Orthogonal Latin Squares and the Falsity of Euler's Conjecture

Aloke Dey*

1. Introduction

The problems relating to the existence and construction of orthogonal Latin squares have fascinated researchers for several centuries now. Though many important discoveries have been made, some problems still remain unresolved. Latin squares and orthogonal Latin squares have a beautiful underlying structure and are related to other combinatorial objects. These have applications in different areas, including statistical design of experiments and cryptology. Comprehensive accounts of the theory and applications of Latin squares are available in the books by J. Dénes and A. D. Keedwell (1974, 1991) and C. F. Laywine and G. L. Mullen (1998).

One of the most intriguing questions about orthogonal Latin squares was raised in the 18th century. In 1782, Leonhard Euler made a famous conjecture that there does not exist a pair of orthogonal Latin squares of order $4t + 2$, where $t \geq 1$ is an integer. The first serious doubts on the truth of Euler's conjecture were raised by R. C. Bose and S. S. Shrikhande on the one hand and by E. T. Parker on the other, both appearing in 1959. Subsequently, all of them collaborated to prove that Euler's conjecture was indeed false for every integer $t > 1$. This is considered as a landmark result in combinatorial designs. In this article, we present a brief survey of some of the important results on orthogonal Latin squares with emphasis on the work of Bose and Shrikhande leading to the falsity of Euler's conjecture. In the last section, we mention some historical facts related to orthogonal Latin squares.

2. Orthogonal Latin Squares

A Latin square of *order* (or, side) s is an $s \times s$ array with entries from a set of s distinct symbols (or, letters) such that each symbol appears in each row and

*Indian Statistical Institute, New Delhi

R. Bhatia et al. (Eds.), *Connected at Infinity II*

each column precisely once. Two Latin squares of the same order are said to be *orthogonal* to each other if, when any of the squares is superimposed on the other, every ordered pair of symbols appears exactly once. Orthogonal Latin squares can be equivalently defined as follows: Two Latin squares of side s, $L_1 = (a_{ij})$ on symbols from a set S_1, and $L_2 = (b_{ij})$ on symbols from a set S_2, are orthogonal if every element in $S_1 \times S_2$ occurs exactly once among the s^2 pairs (a_{ij}, b_{ij}), $1 \leq i, j \leq s$. For example, consider the following pair of Latin squares of order $s = 4$:

$$L_1 = \begin{matrix} A & C & D & B \\ B & D & C & A \\ C & A & B & D \\ D & B & A & C \end{matrix}, \quad L_2 = \begin{matrix} \alpha & \delta & \beta & \gamma \\ \beta & \gamma & \alpha & \delta \\ \gamma & \beta & \delta & \alpha \\ \delta & \alpha & \gamma & \beta \end{matrix}.$$

Superimposing L_2 over L_1, one gets the following arrangement:

$$L = \begin{matrix} A\alpha & C\delta & D\beta & B\gamma \\ B\beta & D\gamma & C\alpha & A\delta \\ C\gamma & A\beta & B\delta & D\alpha \\ D\delta & B\alpha & A\gamma & C\beta \end{matrix}.$$

Clearly, L_1 and L_2 are orthogonal to each other. The arrangement like L is called an *Eulerian square*, named after the legendary mathematician Euler (1707–1783). Euler studied such objects in 1782 and also made a famous conjecture about their existence.

If in a set of Latin squares every pair is orthogonal, then the set is said to form a set of *mutually orthogonal Latin squares* (MOLS). It is a nice exercise to show that the number of MOLS of order s is bounded above by $s - 1$. When this upper bound is attained, we say that there is a *complete set* of MOLS.

Orthogonal Latin squares are related to other combinatorial objects and we describe some of these. Latin squares are related to quasigroups. Recall that a *quasigroup* is a pair $< Q, * >$, where Q is a set and $*$ is a binary operation on Q, such that the equations $a*x = b$ and $y*a = b$ are uniquely solvable for every pair of elements $a, b \in Q$. It is easy to see that the Cayley (or 'multiplication') table of a quasigroup (with the headline and sideline removed) is a Latin square. Two quasigroups $< Q, \odot >$ and $< Q, \oplus >$ with binary operations $\odot$ and $\oplus$, defined over the same set Q are said to be *orthogonal* if the equations $x \odot y = z \odot t$ and $x \oplus y = z \oplus t$ together imply that $x = z$ and $y = t$. When a pair of quasigroups $< Q, \odot >$ and $< Q, \oplus >$ are orthogonal, their corresponding Latin squares are also orthogonal. A pair of orthogonal Latin squares, derived from

two orthogonal quasigroups with 3 elements is shown below:

$\odot$	1	2	3
1	1	3	2
2	2	1	3
3	3	2	1

$\oplus$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Another object related to orthogonal Latin squares is an *orthogonal array*. An orthogonal array $OA(N, k, s, g)$ of strength g $(2 \leq g \leq k)$ is a $k \times N$ matrix A with entries from a finite set S containing $s \geq 2$ elements, such that in any $g \times N$ sub-matrix of A, each of the g-tuples of symbols from S occurs the same number of times, say λ times, as a column. It follows then that in an $OA(N, k, s, g)$, $N = \lambda s^g$. The integer λ is called the *index* of the array.

Let $\{L_u, 1 \leq u \leq k\}$ be a set of k MOLS of order s on symbols $1, 2, \ldots, s$. Form a $(k+2) \times s^2$ array $A = (a_{ij})$ whose columns are

$$(i, j, L_1(i,j), L_2(i,j), \ldots, L_k(i,j))' \text{ for } 1 \leq i, j \leq s.$$

Then, one can show that A is an orthogonal array $OA(s^2, k+2, s, 2)$ of strength *two* and index unity. Conversely, reversing the above steps one can obtain k MOLS of order s from an $OA(s^2, k+2, s, 2)$. As an example, consider the following three MOLS of order 4:

$$L_1 = \begin{matrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{matrix}, \quad L_2 = \begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{matrix}, \quad L_3 = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix}.$$

Following the steps of construction just described, one gets an $OA(16, 5, 4, 2)$, displayed below.

$$\begin{bmatrix} 1111 & 2222 & 3333 & 4444 \\ 1234 & 1234 & 1234 & 1234 \\ 1234 & 4321 & 2143 & 3412 \\ 1234 & 3412 & 4321 & 2143 \\ 1234 & 2143 & 3412 & 4321 \end{bmatrix}.$$

As stated earlier, the maximum number of MOLS of order s is $s-1$. This upper bound is attainable if s is a prime or a prime power. The problem of construction of a complete set of MOLS of order s when $s = p^n$ where p is a prime and n is a positive integer was solved by Bose (1938) and independently, by W. L. Stevens (1939). We briefly describe below the method given by Bose (1938).

Let s be a prime or a prime power and let $GF(s)$ denote the Galois field of order s with elements $\rho_0 = 0, \rho_1 = 1, \rho_2, \ldots, \rho_{s-1}$. Consider a square L_i, whose

(r,t)th cell is filled by the element

$$\rho_r + \rho_i \rho_t, \quad 1 \leq i \leq s-1, \; 0 \leq r,t \leq s-1.$$

It can be verified that (i) L_i is a Latin square of order s for each i and (ii) for $i \neq j$, L_i and L_j are orthogonal. This then provides a method of constructing a complete set of MOLS of order s, where s is a prime or a prime power.

3. Connection with Finite Projective Planes

Bose (1938) showed that there is a 1-1 relation between a complete set of MOLS and a finite projective plane. Consider a (finite) set of elements, called *points*, certain subsets of points, called *lines* and an *incidence relation* between them. The set of points and lines are said to form a *finite projective plane* if the following axioms hold:

P1: There is exactly one line which is incident with every pair of distinct points, i.e., there is exactly one line through a pair of distinct points.

P2: There is exactly one point in common with every pair of distinct lines.

P3: There exist four points, no three of which are incident with the same line.

Note that there is a symmetry in the axioms P1–P3, making the principle of duality hold in the geometry in the sense that the roles of points and lines can be interchanged, without affecting the properties of the geometry. In a finite projective plane, each line is incident with $(s+1)$ points and each point is incident with $(s+1)$ lines, where $s \geq 2$ is an integer. The total number of points, as also the total number of lines, in a finite projective plane is (s^2+s+1). A finite projective plane in which each line has $(s+1)$ points is said to be of *order* s.

A finite projective plane of order $s(\geq 2)$ where s is a prime or a prime power can be constructed as follows. Let $s = p^q$, where p is a prime and q, a positive integer. An ordered triplet (x,y,z), where $x,y,z \in GF(s)$ and $(x,y,z) \neq (0,0,0)$, is said to define a point of the finite projective plane. Two ordered triplets (x_1,x_2,x_3) and (y_1,y_2,y_3) define the same point if and only if $y_i = cx_i$, $(i = 1,2,3)$, where $(0 \neq c) \in GF(s)$. A linear homogeneous equation $ax + by + cz = 0 \pmod{s}$, where $a,b,c \in GF(s)$ and $(a,b,c) \neq (0,0,0)$, defines a line. Two such equations define the same line if their corresponding coefficients are proportional. The point (x_0,y_0,z_0) is said to be incident with the line $ax + by + cz$ if $ax_0 + by_0 + cz_0 = 0$. The set of points, lines and the incidence relation so defined can be verified to satisfy axioms P1–P3 and thus form a finite projective plane of order s.

We now describe the connection between a complete set of MOLS and a finite projective plane, both of order s, where s is a prime or a prime power.

Let ℓ be a line in a finite projective plane and $x_r, x_c, x_1, \ldots, x_{s-1}$ be the points on ℓ. The remaining $s(s+1)$ lines (other than ℓ) can be partitioned into $(s+1)$ sets of s lines each, such that any pair of lines in the same set intersect ℓ at some point. We may call ℓ and the points on it as the line and points at infinity, respectively. Let us delete the line ℓ and all points on it and, call the remaining lines and points as finite lines and finite points. Then the set of lines intersecting at say, x defines a *pencil* of finite lines, which may be denoted as $[x]$. The finite lines thus get partitioned into pencils of lines $[x_r], [x_c], [x_1], [x_2], \ldots, [x_{s-1}]$. Let the s lines in a pencil be labeled by the integers $0, 1, \ldots, s-1$. The lines of $[x_r]$ and $[x_c]$ can be associated with the rows and columns, respectively, of an $s \times s$ array, such that the (u, v)th cell of the array is the point of intersection of line u of $[x_r]$ and line v of $[x_c]$. For $1 \leq i \leq s-1$, corresponding to the pencil $[x_i]$, let us form a square L_i whose (u, v)th entry is the number corresponding to the line of $[x_i]$ which passes through the point corresponding to the cell (u, v). Then, it can be shown that L_i is a Latin square of order s. Through the point corresponding to the (u, v)th cell, there is exactly one line of $[x_i]$ and one line of $[x_j]$, $i, j = 1, 2, \ldots, s-1, i \neq j$. This shows that for $i \neq j$, the Latin squares L_i and L_j are orthogonal.

Conversely, let $L_1, L_2, \ldots, L_{s-1}$ be a complete set of MOLS of order s whose symbols, without loss of generality, can be taken to be $0, 1, \ldots, s-1$. Let L_R (respectively, L_C) be two $s \times s$ arrays in which the symbol i appears in all the cells of the row (respectively, column) numbered $i, 0 \leq i \leq s-1$. Define s^2 points $(i, j), 0 \leq i, j \leq s-1$. Join the points with the same first coordinate by a line. Then we have s lines, which are parallel (i.e., have no common point). Let these lines intersect at a new point x_R. Similarly, obtain s lines by joining the points with the same second coordinate and let these lines intersect at a new point, say x_C. For the Latin square L_i, let the s^2 cells be identified with the s^2 points described above. Join the points corresponding to the same integer in L_i and let these s lines intersect at a new point $x_i, 1 \leq i \leq s-1$. Finally, join $x_R, x_C, x_1, \ldots, x_{s-1}$ by a line. Then it can be verified that this collection of points and lines forms a finite projective plane.

As noted above, a finite projective plane of order s exists if s is a prime or a prime power and this plane coexists with a complete set of MOLS of order s. A natural question then is: for what other values of s does a finite projective plane exist? This is one of the most difficult questions in finite geometry. Unfortunately, very little is known. The earliest result about the existence of finite projective planes (of non-prime power orders) is due to R. H. Bruck and H. J. Ryser (1949). This result forms a special case of the results in S. Chowla and Ryser (1950) and Shrikhande (1950), given in different forms. We state below the result, called the *Bruck-Ryser-Chowla Theorem* in the language of finite projective planes, though an equivalent statement in terms of the exis-

tence conditions of certain balanced incomplete block designs is also used in the literature.

Theorem 3.1. *If a projective plane of order* $s \equiv 1$ *or* $2 \pmod 4$ *exists, then* s *is the sum of squares of two integers.*

Equivalently, the above result states that if $s \equiv 1$ or $2 \pmod 4$, then no finite projective plane of order s exists unless s is the sum of squares of two integers. Thus, Theorem 3.1 rules out the existence of a finite projective plane of orders $s = 6$ and 14. However, it does not rule out the existence of a projective plane of order 10. C. W. H. Lam, L. H.Thiel and S. Swiercz (1989) showed the non-existence of a finite projective plane of order 10 through a massive computer search. Nothing more than the above stated results on the existence of a finite projective plane of order s, where s is neither a prime nor a prime power seems to be known.

4. The MacNeish-Mann Conjecture

For an integer s, let $N(s)$ denote the maximum number of MOLS of order s. Then, as seen earlier, $N(s) \geq s - 1$, if s is a prime or a prime power. A challenging problem is to determine the value of $N(s)$ (or, bounds on $N(s)$) when s is neither a prime nor a prime power. One of the earliest results in this direction is due to H. F. MacNeish (1922); this was generalized somewhat and put on an algebraic foundation by H. B. Mann (1942). Let $s = p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$ be the prime-power decomposition of s, where $p_1, \ldots, p_m$ are distinct primes and $n_1, \ldots, n_m$ are positive integers. Define

$$n(s) = min\{p_1^{n_1}, p_2^{n_2} \ldots, p_m^{n_m}\} - 1. \tag{4.1}$$

MacNeish (1922) showed that $N(s) \geq n(s)$. MacNeish went further to conjecture that $n(s)$ is also the upper bound on $N(s)$ and therefore, $N(s) = n(s)$. The MacNeish-Mann construction of $n(s)$ MOLS of order s can be described as follows: Consider the system of s elements

$$\gamma = (g_1, g_2, \ldots, g_m),$$

where for $1 \leq i \leq m$, $g_i \in GF(p_i^{n_i})$. The addition and multiplication of these elements are defined by the following rules:

$$\begin{aligned} \gamma_1 + \gamma_2 &= (g_1, \ldots, g_m) + (h_1, \ldots, h_m) \\ &= (g_1 + h_1, \ldots, g_m + h_m); \\ \gamma_1 \gamma_2 &= (g_1 h_1, \ldots, g_m h_m), \end{aligned}$$

where the operations above in each component are as defined in the corresponding Galois field. The system so constructed is however, not a field, as not all elements in the system have a multiplicative inverse.

Let $g_i^{(0)} = 0, g_i^{(1)} = 1, g_i^{(2)}, \ldots, g_i^{(t_i)}$ be the elements of $GF(p_i^{n_i})$, $1 \leq i \leq m$, where $t_i = p_i^{n_i} - 1$. Let $n(s)$ be as in (4.1). Then,

$$\gamma_j = [g_1^{(j)}, g_2^{(j)}, \ldots, g_m^{(j)}],\ 0 \leq j \leq n(s), \tag{4.2}$$

possesses inverses and so does $\gamma_i - \gamma_j$ for $i \neq j$. Let us label the points γ in such a way that $0 = \gamma_0 = (0, 0, \ldots, 0)$ and the next $n(s)$ elements are given by (4.2). Form the $n(s)$ arrays L_j, whose (u, v)th element is filled by the element $\gamma_u + \gamma_j \gamma_v$ for $1 \leq j \leq n(s)$; $0 \leq u, v \leq s - 1$. Then, for a given j, L_j is a Latin square and $L_1, L_2, \ldots L_{n(s)}$ form a set of MOLS of order s (for a proof of this assertion, see e.g., Mann (1949, p. 140)).

Parker (1959a) showed that the MacNeish conjecture (also called the MacNeish-Mann conjecture) is false. Note that had the MacNeish-Mann conjecture been true, it would have shown the truth of Euler's conjecture as, by the MacNeish-Mann conjecture, $N(s) = 1$ if $s \equiv 2 \pmod 4$. Though the result of Parker cast doubts on the truth of Euler's conjecture, it did not show its falsity. In order to describe the result of Parker, we recall the definitions of balanced incomplete block (BIB) designs and, Mersenne and Fermat primes.

Let $\mathcal{V}$ be a finite set of v objects (or, *treatments*, using the terminology of statistical design of experiments) and $\mathcal{B}$, a collection of k-subsets of $\mathcal{V}$, where $2 \leq k < v$; these subsets are called *blocks*. The pair $(\mathcal{V}, \mathcal{B})$ is a *balanced incomplete block* (BIB) design if (i) every treatment appears in r blocks and (ii) each pair of treatments occurs together in λ blocks. If $|\mathcal{B}| = b$, where $|\cdot|$ denotes the cardinality of a set, then the integers v, b, r, k, λ are called the parameters of a BIB design. A set of necessary (but not sufficient) conditions for the existence of a BIB design is

$$vr = bk,\ \lambda(v - 1) = r(k - 1),\ b \geq v.$$

In view of the first two indentities, one can write the parameters of a BIB design in terms of three independent parameters, say v, k and λ. Henceforth, we shall always denote a BIB design by the triple (v, k, λ). A BIB design (v, k, λ) is *symmetric* if $v = b$ and is said to be *resolvable* if its blocks can be partitioned into r sets, each set containing b/r blocks, such that each treatment appears exactly once in each set.

A *Mersenne prime* is a prime number of the form $2^p - 1 = M_p$ (say). For instance, $M_2 = 3, M_3 = 7, M_5 = 31$. If $2^p - 1$ is a prime, then so is p. However, the converse is not true; for example, $M_{11} = 2047 = (23)(89)$ is *not* a prime. A *Fermat prime* is a Fermat number $F_n = 2^{2^n} + 1$ which is a prime. For instance, $F_0 = 3, F_1 = 5, F_2 = 17$. No Fermat primes are known for $n > 4$.

Parker (1959a) proved the following result.

Theorem 4.1. *If there exists a BIB design* (v, k, λ) *with* $\lambda = 1$ *and* k *is the order of a finite projective plane, then there exists a set of* $k-2$ *MOLS of order* v.

Theorem 4.1 was specialized and slightly strengthened by Parker (1959a) to yield the following result.

Theorem 4.2. *If* m *is a Mersenne prime larger than 3, or* $m+1$ *is a Fermat prime larger than 3, then there exists a set of* m *MOLS of order* $m^2 + m + 1$.

The first case where Theorem 4.2 applies is $m = 4$, which yields a set of 4 MOLS of order $21(= 4^2 + 4 + 1)$. Note that for all orders covered by Theorem 4.2, $m \equiv 1 \pmod 3$ and $m^2 + m + 1 \equiv 3 \pmod 9$. Therefore, the construction of MacNeish produces only $n(s) = 2$ orthogonal Latin squares. We now know that there exist 5 MOLS of order $s = 21$ (A. V. Nazarok, 1991).

5. Falsity of Euler's Conjecture

The existence of an *Eulerian square* of order s defined in Section 2 is clearly equivalent to that of a pair of orthogonal Latin squares of order s. Eulerian squares are also known by the name *graeco-latin squares* in the statistical literature as, traditionally, one of the squares involved was written using Latin alphabets and the other, using Greek alphabets. In 1779, Euler started looking at the problem of finding Eulerian squares of every order. In fact, in his 1779 paper (which was published in 1782), Euler was able to construct an Eulerian square of every order s, where s is (i) either an odd integer or, (ii) a multiple of 4. Thus, the existence of Eulerian squares of all orders s where $s \equiv 0, 1,$ or $3 \pmod 4$ was settled by Euler in 1782. The only case not settled till then was for orders $s \equiv 2 \pmod 4$. This brings us to the problem of 36 officers, stated below.

"There are 36 army officers, 6 from each rank and 6 from each regiment. Is it possible to arrange these 36 officers in a 6×6 square arrangement such that each rank and each regiment shows up in each row and each column?"

How did this problem arise in the first place? Folklore has the following 'explanation':

"It appears that the Emperor was to visit a garrison town in which six regiments were quartered and the commandant took into his head to arrange 36 officers in a square, one of each rank from each regiment, so that, whichever

row or column the Emperor walked along, he would meet one officer of each of the six ranks and one from each of the six regiments".

The commandant, of course, had set himself an impossible task as, the solution to the problem is provided by a 6×6 Eulerian square, which was later shown to be non-existent. Euler (1782) himself could not find an Eulerian square of order 6; he proceeded to 'show' the non-existence of such a square using an argument that is not entirely correct in method but correct in its conclusion. Having failed to construct an Eulerian square of order 6, Euler went on to make the following conjecture.

Euler's Conjecture: *No Eulerian square of order* $s \equiv 2 \pmod 4$ *exists.*

G. Tarry in 1900, by an exhaustive and laborious search showed the impossibility when $s = 6$. A shorter proof of the non-existence of an Eulerian square of order 6, based on coding theory was given by D. R. Stinson (1984). J. Peterson (1901) and P. Wernicke (1910) made errorneous attempts to prove Euler's conjecture as did MacNeish (1922). The arguments used by Peterson and MacNeish were shown to be false by F. W. Levi (1942) and the falsity of Wernicke's argument was shown by MacNeish (1921). Two leading statisticians, R. A. Fisher and F. Yates, in 1934 published a list of all possible Latin squares of order 6 and concluded as below:

"Euler's conclusion that no Greaco-Latin 6×6 square exists is easily verified from the 12 types of 6×6 Latin squares exemplified in this paper".

The first result casting serious doubts on the truth of Euler's conjecture is due to Bose and Shrikhande (1959) who were able to construct an Eulerian square of order $s = 22$. In their construction, Bose and Shrikhande (1959) used a class of designs called *pairwise balanced* designs, which may be viewed as a generalization of BIB designs. Let $\mathcal{V}$ be a finite set of v treatments and consider b blocks (subsets of $\mathcal{V}$), which are possibly of different sizes. These blocks form a pairwise balanced design of index unity and type $(v; k_1, k_2, \ldots, k_m)$ if each block contains either k_1 or k_2 or, $\ldots, k_m$ treatments and every pair of distinct treatments occurs exactly in one block, where for $1 \leq i \leq m$, $k_i \leq v$, $k_i \neq k_j$. Bose and Shrikhande (1959) proved the following result.

Lemma 5.1. *Suppose there exists a set* S *of* $q - 1$ *MOLS of order* k*, then we can construct a* $q \times k(k-1)$ *matrix* P*, with entries* $1, 2, \ldots, k$*, such that any ordered pair* $\binom{i}{j}$*,* $i \neq j$*, occurs as a column exactly once in any two-rowed submatrix of* P*.*

Proof. Without loss of generality, let the first row of each Latin square in the set S have symbols $1, 2, \ldots, k$, in that order. Prefix the set S by a $k \times k$ array containing the symbol i in each position of the ith column. If the elements of

each square are written in a single row such that the symbol in the ith row and jth column occupies the nth position in the row, where $n = k(i-1)+j$, then one can display these squares in the form of an orthogonal array $OA(k^2, q, k, 2)$. By deleting the first k columns, we get the desired matrix P. □

Let γ be a column of k distinct treatments $t_1, t_2, \ldots, t_k$ in that order. Let $P(\gamma)$ denote the $q \times k(k-1)$ matrix obtained by replacing the symbol i in P, by the treatment t_i occupying the ith position in γ, $1 \leq i \leq k$. Clearly every treatment occurs exactly $k-1$ times in every row of $P(\gamma)$ and any ordered pair $\binom{t_i}{t_j}$ occurs as a column exactly once in every two-rowed submatrix of $P(\gamma)$. We are now in a position to state the main result of Bose and Shrikhande (1959).

Theorem 5.1. *Let there exist a pairwise balanced design of index unity and type $(v; k_1, \ldots, k_m)$ and suppose there exist $q_i - 1$ MOLS of order k_i. If $q = min\{q_1, \ldots, q_m\}$, then there exist $q-2$ MOLS of order v.*

Proof. Let the treatments of the pairwise balanced design be $t_1, \ldots, t_v$ and let the blocks of the design, written as columns which contain k_i treatments be denoted by $\gamma_{i1}, \ldots, \gamma_{ib_i}$, where for $1 \leq i \leq m$, b_i is the number of blocks of size k_i in the pairwise balanced design.

Let P_i be the matrix of order $q_i \times k(k-1)$ defined in Lemma 5.1, the elements of P_i being the symbols $1, 2, \ldots, k$. Let $C_{ij} = P_i(\gamma_{ij})$ be the matrix obtained from P_i and γ_{ij}. Suppose C^*_{ij} is obtained from C_{ij} by retaining any q rows. Define the $q \times v(v-1)$ matrix

$$C^* = [C^*_{11}, C^*_{12}, \ldots, C^*_{1b_1}, \ldots, C^*_{m1}, C^*_{m2}, \ldots, C^*_{mb_m}].$$

Let C^*_0 be a $q \times v$ matrix whose ith column contains t_i in every position, $1 \leq i \leq v$. Then, $[C^*_0, C^*]$ is an orthogonal array $OA(v^2, q, v, 2)$. Using any two rows of this orthogonal array to coordinatize, we get $q-2$ MOLS of order v. □

As an illustration of Theorem 5.1, consider a BIB design $(15, 3, 1)$, which has $b = 35$ blocks and each treatment is replicated $r = 7$ times. A resolvable solution for this design exists. Consider this resolvable BIB design and to each block of a replication, add a new treatment θ_i, $1 \leq i \leq 7$. Next, add a new block containing the treatments $\theta_1, \theta_2, \ldots, \theta_7$. This process gives us a pairwise balanced design of index unity and type $(22; 4, 7)$. Since there exist $q_1 = 3$ MOLS of order 4 and $q_2 = 6$ MOLS of order 7, an application of Theorem 5.1 shows that there exists a pair of orthogonal Latin squares of order 22, or equivalently, an Eulerian square of order 22.

In the same year, Parker (1959b) proved the following result.

Theorem 5.2. *There exists an Eulerian square of order $s = (3q-1)/2$, where $q = 3 \pmod 4$ is a prime or a prime power > 3.*

Parker's method fails for $q = 3$. For $q = 7$, one obtains a pair of orthogonal Latin squares of order 10, or an Eulerian square of order 10. This square is shown below.

00	47	18	76	29	93	85	34	61	52
86	11	57	28	70	39	94	45	02	63
95	80	22	67	38	71	49	56	13	04
59	96	81	33	07	48	72	60	24	15
73	69	90	82	44	17	58	01	35	26
68	74	09	91	83	55	27	12	46	30
37	08	75	19	92	84	66	23	50	41
14	25	36	40	51	62	03	77	88	99
21	32	43	54	65	06	10	89	97	78
42	53	64	05	16	20	31	98	79	87

Once Eulerian squares of orders 10 and 22 were found, more doubts about the validity of Euler's conjecture arose as both 10 and 22 are congruent to 2 mod 4. The result in Theorem 5.1, which may be viewed as a generalization of Theorem 4.1, was further strengthened by Bose and Shrikhande (1960), again using pairwise balanced designs of index unity. Consider a pairwise balanced design d of index unity and of the type $(v; k_1, k_2, \ldots, k_m)$ and as before, for $1 \leq i \leq m$, let b_i be the number of blocks in d which are of size k_i. Let d_i, $1 \leq i \leq m$, be the subdesign of d consisting of the b_i blocks of size k_i each. Then, d_i, $1 \leq i \leq m$, is called the ith *equiblock component* of d. A subset of blocks belonging to any equiblock component d_i is said to be of type I if every treatment occurs in the subset exactly k_i times. A subset of blocks belonging to any equiblock component d_i is said to be of type II if every treatment occurs in the subset exactly once. The component d_i is said to be *separable* if the blocks can be divided into subsets of type I or type II. The design d is called separable if each equiblock component d_i is separable. Bose and Shrikhande (1960) proved the following result.

Theorem 5.3. *Let there exist a pairwise balanced design d of index unity and type $(v; k_1, \ldots, k_m)$ and suppose there exist $q_i - 1$ MOLS of order k_i. If*

$$q = min\{q_1, q_2, \ldots, q_m\}$$

then there exist at least $q - 2$ MOLS of order v. Furthermore, if d is separable, then the number of MOLS of order v is at least $q - 1$.

Numerous applications of Theorem 5.3 were made by Bose and Shrikhande (1960) to obtain sets of MOLS. In particular, they proved the following result.

Theorem 5.4. *There exist at least two orthogonal Latin squares of order $s = 36m + 22$, where $m \geq 0$ is an integer.*

Theorem 5.4 shows the falsity of the Euler's conjecture for infinitely many values of $s \equiv 2 \pmod 4$, $s \geq 22$.

That the Euler's conjecture is false for *all* orders $s = 4t+2$, $t > 1$ was shown by Bose, Shrikhande and Parker (1960). Their method consisted of finding an appropriate pairwise balanced design of index unity. Recall the definition of equiblock components of a pairwise balanced design of index unity. A set of equiblock components $d_1, d_2, \ldots, d_l$, $l < m$, is said to be a *clear* set if any pair of blocks among the $\sum_{i=1}^{l} b_i$ blocks comprising $d_1, \ldots, d_l$ are disjoint. The main result of Bose, Shrikhande and Parker (1960) can now be stated.

Theorem 5.5. *Let there exist a pairwise balanced design d of index unity and type $(v; k_1, k_2, \ldots, k_m)$ such that the equiblock components $d_1, d_2, \ldots, d_l$, $l < m$, is a clear set. If there exists a set of $q_i - 1$ MOLS of order k_i, $1 \leq i \leq m$, and if $q^* = min\{q_1 + 1, \ldots, q_l + 1, q_{l+1}, \ldots, q_m\}$, then there exist at least $q^* - 2$ MOLS of order v.*

Bose, Shrikhande and Parker (1960) then gave methods of construction of pairwise balanced designs of the type demanded in Theorem 5.5 using BIB designs with $\lambda = 1$, resolvable BIB designs and *group divisible* (GD) designs. An arrangement of $v = lm$ treatments and b blocks, each containing k distinct treatments, $(2 \leq k < v)$, is said to be a GD design if the treatments can be grouped into l groups of m treatments each, such that any two treatments of the same group appear together in λ_1 blocks and any pair of treatments belonging to different groups appear together in λ_2 blocks. In the context of orthogonal Latin squares, GD designs with $\lambda_1 = 0, \lambda_2 = 1$ play a special role as, these can be used to obtain pairwise balanced designs required in Theorem 5.5. A group divisible design is denoted by $GD(v; k, m; \lambda_1, \lambda_2)$. Let r denote the common replication of a treatment in a GD design. GD designs can be classified into three sub-classes: (i) singular, if $r - \lambda_1 = 0$; (ii) semi-regular, if $r - \lambda_1 > 0$, $rk - v\lambda_2 = 0$; (iii) regular, if $r - \lambda_1 > 0$, $rk - v\lambda_2 > 0$.

We first consider an application of Theorem 5.5. Consider a BIB design with $\lambda = 1$, which we shall denote by BIB(v, k). If we delete any three treatments, say $\alpha_1, \alpha_2, \alpha_3$ not occurring in the same block of a BIB(v, k), we get a pairwise balanced design d of index unity and type $(v - 3; k, k - 1, k - 2)$. Since in a BIB(v, k), no pair of blocks has more than one treatment in common, the three blocks of d obtained by deleting (α_1, α_2), (α_1, α_3) and (α_2, α_3) have no treatment in common and thus form a clear equiblock component. Hence, we get the following result.

Theorem 5.6. *The existence of a BIB(v, k) implies that*

$$N(v - 3) \geq min\{N(k), N(k - 1), N(k - 2) + 1\} - 1.$$

As an application of Theorem 5.6, consider BIB(v, k) designs with $k = 5$ and $v = 21, 25, 41, 45, 61, 65, 85, 125$, all of which do exist. By invoking Theorem 5.6, we see that there there exist at least two MOLS of each of the following orders: 18, 22, 38, 42, 58, 62, 82 and 122.

Using a resolvable $GD(km; k, m; 0, 1)$ design, Bose, Shrikhande and Parker (1960) proved the following result.

Theorem 5.7. *If* $k \leq N(m) + 1$, *then*
(i) $N(km + 1) \geq min\{N(k), N(k + 1), N(m) + 1\} - 1$,
(ii) $N(km + x) \geq min\{N(k), N(k + 1), N(m) + 1, N(x) + 1\} - 1$ *if* $1 < x < m$.

Towards proving the falsity of Euler's conjecture for all orders $s \equiv 2 \pmod 4$, $s > 6$, Bose, Shrikhande and Parker (1960) first proved the following result.

Lemma 5.2. *There exist at least two MOLS of order* $s \equiv 2 \pmod 4$ *if* $6 < s \leq 726$.

Proof. Bose, Shrikhande and Parker (1960) first showed that there exist at least two MOLS of order s, where $10 \leq s \leq 154$, $s \equiv 2 \pmod 4$, by improving upon the lower bounds on $N(s)$ given by Bose and Shrikhande (1960). Any integer lying in the closed interval $I_i = [a_i, b_i]$ shown in the following table can be expressed in the form

$$s = 4m_i + x_i, \ 10 \leq x_i \leq c_i,$$

where m_i and c_i are as given in the following table (*cf.* Bose, Shrikhande and Parker, 1960).

i	$I_i[a_i, b_i]$	m_i	c_i
1	[158, 182]	37	34
2	[186, 218]	44	42
3	[222, 262]	53	50
4	[266, 310]	64	54
5	[314, 374]	76	70
6	[378, 454]	92	86
7	[458, 550]	112	102
8	[554, 662]	136	118
9	[666, 726]	164	70

It is easily seen that $N(m_i) \geq n(m_i) \geq 3$. Also, $N(x_i) \geq 2$, since $10 \leq x_i \leq c_i < 154$. If we take $k = 4$ in part (ii) of Theorem 5.7, the conditions $k \leq N(m_i) + 1$ and $1 < x_i < m_i$ are satisfied. Hence, if s lies in any of the closed

intervals I_i $(1 \leq i \leq 9)$, $N(s) \geq 2$. The proof is completed by noting that any $s \equiv 2 \pmod 4$ satisfying $154 < s \leq 726$ lies in one of the intervals I_i. □

The following is the final result due to Bose, Shrikhande and Parker (1960), proving the falsity of Euler's conjecture.

Theorem 5.8. *There exists at least two MOLS of side $s > 2$, $s \neq 6$.*

Proof. If $s \equiv 0 \pmod 4$ or s is odd, then $N(s) \geq 2$, as shown by Euler (1782). In view of Lemma 5.2, it thus suffices to prove the result for orders $s \equiv 2 \pmod 4$, $s \geq 730$. If s satisfies these conditions, one can write

$$s - 10 = 144g + 4u,\ g \geq 5,\ 0 \leq u \leq 35,$$

so that $s = 4(36g) + 4u + 10$. In the prime power decomposition of $36g$, the least factor is greater than or equal to 4, and thus, $N(36g) \geq 3$. If in part (ii) of Theorem 5.7, we take $k = 4, m = 36g, x = 4u + 10$, then $k \leq 1 + N(m)$. Also, $10 \leq x \leq 150, m \geq 180$. Hence $1 < x < m$ and $N(x) \geq 2$. It follows now that $N(s) \geq 2$. □

We conclude this section by noting that using universal algebra, T. Evans (1982) showed that there are an infinite number of values of $s \equiv 2 \pmod 4$ for which there exists an Eulerian square of order $s > 6$.

6. Historical Notes

The literature on Latin squares is at least three centuries old, one of the earliest references being a monograph *Koo-Soo-Ryak* by Choi Seok-Jeong (1646–1715), who used orthogonal Latin squares of order 9 to construct a magic square and stated that he cannot find orthogonal Latin squares of order 10.

Recall that a (traditional) *magic square* of order $n \geq 2$ with magic constant $e = n(n^2 + 1)/2$ is an $n \times n$ matrix $A = (a_{ij})$ with entries $1, 2, \ldots, n^2$, such that:

(i) $\sum_{i=1}^{n} a_{ij} = e, 1 \leq j \leq n$,
(ii) $\sum_{j=1}^{n} a_{ij} = e, 1 \leq i \leq n$,
(iii) $\sum_{i=1}^{n} a_{ii} = e$, and,
(iv) $\sum_{i=1}^{n} a_{i,(n-i+1)} = e$.

As noted by I. Anderson, C. J. Colbourn, J. H. Dinitz and T. S. Griggs (2007), Latin square amulets go back to medieval Islam (c1200). A magic square of the famous Arab sufi, Ahmad ibn Ali ibn Yusuf al-Buni indicates the knowledge of a pair of orthogonal Latin squares of order 4. A new edition of J. Ozanam's four-volume treatise "Récréations mathématiques et physiques ...", published in 1723 had the following puzzle:

"There are 16 playing cards of four denominations, ace, king, queen and jack from each of the four suits, spade, heart, diamond and club. Is it possible to arrange these 16 cards in a 4×4 square such that each denomination and each suit appears in each row, each column and (additionally) on the two diagonals exactly once?"

It can be verified easily that the Eulerian square of order 4 given in Section 2 provides a solution to the above puzzle. Thus, there is evidence of the existence of Eulerian squares much before Euler!

Euler's interest in this area also probably originated from the connection of Eulerian squares to magic squares. Euler, in a paper entitled "De quadratis magicis" and read before the Academy of Sciences at St. Petersburg on October 17, 1776, constructed magic squares of orders 3, 4 and 5 from orthogonal Latin squares. He could not construct an Eulerian square of order 6 which prompted him to make his conjecture. For over a century, no progress was made on this problem, though it was not totally neglected by mathematicians of that time. In 1842, C. F. Gauss and H. C. Schumacher corresponded about a work of T. Clausen, who apparently established the impossibility of an Eulerian square when $s = 6$ and conjectured the impossibility when $s = 2 \pmod 4$. This work unfortunately was never published!

In 1896, E. H. Moore published a very influential paper "Tactical Memoranda I–III" in the American Journal of Mathematics. In Memorandum II of this paper, Moore used finite fields of order s to construct a complete set of MOLS of order s, a result rediscovered subsequently by Bose (1938) and independently by Stevens (1939). Moore also proved that if there exist t MOLS of order m and of order n, then there exist t MOLS of order mn, a fact established later by MacNeish (1922) also. MacNeish, Bose, Stevens were all apparently unaware of the contribution of Moore.

The final results of Bose, Shrikhande and Parker on the falsity of Euler's conjecture for all orders $s \equiv 2 \pmod 4$, $s > 6$, were announced in the annual meeting of the American Mathematical Society, held in New York during the last week of April, 1959. This major result was reported on the front page of the Sunday edition of the New York Times of April 26, 1959. Since then the trio Bose-Shrikhande-Parker became known as "Euler's Spoilers"!

Acknowledgment

This work was supported by the Indian National Science Academy under the Senior Scientist scheme of the Academy. The support is gratefully acknowledged.

References

Anderson, I., C. J. Colbourn, J. H. Dinitz and T. S. Griggs (2007). Design theory: Antiquity to 1950. In: *Handbook of Combinatorial Designs*, 2nd. ed. (C. J. Colbourn and J. H. Dinitz, Eds.). New York: Chapman and Hall/CRC, pp. 11–22.

Bose, R. C. (1938). On the application of the properties of Galois fields to the problem of construction of hyper-Greaco-latin squares. *Sankhyā* **3**, 323–338.

Bose, R. C. and S. S. Shrikhande (1959). On the falsity of Euler's conjecture about the non-existence of two orthogonal latin squares of order 4t+2. *Proc. Natl. Acad. Sci. U. S. A.* **45**, 734–737.

Bose, R. C. and S. S. Shrikhande (1960). On the construction of sets of mutually orthogonal latin squares and the falsity of a conjecture of Euler. *Trans. Amer. Math. Soc.* **95**, 191–209.

Bose, R. C., S. S. Shrikhande and E. T. Parker (1960). Further results on the constructon of mutually orthogonal latin squares and the falsity of Euler's conjecture. *Can. J. Math.* **12**, 189–203.

Bruck, R. H. and H. J. Ryser (1949). The nonexistence of certain finite projective planes. *Can. J. Math.* **1**, 88–93.

Chowla, S. and H. J. Ryser (1950). Combinatorial problems. *Can. J. Math.* **2**, 93–99.

Dénes, J. and A. D. Keedwell (1974). *Latin Squares and Their Applications.* New York: Academic Press.

Dénes, J. and A. D. Keedwell (eds.) (1991). *Latin Squares: New Developments in the Theory and Applications.* Amsterdam: North-Holland. Annals of Discrete Mathematics **46**.

Euler, L. (1782). Recherches sur une nouvelle espece de quarrés magiques. *Verh. Zeeuw. Gen. Weten. Vlissengen* **9**, 85–239.

Evans, T. (1982). Universal algebra and Euler's officer problem. *Amer. Math. Monthly* **86**, 466–479.

Fisher, R. A. and F. Yates (1934). The 6 × 6 Latin squares. *J. Cambridge Phil. Soc.* **30**, 492–507.

Lam, C. W. H., L. H. Thiel and S. Swiercz (1989). The nonexistence of finite projective planes of order 10. *Can. J. Math.* **41**, 1117–1123.

Laywine, C. F. and G. L. Mullen (1998). *Discrete Mathematics Using Latin Squares.* New York: Wiley.

Levi, F. W. (1942). *Finite Geometrical Systems.* University of Calcutta.

MacNeish, H. F. (1921). Das problem der 36 offiziere. *Ber. Deuts. Mat. Ver.* **30**, 151–153.

MacNeish, H. F. (1922). Euler squares. *Ann. Math.* **23**, 221–227.

Mann, H. B. (1942). The construction of orthogonal latin squares. *Ann. Math. Statist.* **13**, 418–423.

Mann, H. B. (1949). *Analysis and Design of Experiments.* New York: Dover.

Moore, E. H. (1896). Tactical memoranda I–III. *Amer. J. Math.* **18**, 264–303.

Nazarok, A. V. (1991). Five pairwise orthogonal latin squares of order 21. *Issled. Oper. ASU*, 54–56.

Ozanam, J. (1723). *Récréations Mathématiques et Physiques, qui contiennent Plusieurs Problémes utiles & agréables, d'Arithmetique, de Geometrie, d'Optique, de Gnomonique, de Cosmographie, de Mécanique, de Pyrotechnie, & de Physique.* 4 Vols. Paris: Jombert (updated edition).

Parker, E. T. (1959a). Construction of some sets of pairwise orthogonal Latin squares. *Proc. Amer. Math. Soc.* **10**, 946–951.

Parker, E. T. (1959b). Orthogonal latin squares. *Proc. Natl. Acad. Sci. U. S. A.* **45**, 859–862.

Peterson, J. (1901). Les 36 officieurs. *Ann. Math.* **1**, 413–427.

Shrikhande, S. S. (1950). The impossibility of certain symmetrical balanced incomplete block designs. *Ann. Math. Statist.* **21**, 106–111.

Stevens, W. L. (1939). The completely orthogonalised Latin squares. *Ann. Eugen.* **9**, 82–93.

Stinson, D. R. (1984). A short proof of the nonexistence of a pair of orthogonal Latin squares of order six. *J. Combin. Theor. Ser. A* **36**, 373–376.

Tarry, G. (1900). Le probléme des 36 officers. *Comptes Rendus de l'Association Francaise pour l'Avancement des Sciences: Série de mathématiques, astronomie, géodésie et mécanique* **29**, 170–203.

Wernicke, P. (1910). Das problem der 36 offiziere. *Deutsche Math.-Ver.* **19**, 264–267.