Konuralp Journal of Mathematics, 6 (1) (2018) 54-56

Konuralp Journal of Mathematics

Journal Homepage: www.dergipark.gov.tr/konuralpjournalmath
e-ISSN: 2147-625X

Codes Generated by Special Matrices on $\mathbb{F}_2[u]/_{<u^3>}$

Mustafa Özkan[1*] **and Figen Öke**[2]

[1]*Department of Mathematics, Faculty of Science, Trakya University, Edirne, Turkey*
[2]*Department of Mathematics, Faculty of Science, Trakya University, Edirne, Turkey*
[*]*Corresponding author E-mail: mustafaozkan@trakya.edu.tr*

Abstract

In this study, the results obtained by authors M. Ozkan and F. Oke [2] is extended the ring $\mathbb{F}_2[u]/_{<u^3>}$. Certain matrices lexicographically ordered are written using the elements of $\mathbb{F}_2[u]/_{<u^3>}$. The relations between the codes generated by these matrices and Hadamard codes are given.

Keywords: *Lexicographically ordered, Hadamard Codes, Codes over Ring.*
2010 Mathematics Subject Classification: *94B05, 94B15.*

1. Introduction

Z_4- Linear Hadamard codes and extented perfect codes were introduced in [3]. $(1-u^2)$-cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ and the codes over $\mathbb{F}_2$ which are the Gray images of $(1-u^2)$-cyclic or cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ were characterized in [4]. The extended abstract of this paper is published by AIP [1].
In this study, the codes over the ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$, where $u^3=0$ defining by matrices given in section 3. Construction of matrices are given and it is shown that the Gray images of these codes are Hadamard codes. It is seen that the codes written over the field $\mathbb{F}_2$ are quasi-cyclic codes of index 4. Also some comments are given on the parameters of these codes.

2. Basic Definition

The ring $\mathbb{F}_2[u]/_{<u^3>}=\{a_0+a_1.u+a_2.u^2+\langle u^3\rangle \mid a_i\in F_2, i=0,1,2\}$ is isomorphic to the ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ and it is also isomorphic to the ring $\mathbb{F}_2[u]/_{<u^3>}$ where $u^3=0$.
The set of cosets $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2=\{0,1,u,u^2,1+u,1+u^2,u+u^2,1+u+u^2\}$ is a ring with usual addition and multiplication under the condition $u^3=0$.
All the principle ideals of the ring $R_2=\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ are listed below:
$(0)=\{0\},(u^2)=\{0,u^2\},(u)=(u+u^2)=\{0,u,u^2,u+u^2\},(1)=(1+u)=(1+u^2)=(1+u+u^2)=R_2$.
The relation $(0)\subset(u^2)\subset(u)=(u+u^2)\subset(1+u)=(1+u^2)=(1+u+u^2)=(1)=R_2$ is satisfied for the ideals of the ring R_2.
A linear code C over the ring R_2 of length n is a R_2 submodule of R_2^n . Also a linear code C over $\mathbb{F}_2$ of length n is a n subspace of $\mathbb{F}_2^n$. An element of C is called a codeword.
Let C be a code over $\mathbb{F}_2$ of length n and let $c=(c_o,c_1,...,c_{n-1})$ be a codeword of C. The Hamming weight of C is defined as
$w_H(c)=\sum_{i=0}^{n-1} w_H(c_i)$ where

$$w_H(c_i)=0 \text{ if } c_i=0 \text{ and } w_H(c_i)=1 \text{ if } c_i=1\ .$$

The Lee distance $d_H(c,c')$ between any distinct vectors $c,c'\in\mathbb{F}_2{}^n$ is defined to be $w_H(c-c')$. The minimum Hamming distance of C is called as $d_H(C)=\min\{d_H(c,c')\}$ for any $c,c'\in C, c\neq c'$
The Lee weight $w_L(r)$ of $r\in R_2$ is given by

Article History: **Received XX.XX.XXX, Accepted XX.XX.XXX, Available online XX.XX.XXXX**
Email addresses: , mustafaozkan@trakya.edu.tr (Mustafa Özkan), figenoke@gmail.com (Figen Öke)

$$w_L(r) = \begin{cases} 0 \ ; r = 0 \\ 4 \ ; r = u^2 \\ 2 \ ; \ otherwise \end{cases}$$

This extends to Lee weight function in R_2^n such that $w_L(r) = \sum_{i=0}^{n-1} w_L(r_i)$ for $r = (r_o, r_1, ..., r_{n-1}) \in R_2^n$. The Lee distance $d_L(x, y)$ between any distinct vectors $x, y \in R_2^n$ is defined to be $w_L(x-y)$. The d_L minimum Lee distance of C is defined as $d_L(C) = \min\{d_L(x,y)\}$ for any $x, y \in C$, $x \neq y$.

A $n \times n$ matrix such that all components are -1 or 1 and $M.M^t = n.I$ is called Hadamard matrix. An $n \times n$ matrix is called binary normalized Hadamard matrix if it is obtained from M_n $n \times n$ normalized Hadamard matrix writing 0 instead of 1 and writing 1 instead of -1. Let A_n be binary normalization of a binary Hadamard matrix M_n.

Think that each row of A_n is a vector. Then it is seen that the distance of between two vectors is $\frac{n}{2}$.

Writing each row of matrix as a vector which has length n and adding themselves and their complements to back of these vectors respectively, new vectors which has $2n$ length are obtained. Construct these new vectors in the form of code words. If completions of these codewords join to this set, it is obtained that a Hadamard code including $4n$ elements. Thus the minimum distance of this code is n .

Generally the Gray map is defined as :

$$\Phi : R_2^n \to \mathbb{F}_2^{4n}$$

$$(r_1, r_2, ..., r_n) \mapsto \Phi(r_1, r_2, ..., r_n) =$$

$$(c_1, c_2, ..., c_n, a_1 + c_1, a_2 + c_2, ..., a_n + c_n, b_1 + c_1, b_2 + c_2, ..., b_n + c_n, a_1 + b_1 + c_1, a_2 + b_2 + c_2, ..., a_n + b_n + c_n)$$

where $r_i = a_i + b_i.u + c_i.u^2 \in R_2$ for $0 < i < n+1$.

Therefore C is a code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ which has length n, it's image $\Phi(C)$ under the Gray map is a binary code which has length $4n$. There is a relation $d_L(a,b) = d_H(\Phi(a), \Phi(b))$ for $a, b \in R_2^n$ between Lee distance d_L over R_2^n and Hamming distance d_H over $\mathbb{F}_2^{4n}$. This means that Gray map is an isometry.

3. Structure of Hadamard codes

Generating matrices of the new special code will be constructed according the rules given below :

Choose that all elements of first row of the matrix M^{α_1,α_2} from the set $\{1\}$, choose that the elements of the other rows from the set $\{0, 1, u, u^2, 1+u, 1+u^2, u+u^2, 1+u+u^2\}$ if $\alpha_2 = 0$ and from the set $\{0, u^2\}$ if $\alpha_1 = 0$. Compare that colums of this matrix by lexicographically ordering. This matrix constructed above is a special matrix which has $\alpha_1 + \alpha_2 + 1$ rows.

Certain examples for the matrix M^{α_1,α_2} constructed above are given below :

$$M^{0,0} = [1]_{1x1}, M^{0,1} = \begin{bmatrix} 1 & 1 \\ 0 & u^2 \end{bmatrix}_{2x2}, M^{0,2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & u^2 \end{bmatrix}_{3x4},$$

$$M^{0,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & u^2 & u^2 & u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & 0 & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & u^2 & 0 & u^2 & 0 & u^2 \end{bmatrix}_{4x8}, M^{1,0} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & u & u^2 & 1+u & 1+u^2 & u+u^2 & 1+u+u^2 \end{bmatrix}_{2x8},$$

$$M^{1,1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & u & u & u^2 & u^2 & 1+u & 1+u & 1+u^2 & 1+u^2 & u+u^2 & u+u^2 & 1+u+u^2 & 1+u+u^2 \\ 0 & u^2 & 0 & u^2 & 0 & u^2 & 0 & u^2 & 0 & u^2 & 0 & u^2 & 0 & u^2 & 0 & u^2 \end{bmatrix}_{3x16}.$$

Define the code $C^{\alpha_1,\alpha_2} = \{ (c_1, c_2).M^{\alpha_1,\alpha_2} \mid c_1 \in R_2^{\alpha_1+1}, c_2 \in IF_2^{\alpha_2} \}$ which has a generator matrix M^{α_1,α_2}, where α_1, α_2 positive integers. The lenght of this code is $n = 2^{3\alpha_1+\alpha_2}$. Moreover, the parameters of the code C^{α_1,α_2} over $IF_2 + uIF_2 + u^2IF_2$ are $(n, 8n, 2n)$.

Theorem 3.1. *Let $\Phi : R_2^n \to \mathbb{F}_2^{4n}$ be Gray map. If C^{α_1,α_2} is a code generated by the matrix M^{α_1,α_2} over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, it's image $\Phi(C^{\alpha_1,\alpha_2})$ under the Gray map is the $(4n, 8n, 2n)$_ Hadamard code over the field $\mathbb{F}_2$.*

Proof. Writing the code C^{α_1,α_2} generated by matrix M^{α_1,α_2} which has the dimension $(\alpha_1 + \alpha_2 + 1) \times n$ of the form $C^{\alpha_1,\alpha_2} = \{ (c_1, c_2).M^{\alpha_1,\alpha_2} \mid c_1 \in R_2^{\alpha_1+1}, c_2 \in IF_2^{\alpha_2} \}$ the proof is obtained as in [1] .

□

Lemma 3.2. *The dual code of $(C^{\alpha_1,\alpha_2})^\perp$ is a $(n, \frac{8^n}{8n}, 4)$_ code and it's image $\Phi((C^{\alpha_1,\alpha_2})^\perp)$ under the Gray map is a $(4n, \frac{8^n}{8n}, 4)$_code, in except the case $\alpha_1 = \alpha_2 = 0$.*

Proof. The generator matrix M^{α_1,α_2} of C^{α_1,α_2} is the parity-check matrix of the dual code $(C^{\alpha_1,\alpha_2})^\perp$. The dual code of $(C^{\alpha_1,\alpha_2})^\perp$ contains elements c of R_2^n satisfied $M^{\alpha_1,\alpha_2}.c^T = 0$. It is easily seen that the number of words satisfied this condition is $\frac{8^n}{8n}$ and the minimum weight a word is 4. Thus $(C^{\alpha_1,\alpha_2})^\perp$ is $(n, \frac{8^n}{8n}, 4)$_ code. Also it is seen that $\Phi((C^{\alpha_1,\alpha_2})^\perp)$ has the parameter $(4n, \frac{8^n}{8n}, 4)$.

□

4. cyclic codes and quasi-cyclic codes of index 4

Each codeword c in such a code C is an $n-$tuple of the form $c=(c_1,c_2,...,c_n)\in R_2^n$ can be represented by

$$c=(c_1,c_2,...,c_n)\longleftrightarrow c(x)=\sum_{i=1}^{n}c_i.x^i\in R_2[x]\ .$$

Definition 4.1. *Let $C^{\alpha_1,\alpha_2}\subseteq R_2^n$ be a linear code , where $n=2^{3\alpha_1+\alpha_2}$. Define the map*

$$\tau\ :\ R_2^n\to R_2^n$$
$$(c_1,c_2,...,c_n)\mapsto\tau(c_1,c_2,...,c_n)=(c_n,c_1,...,c_{n-1})$$

If $\tau(C^{\alpha_1,\alpha_2})=C^{\alpha_1,\alpha_2}$ then C^{α_1,α_2} is a cyclic code over R_2.

Definition 4.2. *Let $D^{\alpha_1,\alpha_2}\subseteq\mathbb{F}_2^{4n}$ be a linear code and $n=2^{3\alpha_1+\alpha_2}$. Define the map*

$$\sigma^{\otimes 4}\ :\ \mathbb{F}_2^{4n}\to\mathbb{F}_2^{4n}$$
$$(d_1,d_2,...,d_{4n})\mapsto\sigma^{\otimes 4}(d_1,d_2,...,d_{4n})=(d_n,d_1,...,d_{n-1},d_{2n},d_{n+1},...d_{2n-1},d_{3n},d_{2n+1},...d_{3n-1},d_{4n},d_{3n+1},...d_{4n-1})$$

If $\sigma^{\otimes 4}(D^{\alpha_1,\alpha_2})=D^{\alpha_1,\alpha_2}$ then D^{α_1,α_2} is a quasi-cyclic code of index 4 over $\mathbb{F}_2$.

Lemma 4.3. *$\Phi\tau=\sigma^{\otimes 4}\Phi$ is satisfied.*

Proof. Let $x=(x_1,x_2,...,x_n)\in R_2^n$ where $x_i=a_i+ub_i+u^2c_i\in R_2$ for $1\leqslant i\leqslant n$. If $\tau(x)=\tau(x_1,x_2,...,x_n)=(x_n,x_1,...,x_{n-1})$, then
$\Phi\tau(x)=\Phi(\tau(x_1,x_2,...,x_n))=\Phi(x_n,x_1,...,x_{n-1})=\Phi(a_n+ub_n+u^2c_n,a_1+ub_1+u^2c_1,a_2+ub_2+u^2c_2,...,a_{n-1}+ub_{n-1}+u^2c_{n-1})=(c_n,c_1,c_2,...,c_{n-1},a_n+c_n,a_1+c_1,a_2+c_2,...,a_{n-1}+c_{n-1},b_n+c_n,b_1+c_1,b_2+c_2,...,b_{n-1}+c_{n-1},a_n+b_n+c_n,a_1+b_1+c_1,a_2+b_2+c_2,...,a_{n-1}+b_{n-1}+c_{n-1})$. On the other hand,
$\Phi(x)=\Phi(x_1,x_2,...,x_n)=\Phi(a_1+ub_1+u^2c_1,a_2+ub_2+u^2c_2,...,a_n+ub_n+u^2c_n)=(c_1,c_2,...,c_n,a_1+c_1,a_2+c_2,...,a_n+c_n,b_1+c_1,b_2+c_2,...,b_n+c_n,a_1+b_1+c_1,a_2+b_2+c_2,...,a_n+b_n+c_n)$ then
$\sigma^{\otimes 4}(\Phi(x))=(c_n,c_1,c_2,...,c_{n-1},a_n+c_n,a_1+c_1,a_2+c_2,...,a_{n-1}+c_{n-1},b_n+c_n,b_1+c_1,b_2+c_2,...,b_{n-1}+c_{n-1},a_n+b_n+c_n,a_1+b_1+c_1,a_2+b_2+c_2,...,a_{n-1}+b_{n-1}+c_{n-1})$.

□

Theorem 4.4. *The Hadamard code which is obtained by using the matrix M^{α_1,α_2} is a quasi-cyclic code of index 4, in except the case $\alpha_2=0$.*

Proof. Considering the images of C^{α_1,α_2} under the maps $\sigma^{\otimes 4}\Phi$, $\Phi\tau$, the proof is completed as in [1].

□

Example 4.5. *Write the matrix $M^{0,1}$ to define the code $C^{0,1}$, $M^{0,1}=\begin{bmatrix}1&1\\0&u^2\end{bmatrix}_{2x2}$. Then the elements of the code $C^{0,1}$ are of the form $c=(c_1,c_2).M^{0,1}$, where $c_1\in R_2$, $c_2\in\mathbb{F}_2$.$C^{0,1}=\{\,0\,0\,,0\,u^2\,,1\,1\,,1\,1+u^2\,,u\,u\,,u\,u+u^2\,,u^2\,u^2\,,u^2\,0\,,1+u\,1+u\,,1+u\,1+u+u^2\,,1+u^2\,1+u^2\,1+u^2\,1\,,u+u^2\,u+u^2\,,u+u^2\,u\,,1+u+u^2\,1+u+u^2\,,1+u+u^2\,1+u\,\}\subseteq R_2^2$. It is seen that $d_L(C^{0,1})=4$, $\left|C^{0,1}\right|=16$ and then this is a $(2,16,4)$_code.Therefore $\Phi(C^{0,1})=\{\,00000000,01010101,00110011,01100110,\ 11111111,10101010,11001100,10011001,00001111,01011010,00111100,01101001,\ 11110000,10100101,11000011,10010110\,\}\subseteq\mathbb{F}_2^8$ is a $(8,16,4)$_Hadamard code.*

Let $A_4=\begin{bmatrix}1&1&1&1\\-1&1&-1&1\\-1&-1&1&1\\1&-1&-1&1\end{bmatrix}_{4x4}$ be a normalized Hadamard matrix. Writing 0 instead of 1 and 1 instead of -1 , the vectors 0000, 1010, 1100 and 0110 are obtained. Adding themselves and their complements to back of these vectors respectively, new vectors 0000, 1010, 1100, 0110, 1111, 0101, 0011 and 1001 are obtained. Then using the method given above, the new codewords 00000000, 01010101, 00110011, 01100110, 11111111, 10101010, 11001100, 10011001, 00001111, 01011010, 00111100 01101001, 11110000, 10100101, 11000011, 10010110 are obtained. The code $\Phi(C^{0,2})$ formed by these codewords is a $(8,16,4)$_Hadamard code. Moreover $(C^{0,1})^{\perp}=\{\,0\,0\,,u\,u,u^2\,u^2\,,u+u^2\,u+u^2\,\}\subseteq\mathbb{F}_2^2$ and $\Phi((C^{0,1})^{\perp})=\{\,00000000,00001111,11111111,11110000\}\subseteq\mathbb{F}_2^8$. $C^{0,1}$ is a cyclic code such that the equation $\tau(C^{0,1})=C^{0,1}$ is provided. Similarly $\Phi(C^{0,1})$ is quasi-cyclic code of index 4 such that the equation $\sigma^{\otimes 4}(\Phi(C^{0,1}))=\Phi(C^{0,1})$ is satisfied.

References

[1] Özkan, M. and Öke, F., On Codes written by matrices Lexicographically ordered, AIP Conf. Proceeding Vol:1926 (2018), 020035-1-020035-3.

[2] Özkan, M. and Öke, F., A relation between Hadamard codes and some special codes over $\mathbb{F}_2+u\mathbb{F}_2$, App Mathematics and Inf. Sci. Vol:10, No:2 (2016), 701-704.

[3] Krotov, D. S., Z4-linear perfect codes, Diskretn. Anal. Issled. Oper. Ser.1 Vol:7, No:4 (2000), 78-90.

[4] Qian, J. , Zhang, L. and Zhu S., Constacyclic and cycliccodes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$, IEICE Trans. Fundamentals, E89-A, No: 6, (2006)1863-1865.

[5] Vermani, L. R., *Elements of Algebraic Coding Theory*tivity, Chapman Hall , India, 1996.

[6] Udomkavanich, P., Jitman, S., On the Gray Image of $(1-u^m)$-Cyclic Codes $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}+...+u^m\mathbb{F}_{p^k}$, Int. J. Contemp. Math. Sciences, Vol.26, No: 4, (2009)1265-1272.