \ldots, b_{n-1,t}).$$

Therefore $\psi(w) = (\acute{w_1}, \acute{w_2}, \ldots, \acute{w_t})$, where $\acute{w_1} = (b_{01}, b_{11}, \ldots, b_{n-1,1}) \in {R_1}^n$, $\acute{w_2} = (b_{02}, b_{12}, \ldots, b_{n-1,2}) \in {R_2}^n, \ldots, \acute{w_t} = (b_{0t}, b_{1t}, \ldots, b_{n-1,t}) \in {R_t}^n$. Similarly $\psi(e) = (\acute{e_1}, \acute{e_2}, \ldots, \acute{e_t})$. So $\acute{w_i} - \acute{e_i} = \acute{c_i} \in C_i$. Then $\acute{w_i}$ will be decoded in the code C_i.

Theorem 4.1. *Let $R \simeq e_1R_1 \oplus e_2R_2 \oplus \ldots \oplus e_tR_t$ is a principal ideal ring, where R_i a chain ring for $i = 1, 2, \ldots, t$. Let C_i be a linear code over R_i and $C = CRT(C_1, C_2, \ldots, C_t)$, then C is a cyclic code over R if and only if C_i is a cyclic code over R_i.*
Proof. *Clrarly $C \simeq e_1C_1 \oplus e_2C_2 \oplus \cdots \oplus e_tC_t$. For $i = 1, 2, \ldots, t$, let C_i be a cyclic code of length n over R_i and $c = (c_0, c_1, \ldots, c_{n-1}) \in C$. For $k = 0, 1, 2, \ldots, n-1$, $c_k = e_1c_{1,k} + e_2c_{2,k} + \cdots + e_tc_{t,k}$. Since $(c_{i,n-1}, c_{i,0}, \ldots, c_{i,n-2}) \in C_i$ for $i = 0, 1, 2, \ldots, n-1$, then $e_1(c_{1,n-1}, c_{1,0}, \ldots, c_{1,n-2}) + \cdots + e_t(c_{t,n-1}, c_{t,0}, \ldots, c_{t,n-2}) \in e_1R_1 \oplus e_2R_2 \oplus \cdots \oplus e_tR_t$. Therefore $(e_1c_{1,n-1} + e_2c_{2,n-1} + \ldots + e_tc_{t,n-1}, e_1c_{1,0} + e_2c_{2,0} + ... + e_tc_{t,0}, \ldots, e_1c_{1,n-2} + e_2c_{2,n-2} + \cdots + e_tc_{t,n-2}) \in C$. So $\sigma(c_0, c_1, \ldots, c_{n-1}) \in C$, this implies that C is a cyclic code. The proof of converse is obvious.* □

Theorem 4.2. ([1], *Theorem* 3.6) *Let R be a finite chain ring and n be an integer which is not divisible by the characteristic of the residue field $\frac{R}{m}$. Then $\frac{R[x]}{\langle x^n - 1 \rangle}$ is a principal ideal ring.* □

Theorem 4.3. *Let $R \simeq e_1R_1 \oplus e_2R_2 \oplus \ldots \oplus e_tR_t$ be a principal ideal ring, where R_i is a chain ring with maximal ideal m_i, for $i = 1,2,\ldots,t$. Suppose C_i is a linear code of length n over R_i and n is not divisible by the characteristic of the residue field $\frac{R_i}{m_i}$, for $i = 1,2,\ldots,t$, then $CRT(C_1,C_2,\ldots,C_t) = \langle e_1f_1(x), e_2f_2(x),\ldots,e_tf_t(x)\rangle$, where $C_i = \langle f_i(x)\rangle$.*

Proof. *Let $e_1c_1(x)+e_2c_2(x)+\cdots+e_tc_t(x)$, where $c_i(x) \in C_i = \langle f_i(x)\rangle$ for $i = 1,2,\ldots,t$. So $c_i(x) = f_i(x)h_i(x)$ for some $h_i(x) \in R[x]$. Therefore $c(x) = e_1f_1(x)h_1(x)+e_2f_2(x)h_2(x)+\cdots+e_tf_t(x)h_t(x)$ this implies that $c(x) \in \langle e_1f_1(x), e_2f_2(x),\ldots,e_tf_t(x)\rangle$. Conversely let $c(x) \in \langle e_1f_1(x), e_2f_2(x),\ldots,e_tf_t(x)\rangle$, then $c(x) = e_1f_1(x)r_1(x)+e_2f_2(x)r_2(x)+\cdots+e_tf_t(x)r_t(x)$, where $r_i \in R[x]$ for $i = 1,2,\ldots,t$. As there is $s_i(x) \in R_i(x)$, such that $e_is_i(x) = e_ir_i(x)$, then $s_i(x)f_i(x) \in C_i$. Therefore $c(x) = e_1f_1(x)s_1(x)+e_2f_2(x)s_2(x)+\cdots+e_tf_t(x)s_t(x) \in e_1C_1 \oplus e_2C_2 \oplus \ldots \oplus e_tC_t$.* $\square$

Corollary 4.4. *In the last theorem $C = \langle e_1f_1(x)+e_2f_2(x)+\ldots+e_tf_t(x)\rangle$.*

Theorem 4.5. ([2], *Lemma* 2.5) *For $i = 1,2,\ldots,s$, let C_i be a code of length n, over R_i. Then $d_H(CRT(C_1,\ldots,C_s)) = min\{d_H(C_i)\}$.* $\square$

With the above notation, we have the following theorem.

Theorem 4.6. *Let $C = CRT(C_1,C_2,\ldots,C_t)$ be a cyclic code of length n over the principal ideal ring R and $w(x) = e_1w_1(x)+e_2w_2(x)+\cdots+e_tw_t(x)$ be a received word with an error $e(x)$. If $w_H(e(x)) \le \lfloor (d_H(C)-1)/2 \rfloor$, then $w_i(x)$ can be decoded in code C_i for $i = 1,2,\ldots,t$.* $\square$

Let β be a 11-th root of unity in Galois field $GF(3^5)$. The Golay code G_{11} is a cyclic code with generator $f_1(x) = \Pi_{i\in Q}(x-\beta^i)$,where $Q = \{j^2(mod\ 11) : j = 1,2,\ldots,10\}$. The Golay code G_{11} is a $[11,6,5]$ code. So it is a perfect two correcting code. Let $c \in C$ and $w(x) = c(x)+e(x)$ be a received word with an error $e(x)$, the syndromes S_i of the received word $w(x)$ is defined as $S_i = w(\beta^i) = e(\beta^i)$ for $i \in Q$.

Theorem 4.7. ([4],*proposition* 1) *Let C be the Golay code G_{11}, then*
a) A received word has no error if and only if $S_1 = 0$.
b) A received word has one error if and only if $S_1^{22} = 1$.
c) If $S_1^{22} = 1$, then the error in the received word has value S_1^{11} and location i, with $0 \le i \le 10$, where $\beta^i = S_1^{12}$. $\square$

Example 2: Suppose $C = CRT(G_{11},C_2)$ is cyclic code of length 11 overZ_6, where $C_2 = \langle f_1(x)\rangle$, $f_1(x) = \frac{x^{11}-1}{x-1}$, so $d_H(C) = 5$.
Let $w = (00,00,00,00,10,00,00,00,00,00,01)$ be received word, then $\acute{w}_1, \acute{w}_2$ will be decoded in ternary Golay code G_{11} and binary code C_2, respectively. By using of Table 1 in [4], $S_1 = \acute{w}_1(\beta) = \alpha^{88} \neq 0$. Also using of algorithm 1 in [4] implies that the error is $\sigma_{11,1}(z) = 1-{S_1}^{12}z = 1-(\alpha^{88})^{12}z = 1-\alpha^{88}z$. By the Chien search this polynomial has one root, therefore the received codeword has value ${S_1}^{11} = (\alpha^{88})^{11} = 1$, and location i with $0 \le i \le 10$, where $\alpha^i = {S_1}^{12}$. Then $\alpha^i = \alpha^{88} = \beta^4$, so $\acute{e}_1(x) = x^4$. It is easy to see that $\acute{e}_2(x) = x^{10}$. So $\acute{e} = (00,00,00,00,10,00,00,00,00,00,01)$. $\square$

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

References

[1] H. Q. Dinh, S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory.*, **50** , 1728-1744 (2004).

[2] S.T. Dougherty, J. L. Kim, H. Kulosman, MDS codes over finite principal ideal rings,*Des. Codes Crypt.*, **50** ,77-92 (2009).

[3] K. Guenda, T. A. Gulliver, MDS and self-dual codes over rings, *Finite Fields Appl.*, **18** , 1061-1075 (2012).

[4] R. J. Higgs, J. F. Humphreys, Decoding the ternary Golay code,*IEEE Trans. Inform. Theory.*,**39** , 1043-1046 (1993).

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

[6] A. Kaya, B. Yildiz and I. Siap, Quadratic residue codes over $F_p + vFp$ and their Gray images, *J. Pure Appl. Algebra.*, **218** , 1999-2011 (2014).

[7] S. Zhu, L. Wang, A class of constacyclic codes over $F_p + vF_p$ and its Gray image, *Discrete Mathematics.*, **311**, 2677-2682 (2011).

Author information

Mohammad Reza Alimoradi, Department of Mathematics, University of Malayer, Malayer, Iran.
E-mail: malimoradisharif@yahoo.com

Received: 2022-04-18
Accepted: 2022-08-28