International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.01, January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

ERROR-CORRECTING CODES AND LATIN SQUARES

Ritu Ahuja

Department of Mathematics, Khalsa College for Women, Civil Lines,
Ludhiana – 141001, Punjab, (India)

ABSTRACT

Data stored and transmitted in digital form in computers is subject to errors due to physical medium. Error correcting codes are used to correct errors occurred due to noise. They are widely used in modern technology to protect information from errors. There are various ways to construct codes. The idea of code construction with the aid of latin squares is not new. The paper reviews error correcting codes based on the concept and theory of Lain squares and the characteristics of orthogonal latin squares can be employed to correct errors in the codes.

Keywords: Error Correcting Codes, Latin Squares, Noise

I INTRODUCTION

Coding Theory is an important subject of study and of great mathematical interest. As such a great deal of research is being devoted so as to find efficient codes by which digital information can be transited reliably through a noisy channel. Noise may be human error, thermal noise, imperfections in equipment etc. Noise in the communication channel distorts (corrupts) the information, hence the message received at the receiver is different from the original message sent. Error correcting codes provide us a tool to identify any errors occurred, locate them and correct them. So that the data can be sent as reliably as possible.

II ERROR CORRECTING CODES

A binary data is a sequence of 0's and 1's. An error correcting code adds some check digits (referred to as redundancy) to the original message that helps to detect if an error occurred in the message. In addition to detection more check digits can be added so that correction can be made in the received message. Several schemes exist to achieve error detection and correction. All error detection codes transmit more bits than were in the original data. The encoder transforms an n-letter word x into an m-letter world y with n<m. The decoder has to recover x correctly when upto r letters of y may be in error. When information is sent over a channel, we

distinguish the cases whether the symbol is transmitted correctly or not. The difference of input and output sequence is measured by Hamming Distance.

Def. 1 (Hamming distance)

Hamming distance between two vectors (x_1, x_2,.... x_n) and (y_1, y_2,.. y_n) is the number of positions where x and y differ.

$$d(x,y) = \{i: x_i \neq y_i, 1 \leq i \leq n\}$$

Hamming weight of a sequence equals the number of non-zero positions in the vector.

Def. 2: A block code B of length n is a subset of all possible vectors of length n over an alphabet A.

Def. 3 (Linear Code): A q-ary linear code of length n is a subspace of vector space of all n-tuples over galois field q.

An (n,M,d)-code is a code of length n, containing M codewords and having minimum distance d. We denote by $A_q(n,d)$ the largest value of M s.t. there exists a q-ary (n,M,d)-code.

Def. 4 (Minimum distance): The minimum distance of a block code is the minimum number of positions in which two distinct codes differ i.e.

$$d_{min} = \min\{d(x,y): x \neq y\}$$

Error correcting ability of a code is related to its minimum distance.

Theorem 1: A code with minimum distance d can be used either to detect upto $d - 1$ errors or to correct upto $\frac{d-1}{2}$ errors.

Proof follows from the definition of minimum distance

LATIN SQUARE

A Latin Square of order q is a $q \times q$ array whose entries are from a set of q distinct symbols such that every symbol is contained exactly once in each row and each column.

Theorem 2: There exist a Latin square of order n for every positive integer n with Z_n as the set of objects.

Proof: We can take 1, 2, … n as the first row and cycle it round once for each subsequent row to get

1 2 3 ….. n
2 3 4 …. n 1
3 4 5 . n 1 2
……
n 1 2 ….. n – 1

Addition table of $Z_n = \frac{Z}{nZ}$ can also be taken as a Latin square of order n.

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.01, January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

ORTHOGONALITY

Def. 5 Two Lain squares A = (a_{ij}) and B = (b_{ij}) of order q are mutually orthogonal if the q^2 ordered pairs (a_{ij}, b_{ij}), $i, j = 1, 2, \ldots n$ are all distinct.

Example 1.

$$\begin{matrix} a & b & c \\ b & c & a \\ c & a & b \end{matrix} \quad \text{and} \quad \begin{matrix} a & b & c \\ c & a & b \\ b & c & a \end{matrix}$$

for a pair of mutually orthogonal Latin squares (MOLS) of order 3. Because, when superimposed they give

$$\begin{matrix} (a,a) & (b,b) & (c,c) \\ (b,c) & (c,a) & (a,b) \\ (c,b) & (a,c) & (b,a) \end{matrix}$$

Example 2: MOLS of order 2 do not exist.

Let V = {1, 2}

Only Latin squares of order 2 are $\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix}$ and $\begin{matrix} 2 & 1 \\ 1 & 2 \end{matrix}$, which are not mutually orthogonal

Latin squares from finite fields

Orthogonal Latin squares can be constructed from finite fields.We first give an example.A theorem in this regard follows.

Theorem 3: If n = p^t, where p is a prime and t ≥ 1, then there exist n – 1 mutually orthogonal latin squares of order n.

Example: We consider finite field Z_5 to construct 4 mutually orthogonal Latin squares of order 5.

Let $f_1 = 1$, $f_2 = 2$, $f_3 = 3$, $f_4 = 5$, $f_5 = 0$

The first Latin square $A_1 = (a_{ij}^{(1)})$ are given by $a_{ij}^{(1)} = f_i + f_j$

		j	1	2	3	4	5
f_i			1	2	3	4	5
i	f_i						
1	1		2	3	4	0	1
2	2		3	4	0	1	2
3	3		4	0	1	2	3
4	4		0	1	2	3	4
5	0		1	2	3	4	0

Similarly, the second Latin square $A_2 = (a_{ij}^{(2)})$ is given by $a_{ij}^{(2)} = 2f_i + f_j$

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.01, January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

f_j / i	f_i	$2f_i$	1	2	3	4	5
			1	2	3	4	5
1	1	2	3	4	0	1	2
2	2	4	0	1	2	3	4
3	3	1	2	3	4	0	1
4	4	3	4	0	1	2	3
5	0	0	1	2	3	4	0

Repeating similar calculation for A_3 and A_4 we obtain the squares:

$$A_1 = \begin{matrix} 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{matrix}$$

$$A_2 = \begin{matrix} 3 & 4 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \end{matrix}$$

$$A_3 = \begin{matrix} 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \end{matrix}$$

$$A_4 = \begin{matrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{matrix}$$

Definition 5: Let $A = (a_{ij})_{m\times m}$ and $B = (b_{ij})_{n\times n}$ two Latin square. Their direct product $C = A\times B$ is an $mn \times mn$ array, indexed by the elements of $\{1,\ldots m\} \times \{1,\ldots,n\}$ and entries $C_{(I,j),(k,l)} = (a_{ik}, b_{ji})$

Example: Consider the following two Latin square

$$\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix} \quad , \quad \begin{matrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{matrix}$$

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.01, January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Their direct product, according to definition, is

	(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)
(1,1)	(1,2), (1,3), (1,1), (2,2), (2,3), (2,1)
(1,2)	(1,3), (1,1), (1,2), (2,3), (2,1), (2,2)
(1,3)	(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)
(2,1)	(2,2), (2,3), (2,1), (1,2), (1,3), (1,1)
(2,2)	(2,3), (2,1), (2,2), (1,3), (1,1), (1,2)
(2,3)	(2,1), (2,2), (2,3), (1,1), (1,2), (1,3)

After renumbering this becomes

2	3	1	5	6	4
3	1	2	6	4	5
1	2	3	4	5	6
5	6	4	2	3	1
6	4	5	3	1	2
4	5	6	1	2	3

Theorem 4: If A and B are orthogonal Latin squares of order m, and if C and D are orthogonal Latin squares of order n. then A × C and B × D are orthogonal Latin squares.

Corollary: If $n \neq 2 \pmod 4$ then there exists a pair of orthogonal Latin squares of order n.

Proof: Let $n=p_1^{a1} p_2^{a2} \ldots\ldots pk^{ak}$ be the decomposition of n into a product of primes, while $p_1 < \ldots\ldots < p_k$, since $n \neq 2 \pmod 4$ it follows that $p_1^{a1} > 2$, and so $p_i^{ai} > 2$ for every i , by theorem (4), for each i ($1 \leq i \leq k$) there exist a pair Ai, Bi of orthogonal Latin squares of order pi^{a1}, but then the Latin square A = A1 ×…….×Ak and B = B1 ×…….×Bk are orthogonal by theorem (5) and have order n.

Theorem 5: $A_q(4,3) \leq q^2$, for all q

Proof: Suppose C is a q-ary (4, M, 3)-code and let $x = x_1x_2x_3x_4$ and $y = y_1y_2y_3y_4$ be distinct code words of C. Then $(x_1, x_2) \neq (y_1, y_2)$, for otherwise x and y could differ only in the last two paces. Contradicting d(C) = 3. Thus the M ordered pairs obtained by deleting the last two coordinates from C are all distinct vectors of $(F_q)^2$ and so we must have $M \leq q^2$

Since q^2 ordered pairs starting off the code words of such code are distinct, such a code must have form $\{(i, j, a_{ij}, b_{ij}) \mid i,j \in F^2_q\}$

We now review the connection between such codes and mutually orthogonal Latin squares.

Theorem 6: There exists a q-ary ($4, q^2, 3$) code if and only if there exists a pair of mutually orthogonal Latin squares of order q.

Proof: We show that a code

$C = \{(i,j, a_{ij},b_{ij}) \mid (i,j) \in F^2_q\}$ is ($4, q^2, 3$)-code if an only if $A = [a_{ij}]$ and $B = [b_{ij}]$ form a pair of mutually orthogonal Latin squares of order q.

Minimum distance 3 is possible if an only if for every pair of co-ordinate position, the ordered pairs appearing in those positions are distinct. The q^2 pairs (i, a_{ij}) and q^2 pairs (j, a_{ij}) are distinct if and only if A is a Latin square. q^2 pairs (i, b_{ij}) and (j, b_{ij}) each are distinct if an only if B is a Latin square. Finally q^2 pairs (a_{ij}, b_{ij}) are distinct if an only if A and B are mutually orthogonal.

So, Aq (4, 3) = q^2 if an only if there exists a pair of MOLS of order q.

Theorem7: If q is a prime power and $q \neq 2$, then there exists a pair of orthogonal Latin squares of order q.

Proof: Let F_q be the field GF(q) = $\{\lambda_0, \lambda_1, \ldots\ldots \lambda_{q-1}\}$, where $\lambda_0 = 0$ (if q is prime, we may take $\lambda_i = i$ for each i). Let μ and v be two distinct non-zero elements GF(q). Let A = $[a_{ij}]$ and B = $[b_{ij}]$ be q×q arrays defined by

$a_{ij} = \lambda_i + \mu\lambda_j$ and $b_{ij} = \lambda_i + v\lambda_j$

(The rows and columns of A and B are indexed by 0, 1,…….q – 1). We first verify that A and B are Latin squares. If two elements in the same row of A are identical, then we have

$\lambda_i + \mu\lambda_j = \lambda_i + \mu\lambda_{j'}$, i.e. $\mu\lambda_i = \mu\lambda_{j'}$ and

Implying $j = j'$, since $\mu \neq 0$. Similarly, if two elements in the same column of A are identical, then we have

$\lambda_i + \mu\lambda_j = \lambda_{i'} + \mu\lambda_j$, i.e. $\lambda_i = \lambda_{i'}$

Implying that i = i'. Thus A, and similarly B, are Latin squares. To show A and B are orthogonal, suppose on the contrary that $(a_{ij}, b_{ij}) = (a_{i'j'}, b_{i'j'})$, i.e. assume that the same ordered pair appears twice in the superposition of the squares. Then

$$\lambda_i + \mu\lambda_j = \lambda_{i'} + \mu\lambda_{j'}$$

and $$\lambda_i + v\lambda_j = \lambda_{i'} + v\lambda_{j'}$$

which on subtraction implies that

$$(\mu - v)\lambda_j = (\mu - v)\lambda_i$$

Since $\mu \neq v$, we have j = j' and, consequently i = i'

Cor. Consider the field GF(q) = $\{\lambda_0, \lambda_1, \ldots\ldots \lambda_{q-1}\}$, where $\lambda_0 = 0$.Let $A_1, A_2, \ldots A_{q-1}$ be qxq arrays,with rows and coloumns indexed by 0,1,2,….q-1, in which (i,j)th entry of A_k is the element of GF(q) defined by $a_{ij}^{(k)} = \lambda_i + \lambda_k \lambda_j$ It follows exactly as in the proof of above theorem,that $A_1, A_2, \ldots A_{q-1}$ form a set of mutually orthogonal latin squares of order q.This proves theorem 7.

Theorem 8: If q = 0, 1, or 3 (mod 4), then there exists a pair of mutually orthogonal Latin square of order q.

Proof: Suppose q = 0, 1 or 3 (mod 4). Then q is either odd or is divisible by 4. Hence, if $q = p_1^{h_1} p_2^{h_2} \ldots\ldots\ldots p_t^{h_t}$ is the prime factorization of q, where $p_1, p_2 \ldots\ldots\ldots p_t$ are distinct primes and $h_1, h_2 \ldots\ldots h_t$ are positive integers, then $p_i^{h_i} \geq 3$ for each i. Thus, by Theorem 10.8, there exists a pair of MOLS of order $p_i^{h_i}$ for each i. Repeated application of Theorem 10.10 then gives a pair of MOLS of order $p_1^{h_1} p_2^{h_2} \ldots\ldots\ldots p_t^{h_t} = q$

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.01, January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

According to Bose, Shrikhande and Parker (1960). There exists a pair of mutually orthogonal Latin squares of order q for all q except q = 2 and 6.

An important result follows from this and theorems 5 and 6

Result: $Aq(4,3) = q^2$ for all $q \neq 2, 6$

Theorem 9: $A_6(4, 3) = 34$

Proof: The arrays

$$A = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 3 & 4 & 6 & 5 & 1 & 2 \\ 4 & 3 & 5 & 6 & 2 & 1 \\ 5 & 6 & 2 & 1 & 4 & 3 \\ 5 & 6 & 2 & 1 & 4 & 3 \\ 6 & 5 & 1 & 2 & 3 & 4 \end{array} \quad \text{and } B = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 6 & 5 & 1 & 2 & 4 & 3 \\ 4 & 3 & 6 & 5 & 2 & 1 \\ 5 & 6 & 2 & 1 & 3 & 4 \end{array}$$

form a pair of Latin squares which are as close to being orthogonal as is possible. They fail only in that $(a_{65}, b_{65}) = (a_{13}, b_{13})$ and $(a_{66}, b_{66}) = (a_{14}, b_{14})$. Thus the code

$\{(i, j, a_{ij}, b_{ij}) \mid (i, j) \in (F_6)^2, (i, j) \neq (6, 5) \text{ or } (6, 6)\}$ is a (4, 34, 3)-code.

Now if there existed a (4, 35, 3)-code C over F_6, then C would have the form

$$\{(i, j, a_{ij}, b_{ij}) \mid (i, j) \in (F_6)^2, (i, j) \neq (i_0, j_0)\}$$

for some (i_0, j_0). It can be shown that the partial 6×6 arrays $A = [a_{ij}]$ and $B = [b_{ij}]$, each having the $(i_0, j_0)^{th}$ entry missing, can be completed to Latin squares which must be mutually orthogonal. This contradicts Tarry's non-existence result of mutually orthogonal squares of order 6.

Theorem 10: A q-ary $(n, q^2, n-1)$-code is equivalent to a set of n – 2 mutually orthogonal Latin square of order q.

Proof: As in theorem ,an $(n,q^2, n-1)$-code C over F_q has the form

$\{ (i,j,a_{ij}^{(1)}, a_{ij}^{(2)},\ldots, a_{ij}^{(n-2)}) \mid (i,j) \text{ ε } (F_q)^2\}$

It can be shown that d(C)= n-1 if and only if $A_1, A_2,\ldots A_{n-2}$,where $A_k= [a_{ij}^{(2)}]$

III CONCLUSION

There are various ways of constructing error correcting codes. Constructing them with the help of Latin squares provides another efficient way of constructing error correcting codes. We have seen a connection between the error connecting codes and Latin squares. In this regards, the optimal codes of length 4 and distance 3 were reviewed in this paper. Codes of higher length and distance can also be constructed using Latin squares. However, the codes of higher length are constructed with help of isotopic Latin squares. Abstract Latin squares, block designs and finite geometry, which is not the scope of present paper.

REFERENCES

1. E. R. Berlekamp, *algebraic coding theory* (MC Graw - Hill).

2. A. Nayak, *error-correction codes* (UWMath 135, July 29, 2005).

3. R.Hill A, *first course in coding theory* (clarendon press,Oxford).

4. Sagheer AM, Abdul-Jabbar MAW, Error correcting codes using latin square. J. of al-anabar university of pure science 2 (3), 2008, 1-10.

4. J. Higham , A Product Theorem For Row- Complete Latin Squares. *J. Combi. Des 5*, 1997, 311-318.

5. M. Y. Hsiao, D. C. Bossen and R. T.Chien, Orthogonal Latin Square codes, 1969

6. http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/LATIN%20SQUARESandCODES.htm

7. R.M.Wilson, *Concerning the number of mutually orthogonal latin squares* (Discrete Math., 9/1974, 181-198)