8

Latin Squares

8.1 Latin Rectangles

Let S be a finite set with n elements. A *latin rectangle* based on S is an r by s matrix

$$A = [a_{ij}], \quad (i = 1, 2, \ldots, r; j = 1, 2, \ldots, s)$$

with the property that each row and each column of A contain distinct elements of S. The number r of rows and the number s of columns of the latin rectangle A satisfy $r \leq n$ and $s \leq n$. Usually the set S is chosen to be the set $\{1, 2, \ldots, n\}$ consisting of the first n positive integers. The matrix

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

is a 3 by 5 latin rectangle based on $\{1, 2, 3, 4, 5\}$. If $s = n$, as it does in this example, then each row of the latin rectangle A contains a permutation of S and these permutations have the property that no column contains a repeated element. If the first row contains the permutation $(1, 2, \ldots, n)$, then the r by n latin rectangle is called *normalized.* An n by n latin rectangle based on the set S of n elements is a *latin square* of order n. Thus in a latin square each row and each column contains a permutation of S. The elements of S can always be labeled to normalize a latin square.

Let G be a group of order n whose set of elements in some order is $a_1, a_2, \ldots, a_n$, and let the binary operation of G be denoted by $*$. A *Cayley table* of G is the matrix $A = [a_{ij}]$ of order n in which

$$a_{ij} = a_i * a_j, \quad (i, j = 1, 2, \ldots, n).$$

The axioms for a group imply that A is a latin square of order n based on the set $\{a_1, a_2, \ldots, a_n\}$. Cyclic groups of order n give particularly simple examples of latin squares of order n. If P is a permutation matrix of order n, then PAP^T is also a Cayley table of G. If a_1 is the identity element of G, then the first row of A contains the permutation $a_1, a_2, \ldots, a_n$. Let P and Q be permutation matrices of order n. It is common to also call PAQ a Cayley table for G. Not every latin square is a Cayley table of a group because the axiom of associativity for a group imposes a further restriction on a Cayley table of a group. The algebraic systems whose Cayley tables are latin squares are called *quasigroups*. A Cayley table of a commutative group (or commutative quasigroup) is a symmetric latin square.

Let A be a latin square of order n based on $\{1, 2, \ldots, n\}$. Let P_i be the (0,1)-matrix of order n whose 1's are in those positions which in A are occupied by i. Then P_i is a permutation matrix of order $n, (i = 1, 2, \ldots, n)$. Moreover,

$$J_n = P_1 + P_2 + \cdots + P_n \tag{8.1}$$

and

$$A = 1P_1 + 2P_2 + \cdots + nP_n \tag{8.2}$$

are decompositions of the all 1's matrix J_n and A, respectively. Conversely, if (8.1) is a decomposition of J_n into n permutation matrices, then (8.2) defines a latin square A.

The matrix J_n is the reduced adjacency matrix of the complete bipartite graph $K_{n,n}$. The latin square A assigns a color from the color set $\{1, 2, \ldots, n\}$ to each of the edges of $K_{n,n}$ in such a way that adjacent edges are assigned different colors. Thus the set M_i of edges of color i is a perfect matching of $K_{n,n}$. The permutation matrix P_i is the reduced adjacency matrix of the spanning bipartite subgraph of $K_{n,n}$ whose set of edges is M_i. Conversely, an assignment of a color from the color set $\{1, 2, \ldots, n\}$ to each of the edges of $K_{n,n}$ produces a latin square of order n provided adjacent edges are assigned different colors.

Let $A = [a_{ij}]$ be a latin square of order n based on a set S. A *partial transversal* of size t of A is a set of t positions such that no two of the positions are on the same line and these positions are occupied in A by distinct elements. A *transversal* of A is a partial transversal of size n. Thus a transversal is a set of positions

$$\{(1, \sigma(1)), (2, \sigma(2)), \ldots, (n, \sigma(n))\}$$

where σ is a permutation of $\{1, 2, \ldots, n\}$ and

$$\{a_{1\sigma(1)}, a_{2\sigma(2)}, \ldots, a_{n\sigma(n)}\} = S.$$

Transversals are also known as *complete mappings* of quasigroups.

In terms of the decompositions (8.1) and (8.2) a transversal of A can be viewed as a permutation matrix Q of order n which for each $i = 1, 2, \ldots, n$ has exactly one 1 in common with P_i. Thus in a coloring of the edges of the complete bipartite graph $K_{n,n}$ with n colors, a transversal corresponds to a perfect matching with all edges colored differently.

Let A be a Cayley table for a group of odd order n with elements $a_1, a_2, \ldots, a_n$. Then each element of G has a unique square root and thus $\{a_1^2, a_2^2, \ldots, a_n^2\} = \{a_1, a_2, \ldots, a_n\}$. Hence the set of positions of the main diagonal is a transversal of A. A group of even order need not have a transversal as the group of order 2 shows. Conditions for the existence and the nonexistence of transversals in Cayley tables of groups of even order are discussed in Dénes and Keedwell[1974].

Let $A = [a_{ij}]$ be a latin square of order n based on the set $\{1, 2, \ldots, n\}$. A matrix obtained from A by row permutations and by column permutations is also a latin square as is the transposed matrix A^T. We may also apply a permutation to the elements of the set $\{1, 2, \ldots, n\}$ and obtain a latin square. There is one further basic transformation of latin squares which is less obvious and which we now discuss. To the latin square A of order n there corresponds a three-dimensional array

$$C = [c_{ijk}], \quad (i, j, k = 1, 2, \ldots, n) \tag{8.3}$$

of 0's and 1's in which $c_{ijk} = 1$ if and only if $a_{ij} = k$. A *line* of the array C is a set of positions (i, j, k) obtained by fixing two of $i, j,$ and k and allowing the other index to vary from 1 to n. The array C obtained from the latin square of order n has the property that each line contains exactly one 1. Such an array is a 3-*dimensional line permutation matrix* of order n. Conversely, from a 3-dimensional line permutation matrix $C = [c_{ijk}]$ of order n one obtains a latin square $A = [a_{ij}]$ of order n by defining $a_{ij} = k$ if $c_{ijk} = 1$.

Let C be the 3-dimensional line permutation matrix of order n corresponding to the latin square A. Let (p, q, r) be a permutation of the three indices i, j and k of C and let $C_{(p,q,r)}$ be the 3-dimensional matrix obtained from C by taking the indices in the order p, q, r. Thus, for instance, $C_{(3,1,2)} = [x_{ijk}]$ where $x_{ijk} = c_{kij}$ for i, j and k between 1 and n. The matrix $C_{(p,q,r)}$ is a 3-dimensional line permutation matrix of order n and thus there corresponds a latin square $A_{(p,q,r)}$ of order n. We have $A_{(1,2,3)} = A$ and $A_{(2,1,3)} = A^T$. The latin square $A_{(3,2,1)}$ is the latin square obtained from A by interchanging row indices with elements. The (i, j)-entry of $A_{(3,1,2)}$ is k provided $a_{kj} = i$. Similarly, $A_{(1,3,2)}$ is the latin square obtained from A by interchanging column indices with elements. For example, let

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 4 & 1 & 3 \end{bmatrix}. \tag{8.4}$$

Then

$$A_{(3,2,1)} = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

and

$$A_{(1,3,2)} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 4 & 3 & 2 & 1 \\ 3 & 1 & 4 & 2 \end{bmatrix}.$$

Two latin squares A and B of order n based on $\{1, 2, \ldots, n\}$ are *equivalent* provided there is a permutation (p, q, r) of $\{1, 2, 3\}$ such that B can be obtained from $A_{(p,q,r)}$ by permutation of its rows, columns and elements. Any two latin squares of order 3 are equivalent. A latin square of order 4 is equivalent to one of the two latin squares

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}. \tag{8.5}$$

The first of these latin squares C has the property that $C_{(p,q,r)} = C$ for each permutation (p, q, r) of $\{1, 2, 3\}$. More generally, let G be an elementary abelian 2-group with elements $\{a_1, a_2, \ldots, a_n\}$ where a_1 is the identity element. The Cayley table C of G has the property that $C_{(p,q,r)} = C$ for each permutation (p, q, r) of $\{1, 2, 3\}$.

Higher dimensional latin configurations are discussed by Jurkat and Ryser[1968].

Exercises

1. Find an example of a latin square A such that for no permutation matrices P and Q is PAQ a Cayley table of a group.
2. Find an example of a group of even order $n > 2$ whose Cayley table does not have a transversal.
3. Prove that all latin squares of order 3 are equivalent. Also prove that a latin square of order 4 is equivalent to one of the two latin squares given in (8.5).
4. Construct a Cayley table for the group of permutations of $\{1, 2, 3\}$ and obtain a latin square of order 6.
5. Let A be the latin square given in (8.4). Construct all the latin squares $A_{(p,q,r)}$.

References

J. Dénes and A.D. Keedwell[1974], *Latin Squares and Their Applications*, Academic Press, New York.

M. Hall, Jr.[1986], *Combinatorial Theory*, 2d edition, Wiley, New York.

W.B. Jurkat and H.J. Ryser[1968], Extremal configurations and decomposition theorems, *J. Algebra*, 8, pp. 194–222.

H.J. Ryser[1963], *Combinatorial Mathematics*, Carus Mathematical Monograph No. 14, Math. Assoc. of America, Washington, D.C.

8.2 Partial Transversals

Let $A = [a_{ij}]$ be a latin square of order n. If A has a transversal then each latin square equivalent to A also has a transversal. The following theorem of Mann[1942] shows in particular that a Cayley table of a cyclic group of even order (a circulant matrix of even order) does not have a transversal.

Theorem 8.2.1. *A Cayley table of an abelian group of even order with a unique element of order two does not have a transversal.*

Proof. Let n be an even integer and let G be an abelian group with elements $a_1, a_2, \ldots, a_n$. Assume that G has a unique element x of order 2. We have $x = a_1 * a_2 * \cdots * a_n$. Let $A = [a_{ij}]$ be the Cayley table of G in which $a_{ij} = a_i * a_j, (i, j = 1, 2, \ldots, n)$. Suppose that A has a transversal. Then there exists a permutation $(j_1, j_2, \ldots, j_n)$ of $\{1, 2, \ldots, n\}$ such that

$$\{a_1, a_2, \ldots, a_n\} = \{a_1 * a_{j_1}, a_2 * a_{j_2}, \ldots, a_n * a_{j_n}\}.$$

Since G is abelian, we obtain

$$\begin{aligned} x &= (a_1 * a_{j_1}) * (a_2 * a_{j_2}) * \cdots * (a_n * a_{j_n}) \\ &= (a_1 * a_2 * \cdots a_n) * (a_{j_1} * a_{j_2} * \cdots * a_{j_n}) = x * x, \end{aligned}$$

and this contradicts the fact that x has order 2. Therefore A does not have a transversal. □

As noted in the previous section a Cayley table of a group of odd order always has a transversal. It has been proved by Paige[1947] that a Cayley table of an abelian group G of even order n has a transversal if G does not have a unique element of order two. Thus *a Cayley table of an abelian group of even order has a transversal if and only if it does not have a unique element of order two.* We now state without proof a more general theorem of Hall[1952].

Theorem 8.2.2. *Let G be an abelian group with elements $a_1, a_2, \ldots, a_n$ and let A be a Cayley table of G. Let $k_1, k_2, \ldots, k_n$ be a sequence of non-negative integers with $k_1 + k_2 + \cdots + k_n = n$. Then there exists in A n*

positions no two on the same line such that in these positions a_i occurs exactly k_i times if and only if $a_1^{k_1} * a_2^{k_2} * \cdots * a_n^{k_n}$ is the identity element of G.

If $k_1 = k_2 = \cdots = k_n = 1$, then Theorem 8.2.2 asserts that A has a transversal if and only if

$$a_1 * a_2 * \cdots * a_n = 1, \tag{8.6}$$

the identity element of G. If G has odd order, (8.6) is satisfied. If G has even order, (8.6) is satisfied if and only if G has more than one element of order two.

It has been conjectured by Ryser[1967] that every latin square of odd order n has a transversal and by Brualdi (see Dénes and Keedwell[1974]) that every latin square of even order n has a partial transversal of size $n-1$. These conjectures remain unsettled (see Erdös et al.[1988]). The remainder of this section concerns the progress that has been made toward the resolution of these conjectures. First we remark that Theorem 8.2.2 implies at once that the Cayley table of an abelian group of order n has a partial transversal of size $n-1$ containing any specified subset of $n-1$ elements of G.

Let A be a matrix of order n whose elements come from a set S. A *weak transversal* of A is a set W of n positions of A no two from the same line with the property that each element of S occurs at most twice in the positions of W.

Theorem 8.2.3. *A matrix of order n with no repeated element in a row or in a column has a weak transversal. In particular, a latin square of order n has a weak transversal.*

Proof. We prove the theorem by induction on n. If $n = 1$ the conclusion is trivial. Suppose that $n > 1$ and let A be a matrix of order n such that each row and each column contains distinct elements. Let A' be the matrix obtained from A by deleting the first row and the first column. By the inductive hypothesis A' has a weak transversal. Without loss of generality we assume that the $n-1$ diagonal positions of A' form a weak transversal, and that the elements in these positions are $1, 1, 2, 2, \ldots, r, r, r+1, r+2, \ldots, r+s$ where $2r+s = n-1$. If the element in position (1,1) does not equal any of $1, 2, \ldots, r$, then the n diagonal positions of A form a weak transversal. Otherwise we assume without loss of generality that 1 is in position (1,1). Because row 1 of A contains distinct elements, row 1 contains $r+1$ distinct elements $x_1, x_2, \ldots, x_r$ each of which is different from $1, 2, \ldots, r$. Because column 1 has distinct elements, there is an element x_i in row 1 such that the element y in column 1 which is symmetrically opposite x_i is different from $1, 2, \ldots, r$. Let this x_i and

y occupy positions $(1,k)$ and $(k,1)$, respectively. The set of n positions

$$\{(i,i) : i \neq 1,k\} \cup \{(1,k),(k,1)\}$$

is a weak transversal of A. □

It is an immediate consequence of Theorem 8.2.3 that a latin square of order n has a partial transversal of size $\lceil n/2 \rceil$. Koksma[1969] proved that for $n \geq 3$ there is a partial transversal of size at least $\lceil (2n+1)/3 \rceil$. Koksma's method was refined by de Vries and Wieringa[1978] who obtained the lower bound of $\lceil (4n-3)/5 \rceil$ for the size of a partial transversal of a latin square of order n if $n \geq 12$. Woolbright[1978] and independently Brouwer, de Vries and Wieringa[1978] showed that a latin square of order n has a partial transversal of size at least $\lceil n - \sqrt{n} \rceil$. We rely on the proof of Brouwer et al.

Theorem 8.2.4. *A latin square of order n has a partial transversal of size t for some t satisfying the inequality $(n-t)(n-t+1) \leq n$.*

Proof. Let $A = [a_{ij}]$ be a latin square of order n based on $\{1,2,\ldots,n\}$ and let t be the largest size of a partial transversal of A. Without loss of generality we assume that $T = \{(1,1),(2,2),\ldots,(t,t)\}$ is a partial transversal of A and that $a_{kk} = k, (k = 1,2,\ldots,t)$. Let $r = n - t$ and let $R = \{t+1, t+2, \ldots, n\}$. We inductively define subsets $W_0, W_1, \ldots, W_r$ of $\{1,\ldots,n\}$ as follows:

$$W_0 = \emptyset,$$

$$W_i = \{j : a_{j,t+i} \in W_{i-1} \cup R\}, \quad (i = 1,2,\ldots,r).$$

Let

$$V_i = \{(j, t+i) : j \in W_i\}, \quad (i = 1,2,\ldots,r)$$

and let

$$V = V_1 \cup V_2 \cup \cdots \cup V_r.$$

We define a digraph D with vertex set V by putting an arc from $(j,t+i)$ to $(k,t+l)$ if and only if $i < l$ and $j = a_{k,t+l}$.

Suppose that in D there is a path from a vertex $(j,t+i)$ to a vertex $(k,t+l)$ such that $a_{j,t+i} \in R$ and $k \in R$. Let

$$(j,t+i) = (j_0, t+i_0) \to (j_1, t+i_1) \to \cdots \to (j_p, t+i_p) = (k, t+l)$$

be such a path γ of smallest length. This path is pictured schematically in Figure 8.1, in which u denotes an element of R.

Let

$$T' = (T - \{(j_0,j_0),\ldots,(j_{p-1},j_{p-1})\}) \cup \{(j_0,t+i_0),(j_1,t+i_1),\ldots,(j_p,t+i_p)\}.$$

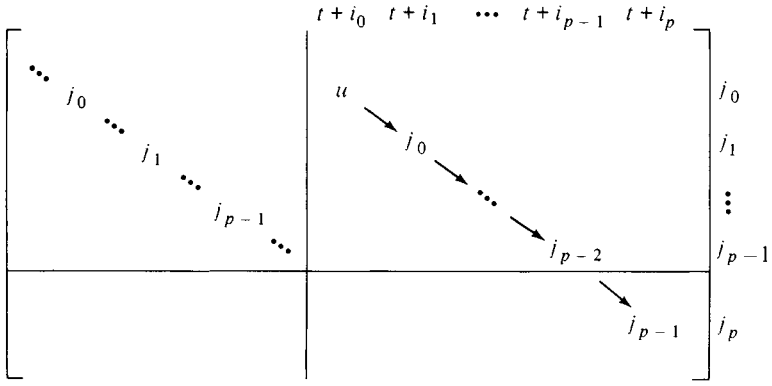

Figure 8.1

No two of the positions in T' belong to the same column. Suppose that two positions in T' belong to the same row. Then there are integers r and s with $0 \leq r < s \leq p$ and with $j_r = j_s$. If $s = p$ then $j_r = j_p = k$ and

$$(j_0, t+i_0) \to (j_1, t+i_1) \to \cdots \to (j_r, t+i_r)$$

is a path which contradicts the choice of γ. If $s < p$ then $j_r = j_s = a_{s+1,t+j_{s+1}}$ and

$$(j_0, t+i_0) \to \cdots \to (j_r, t+i_r) \to (j_{s+1}, t+j_{s+1}) \to \cdots \to (j_p, t+i_p)$$

is a path which contradicts the choice of γ. We therefore conclude that no two positions in T' belong to the same row. The elements in the $t+1$ positions of T' are the numbers $1, 2, \ldots, t$ and u. Because u is an element of R, T' is a partial transversal of size $t+1$, and this contradicts our choice of T. We now conclude that there is no path in D satisfying the conditions of the path γ. The definition of the sets W_i now implies that

$$W_0 \cup W_1 \cup \cdots \cup W_r \subseteq \{1, 2, \ldots, t\}$$

and

$$|W_i| = |W_{i-1}| + r, \quad (i = 1, 2, \ldots, r).$$

Hence $|W_r| = r^2$ and therefore

$$r^2 \leq t = n - r.$$

Because $r = n - t$ the theorem follows. □

Theorem 8.2.4 has been extended by Csima[1979] to more general combinatorial configurations. In addition Shor[1982] has shown that every latin

square of order n has a partial transversal of size at least $n - 5.53(\ell n\ n)^2$. This number is greater than $n - \sqrt{n}$ for $n \geq 2,000,000$.

As already remarked a latin square of order n corresponds to an assignment of one of n colors to each edge of the complete bipartite graph $K_{n,n}$ so that adjacent edges are assigned different colors, and a transversal corresponds to a perfect matching of n differently colored edges. Woolbright and Fu[1987] have obtained a coloring theorem for the complete graph K_{2n} with an even number $2n$ of vertices which answers a question which is analogous to the question of the existence of a transversal in a latin square. This theorem asserts the following: *Suppose that each edge of K_{2n} is assigned a color from a set of $2n-1$ colors so that adjacent edges are assigned different colors. If $n \geq 8$, then there exists a perfect matching of n differently colored edges.* In contrast to the case of bipartite graphs, not all of the colors appear as colors of the edges of the perfect matching.

Finally we remark that Ryser[1967] conjectured that the number of transversals of a latin square of order n is congruent to n modulo 2. If n is odd, then this conjecture is stronger than the conjecture that a latin square of odd order has a transversal. If n is even then the conjecture has been proved by Balasubramanian[1990], but notice that there is no implication concerning the existence of a transversal in a latin square of even order n. According to Parker [private communication], there are many latin squares of order 7, the number of whose transversals is an even positive integer. One such is

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 7 & 4 & 5 & 1 \\ 3 & 4 & 7 & 5 & 1 & 2 & 6 \\ 4 & 6 & 1 & 2 & 3 & 7 & 5 \\ 5 & 7 & 2 & 1 & 6 & 4 & 3 \\ 6 & 5 & 4 & 3 & 7 & 1 & 2 \\ 7 & 1 & 5 & 6 & 2 & 3 & 4 \end{bmatrix}.$$

Exercises

1. Let A be a latin square of order n. Let t be the maximal size of a partial transversal of A. Prove that t is the maximal size of a partial transversal of each latin square equivalent to A.
2. Prove that the condition given in Theorem 8.2.2 is a necessary condition for there to exist n positions in a Cayley table of an abelian group with the stated properties.
3. Prove that Theorem 8.2.2 implies that a Cayley table of an abelian group G has a partial transversal of size $n-1$ containing any specified subset of $n-1$ elements of G.
4. Prove that the number of transversals of a latin square of even order is an even nonnegative integer (Balasubramanian[1990]).

References

K. Balasubramanian[1990], On transversals in latin squares, *Linear Alg. Applics.*, 131, pp. 125–129.

A.E. Brouwer, A.J. de Vries and R.M.A. Wieringa[1978], A lower bound for the length of partial transversals in a latin square, *Nieuw Archief voor Wiskunde* (3), XXVI, pp. 330–332.

J. Csima[1979], On the plane term rank of three dimensional matrices, *Discrete Math.*, 28, pp. 147–152.

J. Dénes and A.D. Keedwell[1974], *Latin Squares and Their Applications*, Academic Press, New York.

P. Erdös, D.R. Hickerson, D.A. Norton and S.K. Stein[1988], Has every latin square of order n a partial transversal of size $n-1$?, *Amer. Math. Monthly*, 95, pp. 428–430.

M. Hall, Jr.[1952], A combinatorial problem on abelian groups, *Proc. Amer. Math. Soc.*, 3, pp. 584–587.

K.K. Koksma[1969], A lower bound for the order of a partial transversal, *J. Combin. Theory*, 7, pp. 94–95.

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

L.J. Paige[1947], A note on finite abelian groups, *Bull. Amer. Math. Soc.*, 53, pp. 590–593.

H.J. Ryser[1967], Neuere Probleme in der Kombinatorik (prepared by D.W. Miller), *Vorträge über Kombinatorik*, Oberwolfach, pp. 69–91.

P.W. Shor[1982], A lower bound for the length of a partial transversal in a latin square, *J. Combin. Theory, Ser. A*, 33, pp. 1–8.

A.J. de Vries and R.M.A. Wieringa, Een ondergrens voor de lengte van een partiele transversaal in een Latijns vierkant, preprint.

D.E. Woolbright[1978], An $n \times n$ latin square has a transversal with at least $n - \sqrt{n}$ distinct symbols, *J. Combin. Theory, Ser. A*, 24, pp. 235–237.

D.E. Woolbright and H.-L. Fu[1987], The rainbow theorem of 1-factorization, preprint.

8.3 Partial Latin Squares

Let S be the set $\{1, 2, \ldots, n\}$. We now consider matrices A of order n whose elements come from $S \cup \{\diamond\}$ where each occurrence of $\diamond$ is to be regarded as an unspecified element of A. Such a matrix A is called a *partial latin square* of order n provided that each element of S occurs at most once in each row and in each column. Notice that in a partial latin square there is no restriction on the number of times the symbol $\diamond$ may occur in a row or column. If each occurrence of the symbol $\diamond$ can be replaced by an element of S in such a way that the resulting matrix B is a latin square, then we say that the partial latin square A can be *completed to a latin square* and we call B a *completion* of A. A completion of A is a latin square which agrees with A in the elements specified.

Not every partial latin square of order n can be completed. Two simple

examples with n specified elements which have no completion are

$$\begin{bmatrix} 1 & \cdots & \diamond & \diamond \\ \vdots & \ddots & \vdots & \vdots \\ \diamond & \cdots & 1 & \diamond \\ \diamond & \cdots & \diamond & 2 \end{bmatrix} \tag{8.7}$$

and

$$\begin{bmatrix} 1 & 2 & \cdots & n-1 & \diamond \\ \diamond & \diamond & \cdots & \diamond & n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \diamond & \diamond & \cdots & \diamond & \diamond \end{bmatrix}. \tag{8.8}$$

There does not exist a latin square of order n which agrees with (8.7) or with (8.8). Notice that if we extend the construction for latin squares which interchanges row indices and elements so that it applies to partial latin squares, then (8.8) can be obtained from (8.7) in this way.

We now regard an r by s latin rectangle based on the set $S = \{1, 2, \ldots, n\}$ as a partial latin square of order n in which only the elements in the r by s rectangle in the upper left corner have been specified. The following theorem is from Hall[1945].

Theorem 8.3.1. *Let A be an r by n latin rectangle based on $\{1, 2, \ldots, n\}$. Then A can be completed to a latin square of order n.*

Proof. Let $C = [c_{ij}]$ be the (0,1)-matrix of order n in which $c_{ij} = 1$ if and only if the element i does not occur in column j of $A, (i, j = 1, 2, \ldots, n)$. Because A is an r by n latin rectangle each element of $\{1, 2, \ldots, n\}$ occurs once in each row of A and once in each of r different columns of A. It follows that each line sum of C equals $n - r$. We now apply Theorem 4.4.3 to C and conclude that there is a decomposition

$$C = P_1 + P_2 + \cdots + P_{n-r}$$

in which each P_i is a permutation matrix of order n. Let the 1's of P_1 occur in positions $(1, k_1), (2, k_2), \ldots, (n, k_n)$. Then $k_1, k_2, \ldots, k_n$ is a permutation of $\{1, 2, \ldots, n\}$ and we may adjoin this permutation to the r by n latin rectangle A to obtain an $r + 1$ by n latin rectangle. Repeating with $P_2, \ldots, P_{n-r}$ we obtain a latin square of order n. □

Now suppose that A is a partial latin square of order n based on $\{1, 2, \ldots, n\}$ in which each specified element lies in one of rows $1, 2, \ldots, r+1$. Suppose further that all the elements in rows $1, 2, \ldots, r$ have been specified and that exactly d elements in row $r + 1$ are specified where $1 \leq d \leq n - 1$. Then Brualdi and Csima[1986] proved that for fixed n, r and d each partial

latin square with the above properties can be completed to a latin square of order n if and only if either $d = 1, r = n - 1$ or $d \leq n - 2r$.

If $s < n$, an r by s latin rectangle A need not have a completion to a latin square of order n. For example, the 2 by 2 latin rectangle

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

based on $\{1, 2, 3\}$ has no completion to a latin square of order 3. Ryser[1951] obtained necessary and sufficient conditions in order that an r by s latin rectangle have a completion to a latin square.

Theorem 8.3.2. *Let A be an r by s latin rectangle based on $\{1, 2, \ldots, n\}$, and let $N(j)$ denote the number of times that the element j occurs in A, $(j = 1, 2, \ldots, n)$. Then A can be completed to a latin square of order n if and only if*

$$N(j) \geq r + s - n, \quad (j = 1, 2, \ldots, n). \tag{8.9}$$

Proof. First suppose that there is a latin square B of order n which is a completion of A. Let j be an element of $\{1, 2, \ldots, n\}$. Then j occurs $n - r$ times in the last $n - r$ rows of B and $n - s$ times in the last $n - s$ columns, and hence at least $n - (n - r) - (n - s) = r + s - n$ times in the upper left r by s rectangle of B. Because this r by s rectangle is A (8.9) holds.

Now suppose that (8.9) is satisfied. It suffices to show that A may be extended to an r by n latin rectangle B based on $\{1, 2, \ldots, n\}$, for then we may apply Theorem 8.3.1 to B and obtain a completion of A. Let $D = [d_{ij}]$ be the r by n (0,1)-matrix in which $d_{ij} = 1$ if and only if the element j does not occur in row i of A, $(i = 1, 2, \ldots, r; j = 1, 2, \ldots, n)$. Each row sum of D equals $n - s$. The sum of the entries in column j of D equals $r - N(j)$ which by (8.9) is at most equal to $n - s$. We now apply Theorem 4.4.3 to D and conclude that there is a decomposition

$$D = Q_1 + Q_2 + \cdots + Q_{n-s}$$

where each Q_i is an r by n subpermutation matrix. Since the number of 1's in D equals $r(n - s)$ each Q_i is a subpermutation matrix of rank r. Let the 1's of Q_i occur in positions $(1, j_{1i}), (2, j_{2i}), \ldots, (r, j_{ri})$. Then $j_{1i}, j_{2i}, \ldots, j_{ri}$ is an r-permutation of the set $\{1, 2, \ldots, n\}$. We now adjoin $j_{1i}, j_{2i}, \ldots, j_{ri}$ as a column to the r by s latin rectangle A for each $i = 1, 2, \ldots, n - s$ and obtain an r by n latin rectangle B. □

Corollary 8.3.3. *Let A be a partial latin square of order n whose specified elements all belong to the r by s rectangle L in its upper left corner. Assume that $r + s \leq n$. Then A can be completed to a latin square of order n.*

Proof. Suppose that the element in position (i, j) of A is unspecified where $1 \leq i \leq r$ and $1 \leq j \leq s$. The number of distinct integers that occur in row i or row j of A is at most $r + s - 2 \leq n - 2$. Hence there is a partial latin square of order n which can be obtained from A by specifying the element in position (i, j). Proceeding like this we conclude that there is a partial latin square B of order n which can be obtained from A by specifying all the unspecified elements in the r by s rectangle L. Because $r + s \leq n$ it now follows from Theorem 8.3.2 that B and hence A can be completed to a latin square of order n. □

When it happens that a partial latin square of order n does not have a completion to a latin square of order n, there are two natural ways to proceed. One is to embed the partial latin square in a latin square of larger order. The other is to partition the partial latin square into parts each of which has a completion to a latin square of order n. The next two theorems address these two possibilities. The first is due to Evans[1960] and the second is due to Opencomb[1984].

Theorem 8.3.4. *Let A be a partial latin square of order n. Then there is a latin square of order $2n$ which contains A in its upper left corner.*

Proof. We enlarge A to a partial latin square of order $2n$ in which all of the specified elements belong to the upper left n by n rectangle and then apply Corollary 8.3.3. □

Theorem 8.3.5. *Let $A = [a_{ij}]$ be a partial latin square of order n. Then there exist four latin squares B_1, B_2, B_3 and B_4 of order n such that for each specified element a_{ij} of A at least one of B_1, B_2, B_3 and B_4 has the property that the element in position (i, j) equals a_{ij}.*

Proof. First suppose that n is even, and let

$$A = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}$$

be a partition of A into four submatrices of order $n/2$. Let A_i' be the partial latin square of order n which is obtained from A by replacing all specified elements in A_1, A_2, A_3 and A_4 with $\diamond$ except for those specified in $A_i, (i = 1, 2, 3, 4)$. By Corollary 8.3.3 each A_i' can be completed to a latin square of order n.

Now assume that $n = 2m + 1$ is odd. If every element of A is specified then we let $B_1 = A$ and let B_2, B_3 and B_4 be arbitrary latin squares of order n. Now suppose that some element of A is unspecified. Without loss of generality we assume that the element in position $(m + 1, m + 1)$ is not specified. Except for this position, A can be partitioned into four submatrices A_1, A_2, A_3 and A_4 of sizes m by $m + 1$, $m + 1$ by m, m by

$m+1$ and $m+1$ by m, respectively. By Corollary 8.3.3 each A_i can be completed to a latin square of order n. □

It has been conjectured by Daykin and Häggvist[1981] that a partial latin square of order n can always be partitioned into two parts each of which can be completed to a latin square of order n.

The partial latin squares (8.7) and (8.8) of order n have n specified elements and cannot be completed to a latin square of order n. Evans[1960] conjectured that a partial latin square of order n with at most $n-1$ specified elements can always be completed to a latin square of order n. Häggvist[1976] proved this conjecture provided $n \geq 1111$. The conjecture was proved in its entirety by Smetaniuk[1981] and Anderson and Hilton[1983]. The remainder of this section is devoted primarily to Smetaniuk's proof of the conjecture of Evans.

First we make the following definition. Let X be a matrix of order m. The set $\{(1,m),(2,m-1),\ldots,(m,1)\}$ of positions of X is called the *back diagonal* of X. Now let A be a latin square of order n based on the set $\{1,2,\ldots,n\}$. We define a partial latin square $P(A)$ of order $n+1$ based on $\{1,2,\ldots,n+1\}$ as follows. The elements on the back diagonal of $P(A)$ are all equal to $n+1$. The triangular part of $P(A)$ *above* its back diagonal is the same as the triangular part of A on and above its back diagonal. All elements of $P(A)$ below its back diagonal are equal to $\diamond$ and thus are unspecified. For example, if

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix},$$

then

$$P(A) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & \diamond \\ 2 & 4 & \diamond & \diamond \\ 4 & \diamond & \diamond & \diamond \end{bmatrix}.$$

Theorem 8.3.6. *Let $A = [a_{ij}]$ be a latin square of order n based on $\{1,2,\ldots,n\}$. Then the partial latin square $P(A)$ can be completed to a latin square of order $n+1$.*

Proof. We define inductively a sequence $L_1, L_2, \ldots, L_{n+1}$ of partial latin squares of order $n+1$. First we let L_1 equal $P(A)$ and we observe that all the elements in column 1 are specified. For $k = 1,2,\ldots,n$, L_{k+1} is to be obtained from L_k by specifying those elements in column $k+1$ below its back diagonal. Thus L_{k+1} will have all its elements in columns $1,2,\ldots,k+1$ specified, and L_{n+1} will be a completion of $P(A)$ to a latin square of order $n+1$.

Suppose that the partial latin squares $L_1, L_2, \ldots, L_k$ have been defined where $k \leq n-1$. Let i be one of the $k-1$ integers $n+2-k, n+3-k, \ldots, n$. We define the *deficiency* $d(i, L_k)$ of row i of L_k to be the set of those integers j such that j occurs in the first k positions of row i of A but not in row i of L_k. It follows from the definition of $P(A)$ that

$$d(n+2-k, L_k) = \{a_{n+2-k,k}\}, \quad (k = 2, 3, \ldots, n). \tag{8.10}$$

We now define L_2 by specifying the last element in column 2 of L_1 to be a_{n2}. We note that L_2 is a partial latin square. We assume inductively that

$$\begin{gathered} d(i, L_k) \text{ contains a unique element for each } i = n+2-k, \ldots, n \\ \text{and these } k-1 \text{ elements are distinct.} \end{gathered} \tag{8.11}$$

If $d(i, L_k) = \{y\}$ we now write $d(i, L_k) = y$. We also assume inductively that

$$\begin{gathered} \text{the specified elements in row } n+1 \text{ of } L_k \text{ are} \\ \{n+1\} \cup \{d(j, L_k) : j = n+2-k, \ldots, n\}. \end{gathered} \tag{8.12}$$

Properties (8.11) and (8.12) hold if $k = 2$. We now show how to define a partial latin square L_{k+1} by specifying the elements of column $k+1$ of L_k below its back diagonal in such a way that properties (8.11) and (8.12) hold with k replaced by $k+1$.

We begin with the element $a_{n+1-k,k+1}$ and determine the longest sequence of the form

$$a_{i_0,k+1}, d(i_1, L_k), a_{i_1,k+1}, d(i_2, L_k), a_{i_2,k+1}, \ldots, d(i_p, L_k), a_{i_p,k+1}, \tag{8.13}$$

where $i_0 = n+1-k, i_1, \ldots, i_p$ are distinct integers from the set $\{n+1-k, n+2-k, \ldots, n\}$ satisfying

$$\begin{aligned} d(i_1, L_k) &= a_{i_0,k+1}, \\ d(i_2, L_k) &= a_{i_1,k+1}, \\ &\cdots \\ d(i_p, L_k) &= a_{i_{p-1},k+1}. \end{aligned} \tag{8.14}$$

Because the sequence (8.13) is the longest sequence satisfying (8.14) it follows from the inductive property (8.11) that $a_{i_p,k+1}$ does not equal $d(j, L_k)$ for any integer j with $n+2-k \leq j \leq n$. We now specify the element below the back diagonal in row i of column $k+1$ of L_{k+1} to be

$$\begin{cases} d(i, L_k), & \text{if } i \text{ is one of } i_1, i_2, \ldots, i_p, \\ a_{i_p,k+1}, & \text{if } i = n+1, \\ a_{i,k+1}, & \text{if } i \text{ is not one of } i_1, i_2, \ldots, i_p, n+1. \end{cases}$$

It follows from the construction and the inductive property (8.12) that L_{k+1} is a partial latin square of order $n+1$ with all of its elements in the first $k+1$ columns specified. Moreover,

$$\begin{aligned} d(i, L_{k+1}) &= a_{i,k+1} && \text{if } i \text{ is one of } i_1, i_2, \ldots, i_k \text{ and} \\ d(i, L_{k+1}) &= d(i, L_k) && \text{if } n+1-k \leq i \leq n \text{ and } i \text{ is not one} \\ & && \text{of } i_1, i_2, \ldots, i_p. \end{aligned}$$

The inductive properties (8.11) and (8.12) now hold with k replaced by $k+1$. Hence we obtain a sequence $L_1, L_2, \ldots, L_n$ of partial latin squares of order $n+1$. The partial latin square L_n has all of its entries specified except for those below the back diagonal in column $n+1$. If we specify the element in row i of column $n+1$ of L_n to be the element in $\{1, 2, \ldots, n+1\}$ which does not yet appear in row i, $(i = 2, 3, \ldots, n+1)$, then we obtain a completion L_{n+1} of $P(A)$. □

If A is a latin square of order n, then the latin square E_A of order $n+1$ obtained by completing $P(A)$ as in the proof of Theorem 8.3.6 is called the *enlargement* of A. As an illustration we construct the enlargement of the latin square

$$A = \begin{bmatrix} 3 & 5 & 1 & 7 & 6 & 2 & 4 \\ 6 & 7 & 3 & 2 & 4 & 1 & 5 \\ 5 & 2 & 4 & 6 & 1 & 7 & 3 \\ 1 & 6 & 5 & 4 & 7 & 3 & 2 \\ 2 & 1 & 6 & 5 & 3 & 4 & 7 \\ 4 & 3 & 7 & 1 & 2 & 5 & 6 \\ 7 & 4 & 2 & 3 & 5 & 6 & 1 \end{bmatrix}$$

for which

$$P(A) = \begin{bmatrix} 3 & 5 & 1 & 7 & 6 & 2 & 4 & 8 \\ 6 & 7 & 3 & 2 & 4 & 1 & 8 & \diamond \\ 5 & 2 & 4 & 6 & 1 & 8 & \diamond & \diamond \\ 1 & 6 & 5 & 4 & 8 & \diamond & \diamond & \diamond \\ 2 & 1 & 6 & 8 & \diamond & \diamond & \diamond & \diamond \\ 4 & 3 & 8 & \diamond & \diamond & \diamond & \diamond & \diamond \\ 7 & 8 & \diamond & \diamond & \diamond & \diamond & \diamond & \diamond \\ 8 & \diamond & \diamond & \diamond & \diamond & \diamond & \diamond & \diamond \end{bmatrix}$$

In the enlargement E_A of A below, the superscript preceding elements in positions (i, j) on and below the main diagonal equals the element in

position (i,j) of $A, (1 \leq i \leq j \leq n)$. These elements are used in carrying out the construction of E_A.

$$E_A = \begin{bmatrix} 3 & 5 & 1 & 7 & 6 & 2 & 4 & 8 \\ 6 & 7 & 3 & 2 & 4 & 1 & {}^{5}8 & 5 \\ 5 & 2 & 4 & 6 & 1 & {}^{7}8 & {}^{3}7 & 3 \\ 1 & 6 & 5 & 4 & {}^{7}8 & {}^{3}7 & {}^{2}3 & 2 \\ 2 & 1 & 6 & {}^{5}8 & {}^{3}3 & {}^{4}4 & {}^{7}5 & 7 \\ 4 & 3 & {}^{7}8 & {}^{1}1 & {}^{2}7 & {}^{5}5 & {}^{6}2 & 6 \\ 7 & {}^{4}8 & {}^{2}2 & {}^{3}3 & {}^{5}5 & {}^{6}6 & {}^{1}1 & 4 \\ 8 & 4 & 7 & 5 & 2 & 3 & 6 & 1 \end{bmatrix}$$

If, for instance, $k = 6$ the sequence (8.13) in the proof of Theorem 8.3.6 is

$$5, d(5, L_6), 7, d(3, L_6), 3, d(4, L_6), 2, d(6, L_6), 6.$$

Theorem 8.3.6 provides the key step in an inductive proof of the Evans conjecture. The following lemma is also used in the inductive proof.

Lemma 8.3.7. *Let X be an n by n array with at most $n-1$ of its elements specified, and let z be one of its specified elements. Then it is possible to permute the rows and the columns of X so that in the resulting array Y, z occurs on the back diagonal and the other specified elements of Y occur above the back diagonal.*

Proof. If $n = 2$ the lemma holds. We assume that $n > 2$ and proceed by induction on n. If all of the specified elements of X are in one row, we permute the rows of X so that the specified elements are in row 1, and then permute the columns so that z is in the last position of the first row. The resulting array Y satisfies the conclusions of the lemma. We now assume that there is an i such that row i does not contain z but contains at least one specified element. Since X has only $n-1$ specified elements, there is a j such that column j of X has no specified element. We now permute the rows of X so that row i of X becomes the first row and we permute the columns so that column j becomes the last column. Let X' be the $n-1$ by $n-1$ array in the lower left corner. Then X' has at most $n-2$ specified elements and one of these is z. Applying the inductive hypothesis to X' we complete the proof. □

The following theorem contains the solution to the Evans conjecture.

Theorem 8.3.8. *A partial latin square of order n with at most $n-1$ specified elements can always be completed to a latin square of order n.*

Proof. Let A be a partial latin square of order n based on the set $\{1, 2, \ldots, n\}$ with at most $n-1$ specified elements. If A has less than $n-1$

specified elements, then it is possible to specify another element so as to obtain a partial latin square. Hence we assume that A has $n-1$ specified elements. We prove the theorem by induction on n. If $n = 1$ or 2, the theorem holds. Now assume that $n > 2$.

First suppose that some integer in $\{1, 2, \ldots, n\}$ occurs exactly once in A. Without loss of generality we assume that n occurs exactly once in A. By Lemma 8.3.7 we also assume without loss of generality that n occurs on the back diagonal of A and that the other specified elements of A occur above the back diagonal. Let B be the $n-1$ by $n-1$ array obtained by deleting the last row and the last column of A and deleting the element n on A's back diagonal. Then B is a partial latin square of order $n-1$ based on the set $\{1, 2, \ldots, n-1\}$ with $n-2$ prescribed elements. By the inductive hypothesis B can be completed to a latin square C of order $n-1$. By Theorem 8.3.6 $P(C)$ can be completed to a latin square E_C of order $n-1$ based on the set $\{1, 2, \ldots, n\}$. The enlargement E_C has n throughout its back diagonal and hence is a completion of A to a latin square of order n.

Now suppose that every integer that occurs in A occurs at least twice. Thus the number of different integers that occur in A is at most $\lfloor (n-1)/2 \rfloor$. Suppose that there exists an integer i such that row i of A contains exactly one specified element. Then we replace A by the equivalent[1] partial latin square $A_{(3,2,1)}$ in which the row indices and the elements have been interchanged. The integer i occurs exactly once in $A_{(3,2,1)}$ and hence as proved above $A_{(3,2,1)}$ has a completion to a latin square U. The latin square $U_{(3,2,1)}$ is a completion of A. Thus we may now assume that no row of A contains exactly one specified element. Similarly, we may now also assume that no column of A contains exactly one specified element. Thus the specified elements of A lie in an r by s rectangle where $r \leq \lfloor (n-1)/2 \rfloor$ and $s \leq \lfloor (n-1)/2 \rfloor$. By Corollary 8.3.3 A can be completed to a latin square of order n. □

Theorem 8.3.8 has an equivalent formulation in terms of (0,1)-matrices.

Theorem 8.3.9. *Let B be a $(0,1)$-matrix with at most $n-1$ 1's, and let k be a positive integer with $k \leq n-1$. Assume that $B = Q_1 + Q_2 + \cdots + Q_k$ is a decomposition of B into subpermutation matrices $Q_1, Q_2, \ldots, Q_k$ of order n. Then there exist subpermutation matrices $P_1, P_2, \ldots, P_k$ of order n such that*

$$C = P_1 + P_2 + \cdots + P_k$$

is a $(0,1)$-matrix and $Q_i \leq P_i, (i = 1, 2, \ldots, k)$.

Proof. The array

$$A = 1Q_1 + 2Q_2 + \cdots + kQ_k$$

[1] We owe to B.L. Shader the observation that replacing A by an equivalent partial latin square enables one to avoid the theorem of Lindner[1970].

is a partial latin square of order n with at most $n-1$ specified elements. By Theorem 8.3.8 A can be completed to a latin square. This latin square is of the form

$$1P_1 + 2P_2 + \cdots + nP_n$$

where $P_1, P_2, \ldots, P_n$ are permutation matrices of order n and where $Q_i \leq P_i, (i = 1, 2, \ldots, k)$. The matrix

$$C = P_1 + P_2 + \cdots + P_k$$

is a (0,1)-matrix satisfying the conclusions of the theorem. □

Finally we remark that Andersen and Hilton[1983] showed that a partial latin square A of order n with n prescribed elements can be completed to a latin square of order n if and only if A is not equivalent to

$$\begin{bmatrix} 1 & 2 & \cdots & k & \diamond & \cdots & \diamond \\ \diamond & \diamond & \cdots & \diamond & k+1 & \cdots & \diamond \\ & & \cdots & & \vdots & \ddots & \diamond \\ \diamond & \diamond & \cdots & \diamond & \diamond & \cdots & k+1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \end{bmatrix} \tag{8.15}$$

for any $k = 1, 2, \ldots, n-1$. Damerell[1983] showed that Smetaniuk's proof of the Evans conjecture could be extended to yield a proof of this result as well.

Colburn[1984] has proved that the decision problem *Can a partial latin square of order n be completed to a latin square?* is an NP-complete problem.

Exercises

1. For each integer $n \geq 4$ show that there exists a partial latin square of order n which cannot be embedded in a latin square of any order strictly less than $2n$ (Evans[1960]).
2. Prove that the partial latin squares of order n given by (8.15) can be partitioned into two parts each of which can be completed to a latin square of order n.
3. Determine the enlargement of a Cayley table of a cyclic group of order 7.
4. Complete the partial latin square A given below to a latin square:

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

5. Let n be a positive integer. Show that Lemma 8.3.7 does not hold in general if the array X has more than n specified elements.
6. Prove that a symmetric latin square of odd order has a transversal.
7. Let A be a partial latin square of order n whose specified elements all belong to an r by r square L in its upper left corner. Assume that each element of

L is specified and that L is symmetric. Prove that A can be completed to a *symmetric* latin square if and only if the number $N(j)$ of times the element j occurs in L satisfies the following two conditions:

(i) $N(j) \geq 2r - n, (j = 1, 2, \ldots, n)$;

(ii) $N(j) \equiv n \pmod 2$ for at least r of the integers $j = 1, 2, \ldots, n$ (Cruse[1974]).

8. Let A be a symmetric partial latin square of order n. Prove that there is a symmetric latin square of order $2n$ which contains A in its upper left corner. (A *symmetric partial latin square* is a partial latin square which, considered as a matrix with elements from $\{1, 2, \ldots, n, \diamond\}$, is symmetric.) For each integer $n \geq 4$ show that there exists a symmetric partial latin square of order n which cannot be embedded in this way in any symmetric latin square of order strictly less than $2n$(Cruse[1974]).

References

L.D. Andersen and A.J.W. Hilton[1983], Thanks Evans!, *Proc. London Math. Soc.* (3), 47, pp. 507–522.

R.A. Brualdi and J. Csima[1986], Extending subpermutation matrices in regular classes of matrices, *Discrete Math.*, 62, pp. 99–101.

C.C. Colburn[1984], The complexity of completing partial latin squares, *Discrete Applied Math.*, 8, pp. 25–30.

A.B. Cruse[1974], On embedding incomplete symmetric latin squares, *J. Combin. Theory, Ser. A*, 16, pp. 18–22.

R.M. Damerell[1983], On Smetaniuk's construction for latin squares and the Andersen-Hilton theorem, *Proc. London Math. Soc.* (3), 47, pp. 523–526.

D.E. Daykin and R. Häggvist[1981], Problem No. 6347, *Amer. Math. Monthly*, 88, p. 446.

T. Evans[1960], Embedding incomplete latin squares, *Amer. Math. Monthly*, 67, pp. 958–961.

R. Häggvist[1978], A solution to the Evans conjecture for latin squares of large size, *Combinatorics*, Proc. Conf. on Combinatorics, Kesthely (Hungary) 1976, János Bolyai Math. Soc. and North Holland, pp. 495–513.

M. Hall Jr.[1945], An existence theorem for latin squares, *Bull. Amer. Math. Soc.* 51, pp. 387–388.

C.C. Lindner[1970], On completing latin rectangles, *Canad. Math. Bull.*, 13, pp. 65–68.

W.E. Opencomb[1984], On the intricacy of combinatorial problems, *Discrete Math.*, 50, pp. 71–97.

H.J. Ryser[1951], A combinatorial theorem with an application to latin rectangles, *Proc. Amer. Math. Soc.*, 2, pp. 550–552.

B. Smetaniuk[1981], A new construction for latin squares I. Proof of the Evans conjecture, *Ars Combinatoria*, 11, pp. 155–172.

8.4 Orthogonal Latin Squares

Let A be a latin square of order n based on the set $S = \{1, 2, \ldots, n\}$. We let

$$X = \{(i, j) : i, j = 1, 2, \ldots, n\}$$

denote the set of n^2 positions of A, and we now call the elements of X *points*. The set of points

$$\{(i,1),(i,2),\ldots,(i,n)\},\quad (i=1,2,\ldots,n)$$

in a row is a *horizontal line*. The set of points

$$\{(1,j),(2,j),\ldots,(n,j)\},\quad (j=1,2,\ldots,n)$$

in a column is a *vertical line*. Each horizontal line contains n points, and the set $H(A)$ of horizontal lines partitions the set X of points. A similar statement holds for the set $V(A)$ of vertical lines. Because A is a latin square, there are permutation matrices $P_1, P_2, \ldots, P_n$ of order n such that

$$J_n = P_1 + P_2 + \cdots + P_n$$

and

$$A = 1P_1 + 2P_2 + \cdots + nP_n.$$

Each permutation matrix P_i determines a set of n points which we call a *latin line* of A. The set $L(A)$ of the n latin lines of A also partition the n^2 points of X. Unlike $H(A)$ and $V(A)$ the set $L(A)$ of latin lines depends on the elements of A. The latin squares obtained from A by permuting the lines within each of the three classes and by permuting the three classes are the latin squares which are equivalent to A.

We now seek to arrange the elements of S in an n by n array B in such a way that each line of each of the classes $H(A), V(A)$ and $L(A)$ contains each element of S exactly once. Such an array B is a latin square with the additional property that each latin line of A contains each element of S exactly once. For example, let

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

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

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

The latin square

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

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

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

is of the desired type because each latin line of B has exactly one point in common with each latin line of A.

We define two latin squares A and B to be *orthogonal* provided each latin line of A and each latin line of B have exactly one point in common. Thus the latin squares $A = [a_{ij}]$ and $B = [b_{ij}]$ of order n are orthogonal if and only if the n^2 ordered pairs

$$(a_{ij}, b_{ij}), \quad (i, j = 1, 2, \ldots, n)$$

are distinct. If A and B are orthogonal latin squares then each is an *orthogonal mate* of the other. The latin squares A and B of order 4 above are orthogonal latin squares. It follows from the definition that if A has an orthogonal mate, then A has a transversal and indeed the n^2 positions of A can be partitioned into n transversals (such a partition is the set of n latin lines of an orthogonal mate B). A latin square with no transversal cannot therefore have an orthogonal mate. Thus two latin squares of order 2 are never orthogonal. More generally, we conclude from Theorem 8.2.1 that a Cayley table of an abelian group of even order with a unique element of order two does not have an orthogonal mate.

The question of the existence of orthogonal latin squares was raised by Euler[1782] in the following *problem of the* 36 *officers*:

> Is it possible to arrange 36 officers of 6 different ranks and from 6 different regiments in a square formation of size 6 by 6 so that each row and each column of this formation contains exactly one officer of each rank and exactly one officer from each regiment?

If we label the 6 ranks and the 6 regiments from 1 through 6, then this problem asks for two orthogonal latin squares of order 6. Euler was unable

to find such a pair of latin squares and conjectured that no pair existed. Tarry[1901] verified that there was no pair of orthogonal latin squares of order 6. While the notion of orthogonal latin squares originated in this recreational problem of Euler, it has since become important in the design of statistical experiments (see, e.g., Raghavarao[1971] and Joshi[1987]). Orthogonal latin squares are also of fundamental importance in the study of finite projective planes.

We now extend our definition of orthogonality of latin squares to any finite set of latin squares of the same order. The latin squares $A_1, A_2, \ldots, A_t$ of order n are *mutually orthogonal* provided A_i and A_j are orthogonal for all i different from j. If $A_1, A_2, \ldots, A_t$ are mutually orthogonal latin squares of order n and A_i' is a latin square equivalent to $A_i, (i = 1, 2, \ldots, t)$, then $A_1', A_2', \ldots, A_t'$ are also mutually orthogonal latin squares.

Let $N(n)$ denote the largest number of mutually orthogonal latin squares of order n. Thus $N(1) = 2$ (because a latin square of order 1 is orthogonal to itself) and $N(2) = 1$. By Tarry's verification $N(6) = 1$. It is not difficult to show that $N(n) \geq 2$ for every odd integer $n \geq 3$.

Theorem 8.4.1. *If A is a Cayley table of an abelian group of odd order $n \geq 3$, then A has an orthogonal mate. In particular, $N(n) \geq 2$ for each odd integer $n \geq 3$.*

Proof. Let $a_1, a_2, \ldots, a_n$ be the elements of an (additive) abelian group of odd order $n \geq 3$. Let $A = [a_{ij}]$ be the Cayley table of G in which

$$a_{ij} = a_i + a_j, \quad (i, j = 1, 2, \ldots, n).$$

Let the matrix $B = [b_{ij}]$ of order n be defined by

$$b_{ij} = a_i - a_j, \quad (i, j = 1, 2, \ldots, n).$$

Then B is a latin square (B is a column permutation of a Cayley table for G). Because G has odd order each element of G can be written in the form $a_k + a_k$ for some integer $k = 1, 2, \ldots, n$. Let x and y be arbitrary elements of G. Then there exists i and j such that $a_i + a_i = x + y$ and $a_j + a_j = x - y$ implying that

$$a_i + a_j = x \qquad \text{and} \qquad a_i - a_j = y.$$

Therefore A and B are orthogonal latin squares. □

We also have the following elementary result.

Theorem 8.4.2. *If $A_1, A_2, \ldots, A_t$ are mutually orthogonal latin squares of order $n \geq 2$, then $t \leq n - 1$. Thus $N(n) \leq n - 1$ for $n \geq 2$.*

Proof. Without loss of generality we assume that the first row of each of the latin squares A_i is $1, 2, \ldots, n$. Thus no A_i has a 1 in the $(2,1)$ position nor can two of the latin squares have the same element in the $(2,1)$ position. Hence $t \leq n-1$. □

The upper bound for $N(n)$ in Theorem 8.4.2 is attained if n is a power of a prime number. The verification of this statement uses the existence of the Galois fields $GF(p^\alpha)$ where p is a prime and α is a positive integer.

Theorem 8.4.3. *Let $n = p^\alpha$ where p is a prime and α is a positive integer. Then there exist $n-1$ mutually orthogonal latin squares of order n and hence $N(n) = n-1$.*

Proof. Let the elements of the Galois field $GF(p^\alpha)$ be denoted by $a_1 = 0, a_2, \ldots, a_n$. For $k = 2, 3, \ldots, n$ we define n by n matrices

$$A^{(k)} = [a_{ij}^{(k)}], \quad (i, j = 1, \ldots, n)$$

where

$$a_{ij}^{(k)} = a_k a_i + a_j.$$

Suppose that $A^{(k)}$ has two equal elements in row i. Then there exist integers j and j' such that

$$a_k a_i + a_j = a_k a_i + a_{j'},$$

implying that $a_j = a_{j'}$ and hence $j = j'$. Now suppose that A has two equal elements in column j. Then there exist integers i and i' such that

$$a_k a_i + a_j = a_k a_{i'} + a_j,$$

which implies, because $a_k \neq 0$, that $a_i = a_{i'}$ and hence $i = i'$. It follows that each $A^{(k)}$ is a latin square.

Now let k and l be integers with $2 \leq k < l \leq n$. We show that $A^{(k)}$ and $A^{(l)}$ are orthogonal. Suppose that

$$\left(a_{ij}^{(k)}, a_{ij}^{(l)}\right) = \left(a_{i'j'}^{(k)}, a_{i'j'}^{(l)}\right).$$

Then

$$a_k a_i + a_j = a_k a_{i'} + a_{j'} \tag{8.16}$$

and

$$a_l a_i + a_j = a_l a_{i'} + a_{j'}. \tag{8.17}$$

Subtracting (8.17) from (8.16) we obtain

$$(a_l - a_k) a_i = (a_l - a_k) a_{i'}. \tag{8.18}$$

Because $a_l \neq a_k$, (8.18) implies that $a_i = a_{i'}$. Substituting into (8.16) we also get $a_j = a_{j'}$. Hence $i = i'$ and $j = j'$ and it follows that $A^{(k)}$ and $A^{(l)}$ are orthogonal. □

We now show how to combine two pairs of orthogonal latin squares to obtain a pair of orthogonal latin squares of larger order. Let $X = [x_{ij}]$ and $Y = [y_{ij}]$ be matrices of orders m and n, respectively. The matrix

$$X \otimes Y = [(x_{ij}, y_{kl})], \quad (i, j = 1, 2, \ldots, m; k, l = 1, 2, \ldots, n)$$

of order mn is called the *symbolic direct product* of X and Y. Its rows and columns are indexed by the ordered pairs $(r, s), (r = 1, 2, \ldots, m; s = 1, 2, \ldots, n)$ in lexicographic order. The elements of $X \otimes Y$ are the ordered pairs of the elements of X with the elements of Y. The following theorem is from MacNeish[1922].

Theorem 8.4.4. *Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be orthogonal latin squares of order m, and let $C = [c_{kl}]$ and $D = [d_{kl}]$ be orthogonal latin squares of order n. Then $A \otimes C$ and $B \otimes D$ are orthogonal latin squares of order mn.*

Proof. Let the latin squares A and B be based on the set $S = \{1, 2, \ldots, m\}$ and let the latin squares C and D be based on the set $T = \{1, 2, \ldots, n\}$. Then $A \otimes C$ and $B \otimes D$ are latin squares based on the cartesian product $S \times T$ with rows and columns indexed by the elements of $S \times T$. We now show that $A \otimes C$ and $B \otimes D$ are orthogonal.

Suppose that

$$((a_{ij}, c_{kl}), (b_{ij}, d_{kl})) = ((a_{i'j'}, c_{k'l'}), (b_{i'j'}, d_{k'l'})).$$

Then

$$(a_{ij}, c_{kl}) = (a_{i'j'}, c_{k'l'}) \qquad \text{and} \qquad (b_{ij}, d_{kl}) = (b_{i'j'}, d_{k'l'}),$$

and hence

$$a_{ij} = a_{i'j'} \qquad \text{and} \qquad b_{ij} = b_{i'j'} \tag{8.19}$$

and

$$c_{kl} = c_{k'l'} \qquad \text{and} \qquad d_{kl} = d_{k'l'}. \tag{8.20}$$

Because A and B are orthogonal, (8.19) implies that $i = i'$ and $j = j'$. Because C and D are orthogonal, (8.20) implies that $k = k'$ and $l = l'$. Hence $(i, j) = (i', j')$ and $(k, l) = (k', l')$, and it follows that $A \otimes C$ and $B \otimes D$ are orthogonal. □

Corollary 8.4.5. *Let $m_1, m_2, \ldots, m_k$ be positive integers. Then*

$$N(m_1 m_2 \cdots m_k) \geq \min\{N(m_i) : i = 1, 2, \ldots, k\}. \tag{8.21}$$

Proof. The inequality (8.21) follows from repeated application of Theorem 8.4.4. □

By applying Theorem 8.4.3 and Corollary 8.4.5 we obtain the following lower bound for the number $N(n)$ of mutually orthogonal latin squares of order n.

Corollary 8.4.6. *Let $n \geq 2$ be an integer and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes. Then*

$$N(n) \geq \min\{p_i^{\alpha_i} - 1 : i = 1, 2, \ldots, k\}. \tag{8.22}$$

In particular, if n is not of the form $4m + 2$, then $N(n) \geq 2$.

It was conjectured by MacNeish[1922] that equality holds in (8.22) for every integer $n \geq 2$. By Theorem 8.4.3 MacNeish's conjecture holds if n is a power of a prime. MacNeish's conjecture has its origin in a conjecture of Euler[1782] which asserts that there does not exist a pair of orthogonal latin squares of order n for any integer n which is twice an odd number. Euler's conjecture thus asserts that if $n \geq 6$ and n is of the form $4m + 2$, then $N(n) = 1$, which is in agreement with MacNeish's conjecture for these integers n. While Tarry [1901] verified the validity of Euler's conjecture for $n = 6$, the combined efforts of Bose, Shrikhande and Parker[1960] disproved Euler's conjecture in *all* other cases.

Theorem 8.4.7. *Let $n > 6$ be an integer of the form $4m+2$. Then there exists a pair of orthogonal latin squares of order n.*

We shall not give a complete proof of Theorem 8.4.7. We shall only discuss some of the techniques of construction which are used in its proof.

Parker[1959a] disproved MacNeish's conjecture by showing that $N(21) \geq 3$. Then Bose and Shrikhande[1959, 1960b] disproved Euler's conjecture by showing that $N(50) \geq 5$ and $N(22) \geq 2$. Parker[1959b] constructed a pair of orthogonal latin squares of order 10 thereby showing that $N(10) \geq 2$ and thus settling negatively the smallest unsolved case of the Euler conjecture since Tarry[1901] had verified that $N(6) = 1$.

The following two orthogonal latin squares of order 10 based on the set $\{0, 1, 2, \ldots, 9\}$ are those constructed by Parker[1959b].

$$\begin{bmatrix} 0 & 6 & 5 & 4 & 7 & 8 & 9 & 1 & 2 & 3 \\ 9 & 1 & 0 & 6 & 5 & 7 & 8 & 2 & 3 & 4 \\ 8 & 9 & 2 & 1 & 0 & 6 & 7 & 3 & 4 & 5 \\ 7 & 8 & 9 & 3 & 2 & 1 & 0 & 4 & 5 & 6 \\ 1 & 7 & 8 & 9 & 4 & 3 & 2 & 5 & 6 & 0 \\ 3 & 2 & 7 & 8 & 9 & 5 & 4 & 6 & 0 & 1 \\ 5 & 4 & 3 & 7 & 8 & 9 & 6 & 0 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & 7 & 8 & 9 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 & 9 & 7 & 8 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 & 8 & 9 & 7 \end{bmatrix} \quad \begin{bmatrix} 0 & 9 & 8 & 7 & 1 & 3 & 5 & 2 & 4 & 6 \\ 6 & 1 & 9 & 8 & 7 & 2 & 4 & 3 & 5 & 0 \\ 5 & 0 & 2 & 9 & 8 & 7 & 3 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & 9 & 8 & 7 & 5 & 0 & 2 \\ 7 & 5 & 0 & 2 & 4 & 9 & 8 & 6 & 1 & 3 \\ 8 & 7 & 6 & 1 & 3 & 5 & 9 & 0 & 2 & 4 \\ 9 & 8 & 7 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & 8 & 9 & 7 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 & 9 & 7 & 8 \end{bmatrix}$$

This construction for a pair of orthogonal latin squares of order 10 was generalized by Bose, Shrikhande and Parker[1960] and by Menon[1961] to give a pair of orthogonal latin squares of order $n = 3m+1$ for every $m \geq 3$ satisfying $N(m) \geq 2$.

Theorem 8.4.8. *Let m be an integer for which there exists a pair of orthogonal latin squares of order m. Then there exists a pair of orthogonal latin squares of order $n = 3m + 1$.*

Proof. Let σ be the permutation of $\{0, 1, \ldots, 2m\}$ defined by $\sigma(i) \equiv i + 1 \pmod{2m+1}$. Let P denote the permutation matrix of order $2m+1$ corresponding to σ. Then P^k is the permutation matrix corresponding to $\sigma^k, (k = 0, 1, \ldots, 2m)$. We first construct a matrix $X = [x_{ij}]$ of order $2m+1$ as follows. The elements on the main diagonal of X (the positions in which $P^0 = I_{2m+1}$ has 1's) are $0, 1, \ldots, 2m$. For $k = 1, 2, \ldots, m$ the elements of X in those positions in which P^k has 1's are $2m-(k-1), 2m-(k-2), \ldots, 0, 1, \ldots, 2m-k \pmod{2m+1}$ in the order of their row index. For $k = m+1, m+2, \ldots, 2m$ the elements of X in those positions in which P^k has 1's are $2m+1, 2m+2, \ldots, 3m$ again in the order of their row index.

Next we construct a $2m+1$ by m matrix Y as follows. The elements in the first column of Y are $1, 2, \ldots, 2m, 0$ in the order of their row index. The elements in column k of Y are obtained by cyclically shifting upwards by one row the elements in column $k-1$ of $Y, (k = 2, 3, \ldots, m)$.

Finally we construct an m by $2m+1$ matrix Z. The elements in the first row of Z are $2, 3, \ldots, 2m, 0, 1$ in the order of their column index. The elements in row k of Z are obtained by cyclically shifting to the left by two columns the elements in row $k-1$ of $Z, (k = 2, 3, \ldots, m)$.

Let U and V be orthogonal latin squares of order m based on the m-element set $\{2m+1, 2m+2, \ldots, 3m\}$. Then it can be verified that

$$\begin{bmatrix} X & Y \\ Z & U \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} X^T & Z^T \\ Y^T & V \end{bmatrix}$$

are orthogonal latin squares of order $3m+1$ based on $\{0, 1, 2, \ldots, 3m\}$. □

Corollary 8.4.9. *Let n be a positive integer satisfying $n \equiv 10 \pmod{12}$. Then there exists a pair of orthogonal latin squares of order n.*

Proof. Let n be an integer satisfying the hypothesis. Then there exists a nonnegative integer k such that $n = 3(4k+3)+1$. By Theorem 8.4.1 there exists a pair of orthogonal latin squares of order $4k+3$. We now apply Theorem 8.4.8 with $m = 4k+3$. □

To further discuss constructions of orthogonal latin squares, we continue with the geometric interpretation of latin squares given at the beginning of the section. Let $A_1, A_2, \ldots, A_t$ be a set of t mutually orthogonal latin

squares of order n based on the set $\{1, 2, \ldots, n\}$, and let L_i denote the set of latin lines of $A_i, (i = 1, 2, \ldots, t)$. Let H denote the set of horizontal lines (of each A_i) and V the set of vertical lines. Thus each of the $t + 2$ sets

$$H, V, L_1, L_2, \ldots, L_t$$

consists of n pairwise disjoint lines of n points each of which partition the point set $X = \{(i, j) : i, j = 1, 2, \ldots, n\}$. We call each of these sets a *parallel class* of lines. Because $A_1, A_2, \ldots, A_t$ are mutually orthogonal, lines from different parallel classes have exactly one point in common. We are thus led to make the following general definition (Bruck[1951,1963]).

Let $n \geq 2$ be an integer. Let X be a set of n^2 elements called *points*, and let $\mathcal{B} = \{T_1, T_2, \ldots, T_r\}$ where

$$T_i = T_i^1, T_i^2, \ldots, T_i^n$$

is a partition of X into n sets of n points each. The sets $T_i^j, (j = 1, 2, \ldots, n)$ in T_i are called *lines* and each T_i is a *parallel class* of lines. The pair $(X, \mathcal{B})$ is an (n, r)-*net* provided that lines in different parallel classes intersect in exactly one point. It follows from our previous discussion that if there exists a set of t mutually orthogonal latin squares of order n, then there exists an $(n, t + 2)$-net. The converse also holds.

Theorem 8.4.10. *Let $n \geq 2$ and $r \geq 2$ be integers. Then $N(n) \geq r - 2$ if and only if an (n, r)-net exists.*

Proof. If $N(n) \geq r-2$, then an (n, r)-net exists. Now suppose that $(X, \mathcal{B})$ is an (n, r)-net where $\mathcal{B} = \{T_1, T_2, \ldots, T_r\}$. We may label the n^2 points of X so that

$$X = \{(i, j) : i, j = 1, 2, \ldots, n\},$$
$$T_1^i = \{\{(i, j) : j = 1, 2, \ldots, n\}\}, \quad (1 \leq i \leq n)$$

and

$$T_2^j = \{\{(i, j) : i = 1, 2, \ldots, n\}\}, \quad (i \leq j \leq n).$$

Let

$$P_k^{(l)}, \quad (k = 3, 4, \ldots, r; l = 1, 2, \ldots, n)$$

be the (0,1)-matrix of order n whose 1's are in those positions (i, j) for which (i, j) is a point of the lth line of T_k. Then each $P_k^{(l)}$ is a permutation matrix of order n and the $r - 2$ matrices

$$A_k = 1P_k^{(1)} + 2P_k^{(2)} + \cdots + nP_k^{(n)}, \quad (k = 3, 4, \ldots, r)$$

are mutually orthogonal latin squares of order n. □

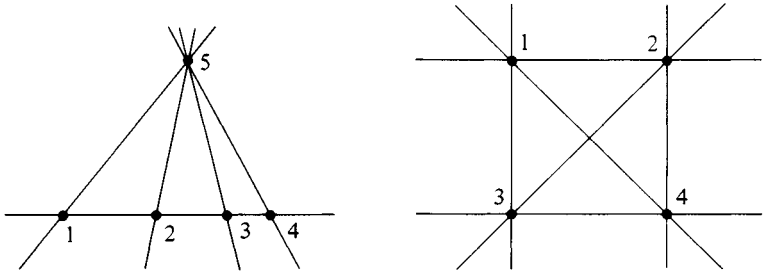

Figure 8.2

Bose and Shrikhande[1960a] defined another combinatorial configuration as follows. Let X be a finite set of elements called *points*, and let $\mathcal{A}$ be a collection of subsets of X called *lines* (or *blocks*). Then the pair $(X, \mathcal{A})$ is a *pairwise balanced design* provided:

(L1) *Each line in $\mathcal{A}$ contains at least two points.*

and

(L2) *For each pair x, y of distinct points in X, there is exactly one line in $\mathcal{A}$ containing both x and y.*

A simple example of a pairwise balanced design is obtained by letting

$$X = \{1, 2, 3, 4, 5\}$$

and

$$\mathcal{A} = \{\{1, 2, 3, 4\}, \{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}.$$

Another simple example is obtained by letting $X = \{1, 2, 3, 4\}$ and $\mathcal{A} = \mathcal{P}_2(X)$, the collection of all two element subsets of X. These two examples are pictured geometrically in Figure 8.2.

An *affine plane* is a pairwise balanced design $(X, \mathcal{A})$ which satisfies the additional properties:

(L3) (Playfair's axiom or the parallel postulate) *For each point x in X and each line A in $\mathcal{A}$ not containing x, there is a unique line B in $\mathcal{A}$ which contains x but has no points in common with A.*

and

(L4) (A nondegeneracy condition) *There exist four points in X no three of which are together in a line of $\mathcal{A}$.*

The pairwise balanced design in Figure 8.2 which has four points is an affine plane.

Let p be a prime number and let α be a positive integer. The finite field $GF(p^\alpha)$ with $n = p^\alpha$ elements can be used to construct an affine plane. This construction, which mimics the analytic representation of the real Euclidean plane, proceeds as follows.

Let the set of n^2 points be

$$X = \{(a, b) : a, b \text{ in } GF(p^\alpha)\}.$$

A line in $\mathcal{A}$ is defined to be a set of points which satisfies a linear equation $ax + by + c = 0$ where a, b and c are elements of $GF(p^\alpha)$ with not both a and b equal to 0. Thus the lines are in one-to-one correspondence with the set of $n^2 + n$ linear equations of the form

$$\begin{aligned} x &= a \qquad (a \text{ in } GF(p^\alpha)) \\ y &= mx + b \quad (m, b \text{ in } GF(p^\alpha)) \end{aligned}.$$

It is now entirely straightforward to verify that the pair $(X, \mathcal{A})$ is an affine plane. We call a plane constructed in this way a *Galois affine plane* and denote it by $AP(p^\alpha)$. The affine plane $AP(p^\alpha)$ has n^2 points and $n^2 + n$ lines; in addition, each line contains n points and each point is contained in $n + 1$ lines. In the next theorem we show that arithmetic conditions like these hold for affine planes in general.

Let $(X, \mathcal{A})$ be an affine plane. Two lines in $\mathcal{A}$ are called *parallel* provided the lines are identical or have no point in common. It follows from the definition of an affine plane that the relation of parallelism is an equivalence relation on $\mathcal{A}$. Hence the lines in $\mathcal{A}$ are partitioned into parallel classes of lines. Two lines in the same class are parallel while lines from each of two different classes have exactly one point in common.

Theorem 8.4.11. *Let $(X, \mathcal{A})$ be an affine plane. Then there exists an integer $n \geq 2$ for which the following properties hold:*

$$X \text{ has } n^2 \text{ points.} \tag{8.23}$$

$$\mathcal{A} \text{ has } n^2 + n \text{ lines.} \tag{8.24}$$

$$\text{Each line in } \mathcal{A} \text{ contains } n \text{ points.} \tag{8.25}$$

$$\text{Each point in } X \text{ is contained in } n + 1 \text{ lines.} \tag{8.26}$$

$$\text{There are } n + 1 \text{ parallel classes of lines.} \tag{8.27}$$

$$\text{Each parallel class contains } n \text{ lines.} \tag{8.28}$$

Proof. We first show that (8.25) holds. Let B and B' be distinct lines in $\mathcal{A}$. First suppose that B and B' have a point x in common. By (L1) and (L2) there exist a point $a \neq x$ on B and a point $b \neq x$ on B', and a line B'' containing both a and b. By Playfair's axiom (L3) there exist a line containing x which is parallel to B'' and hence there exists a point z

contained in neither B nor B'. It follows from (L2) and Playfair's axiom (L3) that exactly one line containing z intersects B but not B' and exactly one line containing z intersects B' but not B. We thus conclude that B and B' have the same number of points. Now suppose that B and B' are parallel. Let c be a point on B and let d be a point on B'. Then there is a line B^* containing both c and d. As above B and B^* have the same number of points, and B' and B^* have the same number of points. Thus in this case also B and B' have the same number of points. Therefore there exists an integer $n \geq 2$ such that (8.25) holds. By (L2) and Playfair's axiom (L3), (8.26) also holds. From (L2) and (8.26) we obtain (8.23). From (8.26) we conclude that there are $n+1$ parallel classes of lines and each of these parallel classes contains n lines. Hence (8.24), (8.27) and (8.28) also hold. □

Let $(X, \mathcal{A})$ be an affine plane. The integer $n \geq 2$ satisfying the conclusions of Theorem 8.4.12 is called the *order* of the affine plane. The Galois affine plane $AP(p^\alpha)$ has order $n = p^\alpha$. It is not known whether there exist affine planes whose orders do not equal a prime power, although there exist affine planes which are not Galois affine planes.

Theorem 8.4.12. *Let $n \geq 2$ be an integer. Then the following are equivalent:*

(i) There is a set of $n-1$ mutually orthogonal latin squares of order n.
(ii) There is an $(n, n+1)$-net.
(iii) There is an affine plane of order n.

Proof. The equivalence of (i) and (ii) follows from Theorem 8.4.10. It follows from Theorem 8.4.11 that (iii) implies (ii). Now supppose that (ii) holds and let $(X, \mathcal{B})$ be an $(n, n+1)$-net. Let $\mathcal{A}$ be the set of all lines in the net. One may directly show that $(X, \mathcal{A})$ is an affine plane of order n. □

A *projective plane* is a pairwise balanced design $(X, \mathcal{A})$ which satisfies the nondegeneracy condition (L4) and the additional property

(L5) (The no-parallels postulate) *Two distinct lines in $\mathcal{A}$ have exactly one point in common.*

Let the parallel classes of lines of an affine plane $(X, \mathcal{A})$ be $T_1, T_2, \ldots, T_{n+1}$. Let $Y = \{y_1, y_2, \ldots, y_{n+1}\}$ be a set of $n+1$ points which is disjoint from X. By adjoining y_i to each line of $T_i, (i = 1, 2, \ldots, n+1)$ and adjoining Y as a new line to $\mathcal{A}$ we obtain a projective plane $(X \cup Y, \mathcal{A}')$ with n^2+n+1 points and n^2+n+1 lines. Each line of $\mathcal{A}'$ contains exactly $n+1$ points of $X \cup Y$, and each point of $X \cup Y$ is contained in exactly $n+1$ lines of $\mathcal{A}'$. Conversely, upon removing from a projective plane the set of points on any prescribed line B and removing the line B we obtain an affine plane. The

order of the projective plane is defined to be the order of the resulting affine plane. Hence by Theorem 8.4.12 *a projective plane of order $n \geq 2$ exists if and only if there exist $n-1$ mutually orthogonal latin squares of order n.* These connections between orthogonal latin squares and projective and affine planes are due to Bose[1938].

We now describe two constructions of Bose, Shrikhande and Parker which combine a set of mutually orthogonal latin squares and a pairwise balanced design in order to obtain another set of mutually orthogonal latin squares.

A latin square of order n based on an n-set S is *idempotent* provided its main diagonal is a transversal. A latin square with a transversal is equivalent (under row and column permutations only) to an idempotent latin square. Let $A_0, A_1, \ldots, A_k$ be $k+1$ mutually orthogonal latin squares of order n. Without loss of generality, we assume that the elements on the main diagonal of A_0 are identical. Then for $i \geq 1$ the main diagonal of A_i is a transversal of A_i, and hence A_i is an idempotent latin square. Thus from the set $A_0, A_1, \ldots, A_k$ of $k+1$ mutually orthogonal latin squares of order n we obtain a set $A_1', A_2', \ldots, A_k'$ of k mutually orthogonal idempotent latin squares of order n.

Theorem 8.4.13. *Let $(X, \mathcal{A})$ be a pairwise balanced design with n points and m blocks $B_1, B_2, \ldots, B_m$. Let n_i denote the number of points in B_i, $(i = 1, 2, \ldots, m)$. If there exists a set of $t \geq 2$ mutually orthogonal idempotent latin squares of order n_i for each $i = 1, 2, \ldots, m$, then there exists a set of t mutually orthogonal idempotent latin squares of order n.*

Proof. Without loss of generality we assume that the set of points is $X = \{1, 2, \ldots, n\}$. Suppose that

$$A_i^{(1)}, A_i^{(2)}, \ldots, A_i^{(t)}, \quad (i = 1, 2, \ldots, m) \tag{8.29}$$

is a set of t mutually orthogonal idempotent latin squares of order n_i based on the set B_i of n_i points. We assume that the rows and columns of each $A_i^{(r)}$ are indexed by the elements of B_i in the same order and that for each x in B_i the element x occurs in the main diagonal position of $A_i^{(r)}$ corresponding to x. For each $k = 1, 2, \ldots, t$ we define a matrix $A^{(k)}$ of order n by

the element in position (p, p) of $A^{(k)}$ is p, $\quad (p = 1, 2, \ldots, n)$

and

the element in position (p, q) of $A^{(k)}$ equals the element in position (p, q) of $A_i^{(k)}$ where i is chosen so that B_i is the unique line in $\mathcal{A}$ containing both p and q.

We first show that each $A^{(k)}$ is a latin square, and hence an idempotent latin square. Suppose that the element u occurs in both the (p, q_1)

and (p, q_2) positions of $A^{(k)}$ where $q_1 \neq q_2$. The idempotence of the latin squares in (8.29) implies that none of q_1,q_2 and u equals p. Thus there exists a unique block of $\mathcal{A}$ which contains both p and q_1 and a unique block containing both p and q_2, and these two blocks also contain u. Hence p and u are in two distinct blocks contradicting the axiom (L2) for a pairwise balanced block design. Thus no element occurs twice in a row of $A^{(k)}$, and in a similar way one shows that no element occurs twice in a column. Hence $A^{(k)}$ is a latin square.

We now show that $A^{(k)}$ and $A^{(l)}$ are orthogonal for $k \neq l$. Let i and j be points in X. We show that there exist p and q such that the element in position (p, q) of $A^{(k)}$ is i and the element in position (p, q) of $A^{(l)}$ is j. If $j = i$, then we choose p and q equal to i. Now suppose that $i \neq j$. Then there exists a unique block B_r containing both i and j. Because $A_r^{(k)}$ and $A_r^{(l)}$ are orthogonal, there exist p and q in B_r such that the element in position (p, q) of $A_r^{(k)}$ is i and the element in position (p, q) of $A_r^{(l)}$ is j. It now follows that the element in position (p, q) of $A^{(k)}$ is i and the element in position (p, q) of $A^{(l)}$ is j. Hence $A^{(k)}$ and $A^{(l)}$ are orthogonal if $k \neq l$. □

We illustrate the application of Theorem 8.4.13 in obtaining mutually orthogonal latin squares.

Let $(X, \mathcal{A})$ be a projective plane of order 4. Thus X has 21 points and $\mathcal{A}$ has 21 lines, and each line contains 5 points. Since 5 is a prime number, there exists an affine plane of order 5. Therefore by Theorem 8.4.12 there exist four mutually orthogonal latin squares of order 5. Hence there exist three mutually orthogonal idempotent latin squares of order 5. Applying Theorem 8.4.13 we obtain three mutually orthogonal latin squares of order 21. Thus $N(21) \geq 3$. We observe that MacNeish's conjecture asserted that $N(21) = 2$.

Now let $(X, \mathcal{A})$ be a projective plane of order 8. Thus X has 73 points and 73 lines, and each line contains 9 points. Let a, b and c be three points of X not all on the same line. Let X' be obtained from X by removing the three points a, b and c, and let $\mathcal{A}'$ be obtained from $\mathcal{A}$ by removing the points a, b and c from those lines containing them. Then the pair $(X, \mathcal{A}')$ is a pairwise balanced design with 70 points and 73 blocks, and each block contains 7, 8 or 9 points. Because $N(9) = 8 > N(8) = 7 > N(7) = 6$, there exist 5 mutually orthogonal idempotent latin squares of each of the orders 7, 8 and 9. Applying Theorem 8.4.13 we conclude that $N(70) \geq 5$. We observe that Euler's conjecture asserted that $N(70) = 1$.

Theorem 8.4.14. *Let $(X, \mathcal{A})$ be a pairwise balanced design with n points and m blocks $B_1, B_2, \ldots, B_m$. Let n_i equal the number of points in B_i, $(i = 1, 2, \ldots, m)$. Suppose that for some positive integer s with $s \leq m$, the blocks $B_1, B_2, \ldots, B_s$ are pairwise disjoint. If there exists a set of $t \geq 2$ mutually*

orthogonal latin squares of order n_i for each $i = 1, 2, \ldots, s$ and there exists a set of t mutually orthogonal idempotent latin squares of order n_i for each $i = s+1, s+2, \ldots, m$, then there exists a set of t mutually orthogonal latin squares of order n.

Proof. We continue with the notation used in the proof of Theorem 8.4.13, but now the mutually orthogonal latin squares

$$A_i^{(1)}, A_i^{(2)}, \ldots, A_i^{(t)}$$

of order n_i based on the set B_i of points are assumed to be idempotent only for $i = s+1, s+2, \ldots, m$. The matrices $A^{(k)}$ are defined as in the proof of Theorem 8.4.13 with, however, the following change: If p is a point which belongs to B_r for some $r = 1, 2, \ldots, s$ the element in position (p, p) of $A^{(k)}$ equals the element in position (p, p) of $A_r^{(k)}$. One may modify the proof of Theorem 8.4.13 to show that $A^{(1)}, A^{(2)}, \ldots, A^{(k)}$ are orthogonal latin squares of order n. □

The pairwise balanced design $(X', \mathcal{A}')$ with 70 points and 73 lines defined in the paragraph immediately preceding Theorem 8.4.14 has exactly three blocks with 7 points and these blocks are pairwise disjoint. The other lines have 8 or 9 points. Hence Theorem 8.4.14 implies that $N(70) \geq 6$. Applying Theorem 8.4.14 to the pairwise balanced design obtained by removing three noncollinear points from a projective plane of order 4 we obtain $N(18) \geq 2$.

A "complete disproof" of the Euler conjecture can be found in Dénes and Keedwell[1974], Hall[1986], Raghavarao[1971] and Zhu[1982].

Exercises

1. Construct a pair of orthogonal latin squares of order 9.
2. Construct a pair of orthogonal latin squares of order 12.
3. Use the construction in the proof of Theorem 8.4.8 in order to obtain a pair of orthogonal latin squares of order 16.
4. Prove that there exists a symmetric, idempotent latin square of order n if and only if n is odd.
5. Prove that a set of $n-2$ mutually orthogonal latin squares of order n can be extended to a set of $n-1$ mutually orthogonal latin squares of order n. (In fact Shrikhande[1961] has shown that a set of $n-3$ mutually orthogonal latin squares of order n can be extended to a set of $n-1$ mutually orthogonal latin squares of order n.)
6. Show that the latin squares of order $3m+1$ constructed in the proof of Theorem 8.4.8 are indeed orthogonal.
7. Let $(X, \mathcal{A})$ be a projective plane of order n. Let Y be obtained from X by removing four points, no three of which are together on a line in $\mathcal{A}$ and let $\mathcal{A}'$ be obtained by intersecting the lines in $\mathcal{A}$ with Y. Show that $(Y, \mathcal{A}')$ is a pairwise balanced design in which each line contains $n-1$, n or $n+1$ points.
8. Use Exercise 7 and Theorem 8.4.13 to show that $N(69) \geq 5$.
9. Let $N_I(n)$ denote the largest number of mutually orthogonal idempotent latin

squares of order n. Prove that for all positive integers m and n, $N_I(mn) \geq N_I(m)N_I(n)$.

10. Complete the proof of Theorem 8.4.14.

References

R.C. Bose[1938], On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares, *Sankhyā*, 3, pp. 323–338.

R.C. Bose, S.S. Shrikhande and E.T. Parker[1960], Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.*, 12, pp. 189–203.

R.C. Bose 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. Nat. Acad. Sci. U.S.A.*, 45, pp. 734–737.

[1960a], On the composition of balanced incomplete block designs, *Canad. J. Math.*, 12, pp. 177–188.

[1960b], On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Trans. Amer. Math. Soc.*, 95, pp. 191–209.

R.H. Bruck[1951], Finite nets. I. Numerical invariants, *Canad. J. Math.*, 3, pp. 94–107.

[1963], Finite nets. II. Uniqueness and imbedding, *Pac. J. Math.*, 13, pp. 421–457.

J. Dénes and A.D. Keedwell[1974], *Latin Squares and Their Application*, Academic Press, New York.

M. Hall Jr.[1986], *Combinatorial Theory*, 2d edition, Wiley, New York.

D.D. Joshi[1987], *Linear Estimation and Design of Experiments*, Wiley, New York.

H.F. MacNeish[1922], Euler squares, *Ann. Math.*, 23, pp. 221–227.

P.K. Menon[1961], Method of constructing two mutually orthogonal latin squares of order $3n+1$, *Sankhyā* A, 23, pp. 281–282.

E.T. Parker[1959a], Construction of some sets of mutually orthogonal Latin squares, *Proc. Amer. Math. Soc.*, 10, pp. 946–949.

[1959b], Orthogonal Latin squares, *Proc. Nat. Acad. Sci.*, 45, pp. 859–862.

D. Raghavarao[1971], *Construction and combinatorial problems in design of experiments*, Wiley, New York (reprinted[1988] by Dover, Mineola, NY).

S.S. Shrikhande[1961], A note on mutually orthogonal latin squares, *Sankhyā* A, 23, pp. 115–116.

G. Tarry[1900,1901], Le problème de 36 officeurs, *Compte Rendu de l'Association Française pour l'Avancement de Science Naturel*, 1, pp. 122–123, and 2, pp. 170–203.

L. Zhu[1982], A short disproof of Euler's conjecture concerning orthogonal latin squares, *Ars Combinatoria*, 14, pp. 47–55.

8.5 Enumeration and Self-Orthogonality

In this final section we discuss without proof some results concerning the enumeration of latin squares, and latin squares which are orthogonal to their transpose.

One of the major unsolved problems in the theory of latin squares is the determination of the number L_n of distinct latin squares of order n based

on the set $S = \{1, 2, \ldots, n\}$, and more generally the number $L_{r,n}$ of distinct r by n latin rectangles based on S.

The number ℓ_n of normalized latin squares and the number $\ell_{r,n}$ of normalized latin rectangles satisfy, respectively,

$$L_n = n!\ell_n \qquad \text{and} \qquad L_{r,n} = n!\ell_{r,n}.$$

We have $\ell_{1,n} = 1$ and $\ell_{2,n} = D_n$ where

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right)$$

is the number of derangements of $\{1, 2, \ldots, n\}$. The formula of Riordan[1946]

$$\ell_{3,n} = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} D_{n-k} D_k U_{n-2k}$$

gives the number of 3 by n normalized latin rectangles in terms of binomial coefficients, derangements and ménage numbers U_{n-2k}. The number $\ell_{3,n}$ is also known (see Goulden and Jackson[1983]) to be the coefficient of $x^n/n!$ in

$$e^{2x} \sum_{n=0}^{\infty} n! \frac{x^n}{(1+x)^{3n+3}}.$$

This exponential generating function for $\ell_{3,n}$ was generalized by Gessel [1985]. An explicit formula for $L(4, n)$, and thus for $\ell(4, n)$, is given in Athreya, Pranesacher and Singhi[1980] and Pranesachar[1981]. Nechvatal [1981], Athreya, Pranesachar and Singhi[1980], Pranesachar[1981] and Gessel[1987] obtained formulas for $L(r, n)$ in terms of the Möbius function for the partitions of a set. Formulas for the numbers $\ell_n, (n = 1, 2, \ldots, 9)$ are given in Ryser[1963] and Bammell and Rothstein[1975].

Hall[1948] proved that

$$L_{r+1,n} \geq (n-r)!L_{r,n}, \quad (r = 1, 2, \ldots, n-1) \tag{8.30}$$

from which it follows that

$$L_n \geq n!(n-1)! \cdots 2!1!. \tag{8.31}$$

The inequality (8.30) is a consequence of Theorem 7.4.1. Smetaniuk[1982] improved (8.31) by showing that in fact

$$L_n \geq n!L_{n-1}, \quad (n \geq 2). \tag{8.32}$$

It follows from (8.32) that L_n is a strictly increasing function of n. Jucys showed that L_n is a structure constant of an algebra defined on magic squares of order n from which he was then able to express L_n in terms

of the eigenvalues of a certain element of the algebra. Euler, Burkhard and Grommes[1986] investigated the facial structure of a certain polytope associated with latin squares of order n.

It follows from results in section 8.4 that the number $N(n)$ of mutually orthogonal latin squares of order n satisfies

$$N(n) \leq n-1, \quad (n \geq 2)$$

with equality if and only if there exists a projective (or affine) plane of order n. In particular, $N(n) = n-1$ if n is a power of a prime number. Thus we have

$$N(n) = n-1 \text{ if } n = 2,3,4,5,7,8,9$$

and by Tarry's verification we also have $N(6) = 1$. The first undecided value of $N(n)$ is $N(10)$. From the construction of Parker we know that $N(10) \geq 2$. As noted in section 1.3 it has recently been concluded by an extensive computer calculation that there does not exist a projective plane of order 10. Hence it follows that $N(10) \leq 8$. But a little more can be said.

Theorem 8.5.1. *Let $A_1, A_2, \ldots, A_{n-2}$ be $n-2$ mutually orthogonal latin squares of order $n \geq 3$. Then there exists a latin square A_{n-1} of order n such that $A_1, A_2, \ldots, A_{n-2}, A_{n-1}$ are mutually orthogonal latin squares of order n. In particular, $N(n) \neq n-2$ for all $n \geq 3$.*

Proof. Let

$$A^{(t)} = \left[a_{ij}^{(t)} : i,j = 1,2,\ldots,n\right], \quad (t = 1,2,\ldots,n-2).$$

Let $L_1, L_2, \ldots, L_{n-2}$ be the sets of latin lines of these latin squares, and let H and V be, respectively, the set of horizontal and the set of vertical lines. Each point belongs to one line of each of these n classes, each class consists of n pairwise disjoint lines and each line contains n points. It follows that the relation defined on points by

$$(i,j) \sim (i',j')$$

if and only if $i = i'$ and $j = j'$, or there does not exist a line containing both (i,j) and (i',j') is an equivalence relation. This equivalence relation partitions the set $\{(i,j) : i,j = 1,2,\ldots,n\}$ of points into n equivalence classes

$$\ell^1, \ell^2, \ldots, \ell^n \tag{8.33}$$

and each equivalence class ℓ^j contains n points. The equivalence classes (8.33) are the latin lines of a latin square

$$A^{(n-1)} = \left[a_{ij}^{(n-1)}\right]$$

orthogonal to each of $A^{(1)}, A^{(2)}, \ldots, A^{(n-2)}$. More specifically, if we define

$$a_{ij}^{(n-1)} = k$$

if (i,j) belongs to ℓ^k, $(i,j = 1,2,\ldots,n)$, then A^{n-1} is a latin square which is orthogonal to each of $A^{(1)}, A^{(2)}, \ldots, A^{(n-2)}$. □

We therefore have that $N(10) \leq 7$ and more generally that $N(n) \leq n-3$ whenever there does not exist a projective (affine) plane of order n. We remark that the inequality $N(10) \geq 2$ has never been improved. However, the general inequality $N(n) \geq 2, (n > 6)$ has been improved. For example, Guérin has proved that $N(n) \geq 4, (n \geq 53)$, Hanani[1970] has proved that $N(n) \geq 5, (n \geq 63)$ and Wilson[1974] has proved that $N(n) \geq 6, (n \geq 91)$. In addition, Beth[1983], improving a result of Wilson[1974], has shown that

$$N(n) \geq n^{1/14.8} - 2$$

for all n sufficiently large.

A latin square A is called *self-orthogonal* provided A is orthogonal to its transpose A^T. The main diagonal of a self-orthogonal latin square is necessarily a transversal. Because there does not exist a pair of orthogonal latin squares of either of the orders 2 and 6, no latin square of order 2 or 6 can be orthogonal to its transpose. A simple examination reveals that there does not exist a self-orthogonal latin square of order 3. Modifying existing techniques and using some special constructions, Brayton, Coppersmith and Hoffman[1974] have shown how to construct a self-orthogonal latin square of order n for each positive integer n different from 2, 3 and 6. It follows that for those integers n for which there exists a pair of orthogonal latin squares of order n, there exists a self-orthogonal latin square of order n except if $n = 3$.

We now describe a construction of Mendelsohn for a self-orthogonal latin square of order n for all prime powers $n \neq 2, 3$.

We begin with the Galois field $GF(q)$ where $q \neq 2, 3$. There exists an element λ in this field with λ different from 0,1 and 2^{-1}. Let the elements of $GF(q)$ be denoted by $a_1, a_2, \ldots, a_q$. We define a matrix $A = [a_{ij}]$ of order q by

$$a_{ij} = \lambda a_i + (1-\lambda)a_j, \quad (i,j = 1,2,\ldots,n).$$

Because $\lambda \neq 0, 1$, A is a latin square of order q based on the set of elements of $GF(q)$. We now show that A is orthogonal to A^T. If not then there exist i, j, k and l such that

$$\lambda a_i + (1-\lambda)a_j = \lambda a_k + (1-\lambda)a_l \tag{8.34}$$

and

$$\lambda a_j + (1-\lambda)a_i = \lambda a_l + (1-\lambda)a_k. \tag{8.35}$$

Adding (8.34) and (8.35) we obtain

$$a_i + a_j = a_k + a_l. \tag{8.36}$$

Substituting (8.36) into (8.34) and using the fact that $\lambda \neq 2^{-1}$, we get $a_i = a_k$ and $a_j = a_l$. Hence $i = k$ and $j = l$, and A is orthogonal to A^T. A self-orthogonal latin square of order 5 constructed in this way using the field $GF(5) = \{0, 1, 2, 3, 4\}$ of integers modulo 5 and $\lambda = 2$ is

$$A = [a_{ij}] = \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 2 & 1 & 0 & 4 & 3 \\ 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 4 & 3 & 2 \\ 3 & 2 & 1 & 0 & 4 \end{bmatrix}.$$

Here $a_{ij} = 2i - j \bmod 5, (i, j = 0, 1, 2, 3, 4)$.

The symbolic direct product $X \otimes Y$ of matrices X and Y of orders m and n, respectively, satisfies $(X \otimes Y)^T = X^T \otimes Y^T$. Hence the preceding construction and Theorem 8.4.4 can be used to obtain a self-orthogonal latin square of order n for each integer $n > 1$ whose prime factorization does not contain exactly one 2 or exactly one 3.

We conclude with an application of self-orthogonal latin squares to *spouse-avoiding mixed doubles round robin tournaments* as described by Brayton, Coppersmith and Hoffman[1974].

It is desired to arrange a schedule of mixed doubles matches for n married couples which has the following four properties:

(i) In each match two teams, each composed of one man and one woman, compete.
(ii) A husband and wife pair never appear in the same match, as either partners or opponents.
(iii) Two players of the same sex oppose each other exactly once.
(iv) Two players of the opposite sex, if not married to each other, play in exactly one match as partners and in exactly one match as opponents.

In such a tournament each person plays $n - 1$ matches and hence there are a total of $n(n-1)/2$ matches.

Let the couples be labeled $1, 2, \ldots, n$ and let the husband and wife of couple i be M_i and $W_i, (i = 1, 2, \ldots, n)$. Let $A = [a_{ij}]$ be a self-orthogonal latin square of order n based on the set $\{1, 2, \ldots, n\}$. The main diagonal of A is a transversal and without loss of generality we assume that $a_{ii} = i$, $(i = 1, 2, \ldots, n)$. The $n(n-1)/2$ matches

$$\{M_i, W_{a_{ij}}\} \text{ versus } \{M_j, W_{a_{ji}}\}, \quad (1 \leq i < j \leq n)$$

determine a spouse-avoiding mixed doubles round robin tournament. Conditions (i)–(iv) follow from the fact that A is a self-orthogonal latin square of order n with main diagonal $1, 2, \ldots, n$.

Conversely, given a spouse-avoiding mixed doubles round robin tournament, a self-orthogonal latin square $A = [a_{ij}]$ of order n is obtained by defining a_{ii} to be $i, (i = 1, 2, \ldots, n)$ and defining a_{ij} to be k provided W_k is the partner of M_i in the match in which M_i opposes M_j.

Exercises

1. Show that (8.30) is a consequence of Theorem 7.4.1.
2. Construct a self-orthogonal latin square of order 7.
3. Construct a self-orthogonal latin square of order 20.
4. Verify that a spouse-avoiding mixed doubles round robin tournament with n couples gives a self-orthogonal latin square as described at the end of this section.

References

K.B. Athreya, C.B. Pranesachar and N.M. Singhi[1980], On the number of latin rectangles and chromatic polynomial of $L(K_{r,s})$, *Europ. J. Combinatorics*, 1, pp. 9–17.

S.E. Bammel and J. Rothstein[1975], The number of 9×9 latin squares, *Discrete Math.*, 11, pp. 93–95.

T. Beth[1983], Eine Bemerkung zur Abschätzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren, *Abh. Math. Sem. Hamburg*, 53, pp. 284–288.

R.K. Brayton, D. Coppersmith and A.J. Hoffman[1974], Self-orthogonal latin squares of all orders $n \neq 2, 3, 6$, *Bull. Amer. Math. Soc.*, 80, pp. 116–118.

R. Euler, R.E. Burkhard and R. Grommes[1986], On latin squares and the facial structure of related polytopes, *Discrete Math.*, 62, pp. 155–181.

I. Gessel[1985], Counting three-line latin rectangles, *Proc. Colloque de Combinatoire Énumérative*, UQAM, pp. 106–111.

[1987], Counting latin rectangles, *Bull. Amer. Math. Soc. (new Series)*, 16, pp. 79–82.

R. Guérin[1968], Existence et propriétés des carrés latins orthogonaux II, *Publ. Inst. Statist. Univ. Paris*, 15, pp. 215–293.

M. Hall Jr.[1948], Distinct representatives of subsets, *Bull. Amer. Math. Soc.*, 54, pp. 958–961.

H. Hanani[1970], On the number of orthogonal latin squares, *J. Combin. Theory*, 8, pp. 247–271.

A.-A.A. Jucys[1976], The number of distinct latin squares as a group-theoretical constant, *J. Combin. Theory, Ser. A*, 20, pp. 265–272.

J.R. Nechvatal[1981], Asymptotic enumeration of generalized latin rectangles, *Utilitas Math.*, 20, pp. 273–292.

C.R. Pranesachar, Enumeration of latin rectangles via SDR's, *Combinatorics and Graph Theory* (S.B. Rao, ed.), Lecture Notes in Math., 885, Springer-Verlag, Berlin and New York, pp. 380–390.

J. Riordan[1946], Three-line latin rectangles - II, *Amer. Math. Monthly*, 53, pp. 18–20.

H.J. Ryser[1963], *Combinatorial Mathematics*, Carus Mathematical Monograph No. 14, Math. Assoc. of America, Washington, D.C.

B. Smetaniuk[1982], A new construction on latin squares - II: The number of latin squares is strictly increasing, *Ars Combinatoria*, 14, pp. 131–145.

R.M. Wilson[1974], Concerning the number of mutually orthogonal latin squares, *Discrete Math.*, 9, pp. 181–198.

[1974], A few more squares, *Congressus Numerantium*, No. X, pp. 675–680.