Available online at http://www.iorajournal.org/index.php/ijgor/index

International Journal of Global Operations Research

e-ISSN: 2722-1016
p-ISSN: 2723-1739

Vol. 3, No. 2, pp. 74-79, 2022

The Connection Between Finite Projective Planes and Latin Squares

Mochamad Suyudi[1*]

[1] Department of Mathematics, Faculty of Mathematics and Natural Sciences, University of Padjadjaran
Jl. Ir. Soekarno KM 21 Jatinangor, Sumedang Indonesia

**Corresponding author email: moch.suyudi@gmail.com*

Abstract

A Latin square arrangement is an arrangement of *r* symbols in r rows and c columns, such that every symbol occurs once in each row and each column. When two Latin squares of same order are superimposed on one another, in the resultant array if every ordered pair of symbols occurs exactly once, then the two Latin squares are said to be orthogonal. If in a set of Latin squares, any two Latin squares are orthogonal then the set is called Mutually Orthogonal Latin Squares of order r. Methods of constructing when *p* is prime or prime power are discussed here. A finite projective plane of order *n* exists if *n* is a prime or power of a prime number and it has been assumed that this is the only one that exists, reminiscent of the conjecture about the existence of $n-1$ Latin squares *n x n* orthogonal to each other, so that these two existence problems are equivalent.

Keywords: Latin square, mutually orthogonal latin squares, finite projective plane.

1. Introduction

Finite projective planes, despite following a rather short set of axioms do not have much know about them and are very hard to find, unless specific circumstances are met. Not only are they hard to find, but we do not know even whether they are possible or impossible to create outside these circumstances. The main purpose of this thesis is exploring this question: for which cases is it possible to construct planes and how, as well as proving a specific case as impossible for a plane by a computer search. The thesis also seeks to cultivate a general understanding for these structures by using graphical tools in order to support a visual intuition of these rather abstract objects, as well as by showcasing a potential application in secret sharing (Hall, 1967).

At times the situations the experimenters found themselves made them to be totally engulfed in constructing designs in an efficient way without losing no or much information. This kind of situations arise when the number of experimental units in an experiment is often larger than that can be accommodated in the available blocks of relatively uniform experimental units, in this situation it is often desirable to have resolvable incomplete block designs in which the incomplete blocks can be arranged in complete blocks or replicates. Nowadays, it has been noticed that the levels at which the treatments increase are so high due to a lot of favorable factors that are peculiar to different field of studies while the experimental units that receive the treatments are smaller in numbers. Meanwhile, for the experimenters to be able to rise to these occasions or challenges, the use of resolvable incomplete block designs is inevitable.

From Latin square enumeration for example, refer to (Wilson, 1974), we can know that how many Latin squares can exist for a given s the order of the Latin square, but question is of their construction. There seems to be no good algorithm for constructing a random Latin square. One natural approach to counting and constructing Latin squares is to do it one row at a time, there by defining, “Latin rectangles”, and then try to obtain exact and asymptotic formulae, using the structural properties of the under lying templates (Denes and Keedwell, 1974; Denes, and Keedwell, 1991). Latin Squares were invented and studied by Euler in 1782.

A Latin square arrangement is an arrangement of *r* symbol in r^2 cells arranged in *r* rows and *r* columns such that each symbol occurs once in each row and in each column. This *r* is called the order of the Latin square. Two Latin squares of the same order *r* when superimposed on one another and if each pair of symbols in the resultant array occurs only once they are called orthogonal. On a given set of *N* Latin squares any two Latin squares are Orthogonal

then the set is called mutually orthogonal latin squares of order *r*. The cardinality of this set N is denoted by $O(N) \leq r - 1$.

2. Method

A `Latin square' is a square array or matrix in which each row and each column consists of the same set of entries without repetition. We shall generally restrict attention to Latin squares and rectangles in which the entries are positive integers. A *p x q* Latin rectangle (with entries in {1, 2, …, *n*}) is a *p x q* matrix with entries chosen from {1, 2, ... , *n*} and with no repeated entry in any row or column. In the cases when $p = q = n$ it is called a Latin square: in that case each row and each column consist precisely of the *n* numbers 1, 2, … and *n*.

Any *p x n* Latin rectangle with entries in {1, ..., *n*} can be extended to an *n x n* Latin square (Bryant, Victor.1993). Let *L* be a *p x q* Latin rectangle with entries in {1, ..., *n*} and let *r* and *m* be integers with $0 \leq r \leq m < p$. Then the number of members of (1, ..., *n*} which occur exactly *m* times in *L* and which occur in all of the first *r* rows of *L* cannot exceed

$$\frac{(n-q)(P-r)}{p-m} \tag{1}$$

Let *t* members of {1, … *n*} occur exactly *m* times in *L* and occur in all the first *r* rows of *L*. Then those *t* numbers each occur exactly *m* – *r* times in the lower shaded region of *L*. The other $n - t$ numbers in {1, …, *n*} each occur at most $p - r$ times in that same shaded region. So, counting the total occurrences in that shaded region gives

$$(p-r)q \leq t(m-r) + (n-t)(p-r) \tag{2}$$

which reduces to

$$t(p-m) \leq (n-q)(p-r) \tag{3}$$

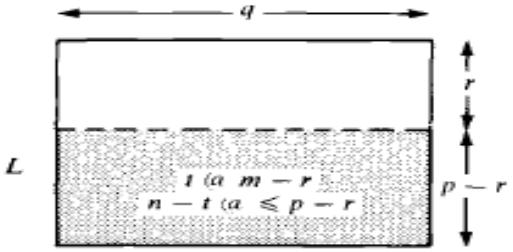

Figure 1. The *p x q* Latin rectangle *L*

The *p x q* Latin rectangle *L* with entries in {1, ... , *n*} can be extended to an *n x n* Latin square if and only if *L*(*i*), the number of occurrences of *i* in *L*, satisfies $L(i) \geq p + q - n$ for each *i* with $1 \leq i \leq n$.
Assume first that *L* can be extended to an *n x n* Latin square as shown:

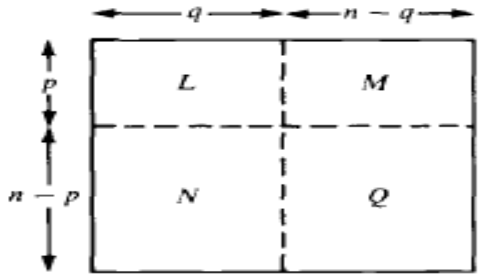

Figure 2. The *n x n* Latin rectangle *L*

Then *i* occurs $L(i)$ times in *L*, and *p* times in *L* and *M* together. So, *i* occurs $p - L(i)$ times in *M*. But *i* occurs $n - q$ times in *M* and *Q* together.

If *n* is a prime or a power of a prime then there exists $n - 1$ mutually orthogonal *n x n* Latin squares (Bryant, Victor.1993). Until now our *n x n* Latin squares have had entries from {1, 2, ... , *n*} but in this it is more convenient to choose the entries from {0, 1, . . . , *n* – 1}. In modular arithmetic the set of numbers {0, 1, 2, ..., *n* – 1} can be added and multiplified in a fairly sensible way `mod *n*' to give answers back in the same set. So, for example, the addition and multiplication tables `mod 5' are as shown:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition mod 5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication mod 5

Figure 3. The Addition and Multiplication Tables `mod 5'

Essentially the arithmetic operations are the normal ones but then the answers are reduced `mod *n*' by taking away all possible multiples of *n*. (If you have studied sufficient abstract algebra, you will know that in the case when *n* is prime the above process defines a `field'.)

Now let *n* be prime and let + and · denote addition and multiplication `mod *n*'. Define a collection $L_1, \ldots, L_{n-1}$ of *n x n* matrices by the rule that the (*i, j*)th entry of L_k is $k * (i-1) + (j-1)$. (If we do this in the case *n* = 5 we will get four 5 x 5 Latin squares very closely related to the collection displayed in the earlier example.) Clearly this process defines a collection of *n x n* matrices with entries chosen from {0, 1 …, *n* – 1} we now show that this collection consists of *n* – 1mutually orthogonal *n x n* Latin squares.

(i) L_k has no repeated entry in column *j*. If the (*i, j*)th entry equals the *(i', j*)th entry in L_k, where $i > i'$, then $k * (i-1) + (j-1) = k * (i'-1) + (j-1)$ and (as + and · behave very naturally) we can deduce that $k * (i-1) = k * (i'-1)$. This means that $k(i-1)$ and $k(i'-1)$ give the same remainder when divided by *n* and that their difference, $k(i-i')$, is divisible by *n*. Since *n* is prime, we can deduce that either *k* or $i - i'$ is divisible by *n*. But as $1 \le k \le n-1$, and $1 \le i - i' \le n-1$ this is clearly impossible. Hence no L_k has a repeated entry in any of its columns.

(ii) L_k has no repeated entry in row *i*. This is very similar to (*i*), but slightly easier, and is left as an exercise.

(iii) Properties (i) and (ii) confirm that each L_k is a Latin square. We now show that L_k and $L_{k'}$, are orthogonal.

If $k \neq k'$ and L_k and $L_{k'}$ are not orthogonal then across these two squares some pair will occur twice, in the (*i, j*)th and (*i', j'*)th places, say.

$$L_k = \begin{pmatrix} & x & & \\ & & & x \\ & & & \end{pmatrix} \begin{matrix} \\ \leftarrow i \\ \leftarrow i' \\ \\ \uparrow \quad \uparrow \\ j \quad j' \end{matrix} \qquad L_{k'} = \begin{pmatrix} & y & & \\ & & & y \\ & & & \end{pmatrix} \begin{matrix} \\ \leftarrow i \\ \leftarrow i' \\ \\ \uparrow \quad \uparrow \\ j \quad j' \end{matrix}$$

Figure 4. L_k and $L_{k'}$, Orthogonality

But then the (*i, j*)th entry of L_k will equal the (*i', j'*)th entry of L_k and the (*i, j*)th entry of $L_{k'}$ will equal the (*i', j'*)th entry of $L_{k'}$; i.e. $k * (i-1) + (j-1) = k * (i'-1) + (j'-1)$ and $k' * (i-1) + (j-1) = k' * (i'-1) + (j'-1)$. Subtracting these two equations shows us that $(k-k')(i-i')$ is divisible by *n*, but an argument similar to that in (i) using the primness of *n* shows that this is impossible. Hence L_k and $L_{k'}$ are indeed orthogonal. We have therefore seen how to construct $n-1$ mutually orthogonal *n x n* Latin squares in the case when *n* is prime. We now give a brief outline of how to extend this to the case when *n* is a power of a prime.

In our construction above the key fact about {0, 1, ..., $n-1$} under + and · is that it forms a field (essentially the operations behave in a sensible arithmetic fashion and, in particular, if the product of two numbers is zero then one of the numbers must itself be zero). In the case when *n* is a power of a prime this set-up fails to be a field (for example if $n = p^r$ where $r > 1$ then $p^* p^{r-1} = 0$). However, in this case it is still possible to define other operations of addition and multiplication on {0, 1, ..., -1 } which make it into a field: this field is known as the Galois field GF(*n*). The details of the operations (defined via polynomials) need not concern us here but once we know that such a field exists the first part of this proof can easily be generalized to the case when *n* is a power of a prime.

In that proof we essentially saw that if there exists a field of *n* elements then there exist $n-1$ mutually orthogonal *n x n* Latin squares (but not conversely) and it is known that such a field exists precisely when *n* is a prime or a power of a prime. But it still remains an unsolved conjecture that there exists a `full set' of *n* – 1 mutually orthogonal *n x n* Latin squares if and only if *n* is a prime or a power of a prime. We shall return to this conjecture shortly.

3. Results and Discussion

There exists a finite projective plane of order *n* if and only if there exist *n* – 1 mutually orthogonal *n x n* Latin squares. Sketch We shall merely illustrate the connection between the two problems by constructing a finite projective plane of order 3 from two given orthogonal 3 x 3 Latin squares and, conversely, by constructing two orthogonal 3 x 3 Latin squares from a given finite projective plane of order 3. Of course, this does not constitute a proof of the general result but the techniques do generalize easily, and we include some comments about the general case.
Start with two orthogonal 3 x 3 Latin squares:

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

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

$$M = \begin{pmatrix} 1 & 1 & 3 & 2 \\ 1 & 2 & 1 & 1 \\ 1 & 3 & 2 & 3 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 3 & 3 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 1 & 3 \\ 3 & 2 & 2 & 2 \\ 3 & 3 & 3 & 1 \end{pmatrix}$$

← e.g. the (1, 3)rd entry of L_1 is 2 and of L_2 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 referring to the columns 1 - 4 and the rows 1 - 9). Then 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 in 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). Overall this gives the following 13 `lines':

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

It is now straightforward to check that these 13 points and sets satisfy the axioms of a finite projective plane in the case *n* = 3. In general, the $n-1$ mutually orthogonal *n x n* Latin squares will give an $n^2 \times (n+1)$ matrix *M* with entries in {1, …, *n*} and with no rectangle of entries of the form

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

The above construction will then give $n^2 + n + 1$ points $\{c_1, \dots, c_{n-1}, r_1, r_{n^2}\}$ 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

$\{c_j, r_i, \ldots\}$ 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 in the j'^{th} column. 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 consist of 13 points and 13 lines, with each line consisting of 4 points. Label the points of one of the j-lines as c_1, c_2, c_3, c_4 and label the remaining points as $r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8,$ dan r_9. Then, for example, the lines might be:

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

The fact that any two of the lines meet in a single point means that, apart from the line $\{c_1, c_2, c_3, c_4\}$, the remaining 12 lines are bound to fall into four groups of 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:	$\{c_4, r_2, r_4, r_9\}$	$\{c_4, r_1, r_6, r_8\}$	$\{c_4, r_3, r_5, r_7\}$
	1	2	3

Call the first set in each row `1', the second set `2' and the third set `3', as shown. Then define a 9 x 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 labelled k. In our example this gives rise to the matrix

$$M = \begin{pmatrix} 1 & 1 & 3 & 2 \\ 1 & 2 & 1 & 1 \\ 1 & 3 & 2 & 3 \\ 2 & 1 & 2 & 1 \\ 2 & 2 & 3 & 3 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 1 & 3 \\ 3 & 2 & 2 & 2 \\ 3 & 3 & 3 & 1 \end{pmatrix}$$

e.g. $\{c_4, r_5\}$ lies in the set number 3

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

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

This process will work in general: the finite projective plane will consist 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, ..., n}. The finite projective plane axioms will ensure that the matrix M has the usual non-rectangle property because entries of the form

$$i \rightarrow \quad x \quad \ldots \quad y$$

$$i' \rightarrow \quad x \quad \ldots \quad y$$

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

4. Conclusion

Finite projective planes of order n = 2, 3, 4, 5, 7, 8, 9, and 11 all exist because these are all primes or powers of primes and are thus covered by the existence for $n - 1$ mutually orthogonal *n x n* latin squares . There are no finite projective planes of order 6 because, as we noted earlier, there are no orthogonal pairs of Latin 6 x 6 squares.

References

Bryant, Victor.(1993). Aspects of combinatorics : a wide-ranging introduction. Cambridge university press

Denes, J. and Keedwell, A. D. (1974). *Latin squares and their Applications*. Academic Press, New York. 1974.

Denes, J., and Keedwell, A.D. (Eds). (1991). Latin squares: New Developments in Theory and Application Ann. Discrete Mathematics 46, North Holland, New York 1991.

Euler, L. Recherches sur une nouvelle espace de quarries magiques. (1782). Verhandelingen uitegegeren door het zeeuwseh Genoolschap der wetenschappen te Vlissingen **9,** 85-239.

Hall, M. (1967). Combinatorial theory. Waltham, Mass : Blaisdell Pub. Co.

Wilson. R.M. (1974). Concerning the number of mutually orthogonal Latin squares. Discrete Mathematics, **9**, 181-198