الجماهيرية العربية الليبية الشعبية ألاشتراكية العظمى

كلية العلوم / قسم الرياضيات

جامعة التحدي

المربع اللاتيني وتطابقه مع الإسقاط في المستويات

أطروحة لاستكمال متطلبات درجة الإجازة العليا الماجستير في الرياضيات بكلية العلوم جامعة التحدي

مقدمه من

الطالب:طارق عمر حمد بالطيب

أشراف

الدكتور:شعبان علي طربينه

إن الجماهيرية العربية الليبية الشعبية الاشتراكية العظمى

جامعة التحدي

سرت

التاريخ :
الموافق : 15-1-2007 ف
الرقم الإشاري : ك ع / 22 / 1 / 7

Faculty of Science

Department of Mathematics

Title of Thesis

((Latin Squares Corresponding to Projective Planes))

By

Tarek O. Bel-Tayyeb

Approved by:

Dr. Shaban A. Traina ....
(Supervisor)

Dr. Ibrahim A. Tentush ....
(External examiner)

Dr. Ameer Abdul M. Jaseem ....
(Internal examiner)

Countersigned by:

Dr. Mohamed Ali Salem

(Dean of Faculty of Science)

www.altahadi.edu.ly

@altahadi.edu.ly 674 054 / 60361 - 62151 054/ 60363 - 65704

الجماهيرية العربية الليبية الشعبية الاشتراكية العظمى
جامعة التحدي
سرت

التاريخ : ....
الموافق : 2007.01.10 ف
الرقم الاشاري : ك ع /22/1/2007

كليــــة العلــــوم

قســـم الرياضيات

عنـــوان البحــث

((المربع اللاتيني و تطابقه مع الإسقاط في المستويات))

مقدمـــة مـــن الطـــالب

طارق عمر حمد أبوالطيب

*** * لجنـــة المناقشـــة :**

الدكتور / شعبان علي طرينه ....
(مشـــرف الرســـالــة)

الدكتور / أمير عبدالمجيد خواجه ....
(ممتحـــن داخلـــي)

الدكتور / إبراهيم عبدالله تنتوش ....
(ممتحـــن خارجـــي)

يعتمـــد :-

د. ....

أمين اللجنة الشعبية لكلية العلوم

www.altahadi.edu.ly

@altahadi.edu.ly 674 ✉ 054 / 60361 - 62151 ☏ 054/ 60363 - 65704 ☎

الإهداء

إلى الأمي الذي علم المتعلمين إلي الذي قال "من سلك طريقا يلتمس فيه علما سهل الله له طريقا إلى الجنة "سيدنا **محمد** صلى الله عليه وسلم وعلى أله وصحبه وجميع الأنبياء والمرسلين.

وإلى من كانا سببا في وجودي وباباً من أبواب رحمت ربي إلى **أبي وأمي** و إلى **أخوتي وأخواتي** .

شكر و تقدير

لأستاذنا الفاضل الدكتور شعبان طرينه على ما تفضل به على الإشراف والتوجيه والتعليم ، ولما لمسته من حسن خلقه وتواضعه الجم ، ورحابة صدره ، وجديته الصادقة ، وتوجيهاته القيمة ، وحرصه الشديد على تنمية قدرات الباحث العلمية والفكرية ، وأسلوبه المميز في المتابعة ، حتى ظهر البحث بهذه الصورة ، فله مني الدعاء بأن يبارك الله في علمه وعمله وجهده ... آمين .

ولأساتذة وطلبه قسم الرياضيات بجامعة التحدي وأهل سرت الكرام وجميع الأحباب والأصحاب .

TABLE OF CONTENTS

INTRODUCTION

The great mathematician Leonhard Euler introduced Latin squares in 1783 as a "Nouveau espece de carres magiques", a new kind of magic squares. He also defined what he meant by orthogonal Latin squares, which led to a famous conjecture of his that went unsolved for over *100* years. In *1900*, G. Tarry proved a particular case of the conjecture. it was shown in 1960 by Bose, Shrikhande. and Parker, except for this one case, the conjecture was false.

So, the main aim of this thesis is to present some important information about Latin square and projective plane which have an important role in some applications as experimental designs, geometry, graph theory, and grouped multiplication tables.

Even though, the less availability of professional books for the subject. I had to do a lot of search to find the little available book containing details about the subject .I also had to search through the internet to excess to some journals for papers and to obtain some more in formation up to date concerning the subject .

To emphasize the idea of this thesis briefly, we have divided the thesis to three chapters:

- Chapter *1*: contains some principle, definitions and theorems of Latin squares, Quasigroup and Latin rectangle and how to extend it to a Latin square.
- Chapter *2*: explain the meaning of orthothognality in set of mutually orthogonal Latin squares and their countable numbers. Euler's conjecture is mentioned and Tarry result concerning the falsity of the Euler's conjectureis given.
- Chapter *3*: the meaning of projective planes and some important theorems are discussed and some more connect projective planes with set of mutually orthogonal Latin squares are presented .

Throughout this thesis ,some examples are given to clarify the definitions and theorems that are used .

A new result concerning Orthognality has been reach is given at the end of the third chapter.

Chapter one

1.1 Latin Square:

Definition (1.1.1):[12] [10]

A Latin square of order n is an $n \times n$ array in which n^2 symbols, taken from a set A $(A = \{0, 1, 2, ..., n-1\})$ are arranged so that each symbol occurs only once in each row and exactly once in each column.

Example (1.1.2):

The following are Latin squares of order 2, 3, and 4

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \& \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \& \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

Theorem (1.1.3):[10]

For all $n \geq 1$, there exist a Latin square of order n.

Proof:

Consider the $n \times n$ array A defined by $a_{ij} \equiv (i + j) \pmod{n}$ $i, j = 0, 1, ..., n$. We claim that A is a Latin square of order n.

Case (I):

Trivially: A is taken over an n-set of elements, namely the congruence classes module n.

Case (II):

Assume two entries of the same row, say (i, j_1) and (i, j_2), $j_1 \neq j_2$ are identical. But

$$a_{ij_1} = a_{ij_2}$$
$$\Rightarrow (i + j_1) \equiv (i + j_2)(\text{mod } n)$$
$$\Rightarrow \quad j_1 \equiv j_2 (\text{mod } n)$$
$$\Rightarrow \quad j_1 = j_2, \quad \text{as} \quad 0 \le j_1, \; j_2 \le n-1$$

This contradiction gives that the row elements are unique.

Case III:

Assume two entries of the same column, say (i_1, j) and (i_2, j), $i_1 \neq i_2$ are identical. But

$$a_{i_1 j} = a_{i_2 j}$$
$$\Rightarrow (i_1 + j) \equiv (i_2 + j)(\text{mod } n)$$
$$\Rightarrow \quad i_1 \equiv i_2 (\text{mod } n)$$
$$\Rightarrow \quad i_1 = i_2, \quad \text{as} \quad 0 \le i_1, \; i_2 \le n-1$$

This contradiction gives that the column elements are unique. Having demonstrated these three cases. A is a Latin square of order n.

Definition (1.1.4): [18]

A Latin square of order n (on the set *{1, 2, ..., n}* or on the set *{0, 1, 2, ..., n-1}*) is reduced , normalized or in standard form if in the first row and column the elements occur in increasing order.

Example (1.1.5):

The following Latin square of order five is in standard form.

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 & 0 \\ 2 & 4 & 1 & 0 & 3 \\ 3 & 2 & 0 & 4 & 1 \\ 4 & 0 & 3 & 1 & 2 \end{bmatrix}$$

Remark:[10]

The canonical construction of a Latin square of order n define by $a_{ij} \equiv (i+j) \pmod n$ is in standard form. where i, j = 1,2,3,..........,n-1

Observe that the rows, columns, and elements of a Latin square can be permuted so as to maintain a Latin square.

To this effect we can put any Latin square into standard form.

Example (1.1.6):

We can put the following Latin square of order four into standard form in several ways:

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

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

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

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

Definition (1.1.7): [12]

Two Latin squares are said to be isotopic if one can be obtained from the other by permuting rows, columns and symbols.

The equivalence classes of Latin squares under the isotopy relation are called isotopy classes. Note that there will in general be more than one reduced Latin square in an isotopy class.

Example (1.1.8):

The two Latin squares of order 4 are:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix} \& \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

Note that : the second Latin square can be obtained by permuting rows in the first Latin square .i.e. the two Latin square are isotopic .

Definition (1.1.7): [12]

Two Latin squares are said to be isotopic if one can be obtained from the other by permuting rows, columns and symbols.

The equivalence classes of Latin squares under the isotopy relation are called isotopy classes. Note that there will in general be more than one reduced Latin square in an isotopy class.

Example (1.1.8):

The two Latin squares of order 4 are:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix} \& \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

Note that : can be obtained the second Latin square by permuting rows in the first Latin square ,i.e. the two Latin square are isotopic .

1.2 The number of Latin square of various size: [18], [28], [9] ,[17], [16], [24]

For each $n \geq 1$ the total number of Latin squares of order n denoted by $LS(n)$ (Laywine and Muller, 1998) is given by:

$$LS(n) = n!(n-1)!\,T(n)$$

Where $T(n)$ denotes the number of reduced Latin squares of order n. The number of Latin squares of order n ($LS(n)$) increases very quickly with n and is indeed great, even for rather small n. It should be noted that the number of reduced Latin squares is exactly known for $n \leq 10$ (McKay and Rogoyski, 1995) [see table 1] for $n = 11, 12, \ldots, 15$, $T(n)$ is estimated in Table 2.

For $n > 15$ the bounds of $LS(n)$ can be calculated (Jacobson and Matthews, 1996) using the formula:

$$\prod_{k=1}^{n}(K!)^{\frac{n}{k}} \geq LS(n) \geq \frac{(n!)^{2n}}{n^{n^2}}$$

In tables 1,2,3 and 4 some upper and lower bounds of $T(n)$ and $LS(n)$ for several values of n, most frequently used in practice are given.

Table 1: Number of reduced Latin square $T(n)$.

n	$T(n)$
2	1
3	1
4	4
5	56
6	9048
7	16942080
8	535281401585
9	377597570964258816
10	7580721483160132811489280

Table 2: Estimates of $T(n)$ for $n = 11, 12, 13, 14, 15$.

n	$T(n)$
11	$5.36 \cdot 10^{33}$
12	$1.62 \cdot 10^{44}$
13	$2.51 \cdot 10^{56}$
14	$2.33 \cdot 10^{70}$
15	$1.50 \cdot 10^{86}$

Table 3: Number of Latin square $LS(n)$.

n	$LS(n)$
1	1
2	2
3	12
4	576
5	161280
6	812851200
7	61479419904000
8	108776032459082956800
9	5524751496156892842531225600

Table 4: Estimates of LS(n) for $n = 2^k$, $k = 4, 5, 6, 7, 8$.

$0.689.10^{138} \geq LS(16) \geq 0.101.10^{119}$

$0.985.10^{784} \geq LS(32) \geq 0.414.10^{726}$

$0.176.10^{4169} \geq LS(64) \geq 0.133.10^{4008}$

$0.164.10^{21091} \geq LS(128) \geq 0.337.10^{20666}$

$0.753.10^{102805} \geq LS(256) \geq 0.304.10^{101724}$

1.3 Quasigroup:

Definition (1.3.1): [12], [27], [23]

A set S is called a quasigroup if there is a binary operation (.) defined on S and if, when any two element a, b of S are given, the equations $a.x = b$ and $y.a = b$ each have exactly one solution.

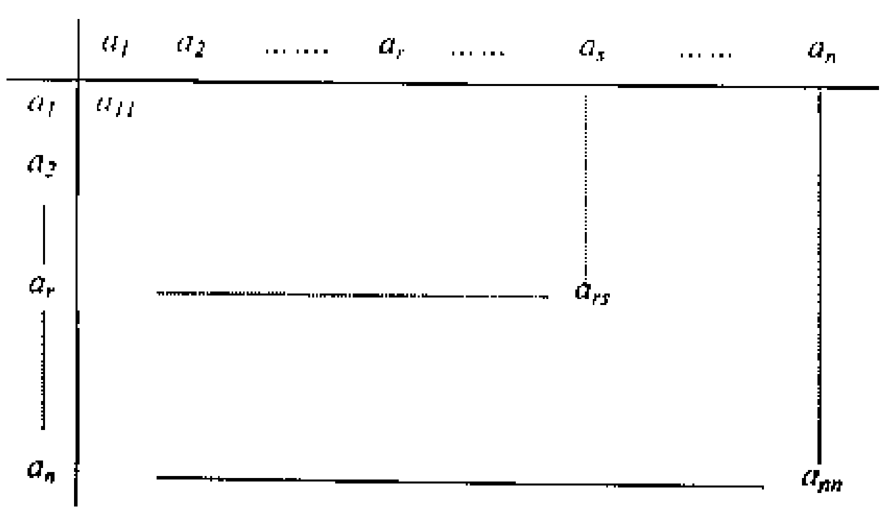
Theorem (1.3.2): [1]

The multiplication table of a quasigroup is a Latin square.

Proof:

Let $a_1, a_2, \ldots, a_n$ be the element of the quasigroup and let its multiplication table be as shown in the figure below, where the entry a_{rs} which occurs in the r^{th} row and the s^{th} column is the product $a_r a_s$ of the elements a_r and a_s.

If the same entry occurred twice in the r^{th} row, say in the s^{th} and t^{th} columns so that $a_{rs} = a_{rt} = b$ say, we would have two solutions to the equation $a_r x = b$ in contradiction to the quasigroup axioms. Similarly, if the same entry occurred twice in the s^{th} column, we would have two solutions to the equation $ya_j = c$ for some c. We conclude that each element of the quasigroup occurs exactly once in each row and once in each column, and so the unbordered multiplication table is a Latin square.



Example (1.3.3): [8]

Consider the set of integers modulo 3 with respect to the operation defined by $a * b = 2a + b + 1$.

The multiplication of this quasigroup is shown in the figure below and we see at once that it is a Latin square.

*	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

More generally, the operation $a * b = ha + kb + l$, where addition is modulo n and h, k and l are fixed integers with h and k prime to n ,defines a quasigroup on the set $M = \{0, 1, \ldots, n-1\}$.

Definition (1.3.4): [12]

A set S forms a groupoid (S, .) with respect to a binary operation (.) if, with each ordered pair of elements a, b of S is associated a uniquely determined element $a . b$ of S.

A groupoid whose binary operation is associative is called semigroup.

Remark:

The previous theorem shows that multiplication table of groupoid is a Latin square if and only if the groupoid is a quasi group. Thus, in particular, the multiplication table of a semigroup is not a Latin square unless the semi-group is a group.

Corollary (1.3.5): [12]

The cayley table of a finite group G it is a Latin square, in other words a square matrix $[a_{ij}]$ each row and each column of which is a permutation of the elements of G.

1.4 Latin Sub-squares and Sub-Quasigroups:

Definition: (1.4.1): [12]

Let the square matrix A shown in *Fig. (1)* be a Latin square. Then, if the square sub-matrix B shown in *Fig. (2)* (where $1 \le i, j, \ldots\ldots, l, p, q, \ldots, s \le n$) is again a Latin square, B is called a Latin sub-square of A..

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n3} & \cdots & a_{nn} \end{bmatrix} \qquad B = \begin{bmatrix} a_{ip} & a_{iq} & \cdots & a_{is} \\ a_{jp} & a_{jq} & \cdots & a_{js} \\ \vdots & \vdots & & \vdots \\ a_{lp} & a_{lq} & \cdots & a_{ls} \end{bmatrix}$$

Figure 1 *Figure 2*

Thus, the Latin square corresponding to the cayley table of sub-quasigroup Q' of any quasigroup Q is Latin sub-square of the Latin square defined by the cayley table of Q.

Example (1.4.2): [12] ,[18]

In *Fig. (3)*, the cayley table of a quasigroup of order 10 is shown which has a subquasigroup of order 4 (consisting of the elements 1, 2, 3, 4) and also one of order 5 (with elements 3, 4, 5, 6, 7) the intersection of which is a subquasigroup of order 2 (with element 3, 4).

	0	8	9	1	2	3	4	5	6	7
5	1	9	2	8	0	6	7	4	5	3
6	8	2	1	0	9	7	5	3	4	6
7	2	1	0	9	8	5	6	7	3	4
3	0	8	9	1	2	3	4	6	7	5
4	9	0	8	2	1	4	3	5	6	7
1	5	6	7	3	4	1	2	0	8	9
2	6	7	5	4	3	2	1	8	9	0
0	7	4	3	5	6	0	9	1	2	8
8	3	5	4	6	7	8	0	9	1	2
9	4	3	6	7	5	9	8	2	0	1

Figure 3

Theorems (1.4.3): [12].[27],[8], [23]

1- For a given integer n and k, n arbitrary and $k \leq n/2$, there exists a quasi group of order n which contains at least one sub-quasi group of order k.

2- No Latin square which is the union of two disjoint Latin sub-squares exists.

3- For arbitrary $n (n \geq 4)$, there exists a Latin square of order n having a Latin sub-square of order 2.

1.5 Latin Rectangle :

Definition (1.5.1): [12] ,[27]

Let m and n be integers with $m < n$. An m - *by* $-n$ is a Latin rectangle if each of the integers *1, 2, ..., n* occurs exactly once in each row and at most once in each column.

Example (1.5.2):

An example of *3 - by -5* Latin rectangle is:

$$L = \begin{bmatrix} 3 & 1 & 2 & 5 & 4 \\ 1 & 3 & 5 & 4 & 2 \\ 4 & 5 & 3 & 2 & 1 \end{bmatrix}$$

We say that *an m - by - n* Latin rectangle L can be extended to a Latin square of order n provided it is possible to attach n-m rows to L and obtain a Latin square of order n.

Theorem (1.5.3): [7]

An *m - by - n* Latin rectangle can always be extended to a Latin square of order n.

Example (1.5.4): [31]

To add an extra row to the Latin rectangle $\begin{bmatrix} 1 & 2 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix}$

To create a *3 x 5* Latin rectangle with entries in *{1,2,3,4,5}* is equivalent to finding distinct representatives of the sets shown below:

$$\begin{bmatrix} 1 & 2 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ \{2,3,4\} & \{3,4,5\} & \{1,3,5\} & \{1,2,4\} & \{1,2,5\} \end{bmatrix}$$

One such collection is shown in bold point:

Those representatives could be used as the entries of the next row. We could then continue in a similar way to extend the 3×5 Latin rectangle to a 4×5 Latin rectangle and finally to a 5×5 Latin square.

Example (1.5.5): [31]

The following can not be extended to 6×6 Latin square

$$\begin{bmatrix} 6 & 1 & 2 & 3 \\ 5 & 6 & 3 & 1 \\ 1 & 3 & 6 & 2 \\ 3 & 2 & 4 & 6 \end{bmatrix}$$

One way to see this is note that in any extension to 6×6 Latin square as shown we would need three 5_s in the box, but they will not fit because there are only two columns for them.

Remark:

Assume that we are given a $p \times q$ Latin rectangle L with entries in $\{1, \ldots, n\}$. with $L(i) \geq p + q - n$ for $1 \leq i \leq n$, and that we wish to extend L to an $n \times n$ Latin square. The moral of the above example is that when we add a column to L to give a $p \times (q + 1)$ Latin rectangle L' we must do it in such a way that the process can then be repeated.

So we require that $L'(i)$, the number of occurrences of i in L', must satisfy:

$$L'(i) \geq p+(q+1)-n$$

Therefore, if for some i we have $L(i) = p + q - n$, then we must ensure that i is included in the new column. So let

$$p = \{i : 1 \leq i \leq n \text{ and } L(i) = p+q-n\}$$

Then for the process to be continue the extra column must include the set p, for in that even each i will occur in the new rectangle at least $p + (q + 1) - n$ times.

Example (1.5.6): [31]

The example below, can be extended to 5 × 5 Latin square.

$$L = \begin{bmatrix} 1 & 3 & 4 \\ 4 & 1 & 5 \end{bmatrix}$$

Here the given L is $p \times q = 2 \times 3$ and so $p = 2$, $q = 3$ and $n = 5$. Thus $p + q - n$ is 0 and it is clear that $L(i) \geq p + q - n$ for each i, $(1 \leq i \leq n)$.

We shall start by extending L to a 2 × 4 Latin rectangle by the addition of an extra column,

$$\begin{bmatrix} 1 & 3 & 4 & - \\ 4 & 1 & 5 & - \end{bmatrix} \begin{matrix} \leftarrow \in \{2,5\} \\ \leftarrow \in \{2,3\} \end{matrix}$$

This can be done in any one of the three ways; in each way we can then try to extend to a 2 × 5 Latin rectangle.

$$\begin{bmatrix}1&3&4&2\\4&1&5&3\end{bmatrix}\to\begin{bmatrix}1&3&4&2&5\\4&1&5&3&2\end{bmatrix}$$

$$\begin{bmatrix}1&3&4&5\\4&1&5&2\end{bmatrix}\to\begin{bmatrix}1&3&4&5&2\\4&1&5&2&3\end{bmatrix}$$

In these two cases we now have a 2 × 5 Latin rectangle and, by the previous theorem, these can be extended to 5 × 5 Latin square.

$$\begin{bmatrix}1&3&4&5\\4&1&5&3\end{bmatrix}\to \text{impossible}$$

Hence, the 2 × 4 Latin rectangle could not be extended because $p = 2$, $q = 4$ and $p + q - n = 1$. But $L(2) = 0$ and so $L(2) < p + q - n$.

Example (1.5.7): [31]

By using the last techniques to extend

$$\begin{bmatrix}5&6&1\\6&5&2\\1&2&3\end{bmatrix}$$

To a 6 × 6 Latin square, we shall follow the process through in full because it shows the significance of the set p.

$$\begin{bmatrix}5&6&1&-\\6&5&2&-\\1&2&3&-\end{bmatrix}\begin{matrix}\leftarrow\in\{2,3,4\}\\\leftarrow\in\{1,3,4\}\\\leftarrow\in\{4,5,6\}\end{matrix}$$

$$p + q - n = 3 + 3 - 6 = 0$$

The new column must include the set

$$p = \{i : L(i) = 0\} = \{4\}$$

Once such transversal is shown in bold print and the process can continue

$$\begin{bmatrix} 5 & 6 & 1 & 4 & - \\ 6 & 5 & 2 & 1 & - \\ 1 & 2 & 3 & 5 & - \end{bmatrix} \begin{matrix} \leftarrow \in \{2,3\} \\ \leftarrow \in \{3,4\} \\ \leftarrow \in \{4,6\} \end{matrix}$$

$$p + q - n = 3 + 4 - 6 = 1$$

The new column must include the set

$$p = \{i : L(i) = 1\} = \{3,4\}$$

Once such transversal is shown in bold print and the process can continue

$$\begin{bmatrix} 5 & 6 & 1 & 4 & 3 & - \\ 6 & 5 & 2 & 1 & 4 & - \\ 1 & 2 & 3 & 5 & 6 & - \end{bmatrix} \begin{matrix} \leftarrow \in \{2\} \\ \leftarrow \in \{3\} \\ \leftarrow \in \{4\} \end{matrix}$$

The new column must include the set

$$p = \{i : L(i) = 2\} = \{2,3,4\}$$

Once such transversal (!) is shown in bold print and it gives the 3 × 6 Latin rectangle

$$\begin{bmatrix} 5 & 6 & 1 & 4 & 3 & 2 \\ 6 & 5 & 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{bmatrix}$$

By the previous theorem this can now be extended to a 6×6 Latin square, one such being

$$\begin{bmatrix} 5 & 6 & 1 & 4 & 3 & 2 \\ 6 & 5 & 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 5 & 6 & 4 \\ 2 & 3 & 4 & 6 & 1 & 5 \\ 4 & 1 & 5 & 3 & 2 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{bmatrix}$$

Chapter two

2.1- Orthogonality:

Definition (2.1.1): [18]

Given two Latin square A and B of order n, the join (A, B) is the n × n array defined by $(A, B)_{ij} = (A_{ij}, B_{ij}),\ 0 \le i, j \le n - 1.$

Example (2.1.2): [18]

The Joint of

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \\ 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \end{bmatrix}$$

are

$$(A,B) = \begin{bmatrix} (0.1) & (1.3) & (2.2) & (3.0) \\ (1.2) & (2.0) & (3.1) & (0.3) \\ (2.0) & (3.2) & (0.3) & (1.1) \\ (3.3) & (0.1) & (1.0) & (2.2) \end{bmatrix}$$

and

$$(B,A) = \begin{bmatrix} (1.0) & (3.1) & (2.2) & (0.3) \\ (2.1) & (0.2) & (1.3) & (3.0) \\ (0.2) & (2.3) & (3.0) & (1.1) \\ (3.3) & (1.0) & (0.1) & (2.2) \end{bmatrix}$$

Definition (2.1.3): [18]

Two Latin squares $A = (a_{ij})$ and $B = (b_{ij})$ of order n are orthogonal if the n^2 ordered pairs $(a_{ij}, b_{ij}),\ 0 \le i, j \le n - 1$ are distinct.

Example (2.1.4):

The Latin squares of example (2.1.2) are not orthogonal as the *(0,0)* entry and *(3,1)* entry of *(A, B)* are both *(0, 1)*

Example (2.1.5):

The joint of

$$A=\begin{bmatrix}0&1&3&2\\1&0&2&3\\3&2&0&1\\2&3&1&0\end{bmatrix},\qquad B=\begin{bmatrix}1&3&2&0\\2&0&1&3\\0&2&3&1\\3&1&0&2\end{bmatrix}.$$

is

$$(A,B)=\begin{bmatrix}(0,1)&(1,3)&(3,2)&(2,0)\\(1,2)&(0,0)&(2,1)&(3,3)\\(3,0)&(2,2)&(0,3)&(1,1)\\(2,3)&(3,1)&(1,0)&(0,2)\end{bmatrix}$$

So. A and B are orthogonal.

2.2- Orthogonal Mates and Transversal:

We often refer to one of a pair of orthogonal Latin squares as being an orthogonal mate to the other.

Euler was originally interested in such pairs and in his writings he would always use a Latin letters for the first square and Greek letters for the second. Thus, when he referred to the first of the squares he referred to the Latin square.

When referring to both of the orthogonal squares he used the term Graco-Latin squares, which is now call orthogonal Latin squares

Definition (2.2.1): [16]

A transversal Latin square of order n is a set of n positions, exactly one from each row and each column, such that those positions contain each of the entries 0, 1, …, n - 1 exactly once.

Example (2.2.2):

$$\text{Consider } A = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}$$

The *(0,0), (1,3), (2,1)*, and *(3,2)* position constitute a transversal of A.

Theorem (2.2.3): [12]

If a Latin square L of order n has n-1 disjoint transversals, then it has n disjoint transversal.

Proof:

Each transversal of L consumes one cell in each row, one cell in each column, and one of each of the n symbols, hence, $n - 1$ disjoint transversal consume $n - 1$ cells in each row, $n - 1$ cells in each column, and $n - 1$ of each of the n symbols. Thus, what remains in L is one cell in each row, one cell in each column and one of the n symbols, i.e. n^{th} disjoint transversal.

Theorem (2.2.4): [12]

Let A be the Latin square of order $2k$ defined by $a_{ij} \equiv (i+j) \pmod{2k}$, $(1 \le i,j \le 2k)$, then A contains no transversal.

Proof:

Suppose that cells $(1, j_1), (2, j_2), \ldots, (2k, J_{2k})$ contain $\{a_{1j_1}, a_{2j_2}, \ldots a_{2kj_{2k}}\} = (1, 2, \ldots, 2k)$ and summing both sides yields $a_{1j_1} + a_{2j_2} + \ldots + a_{2kj_{2k}} = k(2k + 1)$. Now $a_{ij_i} \equiv i + j_i \pmod{2k}$, so $j_1, j_2, \ldots, j_{2k}$ is a reordering of $1, 2, \ldots, 2k$ so $(1 + j_1) + (2 + j_2) + \ldots + (2k + j_{2k}) = 2(1 + \ldots + 2k) = 2k(2k + 1)$. Substituting we get:

$$0 \equiv k \pmod{2k} \quad \text{a contradiction.}$$

In the context of transversals we present an alternative definition of orthogonality.

Definition (2.2.5): [12]

Two Latin squares A and B of the same order are orthogonal if for any symbol x in A, the position in which x resides in A constitute a transversal of B.

Theorem (2.2.6): [26]

A Latin square of order n possesses an orthogonal mate if and only if it has n disjoint transversal.

2.3 Orthogonal Latin Square of Odd and Even Order:

(a) Odd Order: [10]

If the Latin square in question is the multiplication table of a group of odd order n, then it can be shown that the existence of a single transversal implies the existence of n disjoint transversals. So we conclude that the square has an orthogonal mate.

Theorem [L-Euler, (1782)] (2.3.1): [10]

The multiplication table of any group of odd order forms a Latin square which possesses an orthogonal mate.

Corollary (2.3.2): [10] [23]

1- There exist pairs of orthogonal Latin squares of every odd order.

2- Any Latin square of odd order has a transversal.

Theorem [Man. H. B. (1942) (2.3.3): [12]

No pair of orthogonal Latin square based on a group can exist when n is an odd multiple of two.

(b) Even Order: [10]

The existence question for pairs of orthogonal Latin squares of even order is much more difficult to settle and has a long and famous history. To start with, there are only two Latin squares of order 2 and they are not orthogonal (since, it has no transversal). We have given an example of a pair of orthogonal squares of order 4.

The next case, that of order 6, is the problem that originally interested Euler in the subject, called the **Problem of the 36 Officers**. Euler stated it as follows in 1779: "Arrange 36 officers, 6 from each of regiments, of 6 different ranks, into a 6 × 6 square, so that each row and each file contains one officer of each rank and one officer of each regiment".

2.4 Euler's Conjecture and Tarry's Results:

Euler's Conjecture (2.4.1): [9] ,[10], [16] ,[1]

As brilliant a mathematician as Euler was, he was unable to find such a pair of squares and unable to prove that they did not exist. Based on his experience with the problem and some other pieces of evidence (such as the corollary, which he was aware of), Euler made a conjecture which included and went beyond this problem.

Euler's Conjecture there does not exist an orthogonal mate for any Latin square of order n if $n \equiv 2 \pmod 4$.

Tarry's Results(2.4.2): [9] ,10], [16] ,[1]

120 years after Euler first stated the problem, Tarry in 1900 settled the problem of the 36 officers in the negative. His method was straight-forward, he listed out all of the 812,851,200 Latin squares of order 6 and examined each pair for orthogonality and found none [actually by working with reduced squares he simplified the problem to checking only 9408 pairs, but of course this was all done by hand]. It was beginning to look like the old master who had pulled off a coupe, but in 1960 Bose, Shrikhande and Parker shocked the mathematical community by proving that for $n > 6$ Euler's conjecture is false. Their original method is long, complicated and involved, looking at number of special cases, but has since been simplified.

Theorem [Bose, Parker (1960)] (2.4.3): [6], [29]

There exist orthogonal mate for every order n except for *n = 2 or n = 6* when they cannot exist.

In *1984* D. R. Stinson gave a clever 3 page proof that there do not exist orthogonal mate of order 6.

Showed by a counter example Bose, Parker *(1960)*, there exist an orthogonal Latin square of order 10.

$$\begin{bmatrix}
(4,6) & (5,7) & (6,8) & (7,0) & (8,1) & (0,2) & (1,3) & (2,4) & (3,5) & (9,9) \\
(7,1) & (9,4) & (3,7) & (6,5) & (1,2) & (4,0) & (2,9) & (0,6) & (8,8) & (5,3) \\
(9,3) & (2,6) & (5,4) & (0,1) & (3,8) & (1,9) & (8,5) & (7,7) & (6,0) & (4,2) \\
(1,5) & (4,3) & (8,0) & (2,7) & (0,9) & (7,4) & (6,6) & (5,8) & (9,2) & (3,1) \\
(3,2) & (7,8) & (1,6) & (8,9) & (6,3) & (5,5) & (4,7) & (9,1) & (0,4) & (2,0) \\
(6,7) & (0,5) & (7,9) & (5,2) & (4,4) & (3,6) & (9,0) & (8,3) & (2,1) & (1,8) \\
(8,4) & (6,9) & (4,1) & (3,3) & (2,5) & (9,8) & (7,2) & (1,0) & (5,6) & (0,7) \\
(5,9) & (3,0) & (2,2) & (1,4) & (9,7) & (6,1) & (0,8) & (4,5) & (7,3) & (8,6) \\
(2,8) & (1,1) & (0,3) & (9,6) & (5,0) & (8,7) & (3,4) & (6.2) & (4,9) & (7,5) \\
(0,0) & (8.2) & (9.5) & (4,8) & (7.6) & (2,3) & (5,1) & (3,9) & (1,7) & (6,4)
\end{bmatrix}.$$

Theorem [Mann H. B. (1950)] (2.4.4): [12]

If a Latin square L of order $4k + 2$ represents the cayley table of a quasigroup which contains a sub-quasigroup of order $2k + 1$ then L has no orthogonal mate.

Remark

The converse of the theorem is not necessary true .

2.5 Set of Mutually Orthogonal Latin Squares:

Definition (2.5.1): [9] ,[10], [16] , [26], [1]

A set of Latin squares of the same order, each of which is an orthogonal mate of each of the other is called set of mutually orthogonal Latin square. This mouthful is often shortened to its acronym "**MOLS**".

Example (2.5.2):

The following Latin square of order 4 are mutually orthogonal Latin square.

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

2.6 Equivalents MOLS:

Definition (2.6.1): [26]

Two sets of MOLS with the same number of Latin squares are said to be equivalent sets of MOLS if one can be obtained from the other by any combination of simultaneously permuting the rows of all the Latin squares, simultaneously permuting the columns of all the Latin squares and renaming the elements of any Latin square.

Theorem (2.6.2): [10]

A set of m MOLS of order n is equivalent to an $n^2 \times (m + 2)$ orthogonal array.

Example (2.6.3): [10]

A pair of orthogonal Latin squares of order 4 is equivalent to an $n^2 x4 = 16 \times 4$ orthogonal array.

$$\begin{bmatrix} (1.1) & (2.2) & (3.3) & (4.4) \\ (2.3) & (1.4) & (4.1) & (3.2) \\ (3.4) & (4.3) & (1.2) & (2.1) \\ (4.2) & (3.1) & (2.4) & (1.3) \end{bmatrix} \; : \; \begin{bmatrix} 1111 \\ 1222 \\ 1333 \\ 1444 \\ 2123 \\ 2214 \\ 2341 \\ 2432 \\ 3134 \\ 3243 \\ 3312 \\ 3421 \\ 4142 \\ 4231 \\ 4324 \\ 4413 \end{bmatrix}$$

Each row of the array consists of:

(i) row

(ii) column

(iii) symbol in first square

(iv) symbol in second square

Lemma (2.6.4): [26]

Any set of MOLS is equivalent to a set where each Latin square has the first row in natural order and one of the Latin squares (usually the first) is reduced (or standard form) (i.e. 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 each Latin square, so that the first rows are all in natural order. Now take any Latin square and simultaneously permute the rows of all the Latin squares so that the first column of this Latin square is in natural order (this will not affect the first row since it is natural order and so starts with the smallest element).

The result is an equivalent set with the required properties.

2.7 Number of MOLS and Complete set of Mols:

Theorem (2.7.1): [12],[10], [26]

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 has the same number of Latin square in it.

Consider the entries in first column and second row of all of the Latin squares in standard form.

No two Latin squares can have the same entry in this cell. Suppose two Latin squares had an r, say, in this cell, then in the superimposed Latin square the ordered pair (r, r) would appear in this cell and also in the r^{th} cell of the first row because both Latin squares have the same first row, and so the two Latin 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 $n-1$ Latin squares.

Definition (2.7.2): [12],[25]

A set of MOLS of order n containing *n-1* Latin squares is called a **complete set**. We now have an existence question, for which order do complete sets of MOLS exist?

We know by examples that complete sets exist of order 2 (only one square), 3 and 4 and also that no complete set exists for orders 6 and 10. Complete sets of MOLS for any order, which is a prime or power of, prime can be constructed.

However, it's an open problem of long standing.

Theorem (2.7.3): [12]

If n is prime or a power of a prime then there exist a set of *n-1* mutually orthogonal Latin square.

In general we denote the maximum number of MOLS of order n by *N(n)*. Its customary to define $N(0) = N(1) = \infty$.

Corollary (2.7.4): [10]

If $n \equiv 1 \pmod 2$ then $N(n) \geq 2$, for all n>1 except n = 6.

Proof:

Consider two Latin square A and B of order $n \equiv 1 \pmod 2$ defined by $a_{ij} \equiv (i+j)$ (mod n) and $b_{ij} \equiv (i-j)$ (mod n) we claim that these are orthogonal Latin squares. We must first verify that A and B are Latin square. We have shown A to be a Latin square in proving that for any n, a Latin squares of order n exists. the argument that B is Latin square is analogous.

We must also confirm that A and B are orthogonal. Assume that two distinct position of the join *(A, B)* have identical entries; that is, there exist i_1, i_2, j_1 and j_2 such that

$$(i_1, j_1) \neq (i_2, j_2) \quad \text{(as position).}$$
$$(A,B)_{i_1 j_1} = (A,B)_{i_2 j_2} \quad \text{(as entries)}$$

Now:

$$(A,B)_{i_1 j_1} = (A,B)_{i_2 j_2}$$
$$\Rightarrow (A_{i_1 j_1}, B_{i_1 j_1}) = (A_{i_2 j_2}, B_{i_2 j_2})$$
$$\Rightarrow (i_1 + j_1, i_1 - j_1) = (i_2 + j_2, i_2 - j_2) \quad \text{[all considered Modulo n]}$$
$$\Rightarrow (i_1 + j_1) \equiv (i_2 + j_2) \pmod{n}$$
$$\Rightarrow (i_1 - j_1) \equiv (i_2 - j_2) \pmod{n}$$
$$\Rightarrow 2i_1 \equiv 2i_2 \pmod{n}, \quad 2j_1 \equiv 2j_2 \pmod{n} \text{[by adding and subtracting]}$$
$$\Rightarrow i_1 \equiv i_2 \pmod{n}, \quad j_1 \equiv j_2 \pmod{n}$$
$$\Rightarrow i_1 = i_2, \quad j_1 = j_2 \ [\text{as } 0 \leq i_1, i_2, j_1, j_2 \leq n-1]$$
$$\Rightarrow (i_1, j_1) = (i_2, j_2)$$

This contradiction gives that entries of the join are unique.

(Note: it suffices to show either $i_1 = i_2$ or j1 = j2, since A is a Latin square, $i_1 = i_2$ and $A_{i_1 j_1} = A_{i_2 j_2}$ would imply that j1 = j2 and similarly, j1 = j2 and $A_{i_1 j_1} = A_{i_2 j_2}$ would imply that ($i_1 = i_2$). Having demonstrated these properties, A and B are a pair of orthogonal Latin squares of order n. Therefore If *n ≡ 1 (mod n)* then *N(n) ≥ 2.*

Corollary (2.7.5): [18]

$$N(n) \geq 2 \text{ for all } n \geq 3, \text{ except } n = 6$$

The following table gives the best known lower bounds for N(n) for $0 \leq n \leq 499$.

Add the row and column indices to obtain the order.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	∞	∞	1	2	3	4	1	6	7	8	2	10	5	12	3	4	15	16	3	18
20	4	5	3	22	5	24	4	26	5	28	4	30	31	5	4	5	5	36	4	4
40	7	40	5	42	5	6	4	46	6	48	6	5	5	52	5	5	7	7	5	58
60	4	60	4	6	63	7	5	66	5	6	6	70	7	72	5	5	6	6	6	78
80	9	80	8	82	6	6	6	6	7	88	6	7	6	6	6	6	7	96	6	8
100	8	100	6	102	7	7	6	106	6	108	6	6	13	112	6	7	6	8	6	6
120	7	120	6	6	6	124	6	126	127	7	6	130	6	7	6	7	7	136	6	138
140	6	7	6	10	10	7	6	7	6	148	6	150	7	8	8	7	6	156	7	6
160	9	7	6	162	6	7	6	166	7	168	6	8	6	172	6	6	14	9	6	178
180	6	180	6	6	7	8	6	10	6	8	6	190	7	192	6	7	6	196	6	198
200	7	8	6	7	6	8	6	8	14	11	10	210	6	7	6	7	7	8	6	10
220	6	12	6	222	13	8	6	226	6	228	6	7	7	232	6	7	6	7	6	238
240	7	240	6	242	6	7	6	12	7	7	6	250	6	12	9	7	255	256	6	12
260	6	8	8	262	7	8	6	10	6	268	6	270	15	16	6	13	10	276	6	9
280	7	280	6	282	6	12	6	7	15	288	6	6	6	292	6	6	7	10	10	12
300	6	7	6	6	15	15	6	306	6	7	6	310	7	312	6	10	7	316	6	10
320	15	15	6	16	6	12	6	7	7	9	6	330	6	8	6	6	8	336	6	7
340	6	10	10	342	7	7	6	346	6	348	8	12	18	352	6	9	6	9	6	358
360	8	360	6	7	6	10	6	366	15	15	6	15	6	372	6	15	7	13	6	378
380	6	12	6	382	15	15	6	15	6	388	6	16	7	8	6	7	6	396	6	7
400	15	400	7	15	11	7	6	15	8	408	6	13	8	12	10	9	18	15	6	418
420	6	420	6	15	7	16	6	7	6	10	6	430	15	432	6	15	6	18	6	438
440	7	15	6	442	6	13	6	11	15	448	6	15	6	7	6	15	7	456	6	16
460	6	460	6	462	15	15	6	466	6	7	6	15	7	15	10	18	6	15	6	478
480	15	15	6	16	6	7	6	486	7	15	6	490	6	16	6	7	15	15	6	498

Chapter three

3.1 Projective Plane:

Definition (3.1.1): [9]

Consider incidence structures (whose elements are called points and lines) having the following properties:

(P1) Any two points are incident with a unique line.

(P2) Any two lines are incident with a unique point.

This class of structures contains some degenerate ones (containing a line incident with no, one or all points, or dually) which we do not want to consider. Slightly less degenerate is the following type: one line l is incident with all the points except one; each remaining line is incident with the point not on l and one other. (This includes a triangle, where any line can play the role of l). An axiom which excludes all of these is

(P3) There exist four points, no three incident with a common line.

A structure satisfying *(P1)*, *(P2)* and *(P3)* is called a projective plane

Remark:

1- If the elements are finite then the projective plane is called a finite projective plane.

2- Any projective plane must contain at least 7 points.

We can define the finite projective plane as the following definition.

Definition (3.1.2): [22]

A finite projective plane of order n, with $n > 1$,is a collection of $n^2 + n + 1$ lines and $n^2 + n + 1$ points such that:

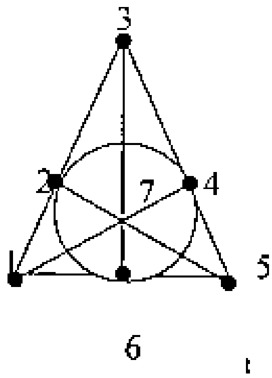
1- every line contains $n + 1$ points,

2- every point is on $n + 1$ lines,

3- any two distinct lines intersect at exactly one point, and

4- any two distinct points lie on exactly one line.

Example (3.1.3): [9]



The smallest non-trivial example is of order 2, there are seven points P = {1.2.3.4.5.6.7}, and there are seven lines labeled L_1 to L_7 such that L consist of the following sets:

$L_1 = \{1.2.3\}$, $L_2 = \{3.4.5\}$, $L_3 = \{1.5.6\}$, $L_4 = \{1.4.7\}$
$L_5 = \{2.5.7\}$, $L_6 = \{3.6.7\}$, $L_7 = \{2.4.6\}$

And that they have the following properties:

1- every line contains three points,
2- every point is on three lines,
3- any two distinct lines intersect at exactly one point, and
4- any two distinct point lie on exactly one line.

Definition (3.1.4): [15]

A finite projective plane having $n + 1$ points on every line is said to be of order n.

Theorem (3.1.5): [12] ,[25]

There exists a finite projective plane of order n if and only if there exists a complete set of mutually orthogonal Latin squares of order n.

Proof:

The construction of the projective plane of order n from a complete set of MOLS of order n.

Let π be a finite projective plane of order n, select any line l of π and arbitrarily label with the digits $1, \ldots, n$ each line which passes through a point of l, for each point of l. Now select two points of l. The lines which pass through these points will be used to index rows and columns of the Latin squares, so label one of the points R and the other C, the n^2 points of intersection of the lines through R and C are associated with pairs of numbers, the number of the line through R and the number of the line through C. Now, for each point of l other than R or C, we will form a Latin square in the following way. If P is the point on l, we have already labeled all the lines through P other than l, the n^2 points of intersection of the R and C lines must all lie on the n label through P. In the cell of the square corresponding to one of the intersection points we place the label of the line through P which passes through this point. It is easy to see that the square produced this way is a Latin square of order n. This procedure is repeated for each of the points of l, giving $n - 1$ Latin squares.

To see that they are mutually orthogonal, consider two such squares and suppose that when superimposed there are two cells containing (a, b). Since the two cells of the first square received the label a, the two points which correspond to the cells must have been on the same line (labeled a) going through a point of l, since these same cells have the label b in the second square, the two points must also be on the line labeled b passing through a different pint of l. This is impossible (by definition projective plane (a)), so we note that these squares must be mutually orthogonal.

- *An Example explain the proof of the theorem (3.1.5)*

Consider the set of 2 MOLS of order 3.

($\Leftarrow$) Start with two orthogonal 3×3 Latin squares:

$$L_1 = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix} \qquad L_2 = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix}$$

Then write them as one combined matrix as we did earlier:

$$M = \begin{bmatrix} 1 & 1 & 3 & 2 \\ 1 & 2 & 1 & 1 \\ 1 & 3 & 2 & 3 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 3 & 3 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 1 & 3 \\ 3 & 2 & 2 & 2 \\ 3 & 3 & 3 & 1 \end{bmatrix} \leftarrow \text{e.g. the } (1.3)^{rd} \text{ entry of } L_1 \text{ is 2 and of } L_2 \text{ is 3}$$

Now introduce a set of 13 points

$$\{c_1, c_2, c_3, c_4, r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_9\}$$

(which can be thought of as a referring to the column 1-4 and the rows 1-9). Consider lines formed by the following subsets of four of those points:

$$\{c_1, c_2, c_3, c_4\}$$

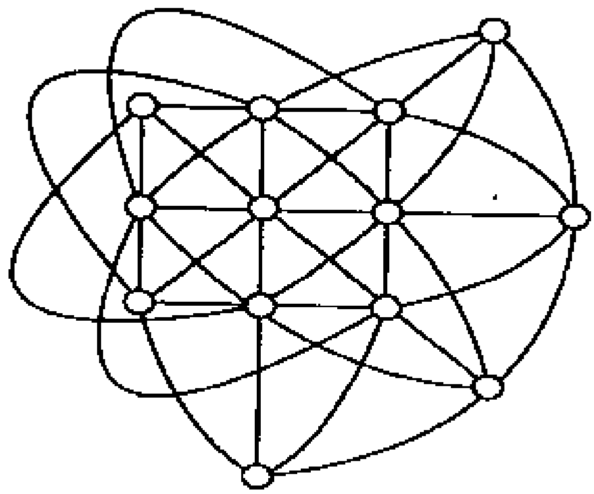
and any of the form:

$$\{c_j, r_s, r_t, r_u\}$$

where the three entries in M in the j^{th} column and rows s, t and u are the same.

For example, one of these sets will be $\{c_2, r_3, r_6, r_9\}$ because the entries in rows 3, 6 and 9 of column 2 are all the same (namely 3). Over all this gives the following 13 (lines):

$$\{c_1, c_2, c_3, c_4\}\ \{c_1, r_1, r_2, r_3\}\ \{c_1, r_4, r_5, r_6\}\ \{c_1, r_7, r_8, r_9\}$$
$$\{c_2, r_1, r_4, r_7\}\ \{c_2, r_2, r_5, r_8\}\ \{c_2, r_3, r_6, r_9\}\ \{c_3, r_2, r_6, r_7\}.$$
$$\{c_3, r_3, r_4, r_8\}\ \{c_3, r_1, r_5, r_9\}\ \{c_4, r_2, r_4, r_9\}\ \{c_4, r_1, r_6, r_8\}$$
$$\{c_4, r_3, r_5, r_7\}$$



It is now straight forward to check that these 13 points and sets satisfy the axioms of a finite projective plane in the case $n = 3$. In general the $n - 1$

MOLS of order n will give an $n^2 \times (n+1)$ matrix M with entries in $\{1, \ldots, n\}$ and with no rectangle of entries of the form:

$$\begin{matrix} x & \cdots & y \\ \vdots & & \vdots \\ x & \cdots & y \end{matrix}$$

The above construction will then give $n^2 + n + 1$ points $\{c_1, c_2, c_3, \ldots, c_{n+1}, r_1, \ldots, r_{n^2}\}$ and $n^2 + n + 1$ lines each containing $n + 1$ points and such that each pair of points lies in just one line.

In general the non-rectangle property of M will ensure that these points and lines satisfy the axioms of a finite projective plane. For example how many points will be in both the lines:

$$\{c_j, r_i, \ldots\} \text{ and } \{c_{j'}, r_{i'}, \ldots\} \; ?$$

If $j = j'$ then the c_j is clearly the only point in common. And if $j \neq j'$ then the first line will have resulted from all the rows containing a (1) say in the j^{th} column, and the second line will have resulted from all the rows containing a (2) say the j' the column.

$$\begin{bmatrix} & 2 \\ 1 & \\ & 2 \\ 1 & 2 \\ 1 & \\ & 2 \\ 1 & \end{bmatrix} \begin{matrix} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \end{matrix}$$

$$\uparrow$$

$$j \quad j'$$

The non-rectangle property of M ensures that the pair (1,2) occurs precisely once across the columns j and j' (in the i^{th} row, say as shown) and hence that the two given lines intersect in the one point r_i

(⇒) Conversely assume that we are given a finite projective plane of order 3. It will consists of 13 points and 13 lines, with each line consisting of 4 points. Label the points of one of the lines as c_1, c_2, c_3, c_4 and label the remaining points as r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8 and r_9. Then, for example, the lines are:

$$\{c_1,c_2,c_3,c_4\}\ \{c_1,r_1,r_2,r_3\}\ \{c_1,r_4,r_5,r_6\}\ \{c_1,r_7,r_8,r_9\}$$
$$\{c_2,r_1,r_4,r_7\}\ \{c_2,r_2,r_5,r_8\}\ \{c_2,r_3,r_6,r_9\}\ \{c_3,r_2,r_6,r_7\}$$
$$\{c_3,r_1,r_5,r_9\}\ \{c_4,r_2,r_4,r_9\}\ \{c_4,r_1,r_6,r_8\}\ \{c_4,r_3,r_5,r_7\}$$
$$\{c_3,r_3,r_4,r_8\}$$

The fact that any two of the lines meet in a single point means that, a part from the line $\{c_1, c_2, c_3, c_4\}$. The remaining 12 lines are bound to fall into four groups of the three as follows:

Containing c_1: $\{c_1,r_1,r_2,r_3\}\ \{c_1,r_4,r_5,r_6\}\ \{c_1,r_7,r_8,r_9\}$

Containing c_2: $\{c_2,r_1,r_4,r_7\}\ \{c_2,r_2,r_5,r_8\}\ \{c_2,r_3,r_6,r_9\}$

Containing c_3: $\{c_3,r_2,r_6,r_7\}\ \{c_3,r_3,r_4,r_8\}\ \{c_3,r_1,r_5,r_9\}$

Containing c_4: $\{c_4,r_2,r_4,r_9\}\ \{c_4,r_1,r_6,r_8\}\ \{c_4,r_3,r_5,r_7\}$

Call the first set in each row (1), the second set (2) and the third set (3) as shown.

Define a 9×4 matrix M by the rule that the $(i, j)^{th}$ entry is k if the pair $\{c_j, r_i\}$ lies in a set labeled k. In our example this gives rise to the matrix

$$M = \begin{bmatrix} 1 & 1 & 3 & 2 \\ 1 & 2 & 1 & 1 \\ 1 & 3 & 2 & 3 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 3 & 3 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 1 & 3 \\ 3 & 2 & 2 & 2 \\ 3 & 3 & 3 & 1 \end{bmatrix} \leftarrow \text{e.g. } \{c_4, r_5\} \text{ lies in the set number 3.}$$

We can then use this matrix to read off, in the usual way, the two orthogonal 3×3 Latin squares.

$$L_1 = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix} \qquad L_2 = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix}$$

This process will work in general: the finite plan will consists of $n^2 + n + 1$ points and lines and will give rise to an $n^2 \times (n + 1)$ matrix M with entries in $\{1, \ldots, n\}$. the finite projective plane axioms will ensure that the matrix M has the usual non-rectangle property because entries of the form

$$\begin{matrix} i \rightarrow x \ldots y \\ i' \rightarrow x \ldots y \end{matrix}$$

would mean that $\{r_i, r_{i'}\}$ lies in two of the lines. Hence M will give rise to n - 1 mutually orthogonal n × n Latin squares as required.

Corollary (3.1.6): [2]

For every integer n that is power of prime number, there exists at least one projective plane of order n, (and consequently at least one complete set of MOLS of order n).

Remarks:

1- Why does Bose's result explain the non-existence of a finite projective plane of order 6?

It states that such a finite projective plane exists if and only if there exist a complete set of five mutually orthogonal Latin square of order six.

The possible existence of even a pair of orthogonal Latin square of order six was found older problem.

Euler found no solution to this particular problem. He then conjectured that no solution exists if the order of the latin square is of the form $n \equiv 2 \pmod 4$.

This is the famous Euler's conjecture. The first case n = 2 is trivially impossible.

2- Tarry around 1900 verified by a systematic enumeration that Euler's conjecture holds for $n = 6$. Since there does not exist even a pair of orthogonal Latin squares, Bose's result implies the non-existence of a projective plane of order 6. Yet, there is something unpleasant about systematic hand enumeration. It is messy and it is an error plane.

Mathematicians did find a better explanation in the celebrated Bruck-Ryser theorem, which was published in 1949.

Theorem (3.1.7): [9], [10], [29]

If $n \equiv 1$ or $2 \pmod 4$ then a finite projective plane of order n does not exist unless n is the sum of two integral squares.

Proof:

Since $n^2 + n + 1$ is always odd, by them implies a necessary condition for the existence of a projective plane of order n is that the equation

$$x^2 = ny^2 + (-1)^{n(n+1)/2} z^2$$

has a solution in integers x, y and z not all which are 0.

If $n \equiv 0$ or $3 \pmod 4$ then $n(n+1)/2$ is even and the equation has the solution $x = 1, y = 0, z = 1$.

For $n \equiv 1$ or $2 \pmod 4$, $n(n \div 1)/2$ is odd and we may rewrite the equation as

$$x^2 + z^2 = ny^2$$

Now, if n is sum of two integral squares, say $n = a^2 + b^2$, then there are solution $x = ay$ and $z = by$, for any integer y. On the other hand, if n is not the sum of two squares, then it can be shown that this equation has no integral solution (this requires some heavy duty number theory so it is omitted).

3.2 Facts on finite projective planes : [9], [10], [29] ,[1]

1- The Bruck-Ryser theorem shows that are no projective plans of order 6, 14, 21, 22, ...

2- The last theorem implies that there does not exist a finite projective plane of order 6. As a result we could have inferred since no pair, let alone a complete set, of MOLS of order 6 exists.

Now that we have a good explanation of the non-existence of a finite projective plane of order 6.

What is the next unknown case? It's $n = 10$, since $10 = 1^2 + 3^2$, a finite projective plane of order 10 would exist if the necessary condition of the Bruck-Ryser theorem is also sufficient. On the other hand, $10 \equiv 2 \pmod 4$, and so if one believes Euler's conjecture then it does not exists.

3- In *1989* Lam, Thiel and Swiercz proved that there is no projective plane of order 10 which involved great amounts of computers power and time.

4- The following table summarizes the known fact about the existence and number of projective planes of order n for $1 \leq n \leq 20$ which was established by a large computer search.

Order	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Number of projective planes	1	1	1	1	0	1	1	4	0	≥1	?	≥1	0	?	≥22	≥1	?	≥1	?

3.3 Final result

The result of Tarry [10] [6] [5] [29] [1] ,in which he tested a huge number of Latin squares of 6 in order to conclude the falsity of Euler's conjecture.

Bose ,shrikhand [6] and stinson [29] gives tow a different proof s for the non-existence of orthogonal mate of order 6, the proof was very complicated and lengthy.

Finally .Appa,Magos and mourtos [1] provide the same result for n = 6 and their method of proof was algebraic rather than enumerative ,they applied linear programming in order to obtain the appropriate result.

The strong correlation between orthogonal Latin squares and finite projective planes up to isomorphism guide us to the following theorem.

Theorem(3.2.1)

There exist orthogonal mate for every Latin square of order n except for $n=2$ *or* $n=6$

Proof

For n=2 ,there exist no orthogonal mate since it has no transversal .

While in the case $n=6$, there exist no finite projective plane of order 6 , because there are no integers x and y such that $x^2 + y^2 = 6$ [by theorem (3.1.7)] . The result is reached by theorem (3.1.5) .

ملخص البحث

في بحثنا هذا كان الهدف الأساسي هو تجميع المعلومات الأساسية الهامة عن المربعات اللاتينية و المستويات الاسقاطية المحدودة لما يمثله من أهمية في بعض التطبيقات مثل تصميم التجارب، وفي نظرية الرسم البياني وجداول الضرب المجمعة (وإن لم نتطرق لتلك التطبيقات).

فمع عدم توفر الكتب المختصة لهذا الموضوع، فقد بذلنا قصارى جهدنا في البحث والدراسة من خلال القليل المتوفر من بعض أجزاء من الكتب وشبكة المعلومات، والأوراق البحثية للحصول على المعلومات عن ذلك المصطلح (المربع اللاتيني) منذ ظهوره وحتى الآن.

ولتوضيح فكرة هذا البحث بإيجاز قمنا بتجزئته إلى ثلاث أبواب:

- الباب الأول: تناولنا فيه بعض التعاريف والنظريات الأساسية للمربع اللاتيني وشبيه الزمرة والمستطيل اللاتيني وكيفية تحويله إلى مربع لاتيني.
- الباب الثاني: خصص لمفهوم التعامد في مجموعة متبادلة من المربعات اللاتينية وأعدادها الممكن حصرها مع التطرق للتخمين المشهور لأويلر ونتيجة تيري بإيجاز.
- والباب الثالث تناولنا فيه مفهوم المستويات الاسقاطية المحدودة والنظريات الهامة عليه، والنظرية التي تربطه مع مجموعة متبادلة من المربعات اللاتينية.

في هذا البحث تم توظيف بعض الأمثلة لخدمة التعريفات والنظريات وبعض هذه الأمثلة جديد.

ينتهي البحث بنتيجة نهائية تضمنت صيغة جديدة لأثبات نظرية سابقة لم يسبق الوصول إليها حسب ما تبين لنا.

References

[1] Appa ,G., Magos , D., Mourtos , I., "*An LP-based proof for the non-existence of a pair of orthogonal Latin squares of order 6*", Operation research letters 32 (2004) 336-344.

[2] Appa ,G., Magos , D., Mourtos , I., "*Searching for mutually orthogonal Latin square via integer and constraint programming*", European Journal of Operational Research, Article in press (2005).

[3] Babai, L.,"*Discrete math*", lecture notes, http://people.cs.uchicago.edu/ , (2004).

[4] Batten, L. M., "*Combinatorics of finite geometries*", first published (1986).

[5] Bobkoski, C. "*Latin square*", lecture notes, Math 540.

[6] Bose, R. c., Shrikhande, S. S., "*On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin square of order 4t + 2*", proceedings American Mathematical Society, 95 (1960), pp. 189-203.

[7] Brualdi, R. A., "*Introductory combinatoric*", New Jersey: Prentice Hall (2004).

[8] Burris, S., Sankappanavar, H. P., "*A course in universal algebra*", Millennium edition,(2000).

[9] Cameron, P. J., "*Encyclopaedia of Design Theory*", www.designtheory.org , (2003).

[10] Colbourn, C. J., Dinitz, J. H., "*Handbook of combinatorial designs*",CRC press,(1996).

[11] Cullinane, S. H., "*Latin square geometry: Orthogonal Latin Squares as Skew Lines*", Notes on finite geometry, www.log24.com/notes , (1978).

[12] Denes, J., Keedwell, A., D., "*Latin square and their applications*", Academic Press, New York (1974).

[13] Drake, D. A., Van Rees, G. H. A., Wallis, W. D., "*Maximal sets of mutually orthogonal Latin square*", Discrete Mathematics 194 (1999) 87- 94.

[14] Gilbert, W. J., Nicholson W. K., "*Modern algebra with applications*", John Wiley & Sons, second edition. (2003).

[15] Graham, R. L., Grötschel, M., Lovase, L., "*Handbook of combinatoric*", Volume I, Elsevier press ,(1995).

[16] Golomb, S. W., "*Latin Squares and Transversals Solutions* ", IEE Information Theory Society Newsletter ,Vol. 53, No. 3, pp.(1059-2362).

[17] Huang, J., Ruriko, Y.,"*A method for Enumerating the number of 9×9 Diagonal Latin square with positional constraints*", Disc. Math.,124(1999), pp. 89-103.

[18] Johan, G., Jonathan, L., Jerrold W., Douglas R., "*Handbook of discrete and combinatorial mathematics*", Boca Raton London & New York Washington D.C. (2000).

[19] Keedwell, A.D., Mullen, G.L., "*Sets of partially orthogonal Latin square and projective plane*", Discrete mathematics, 288 (2004), pp 49-60

[20] Koscielny, C., "*Generating Quasi-groups for cryptographic applications*", int. J. Appl. Math. Comput. Sci. (2002), Vol. 12, No. 4, 559-569

[21] kraitchik,m. " Euler (Graco-Latin) squares " mathematical , New York 1942 , (179-182).

[22] Lam, C. W. H., "*The search for a finite projective plane of order 10*" ,Amer. Math. Monthly, November 30, (2005).

[23] McKay, B. D., Meynert, A., "*Small Latin squares, Quasigroups and loops*", Australian Research Council, (2001).

[24] McKay .B.D and manless .J,m. "on the number of Latin squares " Ann .Combi ,9,335-344,2005.

[25] Owns, P. J.," *Complete sets of pair wise orthogonal Latin square and the corresponding projective planes*", Journal of combinatorial theory, Series A , Mar. (1992).

[26] Parker, E. T., *"Construction of some sets of mutually orthogonal Latin squares"*. 10 (1944), pp. 249-257.

[27] Sabinin, L. V., "*Smooth Quasigroup and loops*",Kluwer, (1999).

[28] Sankappavaner, S., "*Graduate course in universal algebra*", (1973).

[29] Stinson, D. R., "*A short proof of the non existence of a pair of orthogonal Latin square of order six*", Journal of combinatorial theory, series A, 36 (1984). pp. 373-376

[30] Tarry . G"le proplm de 36 officiers "comte rendude , francasis avanc .sci . naturel ,122-123-1900

[31] Victor, B., "*Aspects of combinatorics*", Com. Univ. Press,(1993).

الجماهيرية العربية الليبية الشعبية ألاشتراكية العظمى

كلية العلوم / قسم الرياضيات

جامعة التحدي

المربع اللاتيني وتطابقه مع الإسقاط في المستويات

أطروحة لاستكمال متطلبات درجة الإجازة العليا الماجستير في الرياضيات بكلية العلوم جامعة التحدي

مقدمه من

الطالب:طارق عمر حمد بالطيب

أشراف

الدكتور:شعبان علي طربينه

التاريخ : ....
الموافق : 2007.1.5 م
الرقم الاشاري : ك ع / 22 /

كليـــة العلـــــوم

قســـم الرياضيات

عنـــوان البحـــث

((المربع اللاتيني و تطابقه مع الإسقاط في المستويات))

مقدمـــة مـــن الطـــالب

طارق عمر محمد أبوالطيب

* * لجنـــة المناقشـــة :

الدكتور / شعبان علي طرينه ....

(مشــرف الرسـالـــة)

الدكتور / أمين عبدالمجيد خواجه ....

(ممتحـن داخلـــي)

الدكتور / إبراهيم عبدالله تنتوش ....

(ممتحـن خارجـي)

يعتمـد :-

د. محمد علي سالم الفرجاني

أمين اللجنة الشعبية لكلية العلوم