Int. J. Contemp. Math. Sciences, Vol. 5, 2010, no. 12, 595 - 602

Type II Codes over $F_2 + uF_2 + u^2F_2 + u^3F_2 + ... + u^mF_2$

Yasemin Cengellenmis

Department of Mathematics
Faculty of Science and Arts
Trakya University, 22030 Edirne, Turkey
ycengellenmis@yahoo.com

Abstract

We define Type II codes over $R = F_2+uF_2+u^2F_2+u^3F_2+....+u^mF_2$, $m = 2k, k \in N$.It is examined the existense of self dual code over R and we have the Gray images of the Type II codes over R.

Mathematics Subject Classificition: 94B05

Keywords: Gray map;Type II codes;Self Dual codes

1. Introduction

Recently, self dual code over rings have received much attention. In [4], they studied Type II codes over $F_2 + uF_2$. Type II codes over $F_4 + uF_4$ were studied in [6]. In [2], Type II codes over $F_{2^m} + uF_{2^m}$ were studied. In [7], they defined Type II codes over $F_2+uF_2+u^2F_2$ as self dual codes with Lee weight a multiple of 4 and they examined the existence of self dual code $F_2+uF_2+u^2F_2$. Morever , they defined a Gray map from $F_2 + uF_2 + u^2F_2$ to F_2 and studied the properties of Type II codes in this rings.

In this paper, it is defined Type II codes over $F_2 + uF_2 + u^2F_2 + u^3F_2 + ... + u^mF_2$, $m = 2k, k \in N$. It is examined the existense of self dual code over

R. We had defined a Gray map from $F_2 + uF_2 + u^2F_2 + u^3F_2 + ... + u^mF_2$ to F_2 in [3]. By using this, we study the properties of the Type II code over R.

2. Preliminaries

Let R be the commutative ring $F_2 + uF_2 + u^2F_2 + u^3F_2 + ... + u^mF_2 := F_2[u]/\langle u^{m+1}\rangle$ where $m = 2k, k \in N$. The ring is endowed with the obvious addition and multiplication with the property that $u^{m+1} = 0$. Then R is a finite chain ring with maximal ideal uR. Since u is nilpotent with nilpotent index $m + 1$, we have

$$R \subset (uR) \subset (u^2R) \ldots \subset (u^{m+1}R) = 0$$

Morever $R/uR \cong F_2$ and $|(u^iR)| = 2|(u^{i+1}R)| = 2^{(m+1)-i}, i = 0, 1, 2, ..., m$.

A linear code C over R of length n is a R-submodule of R^n. A element of C is called a codeword.The Hamming weight $wt_H(c)$ of a codeword c is the number of nonzero components. The minimum weight $wt_H(c)$ of a code C is the smallest weight among all its nonzero codewords.

For $x = (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in R^n$, $d_H(x, y) = |\{i|x_i \neq y_i\}|$ is called Hamming distance between any distinct vectors $x, y \in R^n$ is denoted

$$d_H(x, y) = wt_H(x - y)$$

The minimum Hamming distance between distinct pairs of codewords of a code C is called minimum distance of C and denoted by $d_H(C)$ or simply d_H.

If C is a linear code, then $d_H(C) = wt_H(C)$.

The definition Lee weight of an element $r \in R$ is analogous to the definition of the Lee weight of the element of the ring $Z_{2^{m+1}}$.

For example, if $M = F_2 + uF_2 + u^2F_2 = \{0, 1, u, u^2, v, v^2, uv, v^3\}$ where $u^3 = 0, v = 1 + u, v^2 = 1 + u^2, uv = u + u^2, v^3 = 1 + u + u^2$, the Lee weight a_r of an element r of the ring M is given by the following equations

$$a_r = \begin{cases} 0 & \text{if} \quad r = 0 \\ 1 & \text{if} \quad r = 1 \quad \text{or} \quad r = v^2 \\ 2 & \text{if} \quad r = u \quad \text{or} \quad r = uv \\ 3 & \text{if} \quad r = v \quad \text{or} \quad r = v^3 \\ 4 & \text{if} \quad r = u^2 \end{cases}$$

The definition is analogous to the definition of the Lee weight of the elements of the ring Z_8 where $a_0 = 0, a_1 = a_7 = 1, a_2 = a_6 = 2, a_3 = a_5 = 3, a_4 = 4$.

The Lee weight of an element $x = (x_1, x_2, ..., x_n) \in R^n$ is

$$wt_L(x) = \sum_{i=1}^{n} a_r$$

The Lee distance between $x, y \in R^n$ is denoted $d_L(x, y) = wt_L(x - y)$. The minimum Lee distance d_L of a code C is defined analogously.[1]

Given $x = (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in R^n$ their scalar pruduct is,

$$xy = x_1y_1 + x_2y_2 + \ldots + x_ny_n$$

Two words x, y are called orthogonal if $xy = 0$. For the code C over R, its dual $C^\perp$ is defined as follows,

$$C^\perp = \{x | xy = 0, \forall y \in C\}$$

If $C \subseteq C^\perp$,we say that the code is self-orthogonal and , $C = C^\perp$ we say that the code is self dual. Two codes are equivalent if one can be obtained from the other permuting the coordinates.

Any code over R is permutation equivalent to a code C with generator matrix of the form,

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \dots & A_{0,m+1} \\ 0 & uI_{k_1} & uA_{1,2} & \dots & uA_{1,m+1} \\ 0 & 0 & u^2I_{k_2} & \dots & u^2A_{2,m+1} \\ 0 & 0 & 0 & \dots & u^3A_{3,m+1} \\ \vdots & \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & 0 & \dots & u^mA_{m,m+1} \end{pmatrix}$$

where the matrices $A_{i,j}$ are binary matrices. A code with a generator matrix in this form is of type $\{k_0, k_1, \dots, k_m\}$ and has $2^{(m+1)k_0+mk_1+\cdots+k_m}$ vectors.[8]

We had defined the Gray map ϕ in [3], as follows,

$$\phi : R^n \to F_2^{2^m n}$$

$$\begin{aligned} x_0 + ux_1 + u^2x_2 + ... + u^m x_m \mapsto (&x_m, x_m + x_0, x_m + x_1, x_m + x_1 + x_0, \\ &x_2 + x_m, x_2 + x_m + x_0, x_1 + x_2 + x_m, x_0 + x_1 + x_2 + x_m, \\ &x_3 + x_m, x_0 + x_3 + x_m, x_1 + x_3 + x_m, x_0 + x_1 + x_3 + x_m, \\ &x_2 + x_3 + x_m, x_0 + x_2 + x_3 + x_m, x_1 + x_2 + x_3 + x_m, x_0 + x_1 + x_2 + x_3 + x_m, \\ &x_4 + x_m, x_0 + x_4 + x_m, x_1 + x_4 + x_m, x_0 + x_1 + x_4 + x_m, x_2 + x_4 + x_m, \\ &x_0 + x_2 + x_4 + x_m, x_1 + x_2 + x_4 + x_m, x_0 + x_1 + x_2 + x_4 + x_m, \\ &x_3 + x_4 + x_m, x_0 + x_3 + x_4 + x_m, x_1 + x_3 + x_4 + x_m, \\ &x_0 + x_1 + x_3 + x_4 + x_m, x_2 + x_3 + x_4 + x_m, x_0 + x_2 + x_3 + x_4 + x_m, \\ &x_1 + x_2 + x_3 + x_4 + x_m, x_0 + x_1 + x_2 + x_3 + x_4 + x_m, \\ &\dots, \dots, \dots, ..., x_0 + x_1 + x_2 + x_3 + x_4 + ... + x_m) \end{aligned}$$

where $x_i = (x_0^i, x_1^i, \dots, x_{n-1}^i) \in F_2^n, i = 0, 1, 2, \dots, m$.

Proposition 2.1 The Gray map ϕ is distance preserving map or an isometry from (R^n, d_L) to $F_2^{2^m n}$ under the Hamming distance.

3.Self dual codes over R

In [5], they defined higher torsion codes. We follow the definition given there as in [7].

For the code C over R, we define the following torsion codes over F_2. For $i = 0, 1, 2, \dots, m$, define

$$Tor_i(C) = \{v | u^i v \in C\}$$

In general we note that

$$Tor_0(C) \subseteq Tor_1(C) \ldots \subseteq Tor_m(C)$$

If $i = 0$,$Tor_i(C)$ is called the residue code and is often denoted by $Res(C)$. In particular for a code over R with the following generator matrix

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \ldots & A_{0,m+1} \\ 0 & uI_{k_1} & uA_{1,2} & \ldots & uA_{1,m+1} \\ 0 & 0 & u^2 I_{k_2} & \ldots & u^2 A_{2,m+1} \\ 0 & 0 & 0 & \ldots & u^3 A_{3,m+1} \\ \vdots & \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & 0 & \ldots & u^m A_{m,m+1} \end{pmatrix}$$

the code $Res(C) = Tor_0(C)$ is the binary code generated by

$$\begin{pmatrix} I_{k_0} & \bar{A}_{0,1} & \bar{A}_{0,2} & \ldots & \bar{A}_{0,m+1} \end{pmatrix}$$

where $\bar{A}_{0,j}$ is the reduction modulo u of $A_{0,j}$ for $j = 1, 2, ..., m + 1$

The code $Tor_1(C)$ is the binary code generated by

$$\begin{pmatrix} I_{k_0} & \bar{A}_{0,1} & \bar{A}_{0,2} & \ldots & \bar{A}_{0,m+1} \\ 0 & I_{k_1} & A_{1,2} & \ldots & A_{1,m+1} \end{pmatrix}$$

and the code $Tor_i(C), s = 2, 3, ..., m$ is the binary code generated by

$$\begin{pmatrix} I_{k_0} & \bar{A}_{0,1} & \bar{A}_{0,2} & \ldots & \bar{A}_{0,m+1} \\ 0 & I_{k_1} & A_{1,2} & \ldots & A_{1,m+1} \\ 0 & 0 & I_{k_2} & \ldots & A_{2,m+1} \\ 0 & 0 & 0 & \ldots & A_{3,m+1} \\ \vdots & \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & \ldots & I_{k_s} & A_{s,m+1} \end{pmatrix}$$

A code C over R has $2^{(m+1)k_0+mk_1+\cdots+k_m}$ elements and that

$$|Tor_0(C)||Tor_1(C)| \ldots |Tor_m(C)| = 2^{k_0} 2^{k_0+k_1} \ldots 2^{k_0+k_1+\ldots+k_m}$$

then we have

$$|C| = |Tor_0(C)||Tor_1(C)| \ldots |Tor_m(C)|$$

Lemma 3.1 If C is a self-orthogonal code over R, then $Res(C) = Tor_0(C)$ is a self-orthogonal code over F_2.

Proof: If $[a, \acute{a}] = 0$ in R, then $[a(modu), \acute{a}(modu)] = 0$ in F_2.

As a similar, it can be shown that $Tor_i(C)$ self-orthogonal code over F_2, $i = 1, 2, \ldots, m$.

If C is a code over R of type $\{k_0, k_1, \ldots, k_m\}$ where $m = 2k, k \in N$, then $C^{\perp}$has type $\{n - k_0 - k_1 - \cdots - k_m, k_m, k_{m-1}, \ldots, k_1\}$. So we have

Theorem 3.2 Let C be a self dual code over R of type $\{k_0, k_1, \ldots, k_m\}$. Then $k_i = k_{(m+1)-i}$ for $i = 1, 2, 3, \ldots, m/2$ and $k_0 + k_1 + \cdots + k_{m/2} = n/2$.

Proof: As C is self dual code over R, therefore two type must be equal. So, we have $k_i = k_{(m+1)-i}$ for $i = 1, 2, 3, \ldots, m/2$. Then, if we apply this to the first coordinate in the type, we have $k_0 + k_1 + \cdots + k_{m/2} = n/2$.

Theorem 3.3 [9] Self dual codes of length n exist over F_2 if and only if n is even.

Corollary 3.4 Self dual codes of length n exist over R if and only if n is even .

In this section we study the Gray image of the Type II code over R.

4. The Gray image of type II code over R

Theorem 4.1 Let C be a code of length n over R. If C is self-orthogonal, so is $\phi(C)$. A code C is of Type II code over R if and only if $\phi(C)$ is a Type II code over F_2 The minimum Lee weight of C is equal to the minimum Hamming weight of $\phi(C)$.

Proof: Let $a = a_0 + ua_1 + ... + u^m a_m, b = b_0 + ub_1 u + ... + u^m b_m$ be codewords in C.With Euclidean inner product,

$$ab = a_0 b_0 + (a_0 b_1 + a_1 b_0)u + ... + u^m (a_0 b_m + a_1 b_{m-1} + ... + a_m b_0) = 0$$

Then we have

$$a_0 b_0 = (a_0 b_1 + a_1 b_0)u = ... = (a_0 b_m + a_1 b_{m-1} + ... + a_m b_0) = 0$$

Because C is self orthogonal. Later, we have

$$\phi(a)\phi(b) = (a_m, a_m + a_0, \ldots, a_m + a_{m-1} + \ldots + a_0)(b_m, b_m + b_0, \ldots, b_m + b_{m-1} + \ldots + b_0) = 0$$

Because we study in F_2. Using the fact that ϕ is a isometry, we have the last part of this theorem.

Corollary 4.2 There is a Type II of length n over R if and only if n is even.

References

[1] M.Al Ashker, *Simplex codes over* $\sum_{s=0}^{n} u^s F_2$, Turk J. Math,**29**, (2005), 221–233.

[2] K. Betsumiya, S. Ling and F.R.Nemenzo, *Type II codes over* $F_{2^m} + uF_{2^m}$, Discrete Math.,**275**,no 7,(2004), 43–65.

[3] Y.Cengellenmis, *On the* $(1 - u^m)$- *cyclic codes over* $F_2 + uF_2 + ... + u^m F_m$,Int J Comtemp Math. Sciences, **4**, No 20, (2009), 987–992.

[4] S.T.Dougherty, P. Gaboit, M. Harada, P Sole, *Type II codes over* $F_2 + uF_2$,IEEE Trans.Inf. Theory, **45**, No 6, (1999), 32–45.

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

[6] S.Ling ,P.Sole, *Type II codes over $F_4 + uF_4$*, European J Combin.,**12**,no 7,(2001), 983–997.

[7] Jian Fa Qian, L.Zhang,Z. Yin,*Type II codes over $F_2 + uF_2 + u^2F_2$*, Proceeding of 2006 IEEE Information Theory Workshop,(2006), 21–23.

[8] Jian Fa Qian, W Ma,*Self dual codes over the finite chain rings*, IEEE Information Theory,(2008), 250–252.

[9] E.M.Rains, N.J.Sloane, Self dual codes, Handbook of Coding Theory,(1998).

Received: August, 2009