Extensions of Hadamard Codes Defined on Rings

Mustafa Özkan[1,*], *Figen Öke*[2]

[1]Department of Mathematics, University of Trakya, Edirne, Turkey

[2]Department of Mathematics, University of Trakya, Edirne, Turkey

Abstract. In this study, some special matrices are constructed by choosing certain elements from finite rings and certain codes are written by using these matrices.

These codes are extended to a field. Moreover these codes are classified and more good codes are written.

1 Introduction

Structures of cyclic, constacyclic and quasi-cyclic codes over certain finite chain rings previously were worked . $(1+u)-$Constacyclic and Cyclic codes over the ring $\mathbb{F}_2+u\mathbb{F}_2$ were practiced by Qian J., Zhang L. and Zhu S. in [4]. These subjects were extended to the ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ by the same authors in [5]. Defined codes in $\mathbb{Z}_4$ ring were obtained by Krotov D. in [1] and [2]. Hadamard Code over $\mathbb{Z}_4$ in particular were worked by Krotov D. in [2].

We will deal with codes defined over finite rings and binary codes.

Main aim is to obtain new and good codes. An n. rank square matrix M that total ingredient 1 or -1 where $MM^t=nI$ is defined Hadamard matrix. Hadamard codes are called a code defined by Hadamard matrices. It says that using Hadamard matrices new codes could be obtained.

This study is a generalizations of results obtained in [7, 8, 9] for the finite chain rings over $\mathbb{F}_2$.

*Corresponding author: mustafaozkan@trakya.edu.tr, mustafaozkan22@icloud.com

2 Basics

Let R_m be a ring. C linear code of length n in $\mathbb{F}_2$ is a $\mathbb{F}_2$ - sub space of $\mathbb{F}_2^n$. C linear code of length n in R_m is a R_m - sub module of R_m^n.

Let length of C is n, it's number of elements is M and it's minimum distance is d. Therefore C be called $(n, M, d)\_$ code.

It is known that the ring $R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ with $m \geq 1,\ m \in \mathbb{Z}$ is isomorphic to the ring

$$\mathbb{F}_2[u] \Big/ < u^{m+1} > = \{ x_0 + x_1.u + ... + x_m.u^m + < u^{m+1} > \Big| \ \ x_i \in \mathbb{F}_2,\ 0 \leq i \leq m,\ m \geq 1,\ m \in \mathbb{Z} \}$$

in case $u^{m+1} = 0$. It is known that the $R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ where $u^{m+1} = 0$ is a ring

n. rank square matrix is called binary Hadamard matrix if it is gain from n. rank square Hadamard matrix M_n placing 0 instead of 1 and writing 1 instead of -1.

Let n be an even number. Write all rows of the matrix called foregoing as a vector where have length n. Let us create a set putting into these vectors and respectively their ingredient to back of these vectors. Then this vectors with length $2n$ are obtained. Write all this new vector as a codeword. If completions of codewords add to this set, the minimum distance of this code is n and Hadamard code included $4n$ elements.

The general Gray map is called as follows:

$$\Phi : \ R_m^n \longrightarrow \mathbb{F}_2^{2^m.n}$$

$$a_0 + a_1.u + ... + a_m.u^m \mapsto \ \Phi(a_0 + a_1.u + ... + a_m.u^m)$$

$$\Phi(a_0 + a_1.u + ... + a_m.u^m) = (a_m, a_m + a_0, a_m + a_1, ..., a_m + a_{m-1}, a_m + a_0 + a_1, a_m + a_0 + a_2, ...,$$
$$a_m + a_0 + a_{m-1}, a_m + a_1 + a_2, ..., a_m + a_1 + a_{m-1}, a_m + a_2 + a_3, ..., a_m + a_2 + a_{m-1}, ...,$$
$$a_m + a_{m-2} + a_{m-1}, a_m + a_0 + a_1 + a_2, ..., a_m + a_0 + a_1 + a_{m-1}, ...,$$
$$a_m + a_{m-3} + a_{m-2} + a_{m-1}, a_m + a_0 + a_1 + a_2 + a_3, ...,$$
$$a_m + a_{m-4} + a_{m-3} + a_{m-2} + a_{m-1}, ..., ..., a_m + a_0 + a_1 + ... + a_{m-1})$$

where $a_i \in \mathbb{F}_2^n$, for $0 \leq i \leq m$.

The homogeneous weight $w_{\hom}(r)$ of $r \in R_m$ is given by

$$w_{\hom}(r) = \begin{cases} 0 & ; r = 0 \\ 2^m & ; r = u^m \\ 2^{m-1} & ; otherwise \end{cases}$$

This expanded homogeneous weight function over R_m^n such that $w_{\hom}(r) = \sum_{i=0}^{n-1} w_{\hom}(r_i)$ for $r = (r_o, r_1, ..., r_{n-1}) \in R_m^n$. The homogeneous distance $d_{\hom}(a,b)$ between any different vectors $a, b \in R_m^n$ is called as $w_{\hom L}(a-b)$. The minimum homogeneous distance $d_{\hom}$ of C is called as for each $a, b \in C$, $a \neq b$ $d_{\hom}(C) = \min\{d_{\hom}(a,b)\}$.

Let C of length n is a code in $\mathbb{F}_2$ and $c = (c_o, c_1, ..., c_{n-1})$ 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 $w_H(c_i) = 0$ if $c_i = 0$ and $w_H(c_i) = 1$ if $c_i = 1$. The minimum Hamming distance of C is defined as $d_H(C) = \min\{d_H(c,c')\}$ for any $c, c' \in C, c \neq c'$.

Therefore C of length n is a code in R_m and then $\Phi(C)$ is a binary code of length $2^m.n$.

3 Construction of Hadamard codes

In this chapter, generator matrices were created.

Formed every elements of one row of the matrix $G^{\alpha,\beta}$ from 1, select that the elements of the another rows from $\{0, 1, u, ..., u^m, 1+u, ..., 1+u^m, ..., 1+u+...+u^m\}$ set if $\beta = 0$ and from $\{0, u^m\}$ set if $\alpha = 0$. $G^{\alpha,\beta}$ occured foregoing $\alpha + \beta + 1$ rows. Colums of $G^{\alpha,\beta}$ be lexicographically ordered.

Examples of $G^{\alpha,\beta}$ be given below :

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

$$G^{0,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & u^m & u^m & u^m & u^m \\ 0 & 0 & u^m & u^m & 0 & 0 & u^m & u^m \\ 0 & u^m & 0 & u^m & 0 & u^m & 0 & u^m \end{bmatrix}_{4x8} ,$$

$$G^{1,0} = \begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 & . & . & . & 1 \\ 0 & 1 & u & 1+u & . & . & . & 1+u^m & . & . & . & 1+u+...+u^m \end{bmatrix}_{2\times 2^{m+1}} .$$

Define the code $C^{\alpha,\beta} = \{ (c_1, c_2).G^{\alpha,\beta} \mid c_1 \in R_m^{\alpha+1}, c_2 \in \mathbb{F}_2^{\beta} \}$ which has a generator matrix $G^{\alpha,\beta}$ where α, β are integers such that $\alpha, \beta \geq 0$. The length of $C^{\alpha,\beta}$ code is $n = 2^{(m+1).\alpha+\beta}$ and parameters of code $C^{\alpha,\beta}$ be $(n, 2^{m+1}.n, 2^{m-1}.n)$.

Theorem 3.1 : If $C^{\alpha,\beta}$ is a code generated by the matrix $G^{\alpha,\beta}$ over R_m, it's image $\Phi(C^{\alpha,\beta})$ under the Gray map is the $(2^m.n, 2^{m+1}.n, 2^{m-1}.n)\_$ Hadamard code over the field $\mathbb{F}_2$.

Proof : $C^{\alpha,\beta}$ code be obtained by the matrix $G^{\alpha,\beta}$ which has dimension $(\alpha+\beta+1)\times n$ is of $C^{\alpha,\beta} = \{ (c_1, c_2).G^{\alpha,\beta} \mid c_1 \in R_m^{\alpha+1}, c_2 \in \mathbb{F}_2^{\beta} \}$. The length of The length of $C^{\alpha,\beta}$ is $n = 2^{(m+1).\alpha+\beta}$ and it has $2^{m+1}.n$ elements, i.e. $C^{\alpha,\beta}$ is a $(n, 2^{m+1}.n, 2^{m-1}.n)$- code. Hence $\Phi(C^{\alpha,\beta}) \subseteq \mathbb{F}_2^{2^m.n}$ and $\Phi(C^{\alpha,\beta})$ is a binary Hadamard code with $(2^m.n, 2^{m+1}.n, 2^{m-1}.n)$ parameters.

Theorem 3.2 : The $(C^{\alpha,\beta})^{\perp}$ is a $(n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)\_$ code and it's image $\Phi((C^{\alpha,\beta})^{\perp})$ under the Gray map is a $(2^m.n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)\_$ code, in except the case $\alpha = \beta = 0$.

Proof : The generator matrix $G^{\alpha,\beta}$ of $C^{\alpha,\beta}$ is the parity-check matrix of the dual code $(C^{\alpha,\beta})^{\perp}$. The dual code of $(C^{\alpha,\beta})^{\perp}$ contains elements x of R_m^n satisfied $G^{\alpha,\beta}.x^T = 0$.

It is seen that the number of vectors be $\frac{(2^{m+1})^n}{2^{m+1}.n}$, minimum weight of these vectors be 4 .

Hence $(C^{\alpha,\beta})^{\perp}$ code be $(n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)\_$ code . It is viewed that $\Phi((C^{\alpha,\beta})^{\perp})$ has the parameters $(2^m.n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)$.

4 Conclusion

In this paper; some special matrices are constructed to obtain new Hadamard codes using the elements of the finite chain ring $\mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$. Certain special codes are obtained using these special matrices as generator matrices.

References

1. Krotov, D. S.,Diskretn. Anal. Issled. Oper. Ser.1., **7, 4**. 78–90,(2000)
2. Krotov,D. S. ,Procs. of the International Workshop on Coding and Cryptography, Paris, 329-334,(2001)
3. Vermani, L. R., Chapman Hall, India., (1996)
4. J.F.Qian, L.N.Zhang, S.X. Zhu, Applied Mathematics Letters,**19**,820-823,(2006)
5. J.F.Qian, L.N.Zhang, S. X. Zhu,IEICE Trans.Fundamentals, **E89-a, no 6**,1863-1865,(2006)
6. W. C. Huffman and Vera Pless, Fundamentals of Error Correcting Codes, Cambridge, (2003)
7. M. Özkan and F.Öke , App Mathematics and Inf. Sci. 10 (2), 701-704.,(2016)
8. M. Ozkan, F. Oke, General Letters in Mathematics, 2(1), 110–118, (2017)
9. M. Ozkan, F. Oke, AIP Conf. Proc.,1926, 020035-1–020035-3,(2018).