International Journal of Mathematics and Statistics Studies
Vol.3, No.4, pp.4- 10, July 2015
Published by European Centre for Research Training and Development UK (www.eajournals.org)

ON DESIGN OF BINARY LINEAR BLOCK CODE (BLBC) BASED ON THE COUPLED MATRICES OF HADAMARD RHOTRIX

Khalid Hadi Hameed AL-Jourany
Department of Mathematics , College of Science , University of Diyala – Iraq.

ABSTRACT : In this paper we present a new design for Binary Linear Block code (BLBC) by using the coupled matrices of Hadamard rhotrix . The Hadamard rhotrix of order 3 , 5 , 7 , 9 are used to explained our design ,as well as theorems and propositions are given for this design to the Binary Linear Block code (BLBC) with proofs .

KEYWORDS: Binary Linear Block code (BLBC) , Hadamard Rhotrix , Hamming distance.

INTRODUCTION

Rhotrix is a new concepts introduced in the literature of mathematics in 2003 [1] . It is a mathematical object which is , in some way between 2*2 - dimensional and 3*3 – dimensional matrices . A rhotrix of dimension 3 is defined as :

$$RH_3 = < a_2 \quad \begin{matrix} a_1 \\ a_3 \\ a_5 \end{matrix} \quad a_4 > \qquad \ldots (1)$$

Where $a_1, a_2, a_3, a_4, a_5 \in R$. A rhotrix of higher order is defined in [7] . Algebra and analysis of rhotrices is discussed in the literature [1-3,5-15] . Hadamard rhotrix over finite field is defined in [14-15] . Hadamard rhotrices were used in construct of Balanced Incomplete Block Design (BIBD) [13] .

The Hadamard rhotrix of order n is defined as :

$$RH_n = < a_{d,1} \quad \begin{matrix} a_{d-2,1} \\ a_{d-1,1} \\ a_{d,2} \end{matrix} \quad \begin{matrix} \cdot \\ \cdot \\ a_{d-2,2} \\ a_{d-1,2} \\ \cdot \end{matrix} \quad \begin{matrix} a_{11} \\ a_{31} \\ a_{41} \\ \cdot \\ \vdots \\ \cdot \\ a_{d,n-1} \end{matrix} \quad \begin{matrix} a_{11} \\ a_{21} \\ a_{32} \\ \vdots \\ \cdot \\ a_{d-2,n-1} \\ a_{d-1,n-1} \\ a_{d,n} \end{matrix} \quad \begin{matrix} a_{12} \\ a_{22} \\ \cdot \\ \vdots \\ \cdot \\ a_{d-2,n} \end{matrix} \quad \begin{matrix} \cdot \\ \cdot \\ a_{3,n-1} \\ a_{4,n-1} \\ a_{d-2,n} \end{matrix} \quad \begin{matrix} a_{1,n-1} \\ a_{2,n-1} \\ a_{3,n} \end{matrix} \quad a_{1,n} > \qquad \ldots (2)$$

Two coupled matrices of eq.(1.2) are :

$$V_1 = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{31} & a_{32} & \ldots & a_{3n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{d,1} & a_{d,2} & \ldots & a_{d,n} \end{bmatrix} \qquad \ldots (2a)$$

ISSN 2053-2229 (Print), ISSN 2053-2210 (Online)

$$V_2 = \begin{bmatrix} a_{21} & a_{22} & \cdots & a_{2,n-1} \\ a_{41} & a_{43} & \cdots & a_{4,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{d-1,1} & a_{d-1,2} & \cdots & a_{d-1,n-1} \end{bmatrix} \quad \ldots (2b)$$

Example (1) : Let RH_3 be a Hadamard rhotrix of order 3 defined as :

$$RH_3 = \begin{array}{<{}ccc>{}} & 1 & \\ 0 & 0 & 0 \\ & 1 & \end{array} \quad \ldots (3)$$

The coupled matrices in RH_3 are :

$$V_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \ldots (3a)$$

$$V_2 = [\,0\,] \quad \ldots (3b)$$

Having order 2 and 0 respectively .

Example (2) : The Hadamard rhotrix of order 5 is defined as :

$$RH_5 = \begin{array}{<{}ccccc>{}} & & 1 & & \\ & 0 & 1 & 0 & \\ 1 & 0 & 1 & 1 & 1 \\ & 0 & 0 & 0 & \\ & & 1 & & \end{array} \quad \ldots (4)$$

The coupled matrices in RH_5 are :

$$V_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad \ldots (4a)$$

$$V_2 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad \ldots (4b)$$

Having order 3 and 2 respectively.

Example (3) : Let RH_7 be a Hadamard rhotrix of order 7 defined as :

$$RH_7 = \begin{array}{<{}ccccccc>{}} & & & 1 & & & \\ & & 0 & 1 & 0 & & \\ & 1 & 0 & 1 & 1 & 1 & \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 0 & 1 & 1 & 1 & 1 & \\ & & 1 & 1 & 0 & & \\ & & & 1 & & & \end{array} \quad \ldots (5)$$

Two coupled matrices of RH_7 are :

$$V_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad \ldots (5a)$$

$$V_2 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \ldots (5b)$$

Having order 4 and 3 respectively .

Example (4) : Let RH_9 be a Hadamard rhotrix of order 9 defined as :

ISSN 2053-2229 (Print), ISSN 2053-2210 (Online)

$$RH_9 = < \begin{matrix} & & & & 1 & & & & \\ & & & 1 & 0 & 1 & & & \\ & & 0 & 1 & 1 & 1 & 1 & & \\ & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \\ & 0 & 0 & 1 & 1 & 0 & 1 & 1 & \\ & & 1 & 1 & 1 & 0 & 1 & & \\ & & & 1 & 1 & 0 & & & \\ & & & & 1 & & & & \end{matrix} > \quad . \quad . \quad . \quad (6)$$

Two coupled matrices of RH_9 are :

$$V_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix} \quad . \quad . \quad . \quad (6a)$$

$$V_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad . \quad . \quad . \quad (6b)$$

Having order 5 and 4 respectively .

Binary Linear Block Code (BLBC)

In this section , we shall review the some basic definitions and properties of Binary Linear Block Code , which are used further in this paper .

Definition(1): An (r , s) binary linear block code is a s-dimensional subspace of the r-dimensional vector space $P_r = \{\mathbf{c} = (c_0, c_1, \ldots, c_{r-1}) / \forall\, c_j , c_j \in \{0, 1\} = GF(2)\}$; r is called the length of the code , s th dimension .

Definition(2): An (r , s) BLBC can be specified by any set of s linear independent codeword $c_0, c_1, \ldots, c_{s-1}$. If we arrange the s code words in to a s*r matrix G , G is called a generator matrix for code C.

Definition(3): Let $\mathbf{u}=(u_0 , u_1 , \ldots , u_{s-1})$, where $u_j \in GF(2)$, then : $\mathbf{c}=(c_0, c_1, \ldots, c_{r-1}) = \mathbf{u}G$

Definition(4): Let G= [I_s : A] . Since $\mathbf{c}\, H^t = \mathbf{u}\, G\, H^t = 0$, $G\, H^t$ must be 0 .If H = [- A^t : I_{r-s}] Then $G\, H^t = \mathbf{0}_{s*(r-s)}$, thus the above H is called the parity - check matrix .

Definition(5): The Hamming distance between two code words **c** and **z** is defined as $\mathbf{d}_H(\mathbf{c} , \mathbf{z})$ = the number of components in which **c** and **z** are differ .

Definition(6): The minimum distance $\mathbf{d}_{min}$ of a binary code C , is the smallest distance between two distinct code word : $\mathbf{d}_{min} = \min \{ \mathbf{d}_H(\mathbf{c} , \mathbf{z}) / \mathbf{c} , \mathbf{z} \in C , \mathbf{c} \neq \mathbf{z} \}$.

Definition(7): A BLBC with minimum distance $\mathbf{d}_{min}$ can correct all error patterns of weight less than or equal to $\mathbf{t} = [(\mathbf{d}_{min} - 1) / 2]$, where **t** is called the error correction capability of a code C .

Definition(8): A binary block code C(r,s) of length r and $r = 2^s$ code words is called linear if its 2^s code words form a s- dimensional subspace of the vector space P_r of r- tuples over the field GF(2) = { 0, 1}.

Theorem(1)[4]: A binary code C can correct up to t –errors in any code word iff $\mathbf{d}_H(C) \geq 2t+1$.

ISSN 2053-2229 (Print), ISSN 2053-2210 (Online)

Description of the design:

Consider the Hadamard rhotrix RH_n of order n with their two coupled matrices V_1 and V_2 , then , we will have two generating matrices of the form :

$G_1 = [\ I_1 : V_1\ ]$ and $G_2 = [\ I_2 : V_2\ ]$, where I_1 and I_2 are the identity matrices their orders dependent on the order of V_1 and V_2 respectively with their parity check matrices of the form : $H_1 = [-V_1^t : I_1\ ]$ and $H_2 = [-V_2^t : I_2\ ]$. Also , the code words can be represented by : $\mathbf{c_1} = \mathbf{u}G_1$ and $\mathbf{c_2} = \mathbf{v}G_2$, where **u** and **v** ∈ GF(2) and their lengths dependent on the order of V_1 and V_2 respectively .

Note : In our work we used MATLAB program to find the code C and their minimum Hamming distance ($\mathbf{d}_{min}$) .

Figures :(1),(2),(3),(4) respectively shows the design of binary linear block code based on Hadamard rhotrix of order 3 , 5 , 7 , 9 respectively in above examples with their minimum Hamming distance and the **t-** error correction capability of a code C .

	Code words (C)	$\mathbf{d}_{min}$	$\mathbf{t} = [\ (\mathbf{d}_{min} - 1)\ /2\ ]$
$\mathbf{c_1} = \mathbf{u}G_1$	{0000,0101,1010,1111}	2	0
$\mathbf{c}_2 = \mathbf{v}G_2$	{0}	0	0

Figure(1) : Binary linear Block code C based on RH_3 .

	Code words(C)	$\mathbf{d}_{min}$	$\mathbf{t} = [\ (\mathbf{d}_{min} - 1)\ /2\ ]$
$\mathbf{c_1} = \mathbf{u}G_1$	{000000,001101,010010,011111,100101, 101000,110111,111010}	2	0
$\mathbf{c}_2 = \mathbf{v}G_2$	{0000,0100,1011,1111}	1	0

Figure(2) : Binary linear Block code C based on RH_5 .

	Code words(C)	$\mathbf{d}_{min}$	$\mathbf{t} = [\ (\mathbf{d}_{min} - 1)\ /2\ ]$
$\mathbf{c_1} = \mathbf{u}G_1$	{00000000,00010011,00101110,00111101,01000111, 01010100,01101001,01111010,10001011,10011000, 10100101,10110110,11001100,11011111,11100010, 11110001}	3	1
$\mathbf{c}_2 = \mathbf{v}G_2$	{000000,001111,010011,011100,100111,101000,110100, 111011}	2	0

Figure(3) : Binary linear Block code C based on RH_7 .

	Code words (C)	$\mathbf{d}_{min}$	$\mathbf{t} = [\ (\mathbf{d}_{min} - 1)\ /2\ ]$
$\mathbf{c_1} = \mathbf{u}G_1$	{0000000000,0000110111,0001001110,0001111001,0010001101,	3	1

ISSN 2053-2229 (Print), ISSN 2053-2210 (Online)

	0010111010,0011000011,0011110100,0100011011,0100101100,0101010101,0101100010,0110010110,0110100001,0111011000,0111101111,1000011111,1000101000,1001010001,1001100110,1010010010,1010100101,1011011100,1011101011,1100000100,1100110011,1101001010,1101111101,1110001001,1110111110,1111000111,1111110000}		
$\mathbf{c}_2 = \mathbf{v}G_2$	{00000000,00011011,00101110,00110101,01001101,01010110,01100011,01111000,10000111,10011100,10101001,10110010,11001010,11010001,11100100,111111111}	4	1

Figure(4) : Binary linear Block code C based on RH_9 .

Theorem(1): All the binary block code C which generating by the coupled matrices of Hadamard rhotrix of order 3 , 5 , 7 , 9 respectively are linear .

Proof: Consider the binary block code C which generating by the coupled matrices of Hadamard rhotrix of order 7 in figure (3) :
We need to show that : ∀ code words **x , y** ∈ C and every scalar **β** ∈ {0,1} , it holds that : **x + y** ∈ C , and **β * x** ∈ C .
However , this follows immediately from **x + y = z** ∈ C , **z** is a linear compensation of **x** and **y** .
And **β * x** belongs to C , since :
Case(1) : if **β** = 0 , then , **β * x** = 0 * **x = 0** ∈ C .
Case(2) : if **β** = 1 , then , 1 * **x** = 1 * **x = x** ∈ C .
By using the same processing for the binary block code C which generating by the coupled matrices of Hadamard rhotrix of order 3 , 5 , 9 respectively are linear .

Lemma(1) : For all the binary block code C which generating by the coupled matrices of Hadamard rhotrix of order 3 , 5 , 7, 9 respectively , are contains the zero code word **0 .**
Proof: We will give the proof , in general case :
Let **x** be a code word in C . Since C is a Linear block code (by using theorem (2)) , then **x + x** = **0 .**

Proposition(1):

1. For the code C in figure (1) ($\mathbf{c}_1 = \mathbf{u}G_1$) , we have r =4 , s= 2 .
2. For the code C in figure (2) ($\mathbf{c}_1 = \mathbf{u}G_1$) : we have r = 8 , s= 3 , and ($\mathbf{c}_2 = \mathbf{v}G_2$) : we have r =4 , s= 2 .
3. For the code C in figure (3) ($\mathbf{c}_1 = \mathbf{u}G_1$) : we have r = 16 , s= 4 , and ($\mathbf{c}_2 = \mathbf{v}G_2$) : we have r =8 , s= 3 .
4. For the code C in figure (4) ($\mathbf{c}_1 = \mathbf{u}G_1$) : we have r = 32 , s= 5 , and ($\mathbf{c}_2 = \mathbf{v}G_2$) : we have r =16 , s= 4 .

Proof:
In general proof :This is immediate from the dimension of generator matrices G_1 and G_2 .

ISSN 2053-2229 (Print), ISSN 2053-2210 (Online)

Lemma(2): The minimum Hamming distance of code C in our design is 3 or 4 .

Proof: The parity check matrices H_1 and H_2 for the code C have columns which are all nonzero and no two of which are the same . Hence C code can correct single error .By theorem (1) can correct 1-error , as well as , we conclude that the minimum Hamming distance of C code is at least 3 or 4 .

CONCLUSION:

In the present paper , we have used the Hadamard rhotrix with its coupled matrices to design Binary Linear Block Code (BLB) . Since this code can correct single error , then the Binary Linear Block Code (BLB) code is belong to error - correcting code which has useful applications in communication system .

REFERENCE:

1. Ajibade A.O., "The concepts of rhotrices in mathematical enrichment", Int.J.Math.Educ.Sci.Tech.,34(2),175-179,(2003).
2. Aminu A., "Rhotrix vector spaces ",Int.J.Math.Educ.Sci.Tech.,41(4),531-573,(2010).
3. Kanwar R.K. ,"A study of some analogous properties of rhotrices and matrices ", Ph.D.Thesis, Department of Mathematics and Statistics , Himachal Pradesh University , Shimla , India (2013).
4. Ruud P. , Xin-Wen Wu , Stanislav B. and Relinde J. ,"Error –Correcting Codes and Cryptology ". Cambridge University press, Cambridge , 2012 .
5. Sani B., "Conversion of a rhotrix to a coupled matrix ",Int.J.Math.Educ.Sci.Tech.,39,244-249,(2008).
6. Sani B.," An alternative method for multiplication of rhotrices ",Int.J.Math.Educ.Sci.Tech.,35 , 777-781,(2004).
7. Sani B.,"The row-column multiplication of high dimensional rhotrices ",Int.J.Math.Educ.Sci.Tech.,38(5),657-662,(2007).
8. Sharma P.L. and Kanwar R.K.,"A note on relationship between invertible rhotrices and associated invertible matrices ", Bulletin of Pure and Applied Sciences , 30 E (Math.and Stat.)(2),333-339,(2011).
9. Sharma P.L. and Kanwar R.K.,"Adjoint of a rhotrix and its basic properties ", International J. Mathematical Sciences, 11(3-4),337-343, (2012).
10. Sharma P.L. and Kanwar R.K.,"On inner product space and bilinear forms over rhotrices ", Bulletin of Pure and Applied Sciences , 31E(1),109-118,(2012).
11. Sharma P.L. and Kanwar R.K.,"On involutory and Pascal rhotrices ", International J . of Math.Sci.and Engg.Appls.(IJMSEA),7(IV),133-146,(2013).
12. Sharma P.L. and Kanwar R.K.,"The Cayley –Hamilton theorem for rhotrices ",International J. Mathematics and Analysis, 4,(1),171-178,(2012).
13. Sharma P.L. , Kumar S. ,"Balanced Incomplete Block Design (BIBD) Using Hadamard Rhotrices), International J. Technology. Vol.4 : Issue 1, 62-66 ,(2014).
14. Sharma P.L. , Kumar S. and Rehan M., " On Hadamard rhotrices over finite field ",Bulletin of Pure and Applied Sciences , 32 E (Math. and Stat.) , 181 -190,(2013).

ISSN 2053-2229 (Print), ISSN 2053-2210 (Online)

15. Tudunkaya S.M. and Makanjuola S.O.,"Rhotrices and the construction of finite fields ",Bulletin of Pure and Applied Sciences ,29 E(2),225-229,(2010).

ISSN 2053-2229 (Print), ISSN 2053-2210 (Online)