P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2007,(1), (1 ) :76-81

# THE CONSTRUCTION AND MAXIMAL SET OF MUTUALLY ORTHOGONAL LATIN SQUARES

**MAKARIM A. AL-TURKY**

COMPUTER COLLEGE - UNIVESITY OF AL-ANBAR

**A R T I C L E I N F O**

Received: 25 / 8 /2006
Accepted: 1 / 3 /2007
Available online: 14/6/2012
DOI: 10.37652/juaps.2007.15496
**Keywords:**
Construction .
Maximal Set .
Mutually Orthogonal Latin Squares.

**A B S T R A C T**

Given aset of permutation {p1,p2, … . pk} on aset S, we say that the set of permutation is transitive on S if for every ordered pair of elements a,b € S, there exists at least on Pi for which (a) Pi=b. A permutation set for which there is exactly one Pi which maps a to b is called Sharply transitive.

For example, if on the set consisting of the three elements {1,2,3} we represent the permutation which maps 1 3 ,2 2 and 3 1by (321). Then the following set of permutation is transitive.(123),(132),(213) and (321) and the last three permutation form sharply transitive set. This construction give a set of mutually orthogonal latin squares. A set S of mutually orthogonal latin squares(MOLS) is maximal if no latin square is orthogonal to each member of S.

**Introduction:**

A latin square is an arrangement of m variables x1, x2, ….,xm into m rows and m columns such that no row and no column contains any of the varibables twice. Many of the application in the theory of latin squares involves same are lationship between squares of the order called orthogonally.

Two latin squares L1=|aij| and L2=|bij| on n symbols 1,2,…n are said to be orthogonal if every order pair of symbols occurs exactly once among the n2 pairs (aij,bij), i=1,2,…..,n. j=1,2,……n

For example, a pair of orthogonal order 3 latin squares and the q distinct ordered pairs that they form

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 1 | 2 | 1 | 3 | 2,2 | 3,1 | 1,3 |
| 1 | 2 | 3 | 1 | 3 | 2 | 1,1 | 2,3 | 3,2 |
| 3 | 1 | 2 | 3 | 2 | 1 | 3,3 | 1,2 | 2,1 |

Euler was originally interested in such pairs and in his writings he would always use latin letters for the first square and greek letters for second.

Thus, when he referred to only one of the squares he called it the latin square, when referring to both of the orthogonal square he used the term graeco; latin squares, which is the way orthogonal squares are referred to in all the earlier literature.

Orthogonal Mates: given apair of orthogonal latin squares, consider the cells in the first square which contain one particular sympol. By latiness, there is only one of these cells in each row and column, Now consider the cells in the orthogonal matt which correspond to these cells the first square. By orthogonally, the entries in these cells must all be different and so these cells form atransversal in the orthogonal mate.

Theorem (2-1): A given latin square possesses an orthogonal mate if and only if it has n disjoint transversals.

Theorem (2-2): the multiplication table of any group of odd order form a latin square which possesses an orthogonal mate.

* Corresponding author at: COMPUTER COLLEGE - UNIVESITY OF AL-ANBAR, Iraq.
E-mail address: mak_alturky@yahoo.com

Proof: By [1] agroup of odd order has a complete mapping, so by [1] the multiplication table of this group is a latin square which has a transversal. Thus, we have this latin square has an orthogonal mate.

Corollary (2-3): There exist pairs of orthogonal latin squares of every odd order.

Euler's conjecture(2-4): There does not exist an orthogonal mate for any latin square whose order has the form n=4k+2

Theorem (2-5): For any order n≠2 or 6, there exists a pair of orthogonal latin a squares order n.

Definition

Set of Mutually orthogonal latin squares [MOLS]. A set of latin squares of the same order, each of which is an orthogonal mate of each of the othoers is called [MOLS].

For example

| | | |
|---|---|---|
| 1 0 3 2 | 2 3 0 1 | 3 2 1 0 |
| 2 3 0 1 | 3 2 1 0 | 1 0 3 2 |
| 3 2 1 0 | 1 0 3 2 | 2 3 0 1 |
| 0 1 2 3 | 0 1 2 3 | 0 1 2 3 |

Lemma (3-1)[Standard form]: Any set of MOLS is equivalent to a set where each square has the first row in natural order and one of the squares (usually the first) is reduced (it also has its first column in natural order).

Proof: Given a set of MOLS, we can convert it to an equivalent set by renaming the elements in any or all squares, If we do this to each square, we can make the first rows be any thing we like, in particular, we can put them all in natural order. Now, take any square and simultaneously permute the rows of all the squares, so that the first column of this square is in natural order (this will not affect the first row, since it is in natural order and so strarts with the smallest element) The result is an equivalent set with the required properties.

Propostion (3-2): Any set of MOLS is equivalent to a set of MOLS in standard form.

Theorem (3-3): No more than n-1 MOLS of order n can exist.

Proof: Any set of MOLS of order n is equivalent to a set in standard form, which of course has the same number of squares in it.

Consider the enteries in first column and second row of all of the square in standard form.

No two squares can have the same entry in this cell.

Suppose two squares had an r, say, in this cell, then in the superimposed square, the ordered pair (r,r) would appear in this cell and also in the r-th cell of the first row because both squares have the same first row, and so, the two squares can not be orthogonal contradiction.

Now, we can not have a 1 in this cell, since it appears in the first column of the first row.

Thus, there are only n-1 possible entries for this cell and so there can be at most n-1 squares.

Theorem(3-4): Suppose that there exist r MOLS of order n and r MOLS of order m, then there exist r MOLS of order mn.

Proof: Let $A^{(1)}$, $A^{(2)}$……..,$A^{(r)}$ be the set of MOLS of order m and $B^{(1)}$,$B^{(2)}$,…….$B^{(r)}$ be the set of MOLS of order n. for e=1,2,……..,r.

Let ($aij^{(e)}$, $B^{(e)}$) represent the n x n matrix whose h, k entry is the ordered pair ($aij^{(e)}$, $bij^{(e)}$).

Let $C^{(e)}$, be the mn x mn matrix that can be represented schematically by

| | | | |
|---|---|---|---|
| **($9_{11}^{(e)}$, $B^{(e)}$)** | **($9_{12}^{(e)}$, $B^{(e)}$)** | **…** | **($9_{1m}^{(e)}$, $B^{(e)}$)** |
| **($9_{21}^{(e)}$, $B^{(e)}$)** | **($9_{22}^{(e)}$, $B^{(e)}$)** | **…** | **($9_{2m}^{(e)}$, $B^{(e)}$)** |
| **……..** | | | |

P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2007,(1), (1 ) :76-81

| $(9_{m1}^{(e)}, B^{(e)})$ | $(9_{m2}^{(e)}, B^{(e)})$ | … | $(9_{mm}^{(e)}, B^{(e)})$ |
|---|---|---|---|

We will show that $C^{(1)}, C^{(2)}, \ldots, C^{(r)}$ is a set of MOLS of order mn.

We must show that $C^{(e)}$ is a latin square.

Note, first that in a given row, two entries in different columns are given by $(aij^{(e)}, buv^{(e)})$ and $(aik^{(e)}, buw^{(e)})$ and so are distinct since $A^{(e)}$, and $B^{(e)}$ are latin square.

In a given column two entries in different rows are distinct by the same reasoning.

Now, to see that $C^{(e)}$, and $C^{(f)}$ are orthogonal, suppose that

$((aij^{(e)}, duv^{(e)}), ((aij^{(f)}, buv^{(f)})= ((a_{pq}^{(e)}, b_{st}^{(e)}), (a_{pq}^{(f)}, b_{st}^{(f)}))$

Then it follows that

$((aij^{(e)}, aij^{(f)})= ((a_{pq}^{(e)}, a_{pq}^{(f)})$

So, by orthogonality of $A^{(e)}$and $A^{(f)}$, i=p and j=q similarly, or thogonality of $B^{(e)}$ and $B^{(f)}$ Implies that u=s and v=t.

Theorem(3-5): (MaCneish's theorem) [4]: Suppose that $n=P^a{}_1, P^b{}_2, P^c{}_3 \ldots P^t{}_s$ is the prime power decomposition of n, n>1, and r is the smallest of the quantities$(P_1{}^q-1), (P_2{}^b-1), \ldots, (P_s{}^t-1)$ then $N(n) \geq r$.

Where N(n) is the maximum number of MOLS of order n.

Proof: for each prime power $P^*$ in the decomposition we know that there are $P^*$-1 MOLS of that order.

Thus, there are r MOLS for each $P^*$.

Since r is the smallest of theser values.

So, by theorem above r MOLS of order n.

This conjecture was put to rest in 1959 when E.T. Parker [2] shown that $N(21) \geq 4$ by constructing a set of 4 MOLS of oreder 21 the lower bounds of N(n) has shown that

$N(n) \geq 3$ for all $n \geq 52$

$N(n) \geq 4$ for all $n \geq 53$

$N(n) \geq 5$ for all $n \geq 63$

$N(n) \geq 6$ for all $n > 9$

It is also known that $N(n) \longrightarrow \infty$ as $n \longrightarrow \infty$

Corollary(3-6) : If n is not of the form 4k+2, then $N(n) \geq 2$

Proof: For n of this type, either 2 is not a divisor or its power is grater than 1.

In either case, the smallest possible value of $P^*$-1 is 2.

MaCNeish belived that his theorem actually gave the upper bound for N(n) as well (this is true for prime powers).

Therom(3-7): if alatin square L of order 4k+2 contains a latin subsquare of order 2k+1, then L has no orthogonal mate.

Proof: it is easily see that if a latin square has an orthogonal mate. Then any isotope of it also has a mate. $\square$

So we can, without loss of genrality, assume that the sub square occupies the first 2k+1 rows and columns for if not then row and colomn permutations will put it there.

The square L is thus partitioned in to 4(2k+1) * (2k+1) submatrices which we will label as:

$$\left\| \begin{matrix} A & B \\ C & D \end{matrix} \right\|$$

Where A is the given latin subsquare.

Let the 2k+2 symbols which appear in A form a set S, and the remaning 2k+1 symbols of L form a set Q.

No element of S can appear in B or C since both L and A are latin, therfor D is composed entirely of elements of S and B and C entirely of elements of Q (in fact, all four are latin subsquare).

Now con sider a transversal T of L.

Say that there are h cells of t which appear in A since 2k+1 cells of Tmust appear in the first 2k+1 a row of L, and h of these are in A the remaning 2k+1-h must appear in B.

A similar argument for the first 2k+1 column shown that there must be 2k+1-h cells of t in C. in these cells of B and C, all the elements of Q must appear exactly once.

Since ther are 2K+1 elements of Q,

We have 2(2k+1-h)=2k+1

Or this is clearly impossible if h and k are integers, so we may conclude that L has no transversal.

**Construction:**

let $S_1=i$, $S_2,S_3,\ldots\ldots S_r$ be the permutations representing the row of r x r latin square L1 as permutations of its first row and $M_1=i$, $M_2$, $M_3,\ldots M_h$, $h\leq r$, be permutations keeping one sympole of L1 fixed, then the squares $L_i^*$ whose rows are represented by the permutations $M_i\ S_1$, $M_i\ S_2,\ldots\ldots$, $M_i\ S_r$ for i=1,2,…..,h are all latin and will be mutaually orthogonal if, for every choice of i, j $\leq$h, the set of permutations

$S_1^{-1}M_i^{-1}M_jS_1$, $S_2^{-1}M_i^{-1}M_jS_2,\ldots\ldots$, $S_r^{-1}M_i^{-1}M_jS_r$,

Is harply transitive on the sympols of L1.

let L1 be the 4*4 latin square

1 2 3 4

2 1 4 3

3 4 1 3

4 3 2 1

The rows of this square, considered as permutation provide the S's, So

$S_1$= (1 2 3 4), $S_2$= (2 1 4 3), $S_3$= (3 4 1 2), $S_4$= (4 3 2 1)

Now let $M_1$= ( 1 2 3 4 ), $M_2$= ( 1 4 2 3 ), $M_3$= (1 3 4 2),

All of which fix the symbol 1.

Direct calculation now gives as the following:

$M_1S_1$= ( 1 2 3 4), $M_2S_1$= ( 1 4 2 3 ), $M_3S_1$=(1 3 4 2)

$M_1S_2$= ( 2 1 4 3), $M_2S_2$= ( 2 3 1 4 ), $M_3S_2$=(2 4 3 1)

$M_1S_3$= ( 3 4 1 2), $M_2S_3$= ( 3 2 4 1 ), $M_3S_3$=(3 1 2 4)

$M_1S_4$= ( 4 3 2 1), $M_2S_4$= ( 4 1 3 2 ), $M_3S_4$=(4 2 1 3)

So, the three latin square produced are:

| | | |
|---|---|---|
| 1 2 3 4 | 1 4 2 3 | 1 3 4 2 |
| 2 1 4 3 | 2 3 1 4 | 2 4 3 1 |
| 3 4 1 2 | 3 2 4 1 | 3 1 2 4 |
| 4 3 2 1 | 4 1 3 2 | 4 2 1 3 |

and it is not too difficult to see that this is a complete set of MOLS.

Choice of i=2 and j=3, the set of permutations

$S_1^{-1}M_2^{-1}M_3S_1$= (1 4 2 3)

$S_2^{-1}M_2^{-1}M_3S_2$= (3 2 4 1)

$S_3^{-1}M_2^{-1}M_3S_3$= (4 1 3 2)

$S_4^{-1}M_2^{-1}M_3S_4$= (2 3 1 4)

We see that it is a sharply transitive set of permutations on {1,2,3,4}. The same is true for any other choices of i and j.

**Proof of construction:**

First, notice that since L1 contains each symbol exactly once in each column, the permutations $S_1,S_2,\ldots.S_r$ must form a sharply transitive set. If we multiply each of these by afixed permutation, the new set of permutations is again sharply transitive, consequently the columns (and of course the rows) of Li will contain each symbol exactly once, So Li will be Latin.

Secondly, if $U_1,U_2,\ldots,U_r$ are permutations representing the rows, of one latin square Li and if $W_1,W_2,\ldots W_r$ are the permutations representing the rows of another square Lj, then the permutations $U^{-1},W_1,U_2^{-1}W_2,\ldots.,U_r^{-1}W_r$ map the first, second, ….., r-th row of Li respectively to the first, second,….., r-th row of Lj.

If and only if these squares are orthogonal each symbol of Li must map exactly once onto each of the symbols of Lj since each symbol of Li occurs in positions corresponding to those of a transversal of Lj. Thus, Li and Lj are orthogonal iff the permutation $U_1^{-1}W_1, U_2^{-1}W_2,\ldots,U_r^{-1}W_r$ form a sharply transitive set.

To find the permutations Mi of these construction can be found in chapter 7 of Denes & Keedwell.

5-Trails, E.T. Parker's criterion:

Let Є={L1,…s} be a set of MOLS of order υ for each t, represent Lt as Lt= $\begin{vmatrix} A_t & B_t \\ C_t & D_t \end{vmatrix}$

Let $1\le r \le \upsilon$. Suppose that At is a latin square of order r for each t, and that Є is obtained from Є by performing a common row permutation on the Li's and a common column permutation on the Li's. then $Є^-$ is said to be an s-set of (υ, r) –MOLS.

With out loss of generality, we assume that the entries of each Lt of Є belong to a common set of υ elements and that the entries of each At belong to a common subset ∑ of cardinality r. Elements of the set are called little if they are in ∑, big if they are not. A cell is a pair (i, j) with $1\le i, j\le \upsilon$. One says that the (i, j) th entry of a matrix is in cell (i, j) and that the cell(i,j) is in or from row i and column j. We define the trail of Є to be the set of all cells (i, j)with r< i, j such that the (i, j) th entry of Lt is big for each Lt in Є.

Theorem (5-1): (E.T. Parker, 1963, see [7, Theorem 12.3.3])

Let Є be an s-set of (Sr+r+Є,r)MOLS, then Є ≥0, and the trail consists of Є (Sr+Є) cells.

Theorem (5-2): (E.T.Parker, 1963, see [7, theorem 12.3.4]. Let Є be an S-set of (Sr+r+ Є,r) MOLS, Then Є is maximal if $[r^2/ (sr+r+ Є)] < (r- Є)/(s+1)$.

Definition (5-3): A transversal T of Lt is a set of υ cells from distinct rows and distinct columns such that the entries of Lt in T are distinct.

A common transveral to L1,…Ls is called a transversal of Є.

Lemma (5-4): let Є be an s-set of (sr+r+ Є, r) MOLS. If T is a transversal to Є which contains x cells of the subsquares, then T contains x (s+1)-r+ Є cells of the trail.

Proof: Since T meets Sx little entries in the At's,T must meet sr-sx little entries in the Dt's.

Thus, T intersects D1 in sr-sx non-trid cells since T intersects A1 in x cells,T intersects B1in r-x cells and D1 in (sr+ Є) – (r-x)= sr-r+x+ Є cells altogether. $\begin{vmatrix} A_t & B_t \\ C_t & D_t \end{vmatrix}$

Proof of theorem(5-2): suppose that Є is an s-set of (sr+r+ Є,r) MOLS which is not maximal. Then there exists a common orthogonal mate L which induce Sr+r+ Є disjoint transversals on Є.

One of these transversals T contains x cells of the Ai's for some $x\le[ r^2/(sr+r+ Є)]$.

By lemma above, T contains x (s+1)-r+ Є≥0 trail cells. Thus, inequality (1) fails.

Corollary(5-5): Let Є be an s-set of (sr+r+ Є,r) MOLS with Є≥0. If the residue δ of Є-r modulo s+1 satisfies 0≠δ ≥ Є, then Є is maximal.

Proof: Assume, by way of contradiction, the existence of a latin square L which is orthogonal to each square of Є. By lemma above, each of the sr+r+ Є transversal to Є induced by L meets the trail of Є in at least δ cells. Thus, theorem [1] yields the contradiction Є (sr+ Є) ≥ (sr+r+ Є) max { Є,1}.

Corollary(5-6): let Є be an s-set of (sr+r+1,r) MOLS if r ≡1 modulo s+1, then Є is maximal.

**References**

[1]. J. Denes, A.D.Keedwell, latin squares and their ap plications, English Universities Press, London, 197 4, Chapter 5, 11 and 12

[2]. E.T. Parker, "Construction of some sets of mutuall y orthogonal latin squares," Proceedings of the Am erican Mathematical Society, 10 (1959), PP. 946-9 49.

[3]. Henry B. Mann, " The construction of orthogonal l atin squares", Columbia University Mathematical S ociety October 31st, 1942, PP 418-422.

[4]. H.F. Macneish, " Euler squares", Annals of Mathe matics, 23 (1922) PP. 221-227.

[5]. Bose, R.C. & Shrikhande, S.S., "On the constructio n of sets of mutually orthogonal latin squares and F alsity of a conjecture of Euler Transactions of the Am erican Mathematical Society, 95 (1960), PP. 191-209.

[6]. H.B. Mann "on orthogonal latin squares", Bulletin of the American Mathematical society, 50 (1944), PP.24 9-257.

[7]. David A. Darke, G.H.J. Van Rees, W.D.Wallis, "Max imal sets of mutually orthogonal latin squeres" Discre te Mathematics, 194 (1999), PP.87-94.

[8]. D. Jungnickel, Maximal sets of mutually orthogonal l atin squares, in: S.Cohen, H. Niederraiter Eds). Proc. 3rd Intern. Conf. at Univ. Glasgow, 1995, London Mat h. Soc. Lecture Note Series, 233, Cambridge Univ. Pr ess, Cambridge, 1996, PP.129-153.

[9]. E.T. Parker, Noextendibility conditions on mutually orthogonal latin squares, Proc. Amer. Math. Soc. 13 ( 1962), PP. 219-221.

# المجموعة العظمى من المربعات اللاتينية المتعامدة المتبادلة وتكوينها

**مكارم عبدالواحد عبدالجبار**

**Email:** mak_alturky@yahoo.com

**الخلاصة:**

لو كانت لدينا التباديل {P1, P2 ,..... Pk} على المجموعة S . يمكن ان نقول مجموعة التباديل هي متعدية على S إذا كان كل زوج مرتب من العناصر a,b الذي ينتمي إلى S . يوجد على الأقل $P_i=P_j$ مجموعة لتباديل لتطبيق واحد بالتحديد $P^i$ من a إلى b يسمى متعدي جدا ومثال على ذلك لو كانت لدينا مجموعة تتكون من ثلاثة عناصر {1,2,3}يمكن تمثيل التباديل على شكل تطبيق بحيث 3←1,2←2,1←3على الشكل(123) والتباديل المتعدية هي (123) و(132) و(213) و(321) والتباديل الثلاثة الأخيرة تمثل مجموعة متعدية جدا. هذا البناء يعطينا المربعات الاتينية المتعامدة المتبادلة. مجموعه من المربعات الاتينية المتعامدة تعتبر هي المجموعة العظمى اذا كان لايوجد مربع لاتيني متعامد لأي عدد من S.