International Journal of Mathematical Archive-6(8), 2015, 100-103
Available online through www.ijma.info ISSN 2229 – 5046

ON ENCODING AND DECODING OF INFORMATION BY USING THE COUPLED MATRICES OF HADAMAR RHOTRIX

KHALID HADI HAMEED AL-JOURANY*

Department of Mathematics, College of Science, University of Diyala, Diyala-IRAQ.

(Received On: 11-08-15; Revised & Accepted On: 31-08-15)

ABSTRACT

In the present paper, we used Hadamard Rhotrices of order 12 with their coupled matrix to encode a binary linear block code. The standard generator matrix and the parity check matrix are given for this code. Finally, the Syndrome decoding method used to correct errors which appears in transformation information, as well as, we give example to explained this method how work.

Keywords: *Hadamard Rhotrix; Hamming distance; Hamming weight; Syndrome Decoding method.*

1. INTRODUCTION

The basic problem of coding theory is that of communication over an unreliable channel thatresults in errors in the transmitted message. It is worthwhile noting that all communication channels have errors, and thus codes are widely used In fact, they are not just used for network communication, USB channels, satellite communication and so on, but also in disks and other physical media which are also prone to errors.

In addition to their practical application, coding theory has many applications in the theory of computer science [3-4]. Rhotrix is a new concept introduce 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:

$$R_3 = < a2 \quad \begin{matrix} a1 \\ a3 \\ a5 \end{matrix} \quad a4 > \tag{1}$$

Where, a_1, a_2, a_3, a_4, $a_5 \in R$. A rhotrix of higher order is defined in [5]. Algebra and analysis of rhotrices is discussed in the literature [2], [6-9]. Hadamard rhotrix over finite field is defined in [10]. A necessary and sufficient conditions for Hadamardrhotrices and its snb-rhotrices are discussed in [9].

In [9], they are given the coupled matrix of the rhotrix R_{23} is of order 12 defined as:

$$M = \begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&0&1&0&1&1&1&0&0&0&1&0 \\ 1&0&0&1&0&1&1&1&0&0&0&1 \\ 1&1&0&0&1&0&1&1&1&0&0&0 \\ 1&0&1&0&0&1&0&1&1&1&0&0 \\ 1&0&0&1&0&0&1&0&1&1&1&0 \\ 1&0&0&0&1&0&0&1&0&1&1&1 \\ 1&1&0&0&0&1&0&0&1&0&1&1 \\ 1&1&1&0&0&0&1&0&0&1&0&1 \\ 1&1&1&1&0&0&0&1&0&0&1&0 \\ 1&0&1&1&1&0&0&0&1&0&0&1 \\ 1&1&0&1&1&1&0&0&0&1&0&0 \end{bmatrix} \tag{2}$$

From the coupled matrix M, this matrix gives fife matrices, one of them is:

$$W = \begin{bmatrix} 1&0&1&1&1&0&0&0&1&0 \\ 0&1&0&1&1&1&0&0&0&1 \\ 1&0&0&1&0&1&1&1&0&0 \\ 0&1&0&0&1&0&1&1&1&0 \\ 0&0&1&0&0&1&0&1&1&1 \\ 1&1&1&0&0&0&1&0&0&1 \end{bmatrix} \tag{3}$$

*Corresponding Author: Khalid Hadi Hameed Al-Jourany**

Note that, R_{23} Hadamardrhotrix is defined over the GF= {0, 1}.

In our work, we will use the matrix in (3) as generator matrix to construct a linear block code, and used it to: first, encode information (messages), and, second, find the standard generator matrix with their parity check matrix for a linear block code.

2. SOME BASIC CONCEPTS

Definition 1: A binary block code Q(u, v) of length u and $u= 2^v$ code words is called linear if its 2^v code words form a v-dimensional subspace of the vector space V_u of all u-tuples over the field GF(2)={0, 1}.

Basic properties of a linear block code Q(u, v):

1) The zero word (0,0,0,…,0), is always a code word.
2) If c is a code word, then (-c) is also a code word.
3) A linear code is invariant under translation by a code word. That is, if c is a code word in linear code Q(u, v), then Q+c=Q.
4) The dimension v of the linear code Q(u, v) is the dimension of Q as a subspace of V_u over GF(2), i.e, dim(Q) = v.

Definition 2: Let **a** = (a_1, a_2, . . . , a_v), and, b = (b_1, b_2,. . . , b_v). Then, for every i define

$$d(a_i, b_i) = \begin{cases} 1 & ai \neq bi \\ 0 & ai = bi \end{cases} \text{ and define:}$$

$$d(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{u} d(ai, bi) \quad (4)$$

d(**a**, **b**) is called the Hamming distance between **a** and **b**.

Definition 3: The minimum distance of a binary code Q, is the smallest distance between two distinct code word:

$$d(Q) = \min \{d(\mathbf{a}, \mathbf{b}) / \mathbf{a}, \mathbf{b} \in Q, \ \mathbf{a} \neq \mathbf{b}\} \quad (5)$$

Remark: An (u, v)-code of distance d is called an Q(u, v, d(Q)) –code. The values u, v are called the parameters of the code.

Theorem 1: A binary code Q can detect up to t-errors in any code word iff $d(Q) \geq 2t+1$.

Theorem 2: A binary code Q can correct up to t- errors in any code word iff $d(Q) \geq 2t+1$.

Definition 4: Consider a v-bit message m = (m_1, m_2,….,m_v) as a 1*v matrix. Let G be a v*u matrix that begins with the v*v identity matrix I_v. That is G=(I_v, A), where, A is a v*(u-v) matrix, known as generator matrix.

We encode m = (m_1, m_2,…,m_v) as E(m)=m*G, where we do arithmetic modulo 2.

Definition 5: The weight of a code word **a**, denoted by w(**a**), in a binary code is the number of $1^{'s}$ in this code word, and the minimum weight of a linear block code is denoted by:

$$W(Q)=\min\{w(\mathbf{a}) / a \in Q\} \quad (6)$$

Lemma 1: Suppose that **a** and **b** are code word in linear block code Q. Then: d(**a**, **b**)=w(**a**+**b**).

Theorem 2: The minimum distance of a linear block code Q equals the minimum weight of a nonzero code word in Q.

Definition 6: Suppose that G is a v*u generator matrix with:

$$G = (I_v / A) \quad (7)$$

Where A is a v *(u-v) matrix. To G we associate the parity check matrix P, where

$$P = (A^t / I_{u-v}) \quad (8)$$

Then, **a** is a code word iff $P*\mathbf{a}^t=\mathbf{0}$.

Definition 7: The dual of a code Q is denoted by: Q^* ={(**a. b**) = **0,** ∀ **a**, **b**∈Q}.

3. MAINS RESULTS

Consider the matrix in (3), and let the input information (message) m= (m_1, m_2, m_3, m_4, m_5). Since the matrix W orthogonal for each two rows in W, we will delete the last row in W to be more convenient in coding theory to get $u=2^5$ code words and the length of message 5-bits, this is shown in the following equation

$$E(m)=m*W^* \quad (9)$$

MATLAB program for encoding messages:

```
>>  % The  encoding messages by using equation (9)
>> I = (0:31)
>> str = dec2bin(i)
>> input W* % the  generator  matrix
>> E(m)= mod(double(str)*double(W),2); % the  encoding  messages
>> end
```

Theorem 3.1: The block code Q(32,5) is a linear.

Proof: we need to show that: $\forall \mathbf{a}, \mathbf{b} \in Q(32, 5)$ and every scalar $\beta \in GF\{0,1\}$, it holds that: $\mathbf{a}+\mathbf{b} \in Q(32,5)$, and, $\beta * \mathbf{a} \in Q(32,5)$.

However, this follows immediately from eq. (3.1): $\mathbf{a}+\mathbf{b} = \mathbf{c} \in Q(32, 5)$, **c** is a linear compensation of **a** and **b.** And, $\beta * \mathbf{a}$ belongs to $\in Q(32,5)$, since:

Case-1: if $\beta = 0$, then, $\beta * \mathbf{a} = 0 * \mathbf{a} = \mathbf{0} \in Q(32, 5)$.

Case-2: if $\beta = 1$, then, $\beta * \mathbf{a} = =1* \mathbf{a} = \mathbf{a} \in Q(32, 5)$.

Lemma 3.1: The zero code word **0=(**0,0,0,0,0,0,0,0,0,0) belongs to Q (32,5).

Proof: Let **a** be a code word in Q (32, 5). Since Q (32, 5) is a linear block code (by using theorem (3.1)), then, $\mathbf{a} + \mathbf{a} = \mathbf{0}$.

Proposition 3.1:

1) For the code Q (32,5), we have: u=34, v=6
2) Q (32, 5) code is self dual, meaning that: $Q(32, 5) = Q(32, 5)^*$.

Proof: (1): This is immediate from the dimension of generator matrix W^* is 5*10.
(2): we can verify that: $\sum_{i=1}^{5} a_i b_i = \mathbf{0}$, $\forall \mathbf{a}, b \in Q(32, 5)$. Thus $Q(32, 5) \subseteq Q(32,5)^*$.(because every word in Q (32, 5) is also in $Q(32,5)^*$).

Since, dimension $Q(32, 5) = Q(32, 5)^* = 32$.

We have: $Q(32, 5) = Q(32, 5)^*$.

After, we showed that the encoding messages by using W^*. Now, we calculate the parity check matrix for Q (32, 5) code: by using some operations we have:

$$P = [-A^t / I] = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (10)$$

Where P is a parity check matrix for Q (32, 5) code.

Lemma 3.2: The minimum Hamming distance of Q(32, 5) code is 3.

The parity check matrix P has columns which are all nonzero and no two of which are the same. Hence Q(32, 5) code can correct single error. By theorem (2.1) and theorem (2.2) can detect 2-errors and correct 1-error, as well as, we conclude that the minimum Hamming distance of Q(32, 5) code is at least 3.

Note that, the minimum Hamming distance is equal to the minimum Hamming weight is 3.

Now, we want to decode the binary block code Q(32,5,3) by using Syndrome decoding method with the following steps:

1) Compute the Syndrome: $S(r) = r*P^t$, where, $r=(r_1, r_2,\ldots,r_{10})$.
2) If S(r) =0, then r is the code word in Q(32,5,3).
3) If $S(r) \neq 0$, then r is not code word in Q(32,5,3).S(r) will be similar to the column of P. Which show the position of error.

MATLAB program for Syndrome Decoding Method:
>>input r
>>input P^t
>>find $S(r) = r^*P^t$

Example 3.1: Let m=(1,1,0,0,0) be the message The encoding message is (1,1,1,0,0,1,0,0,1,1). Let r=(1,1,1,0,0,1,0,0,0,1) be the transmitted code word over BSC. The problem is to find where the r is transmitted with errors or not.

Solution: From using MATLAB program in the above, we get:
S(r) =(0,0,0,1,0), since $S(r) \neq \mathbf{0}$, then r is not in Q(32,5,3) this is similar to the 9^{th} column of P. Then we have r =(1,1,1,0,0,1,0,0,1,1). Finally, r is the codeword for the message m= (1, 1, 0, 0, 0).

4. CONCLUSION

In this paper, we give anew representation method for encoding and decoding information in communication channel by using the coupled matrices of Hadamard Rhotrix. From our method, we see that, the binary block code Q(32,5,3) is belong to a single error-correcting codes which are very useful applications in communication system, coding theory and Error – Correcting codes.

5. REFERENCES

1. Ajibade A.O., "The concept of rhotrices in mathematical enrichment", Int.J.Math.Educ.Sci.Tec., 34(2), 175-179, (2003).
2. Aminu A. "Rhotrix vector space, "Int. J. Math. Educ. Sci. Tech., 41(4), 531-573, (2010).
3. HoeveH., Timmermans J. and Vries, L.B."Error correction and concealment in the compact disc system". Philips Tech. Rev. 40(166-172), 1982.
4. Robert,J., McEliece . "The reliability of computer memores", Scientific American, 252:2-7, 1985.
5. SaniB. "An alternative method for multiplication of rhotrices", Int. J. Math.. Educ. Sci. Tech., 35,777-781, (2004).
6. SaniB., "The row –column multiplication of high dimensional rhotrices", Int. J. Math. Educ. Sci. Tech., 38 (5), 657-662, (2007).
7. Sharama P.L., Kumar S. and Rehan M. "On construction of Hadamard codes using Hadamard Rhotrices". Int. J. of theortical and Applied Sciences 6(1): 102-113(2014).
8. Sharma P.L. and Kanwar R.K., "Adjoint of rhotrix and its basic properties, "Int.J.Math., Sci.11(3-4), 337-343, (2012).
9. Sharma P.L. and Kanwar R.K. "On involutory and pascalrhotrices", Int. J. Math. Educ. Sci. and Engg.Appls. (IJMSEA), 7(IV), 133-146, (2013).
10. Sharma P.L., Kumar S. and Rehan M. "On Hadamardrhotrix over finite field", Bulletin of pure and Applied Sciences", 32E (Maths. and Stat.) (2), 181-190, (2013).

Source of support: Nil, Conflict of interest: None Declared