Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/100229

A Relation between Hadamard Codes and Some Special Codes over $\mathbb{F}_2 + u\mathbb{F}_2$

Mustafa ÖZKAN and Figen ÖKE*

Department of Mathematics, Faculty of Science, Trakya University, Edirne, Turkey

Received: 26 Aug. 2015, Revised: 13 Nov. 2015, Accepted: 14 Nov. 2015
Published online: 1 Mar. 2016

Abstract: A Hadamard code which is written via a Hadamard matrix is $(2n,4n,n)_{-}$ code. In this study some special codes over $\mathbb{F}_2+u\mathbb{F}_2 = \{0\,,1\,,u\,,1+u\}$ where $u^2 = 0$ are written and it is shown that images of these codes under a Gray map correspond binary Hadamard codes.

Keywords: Hadamard codes, Codes over rings, Linear codes.

1 Introduction

Certain codes as cyclic codes over the ring were studied before. For example, cyclic and constacyclic codes over the ring were studied by Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu in [5]. Again cyclic codes were studied over more general ring by the same group in [6]. Then these codes were studied over the most general finite chain ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + ... + u^m\mathbb{F}_{p^k}$ by P. Udomkavanich and S. Jitman in [8]. It was shown that, the Gray image of a linear negacyclic code over $\mathbb{Z}_4$ is a cyclic code in [3]. It was proved that, the Gray image of a linear cyclic code over $\mathbb{Z}_4$ of length n (n is odd number) is equivalent to a binary cyclic code in [3].

Structures of certain codes over the ring $\mathbb{Z}_4$ were studied by D.S. Krotov in [1,2]. Especially Hadamard codes over $\mathbb{Z}_4$ were studied by him in [2].

Using a Gray mapping, some new codes over a Galois field via codes over $\mathbb{F}_2+u\mathbb{F}_2$ and generally codes over a finite chain ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + ... + u^m\mathbb{F}_{p^k}$ has been obtained. It is known that the distance over $\mathbb{F}_2+u\mathbb{F}_2$ is Lee distance (weight) and the distance over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k} + ... + u^m\mathbb{F}_{p^k}$ is homogeneous distance (weight). It is shown that the new codes obtained by Gray map has the same minimum distance of the previous codes.

In this study $(n,4n,n)_{-}$ codes over $\mathbb{F}_2+u\mathbb{F}_2$ with $u^2=0$ are defined and using these codes $(2n,4n,n)_{-}$ codes over $\mathbb{F}_2$ are obtained. These new codes which obtained by Gray map are Hadamard codes. Moreover these new codes are linear codes and all elements of their generator matrix are elements of the ring $\mathbb{F}_2+u\mathbb{F}_2$ with $u^2 = 0$.

Since scalers used in the composition of these codes are in the binary field, studying on this codes will be more advantage.

2 Preliminaries

The ring $\mathbb{F}_2[u]/_{\langle u^2\rangle} = \left\{a_0 + a_1.u + \langle u^2\rangle \mid a_0, a_1 \in \mathbb{F}_2\right\}$ is isomorphic to the ring $\mathbb{F}_2+u\mathbb{F}_2$ when $u^2 = 0$. Binary operations on the ring $\mathbb{F}_2+u\mathbb{F}_2 = \{0\,,1\,,u\,,1+u\}$ are defined as below:

+	0	1	u	1+u
0	0	1	u	1+u
1	1	0	1+u	u
u	u	1+u	0	1
1+u	1+u	u	1	0

.	0	1	u	1+u
0	0	0	0	0
1	0	1	u	1+u
u	0	u	0	u
1+u	0	1+u	u	1

The ring $R = \mathbb{F}_2+u\mathbb{F}_2$ has three ideals satisfied the inclusion; $\langle 0\rangle \subseteq \langle u\rangle \subseteq \langle 1\rangle = R$. Let C be a $(n,M,d)_{-}$ code. It means that C has the length n , it has M elements and its minimum distance is d .

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

Lee weight of $r = (r_1, r_2, ..., r_n) \in R^n$ is defined as $w_L(r) := \sum\limits_{i=1}^{n} w_L(r_i)$ where $w_L(0) = 0$, $w_L(1) = 1$, $w_L(u) = 2, w_L(1+u) = 1$.

The minimum Lee weight of a code C is defined as $d_L(C) = \min\{d_L(a,b) \mid a,b \in C, a \neq b\}$ where $d_L(a,b) = w_L(a,b)$ is the distance between $a,b \in R^n$, $a \neq b$.

The generator matrix of a code C in the ring $R = \mathbb{F}_2 + u\mathbb{F}_2$ is $G = \begin{bmatrix} G_1 \\ u.G_2 \end{bmatrix}$. Here G_1 is a $k_1 \times n$ matrix which has elements in $\mathbb{F}_2 + u\mathbb{F}_2$ and G_2 is a $k_2 \times n$ matrix which has elements in $\mathbb{F}_2$. Hence $|C| = 2^{2k_1+k_2}$.

The code C written in this study is a $4^{k_1}.2^{k_2}{}_{-}$ code and it is written as

$$C = \left\{ \, c = (c_1, c_2). \begin{bmatrix} G_1 \\ u.G_2 \end{bmatrix} \middle| \, c_1 \in R^{k_1}, c_2 \in \mathbb{F}_2{}^{k_2} \right\}.$$

A $n \times n$ matrix such that all components are -1 or 1 and $M.M^t = n.I$ is called Hadamard matrix. A $n \times n$ 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 normalized Hadamard matrix of a binary Hadamard matrix M_n . If each two rows of A_n are orthogonal then $\frac{n}{2}$ elements are different for these rows of A_n .

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

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

Generally the Gray map is defined as :

$$\Phi \, : \, R^n \to \mathbb{F}_2^{2n}$$

$$(r_1, r_2, ..., r_n) \mapsto \Phi\,(r_1, r_2, ..., r_n) = (b_1, b_2, ..., b_n, a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$$

where $r_i = a_i + ub_i \, \in R$ for $1 \leqslant i \leqslant n$. Therefore C is a code over $\mathbb{F}_2 + u\mathbb{F}_2$ which has length n , its image $\Phi(C)$ under the Gray map will be a binary code which has length $2n$.

There is a relation $d_L(a,b) = d_H(\Phi(a), \Phi(b))$ for $a, b \in R^n$ between Lee distance d_L over R^n and Hamming distance d_H over $\mathbb{F}_2^{2n}$. This means that Gray map is an isometry.

3 Construction

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

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

$$N^{0,0} = [1]\,, N^{0,1} = \begin{bmatrix} 1 & 1 \\ 0 & u \end{bmatrix}, N^{0,2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & u & u \\ 0 & u & 0 & u \end{bmatrix},$$

$$N^{0,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & u & u & u & u \\ 0 & 0 & u & u & 0 & 0 & u & u \\ 0 & u & 0 & u & 0 & u & 0 & u \end{bmatrix}, N^{1,0} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & u & 1+u \end{bmatrix},$$

$$N^{2,0} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & u & u & u & u & 1+u & 1+u & 1+u & 1+u \\ 0 & 1 & u & 1+u & 0 & 1 & u & 1+u & 0 & 1 & u & 1+u & 0 & 1 & u & 1+u \end{bmatrix},$$

$$N^{1,1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & u & u & 1+u & 1+u \\ 0 & u & 0 & u & 0 & u & 0 & u \end{bmatrix}.$$

Define the code $C^{\alpha_1,\alpha_2} = \left\{ \, (c_1, c_2).N^{\alpha_1,\alpha_2} \, \middle| \, c_1 \in R^{\alpha_1+1}, c_2 \in \mathbb{F}_2^{\alpha_2} \right\}$ which has a generator matrix N^{α_1,α_2} where α_1, α_2 are integers such that $\alpha_1, \alpha_2 \geqslant 0$. The lenght of this code is $n = 2^{2\alpha_1+\alpha_2}$. Moreover the parameter of the code C^{α_1,α_2} over $\mathbb{F}_2 + u\mathbb{F}_2$ are $(n, 4n, n)$.

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

Proof : The code C^{α_1,α_2} generated by the matrix N^{α_1,α_2} which has dimension $(\alpha_1 + \alpha_2 + 1) \times n$ is the form $C^{\alpha_1,\alpha_2} = \left\{ \, (c_1, c_2).N^{\alpha_1,\alpha_2} \, \middle| \, c_1 \in R^{\alpha_1+1}, c_2 \in \mathbb{F}_2^{\alpha_2} \right\}$. The length of C^{α_1,α_2} is $n = 2^{2\alpha_1+\alpha_2}$. It is clear that the code $C^{\alpha_1,\alpha_2} \subseteq R^n$ is a repetition code and it has $4n$ elements, i.e. C^{α_1,α_2} is a $(n, 4n, n)_{-}$ code. Hence $\Phi(C^{\alpha_1,\alpha_2}) \subseteq \mathbb{F}_2^{2n}$ and $\Phi(C^{\alpha_1,\alpha_2})$ is a binary Hadamard code with $(2n, 4n, n)$ parameter.

Corollary 3.2 : The dual code of $(C^{\alpha_1,\alpha_2})^{\perp}$ is a $(n, \frac{4^n}{4n}, 4)_{-}$code and its image $\Phi((C^{\alpha_1,\alpha_2})^{\perp})$ under the Gray map is a $(2n, \frac{4^n}{4n}, 4)_{-}$ code, in except the case $\alpha_1 = \alpha_2 = 0$.

Proof : The generator matrix N^{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^n satisfied $N^{\alpha_1,\alpha_2}.c^T = 0$. It is easily seen that the number of words satisfied this condition is $\frac{4^n}{4n}$ and the minimum weight of these words is 4 . Thus $(C^{\alpha_1,\alpha_2})^{\perp}$ is $(n, \frac{4^n}{4n}, 4)_{-}$ code . Also it is seen that $\Phi((C^{\alpha_1,\alpha_2})^{\perp})$ has the parameter $(2n, \frac{4^n}{4n}, 4)$.

4 Cyclic codes and quasi-cyclic codes of index 2

Let $c = (c_1, c_2, ..., c_n)$ be an element of R^n . $c = (c_1, c_2, ..., c_n)$ is mapped one to one with $c(x) = \sum\limits_{i=1}^{n} c_i x^i \in R[x]$.

Definition 4.1 : Let $C^{\alpha_1,\alpha_2}\subseteq R^n$ be a linear code , $n=2^{2\alpha_1+\alpha_2}$ and define the map

$$\tau\ :\ R^n\ \rightarrow\ R^n$$

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

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

Definition 4.2 : Let $D^{\alpha_1,\alpha_2}\subseteq {\mathbb{F}_2}^{2n}$ is a linear code, $n=2^{2\alpha_1+\alpha_2}$ and define the map

$$\sigma^{\otimes 2}\ :\ {\mathbb{F}_2}^{2n}\rightarrow{\mathbb{F}_2}^{2n}$$

$$(d_1,d_2,...,d_{2n})\mapsto\sigma^{\otimes 2}(d_1,d_2,...,d_{2n})=$$
$$(d_n,d_1,...,d_{n-1},d_{2n},d_{n+1},...d_{2n-1})$$

If $\sigma^{\otimes 2}(D^{\alpha_1,\alpha_2})=D^{\alpha_1,\alpha_2}$ then D^{α_1,α_2} is defined as quasi-cyclic code of index 2 over $\mathbb{F}_2$.

Proposition 4.3 : $\sigma^{\otimes 2}\Phi=\Phi\,\tau$.

Proof : Let $c=(c_1,c_2,...,c_n)\in R^n$ where $c_i=a_i+ub_i\in R$ for $1\leqslant i\leqslant n$. If $\Phi(c)=\Phi(c_1,c_2,...,c_n)$ $=\Phi(a_1+ub_1,a_2+ub_2,...,a_n+ub_n)$ $=(b_1,b_2,...,b_n,a_1+b_1,a_2+b_2,...,a_n+b_n)$ then $\sigma^{\otimes 2}(\Phi(c))$ $=(b_n,b_1,...,b_{n-1},a_n+b_n,a_1+b_1,...,a_{n-1}+b_{n-1})$.

On the other hand, $\tau\,(c_1,c_2,...,c_n)=(c_n,c_1,...,c_{n-1})$ .Then $\Phi\,\tau(c)$ $=\Phi(\tau(c_1,c_2,...,c_n))$ $=\Phi(c_n,c_1,...,c_{n-1})=$ $(b_n,b_1,...,b_{n-1},a_n+b_n,a_1+b_1,...,a_{n-1}+b_{n-1})$.

Theorem 4.4 : Hadamard codes which are obtained with N^{α_1,α_2} are quasi-cyclic code of index 2, in except the case $\alpha_2=0$.

Proof : It is seen that the length of the codes C^{α_1,α_2} which are defined in third section by using different matrices N^{α_1,α_2} is $n=2^{2\alpha_1+\alpha_2}$. Therefore the length of the all codes $\Phi(C^{\alpha_1,\alpha_2})$ over $\mathbb{F}_2$ is $2^{2\alpha_1+\alpha_2+1}$ and they are equal to the Hadamard codes that are obtained by using Hadamard matrices. Thus from the previous Proposition the equalitions $\sigma^{\otimes 2}(\Phi(C^{\alpha_1,\alpha_2}))$= $\Phi(\tau(C^{\alpha_1,\alpha_2}))$= $\Phi(C^{\alpha_1,\alpha_2})$ are satisfied. Since Φ is injective, it follows that $\sigma^{\otimes 2}(\Phi(C^{\alpha_1,\alpha_2}))$= $\Phi(C^{\alpha_1,\alpha_2})$. Consequently Hadamard codes $\Phi(C^{\alpha_1,\alpha_2})$ are quasi-cyclic code of index 2.

Example 4.5 : Write the matrix $N^{0,1}$ to define the code $C^{0,1}$. $N^{0,1}=\begin{bmatrix}1&1\\0&u\end{bmatrix}$. Then elements of $C^{0,1}$ are $c=(c_1,c_2).N^{0\,,\,1}$, where $c_1\in R\,,c_2\in\mathbb{F}_2.C^{0,1}=$ $\{00,11,uu,1+u1+u\,,0u\,,11+u\,,u0u+11\}\subseteq R^2$. It is seen that $d_L(C^{0,1})=2$ and $\left|C^{0,1}\right|=8$ and then this is a $(2,8,2)$_code. Therefore $\Phi(C^{0,1})$ $=$ $\{0000\,,0011\,,1111\,,1100\,,0101\,,0110\,,1010\,,1001\}$ $\subseteq$ $\mathbb{F}_2^4$ is a $(4,8,2)$_Hadamard code. Let $A_2=\begin{bmatrix}1&1\\-1&1\end{bmatrix}$ be a normalized Hadamard matrix. Writing 0 instead of 1 and 1 instead of -1 , the vectors 00 and 10 are obtained. (Adding the complements of these vectors the new vectors $00\,,10\,,11\,,01$ are obtained). Then using the method given above, the new codewords $0000\,,0011\,,1111\,,1100\,,0101\,,0110\,,1010\,,1001$ are obtained. The code formed by these codewords is $\Phi(C^{0,1})$ code which is a $(4,8,2)$_Hadamard code. Moreover $(C^{0,1})^{\perp}=\{00\,,uu\}$, $\Phi((C^{0,1})^{\perp})=\{0000\,,1111\}$.

$C^{0,1}$ is a cyclic code as the equation $\tau(C^{0,1})=C^{0,1}$ is provided. Smilarly $\Phi(C^{0,1})$ is quasi-cyclic code of index 2 as the equation $\sigma^{\otimes 2}(\Phi(C^{0,1}))=\Phi(C^{0,1})$ is provided.

Example 4.6 : Write the matrix $N^{0,2}$ to define the code $C^{0,2}$. $N^{0,2}=\begin{bmatrix}1&1&1&1\\0&0&u&u\\0&u&0&u\end{bmatrix}$. Then elements of $C^{0,2}$ are of the form $c=(c_1,c_2).N^{0\,,\,2}$, where $c_1\in R\,,c_2\in\mathbb{F}_2^2$.

$C^{0,2}=\{0000\,,0u0u\,,00uu\,,0uu0\,,1111\,,11+u11$ $+u\,,111+u1+u\,,11+u1+u1\,,uuuu\,,u0u0\,,uu00\,,$ $u00u\,,1+u1+u1+u1+u\,,1+u11+u1\,,1+u1+$ $u11\,,1+u111+u\}\subseteq R^4$.

It is seen that $d_L(C^{0,2})=4$ and $\left|C^{0,2}\right|=16$ and then this is a $(4,16,4)$_ code. Therefore $\Phi(C^{0,2})=\{00000000\,,01010101\,,00110011\,,01100110,$ $00001111\,,01011010\,,00111100\,,01101001\,,11111111\,,$ $10101010\,,11001100\,,10011001,11110000\,,10100101\,,$ $11000011\,,10010110\}\subseteq\mathbb{F}_2^8$ is a $(8,16,4)$_Hadamard code. Let $A_4=\begin{bmatrix}1&1&1&1\\-1&1&-1&1\\-1&-1&1&1\\-1&-1&-1&1\end{bmatrix}$ 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 the complements of these vectors the 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 formed by these codewords is $\Phi(C^{0,2})$ code which is a $(8,16,4)$_Hadamard code. Moreover $(C^{0,2})^{\perp}=C^{0,2}$. $C^{0,2}$ is a cyclic code such that the equation $\tau(C^{0,2})=C^{0,2}$ is provided. Smilarly $\Phi(C^{0,2})$ is quasi-cyclic code of index 2 such that the equation $\sigma^{\otimes 2}(\Phi(C^{0,2}))=\Phi(C^{0,2})$ is provided.

5 Conclusion

Some special matrices are consturucted using the elements of the ring $\mathbb{F}_2+u\mathbb{F}_2$ with $u^2=0$. New codes generating via these matrices are obtained. It is shown that the Gray images of these codes are Hadamard codes over binary field. It is known that Hadamard codes are obtained via Hadamard matrices. It is also seen that a Hadamard code can be obtained by using the construction given in this paper.

The parameters of dual code and of Gray image of dual code are obtained. Moreover it is seen that a Hadamard code is a quasi-cyclic code of index 2.

Thanks to this paper, if we were to work on recurrent creations of Hadamard codes over $\mathbb{F}_2+u\mathbb{F}_2$, good codes would be achieved.

Acknowledgement

The authors are grateful to the anonymous referee for a careful checking of the details.

References

[1] Krotov, D. S., $\mathbb{Z}_4$-linear perfect codes,*Diskretn. Anal. Issled. Oper. Ser.*,**7.4**, 2000, 7890.

[2] Krotov, D. S., $\mathbb{Z}_4$-linear Hadamard and extended perfect codes,*Procs. of the International Workshop on Coding and Cryptography, Paris*, 2001, 329-334.

[3] Wolfmann, J., Negacyclic and cyclic codes over $\mathbb{Z}_4$,*IEEE Trans. Inf. Theory*,**45**, 1999,2592-2605.

[4] Ling S. and Blackford J. T., $\mathbb{Z}_{p^{k+1}}$-Linear codes,*IEEE Trans. Inf. Theory*,**45, no 9**,2002,2527-2532.

[5] Jian-Fa,Q., Zhang L.N. and Zhu S.X., $(1+u)$- cyclic and cyclic codes over the ring $\mathbb{F}_2+u\mathbb{F}_2$,*Applied Mathematics Letters*,**19**, 2006, 820-823.

[6] Jian-Fa,Q., Zhang L.N. and Zhu S.X., Constacyclic and cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$,*IEICE Trans. Fundamentals*,**E86-A6**,2006,1863-1865.

[7] Amarra,M.C., Nemenzo,F.R.,On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$,*Applied Mathematics Letters* ,**21**,2008,1129-1133.

[8] Udomkavanich, P. and 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*,**4 no 26**,2009,1265-1272.

[9] Roman S., Coding and Information Theory,Graduate Texts in Mathematics, *Springer Verlag* ,1992.

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

[11] Huffman,W. C. and Pless,V., Fundamentals of Error Correcting Codes, *Cambridge*, 2003.

Mustafa ÖZKAN is a research assistant of Department of Mathematics at Trakya University in Turkey. He is a phD student at the Trakya University. His research interest is algebraic coding theory.

Figen ÖKE received the phD. degree in mathematics science at the Trakya University in Turkey. She is still works as associate professor at the Trakya University. Her research area is algebra and number theory.