On Linear Codes over a non-chain extension of $\mathbb{Z}_4$

Dr.Bahattin YILDIZ
Department of Mathematics, Fatih University Istanbul-TURKEY

Joint work with Dr Suat Karadeniz

June 2012

Contents

Introduction

Codes over rings have long been part of research in coding theory. Especially after the emergence of the work of Hammons et. al in 1994, a lot of research was directed towards studying codes over $\mathbb{Z}_4$. Later, these studies were mostly generalized to finite chain rings such as Galois rings and rings of the form $\mathbb{F}_2[u]/ < u^m >$, etc. But codes over $\mathbb{Z}_4$ remain a special topic of interest because of the connection with lattices, designs and cryptography. There are a lot of researchers who have studied codes over $\mathbb{Z}_4$ from different perspectives, Wolfmann, Wan, Duursma, Helleseth, Sloane, Sole, Dougherty, Huffman, Gulliver, Pless are just some of the few we can mention here.

Recently, several families of rings have been introduced in coding theory, rings that are not finite chain but are Frobenius. These rings have a rich algebraic structure and they lead to binary codes with large automorphism groups and in some cases new binary codes. The first of these rings was the rig $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ that was studied by B.Y and Karadeniz starting from 2010 and later these were generalized to an infinite family of non-chain rings which we called R_k by Dougherty, Y. and Karedniz. Karadeniz and B.Y have recently found a substantial number of new binary self-dual codes using these rings.

The connection between $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$ is very interesting. Both are commutative rings of size 4, they are both finite-chain rings and they have both been studied quite extensively in relation to coding theory. Some of the main differences between these two rings are that their characteristic is not the same, $\mathbb{F}_2$ is a subring of $\mathbb{F}_2 + u\mathbb{F}_2$ but not that of $\mathbb{Z}_4$ and the Gray images of Z_4-codes are usually not linear while the Gray images of $\mathbb{F}_2 + u\mathbb{F}_2$-codes are linear.

Inspired by this similarity(and difference), and our works on $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ we decided to look at the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$. As it turns out $\mathbb{Z}_4 + u\mathbb{Z}_4$ does look like $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ in many aspects just like $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{Z}_4$ however there are a lot of fundamental differences in their structures. This ring also leads to interesting properties in codes. Our aim in this work is to give a preliminary insight to codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$.

The ring $\mathbb{Z}_4 + u\mathbb{Z}_4$

The ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ is constructed as a commutative, characteristic 4 ring with $u^2 = 0$. The isomorphism

$$\mathbb{Z}_4 + u\mathbb{Z}_4 \cong \mathbb{Z}_4[x]/(x^2)$$

is clearly seen. The units in $\mathbb{Z}_4 + u\mathbb{Z}_4$ are given by

$$\{1, 1+u, 1+2u, 1+3u, 3, 3+u, 3+2u, 3+3u\},$$

while the non-units are given by

$$\{0, 2, u, 2u, 3u, 2+u, 2+2u, 2+3u\}.$$

It has a total of 6 ideals given by

$$\{0\} \subseteq I_{2u} = 2u(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, 2u\} \subseteq I_u, I_2, I_{2+u} \subseteq I_{2,u} \subseteq \mathbb{Z}_4 + u\mathbb{Z}_4 \tag{3.1}$$

where

$$\begin{aligned} I_u &= u(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, u, 2u, 3u\}, \\ I_2 &= 2(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, 2, 2u, 2+2u\}, \\ I_{2+u} &= (2+u)(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, 2+u, 2u, 2+3u\} \\ I_{2,u} &= \{0, 2, u, 2u, 3u, 2+u, 2+2u, 2+3u\}. \end{aligned}$$

Note that $\mathbb{Z}_4 + u\mathbb{Z}_4$ is a local ring with the unique maximal ideal given by $I_{2,u}$. The residue field is given by $(\mathbb{Z}_4 + u\mathbb{Z}_4)/I_{2,u} = \mathbb{F}_2$. Since $Ann(I_{2,u}) = \{0, 2u\}$, and this has dimension 1 over the residue field, thus we have from Wood's results that

Theorem 3.1

$\mathbb{Z}_4 + u\mathbb{Z}_4$ is a local Frobenius ring.

However, since the ideal $\langle 2, u \rangle$ is not principal and the ideals $\langle 2 \rangle$ and $\langle u \rangle$ are not related via inclusion, $\mathbb{Z}_4 + u\mathbb{Z}_4$ is not a finite chain ring nor is it a principal ideal ring.

We divide the units of $\mathbb{Z}_4 + u\mathbb{Z}_4$ into two groups $\mathfrak{U}_1$ and $\mathfrak{U}_2$ calling them units of first type and second type, respectively, as follows:

$$\mathfrak{U}_1 = \{1, 3, 1 + 2u, 3 + 2u\} \tag{3.2}$$

and

$$\mathfrak{U}_2 = \{1 + u, 3 + u, 1 + 3u, 3 + 3u\}. \tag{3.3}$$

The reason that we distinguish between the units is the following observation that can easily be verified:

$$\forall a \in \mathbb{Z}_4 + u\mathbb{Z}_4, \quad a^2 = \begin{cases} 0 & \text{if } a \text{ is a non-unit} \\ 1 & \text{if } a \in \mathfrak{U}_1 \\ 1 + 2u & \text{if } a \in \mathfrak{U}_2. \end{cases} \tag{3.4}$$

Linear Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

Definition 4.1

A linear code C of length n over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ is an $\mathbb{Z}_4 + u\mathbb{Z}_4$-submodule of $(\mathbb{Z}_4 + u\mathbb{Z}_4)^n$.

Since $\mathbb{Z}_4 + u\mathbb{Z}_4$ is not a finite chain ring, we cannot define a standard generating matrix for linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$.
Define $\phi : (\mathbb{Z}_4 + u\mathbb{Z}_4)^n \to \mathbb{Z}_4^{2n}$ by

$$\phi(\bar{a} + u\bar{b}) = (\bar{b}, \bar{a} + \bar{b}), \quad \bar{a}, \bar{b} \in \mathbb{Z}_4^n. \tag{4.1}$$

We now define the Lee weight w_L on $\mathbb{Z}_4 + u\mathbb{Z}_4$ by letting

$$w_L(a + ub) = w_L(b, a + b),$$

where $w_L(b, a + b)$ describes the usual Lee weight on $\mathbb{Z}_4^2$. The Lee distance is defined accordingly. Note that with this definition of the Lee weight and the Gray map we have the following main theorem:

Theorem 4.2

$\phi : (\mathbb{Z}_4 + u\mathbb{Z}_4)^n \to \mathbb{Z}_4^{2n}$ is a distance preserving linear isometry. Thus, if C is a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n, then $\phi(C)$ is a linear code over $\mathbb{Z}_4$ of length $2n$ and the two codes have the same Lee weight enumerators.

MacWilliams Identities

Define the usual inner product as

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= x_1y_1 + x_2y_2 + \cdots + x_ny_n \quad (5.1)$$

where the operations are performed in the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$. Then the dual of a code can be defined accordingly:

Definition 5.1

Let C be a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n, then we define the *dual* of C as

$$C^{\perp} := \{\overline{y} \in (\mathbb{Z}_4 + u\mathbb{Z}_4)^n | < \overline{y}, \overline{x} >= 0, \quad \forall \overline{x} \in C\}.$$

Let $\mathbb{Z}_4 + u\mathbb{Z}_4 = \{g_1, g_2, \ldots, g_{16}\}$ be given as

$$\mathbb{Z}_4 + u\mathbb{Z}_4 = \{0, u, 2u, 3u, 1, 1+u, 1+2u, 1+3u, 2, 2+u, \cdots\}.$$

Definition 5.2

The complete weight enumerator of a linear code C over $\mathbb{Z}_4 + u\mathbb{Z}_4$ is defined as

$$cwe_C(X_1, X_2, \ldots, X_{16}) = \sum_{\bar{c} \in C} (X_1^{n_{g_1}(\bar{c})} X_2^{n_{g_2}(\bar{c})} \ldots X_{16}^{n_{g_{16}}(\bar{c})})$$

where $n_{g_i}(\bar{c})$ is the number of appearances of g_i in the vector $\bar{c}$.

Remark 1

Note that $cwe_C(X_1, X_2, \ldots, X_{16})$ is a homogeneous polynomial in 16 variables with the total degree of each monomial being n, the length of the code. Since $\bar{0} \in C$, we see that the term X_1^n always appears in $cwe_C(X_1, X_2, \ldots, X_{16})$.

Now, since $\mathbb{Z}_4 + u\mathbb{Z}_4$ is a Frobenius ring, the MacWilliams identities for the complete weight enumerator hold. To find the exact identities we define the following character on $\mathbb{Z}_4 + u\mathbb{Z}_4$:

Definition 5.3

Define $\chi : \mathbb{Z}_4 + u\mathbb{Z}_4 \to C^{\times}$ by

$$\chi(a + bu) = i^{a+b}.$$

It is easy to verify that ϕ is a non-trivial character when restricted to each non-zero ideal, hence it is a generating character for $\mathbb{Z}_4 + u\mathbb{Z}_4$.

Then we make up the 16×16 matrix T, by letting $T(i,j) = \chi(g_i g_j)$:

$$
T = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & i & i & i & i & -1 & -1 & -1 & -1 & -i & -i & -i & -i \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & 1 & -i & -i & -i & -i & -1 & -1 & -1 & -1 & i & i & i & i \\
1 & i & -1 & -i & i & -1 & -i & 1 & -1 & -i & 1 & i & -i & 1 & i & -1 \\
1 & i & -1 & -i & -1 & -i & 1 & i & 1 & i & -1 & -i & -1 & -i & 1 & i \\
1 & i & -1 & -i & -i & 1 & i & -1 & -1 & -i & 1 & i & i & -1 & i & 1 \\
1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & i \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & i & -i & i & -i \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & i & -i & i & -i & -1 & 1 & -1 & 1 & -i & i & -i & i \\
1 & -i & -1 & i & -i & -1 & i & 1 & -1 & i & 1 & -i & i & 1 & -i & -1 \\
1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i \\
1 & -i & -1 & i & i & 1 & i & -1 & -1 & i & 1 & -i & -i & -1 & i & 1 \\
1 & -i & -1 & i & -1 & i & 1 & -i & 1 & -i & -1 & i & -1 & i & 1 & -i
\end{bmatrix}.
$$

Now using Wood's general results on Frobenius rings we obtain the MacWilliams identities for the complete weight enumerators:

Theorem 5.4

Let C be a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n and suppose $C^\perp$ is its dual. Then we have

$$cwe_{C^\perp}(X_1, X_2, \dots, X_{16}) = \frac{1}{|C|} cwe_C(T \cdot (X_1, X_2, \dots, X_{16})^t),$$

where $()^t$ denotes the transpose.

But we would like to obtain the MacWilliams identities for the Lee weight enumerators just like in $\mathbb{Z}_4$. To this end we identify the elements in $\mathbb{Z}_4 + u\mathbb{Z}_4$ that have the same Lee weight to write up the symmetrized weight enumerator. To do this we need the following table which gives us the elements of $\mathbb{Z}_4 + u\mathbb{Z}_4$, their Lee weights and the corresponding variables:

a	Lee Weight of a	The corresponding variable
0	0	X_1
u	2	X_2
2u	4	X_3
3u	2	X_4
1	1	X_5
1+u	3	X_6
1+2u	3	X_7
1+3u	1	X_8
2	2	X_9
2+u	2	X_{10}
2+2u	2	X_{11}
2+3u	2	X_{12}
3	1	X_{13}
3+u	1	X_{14}
3+2u	3	X_{15}
3+3u	3	X_{16}

So, looking at the elements that have the same weights we can define the symmetrized weight enumerator as follows:

Definition 5.5

Let C be a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n. Then define the symmetrized weight enumerator of C as

$$swe_C(X,Y,Z,W,S) = cwe_C(X,S,Y,S,W,Z,Z,W,S,S,S,S,W,W,Z,Z). \tag{5.2}$$

Here X represents the elements that have weight 0 (the 0 element); Y represents the elements with weight 4 (the element $2u$); Z represents the elements of weight 3 (the elements $1+u$, $1+2u$, $3+2u$ and $3+3u$; W represents the elements of weight 1 (the elements 1, $1+3u$, 3 and $3+u$)) and finally S represents the elements of weight 2 (the elements 2, u, $3u$, $2+u$, $2+2u$ and $2+3u$).

Now, combining Theorem 5.4 and the definition of the symmetrized weight enumerator, we obtain the following theorem:

Theorem 5.6

Let C be a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n and let $C^\perp$ be its dual. Then we have

$$swe_{C^\perp}(X,Y,Z,W,S) =$$

$$\frac{1}{|C|} swe_C(6S+4W+X+Y+4Z, 6S-4W+X+Y-4Z,$$

$$-2W+X-Y+2Z, 2W+X-Y-2Z, -2S+X+Y).$$

We next define the Lee weight enumerator of a code over $\mathbb{Z}_4 + u\mathbb{Z}_4$:

Definition 5.7

Let C be a linear code over $\mathbb{Z}_4$. Then the Lee weight enumerator of C is given by

$$Lee_C(W,X) = \sum_{\bar{c}\in C} W^{4n-w_L(\bar{c})} X^{w_L(\bar{c})}. \tag{5.3}$$

Considering the weights that the variables X, Y, Z, W, S of the symmetrized weight enumerator represent, we easily get the following theorem

Theorem 5.8

Let C be a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n. Then

$$Lee_C(W,X) = swe_C(W^4, X^4, WX^3, W^3X, W^2X^2).$$

Now combining Theorem 5.6 and Theorem 5.8 we obtain the following theorem:

Theorem 5.9

Let C be a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ *of length* n *and* $C^{\perp}$ *be its dual. With* $Lee_C(W, X)$ *denoting its Lee weight enumerator as was given in (5.3), then we have*

$$Lee_{C^{\perp}}(W, X) = \frac{1}{|C|} Lee_C(W + X, W - X).$$

Self-dual Codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

We start by recalling that a linear code C over $\mathbb{Z}_4 + u\mathbb{Z}_4$ is called self-orthogonal if $C \subseteq C^{\perp}$ and it will be called self-dual if $C = C^{\perp}$. Since the code of length 1 generated by u is a self-dual code over $\mathbb{Z}_4 + u\mathbb{Z}_4$, by taking the direct sums, we see that

Theorem 6.1

Self-dual codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of any length exist.

The next observation is in the form of the following theorem:

Theorem 6.2

(i) *If C is self-orthogonal, then for every codeword $\bar{c} \in C$, $n_{\mathfrak{U}_i}(\bar{c})$ must be even. Here, $n_{\mathfrak{U}_i}(\bar{c})$ denotes the number of units of the ith type(in $\mathfrak{U}_i$) that appear in $\bar{c}$*

(ii) *If C is self-dual of length n, then the all $2u$-vector of length n must be in C.*

Define two maps from $(\mathbb{Z}_4 + u\mathbb{Z}_4)^n$ to $\mathbb{Z}_4^n$ as follows:

$$\mu(\bar{a} + u\bar{b}) = \bar{a} \tag{6.1}$$

and

$$\nu(\bar{a} + u\bar{b}) = \bar{a} + u\bar{b} - \mu(\bar{a} + u\bar{b}) = \bar{b}. \tag{6.2}$$

Since these maps are linear, we see that

Theorem 6.3

If C is a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n, then $\mu(C)$ and $\nu(C)$ are both linear codes over $\mathbb{Z}_4$ of length n.

The following theorem describes the self-dual codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$:

Theorem 6.4

Let C be a self-dual code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length n. Then
a) $\phi(C)$ *is a formally self-dual code over $\mathbb{Z}_4$ of length $2n$.*
b) $\mu(C)$ *is a self-orthogonal code over $\mathbb{Z}_4$ of length n.*
c) *If $\nu(C)$ is self-orthogonal, then $\phi(C)$ is a self-dual code of length $2n$.*

Examples

1. Let C be the linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 4 generated by the vectors

$$\{(u,u,u,u),(1,1,1,1+2u),(0,2+u,2,3u),(0,2,u,2+3u)\}.$$

Then C is a self-dual code of size 256 with Lee weight enumerator $1+112z^6+30z^8+112z^{10}+z^{16}$ and $\phi(C)$ is equivalent to the well known $\mathbb{Z}_4$-Kerdock code $\mathcal{K}_3$, also known as the octacode.

2. Let C be the linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 6 generated by the vectors

$(2+2u, 1+2u, 1, 1+3u, 1+2u, 0), (3+2u, 3+u, 3+u, 1+3u, 1+3u, 3+u)$

and $(3+3u, 2+3u, 3+3u, 3u, 2, 2u)$. Then C is a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 6 of size 2^{12} and minimum Lee weight 6, whose Gray image is the best known $\mathbb{Z}_4$-code of the same parameters.

3. Let C be the linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 7 generated by the vectors $(3+u, 1+3u, 1, 1, 0, 3+2u, 3+2u)$,
$(1+3u, 1+2u, 2+u, 2+2u, 3+2u, 2+u, 3+2u)$ and
$(3+2u, 3+2u, 1+u, 2u, 2+2u, 2, 1)$. Then C is a linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 7 of size 2^{12} and minimum Lee weight 8 whose Gray image is the best known $\mathbb{Z}_4$-code of the same parameters.

4. Let C be the linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 8 generated by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 2+2u & 1 & 1+2u \\ 0 & 1 & 0 & 0 & 2+2u & 3 & 3+2u & 1 \\ 0 & 0 & 1 & 0 & 3 & 3+2u & 1+2u & 2 \\ 0 & 0 & 0 & 1 & 1+2u & 3 & 2 & 3+2u \end{bmatrix}.$$

Then C is a self-dual code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with Lee weight enumerator

$$1 + 380z^8 + 1920z^{10} + 7168z^{12} + 13440z^{14} + 1978z^{16} + \cdots$$

where the rest is completed via symmetry. $\phi(C)$ is a self-dual code over $\mathbb{Z}_4$ of type $(4)^8$ with the same weight enumerator.

5. Let C be the linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 8 generated by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1+2u & 2+u & 1 & 1+2u \\ 0 & 1 & 0 & 0 & 2+u & 3+2u & 3+2u & 1 \\ 0 & 0 & 1 & 0 & 3+2u & 3 & 1+2u & 2+3u \\ 0 & 0 & 0 & 1 & 1 & 3+2u & 2+3u & 3+2u \end{bmatrix}.$$

Then C is a self-dual code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with Lee weight enumerator

$$1 + 492z^8 + 1024z^{10} + 10304z^{12} + 71680z^{14} + 27558z^{16} + \cdots$$

where the rest is completed via symmetry. The Gray image $\phi(C)$ is a not a self-dual code over $\mathbb{Z}_4$, but it is a formally self-dual code of type $(4)^8$ with the same weight enumerator.

6. Let C be the linear code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ of length 8 generated by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1+3u & 2 & 1+u & 1 \\ 0 & 1 & 0 & 0 & 2+2u & 3+3u & 3 & 1+3u \\ 0 & 0 & 1 & 0 & 3+3u & 3 & 1+3u & 2 \\ 0 & 0 & 0 & 1 & 1 & 3+u & 2+2u & 3+3u \end{bmatrix}.$$

Then C is a self-dual code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with Lee weight enumerator

$$1 + 508z^8 + 896z^{10} + 10752z^{12} + 6272z^{14} + 28678z^{16} + \cdots$$

where the rest is completed via symmetry. The Gray image $\phi(C)$ is a not a self-dual code over $\mathbb{Z}_4$, but it is a formally self-dual code of type $(4)^8$ with the same weight enumerator.

THANK YOU FOR YOUR PATIENCE