Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 347–351*

On linear codes over a non-chain extension of $\mathbb{Z}_4$

Bahattin Yildiz byildiz@fatih.edu.tr
Fatih University
Suat Karadeniz skaradeniz@fatih.edu.tr
Fatih University

Abstract. In this paper we discuss linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, which is a natural extension of the ring $\mathbb{Z}_4$. But unlike $\mathbb{Z}_4$ and many other rings studied in coding theory, $\mathbb{Z}_4 + u\mathbb{Z}_4$ is not a finite chain ring. It is however a Frobenius ring with a non-trivial generating character and it leads to MacWilliams identites. We use the MacWilliams identities to construct formally self-dual codes over $\mathbb{Z}_4$. We present some examples.

1 Introduction

Codes over rings have long been part of research in coding theory. Especially after the emergence of [5], 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. For some of the works done in this direction we refer to [3], [4], [6], [8], [9], etc.

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 ([11], [2]).

In this work, we introduce the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$, which is a non-chain, characteristic 4 ring of size 16, with an ideal structure similar to $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. We introduce a Gray map and Lee weight for codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ and we give the MacWilliams identity for the Lee weight enumerators of these codes. We then prove that the Gray image of self-dual codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ are formally self-dual linear codes over $\mathbb{Z}_4$ and we give some examples to good $\mathbb{Z}_4$-codes that are Gray images of codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$.

2 Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

The ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ is constructed as a commutative, characteristic 4 ring with $u^2 = 0$. It is also isomorphic as a ring to the polynomial ring $\mathbb{Z}_4[x]/\langle x^2\rangle$. 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

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

The ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ has a total of 6 ideals given by

$$I_0 = \{0\} \subseteq I_{2u} = 2u(\mathbb{Z}_4 + u\mathbb{Z}_4) = \{0, 2u\} \subseteq I_u, I_2, I_{2+u} \subseteq I_{2,u} \subseteq I_1 = \mathbb{Z}_4 + u\mathbb{Z}_4 \tag{1}$$

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 $I_{2,u}$ and that it is a Frobenius ring. Thus it is a feasible ring for coding theory by [10].

Definition 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 $(\mathbb{Z}_4 + u\mathbb{Z}_4)^n$.*

Define $\phi : (\mathbb{Z}_4 + u\mathbb{Z}_4)^n \to \mathbb{Z}_4^{2n}$ by

$$\phi(\overline{a} + u\overline{b}) = (\overline{b}, \overline{a} + \overline{b}), \quad \overline{a}, \overline{b} \in \mathbb{Z}_4^n. \tag{2}$$

Then define the Lee weight on $\mathbb{Z}_4 + u\mathbb{Z}_4$ by

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

where $w_L((b, a+b))$ describes the usual Lee weight on $\mathbb{Z}_4^2$. Since the Gray map is linear and distance-preserving we have

Theorem 1. *$\phi : (\mathbb{Z}_4 + u\mathbb{Z}_4)^n \to \mathbb{Z}_4^{2n}$ 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.*

3 MacWilliams identities

Definition 2. *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*

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

Here, $<>$ denotes the usual Euclidean inner product.

Then since $\mathbb{Z}_4 + u\mathbb{Z}_4$ is a Frobenius ring there is a MacWilliams identity for the complete weight enumerator of linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$([10]). If we apply the MacWilliams identity to the Lee weight enumerator, we obtain

Theorem 2. *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, we have*

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

This then leads to the following theorem for self-dual codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$:

Theorem 3. *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) *The all $2u$-vector of length n must be in C.*

4 Some examples

- 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 Kerdock code $\mathcal{K}_3$, also known as the octacode.

- 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.

- 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.

- 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.

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

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

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.

- 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.

References

[1] S.T. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, Type IV self-dual codes over rings, *IEEE Trans. Inform. Theory*, **45**, 2345–2360, 1999.

[2] S.T.Dougherty, B.Yildiz and S.Karadeniz, Codes over R_k, Gray Maps and their Binary Images, *Finite Fields Appl.*, **17**, 205–219, 2011.

[3] I.M. Duursma, M. Greferath and S. E. Schmidt, On the Optimal $\mathbb{Z}_4$-codes of TypeII and length 16, *J. Combin. Theory, Series A*, **92** 77–82, 2000.

[4] T.A. Gulliver and M. Harada, Optimal Double Circulant $\mathbb{Z}_4$-codes, *LNCS:AAECC*, **2227**, 122-128, 2001.

[5] A.R. Hammons, V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, **40** 301–319, 1994.

[6] W.C. Huffman, Decompositions and extremal Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, **44**, 800–809, 1998.

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

[8] Z.X. Wan, *Series on Applied Mathematics:Quaternary Codes*, World Scientific, 1997.

[9] J.Wolfmann, Negacyclic and Cyclic Codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, **45**, 2527–2532, 1999.

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

[11] B. Yildiz and S. Karadeniz, Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, *Des. Codes Crypt.*, **54**, 61–81, 2010.