Latin Squares

1 Definition and examples

Definition 1. (Latin Square) *An $n \times n$ Latin square, or a latin square of order n, is a square array with n symbols arranged so that each symbol appears just once in each row and each column.*

Example 2. The following are Latin squares.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} I & A & Q & E \\ A & I & E & Q \\ Q & E & I & A \\ E & Q & A & I \end{pmatrix}. \tag{1}$$

It is clear that we only need to study latin squares of order n where the symbols are $1, 2, ..., n$.

Proposition 3. *Any Latin square can be "normalized", so that the first row and column are $1, 2, ..., n$.*

Example 4. Consider

$$\begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 3 & 2 & 4 \\ 4 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \end{pmatrix} \tag{2}$$

We first re-arrange the rows:

$$\begin{pmatrix} 1 & 3 & 2 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 2 & 3 & 1 \end{pmatrix}. \tag{3}$$

Then re-arrange the columns:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}. \tag{4}$$

Example 5. There are one normalized 2×2 Latin squares, one normalized 3×3 latin square, and four normalized 4×4 latin squares.

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}. \tag{5}$$

Remark 6. The number of normalized latin squares for order 5 is 56, for order 6 is 9408, for order 7 is more than 16 million. The number for order 11 is 48 digits. The number for order 12 is not known.

2 Construction of Latin squares

There are several obvious ways of constructing Latin squares.

Theorem 7. *Let n be a positive integer. Let A be the n-by-n array whose entry a_{ij} in row i and column j is*

$$a_{ij} = b_{ij} + 1, \qquad b_{ij} = (i-1) + (j-1) \qquad (\mathrm{mod}\, n) \tag{6}$$

Then A is a Latin square of order n with symbols $\{1, 2, ..., n\}$.

Proof. Exercise. □

Theorem 8. *Let n be a positive integer. Let m be co-prime to n. Let A be the n-by-n array whose entry a_{ij} in row i and column j is*

$$a_{ij} = b_{ij} + 1, \qquad b_{ij} = m\,(i-1) + (j-1) \qquad (\mathrm{mod}\, n). \tag{7}$$

Then A is a Latin square of order n with symbols $\{1, 2, ..., n\}$.

Proof. Exercise. □

Example 9. Consider the case $n = 4$. Then the above methods both give

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}. \tag{8}$$

Exercise 1. How many different normalized 5×5 Latin squares can be constructed using Theorems 7 and 8?

In fact we have much freedom in constructing a Latin square. We now prove that we can simply start from the first row $1, 2, ..., n$, and then add one row at a time, as long as:

i. each row is a permutation of $1, 2, ..., n$;

ii. no symbol is repeated in any column at any step.

Now we prove that this procedure always works, that is we won't get stuck before the square is finished.

At the mth step, each column has already used m symbols from 1, 2, ..., n. Let the set of the remaining symbols in the ith column be denoted S_i. Then the procedure would be able to continue if and only if there is a permutation $\sigma\colon \{1, 2, ..., n\} \mapsto \{1, 2, ..., n\}$ such that $\sigma(i) \in S_i$.

We now turn this into a graph theoretic problem. Consider a graph of order $2\,n$, with vertices denoted $1_L, ...,$ n_L and $1_R, ..., n_R$. Whenever $j \in S_i$, we draw an edge between i_L and j_R. We do not draw any other edge. Then the existence of the aforementioned permutation is equivalent to a "perfect matching", that is n edges that do not share any end points.

To show the existence of such matching, we invoke the following "Hall's marriage theorem", whose proof is postponed to the end of this section.

Theorem 10. (Hall) *Such n edges exist if and only if for every subset $\{i_1, ..., i_l\}$ of vertices of $\{1_L, ..., n_L\}$, the number of vertices adjacent to them (two vertices are adjacent if they are connected by an edge) is no less than l.*

In light of Theorem 10, all we need to show is that for any $\{i_1, ..., i_l\} \subseteq \{1, 2, ..., n\}$, the union $S_{i_1} \cup \cdots \cup S_{i_l}$ has at least l elements. We show now that this condition is satisfied. Notice that $|S_i| = n - m$ for every i. Now if $|S_{i_1} \cup \cdots \cup S_{i_l}| < l$, then there is one symbol in $S_{i_1} \cup \cdots \cup S_{i_l}$ that is repeated at least $n - m + 1$ times in $S_{i_1}, ..., S_{i_l}$. However this is not possible as at the beginning each symbol is repeated exactly n times, and at each step we take away exactly one copy of $1, 2, ..., n$, reducing the number of repetition exactly by one. Therefore at mth step each symbol is repeated exactly $n - m$ times in $S_1, ..., S_n$ and would be repeated no more than $n - m$ times in $S_{i_1}, ..., S_{i_l}$.

Thus ends the proof.

Proof. (of Hall's Marriage Theorem) The necessity of the condition is obvious. In the following we prove sufficiency.

We prove through induction on n. When $n = 1$ the conclusion is obvious. Now assume that the conclusion holds for $1, 2, ..., n$. Consider a graph with vertices $\{1_L, ..., (n+1)_L, 1_R, ..., (n+1)_R\}$ satisfying the above condition. There are two cases.

i. if for every $l \leqslant n$ and every subset $\{i_1, ..., i_l\} \subseteq \{1_L, ..., (n+1)_L\}$ the number of adjacent vertices is at least $l + 1$, then we can "match up" the left vertices and right vertices as follows:

   - Match up 1_L with any adjacent vertex.
   - Let G' be the graph obtained by deleting these two vertices and the edges emanating from them. Then G' has $2\,n$ vertices and still satisfies the assumption of the theorem. By induction hypothesis we can match up the remaining vertices.

     Exercise 2. Prove that G' still satisfies the assumption.

ii. If there is $l \leqslant n$ and a subset $\{i_1, ..., i_l\} \subseteq \{1_L, ..., (n+1)_L\}$ such that the number of adjacent vertices is exactly l, then we can "match up" the vertices as follows.

   - Let the l adjacent vertices be $\{r_1, ..., r_l\} \subset \{1_R, ..., (n+1)_R\}$. As $l \leqslant n$ by induction hypothesis we can match up $\{i_1, ..., i_l\}$ with $\{r_1, ..., r_l\}$.
   - Delete these $2\ l$ vertices and edges connected to them. What remains is a graph G' with $2\ (n + 1 - l)$ vertices. We claim that G' still satisfies the assumption of the theorem. Then there is a subset $\{l_1, ..., l_k\} \subset \{1_L, ..., (n+1)_L\} - \{i_1, ..., i_l\}$ which has less than k adjacent vertices. But then the subset $\{i_1, ..., i_l, l_1, ..., l_k\}$ violates this assumption in the original graph. Contradiction. □

3 Orthogonal latin squares

Definition 11. (Orthogonal latin squares) *Two $n \times n$ latin squares are orthogonal if, when superimposed, each of the n^2 possible pairings of a symbol from each square appears exactly once.*

Example 12. The following two latin squares are orthogonal:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}. \tag{9}$$

Exercise 3. Are the following 5×5 latin squares orthogonal to each other?

$$\begin{pmatrix} A & B & C & D & E \\ C & D & E & A & B \\ E & A & B & C & D \\ B & C & D & E & A \\ D & E & A & B & C \end{pmatrix}, \qquad \begin{pmatrix} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{pmatrix}. \tag{10}$$

Exercise 4. Prove that there are no orthogonal Latin squares of order 2.

Example 13. We want to test the effects of n different quantities of water and n types of fertilizer on the yield of wheat on a certain type of soil. We see that there are n^2 possible combinations of water and fertilizer. The test field is rectangular and subdivided into n^2 plots, one for each of the n^2 possible water-fertilizer combinations. there is no reason to expect that soil fertility is the same throughout the field. Thus, it may very well be that the first row is of high fertility, and therefore a higher yield of wheat will occur, which is not due solely to the quantity of water and the type of fertilizer used on it. We are likely to minimize the influence of soil fertility on the yield of wheat if we insist that each quantity of water occur no more than once in any row and in any column, and similarly that each type of fertilizer occur no more than once in any row and in any column. Thus the application of the n quantities of water on the n^2 plots should determine a Latin square of order n, and also the application of the n types of fertilizer should determine a Latin square B of order n. Since all n^2 possible water-fertilizer combinations are to be treated, when the two Latin squares A and B are juxtaposed all n^2 combinations should occur once. Thus the Latin squares A and B are to be orthogonal.

Theorem 14. *Let n be a prime. Let $r, s \in \{1, 2, ..., n-1\}$ be two different numbers. Define two arrays $A^r = (a^r_{ij})$ and $A^s = (a^s_{ij})$ through*

$$a^r_{ij} = b^r_{ij} + 1, \qquad b^r_{ij} = r\,(i-1) + (j-1) \pmod n, \tag{11}$$

and

$$a^s_{ij} = b^s_{ij} + 1, \qquad b^s_{ij} = s\,(i-1) + (j-1) \pmod n. \tag{12}$$

Then A^r, A^s are orthogonal Latin squares of order n with symbols $\{1, 2, ..., n\}$.

Proof. All we need to show is that each of the n^2 possible pairs appear exactly once. This is equivalent to each of the n^2 possible pairs appear at most once. Thus we need to show that if

$$\begin{aligned} r\,(i-1) + (j-1) &= r\,(k-1) + (l-1) \pmod n \\ s\,(i-1) + (j-1) &= s\,(k-1) + (l-1) \pmod n \end{aligned}$$

then $i = r, j = s$. Without loss of generality assume $r > s$. Then we have

$$(r-s)\,(i-1) = (r-s)\,(k-1) \pmod n \tag{13}$$

As $r - s \in \{1, 2, ..., n-1\}$ and n is prime, then there is $u \in \{1, 2, ..., n-1\}$ such that $u\,(r-s) = 1 \pmod n$. Multiplying both sides of (13) by u we have

$$i - 1 = k - 1 \pmod n \Longrightarrow i = k. \tag{14}$$

It now follows easily that $j = l$. □

Remark 15. We see that for the above construction to work, all we need are

i. r, n are co-prime. So that A^r is a Latin square;

ii. s, n are co-prime. So that A^s is a Latin square;

iii. r, s are co-prime. So that A^r, A^s are orthogonal.

Exercise 5. Construct a pair of orthogonal Latin squares of order 7.

Exercise 6. Show that the construction method in Theorem 14 does not work for $n = 6$.

Exercise 7. Let n be odd. Define $A = (a_{ij})$ and $B = (b_{ij})$ through

$$a_{ij} - 1 = i + j \pmod{n}, \qquad b_{ij} - 1 = i - j \pmod{n}. \tag{15}$$

Prove that A, B form a pair of orthogonal Latin squares.

Remark 16. It can be shown relatively easily that for every n that is not of the form $4k + 2$ there exists at least one pair of orthogonal Latin squares of order n. Euler conjectured that there are no orthogonal latin square pairs when $n = 4k + 2$ for $k \in \mathbb{N}$. He was only right about $n = 6$. It was proved in 1959 by R. C. Bose, S. S. Shrikhande, and E. T. Parker that there are orthogonal latin square pairs for all $n = 4k + 2$ with $k \geqslant 2$.