GANIT *J. Bangladesh Math. Soc.* (ISSN 1606-3694) **38** (2018) 57-71
DOI: https://doi.org/10.3329/ganit.v38i0.39785

ON CODES OVER THE RINGS $F_q + uF_q + vF_q + uvF_q$

Ibrahim M. Yaghi[1] and Mohammed M. AL-Ashker[2]
[1]Department of Mathematics, Islamic University of Gaza, Palestine
E-mail addresses: general −1987@hotmail.com
[2]Department of Mathematics, Islamic University of Gaza, Palestine
E-mail addresses: mashker@iugaza.edu.ps

Received: 15-04-2018 accepted: 05-09-2018

ABSTRACT

In this paper, we study the structure of linear and self dual codes of an arbitrary length n overhearing $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p and $u^2 = v^2 = 0$, $uv = vu$, Also we obtain the structure of consta-cyclic codes of length $n = q - 1$ over the ring $F_q + uF_q + vF_q + uvF_q$ in the light of studying cyclic codes over $F_q + uF_q + vF_q + uvF_q$ in [6]. This study is a generalization and extension of the works in [7], [8], and [10].

Keyword: finite rings; linear and self dual codes; consta-cyclic codes.

1. Introduction

Codes over finite rings have been studied in the early 1970's [1]. A great deal of attention has been given to codes over finite rings from1991 [5], because of their new role in algebraic coding theory and their successful applications.

Bahattin Yildiz and Suat Karadeniz studied the structure of the ring $F_2 + uF_2 + vF_2 + uvF_2$, where $u^2 = v^2 = 0$ and $uv = vu$, and they obtained the structure of linear codes over this ring of any length n as in [7]. In [8] they proved the existence of self dual codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$ of all lengths and obtained some results about their gray images, also they obtained the structure of cyclic codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$ of any length n in [9], and in the light of the study in [9] they obtained the structure of $(1 + v)$-constacycliccodesovertheringF$F_2 + uF_2 + vF_2 + uvF_2$of odd lengths n as in[10].

In [6], Xu Xiaofang and Liu Xiusheng they obtained the structure of the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p and $u^2 = v^2 = 0$, $uv = vu$. Also they obtained the structure of cyclic codes over the ring $F_q + uF_q + vF_q + uvF_q$ of all lengths n as a generalization of the work done in [9] on the ring $F_2 + uF_2 + vF_2 + uvF_2$.

In this paper we aim to generalize all the previous studies from the ring $F_2 + uF_2 + vF_2 + uvF_2$to the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p and $u^2 = v^2 = 0$, $uv = vu$. This paper is organized as follows:

In section 3, we study linear codes over the ring $F_q + uF_q + vF_q + uvF_q$, first we mention the main properties of the ring from [6] which is important to obtain the structure of linear codes and the uniqueness of it's type, also we define a gray map on the ring $(F_q + uF_q + vF_q + uvF_q)^n$ and through this map we define the lee weight of any codeword.

In section 4, we study self dual codes over the ring $F_q + uF_q + vF_q + uvF_q$, first we study the duality of the gray image of self dual codes then we obtain the existence of self dual codes over the ring $F_q + uF_q + vF_q + uvF_q$ of all lengths using an old result from[2]. In section 5, we study consta-cyclic codes over the ring $F_q + uF_q + vF_q + uvF_q$, which are isomorphic to the ideals of the ring $(F_q + uF_q + vF_q + uvF_q)\,[x]/(x^n-(1 + v))$, using an isomorphism from the ring $(F_q + uF_q + vF_q + uvF_q)[x]/(x^n- (1 + v))$ to the ring $(F_q + uF_q + vF_q + uvF_q)[x]/(x^n-1)$ we obtain the structure of$(1 + v)$-consta cyclic codes over the ring $F_q + uF_q + vF_q + uvF_q$ of length n = q – 1, and another case when n is an odd integer and q is a power of the prime 2, in the light of the study of cyclic codes over the ring $F_q + uF_q + vF_q + uvF_q$[6], also in this section we obtain another gray map from the ring $(F_q + uF_q + vF_q + uvF_q)^n$ to the ring $(F_q + uF_q)^{2n}$.

2. Preliminaries

Definition 2.1. [3] Let F_q^n denote the vector space of all $n-$tuples over finite field F_q,n is the length of the vectors in F_q^n. An (n,M) code C over F_q is a subset of F_q^n of size M, that is $|C| = M$ = the number of all code words of C.

We usually write the vectors $(c_1, c_2, \ldots, c_n)$ in F^n in the form $c_1c_2\ldots c_n$ and call the vectors in C code words.

Definition 2.2. [3] If C is a $k-$dimensional subspace of F_q^n, then C will be called an $[n, k]$ linear code over F_q.

Definition 2.3. [3] Let C be a linear $[n, k]$-code. The set $C^\perp = \{x \in F_q^n \mid x.c = 0, \forall c \in C\}$.

is called the **dual code** for C, where **x.c** is the usual scalar product $x_1c_1 + x_2c_2 + \ldots + x_nc_n$ of the vectors **x** and **c**. **Note** that $C^\perp$ is an $[n, n - k]$code.

Remark: If C is a linear code of length n then $dim(C) + dim(C^\perp) = n$.

Definition 2.4. [3]

The (**Hamming distance**) $d_H(x, y)$ between two vectors $x, y \in F_q^n$ is defined to be the number of coordinates in which x and y differ.

The (**Hamming weight**) $w_H(x)$ of a vector $x \in F_q^n$ is the number of nonzero coordinates in x.

Definition 2.5. [3] For a code C containing at least two words, the minimum distance of a code C, denoted by $d(C)$, is $d(C) = \min\{d(x, y) : x, y \in C, x \,f\!= y\}$.

Definition 2.6. [3] A code C is called self-orthogonal provided $C \subseteq C^\perp$.

Definition 2.7. [3] A code C is called self-dual if $C = C^\perp$.

Remark: [3] The length n of a self-dual code C is even and the dimension of C is $n/2$.

Definition 2.8. [3] Let $c = (c_0,c_1,...,c_{n-1})$ be a word of length n, the cyclic shift $T(c)$is the word of length n

$T(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$.

Definition 2.9. [3] A code C is said to be cyclic if $T(c) \in C$, whenever $c \in C$.

Definition2.10.[4] Let $c = (c_0,c_1,...,c_{n-1})$ be a word of length n, then a $(1 + v)$-consta cyclic shift $\gamma(c)$ is a word of length n

$\gamma(c_0, c_1, ..., c_{n-1}) = ((1 + v)c_{n-1}, c_0, ..., c_{n-2})$

Definition 2.11. [4] A code C is said to be $(1 + v)$-consta cyclic if $\gamma(c) \in C$, whenever $c \in C$.

3. Linear Codes over the Ring $F_q + uF_q + vF_q + uvF_q$

In this section we will make a generalization for the work in[7]. From the ring $F_2 + uF_2 + vF_2 + uvF_2$ tothering $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p, and $u^2 = v^2 = 0$, $uv = vu$.

First lets talk about some properties of the ring $R = F_q + uF_q + vF_q + uvF_q$ which were established in [6]:

Risa Frobenius, localring with characteristic p which is not principal ideal nor chain ring. The ideals can be listed as:

$I_0 = \{0\} \subseteq I_{uv} = uv(F_q + uF_q + vF_q + uvF_q) = uvF_q \subseteq I_u, I_v, I_{u+v} \subseteq I_{u,v} \subseteq I_1 = R$, where

$I_u = u(F_q + uF_q + vF_q + uvF_q) = uF_q + u^2F_q + uvF_q + u^2vF_q = uF_q + uvF_q$,

$I_v = v(F_q + uF_q + vF_q + uvF_q) = vF_q + uvF_q + v^2F_q + uv^2F_q = vF_q + uvF_q$, $I_{u,v} = uF_q + vF_q + uvF_q$,

$I_{u+v} = (u + v)(F_q + uF_q + vF_q + uvF_q) = (u + v)F_q + u(u + v)F_q + v(u + v)F_q + uv(u + v)F_q = (u + v)F_q + (u^2 + uv)F_q + (uv + v^2)F_q + (u^2v + uv^2)F_q = (u + v)F_q + uvF_q + uvF_q = (u + v)F_q + 2uvF_q = (u + v)F_q + uvF_q$, since 2 is a unit in R.

Let $R^* = R - I_{u,v}$, we can see that R^* consists of all units in R. The unique maximal

ideal $I_{u,v}$ is not a principal ideal. $I_{u,v}$ contains all the zero divisors in R.

Remark: [6] Another nice conclusion about the ring R is that if $x = a + bu + cv + duv$ is any element in R, then $x^q = a$, where $a, b, c, d \in F_q$.

Proof. Let $x = a + bu + cv + duv \in R$, where $a, b, c, d \in F_q$. Then

If x is a nonunit then $x \in I_{u,v} = uF_q + vF_q + uvF_q$, so $a = 0$ and $x^q = 0 = a$ since

$u^2 = v^2 = 0$ and $uv = vu$.

If x is a unit then $x \in R - I_{u,v}$, so a

0 and $x^q = a^q$ since $u^2 = v^2 = 0$ and $uv = vu$, but $a \in F_q$ and $F_q - \{0\}$ is a cyclic group under multiplication of order $q - 1$ so $a^{q-1} = 1$ then $a^q = a$ so $x^q = a$.

Remark: $F_q + uF_q + vF_q + uvF_q$ is isomorphic to $F_q[X, Y]/ < X^2, Y^2, XY - YX >$.

Proof. we define a map

$f : F_q + uF_q + vF_q + uvF_q \rightarrow F_q[X, Y]/ <X^2, Y^2, XY - YX >$

s.t. $f(a + bu + cv + duv) = a + bx + cy + dxy + <X^2, Y^2, XY{-}YX>$, $\forall a + bu + cv + duv \in F_q + uF_q + vF_q + uvF_q$, now we show that f is an isomorphism as follows :

Let $h_1, h_2 \in F_q + uF_q + vF_q + uvF_q$ s.t. $h_1 = a_1 + b_1u + c_1v + d_1uv$, $h_2 = a_2 + b_2u + c_2v + d_2uv$ then:

(1) $f(h_1 + h_2) = f(a_1 + b_1u + c_1v + d_1uv + a_2 + b_2u + c_2v + d_2uv) = f((a_1 + a_2) + u(b_1 + b_2) + v(c_1 + c_2) + uv(d_1 + d_2)) = (a_1 + a_2) + (b_1 + b_2)x + (c_1 + c_2)y + (d_1 + d_2)xy + <X^2, Y^2, XY{-}YX> = a_1 + b_1x + c_1y + d_1xy + <X^2, Y^2, XY{-}YX> + a_2 + b_2x + c_2y + d_2xy + <X^2, Y^2, XY - YX> = f(h_1) + f(h_2)$.

(2) $f(h_1h_2) = f((a_1 + b_1u + c_1v + d_1uv)(a_2 + b_2u + c_2v + d_2uv))$, and after some cancelation because $u^2 = v^2 = 0$ we have

$= f(a_1a_2 + u(a_1b_2 + b_1a_2) + v(a_1c_2 + c_1a_2) + uv(a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2))$

$= a_1a_2 + (a_1b_2 + b_1a_2)x + (a_1c_2 + c_1a_2)y + (a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2)xy + <X^2, Y^2, XY{-}YX>$ $f(h_1)\, f(h_2) = (a_1 + b_1x + c_1y + d_1xy + <X^2, Y^2, XY{-}YX>)\,(a_2 + b_2x + c_2y + d_2xy + <X^2, Y^2, XY{-}YX>) = a_1a_2 + a_1b_2x + a_1c_2y + a_1d_2xy + b_1a_2x + b_1b_2x^2 + b_1c_2xy + b_1d_2x^2y + c_1a_2y + c_1b_2xy + c_1c_2y^2 + c_1d_2xy^2 + d_1a_2xy + d_1b_2x^2y + c_2d_1xy^2 + d_1d_2x^2y^2 + <X^2, Y^2, XY{-}YX>$

$= a_1a_2 + (a_1b_2 + b_1a_2)x + (a_1c_2 + c_1a_2)y + (a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2)xy + <X^2, Y^2, XY{-}YX>$

$= f(h_1h_2)$.

(3) Let $f(h_1) = f(h_2)$ that is $a_1 + b_1x + c_1y + d_1xy + <X^2, Y^2, XY{-}YX> = a_2 + b_2x + c_2y + d_2xy + < X^2, Y^2, XY - YX >$

then $(a_1 - a_2) + (b_1 - b_2)x + (c_1 - c_2)y + (d_1 - d_2)xy + <X^2, Y^2, XY{-}YX> = 0 + <X^2, Y^2, XY{-}YX>$

so $(a_1 - a_2) + (b_1 - b_2)x + (c_1 - c_2)y + (d_1 - d_2)xy \in < X^2, Y^2, XY - YX >$

and this happens if and only if $a_1 - a_2 = b_1 - b_2 = c_1 - c_2 = d_1 - d_2 = 0$

which implies $a_1 = a_2$, $b_1 = b_2$, $c_1 = c_2$, $d_1 = d_2$, then $h_1 = h_2$, so f is one to one function.

(4) Since f is one to one function and $| F_q + uF_q + vF_q + uvF_q| = | F_q[X, Y]/ <X^2, Y^2, XY{-}YX > | = q^4$, then f is onto.

From 1, 2, 3 and 4, we have proved that f is an isomorphism.

Definition 3.1. A linear code C of length $n \in N$ over the ring $F_q + uF_q + vF_q + uvF_q$ is an $F_q + uF_q + vF_q + uvF_q$- submodule of $(F_q + uF_q + vF_q + uvF_q)^n$.

Now we classify the generators of the linear codes over R and we define R-linear independence of them to introduce a possible type for linear codes over R.

There are six types of generators for linear codes over R, and we can classify them as

$\bar{a}, \bar{b}, \bar{c}, \bar{d}, \bar{e}, \bar{f}$, where

$\bar{a} \in (F_q + uF_q + vF_q + uvF_q)^n \backslash (I_{u,v})^n$,

$\bar{b} \in (I_{u,v})^n$, $\bar{b} \notin /(\mathrm{I}_u)^n, (I_v)^n, (I_{u+v})^n$,

$\bar{c} \in (I_u)^n \backslash (I_{uv})^n$,

$\bar{d} \in (I_v)^n \backslash (I_{uv})^n$,

$\bar{e} \in (I_{u+v})^n \backslash (I_{uv})^n$,

$\bar{f} \in (I_{uv})^n$.

Remark: [6] The generators of the form $\bar{a}$ contain some units.

Proof. Let $(x_1,x_2,\ldots,x_n) \in \bar{a}$ s.t. $x_i \notin /I_{u,v}$ $\forall i$ then x_i is a unit in $F_q + uF_q + vF_q + uvF_q$, so $\exists$ a unit $x^{-1} \notin /I_{u,v}$ $\forall i$, so $\exists$ $(x^{-}{}_{1_1}, x^{-}{}_{2_1}, \ldots, x^{-}{}_{n_1}) \in \bar{a}$ s.t. $(x_1,x_2,\ldots,x_n)$. $(x^{-}{}_{1_1}, x^{-}{}_{2_1}, \ldots, x^{-}{}_{n_1}) = (x_1.x^{-}{}_1{}^1,\ x_2.x^{-}{}_{2_1}, \ldots,\ x_n.x^{-}{}_{n_1}) = (1,1,\ldots,1)$ which is the unity of $(F_q + uF_q + vF_q + uvF_q)^n$, so$(x_1,x_2,\ldots,x_n)$ is a unit in $(F_q + uF_q + vF_q + uvF_q)^n$.

The generators of the form $\bar{a}$ that contain some units are called free generators.

We next define independence over R for these generators.

Definition 3.2. A subset

$$S = \{\{\bar{a}_i\}_1^{k_1}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6},\}$$

of R^n is said to be R-linearly independent if the only solution to the equation

$$\textstyle\sum_{i=1}^{k_1} \alpha_i \bar{a}_i + \sum_{j=1}^{k_2} \beta_j \bar{b}_j + \sum_{m=1}^{k_3} \gamma_m \bar{c}_m + \sum_{t=1}^{k_4} \mu_t \bar{d}_t + \sum_{r=1}^{k_5} \eta_r \bar{e}_r + \sum_{s=1}^{k_6} \zeta_s \bar{f}_s$$

where

$\alpha_i \in F_q + uF_q + vF_q + uvF_q$, $\beta_j \in F_q + uF_q + vF_q$, $\gamma_m \in F_q + vF_q$, $\mu_t \in F_q + uF_q$, $\eta_r \in$

$F_q + uF_q$, $\zeta_s \in F_q$

is

$\alpha_i, \beta_j, \gamma_m, \mu_t, \eta_r, \zeta_s = 0$ for all indices i, j, m, t, r, s.

Nowwecantakeindependentvectorsasourgeneratorstogeneratealinearcodeover$R$:

Definition 3.3. Suppose

$$S=\{\{\bar{a}_i\}_1^{k_1},\{\bar{b}_j\}_1^{k_2},\{\bar{c}_m\}_1^{k_3},\{\bar{d}_t\}_1^{k_4},\{\bar{e}_r\}_1^{k_5},\{\bar{f}_s\}_1^{k_6},\}$$

is a set of linearly independent generators as was defined above. The linear code C of length n generated by S is the submodule

$\{\sum_{i=1}^{k_1}\alpha_i\bar{a}_i+\sum_{j=1}^{k_2}\beta_j\bar{b}_j+\sum_{m=1}^{k_3}\gamma_m\bar{c}_m+\sum_{t=1}^{k_4}\mu_t\bar{d}_t+\sum_{r=1}^{k_5}\eta_r\bar{e}_r+\sum_{s=1}^{k_6}\zeta_s\bar{f}_s : \alpha_i\in F_q+uF_q+vF_q+uvF_q,$ $\beta_j\in F_q+uF_q+vF_q,\ \gamma_m\in F_q+vF_q,\ \mu_t\in F_q+uF_q,\ \eta_r\in F_q+uF_q,\ \zeta_s\in F_q\}$

In this case we say C is of type $(q^4)^{k_1}(q^3)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(q)^{k_6}$.

The following theorem will be quite useful in establishing the uniqueness of the type for codes over R.

Lemma 3.4. If $S=\{\{\bar{a}_i\}_1^{k_1},\{\bar{b}_j\}_1^{k_2},\{\bar{c}_m\}_1^{k_3},\{\bar{d}_t\}_1^{k_4},\{\bar{e}_r\}_1^{k_5},\{\bar{f}_s\}_1^{k_6}\}$ is a set of linearly independent generators which generate the linear code C, then the number of code words in C that belong to I_{nv}^n is exactly $a^{k_1+2k_2+k_3+k_4+k_5+k_6}$.

Proof. Because of the linear independence the only code words in C that belong to I_{nv}^n can arise from the binary linear combinations of

$$\{\{uv\bar{a}_i\}_1^{k_1},\{u\bar{b}_{j1}\}_1^{k_2},\{v\bar{b}_{j2}\}_1^{k_2},\{v\bar{c}_m\}_1^{k_3},\{u\bar{d}_t\}_1^{k_4},\{u\bar{e}_r\}_1^{k_5},\{\bar{f}_s\}_1^{k_6}\}$$

Again, because of linear independence, these generators will all be linearly independent over F_q. That is why we will have exactly $q^{k_1+2k_2+k_3+k_4+k_5+k_6}$ such codewords.

After this auxiliary result, we are now ready to settle the main question about the uniqueness of the type, given the existence of independent generators.

Theorem 3.5. If $S=\{\{\bar{a}_i\}_1^{k_1},\{\bar{b}_j\}_1^{k_2},\{\bar{c}_m\}_1^{k_3},\{\bar{d}_t\}_1^{k_4},\{\bar{e}_r\}_1^{k_5},\{\bar{f}_s\}_1^{k_6}\}$ is a set of linearly

independent generators which generate the linear code C, then C cannot be generated by another type, i.e. $k_1, k_2, ..., k_6$ are uniquely determined by the code.

Proof. Suppose S generates a linear code C. Then the first equation we get is about the size of the code.

$$a^{k_1+3k_2+2k_3+2k_4+2k_5+k_6}=|C|$$

If we multiply every element of the code by u, the n this will nullify some of the generators, because $uI_u=0$, $uI_{uv}=0$. Since $uI_{u,v}=uI_v=uI_{u+v}=I_{uv}$ and $u(F_2+uF_2+vF_2+uvF_2)=I_u$, the linear independence of the generators tells us that

$$a^{2k_1+k_2+k_4+k_5}=|uC|$$

Similarly we obtain

$$a^{2k_1+k_2+k_3+k_5}=|vC|$$

$$a^{2k_1+k_2+k_3+k_4}=|(u+v)C|.$$

If C_{uv} denotes the set of all code words in C that belong to I_{nv}^{n}, then by the last Lemma we see that

$$a^{k_1 + 2k_2 + k_3 + k_4 + k_5 + k_6} = | C_{uv} |.$$

Finallymultiplyingtheelementsof$R$byuvnullifieseveryelementexcepttheunits, hence we get

$$q^{k_1} = | uvC |$$

Since all the sizes on the right hand side of the equations are powers of q, we will take logarithms base q from the first to the last equation, and calling $\log_q | C | = A_1$, $\log_q | uC | = A_2$ and so on. We obtain the following system of linear equations for K_i^j s:

$$4k_1 + 3k_2 + 2k_3 + 2k_4 + 2k_5 + k_6 = A_1$$

$$2k_1 + k_2 + k_4 + k_5 = A_2$$

$$2k_1 + k_2 + k_3 + k_5 = A_3$$

$$2k_1 + k_2 + k_3 + k_4 = A_4$$

$$k_1 + 2k_2 + k_3 + k_4 + k_5 + k_6 = A_5 k_1 = A_6$$

The coefficient matrix for the system of equations is

$$\begin{pmatrix} 4 & 3 & 2 & 2 & 2 & 1 \\ 2 & 1 & 0 & 1 & 1 & 0 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

which has determinant 1. This proves the uniqueness of $k_1, k_2, ..., k_6$which means we can talk about a unique type for the code C, provided that independent generators are given for C.

Now that we have established the uniqueness of the type for linear codes over R, we can extract some further information about these codes given the type. This will help us

characterize the codes that have independent generators. To this extent, we will take a code C of type $(q^4)^{k_1}$ $(q^3)^{k_2}$ $(u)^{k_3}$ $(v)^{k_4}$ $(u + v)^{k_5}$ $(q)^{k_6}$ which has generators of the form

$$S = \{\{\bar{a}_i\}_1^{k_2}, \{\bar{b}_j\}_1^{k_2}, \{\bar{c}_m\}_1^{k_3}, \{\bar{d}_t\}_1^{k_4}, \{\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6},\}$$

that are linearly independent. The independence tells us that to obtain codewords that fall in the ideal I_{uv}, we need to take the binary combinations of

$$\{\{uv\bar{a}_i\}_1^{k_2}, \{u\bar{b}_j\}_1^{k_2}, \{v\bar{b}_j\}_1^{k_2}, \{v\bar{c}_m\}_1^{k_3}, \{u\bar{d}_t\}_1^{k_4}, \{u\bar{e}_r\}_1^{k_5}, \{\bar{f}_s\}_1^{k_6}\}.$$

Asimilarargumentcaneasilybeemployedtoseethatthecodewordsthatfallentirelyin the ideal I_u will arise from the combinations of the form

$$\sum_{i=1}^{k_1}\alpha_i\bar{a}_i+\sum_{j=1}^{k_2}\beta_j\bar{b}_j+\sum_{m=1}^{k_3}\gamma_m\bar{c}_m+\sum_{t=1}^{k_4}\mu_t\bar{d}_t+\sum_{r=1}^{k_5}\eta_r\bar{e}_r+\sum_{s=1}^{k_6}\zeta_s\bar{f}_s$$

where $\alpha_i \in uF_q + uvF_q$, $\beta_j \in uF_q + vF_q$, $\gamma_m \in F_q + vF_q$, $\mu_t \in uF_q$, $\eta_r \in uF_q$, $\zeta_s \in F_q$. This tells us that the total number of codewords in C that fall entirely in the ideal I_u is

$$a^{2k1 + 2k2 + k3 + k4 + k5 + k6} \quad ....(1)$$

For the ideal I_v, the code words that fall entirely in the ideal I_v will arise from the combinations of the form

$$\sum_{i=1}^{k_1}\alpha_i\bar{a}_i+\sum_{j=1}^{k_2}\beta_j\bar{b}_j+\sum_{m=1}^{k_3}\gamma_m\bar{c}_m+\sum_{t=1}^{k_4}\mu_t\bar{d}_t+\sum_{r=1}^{k_5}\eta_r\bar{e}_r+\sum_{s=1}^{k_6}\zeta_s\bar{f}_s$$

where $\alpha_i \in vF_q + uvF_q$, $\beta_j \in uF_q + vF_q$, $\gamma_m \in vF_q$, $\mu_t \in F_q + uF_q$, $\eta_r \in uF_q$, $\zeta_s \in F_q$. This tells us that the total number of codewords in C that fall entirely in the ideal I_v is

$$a^{2k1 + 2k2 + k3 + k4 + k5 + k6} \quad ....(2)$$

For the ideal I_{u+v}, the code words that fall entirely in the ideal I_{u+v} will arise from the combinations of the form

$$\sum_{i=1}^{k_1}\alpha_i\bar{a}_i+\sum_{j=1}^{k_2}\beta_j\bar{b}_j+\sum_{m=1}^{k_3}\gamma_m\bar{c}_m+\sum_{t=1}^{k_4}\mu_t\bar{d}_t+\sum_{r=1}^{k_5}\eta_r\bar{e}_r+\sum_{s=1}^{k_6}\zeta_s\bar{f}_s$$

where $\alpha_i \in uF_q + vF_q$, $\beta_j \in uF_q + vF_q$, $\gamma_m \in vF_q$, $\mu_t \in uF_q$, $\eta_r \in F_q + uF_q$, $\zeta_s \in F_q$. This tells us that the total number of codewords in C that fall entirely in the ideal I_{u+v} is

$$a^{2k1 + 2k2 + k3 + k4 + k5 + k6} \quad ....(3)$$

For the ideal $I_{u,v}$, for a codeword to be entirely in $I_{u,v}$ it must be of the form

$$\sum_{i=1}^{k_1}\alpha_i\bar{a}_i+\sum_{j=1}^{k_2}\beta_j\bar{b}_j+\sum_{m=1}^{k_3}\gamma_m\bar{c}_m+\sum_{t=1}^{k_4}\mu_t\bar{d}_t+\sum_{r=1}^{k_5}\eta_r\bar{e}_r+\sum_{s=1}^{k_6}\zeta_s\bar{f}_s$$

where $\alpha_i \in uF_q + vF_q + uvF_q$, $\beta_j \in F_q + uF_q + vF_q$, $\gamma_m \in F_q + vF_q$, $\mu_t \in F_q + uF_q$, $\eta_r \in F_q + uF_q$, $\zeta_s \in F_q$. which means the total number of codewords in C that fall entirely in the ideal $I_{u,v}$ is

$$a^{3k1 + 3k2 + 2k3 + 2k4 + 2k5 + k6} \quad ....(4)$$

So, combining the last Lemma with the equations (1),(2),(3) and (4) we obtain the following result:

Lemma 3.6. Let C be a linear code over the ring R of type $(q^4)^{k_1}(q^3)^{k_2}(u)^{k_3}(v)^{k_4}(u+v)^{k_5}(q)^{k_6}$. If N_{uv}, N_u, N_v, N_{u+v}, $N_{u,v}$ denote the number of code words in C that fall entirely in the ideals I_{uv}, I_u, I_v, I_{u+v}, $I_{u,v}$, respectively, then

$$\{N_{uv}, N_u, N_v, N_{u+v}, N_{u,v}\} = q^{k_1+2k_2+k_3+k_4+k_5+k_6}\{1, q^{k_1+k_3}, q^{k_1+k_4}, q^{k_1+k_5}, q^{2k_1+k_2+k_3+k_4+k_5}\}.$$

Definition 3.7. Let $\phi : (F_q + uF_q + vF_q + uvF_q)^n \rightarrow F_q^{4n}$ be the map given by

$\phi(\bar{a}+u\bar{b}+v\bar{c}+uv\bar{d}) = (\bar{a}+\bar{b}+\bar{c}+\bar{d}, \bar{c}+\bar{d}, \bar{b}+\bar{d}, \bar{d})$, where $\bar{a}, u\bar{b}, v\bar{c}, \bar{d} \in F_q^{4n}$.

We note from the definition that φ is a linear map that takes a linear code over $F_q + uF_q + vF_q + uvF_q$ of length n to a linear code of length $4n$. By using this map, we can define the Lee weight w_L as follows:

Definition 3.8. For any element $a + ub + vc + uvd \in F_q + uF_q + vF_q + uvF_q$ we define the lee weight of $a + ub + vc + uvd$ as $w_L(a + ub + vc + uvd) = w_H(a + b + c + d, c + d, b + d, d)$, where w_H denotes the ordinary Hamming weight for codes over F_q, also for any two codewords $c_1, c_2 \in F_q + uF_q + vF_q + uvF_q$ we define the lee distance $d_L(c_1, c_2) = w_L(c_1 - c_2)$.

From the definition of φ we can see that φ is a distance preserving isometry from $((F_q + uF_q + vF_q + uvF_q)^n, d_L)$ to(F^{4n}, d_H),where d_L denotes the lee distance in$(F_q + uF_q + vF_q + uvF_q)^n$ and d_H denotes the hamming distance in F_q^{4n}.

Let $F_q + uF_q + vF_q + uvF_q = \{g_1, g_2, ..., g_{q4}\}$ in some order.

Definition 3.9. The complete weight enumerator of a linear code C over $F_q + uF_q + vF_q + uvF_q$ is defined as

$$cwe_C(X_1, X_2, ..., X_{q4}) = \sum_{\bar{c} \in C} (X_1^{n_{g_1}(\bar{c})} X_2^{n_{g_1}(\bar{c})} ... X_{q4}^{n_{g_4}(\bar{c})}$$

Remark: Note that $cwe_C(X_1, X_2, ..., X_{q4})$ is a homogeneous polynomial in q^4 variables with the total degree of each term being n, the length of the code. Since $\bar{0} \in C$, we see that the term X_1^n always appears in $cwe_C(X_1, X_2, ..., X_q4)$. We also observe that $cwe_C(1, 1, ..., 1) = |C|$.

Recall that $N_u(C)$ was the number of code words in C that lie entirely in the ideal I_u, we can see that

$N_u(C) = cwe_C(x_1, x_2, ..., x_q4)$

with $x_i = 0$ when $g_i \notin /I_u$and$x_i = 1$ when $g_i \in I_u$ Similar descriptions can be given for

N_{uv}, N_v, and so on.

4. Self Dual Codes Over the Ring $F_q + uF_q + vF_q + uvF_q$

In this section we are trying to make an extension for the work in [8], from the ring $F_2 + uF_2 + vF_2 + uvF_2$ to the ring$F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p, and $u^2 = v^2 = 0$, $uv = vu$, The problem we face in this section is that some of the theorems in [8] holds only when the characteristic of the ring is 2 so it holds only for the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime 2, and other theorems in [8] hold for any commutative finite Frobenius ring so it holds for the ring $F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p.

Let $R = F_q + uF_q + vF_q + uvF_q$, where q is a power of the prime p, and lets recall definition 3.7 and definition 3.8 of the gray map φ and the lee weight w_L. Note that φ is linear and distance-preserving map thus we obtain the following lemma, which will later be useful:

Lemma 4.1. If C is a linear code over R of length n, size q^k and minimum lee distance d, then $\varphi(C)$ is an $[4n, k, d]$-linear code over F_q.

Note that if C is a linear code of length n, then $C^\perp$ is also a linear code over R of length n.

Theorem 4.2. Let C be a linear code over R of length n, where q is a power of the prime 2. Then $\varphi(C^{\perp}) \subseteq (\varphi(C))^{\perp}$ with $(\varphi(C))^{\perp}$ denoting the ordinary dual of $(\varphi(C))$ as a code over F_q.

Proof. To prove the theorem, it is enough to show that,

$\langle \bar{x}_1, \bar{x}_2 \rangle = 0 \Rightarrow \varphi(\bar{x}_1).\varphi(\bar{x}_2) = 0$ for all $\bar{x}_1, \bar{x}_2 \in (F_q + uF_q + vF_q + uvF_q)^n$.

To this extent, let's assume that $\bar{x}_1 = \bar{a}_1 + u\bar{b}_1 + v\bar{c}_1 + uv\bar{d}_1$ and that $\bar{x}_2 = \bar{a}_2 + u\bar{b}_2 + v\bar{c}_2 + uv\bar{d}_2$. Then $\langle \bar{x}_1, \bar{x}_2 \rangle = 0$ if and only if $\bar{a}_1.\bar{a}_2 = \bar{a}_1.\bar{b}_2 + \bar{a}_2.\bar{b}_1 = 0, \bar{a}_1.\bar{c}_2 + \bar{c}_1.\bar{a}_2 = 0, \bar{a}_1.\bar{d}_2 + \bar{b}_1.\bar{c}_2 + \bar{c}_1.\bar{b}_2 + \bar{d}_1.\bar{a}_2 = 0$

Now, since $\varphi(\bar{x}_1) = (\bar{a}_1 + \bar{b}_1 + \bar{c}_1 + \bar{d}_1, \bar{c}_1 + \bar{d}_1, \bar{b}_1 + \bar{d}_1, \bar{d}_1)$ and

$\varphi(\bar{x}_2) = (\bar{a}_2 + \bar{b}_2 + \bar{c}_2 + \bar{d}_2, \bar{c}_2 + \bar{d}_2, \bar{b}_2 + \bar{d}_2, \bar{d}_2)$, we get, after some cancelations because of the characteristic being 2,

$\varphi(\bar{x}_1).\varphi(\bar{x}_2) = (\bar{a}_1 + \bar{b}_1 + \bar{c}_1 + \bar{d}_1),(\bar{a}_2 + \bar{b}_2 + \bar{c}_2 + \bar{d}_2) + (\bar{c}_1 + \bar{d}_1).(\bar{c}_2 + \bar{d}_2) + (\bar{b}_1 + \bar{d}_1).(\bar{b}_2 + \bar{d}_2) + \bar{d}_1 + \bar{d}_2$

$= (\bar{a}_1.\bar{a}_2) + (\bar{a}_1.\bar{c}_2 + \bar{a}_2.\bar{c}_1) + (\bar{a}_1.\bar{b}_2 + \bar{b}_1.\bar{a}_2) + (\bar{a}_1.\bar{d}_2 + \bar{b}_1.\bar{c}_2 + \bar{c}_1.\bar{b}_2 + \bar{d}_1.\bar{a}_2) = 0$

We first start with the following lemma which is called the double-annihilator relation from [2], and holds for all Frobenius rings and in particular for our ring R, since R is a Frobenius ring

Lemma 4.3. If C is a linear code over R of length n, then $| C | . | C^{\perp} | = | R |^n = (q^4)^n$.

Theorem4.4. Suppose C is a self-dual linear code over R of length n, where q is a power of the prime 2. Then $\varphi(C)$ is a self-dual linear code of length4n.

Proof. Since C is self dual then $C = C^{\perp}$ and $| C | = | C^{\perp}|$ but by the previous Lemma, $| C |.| C^{\perp}| = (q^4)^n$ then $| C | = | C^{\perp}| = (q)^{\frac{n}{2}} = q^{2n}$, now $\varphi(C^{\perp}) = \varphi(C) \subseteq (\varphi(C))^{\perp}$ by Theorem 4.2 that is $\varphi(C)$ is self orthogonal code, also by the previous Lemma $| C | = | \varphi(C) | = q^{2n}$, and since $| \varphi(C) |.|(\varphi(C))^{\perp}| = (q)^{\frac{n}{2}}$ then $|(\varphi(C))^{\perp}| = q^{2n} = |\varphi(C)|$, combining this result with $\varphi(C) \subseteq (\varphi(C))^{\perp}$ we have $\varphi(C) = (\varphi(C))^{\perp}$, that is $\varphi(C)$ is self dual code of length 4n by Lemma4.1.

We first need an example of a self dual code over R of length n =1.

Example 4.5. Let $R = F_q + uF_q + vF_q + uvF_q$ where q is a power of the prime p and $u^2 = v^2 = 0$, $uv = vu$, and let C be the linear code of length n = 1over R generated by the element $u \in R$ which is not a unit since $u \in I_{u,v}$i.e. $C = <u>$, any element in $<u>$ has the form $u(a + bu + cv + duv) = au + bu^2 + cuv + du^2v = au + b.0 + cuv + d.0 = au + cuv$, for some $a, b, c, d \in F_q$, so $<u> = \{au + cuv : a, c \in F_q\}$ that is $|<u>| = q^2$, moreover if $au + buv, cu + duv \in <u>$then:

1) $(au + buv)^2 = a^2u^2 + 2abu^2v + b^2u^2v^2 = a^2.0 + 2ab.0.v + b^2.0.0 = 0$
2) $(au + buv)(cu + duv) = acu^2 + adu^2v + bcu^2v + bdu^2v^2 = ac.0 + ad.0.v + bc.0.v + bd.0.0 = 0$
   Hence every element of $<u>$ is orthogonal to itself and orthogonal to any other element in $<u>$ so $C \in C^{\perp}$ that is C is self orthogonal, but $| C |.| C^{\perp}| = |R|^n = |R|^1 = q^4$, and since $|C| = q^2$ then $|C^{\perp}| = q^2 = |C|$, combining this result with $C \in C^{\perp}$ we have $C = C^{\perp}$, i.e. $C = <u>$ is a self dual linear code over R of length1.

Now we need to import a lemma from [2] which holds for the ring $R = F_q + uF_q + vF_q + uvF_q$ since R is a finite Frobenius ring.

Lemma 4.6. [2] Let R be a finite Frobenius ring. Let C be a self-dual code of length n over R and D be a self-dual code of length m over R. Then the direct product $C \times D$ is a self-dual code of length n + m over R.

The existence of a self-dual code over R of length $n = 1$ implies by the last lemma that:

Theorem 4.7. Self-dual codes over R of all lengths $n \in N$ exist.

5. (1 + *v*)-Consta Cyclic Codes Over the Ring $F_q + uF_q + vF_q + uvF_q$

In this section we are trying to make an extension for the work in [10] from the ring $F_2 + uF_2 + vF_2 + uvF_2$ to the ring $F_q + uF_q + vF_q + uvF_q$ where q is a power of a prime p, $u^2 = v^2 = 0$ and $uv = vu$.

In this section we denote the ring $F_q + uF_q + vF_q + uvF_q$ as R.

Note that the element $1 + v \in R^* = R - I_{uv}$ as in section 3 which means that $1 + v$ is a unit.

The notions of cyclic and consta-cyclic shifts are standard for codes over all rings.

Briefly, for any ring R, a cyclic shift on R^n is a permutation T such that

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

A $(1 + v)$-consta cyclic shift γ acts on R^n as $\gamma(c_0, c_1, \ldots, c_{n-1}) = ((1 + v)c_{n-1}, c_0, c_1, \ldots, c_{n-2})$.

Using the polynomial representation of code words in R^n in $R[x]$, we see that for a code word $\bar{c} \in R^n$, $T(\bar{c})$ corresponds to $xc(x)$ in $R[x]/(x^n-1)$, while $\gamma(\bar{c})$ corresponds to $xc(x)$ in $R[x]/(x^n - (1 + v))$.

Proposition 5.1. (1) A subset C of R^n is a linear cyclic code of length n over R if and only if its polynomial representation is an ideal of the ring $R_n = R[x]/(x^n-1)$.

(2)A subset C of R^n is a linear $(1 + v)$-consta cyclic code of length n over R if and only if its polynomial representation is an ideal of the ring $S_n=R[x]/(x^n-(1 + v))$.

$(1 + v)$-consta cyclic codes over R where $n = q - 1$

Proposition 5.2. Let $\mu : R[x]/(x^n - 1) \to R[x]/(x^n - (1 + v))$ be defined as $\mu(c(x)) = c((1 + v)x)$.

If $n = q - 1$, then μ is a ring isomorphism from R_n to S_n.

Proof. Note that since $(1 + v) \in R$, then $(1 + v)^q = 1$ by the first Remark in section 3. Now, suppose $a(x) \equiv b(x)\ (mod(x^n-1))$, for some $a(x), b(x) \in R_n$, i.e. $a(x) - b(x) = (x^n - 1)r(x)$ for some $r(x) \in R[x]$. Then

$a((1 + v)x) - b((1 + v)x) = ((1 + v)^n x^n - 1)r((1 + v)x) = ((1 + v)^{q-1} x^n - (1 + v)^q)\, r((1 + v)x) = (1 + v)^{q-1}(x^n - (1 + v))r((1 + v)x)$, which means if $a(x) \equiv b(x)$ $(mod(x^n - 1))$, then $a((1 + v)x) \equiv b((1 + v)x)$ $(mod(x^n - (1 + v)))$, that is $\mu(a(x)) \equiv \mu(b(x))$ $(mod(x^n - (1 + v)))$, this proves that μ is well defined.

to prove the converse let

$\mu(a(x)) \equiv \mu(b(x)) mod(x^n - (1 + v))$, i.e. $a((1 + v)x) \equiv b((1 + v)x)$ $mod(x^n - (1 + v))$, that is $a((1 + v)x) - b((1 + v)x) = (x^n - (1 + v))h(x)$, fore some $h(x) \in R[x]$, now if were place x by $(1 + v)^{q-1}x$ we get:

$$a((1 + v)(1 + v)^{q-1}x) - b((1 + v)\,(1 + v)^{q-1}x) = [x^n(1 + v)^{n(q-1)} - (1 + v)]\, h((1 + v)^{q-1}x) \Rightarrow$$

$$a((1 + v)^q x) - b((1 + v)^q x) = [x^n(1 + v)^{n(q-1)} - (1 + v)]h((1 + v)^{q-1}x) \Rightarrow$$

$$\begin{aligned}
a(x) - b(x) &= [x^n(1 + v)^{(q-1)(q-1)} - (1 + v)]\, h((1 + v)^{q-1}x) \\
&= [x^n(1 + v)^{(q-1)^2} - (1 + v)]h((1 + v)^{q-1}x) \\
&= [x^n(1 + v)^{q^2-2q+1} - (1 + v)]h((1 + v)^{q-1}x) \\
&= [x^n(1 + v)^{q^2}\,(1 + v)^{-2q}(1 + v)^1 - (1 + v)]h((1 + v)^{q-1}x) \\
&= [x^n((1 + v)^q)^2((1 + v)^q)^{-2}(1 + v) - (1 + v)]h((1 + v)^{q-1}x) \\
&= [x^n(1)^2(1)^{-2}(1 + v) - (1 + v)]h((1 + v)^{q-1}x) \\
&= [x^n(1)(1)(1 + v) - (1 + v)]h((1 + v)^{q-1}x) \\
&= [x^n(1 + v) - (1 + v)]h((1 + v)^{q-1}x) \\
&= (1 + v)[x^n - 1]h((1 + v)^{q-1}x),
\end{aligned}$$

which means that $a(x) \equiv b(x)(mod(x^n - 1))$, this proves that μ is injective (one to one), so

$$a(x) \equiv b(x)(mod(x^n - 1)) \Leftrightarrow a((1 + v)x) \equiv b((1 + v)x)(mod(x^n - (1 + v))).$$

But since the rings are finite $|R_n| = |S_n|$ this proves that μ is an isomorphism.

The following is a natural corollary of the proposition:

Corollary 5.3. I is an ideal of R_n if and only if $\mu(I)$ is an ideal of S_n when $n = q - 1$.

Theorem 5.4. [6] Let C be a cyclic code over R of length n where q is the power of the prime p. Then C is an ideal of R_n that can be generated by $C = \langle g_2(x) + up_2(x) + vg_3(x) + uvp_3(x),\ ua_2(x) + vg_4(x) + uvp_4(x),\ vg_1(x) + uvp_1(x),\ uva_1(x) \rangle$ where g_i, p_i, a_i are polynomials in $F_q[x]/(x^n - 1)$with

$$a_1 \mid g_1 \mid (x^n - 1), a_1 \mid p_1 \frac{x^n - 1}{g_1}, a_2 \mid g_2 \mid (x^n - 1), a_2 \mid p_2 \frac{x^n - 1}{g_2} \mid$$

By using the last Theorem and the isomorphism μ defined above, we can classify the $(1 + v)$-consta cyclic codes over R of length $n = q - 1$:

Corollary 5.5. Let C be a $(1 + v)$-consta cyclic code over R of length $n = q - 1$ where q is a power of the prime p. then C is an ideal of $S_n = R[x]/(x^n - (1 + v))$ that can be generated by $C = \langle g_2(\tilde{x}) +$

$up_2(\tilde{x}) + vg_3(\tilde{x}) + uvp_3(\tilde{x}), ua_2(\tilde{x}) + vg_4(\tilde{x}) + uvp_4(\tilde{x}), vg_1(\tilde{x}) + uvp_1(\tilde{x}), uva_1(\tilde{x}) >$ where $\tilde{x}$ with

$= (1 + v)x$ and g_i, p_i, a_i are polynomials in $F_q[x]/(x^n - 1)$

$$a_1 \mid g_1 \mid (x^n - 1), a_1 \mid p_1 \frac{x^n - 1}{g_1}, a_2 \mid g_2 \mid (x^n - 1), a_2 \mid p_2 \frac{x^n - 1}{g_2} \mid$$

Note that if we define $\overline{\mu} : R^n \to R^n$

$\overline{\mu}(c_0, c_1, ..., c_{n-1}) = (c_0, (1 + v)c_1, (1 + v)^2 c_2, ..., (1 + v)^{n-1} c_{n-1})$

we see that $\overline{\mu}$ acts as the vector equivalent of μ on R^n. So, we can restate Corollary 5.3 in terms of vectors as well.

Corollary 5.6. Cisalinearcycliccodeover*R*of length $n = q - 1$ if and only if $\overline{\mu}(C)$ is a linear $(1 + v)$-consta cyclic code of length n over *R*.

Now lets take another especial case:

$(1 + v)$-Consta cyclic codes over *R* When q is a power of 2 If $p = 2$ then the characteristic of *R* is 2, and so

$(1 + v)^2 = 1^2 + 2v + v^2 = 1 + 0 + 0 = 1$ and also if n is any odd number then $(1 + v)^n = (1 + v)$, note that n is odd which means that $gcd(n, p) = 1$ since $p = 2$, in this case we see that things going to work may be the same as in [10].

Proposition 5.7. Let $\mu : R[x]/(x^n - 1) \to R[x]/(x^n - (1 + v))$ be defined as $\mu(c(x)) = c((1 + v)x)$.

If n is odd, then μ is a ring isomorphism from R_n to S_n.

Proof. The same proof of Proposition 3.2 in [10].

Corollary 5.8. I is an ideal of R_n if and only if $\mu(I)$ is an ideal of S_n when n is odd.

Theorem 5.9. [6] Let C be a cyclic code over R of length n where q is the power of the prime p. When $gcd(n, p) = 1$, then C is an ideal of R_n that can be generated by $C = <g_1(x) + up_1(x) + uvb_2(x), vg_2(x) + uvp_2(x) >$ where g_i, p_i, b_2 are polynomials in $F_q[x]/(x^n-1)$ with $p_1|g_1|(x^n-1)$, $p_2|g_2|(x^n-1)$, $g_2|g_1|(x^n-1)$.

By using the last Theorem and the isomorphism μ defined above, we can classify the $(1 + v)$-consta cyclic codes over *R* of odd length.

Corollary 5.10. Let C be a $(1 + v)$-consta cyclic code over R of odd length n, where q is the power of the prime 2, then C is an ideal of S_n that can be generated by $C = <g_1(\tilde{x}) + up_1(\tilde{x}) + uvb_2(\tilde{x}), vg_2(\tilde{x}) + uvp_2(\tilde{x}) >$ where $\tilde{x} = (1 + v)x$ and g_i, p_i, b_2 are polynomials in $F_q[x]/(x^n-1)$ with $p_1|g_1|(x^n-1)$, $p_2|g_2|(x^n-1)$, $g_2|g_1|(x^n-1)$.

Corollary 5.11. C is a linear cyclic code over R of odd length n if and only if $\overline{\mu}\,(C)$isa linear $(1 + v)$-consta cyclic code of length n over R.

Note that if $r = a + ub + vc + uvd \in R$, then $(1 + v)r = a + ub + v(a + c) + uv(b + d)$ which means that

$$w_L(r) = w_H((a + b + c + d, c + d, b + d, d)) = w_H(c + d, a + b + c + d, d, b + d) = w_L((1 + v)r)$$

Going back to the last Corollary, we have the following result:

Corollary 5.12. C is a cyclic code over R of parameters $[n, k, d]$ if and only if $\overline{\mu}\,(C)$ is a $(1 + v)$-consta cyclic code over R of parameters $[n, k, d]$, where n is odd.

Now let $R = F_q + uF_q + vF_q + uvF_q$ and $R_1 = F_q + uF_q$ where q is a power of the prime p.

Expressing elements of R as $a + bu + cv + duv = r + vq$, where $r = a + bu$ and $q = c + du$ are both in R_1, we see that

$$w_L(a + bu + cv + duv) = w_L(r + vq) = w_{L1}\,(q, r + q),$$

where w_L and w_{L1} denotes the Lee weight defined in R and R_1respectively. This leads to the following Gray map $\Phi : R \rightarrow R^2$

$$\Phi(a + ub + vc + duv) = \Phi(r + vq) = (q, q + r) = (c + du, a + c + (b + d)u).$$

It is easy to verify Φ is a linear map and distance preserving. We will extend Φ to R^n naturally as follows:

$$\Phi(c_1, c_2, ..., c_n) = (q_1, q_2, ..., q_n, q_1 + r_1, q_2 + r_2, ..., q_n + r_n),$$

where $c_i = r_i + vq_i$. Now we can say that Φ is a linear isometry from (R^n, Leedistance) to (R^{2n}, Leedistance).

Proposition 5.13. Let γ be the $(1 + v)$-consta cyclic shift on R^n and let T be the cyclic

shift on R^n, with Φ being the previous Gray map from R^n to R^{2n}, then we have $\Phi\gamma = T\,\Phi$.

Proof. The same proof of Proposition 4.1 in [10].

Theorem 5.14. The Gray image of a linear $(1 + v)$-consta cyclic code over R of length n is a linear cyclic cod cover R_1 of length $2n$.

Proof. the same proof of Theorem 4.2 in[10].

We finish this section with some examples

Example 5.15. Let $q = 2^2 = 4$, and let $n = 1$, then $x^1 - 1 = (x - 1).1$ in F_4, let C be the ideal in $S_1 = F_4 + uF_4 + vF_4 + uvF_4[x]/(x-(1 + v))$ generated by $C = \langle 1 + u + uv, v + uv \rangle$of length $n = 1$, Then by corollary 5.9 C is a $(1 + v)$-consta cyclic code over the ring $F_4 + uF_4 + vF_4 + uvF_4$of length $n = 1$, also by Theorem 5.13 $\Phi(C)$ is a cyclic code over $F_4 + uF_4$of length 2.

Example 5.16. Let $q = 3$, and let $n = 2 = q - 1$, then $x^2 - 1 = (x - 1)(x + 1)$ in F_3, let C be the ideal in $S_2 = F_3 + uF_3 + vF_3 + uvF_3[x]/(x^2 - (1 + v))$ generated by $C = <(\tilde{x} + 1) + u(\tilde{x} + 1), u, v(\tilde{x}$ $\tilde{x} - 1) + uv(\tilde{x} - 1), uv>$ of length $n = 2$ where $\tilde{x} = (1 + v)\, x$, Then by corollary 5.5 C is a $(1 + v)$-consta cyclic code over the ring $F_3 + uF_3 + vF_3 + uvF_3$ of length $n = 2$, also by Theorem 5.13 $\Phi(C)$ is a cyclic code over $F_3 + uF_3$ of length 4.

6. Conclusion

In the last section, we have studied (1 + v)-consta-cyclic codes over the ring $F_q + uF_q + vF_q + uvF_q$ when $n = q - 1$.

It would be interesting to investigate (1 + v)-consta-cyclic codes over the ring $F_q + uF_q + vF_q + uvF_q$ when n is odd, or when n is even.

REFERENCES

[1] I.F. Blake, Codes over certain rings, Inform. Contr. 20:396-404, 1972.

[2] S.T. Dougherty, J.L. Kim, H. Kulosman, H. Liu, Self-dual codes over commutative Frobenius rings, Finite Fields Appl., inpress,doi:10.1016/j.ffa.2009.11.004.

[3] W.C. Huffman, V. Pless, Fundementals of Error-Correcting Codes, Cambridge, U.K. Cambridge Univ. Press, 2003.

[4] J.F.Qian, L.N. Zhang, S.X. Zhu,$(1 + v)$−constacyclicandcycliccodesover$F_2 + vF_2$, Appl. Math. Lett, vol.19, pp.820-823, 2006.

[5] J.L. Walker, Algebraic Geometric Codes Over Rings, 1991.

[6] X. Xiaofang, L. Xiusheng, On the Structure of Cyclic Codes over $F_q + uF_q + vF_q + uvF_q$, J. natural sciences of wuhan university, 5, 2011.

[7] B. Yildiz, S. Karadeniz, Linear codes over $F_2 + uF_2 + vF_2 + uvF_2$, Des. Codes Crypt. 54, 2010.

[8] B. Yildiz, S.Karadeniz, Self-dual codes over $F_2 + uF_2 + vF_2 + uvF_2$, J. Frank. Inst. 347, 2010.

[9] B.Yildiz, S. Karadeniz, Cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, Des. Codes Crypt. 58, 2011.

[10] B. Yildiz, S. Karadeniz $(1 + v)$-Consta cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$, J. Frank. Inst.348, 2011.