Linear Codes over Finite Chain Rings

Hongwei Liu[1,2*]
[1]Department of Mathematics
Huazhong Normal University
Wuhan, Hubei 430079, CHINA
[2]Hubei Key Laboratory of Applied Mathematics
Hubei University
Wuhan, Hubei 430062, CHINA
Email: h_w_liu@yahoo.com.cn

October 9, 2009

Abstract

In this paper, we study linear codes over finite chain rings. We relate linear cyclic codes, $(1+\gamma^k)$-cyclic codes and $(1-\gamma^k)$-cyclic codes over a finite chain ring R, where γ is a fixed generator of the unique maximal ideal of the finite chain ring R, and the nilpotency index of γ is $k+1$. We also characterize the structure of $(1+\gamma^k)$-cyclic codes and $(1-\gamma^k)$-cyclic codes over finite chain rings.

*The author would like to sincerely thank the University of Scranton where he stayed while this work was completed. He is supported by the National Natural Science Foundation of China (10871079).

1 Introduction

Codes over finite fields have been studied for more than fifty years. They were studied first over the binary field $\mathbb{F}_2 = \{0, 1\}$, then were extended to an arbitrary q-ary finite field $\mathbb{F}_q$. A linear cyclic code of length n over a finite field $\mathbb{F}_q$ can be viewed as an ideal of the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. The structure of a cyclic code and its dual code is well known. In [7], Hammons et al. showed that there exists an interesting connection between nonlinear binary codes and linear codes over $\mathbb{Z}_4$. Moreover, it is proved in [7] that some non-linear codes of length n, such as the Kerdock, Preparata, and Goethals codes can be viewed as linear codes over $\mathbb{Z}_4$ via the Gray map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. Following this, many papers on linear codes over finite rings appeared in recent years.

In [16], Wolfmann studied linear negacyclic and cyclic codes over $\mathbb{Z}_4$, and showed that the Gray map image of a linear negacyclic code over $\mathbb{Z}_4$ of length n is distance-invariant. Later in [14], some of results in [16] were generalized to codes over $\mathbb{Z}_{2^k}$. Wolfmann also determined in a later paper [17] which linear cyclic codes over $\mathbb{Z}_4$ of odd length have Gray images that are linear binary codes. In [6], Greferath and Schmidt generalized the Gray map to finite chain rings, and produced an example of a $(36, 3^{12}, 15)$ code as the image of a 9-ary lift of the ternary Golay code. Ling and Blackford (see [9]) generalized most of the results in [16],[14] and [17] to the ring $\mathbb{Z}_{p^k+1}$. In [9], the Gray map over $\mathbb{Z}_{p^k+1}$ was introduced, and it is also shown that the Gray map over $\mathbb{Z}_{p^k+1}$ is permutation equivalent to the map given by Greferath and Schmidt in [6]. Meanwhile, researchers are also interested in the structural properties of codes over large families of finite rings, and many papers on the structure of cyclic codes and constacyclic codes over finite rings have appeared in this field.

In this paper, we shall study linear codes over finite chain rings. We generalize some results in [9] to finite chain rings. We relate the structure of cyclic codes and constacyclic codes over finite chain rings. We begin with some definitions.

Throughout this paper, the rings we shall study are finite commutative rings with identity $1 \neq 0$. Let R be a finite ring. Let R^n be the R-module of n-tuples over R. The *Hamming weight* $w(\mathbf{x})$ of the vector $\mathbf{x} = (x_1, \cdots, x_n) \in R^n$ is defined as the cardinality of the set of coordinates of $\mathbf{x}$ that are nonzero. An R-submodule C of R^n is called a *linear code* of

length n over R. We assume throughout that all codes are linear.

If $\mathbf{x}, \mathbf{y} \in R^n$, the *inner product* of $\mathbf{x}, \mathbf{y}$ is defined as follows:

$$[\mathbf{x}, \mathbf{y}] = x_1 y_1 + \cdots + x_n y_n.$$

Two vectors $\mathbf{x}, \mathbf{y} \in R^n$ are called *orthogonal* if $[\mathbf{x}, \mathbf{y}] = 0$. For a code C of length n over R, its *dual code* $C^\perp$ is defined as the set of vectors over R that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{\mathbf{x} \in R^n \mid [\mathbf{x}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}.$$

If S is an arbitrary set, we denote the cardinality of set S by $|S|$. In [18], it is proved that for any linear code C over a finite Frobenius ring,

$$|C| \cdot |C^\perp| = |R|^n. \tag{1}$$

Since a finite chain ring is a special Frobenius ring, the identity above also holds for codes over finite chain rings.

If $C \subseteq C^\perp$, then C is called *self-orthogonal*. Moreover, if $C = C^\perp$, then C is called *self-dual*.

2 Notations and Cyclic Codes over Finite Chain Rings

In this section, we shall give some notations and basic properties of finite chain rings, then we will give some basic concepts of cyclic codes over this class of rings.

An ideal I of a ring R is called *principal* if it generated by one element. A finite ring R is called a *chain ring* if all its ideals are linearly ordered by inclusion. By the definition, we can obtain that all the ideals of the finite chain ring R are principal, since if there exists an ideal I of R such that I is not principal, then we can suppose the ideal I generated by at least two elements. Since R is finite, we can assume $I = \langle a_1, a_2, \cdots, a_s \rangle$, and this implies that $\langle a_1 \rangle \nsubseteq \langle a_2 \rangle$ and $\langle a_2 \rangle \nsubseteq \langle a_1 \rangle$, this contradicts the definition of finite chain rings. This means that R has a unique maximal ideal.

Let R be a finite chain ring, $\mathfrak{m}$ the unique maximal ideal of R, and let γ be the generator of the unique maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = \langle \gamma \rangle = R\gamma$, where $R\gamma = \langle \gamma \rangle = \{\beta\gamma \mid \beta \in R\}$. We know that there exist numbers i such

that $\langle\gamma^i\rangle = \{0\}$, since R is finite. Let e be the minimal number such that $\langle\gamma^e\rangle = \{0\}$. The number e is called the *nilpotency index* of γ.

Let $R^\times$ be the multiplicative group of all units in R. Let $\mathbb{F} = R/\mathfrak{m} = R/\langle\gamma\rangle$ be the residue field of the ring R with characteristic p, where p is a prime number, then $|\mathbb{F}| = q = p^r$ for some integers q and r. Let $\mathbb{F}^\times$ denote the multiplicative group of the residue field $\mathbb{F}$, we know that $|\mathbb{F}^\times| = p^r - 1$. The following two lemmas are well-known (see [11],[12], for example).

Lemma 2.1. *Assume the notations given above. For any $0 \neq r \in R$ there is a unique integer i, $0 \leq i < e$ such that $r = \mu\gamma^i$, with μ a unit in R. The unit μ is unique modulo γ^{e-i} only.*

Lemma 2.2. *Let R be a finite chain ring with maximal ideal $\mathfrak{m} = \langle\gamma\rangle$, where γ is a generator of $\mathfrak{m}$ with nilpotency index e. Let $V \subseteq R$ be a set of representatives for the equivalence classes of R under congruence modulo $\langle\gamma\rangle$. Then*

(i) for all $r \in R$ there exist unique $r_0, \cdots, r_{e-1} \in V$ such that $r = \sum_{i=0}^{e-1} r_i\gamma^i$;

(ii) $|V| = |\mathbb{F}|$;

(iii) $|\langle\gamma^j\rangle| = |\mathbb{F}|^{e-j}$ for $0 \leq j \leq e-1$.

Example 1. Let $R = \mathbb{Z}_4[u]/\langle u^2 - 2\rangle$, then it is easy to check that R is a chain ring but not a Galois ring. The maximal ideal of R is $\mathfrak{m} = \langle u\rangle$ and the nilpotency index of the generator $\gamma = u$ is 4, since $\gamma^2 = 2, \gamma^3 = 2u$ and $\gamma^4 = 0$. The residue field $\mathbb{F}$ of R is $\mathbb{Z}_2$.

Let R be a finite chain ring, let

$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, n \geq 0\}$$

be the polynomial ring over R. Let $0 \neq f(x) = a_0 + a_1x + \cdots + a_nx^n$. If $a_n \neq 0$ then n is called the *degree* of $f(x)$, and we denote the degree of f by $deg(f(x)) = n$. If $f(x)$ is the zero polynomial, we call its degree $-\infty$, and denote it by $deg(0) = -\infty$.

Let $\lambda \in R^\times$, and let

$$R[x]/\langle x^n - \lambda\rangle = \{f(x) + \langle x^n - \lambda\rangle \mid f(x) \in R[x]\}.$$

It is easy to see that each coset in this quotient ring can be represented by a unique polynomial $f(x)$ with $deg(f(x)) < n$. In the following, we

sometimes identify $f(x)+\langle x^n-\lambda\rangle$ with its unique representative polynomial $f(x)$, where $deg(f(x)) < n$. That is

$$R[x]/\langle x^n-\lambda\rangle = \{f(x)+\langle x^n-\lambda\rangle \mid \text{where } deg(f(x)) < n \text{ or } f(x)=0\}.$$

We define the map P_λ as follows:

$$\begin{aligned} P_\lambda : R^n &\to R[x]/\langle x^n-\lambda\rangle, \\ (a_0, a_1, \cdots, a_{n-1}) &\mapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n-\lambda\rangle. \end{aligned}$$

In particular, if we take $\lambda = 1$ then we obtain a special map P_1.

Let C be an arbitrary subset of R^n, we denote the image of C under the map P_λ by $P_\lambda(C)$. For convenience, we use $a(x) = a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ to denote the image of $(a_0, a_1, \cdots, a_{n-1})$ under the maps of both P_λ and P_1.

Let C be a linear code of length n over R and $\lambda \in R^\times$. The code C is called *a λ-cyclic (or constacyclic) code* over R if

$$(c_0, c_1, \cdots, c_{n-1}) \in C \Rightarrow (\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C.$$

Notice that if $\lambda = 1$ then C is a cyclic code.

By the notations given above, we know that

$$P_\lambda(C) = \{c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + \langle x^n-\lambda\rangle \mid (c_0, c_1, \cdots, c_{n-1}) \in C\}.$$

The following lemma can be easily obtained.

Lemma 2.3. *Assume the notations given above. A linear code C of length n over R is a λ-cyclic code if and only if $P_\lambda(C)$ is an ideal of $R[x]/\langle x^n-\lambda\rangle$.*

In particular, we have the following corollary.

Corollary 2.4. *Assume the notations given above. Then a linear code C of length n over R is a cyclic code if and only if $P_1(C)$ is an ideal of $R[x]/\langle x^n-1\rangle$.*

3 Gray Map and Codes over Finite Chain Rings

In the remainder of this paper, we let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, where the nilpotency index of γ is $k+1$. Let $\mathbb{F} = \mathbb{F}_q = R/\langle\gamma\rangle$ be the q-element residue field.

Let n be a positive integer, and let $\mathbf{x} = (x_1, \cdots, x_n), \mathbf{y} = (y_1, \cdots, y_n) \in \mathbb{F}^n$, the tensor product of vectors $\mathbf{x}$ and $\mathbf{y}$ is defined as usual, i.e.,

$$\mathbf{x} \otimes \mathbf{y} = (x_1\mathbf{y}, \cdots, x_n\mathbf{y}) = (x_1y_1, \cdots, x_1y_n, \cdots, x_ny_1, \cdots, x_ny_n),$$

and for $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_n \in \mathbb{F}^n$, the tensor product of these vectors is computed by expanding from right to left, i.e., the tensor product of $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_n$ is the following:

$$\mathbf{x}_1 \otimes \mathbf{x}_2 \otimes \cdots \otimes \mathbf{x}_n = \mathbf{x}_1 \otimes (\mathbf{x}_2 \otimes (\cdots (\mathbf{x}_{n-1} \otimes \mathbf{x}_n) \cdots)).$$

Let $\mathbf{u}, \mathbf{v} \in \mathbb{F}^q$ such that $\mathbf{u} = (\alpha_0, \alpha_1, \cdots, \alpha_{q-1})$ lists the elements of $\mathbb{F}$ with $\alpha_0 = 0$ and $\mathbf{v}$ is the all 1-vector. Let

$$\mathbf{c}_i = (\mathbf{v} + \delta_{i,0}(\mathbf{u} - \mathbf{v})) \otimes (\mathbf{v} + \delta_{i,1}(\mathbf{u} - \mathbf{v})) \otimes \cdots \otimes (\mathbf{v} + \delta_{i,k-1}(\mathbf{u} - \mathbf{v})),$$

where $i = 0, \cdots, k$ and $\delta_{i,j}$ denotes the Kronecker symbol. It is easily to check that the following vectors

$$\begin{aligned}
\mathbf{c}_0 &= \mathbf{u} \otimes \overbrace{\mathbf{v} \otimes \cdots \otimes \mathbf{v}}^{k-1}, \\
\mathbf{c}_1 &= \mathbf{v} \otimes \mathbf{u} \otimes \overbrace{\mathbf{v} \otimes \cdots \otimes \mathbf{v}}^{k-2}, \\
\cdots &= \cdots \\
\mathbf{c}_{k-1} &= \overbrace{\mathbf{v} \otimes \cdots \otimes \mathbf{v}}^{k-1} \otimes \mathbf{u}, \\
\mathbf{c}_k &= \overbrace{\mathbf{v} \otimes \mathbf{v} \otimes \cdots \otimes \mathbf{v}}^{k}
\end{aligned}$$

are linear independent over $\mathbb{F}$. If we identify $(\mathbb{F}^q)^{\otimes k}$ with $\mathbb{F}^{q^k}$, then these vectors above generate a $(k+1)$-dimensional subspace C of $\mathbb{F}^{q^k}$.

Recall that $\mathbf{u} = (\alpha_0, \alpha_1, \cdots, \alpha_{q-1})$ is the vector whose coordinates are the list of all elements of the field $\mathbb{F}$, we have that

$$\begin{aligned}
\mathbf{c}_0 &= (\overbrace{\alpha_0, \cdots, \alpha_0}^{q^{k-1}}, \overbrace{\alpha_1, \cdots, \alpha_1}^{q^{k-1}}, \cdots, \overbrace{\alpha_{q-1}, \cdots, \alpha_{q-1}}^{q^{k-1}}); \\
\mathbf{c}_1 &= (\overbrace{\alpha_0, \cdots, \alpha_0}^{q^{k-2}}, \cdots, \overbrace{\alpha_{q-1}, \cdots, \alpha_{q-1}}^{q^{k-2}}, \cdots, \overbrace{\alpha_0, \cdots, \alpha_0}^{q^{k-2}}, \cdots, \overbrace{\alpha_{q-1}, \cdots, \alpha_{q-1}}^{q^{k-2}}); \\
\cdots &= \cdots; \\
\mathbf{c}_{k-1} &= (\overbrace{\alpha_0, \alpha_1, \cdots, \alpha_{q-1}}^{q}, \overbrace{\alpha_0, \alpha_1, \cdots, \alpha_{q-1}}^{q}, \cdots, \overbrace{\alpha_0, \alpha_1, \cdots, \alpha_{q-1}}^{q}); \\
\mathbf{c}_k &= (\overbrace{1, 1, \cdots, 1}^{q}, \overbrace{1, 1, \cdots, 1}^{q}, \cdots, \overbrace{1, 1, \cdots, 1}^{q}).
\end{aligned}$$

It is easy to see that column vectors of the $k \times q^k$ matrix with $\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_{k-1}$ as its rows contain all the vectors of $\mathbb{F}^k$.

Example 2. Let $q = 3, k = 2$, then $\mathbf{u} = (0, 1, 2)$. We have that

$$\begin{aligned} \mathbf{c}_0 &= \mathbf{u} \otimes \mathbf{v} = (0,0,0,1,1,1,2,2,2), \\ \mathbf{c}_1 &= \mathbf{v} \otimes \mathbf{u} = (0,1,2,0,1,2,0,1,2), \\ \mathbf{c}_2 &= \mathbf{v} \otimes \mathbf{v} = (1,1,1,1,1,1,1,1,1). \end{aligned}$$

This gives that $C = \langle \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2 \rangle$ is a code of length 9 over $\mathbb{F}$.

Let G be a $k \times n$ matrix with $\text{rank}(G) = k$ over $\mathbb{F}$. If any two columns of G are linearly independent, then the code with generating matrix G is called a *projective code*. Moreover, if k is a fixed integer and $n = \frac{q^k-1}{q-1}$, then the code is called a *maximal projective code*. Two $k \times n$ matrices G, G' over $\mathbb{F}$ are *monomial equivalent* if there are a n by n permutation matrix P and a n by n invertible diagonal matrix D such that $G' = GPD$.

A linear code is called *equivweight* if all of its nonzero codewords have same Hamming weight. A linear code is called *quasi-constant* if it contains the all 1-vector and its scalar multiples and all the other nonzero codewords have the same Hamming weight.

Theorem 3.1. *Assume the notations given above, we have*

(i) The code C generated by $\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_k$ is a quasi-constant linear $[q^k, k+1, (q-1)q^{k-1}]$ code with Hamming weight enumerator

$$A(x) = (q-1)x^{q^k} + (q^k - 1)qx^{(q-1)q^{k-1}} + 1;$$

(ii) The generating matrix of C is monomial equivalent to the following matrix

$$G = \begin{pmatrix} G^{(1)} & G^{(2)} & \cdots & G^{(q-1)} & 0 \\ \mathbf{1} & \mathbf{1} & \cdots & \mathbf{1} & 1 \end{pmatrix},$$

where each $G^{(j)}$ is a generating matrix of a maximal projective code with parameters $[\frac{q^k-1}{q-1}, k, q^{k-1}]$.

Proof. (i) Note that the definition of quasi-constant code, and the result can be obtained directly from [6].

(ii) Let

$$G = \begin{pmatrix} \mathbf{c}_0 \\ \cdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \end{pmatrix} = \begin{pmatrix} G_1 & G_2 & \cdots & G_{q^k} \end{pmatrix},$$

where G_j is the jth column of the matrix G. Let

$$\tilde{G} = \begin{pmatrix} \mathbf{c}_0 \\ \cdots \\ \mathbf{c}_{k-2} \\ \mathbf{c}_{k-1} \end{pmatrix} = \begin{pmatrix} \tilde{G}_1 & \tilde{G}_2 & \cdots & \tilde{G}_{q^k} \end{pmatrix},$$

where $\tilde{G}_j \in \mathbb{F}^k$ is the jth column of the matrix $\tilde{G}$. For any nonzero vector $\mathbf{x} = (x_1, \cdots, x_k)^T \in \mathbb{F}^k$, where $(x_1, \cdots, x_k)^T$ denotes the transpose of $(x_1, \cdots, x_k)$, we note that the number of times that a multiple of $\mathbf{x} \in \mathbb{F}^k$ appears in the matrix $\tilde{G}$ is $q-1$, then the result follows directly by permuting the columns of the matrix G. □

It is well-known that there exists a natural surjection $\rho : R \to \mathbb{F}, r \mapsto r + \langle\gamma\rangle$. Let V be the set of representatives for the equivalence classes of R under congruence modulo γ such that $0 \in V$. For any $a \in R$, we know by Lemma 2.2 that a can be written uniquely as follows:

$$a = a_0 + a_1\gamma + \cdots + a_k\gamma^k,$$

where $a_i \in V$. Let $a^{(i)} = \rho(a_i), 0 \le i \le k$, let C be the subspace generated by $\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_k$. *The Gray map* in [6] is generalized to a map over the finite chain ring R as follows:

$$\phi : R \to C, \tag{2}$$

$$a \mapsto a^{(0)}\mathbf{c}_0 + a^{(1)}\mathbf{c}_1 + \cdots + a^{(k)}\mathbf{c}_k. \tag{3}$$

It is easy to see that ϕ is a bijection.

Remark 1. *We note that the definition of the Gray map ϕ is not dependent on the choice of V, since if we have $a_i, a_i' \in V$ such that $a_i \equiv a_i' \pmod{\gamma}$, then $a_i = a_i' + s\gamma$, where $s \in R$, hence $a^{(i)} = \rho(a_i) = \rho(a_i' + s\gamma) = \rho(a_i') = a^{(i')}$.*

We have the following Lemma.

Lemma 3.2. *Let $a, b \in R$, where $a = a_0 + a_1\gamma + \cdots + a_k\gamma^k$ and $b = b_0 + b_1\gamma + \cdots + b_k\gamma^k$. Then*

(i) $\phi(a\gamma^k) = a^{(0)}\mathbf{c}_k$, where $a^{(0)} = \rho(a_0)$;

(ii) $\phi(a \pm \gamma^k b) = \phi(a) \pm \phi(\gamma^k b)$;

(iii) $\phi((1 \pm \gamma^k)a) = \phi(a) \pm \phi(\gamma^k a)$.

Proof. (i) We note that in the ring $R, \gamma^{k+1} = 0$, so

$$a\gamma^k = a_0\gamma^k + a_1\gamma^{k+1} + \cdots + a_k\gamma^{2k} = a_0\gamma^k \in R.$$

Hence $\phi(a\gamma^k) = \phi(a_0\gamma^k) = a^{(0)}\mathbf{c}_k$.

(ii) Since $0 = \gamma^{k+1} \in R$, we have that

$$\begin{aligned} a \pm \gamma^k b &= (a_0 + a_1\gamma + \cdots + a_k\gamma^k) \pm (b_0 + b_1\gamma + \cdots + b_k\gamma^k)\gamma^k \\ &= a_0 + a_1\gamma + \cdots + (a_k \pm b_0)\gamma^k \in R. \end{aligned}$$

This implies that

$$\phi(a \pm \gamma^k b) = a^{(0)}\mathbf{c}_0 + a^{(1)}\mathbf{c}_1 + \cdots + (a^{(k)} \pm b^{(0)})\mathbf{c}_k = \phi(a) \pm \phi(\gamma^k b).$$

(iii) This statement can be obtained by taking $a = b$ in (ii). □

Let $\mathbf{x} = (x_1, \cdots, x_n) \in R^n$, we denote $\phi(\mathbf{x})$ as follows:

$$\phi(\mathbf{x}) = (\phi(x_1), \cdots, \phi(x_n)).$$

By Lemma 3.2, we have that

$$\phi(\mathbf{x} \pm \gamma^k\mathbf{y}) = \phi(\mathbf{x}) \pm \phi(\gamma^k\mathbf{y}).$$

In particular, if $\mathbf{x} = \mathbf{y}$, we have

$$\phi((1 \pm \gamma^k)\mathbf{x}) = \phi(\mathbf{x}) \pm \phi(\gamma^k\mathbf{x}).$$

For $1 \leq j \leq n$, we let

$$x_j = x_{j,0} + x_{j,1}\gamma + \cdots + x_{j,k}\gamma^k,$$

where $x_{j,l} \in V, 0 \leq l \leq k$, we let $\rho(x_{j,l}) = x_{j,l}^{(l)}$. This discussion above gives the following corollary.

Corollary 3.3. *Assume the notations given above. Let* $\mathbf{x}, \mathbf{y} \in R^n$, *then we have that*

(i) $\phi(\mathbf{x}\gamma^k) = (\phi(x_1\gamma^k), \cdots, \phi(x_n\gamma^k)) = (x_{1,0}^{(0)}\mathbf{c}_k, \cdots, x_{n,0}^{(0)}\mathbf{c}_k)$;

(ii) $\phi(\mathbf{x} \pm \gamma^k\mathbf{y}) = \phi(\mathbf{x}) \pm \phi(\gamma^k\mathbf{y})$;

(iii) $\phi((1 \pm \gamma^k)\mathbf{x}) = \phi(\mathbf{x}) \pm \phi(\gamma^k\mathbf{x})$.

Homogeneous weights have been introduced to finite rings by Constantinescu and Heise (see [1]). They can be thought of as a generalization of

the Hamming weight for finite rings. For a finite chain R, the *homogeneous weight* for an element $a \in R$ is defined as

$$w_{\text{hom}}(a) = \begin{cases} 0, & \text{if } a = 0; \\ q^k, & \text{if } 0 \neq a \in \langle \gamma^k \rangle; \\ (q-1)q^{k-1}, & \text{otherwise.} \end{cases} \tag{4}$$

If $\mathbf{x} = (x_1, \cdots, x_n) \in R^n$, the homogeneous weight of $\mathbf{x}$ is defined as follows:

$$w_{\text{hom}}(\mathbf{x}) = \sum_{i=1}^{n} w_{\text{hom}}(x_i).$$

If $\mathbf{x}, \mathbf{y} \in R^n$, the *homogeneous distance* of $\mathbf{x}, \mathbf{y}$ is

$$d_{\text{hom}}(\mathbf{x}, \mathbf{y}) = w_{\text{hom}}(\mathbf{x} - \mathbf{y}).$$

For convenience, we use d_H and w_H to denote the Hamming distance and Hamming weight respectively. We have the following theorem.

Theorem 3.4. *Assume the notations given above. The generalized Gray map ϕ is an isometry from (R^n, d_{hom}) to $(\mathbb{F}^{q^k n}, d_H)$.*

Proof. We know that for any two vectors $\mathbf{x}, \mathbf{y}$ of R^n, $d_{\text{hom}}(\mathbf{x}, \mathbf{y}) = w_{\text{hom}}(\mathbf{x} - \mathbf{y})$.

If $\mathbf{x} - \mathbf{y} = \mathbf{0}$ then

$$d_{\text{hom}}(\mathbf{x}, \mathbf{y}) = w_{\text{hom}}(\mathbf{0}) = 0 = d_H(\phi(\mathbf{x}), \phi(\mathbf{y})).$$

If $\mathbf{x} \neq \mathbf{y}$ and $\mathbf{x} - \mathbf{y} = \gamma^k \mathbf{c}$, where $\mathbf{c} = (c_1, \cdots, c_n)$, let

$$m = |\{0 \neq c_j \in R^\times \mid 1 \leq j \leq n\}|,$$

where $R^\times$ is the multiplicative group of all units in R, then by Equation (4), we get

$$d_{\text{hom}}(\mathbf{x}, \mathbf{y}) = w_{\text{hom}}(\mathbf{x} - \mathbf{y}) = q^k m.$$

Since $\mathbf{x} - \mathbf{y} = \gamma^k \mathbf{c}$, by (ii) in Corollary 3.3, we have that

$$\phi(\mathbf{y}) = \phi(\mathbf{x} - \gamma^k \mathbf{c}) = \phi(\mathbf{x}) - \phi(\gamma^k \mathbf{c}).$$

Hence by (i) in Corollary 3.3, we have

$$w_H(\phi(\mathbf{x}) - \phi(\mathbf{y})) = w_H(\phi(\gamma^k \mathbf{c})) = q^k m.$$

This gives that

$$d_{\text{hom}}(\mathbf{x},\mathbf{y}) = d_H(\phi(\mathbf{x}),\phi(\mathbf{y})).$$

Otherwise, let $\mathbf{x}-\mathbf{y} = (c_1, c_2, \cdots, c_n)$ and let

$$m_1 = |\{0 \neq c_j = \gamma^k d_j \,|\, 1 \leq j \leq n\}|, \;\; m_2 = |\{c_j = 0 \,|\, 1 \leq j \leq n\}|.$$

This gives that there are $n - m_1 - m_2$ nonzero coordinates of $\mathbf{x}-\mathbf{y}$ such that they are in $R\backslash\langle\gamma^k\rangle$, i.e., $\mathbf{x}-\mathbf{y} \in R$, but $\mathbf{x}-\mathbf{y} \notin \langle\gamma^k\rangle$. Hence

$$d_{\text{hom}}(\mathbf{x},\mathbf{y}) = w_{\text{hom}}(\mathbf{x}-\mathbf{y}) = (n-m_1-m_2)(q-1)q^{k-1} + m_1 q^k.$$

On the other hand, if $0 \neq c_j = c_{j,0} + c_{j,1}\gamma + \cdots + c_{j,k}\gamma^k$ then

$$\phi(c_j) = c_{j,k}^{(k)}\mathbf{c}_k \Leftrightarrow c_{j,l} = 0, \forall\, 0 \leq l \leq k-1 \Leftrightarrow c_j = c_{j,k}\gamma^k$$

since ϕ is a bijection. This implies that if $0 \neq c_j \notin \langle\gamma^k\rangle$ then $\phi(c_j) \neq c_{j,k}^{(k)}\mathbf{c}_k$. By (i) in Theorem 3.1, we know that all nonzero codewords in C except $\mathbf{c}_k$ have Hamming weight $(q-1)q^{k-1}$. This gives that for these $0 \neq c_j \notin \langle\gamma^k\rangle$, we have

$$w_H(\phi(c_j)) = (q-1)q^{k-1},$$

and

$$w_H(\phi(c_{j,k}\gamma^k)) = w_H(c_{j,k}^{(k)}\mathbf{c}_k) = q^k.$$

Therefore

$$w_H(\phi(\mathbf{x}) - \phi(\mathbf{y})) = (n-m_1-m_2)(q-1)q^{k-1} + m_1 q^k.$$

Hence the result holds. □

4 λ-Cyclic Codes over Finite Chain Rings

In this section, we consider λ-cyclic codes, where $\lambda = 1+\gamma^k$ or $1-\gamma^k$, are two special units in the finite chain ring R.

Recall that the finite chain ring R has unique maximal ideal $\langle\gamma\rangle$, where the nilpotency index of γ is $k+1$, the cardinality of the residue field $\mathbb{F}$ is $|\mathbb{F}| = q = p^r$ for some r, where p is a prime. Let n be a positive integer with $\gcd(n,p) = 1$. This implies that there exists a unique integer n' in $\{1, 2, \cdots, p-1\}$ satisfying $nn' \equiv 1 \,(\text{mod } p)$. That is, $nn' = 1+ps$ for some integer s. Let

$$\beta = 1 + n'\gamma^k. \tag{5}$$

We know $\gamma^{k+1} = 0$ in R, so $(1+n'\gamma^k)(1-n'\gamma^k) = 1$. Hence β is a unit in R and $\beta^{-1} = (1-n'\gamma^k)$. Furthermore, we have that

$$\begin{aligned}\beta^i &= (1+n'\gamma^k)^i = 1 + \binom{i}{1}1^{i-1}(n'\gamma^k) + \cdots + \binom{i}{j}(n'\gamma^k)^j + \cdots + (n')^i\gamma^{ik} \\ &= 1 + in'\gamma^k.\end{aligned}$$

In particular if $i = n$ then we have that

$$\beta^n = 1 + nn'\gamma^k = 1 + (1+ps)\gamma^k = 1 + \gamma^k + sp\gamma^k = 1 + \gamma^k,$$

since by Lemma 2.1, $p = \mu\gamma^j \in R$ for some $\mu \in R^\times$ and integer $j \geq 1$. Since $(1+\gamma^k)(1-\gamma^k) = 1$, so

$$\beta^{-n} = (\beta^n)^{-1} = 1 - \gamma^k.$$

Let η_β be the following mapping

$$\begin{aligned}\eta_\beta : R[x]/\langle x^n - 1\rangle &\to R[x]/\langle x^n - \beta^{-n}\rangle &(6)\\ a(x) &\mapsto a(\beta x). &(7)\end{aligned}$$

Note that η_β preserves the ring addition and multiplication. If $a(x) = b(x)$ in $R[x]/\langle x^n - 1\rangle$ then we have that $a(x) - b(x) = q(x)(x^n - 1)$ for some $q(x) \in R[x]$. This implies that

$$\begin{aligned}\eta_\beta(a(x) - b(x)) &= \eta_\beta(q(x)(x^n - 1)) = q(\beta x)((\beta x)^n - 1) = q(\beta x)(\beta^n x^n - 1) \\ &= \beta^n q(\beta x)(x^n - \beta^{-n}) \in \langle x^n - \beta^{-n}\rangle.\end{aligned}$$

Hence we have

$$\eta_\beta(a(x)) = \eta_\beta(b(x)).$$

This implies that η_β is well-defined. Let $\eta_{\beta^{-1}}$ be the following correspondence.

$$\begin{aligned}\eta_{\beta^{-1}} : R[x]/\langle x^n - 1\rangle &\to R[x]/\langle x^n - \beta^n\rangle &(8)\\ a(x) &\mapsto a(\beta^{-1}x). &(9)\end{aligned}$$

Using an argument similar that above, we can check the definition $\eta_{\beta^{-1}}$ is well-defined and preserves the ring addition and multiplication.

The following proposition can be easily obtained.

Proposition 4.1. *Assume the notations given above. Let* $\gcd(n,p)=1$. *Then*

(i) The mappings η_β *and* $\eta_{\beta^{-1}}$ *are well-defined and are both ring isomorphisms;*

(ii) I *is an ideal of* $R[x]/\langle x^n-1\rangle$ *if and only if* $\eta_\beta(I)$ *is an ideal of* $R[x]/\langle x^n-\beta^{-n}\rangle$;

(iii) I *is an ideal of* $R[x]/\langle x^n-1\rangle$ *if and only if* $\eta_{\beta^{-1}}(I)$ *is an ideal of* $R[x]/\langle x^n-\beta^n\rangle$.

Let $\mathbf{v}=(v_0,v_1,\cdots,v_{n-1})\in R^n$, we define $\tilde{\eta_\beta}$ as the following map

$$\begin{aligned}\tilde{\eta_\beta}: R^n &\to R^n,\\ (v_0,v_1,\cdots,v_{n-1}) &\mapsto (v_0,v_1\beta,\cdots,v_{n-1}\beta^{n-1}).\end{aligned}$$

We have that

$$\begin{aligned}P_{\beta^{-n}}\circ\tilde{\eta_\beta}(\mathbf{v}) &= P_{\beta^{-n}}\circ\tilde{\eta_\beta}(v_0,v_1,\cdots,v_{n-1})=P_{\beta^{-n}}(v_0,v_1\beta,\cdots,v_{n-1}\beta^{n-1})\\ &= \sum_{l=0}^{n-1}v_l(\beta x)^l=\eta_\beta(\sum_{l=0}^{n-1}v_lx^l)=\eta_\beta\circ P_1(v_0,v_1,\cdots,v_{n-1})=\eta_\beta\circ P_1(\mathbf{v}).\end{aligned}$$

In other words, the following diagram commutes

$$P_{\beta^{-n}}\circ\tilde{\eta_\beta}=\eta_\beta\circ P_1. \tag{10}$$

Equation (10) gives the following commutative diagram

$$\begin{array}{ccc} R^n & \xrightarrow{\tilde{\eta_\beta}} & R^n \\ {\scriptstyle P_1}\downarrow & & \downarrow{\scriptstyle P_{\beta^{-n}}} \\ R[x]/\langle x^n-1\rangle & \xrightarrow{\eta_\beta} & R[x]/\langle x^n-\beta^{-n}\rangle. \end{array}$$

Following the definition of $\tilde{\eta_\beta}$, we can also define $\eta_{\tilde{\beta^{-1}}}$ as the following map

$$\begin{aligned}\eta_{\tilde{\beta^{-1}}}: R^n &\to R^n,\\ (v_0,v_1,\cdots,v_{n-1}) &\mapsto (v_0,v_1\beta^{-1},\cdots,v_{n-1}(\beta^{-1})^{n-1}).\end{aligned}$$

We also have that $P_{\beta^n}\circ\eta_{\tilde{\beta^{-1}}}=\eta_{\beta^{-1}}\circ P_1$.

Note that $\beta^{-n}=1-\gamma^k$ and $\beta^n=1+\gamma^k$. We have the following theorem.

Theorem 4.2. *Assume the notations given above. Let* $\gcd(n,p)=1$ *and let* C *be a subset of* R^n*, then the following statements are equivalent:*

(i) C *is a linear cyclic code;*

(ii) $\tilde{\eta_\beta}(C)$ *is a linear* $(1-\gamma^k)$*-cyclic code;*

(iii) $\eta_{\tilde{\beta^{-1}}}(C)$ *is a linear* $(1+\gamma^k)$*-cyclic code.*

Proof. This theorem is followed by Corollary 2.4, Proposition 4.1 and Equation (10) directly.

Example 3. Let $n=7$ and $R=\mathbb{Z}_4[u]/\langle u^2-2\rangle$ given in Example 1, we have

$$x^7-1=(x-1)(x^3+2x^2+x-1)(x^3-x^2+2x-1).$$

Let $g(x)=x^3+2x^2+x-1$, and let C be the code generated by $g(x)$, then C is a cyclic code of length 7 over R. It is easy to verify that

$$\eta_\beta(g(x))=g(\beta x)=\beta^3(x^3+2\beta^{-1}x^2+\beta^{-2}x-\beta^{-3})=\beta^3(x^3+2x^2+x-\beta^{-1}),$$

since $\beta=1+2u, \beta^{-1}=1-2u$. Then $\tilde{g}(x)=x^3+2x^2+x-\beta^{-1}$ generates a $(1-2u)$-cyclic code.

For the remainder of this section, we focus on the structure of a special type cyclic, $(1-\gamma^k)$-cyclic and $(1+\gamma^k)$-cyclic codes over the finite chain ring R. We have the following theorem.

Theorem 4.3. *Assume* $\gcd(n,p)=1$*, and let* $x^n-1=a(x)b(x)c(x)$*, where* $a(x),b(x)$ *and* $c(x)$ *are monic pairwise relatively prime polynomials in* $R[x]$*, and let* C *be the cyclic code with* $P_1(C)=\langle a(x)b(x),\gamma^k a(x)c(x)\rangle$*. Then*

(i) $P_1(C)$ *is generated by* $g(x)=a(x)(b(x)+\gamma^k)$*.*

(ii) The cardinality of C *is* $(p^r)^{(k+1)\deg c(x)+\deg b(x)}$*.*

Proof. (i) We note that $\gamma^k a(x)b(x), \gamma^k a(x)c(x) \in P_1(C)$. Since $b(x), c(x)$ are relatively prime, there exist $u(x), v(x) \in R[x]$ such that

$$u(x)b(x)+v(x)c(x)=1. \tag{11}$$

This implies that

$$\begin{aligned}\gamma^k a(x) &= \gamma^k a(x)(u(x)b(x)+v(x)c(x))\\ &= u(x)(\gamma^k a(x)b(x))+v(x)(\gamma^k a(x)c(x)) \in P_1(C).\end{aligned}$$

We have

$$g(x)=a(x)(b(x)+\gamma^k)=a(x)b(x)+\gamma^k a(x) \in P_1(C).$$

Therefore $\langle g(x)\rangle \subseteq P_1(C)$.

Conversely, we note that $a(x)b(x)c(x) = x^n - 1 = 0 \in R[x]/\langle x^n - 1\rangle$. This implies that

$$\gamma^k a(x)c(x) = a(x)(b(x) + \gamma^k)c(x) = g(x)c(x) \in \langle g(x)\rangle, \tag{12}$$

On the other hand, we have $\gamma^{2k} = 0$ in R. This gives that

$$\gamma^k a(x)b(x) = \gamma^k(a(x)(b(x) + \gamma^k)) = \gamma^k g(x) \in \langle g(x)\rangle. \tag{13}$$

By Equation (11), (12) and (13), we have that

$$\begin{aligned} \gamma^k a(x) &= \gamma^k a(x)(u(x)b(x) + v(x)c(x)) \\ &= u(x)(\gamma^k a(x)b(x)) + v(x)(\gamma^k a(x)c(x)) \in \langle g(x)\rangle. \end{aligned}$$

Hence

$$a(x)b(x) = g(x) - \gamma^k a(x) \in \langle g(x)\rangle.$$

This gives that $P_1(C) \subseteq \langle g(x)\rangle$. Therefore $P_1(C) = \langle g(x)\rangle$.

(ii) Note that $|\mathbb{F}| = p^r$, and the result follows directly from Theorem 3.4 in [3]. □

Example 4. Let $R = \mathbb{Z}_4[u]/\langle u^2 - 2\rangle$ be the chain ring given in Example 1 and let $n = 7$, we know the characteristic of the residue field of R is 2 and $\gcd(7, 2) = 1$, we have

$$x^7 - 1 = (x - 1)(x^3 + 2x^2 + x - 1)(x^3 - x^2 + 2x - 1) = a(x)b(x)c(x).$$

By Hensel's Lemma ([11], page 256, Theorem XIII.4), we can easily check that $a(x), b(x)$ and $c(x)$ are monic pairwise relatively prime polynomials in $R[x]$. In fact, in $\mathbb{Z}_2[x]$, we have

$$x(x^3 + x + 1) + (x + 1)(x^3 + x^2 + 1) = 1.$$

In $R[x]$, we have

$$(3x - 2)(x^3 + 2x^2 + x - 1) - (3x - 1)(x^3 - x^2 + 2x - 1) = 1.$$

Let C be the cyclic code with

$$P_1(C) = \langle (x - 1)(x^3 + 2x^2 + x - 1), \gamma^3(x - 1)(x^3 - x^2 + 2x - 1)\rangle,$$

where $\gamma = u$ is the generator of the maximal ideal of R with nilpotency index of 4. Then by Theorem 4.3, $P_1(C)$ is generated by

$$g(x) = (x-1)(x^3 + 2x^2 + x - 1 + \gamma^3).$$

The cardinality of C is $2^{(3+1)3+3} = 2^{15}$.

Theorem 4.4. *Assume* $\gcd(n,p) = 1$, *and let* $x^n - 1 = a(x)b(x)c(x)$, *where* $a(x), b(x)$ *and* $c(x)$ *are monic pairwise relatively prime polynomials in* $R[x]$. *Then*

(i) The ring $R[x]/\langle x^n - (1-\gamma^k)\rangle$ *is a principal ideal ring;*

(ii) Let $\tilde{C}$ *be a* $(1-\gamma^k)$*-cyclic code with* $P_{1-\gamma^k}(\tilde{C}) = \langle a'(x)b'(x), \gamma^k a'(x)c'(x)\rangle$, *where*

$$a'(x) = \beta^{-\deg(a(x))}a(\beta x), \quad b'(x) = \beta^{-\deg(b(x))}b(\beta x), \quad c'(x) = \beta^{-\deg(c(x))}c(\beta x).$$

Then $P_{1-\gamma^k}(\tilde{C})$ *is generated by* $\tilde{g}(x) = a'(x)(b'(x) + \gamma^k)$;

(iii) The cardinality of $\tilde{C}$ *is* $(p^r)^{(k+1)\deg(c'(x))+\deg(b'(x))}$.

Proof. (i) This statement follows immediately from the isomorphism η_β in Proposition 4.1 and Corollary 3.7 in [3].

(ii) We have that $\gamma^k a'(x)b'(x), \gamma^k a'(x)c'(x) \in P_{1-\gamma^k}(\tilde{C})$. By Equation (11), we have

$$u(\beta x)b(\beta x) + v(\beta x)c(\beta x) = 1, \tag{14}$$

where $u(x), v(x) \in R[x]$. This implies that

$$u(\beta x)\beta^{\deg(b(x))}b'(x) + v(\beta x)\beta^{\deg(c(x))}c'(x) = 1. \tag{15}$$

Therefore

$$\begin{aligned}\gamma^k a'(x) &= \gamma^k a'(x)(u(\beta x)\beta^{\deg(b(x))}b'(x) + v(\beta x)\beta^{\deg(c(x))}c'(x)) \\ &= u(\beta x)\beta^{\deg(b(x))}(\gamma^k a'(x)b'(x)) + v(\beta x)\beta^{\deg(c(x))}(\gamma^k a'(x)c'(x)) \in P_{1-\gamma^k}(\tilde{C}).\end{aligned}$$

This implies that $\langle \tilde{g}(x)\rangle \subseteq P_{1-\gamma^k}(\tilde{C})$.

Conversely, since $a(x)b(x)c(x) = x^n - 1$, this gives that

$$a(\beta x)b(\beta x)c(\beta x) = (\beta x)^n - 1 = \beta^n(x^n - \beta^{-n}) = \beta^n(x^n - (1-\gamma^k)).$$

We know that $x^n - (1-\gamma^k) = 0$ in $R[x]/\langle x^n - (1-\gamma^k)\rangle$, i.e., $a(\beta x)b(\beta x)c(\beta x) = 0$ in $R[x]/\langle x^n - (1-\gamma^k)\rangle$. Hence

$$\begin{aligned}\gamma^k a'(x)c'(x) &= \beta^{-n}a(\beta x)b(\beta x)c(\beta x) + \gamma^k a'(x)c'(x) \\ &= \beta^{-n}\beta^{\deg(a(x))+\deg(b(x))+\deg(c(x))}a'(x)b'(x)c'(x) + \gamma^k a'(x)c'(x) \\ &= a'(x)(b'(x) + \gamma^k)c'(x) = \tilde{g}(x)c'(x) \in \langle \tilde{g}(x)\rangle.\end{aligned}$$

Notice that $\gamma^{2k} = 0$ in R, this gives that

$$\gamma^k a'(x)b'(x) = \gamma^k(a'(x)(b'(x) + \gamma^k)) = \gamma^k \tilde{g}(x) \in \langle \tilde{g}(x) \rangle. \qquad (16)$$

By Equation (15) and the discussion above, we have that

$$\begin{aligned} \gamma^k a'(x) &= \gamma^k a'(x)(u(\beta x)\beta^{\deg(b(x))}b'(x) + v(\beta x)\beta^{\deg(c(x))}c'(x)) \\ &= u(\beta x)\beta^{\deg(b(x))}(\gamma^k a'(x)b'(x)) + v(\beta x)\beta^{\deg(c(x))}(\gamma^k a'(x)c'(x)) \in \langle \tilde{g}(x) \rangle. \end{aligned}$$

Hence

$$a'(x)b'(x) = \tilde{g}(x) - \gamma^k a'(x) \in \langle \tilde{g}(x) \rangle.$$

This gives that $P_{1-\gamma^k}(\tilde{C}) \subseteq \langle \tilde{g}(x) \rangle$. Therefore $P_{1-\gamma^k}(\tilde{C}) = \langle \tilde{g}(x) \rangle$.

(iii) We note that $\deg(c(x)) = \deg(c'(x))$ and $\deg(b(x)) = \deg(b'(x))$, so the result is easy to obtain from (iii) in Theorem 4.3. □

Example 5. Assume the notations given in Example 4. We know the unique integer n' satisfying $7n' \equiv 1 \pmod 2$ is 1. Hence $\beta = 1 + \gamma^3$ and $\beta^{-1} = 1 - \gamma^3$. We can compute

$$a'(x) = \beta^{-\deg(a(x))}a(\beta x) = x - (1 + \gamma^3)^{-1} = x - (1 - \gamma^3) = x - \beta^{-1},$$

$$\begin{aligned} b'(x) &= \beta^{-\deg(b(x))}b(\beta x) = x^3 + 2(1 - \gamma^3)x^2 + (1 - 2\gamma^3)x - (1 - \gamma^3) \\ &= x^3 + 2x^2 + x - \beta^{-1}, \end{aligned}$$

and

$$\begin{aligned} c'(x) &= \beta^{-\deg(c(x))}c(\beta x) = x^3 - (1 - \gamma^3)x^2 + 2x - (1 - \gamma^3) \\ &= x^3 - \beta^{-1}x^2 + 2x - \beta^{-1}. \end{aligned}$$

Let $\tilde{C}$ be a $(1 - \gamma^3)$-cyclic code with $P_{1-\gamma^3}(\tilde{C}) = \langle a'(x)b'(x), \gamma^3 a'(x)c'(x) \rangle$. Then $P_{1-\gamma^3}(\tilde{C})$ is generated by

$$\tilde{g}(x) = (x - \beta^{-1})(x^3 + 2x^2 + x - 1).$$

The cardinality of $\tilde{C}$ is $2^{(3+1)3+3} = 2^{15}$.

From the proof of Theorem 4.4 , we have the following theorem.

Theorem 4.5. *Assume* $\gcd(n, p) = 1$, *and let* $x^n - 1 = a(x)b(x)c(x)$, *where* $a(x), b(x)$ *and* $c(x)$ *are monic pairwise relatively prime polynomials in* $R[x]$. *Then*

(i) The ring $R[x]/\langle x^n - (1+\gamma^k)\rangle$ *is a principal ideal ring;*

(ii) Let $\tilde{\tilde{C}}$ *be a* $(1+\gamma^k)$*-cyclic code with* $P_{1+\gamma^k}(\tilde{\tilde{C}}) = \langle a''(x)b''(x), \gamma^k a''(x)c''(x)\rangle$, *where*

$$a''(x) = \beta^{\deg(a(x))}a(\beta^{-1}x), \quad b''(x) = \beta^{\deg(b(x))}b(\beta^{-1}x), \quad c''(x) = \beta^{\deg(c(x))}c(\beta^{-1}x).$$

Then $P_{1+\gamma^k}(\tilde{\tilde{C}})$ *is generated by* $\tilde{\tilde{g}}(x) = a''(x)(b''(x)+\gamma^k)$;

(iii) The cardinality of $\tilde{\tilde{C}}$ *is* $(p^r)^{(k+1)\deg(c''(x))+\deg(b''(x))}$.

Acknowledgment: The author is grateful to Professor San Ling and the anonymous referees for their very helpful suggestions and comments on this manuscript.

References

[1] I. Constantinescu, W. Heise, A metric for codes over residue class rings of integers, *Problemy Peredachi Informatsii.* 33 (1997) 22-28.

[2] A. R. Calderbank, N. J. A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes, Cryptogr.* 6 (1995) 21-35.

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

[4] S. T. Dougherty, Y. H. Park, On modular cyclic codes. *Finite Fields Appl.* 13 (2007) 31–57.

[5] G. D. Forney, N. J. A. Sloane, M. Trott, The Nordstrom-Robinson Code is the Binary Image of the Octacode, In Coding and Quantization: DIMACS/IEEE workshop 1992, ed. Calderbank et al., Amer. Math. Soc., pp. 19–26, 1993.

[6] M. Greferath, S. E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, *IEEE Trans. Inform. Theory.* 45 (1999). 2522–2524.

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

[8] P. Kanwar, S. R. López-Permouth, Cyclic codes over the integers modulo p^m, *Finite Fields Appl.* 3 (1997) 334–352.

[9] S. Ling, J. T. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, *IEEE Trans. Inform. Theory.* 48 (2002) 2592–2605.

[10] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland, Amstterdam, 1977.

[11] B. R. McDonald, *Finite Rings with Identity.* Marcel Dekker, Inc., New York, 1974.

[12] G. H. Norton, A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, *Appl. Algebra Engrg. Comm. Comput.* 10 (2000) 489–506.

[13] V. S. Pless, W. C. Huffman, eds., *Handbook of Coding Theory.* Elsevier, Amsterdam, 1998.

[14] H. Tapia-Recillas, G. Vega, A generalization of negacyclic codes, in Proc. int. workshop on coding and cryptography, Augot D. and Carlet C., eds., 2001, pp. 519–529.

[15] J. H. Van Lint, Repeated-root cyclic codes. *IEEE Trans. Inform. Theory.* 37 (1991) 343–345.

[16] J. Wolfmann, Negaciclic and cyclic codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory.* 45 (1999) 2527–2532.

[17] J. Wolfmann, Binary images of cyclic codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory.* 47 (2001) 1773–1779.

[18] J. Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.* 121 (1999) 555-575.