Mutually orthogonal Latin Squares and LSECC
Duncan Prince, Jenny Zhang
January 19, 2015

Author: Duncan Prince
Mutually Orthogonal Latin Squares

A Latin Square is an n by n array filled with n unique symbols. Each symbol appears once in each row and column.
Definition. Two Latin Squares of the same n are said to be "mutually orthogonal" if when you consider the entry from each Latin Square in the same row and column as an ordered pair, and each ordered pair only shows up once. This is a tough concept to explain and understand, so an illustration is very helpful. The image below shows an example of two mutually orthogonal Latin Squares and their "ordered pairs"

1	2	3
2	3	1
3	1	2

,

1	2	3
3	1	2
2	3	1

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

The ordered pairs corresponding to these Latin Squares are in the grid on the right. The ordered pair for the first row and column would be $(1,1)$, and the pair for the first row and second column would be $(2,2)$, and so on.

Each of these ordered pairs must appear only once for the two Latin Squares to be considered mutually orthogonal.

Now that we understand the concept of mutual orthogonality, we can discuss properties and uses of mutually orthogonal Latin Squares. Firstly, it is possible to have more than two Latin Squares that are mutually orthogonal. More than two Latin Squares can all be mutually orthogonal with each other. We have only found the "maximum" amount of mutually orthogonal Latin Squares for very small values of n. One important application of this concept and mutually orthogonal Latin Squares is error correcting codes.
Source: "Latin Squares and Their Applications" by J.Denes A.D.Keedwell.

Author: Jenny Zhang
LSECC: Latin Square Error Correcting Code.
This is a error correcting code method which is used to save the information for the lost may be occur in the transmission media. This technique is uses the characteristics of the Orthogonal Latin Squares and employ it to correct most of the simultaneous errors in bits caused by noise.

Definition:The distance d of a block code is the minimum number of positions in which any two distinct codewords differ
Definition: A code is said to be t-error correcting if when no more than t-error has occured in the transmission of codeword.

If we have $n * n$ Lain Square (aij)(which represents the component in a Latin Square), we can build n^2 codewords, by using ordered triples(i,j,aij), which means (row, column, and the number corresponding to that). These triples are of Hamming distances of at least 2 apart because of constructions Latin Square.

Example.

Let the Latin Square of group Z3, the codewords are:
The latin Square:

$$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$$

The code words:
$(0,0,0),(0,1,1),(0,2,2),(1,0,1),(1,1,2),(1,2,0),(2,0,2),(2,1,0),(2,2,1),$
A single error detecting code formed from Z3 and its corresponding codewords.

Theorem: Any pair of orthogonal Latin Square of order n yields a 1-error correcting code with n^2 code words.

Proof: Let the n^2 code words of length 4 over the alphabet $\{0,1,...,n-1\}$ the code words are merely the 4-tuples code words of the form (i,j,aij,bij) $0 \leq i,\ j \leq n-1$, such that $[aij] = A$ and $[bij] = B$ forming two Latin Squares.
Suppose that $w = (i,j,aij,bij)$ and $w' = (i',j',aij',bij')$ are two such words.
If i=i' and j=j', then clearly the two words are the same. If $aij = ai'j'$ and $bij = b'i'j'$, they must be the same words, since A and B orthogonal. If $i = i'$ and $aij = a'i'j'$ then the words are same, since A is Latin Square.
The other cases are all similar. So the distance of those codewords are 3. And any two codewords of distance 3 which will be corrected one error.

Now, from this theorem we can use sets of orthogonal Latin Squares to construct codes.

If we have $q*q$ Latin Square $L_1, L_2, ..., L_n$, we construct codewords by taking a coordinate pair and adjoining the corresponding element from each Latin Squares. $(i,j,L_1,L_2...,L_n)$
These q^2 codewords have hamming distance of at least $2t+1$ from each other.

We can show that any pair of orthogonal Latin Squares of order n yields a 1-error correcting code with n^2 code words of length 4 over the alphabet $\{0,1,...n-1\}$. Thus any two code words at distance 2 or less are the same and have a code of distance 3 which will correct one error.

Example:
Here is a pair of orthogonal Latin square in mod 4.
$A =$

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}$$

$B =$

$$\begin{bmatrix} 0 & 3 & 2 & 1 \\ 2 & 1 & 0 & 3 \\ 1 & 2 & 3 & 0 \\ 3 & 0 & 1 & 2 \end{bmatrix}$$

The codewords generated from the above orthogonal Latin Square are:

$$(0,0,0,0),(0,1,1,3)(0,2,2,2)(0,3,3,1),(1,01,2),(1,1,0,1)$$
$$(1,2,3,0),(1,3,2,3),(2,0,2,1)(2,1,3,2)(2,2,0,3),(2,3,1,0),$$
$$(3,0,3,3),(3,1,2,0),(3,2,1,1),(3,3,0,2)$$

When the sender want to transmit the following bits:
10 11 02 10 00 01 11 01
The sender do the following for each four bits: Takes the four bits to makes it pair of two bits numbers(i,j)
1.Takes the codewords as (i,j,aij,bij). Send the codeword (i,j,aij,bij)
we set 00=0, 01=1,10=2,11=3
Send the following code word as obtained below:
10=2
11=3
Then he send the codeword:(2,3,1,0)=10 11, 01, 00
01=1
10=2
Then he send the codeword:(1,2,3,0)=01 10 11 00
00=0
01=1
Then he send the codeword:(0,1,1,3)=00 01 01 11
11=3
01=1
Then he send the codeword:(3,1,2,0)=11 01 10 00
And so on for other bits in the transmission media.

Therefore, the data: 1011 0110 0001 1101 is encoded into 1011 0100 0110 1100 0001 0111 1101 1000 and transmitted

Suppose the transmitted bits affected by noise cause the following errors:
1001 0100 0101 1100 1101 0111 1101 0000
The receiver takes each codeword and match with its possible code words and do the following for each eight bits:
1. If the received code match with one of the possible code words there is no error.
2. If the received codeword don't match with one of the possible code words to find almost match three symbols of the codeword and correct it. He takes the first two symbols of the corrected codeword as four bits.
3. Otherwise there is damage in the transmission and send an acknowledgement to the sender to retransmit the data.

Take the first eight bits: 1001 0100 has a single error; the error codeword is 1001 0100=(2,1,1,0). Therefore, the codeword (2,3,1,0) is the only codeword of all the possible codewords that match three elements of the error codeword. So we know that the third bit is changed from 1 to 0. So he should receive 1011.

Take the second eight bits: 0101 1100 have two simultaneous errors; the third bit is changed from 1 to 0 and the fourth bit changed from 0 to 1, where the error codeword is 0101 1100=(1,1,3,0). Therefore, (1,2,3,0) is the only possible codeword of all codewords that matches three elements of the error codeword. So he should receive 0001.

Take the third eight bits: 1101 0111, which have two simultaneous error. The error codeword is (3,1,1,3). (0,1,1,3) is the only possible codeword that can matches with (3,1,1,3) in three same bits. (0,1,1,3)=0001 0111. So he should receive 0001.

Take the fourth eight bits: 1101 0000 has single bit error, where the error codeword is 1101 0000=(3,1,0,0). Therefore, (3,1,2,0) is the only possible codeword of all codewords, that matches three elements of the error codeword. So he should receive 1101. Finally, he receives the data 1011 0110 0001 1101.

Sources: "ERROR CORRECTING CODE USING LATIN SQUARE", by Ali Makki Sagheer