J. Algebra Comb. Discrete Appl.
1(1) • 1-12
Received: 21 April 2014; Accepted: 26 August 2014
DOI 10.13069/jacodesmath.31486

Journal of Algebra Combinatorics Discrete Structures and Applications

Cyclic and constacyclic codes over a non-chain ring

Research Article

Aysegul Bayram[1]*, Irfan Siap[1]**

1. Yildiz Technical University, Faculty of Arts and Science, Department of Mathematics, Istanbul, Turkey

Abstract: In this study, we consider linear and especially cyclic codes over the non-chain ring $Z_p[v]/\langle v^p - v\rangle$ where p is a prime. This is a generalization of the case $p = 3$. Further, in this work the structure of constacyclic codes are studied as well. This study takes advantage mainly from a Gray map which preserves the distance between codes over this ring and p-ary codes and moreover this map enlightens the structure of these codes. Furthermore, a MacWilliams type identity is presented together with some illustrative examples.

2010 MSC: 94B05, 94B15, 11T71

Keywords: Non-chain rings, Linear codes, Cyclic codes, Constacycllic codes, MacWilliams type identity

1. Introduction

Recently, codes over some special finite rings especially chain rings have been studied. More recently, codes over finite non-chain rings have been also considered. However, the study on non-chain rings has proved to be challenging due to the algebraic structure of these rings which does not allow to give a nice and compact presentation of linear codes over these rings. Study on codes over such rings or rings in general is motivated by the existence of some special maps called Gray maps whose images give codes over fields. The existence of such maps is not guaranteed in general. First substantial paper which relates codes over the quaternary ring $\mathbb{Z}_4$ to binary codes is studied initially in [9] where a Gray map is presented. Some important results of this study are the generation of some optimal non-binary codes such as Kerdock, Preparata codes via a Gray map. This particular work motivated the researchers and since then codes over rings have been of great importance to the study. We can list some related studies on this subject that study codes over chain rings such as the ring of four elements $F_2 + uF_2$, the ring of 8 elements $F_2 + uF_2 + u^2F_2$, and a more general chain ring $F_2[u]/\langle u^s\rangle$ are presented in [2–4, 6, 11, 13]. Some Euclidean and Hermitian self-dual codes over the ring $F_2[v]/\langle v^2 - v\rangle$ are related to binary self-dual and formally self-dual codes and optimal self-dual binary codes obtained in [5] which inspired the original work of the authors [4]. Gao studied a new generalization of [4] over F_p under the restriction $v^3 - v$ in

* *E-mail: abayram@yildiz.edu.tr, aaysegulbayram@gmail.com*
** *E-mail: isiap@yildiz.edu.tr*

[8]. Here, the authors mainly further generalize the results in [4] to codes over the ring $Z_p[v]/\langle v^p - v\rangle$ and study algebraic structure, that is, its ideals, units, etc. Furthermore, the authors also determine the algebraic structure of linear, cyclic and constacyclic codes over this generalized ring by means of a Gray map.

In this work, we consider codes over the non-chain ring $Z_p[v]/\langle v^p - v\rangle = \{a_0 + a_1v + ... + a_{p-1}v^{p-1} | a_0, a_1, ..., a_{p-1} \in Z_p \text{ and } v^p = v\}$. In the first section we analyze the structure of the ring and investigate its algebraic properties. Furthermore, linear codes over $Z_p[v]/\langle v^p - v\rangle$ are taken into account and the generator matrices of their Gray images are examined. Then, the dual of a linear code is defined by defining an inner product and relation between linear code and further its dual is presented. The relation between cyclic codes and their duals over $Z_p[v]/\langle v^p - v\rangle$ are also studied. Finally, a class of constacyclic codes have been introduced and dual codes of them are studied.

2. Preliminaries

The ring $R_p = Z_p[v]/\langle v^p - v\rangle$ has p^p elements where p is a prime number. In order to study the structure of this ring, we introduce a linear map ϕ which we refer as a Gray map in the following way:

$$\begin{aligned} \phi : & R_p = Z_p[v]/\langle v^p - v\rangle \to Z_p^p \\ & \alpha = a_0 + a_1v + ... + a_{p-1}v^{p-1} \to \phi(\alpha) = \phi(a_0 + a_1v + ... + a_{p-1}v^{p-1}) = (\alpha(0), \alpha(1), ..., \alpha(p-1)) \end{aligned} \tag{1}$$

where $\alpha(i) = a_0 + a_1i + ... + a_{p-1}i^{p-1} \pmod p$ for all $i \in \{0, 1, ..., p-1\}$.. Indeed, this map is basically the natural one that gives the Chinese Remainder Theorem and hence this map relates the rings R_p and Z_p^p. Due to the fact that the map ϕ is a ring isomorphism, we have

$$R_p \cong Z_p[v]/\langle v\rangle \oplus Z_p[v]/\langle v-1\rangle \oplus \cdots \oplus Z_p[v]/\langle v-(p-1)\rangle \cong Z_p^p.$$

It is not easy to find the structure of lattices of ideals of non-chain rings in general. Here by using the Gray map introduced above, we are able to give the structure of ideals of R_p and further count the number of ideals as follows:

Lemma 2.1. *R_p has exactly 2^p ideals.*

Proof. Since Z_p is a field then its ideals are exactly the zero ideal and Z_p itself, then the number of ideals of Z_p^p is the product of the number of the trivial ideals. Therefore the number of ideals of R_p is 2^p. □

Example 2.2. *Consider the ring R_5. Prior to listing the ideals of R_5 we introduce a short notation such as 11010 which means that the ideal in Z_5^5 which is composed by the zero ideals in its third and fifth coordinates and the all ring in the rest. Also, we note that $a_1a_20a_40$ where $a_i \neq 0$ for $i \in \{1, 2, 4\}$ gives the same ideals since the nonzero elements in the field generate the all field. Therefore, the ideals that generate the all ring have $5^5 = 3125$ elements and naturally the elements that generate these ideals are units of R_5:*

- $11111 \to \langle 1\rangle = \langle 2\rangle = \langle 3\rangle = \langle 4\rangle = \langle 2 + v^2\rangle = ... = \langle 1 + v + 2v^2\rangle$.

  The maximal ideals with 625 elements:
- $11110 \to \langle 1+v\rangle = \langle 2+2v\rangle = \langle 3+3v\rangle = \langle 4+4v\rangle = \langle 1+2v+v^2\rangle = ... = \langle 4+3v+4v^2+4v^3+4v^4\rangle$.
- $11101 \to \langle 2+v\rangle = \langle 4+2v\rangle = \langle 1+3v\rangle = \langle 3+4v\rangle = \langle 4+4v+v^2\rangle = ... = \langle 3+3v+4v^2+4v^3+4v^4\rangle$.
- $11011 \to \langle 3+v\rangle = \langle 1+2v\rangle = \langle 4+3v\rangle = \langle 2+4v\rangle = \langle 4+v+v^2\rangle = ... = \langle 2+3v+4v^2+4v^3+4v^4\rangle$.
- $10111 \to \langle 4+v\rangle = \langle 3+2v\rangle = \langle 2+3v\rangle = \langle 1+4v\rangle = \langle 1+3v+v^2\rangle = ... = \langle 4+4v+4v^2+4v^3+4v^4\rangle$.
- ...

- *11100*→ $\langle 2+3v+v^2\rangle = \langle 4+v+2v^2\rangle = \langle 1+4v+3v^2\rangle = \langle 3+2v+4v^2\rangle = ... = \langle 1+3v+2v^2+4v^3+4v^4\rangle$. *The ideals with 25 elements:*
- 00011 → $\langle 2v+2v^2+(v^3)\rangle = \langle 4v+4v^2+2v^3\rangle = \langle v+v^2+3v^3\rangle = ... = \langle 1+3v+2v^2+4v^3+4v^4\rangle$.
- 00101 → $\langle 3v+v^2+v^3\rangle = \langle v+2v^2+2v^3\rangle = \langle 4v+3v^2+3v^3\rangle = \langle 2v+4v^2+4v^3\rangle = ... = \langle 2v^2+4v^3+4v^4\rangle$.
- ...
- 11000 → $\langle 1+v+v^2+v^3\rangle = \langle 1+2v+2v^2+2v^3\rangle = \langle 3+3v+3v^2+3v^3\rangle = ... = \langle 4+3v+3v^2+3v^3+4v^4\rangle$. *The ideals with 5 elements:*
- 10000 → $\langle 4+v^4\rangle = \langle 3+2v^4\rangle = \langle 2+3v^4\rangle = \langle 1+4v^4\rangle$.
- 01000 → $\langle v+v^2+v^3+v^4\rangle = \langle 2v+2v^2+2v^3+2v^4\rangle = \langle 3v+3v^2+3v^3+3v^4\rangle = \langle 4v+4v^2+4v^3+4v^4\rangle$.
- 00100 → $\langle 3v+4v^2+2v^3+v^4\rangle = \langle v+3v^2+4v^3+2v^4\rangle = \langle 4v+2v^2+v^3+3v^4\rangle = \langle 2v+v^2+3v^3+4v^4\rangle$.
- 00010 → $\langle 2v+4v^2+3v^3+v^4\rangle = \langle 4v+3v^2+v^3+2v^4\rangle = \langle v+2v^2+4v^3+3v^4\rangle = \langle 3v+v^2+2v^3+4v^4\rangle$.
- 00001 → $\langle 4v+v^2+4v^3+v^4\rangle = \langle 3v+2v^2+3v^3+2v^4\rangle = \langle 2v+3v^2+2v^3+3v^4\rangle = \langle v+4v^2+v^3+4v^4\rangle$. *and the zero ideal:*
- 00000 → $\langle 0\rangle$.

Let R be a ring and $a \in R$. If a is nonzero then its Hamming weight denoted by $w(a)$ equals to 1 otherwise it is equal to 0. This is generalized to an n-tuple such that if $a = (a_1, a_2, \ldots, a_n) \in R^n$, then the Hamming weight of a is defined by $w(a) = \sum_{i=1}^{n} w(a_i)$. The Hamming distance between two n-tuples is $d(x, y) = w(x - y)$ where $x, y \in R^n$. It is well known that the Hamming distance is a metric on R^n.

It is possible to characterize the unit elements of R_p and further give the number of elements in an ideal by considering the definition of ϕ together with its properties.

Lemma 2.3. *Suppose that* $I = \langle \alpha \rangle$ *where* $\alpha = a_0 + a_1 v + \ldots + a_{p-1}v^{p-1} \in R_p$. $|I| = p^{\sum_{i=0}^{p-1} w(\alpha(i))}$. *Especially, if* $\alpha(i) \neq 0$ *for all* i, *Then* α *is a unit in* R_p *and vice versa.*

Since the map ϕ is a ring isomorphism, the inverse map of ϕ denoted by $\phi^{-1} : Z_p^p \to R_p$ exists. In the following example we present the inverse map explicitly:

Example 2.4. *The inverse map is defined by*
$\phi^{-1} : Z_5^5 \to R_5$
$(k, l, m, n, t) \to k+(4l+2m+3n+t)v+(4l+m+n+4t)v^2+(4l+3m+2n+t)v^3+4(k+l+m+n+t)v^4$.

Definition 2.5. *(Gray weight) Let* $\alpha = a_0 + a_1 v + ... + a_{p-1}v^{p-1} \in R_p$. *Then*

$$w_G(\alpha) = w(\phi(\alpha)) \tag{2}$$

is called the Gray weight of α.

The Gray distance between two elements α and β of R_p is described by $d_G(\alpha, \beta) = w(\phi(\alpha) - \phi(\beta))$ which also happens to be a linear distance preserving map from (R_p^n, d_G) to (Z_p^{pn}, d).

Example 2.6. *Let* $p = 7$. *If* $\alpha = 1 + v + 5v^2 + 5v^3$ *and* $\beta = 6v + 4v^2 + 5v^3$, *then* $w_G(\alpha) = w(\phi(1 + v + 5v^2 + 5v^3)) = w(1, 5, 0, 2, 6, 0, 0) = 4$ *and* $w_G(\beta) = w(\phi(6v + 4v^2 + 5v^3)) = w(0, 1, 5, 0, 2, 6, 0) = 4$ *hence* $d_G(\alpha, \beta) = w(\phi(\alpha) - \phi(\beta)) = w((1, 5, 0, 2, 6, 0, 0) - (0, 1, 5, 0, 2, 6, 0)) = w((1, 4, 2, 2, 4, 1, 0)) = w(1 + 2v + v^2) = 6$.

Definition 2.7. *Let* $a = (a_1, a_2, .., a_p) \in Z_p^p$. *Then,* $supp(a) = \{i | a_i \neq 0\} \subseteq \{1, 2, ..., p\}$.

We can easily check that:

- If $supp(\phi(\alpha)) = supp(\phi(\beta))$ then $w_G(\alpha) = w_G(\beta)$ where $\alpha, \beta \in R_p$.
- Assume that $\langle\alpha\rangle$ and $\langle\beta\rangle$ are two ideals in R_p. Then, $supp(\phi(\alpha)) = supp(\phi(\beta))$ if and only if $\langle\alpha\rangle = \langle\beta\rangle$.

Therefore, R_p is a principal ideal ring, that is, all ideals in R_p are generated by a single element of R_p similar to the special case $p = 3$ [4] .

Theorem 2.8. *If $I = \langle\alpha_1, \alpha_2, \ldots, \alpha_s\rangle$ is a finitely generated ideal of R_p, then $I = \langle\beta\rangle$ for some $\beta \in R_p$ where $supp(\phi(\beta)) = \bigcup_{i=1}^{s} supp(\phi(\alpha_i))$.*

Example 2.9. *Let $I = \langle\alpha_1, \alpha_2\rangle$ where $\alpha_1 = 3v + v^2 + v^3$ and $\alpha_2 = 1 + 3v + 3v^2 + 3v^3 + 2v^4 \in R_5$. Since*

$$supp(\phi(\alpha_1)) = supp(\phi(3v + v^2 + v^3)) = supp((0, 0, 3, 0, 2)) = \{3, 5\}$$

and

$$supp(\phi(\alpha_2)) = supp(\phi(1 + 3v + 3v^2 + 3v^3 + 2v^4)) = supp((1, 2, 0, 0, 0)) = \{1, 2\}$$

$$supp(\phi(\beta)) = \bigcup_{i=1}^{2} supp(\phi(\alpha_i)) = \{1, 2, 3, 5\},$$

then β can be selected as $4 + 2v + 3v^2 + 3v^3 + 2v^4$ which generates a maximal ideal in R_5.

The units and the elements which generate the maximal ideals in R_p can be classified by means of their Gray images:

Lemma 2.10. *Let $\alpha \in R_p$. The follows hold:*
i) $supp(\phi(\alpha)) = \{1, ..., p\}$ if and only if α is a unit. Hence, R_p has exactly $(p-1)^p$ units .
ii) Suppose $I = \langle\alpha\rangle$. Then, $|\ supp(\phi(\alpha))| = p - 1$, if and only if I is maximal.

3. Linear Codes over R_p

A minimal generating set is comprised for all linear codes by a set of linearly independent and spanning vectors called basis for codes over fields. However, in the case for codes over rings, this is a challenging problem and in most cases impossible since we do not have basis in general for modules. In [2] and in [3], authors gave a basis or a minimal spanning set for the codes of even length over $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2 + \cdots + u^{k-1}Z_2$, respectively. These are all chain rings, that is, the set of all ideals is a chain under set-theoretic inclusion.

Since R_p is not a chain ring, we can not get a generating matrix, easily. To overcome this problem in linear code case some special definitions (modular dependence) and cases of codes over rings are presented in [12] and in [15]. Here, based on the Gray image of the code, the generator matrix of the image code is presented and some results are obtained:

Theorem 3.1. *Assume that the set $\{g_1, g_2, \ldots, g_k\} \subset R_p^n$ is a generating set of a linear code C over R_p of length n where $g_i = (g_{i1}, g_{i2}, \ldots, g_{in})$. Then, the matrix*

$$\phi(G) = \begin{bmatrix} \phi(g_{11}) & \phi(g_{12}) & \cdots & \phi(g_{1n}) \\ \phi(vg_{11}) & \phi(vg_{12}) & \cdots & \phi(vg_{1n}) \\ \phi(v^2g_{11}) & \phi(v^2g_{12}) & \cdots & \phi(v^2g_{1n}) \\ \vdots & \vdots & \vdots & \\ \phi(v^{p-1}g_{11}) & \phi(v^{p-1}g_{12}) & \cdots & \phi(v^{p-1}g_{1n}) \\ \vdots & \vdots & \vdots & \\ \phi(g_{k1}) & \phi(g_{k2}) & \cdots & \phi(g_{kn}) \\ \phi(vg_{k1}) & \phi(vg_{k2}) & \cdots & \phi(vg_{kn}) \\ \phi(v^2g_{k1}) & \phi(v^2g_{k2}) & \cdots & \phi(v^2g_{kn}) \\ \vdots & \vdots & \vdots & \\ \phi(v^{p-1}g_{k1}) & \phi(v^{p-1}g_{k2}) & \cdots & \phi(v^{p-1}g_{kn}) \end{bmatrix}$$

generates $\phi(C)$.

Example 3.2. *Let* $p = 5$ *and suppose that*

$$G = \begin{bmatrix} 2v + 4v^2 + 3v^3 + v^4 & 0 \\ 0 & 4v + v^2 + 4v^3 + v^4 \end{bmatrix}$$

is a generator matrix of C *of length* 2 *over* $R_5 = Z_5[v]/\langle v^5 - v\rangle$.

Then

$$\phi(G) = \begin{bmatrix} 00000 & 00000 \\ 00000 & 00000 \\ 00000 & 00000 \\ 00000 & 00000 \\ 00000 & 00004 \\ 00000 & 00000 \\ 00000 & 00000 \\ 00000 & 00000 \\ 00040 & 00000 \\ 00000 & 00000 \end{bmatrix}.$$

Hence $\phi(G)$ *is a generator matrix of* $\phi(C)$, *with length* 10, *dimension* 2 *and size* $5^2 = 25$.

Another simple and compact way to represent the structure of a generator matrix of $\phi(G)$ is given below. Let $\alpha = g_0 + g_1v + ... + g_{p-1}v^{p-1} \in R_p$ and $\alpha(i) = g_0 + g_1i + ... + g_{p-1}i^{p-1} \pmod p$.

$\phi(\alpha) = \phi(g_0 + g_1v + ... + g_{p-1}v^{p-1}) = (\alpha(0), \alpha(1), ..., \alpha(p-1))$.

Alternatively, after some row operations the generator matrix is then equivalent to a block matrix with blocks $(G_{ij})_{p\times p} = diag(\alpha_{ij}(0), \alpha_{ij}(1), \ldots, \alpha_{ij}(p-1))$.

As mentioned above, we again emphasize that it is a difficult problem to determine the minimal independent sets that generate a linear code over R_p in general due to the fact that R_p is not a chain ring. However, one can adopt a similar approach as presented in both [12] and [15] to capture the size of linear codes over R for some special cases.

Definition 3.3. *A set* $\{g_1, g_2, \ldots, g_k\} \subset R_p^n$ *is called a minimal independent generating set for a code* C, *if*

$$\{\phi(g_1), \phi(vg_1), \ldots, \phi(v^{p-1}g_1), \phi(g_2), \phi(vg_2), \ldots, \phi(v^{p-1}g_2), \ldots, \phi(g_k), \phi(vg_k), \ldots, \phi(v^{p-1}g_k)\} \subset Z_p^{pn}$$

is a Z_p*-linearly independent set.*

Now, having this definition at hand one can determine the size of a code with a generating set which is Z_p-linearly independent:

Lemma 3.4. *If $C = \langle\{g_1, g_2, \ldots, g_k\}\rangle$ where the set $\{g_1, g_2, \ldots, g_k\} \subset R_p^n$ is a minimal independent generating set, then $|C| = p^{pk}$.*

3.1. The Dual Code

In this subsection, an inner product which is introduced as below helps us to construct the dual code of a linear code where the inner product is obtained with the Gray image. We also show the proof of a lemma which relates dual of the code and its Gray image:

Let $g = [g_1, g_2, \ldots, g_n], h = [h_1, h_2, \ldots, h_n] \in R_p^n$, $g_i = g_{i1} + g_{i2}v + \ldots + g_{ip}v^{p-1}$,$h_i = h_{i1} + h_{i2}v + \ldots + h_{ip}v^{p-1}$, $g_i(j) = g_{i1} + g_{i2}j + \ldots + g_{ip}j^{p-1} \pmod p$ and $h_i(j) = h_{i1} + h_{i2}j + \ldots + h_{ip}j^{p-1} \pmod p$.

$$\langle g, h\rangle_\phi = \sum_{i=1}^{n}\sum_{j=1}^{p-1}(g_i(j)h_i(j)).$$

If C is a linear code of length n over the ring R_p, then the dual code is defined by

$$C^\perp = \{h \in R_p^n | \langle g, h\rangle_\phi = 0 \text{ for all } g \in C\}. \tag{3}$$

Lemma 3.5. $\phi(C)^\perp = \phi(C^\perp)$.

Proof. The proof follows from the definitions: If $h \in C^\perp$, then, $\langle g, h\rangle_\phi = 0$ for all $g \in C$. This implies that $\langle\phi(g), \phi(h)\rangle = 0$ for all $\phi(g)$. Hence, $\phi(h) \in (\phi(C))^\perp$. Thus, $\phi(C^\perp) \subset \phi(C)^\perp$. The reverse follows directly by reversing the steps.

□

Example 3.6. *Let*

$$G = \begin{bmatrix} 2+4v^4 & 3+3v+v^2+2v^3+3v^4 \\ 2v^3+2v^4 & 3+4v+3v^4 \end{bmatrix}$$

be a generator matrix of a linear code C over $R_5 = Z_5[v]/\langle v^5 - v\rangle$, Then the image of this code is generated by

$$\phi(G) = \begin{bmatrix} \phi(2+4v^4) & \phi(3+3v+v^2+2v^3+3v^4) \\ \phi(v(2+4v^4)) & \phi(v(3+3v+v^2+2v^3+3v^4)) \\ \phi(v^2(2+4v^4)) & \phi(v^2(3+3v+v^2+2v^3+3v^4)) \\ \phi(v^3(2+4v^4)) & \phi(v^3(3+3v+v^2+2v^3+3v^4)) \\ \phi(v^4(2+4v^4)) & \phi(v^4(3+3v+v^2+2v^3+3v^4)) \\ \phi(2v^3+2v^4) & \phi(3+4v+3v^4) \\ \phi(v(2v^3+2v^4)) & \phi(v(3+4v+3v^4)) \\ \phi(v^2(2v^3+2v^4)) & \phi(v^2(3+4v+3v^4)) \\ \phi(v^3(2v^3+2v^4)) & \phi(v^3(3+4v+3v^4)) \\ \phi(v^4(2v^3+2v^4)) & \phi(v^4(3+4v+3v^4)) \end{bmatrix} = \begin{bmatrix} 2&0&0&0&0&3&0&0&0&0 \\ 0&1&0&0&0&0&2&0&0&0 \\ 0&0&1&0&0&0&0&2&0&0 \\ 0&0&0&1&0&0&0&0&3&0 \\ 0&0&0&0&1&0&0&0&0&2 \\ 0&0&0&0&0&3&0&0&0&0 \\ 0&4&0&0&0&0&0&0&0&0 \\ 0&0&3&0&0&0&0&4&0&0 \\ 0&0&0&1&0&0&0&0&3&0 \\ 0&0&0&0&0&0&0&0&0&2 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

over Z_5*, then* $|C| = 5^9$*. Let*

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 & 0 \end{bmatrix}.$$

is a parity check matrix of $\phi(C)$*.*

Hence $\left|\phi(C)^{\perp}\right| = 5$*. Conversely, for all* $h = [h] \in C^{\perp}$ *such that*

$$h = \left[h_1 + h_2 v + h_3 v^2 + h_4 v^3 + h_5 v^4 \quad h_1^{'} + h_2^{'} v + h_3^{'} v^2 + h_4^{'} v^3 + h_5^{'} v^4\right]$$

then

$$C^{\perp} = \{\ h = \left[(2v + 4v^2 + 3v^3 + v^4)h_5 \quad (v + 2v^2 + 4v^3 + 3v^4)h_5\right], h_5 \in Z_5\}$$

Hence,

$\left|C^{\perp}\right| = 5$*. Therefore,* $\phi(C^{\perp}) = \phi(C)^{\perp}$*.*

3.2. MacWilliams Identity for Codes over R_p

The MacWilliams identity is one of the prominent results in coding theory, which supplies the relationship between the weight enumerator of a linear code and that of its dual code [10]. The distribution of weights for a linear code is crucial to its performance analysis such as, linear programming bound, error correcting capabilities, the extremal weight enumerators related to the dual codes, etc. In this section, we state several lemmas and the main theorem. We also illustrate the theorem with a moderate example.

In this work, we assume that the character χ is described by $\chi(a) = \xi^{a(0)+a(1)+a(2)+\ldots+a(p-1)}$ where $\xi = e^{2\pi i/p}$.

The *Gray weight enumerator* of a linear code C over R_p is defined by

$$W(x, y) = \sum_{c \in C} x^{pn - w_G(c)} y^{w_G(c)}.$$

This section is a generalization of Section 3.2 in [4], so we will not give all proofs in detail here. Therefore we present the statement of lemmas and the main theorem and state an example to show the result.

Lemma 3.7. *1. Assume that* $I \neq \{0\}$ *be an ideal of the ring* R_p*. Then,*

$$\sum_{a \in I} \chi(a) = 0.$$

2. For $a \in R_p$*, we have*

$$\sum_{r \in R_p} \chi(ar) = \begin{cases} p^p, & a = 0 \\ 0, & a \neq 0. \end{cases}$$

3. If $\beta \in R_p$, then

$$\sum_{\alpha \in R_p} \chi\left(\langle \beta, \alpha \rangle\right) x^{p-w_G(\alpha)} y^{w_G(\alpha)} = (x+(p-1)y)^{p-w_G(\beta)} (x-y)^{w_G(\beta)}.$$

The following well known result plays an important role in finalizing the proof of the main theorem:

Lemma 3.8. *[10] If C and its dual $C^{\perp}$ are linear codes over the ring R_p with*

$$\hat{f}(u) = \sum_{v \in R_p^n} \chi\left(\langle u, v \rangle\right) f(v),$$

then

$$\sum_{v \in C^{\perp}} f(v) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u).$$

By combining the lemmas above we get the main theorem that relates the Gray weight enumerators of the code and its dual:

Theorem 3.9. *Suppose that C is a linear code over R_p, then*

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C\left(x+(p-1)y, x-y\right).$$

Example 3.10. *Assume that*

$$G = \begin{bmatrix} 2+3v^4 & 0 \\ 0 & 3v+3v^2+3v^3+3v^4 \end{bmatrix}$$

generates a linear code C over R_5. Then, its Gray weight enumerator is

$$W_C(x,y) = x^{10} + 8x^9y + 16x^8y^2.$$

Therefore, by applying the necessary change of variables in the main theorem, we obtain

$$W_{C^{\perp}}(x,y) = x^{10} + 32x^9y + 448x^8y^2 + 3584x^7y^3 + 17920x^6y^4 + 57344x^5y^5 + 114688x^4y^6 + 131072x^3y^7$$

$$+65536x^2y^8.$$

4. Cyclic Codes over R_p

A very significant and well know class of linear codes is the class of cyclic codes which plays a crucial role in coding theory due to their easy implementation. Since cyclic codes can be described as ideals in some polynomial rings, they have considerable inherent algebraic structure.

In this part we consider the algebraic structure of cyclic codes over the ring R_p. We also study the structure of their duals.

Definition 4.1. *Let σ be a cyclic right shift on the entries of an n-tuple in R^n such that $\sigma(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2})$. For a linear code C, if $\sigma(C) = C$, then C is called a cyclic code of length n.*

After associating a polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ to a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, if C is a cyclic code then, C becomes an ideal of the quotient ring $R[x]/\langle x^n - 1\rangle$.

Let $R_{(n,p)} = R_p[x]/\langle x^n - 1\rangle$. Since $R_p \cong Z_p^p$, then

$$R_p[x]/\langle x^n - 1\rangle \cong Z_p[x]/\langle x^n - 1\rangle \times Z_p[x]/\langle x^n - 1\rangle \times \ldots \times Z_p[x]/\langle x^n - 1\rangle.$$

Let

$$L_{(n,p)} = Z_p[x]/\langle x^n - 1\rangle \times Z_p[x]/\langle x^n - 1\rangle \times \ldots \times Z_p[x]/\langle x^n - 1\rangle.$$

Now as a natural extension of ϕ ,we can get an isomorphism between the rings $R_{(n,p)}$ and $L_{(n,p)}$. We define a projection map

$$\pi_i : Z_p^p \to Z_p,$$

such that $\pi_i((a_1, a_2, \ldots\ a_p)) = a_i$ for $1 \leq i \leq p$. Then, we identify

$$\begin{aligned}\phi :& R_{(n,p)} \to L_{(n,p)}\\ &\phi(\sum_{i=0}^{n} a_i x^i) = (\sum_{i=0}^{n} \pi_1(\phi(a_i))x^i, \sum_{i=0}^{n} \pi_2(\phi(a_i))x^i, \ldots, \sum_{i=0}^{n} \pi_p(\phi(a_i))x^i).\end{aligned}$$

Example 4.2. *Let* $f(x) = (1 + v^2)x^3 + (1 + 3v + v^3)x^2 + (3v^2 + v^4)x + 1$ *in* $R_{(4,5)}$. *Then,* $\phi(f(x)) = (x^3 + x^2 + 1, 2x^3 + 4x + 2, 3x + 1, 2x^2 + 3x + 1, 2x^3 + 2x^2 + 4x + 1)$.

It is easy to get the structure of $R[x]/\langle x^n - 1\rangle$ since this map is an isomorphism.

$R_{(n,p)}$ is a principal ideal ring. We can determine the generator of ideals as follows: Suppose that $I = \langle f_1(x), f_2(x), \ldots, f_s(x)\rangle$ is a finitely generated ideal of $R_{(n,p)}$ where $f_i(x) = \sum_{j=0}^{n} f_{ij}x^j$. Then, for $i = 1, 2, \ldots, p$ let $g_i = gcd_{1\leq j\leq s}(\pi_i(\phi(f_j))), x^n - 1)$. Hence, $I = \langle g(x)\rangle$ where

$$g(x) = \phi^{-1}((g_1(x), g_2(x), \ldots, g_p(x))).$$

Example 4.3. *Let* $I = \langle f_1(x) = (1+v+2v^2+x+(1+2v+v^2)x^2, f_2(x) = 2+2v^2+(1+v+v^2)x+(v+2v^2)x^2\rangle$ *be an ideal of* $R_{(4,3)}$. *Then,* $\phi(f_1(x)) = ((2+x)^2, (2+x)^2, 2+x)$ *and* $\phi(f_2(x)) = (2+x, 1, (2+x)^2)$. *Next,* $g_1 = gcd((2+x)^2, 2+x, x^3-1) = 2+x$, $g_2 = gcd((2+x)^2, 1, x^3-1) = 1$, $g_3 = gcd(2+x, (2+x)^2, x^3-1) = 2 + x$. *So we have* $\phi(I) = \langle(2 + x, 1, 2 + x)\rangle$. *Therefore,* $I = \phi^{-1}(\phi(I)) = \langle\phi^{-1}(2 + x, 1, 2 + x)\rangle = \langle 2 + v + v^2 + (1 + v + v^2)x\rangle$.

The following lemma can be observed as a straightforward result of the above statements and the example:

Lemma 4.4. *If* $C = \langle g(x)\rangle$ *is a cyclic code of length* n *over* R_p *and* $\phi(g(x)) = (g_1, g_2, \ldots, g_p)$ *with* $\deg(gcd(g_i, x^n - 1)) = n - k_i$ *for* $1 \leq i \leq p$, *then* $|C| = p^{\sum_{i=1}^{p} k_i}$.

4.1. The Dual of Cyclic Codes

In this subsection, we study the algebraic structure of the dual of a cyclic code over R_p. Let $C = \langle g(x)\rangle$ be a cyclic code of length n over R_p. Assume that, $\phi(C) = J = \langle(g_1(x), g_2(x), \ldots\ g_p(x))\rangle$ where $g_i = \pi_i(\phi(g(x)))$. The dual of J is the cyclic code

$$J^{\perp} = \langle(h_{1_R}(x), h_{2_R}(x), \ldots, h_{p_R}(x))\rangle,$$

where $h_i(x) = (x^n - 1)/(gcd(x^n - 1, g_i)$ and $h_{i_R}(x)$ is the reciprocal polynomial of $h_i(x)$. Hence, $C^{\perp} = \langle\phi^{-1}(h_{1_R}(x), h_{2_R}(x), \ldots, h_{p_R}(x))\rangle$.

Example 4.5. *Let* $I = \langle f(x) = (3v^4+3v^3+4v)x^3+(4v^4+4v^3+2v^2+1)x^2+(2v^4+4v^2+3)x+(v^3+4v+2) >$ *be an ideal of* $R_{(5,4)}$. *Then,* $\phi(f(x)) = (x^2+3x+2, x^2+4x+2, x+3, x^3+x^2+x+1, x^3+3x^2+4x+2)$. *Next,* $g_1 = gcd(x^2+3x+2, x^4-1) = x^2+3x+2$, $g_2 = gcd(x^2+4x+2, x^4-1) = x^2+4x+2$, $g_3 = gcd(x+3, x^4-1) = x+3$, $g_4 = gcd(x^3+x^2+x+1, x^4-1) = x^3+x^2+x+1$, $g_5 = gcd(x^3+3x^2+4x+2, x^4-1) = x^3+3x^2+4x+2$. *Thus,* $|\langle I\rangle| = 5^9$. $C^{\perp} = \langle \phi^{-1}(h_{1_R}(x), h_{2_R}(x), h_{3_R}(x), h_{4_R}(x), h_{5_R}(x))\rangle = \langle \phi^{-1}((2x^2+2x+1, 3x^2+4x+1, x^3+x^2+x+1, 4x+1, 2x+1))\rangle = \langle (4v^4+3v^3+v^2+2v)x^3+(4v^4+3v^2+4v+2)x^2+(4v^3+4v^2+2v+2)x+1\rangle$. *Therefore,* $\left|\langle C^{\perp}\rangle\right| = 5^{11}$.

5. Constacyclic Codes over R_p

In this section, we study constacyclic codes over R_p.

Definition 5.1. *Let* $\alpha = a_0+a_1v+...+a_{p-1}v^{p-1}$ *be a unit element of* R_p *and* C *be a linear code of length* n *over* R_p. *If for all* $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ *and a unit in* R_p *we have* $(\alpha c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$, *then* C *is called an* α*-constacyclic code or shortly constacyclic code.*

Similar to the cyclic codes case if we associate each codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ with a polynomial $c = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in R[x]$, then C can be viewed as an ideal in $S_{(n,p)} = R_p[x]/\langle x^n - \alpha\rangle$. By applying the Chinese Remainder Theorem, we have the following result:

Let $S_{(n,p)} = R_p[x]/\langle x^n - \alpha\rangle$. Since $R_p \cong Z_p^p$, Then

$$S \cong Z_p[x]/\langle x^n - \alpha(0)\rangle \times Z_p[x]/\langle x^n - \alpha(1)\rangle \times \ldots \times Z_p[x]/\langle x^n - \alpha(p-1)\rangle.$$

For example, let $I = \langle f(x) = (4+3v+v^3+v^4+(1+3v+v^2+4v^3+4v^4)x+(3v+4v^2+2v^3+2v^4)x^2+(2v+v^2+3v^3+4v^4)x^3)\rangle$, be an ideal of $R_{(4,5)}$ then $\phi(f(x)) = (4+x, 4+3x+x^2, 4+2x+x^3, 1+x+x^2, 1+4x+x^2)$.

Since α is a unit element of R_p, then $\alpha(i) \neq 0$ for all $0 \leq i \leq p-1$, the number of constacyclic codes over R_p can be obtain as follows:

Theorem 5.2. *The number of* α*-constacyclic codes of length* n *is equal to* $\prod_{i=0}^{p-1} \delta(i)$ *where*

$$\delta(i) = \begin{cases} \sigma_n, & i = 1, \\ \eta_{(n,i)}, & i = 2, ..., (p-1). \end{cases}$$

σ_n *and* $\eta_{(n,i)}$ *are equal to the number of cyclic and* $\alpha(i)-$*constacyclic codes of length* n *over* Z_p, *respectively.*

Proof. Since α is a unit element of R_p, the Gray image consists of non zero elements of Z_p. If the Gray image contains 1 as a component then the projection code corresponding to that particular component is cyclic which has a generator polynomial as a divisor of $x^n - 1$ over Z_p. In addition, if Gray image contains non zero elements different from 1, call it $\alpha(i)$, then the projection is a $\alpha(i) - constacyclic$ code of length n over Z_p. Therefore, if σ_n and $\eta_{(n,i)}$ are equal to the number of cyclic and $\alpha(i) - constacyclic$ codes of length n over Z_p, respectively, then the number of α-constacyclic codes of length n is equal to $\prod_{i=0}^{p-1} \delta(i)$. □

Example 5.3. *Let* $\phi(4+v+2v^3) = (4, 2, 2, 1, 1) \in Z_5$. *Since the number of* $2-constacyclic$, $negacyclic$ *and cyclic codes over* Z_5 *are* $\delta(2) = \eta_{(4,2)} = 2$, $\delta(4) = \eta_{(4,4)} = 2^2$ *and* $\delta(1) = \sigma_4 = 8$, *respectively then the number of all* $(4+v+2v^3) - constacyclic$ *code length* 4 *over* R_5 *is equal to* $4.2.2.8.8 = 2^{2+1+1+3+3} = 2^{10}$.

The algebraic structure of a dual constacyclic code can be obtained as follows: Suppose $C = \langle g(x)\rangle$ is an α-constacyclic code of length n over R_p. Let $g_i = \pi_i(\phi(g(x)))$, then $\phi(C) = \langle (g_1(x), g_2(x), \ldots g_p(x))\rangle$. The dual of C is an α-constacyclic code which is equal to $\langle \phi^{-1}(h_1(x), h_2(x), \ldots h_p(x))\rangle$, where $h_i(x) = (x^n - \alpha(i))/(g_i(x))$.

Example 5.4. *Let C be a $(1+v+4v^2+3v^3)-$constacyclic code over R_7 generated by $f(x) = (4v^6+4v^5+6v^3+v)x^3+(5v^6+v^5+6v^4+v^3+6v^2+v+1)x+(v^6+5v^5+4v^3+v^2+5v+3)$ which is an ideal of $R_{(3,7)}$. Since $\phi(1+v+4v^2+3v^3) = (1,2,1,2,2,5,1)$ and $\phi(f(x)) = (x+3, x^3+5, 0, 0, x^3+5, x^3+2, x+5)$ then $g_1 = x+3$ and $h_1(x) = (x^3-1)/(x+3) = (x^2+4x+2)$, $g_2 = x^3+5$ and $h_2(x) = (x^3-2)/(x^3+5) = 1$, $g_3 = 0$ and $h_3(x) = 0$, $g_4 = 0$ and $h_4(x) = 0$, $g_5 = x^3+5$ and $h_5(x) = (x^3-2)/(x^3+5) = 1$, $g_6 = x^3+5$ and $h_6(x) = (x^3-5)/(x^3+2) = 1$, $g_7 = x+5$ and $h_7(x) = (x^3-1)/(x+5) = x^2+2x+4$. So, $\phi^{-1}(h_1(x), h_2(x), h_3(x), h_4(x), h_5(x), h_6(x), h_7(x)) = \phi^{-1}(x^2+4x+2, 1, 0, 0, 1, 1, x^2+2x+4) = (5v^6+v^5+6v^4+v^3+6v^2+v+1)x^2+(v^6+2v^5+5v^4+2v^3+5v^2+2v+4)x+(5v^6+v^5+3v^4+3v^3+3v^2+5v+2)$ Therefore, $C^{\perp} = \langle (5v^6+v^5+6v^4+v^3+6v^2+v+1)x^2+(v^6+2v^5+5v^4+2v^3+5v^2+2v+4)x+(5v^6+v^5+3v^4+3v^3+3v^2+5v+2)\rangle$.*

6. Conclusions

We have explored further a new family of codes over a special non-chain ring by generalizing some results in [4]. In general, non-chain rings are very complicated to be studied. Here, by introducing a Gray map the problem has been resolved. Linear, cyclic and constacyclic codes have been introduced. A MacWilliams Type Identity is also proven. This results can be easily generalized to codes over the ring $F_q[v]/\langle v^q - v\rangle$ where F_q is a field with q elements.

Acknowledgment: The preliminary results of this paper are presented in Proceedings of the 2013 International Conference on Computational and Mathematical Methods in Science and Engineering-CMMSE 2013, June 24-27 2013, Almeria, Spain.

References

[1] T. Abualrub, I. Siap, *On the Construction of Cyclic Codes over the Ring $Z_2 + uZ_2$*, WSEAS Trans. on Math., 5(6), 750-756, 2006.

[2] T. Abulraub, I. Siap, *Cyclic Codes over the Rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$*, Designs, Codes and Cryptography, 3(42), 273-287, 2007.

[3] M. Al-Ashker, M. Hamoudeh, *Cyclic codes over $Z_2 + uZ_2 + u^2Z_2 + \cdots + u^{k-1}Z_2$*, Turkish J. Math., 35(4), 737-749, 2011.

[4] A. Bayram, I. Siap, *Structure of Codes over the Ring $Z_3[v]/\langle v^3 - v\rangle$*, Applicable Algebra in Engineering, Communication and Computing, 24(5), 369-386, 2013.

[5] K. Betsumiya, M. Harada, *Optimal self-dual codes over $F_2 \times F_2$, with respect to the Hamming weight*, IEEE Transactions on Information Theory, 50(2), 356-358, 2004.

[6] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over F_2+uF_2*, IEEE Trans. Inf. Theory, 45(4), 1250-1255, 1999.

[7] S.T. Dougherty, B. Yildiz and S. Karadeniz, *Codes over R, Gray Maps and their Binary Images*, Finite Fields and Their Applications, 17(3), 205-219, 2011.

[8] J. Gao, Y. Wang, *Some results on linear codes over $F_p+vF_p+v^3F_p$*, Journal of Applied Mathematics and Computing, May 2014.

[9] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Sole, *The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inf. Theory, 40(2), 301-319, 1994.

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

[11] M. Ozen and I. Siap, *Linear Codes Over $F_q[u]/(u^s)$ with Respect to the Rosenbloom-Tsfasman Metric*, Designs, Codes and Cryptography, 38(1), 17-29, 2006.

[12] Y. H. Park, *Modular independence and generator matrices for codes over $\mathbb{Z}_m$*, Des. Codes Crypt., 50(2), 147-162, 2009.

[13] J.-F. Qian, L.-N. Zhang, and S.-X. Zhu, *Constacyclic and Cyclic Codes over* $F_2 + uF_2 + u^2F_2$, IEICE Trans. Fundamentals, 89(6), 1863-1865, 2006.
[14] B. Yildiz, S. Karadeniz, *Linear Codes over* $F_2 + uF_2 + vF_2 + uvF_2$, Des. Codes Crypt., 54(1), 61-81, 2010.
[15] B. Yildiz, S. Karadeniz, *Cyclic Codes over* $F_2 + uF_2 + vF_2 + uvF_2$, Des. Codes Crypt., 58(3), 221-234, 2011.
[16] S.-X. Zhu, Y. Wang, M.-J. Shi, *Cyclic codes over* $F_2 + vF_2$, ISIT'09 Proceedings of the 2009 IEEE international conference on Symposium on Information Theory, 3, 1719-1722, 2009.