# Lecture 1: Latin Squares!



## 1 Introduction

**Definition.** A **latin square** of order $n$ is a $n \times n$ array, filled with symbols $\{1, \dots n\}$, such that no symbol is repeated twice in any row or column.

**Example.** Here are all of the latin squares of order 2:

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

How many are there of order 3? Well, look at the following matrix:

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

It's pretty easy to see that permuting rows and columns can get us to 12 distinct latin squares; conversely, by doing so we can achieve any possible arrangment of the first row and column, which uniquely forces the remaining $2 \times 2$ square's values.

Enumerating all of the latin squares of order 4 is a much more arduous task, as there are 576 distinct such latin squares. (HW) Using symmetry arguments similar to the above, can you find (not explicitly!) all of these latin squares?

In our example above, we used a number of symmetry arguments to find the latin squares of order 3; consequently, we can kind-of regard these latin squares as all being the "same," up to various permutations of their rows. This motivates the following definition:

**Definition.** Two latin squares $A$ and $B$ are called **equivalent** iff a sequence of permutations of the form

1. $R_{ij}$, the permutation that swaps rows $i$ and $j$,
2. $C_{ij}$, the permutation that swaps columns $i$ and $j$,
3. $S_{ij}$, the permutation that swaps symbols $i$ and $j$,
4. $RC$ the three permutations that swaps all of the rows for all of the columns,
5. $RS$ the three permutations that swaps all of the rows for all of the symbols,
6. $CS$ the three permutations that swaps all of the columns for all of the symbols,

can transform $A$ into $B$.

**Example.** Under our equivalence relation above, we have that the

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

by swapping the third and fourth rows.

Conversely, take this matrix $M$ and write it as a $3 \times 4$ array, where the first, second, and third rows correspond to the rows, columns, and symbols, and the columns correspond to the $4^2$-distinct row-column-symbol pairings in $M$.

$$\left[\begin{array}{c|cccccccccccccccc} R & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ C & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \\ S & 1 & 2 & 3 & 4 & 2 & 3 & 4 & 1 & 3 & 4 & 1 & 2 & 4 & 1 & 2 & 3 \end{array}\right]$$

Call such a matrix an **orthogonal array** $OA(n, 3)$ for any $n$. It is hopefully clear that these correspond uniquely with latin squares.

Why do we mention these objects? Because they give us an excellent way to visualize swapping the rows and columns of our latin square: just permute the corresponding rows of our above matrix!

$$\left[\begin{array}{c|cccccccccccccccc} R & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ C & 1 & 2 & 3 & 4 & 2 & 3 & 4 & 1 & 3 & 4 & 1 & 2 & 4 & 1 & 2 & 3 \\ S & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \end{array}\right]$$

The corresponding matrix to this orthogonal array is then given by

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

which is another matrix equivalent to $M$.

It bears noting that there are inequivalent matrices: for example, consider the following pair of matrices:

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

It is not too hard to show (HW!) that these are inequivalent under our above relations.

**Proposition 1** *Latin squares exist for all $n$.*

**Proof.** Behold!

$$\begin{bmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ n & 1 & \dots & n-2 & n-1 \end{bmatrix}$$

Alternately: take any group of order $n$, and look at its multiplication table. It's not too difficult to show (HW!) that this will always create a latin square. Are there latin squares that don't arise in this way?

# 2 Two Themes: MOLS and PLS

In this class, we are going to explore a pair of questions about latin squares, which we describe in this section:

## 2.1 Mutually Orthogonal Latin Squares

**Definition.** Take a pair of $n \times n$ latin squares $M_1, M_2$, and look at all of the ordered pairs

$$\{ (x, y) \mid x \text{ is the } (i,j)\text{-th entry in } M_1, \text{ and } y \text{ is the } (i,j)\text{-th entry in } M_2. \}$$

If all of these pairs are distinct, then we say that $M_1$ and $M_2$ are **mutually orthogonal**.

**Example.** Consider the following pair of $4 \times 4$ latin squares:

$$\begin{bmatrix} A & K & Q & J \\ Q & J & A & K \\ J & Q & K & A \\ K & A & J & Q \end{bmatrix} \qquad \begin{bmatrix} \spadesuit & \heartsuit & \diamondsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \\ \diamondsuit & \clubsuit & \spadesuit & \heartsuit \end{bmatrix}$$

If we superimpose these two squares, we get the square

$$\begin{bmatrix} A\spadesuit & K\heartsuit & Q\diamondsuit & J\clubsuit \\ Q\clubsuit & J\diamondsuit & A\heartsuit & K\spadesuit \\ J\heartsuit & Q\spadesuit & K\clubsuit & A\diamondsuit \\ K\diamondsuit & A\clubsuit & J\spadesuit & Q\heartsuit \end{bmatrix};$$

as all of the cards represented here are distinct, we can see that $M_1$ and $M_2$ are mutually orthogonal.

**Question 2** *(Euler's Thirty-Six Office Problem) Suppose that we have 36 officers, and split them into 6 regiments all of size 6. Suppose furthermore that within each regiment we give each office a rank from 1 (cadet) to 6 (brigadier). Is there a way to arrange these 36 officers into a 6 by 6 latin square, so that in every row and every column, every rank and regiment is represented?*

In the language of orthogonal latin squares, Euler's question becomes the following:

**Question 3** *Are there a pair of mutually orthogonal* $6 \times 6$ *latin squares?*

As it turns out, there aren't! Motivated by this result, Euler made the following conjecture:

**Conjecture 4** *If* $n \equiv 2 \mod 4$*, then there are no pairs of* $n \times n$ *mutually orthogonal latin squares.*

This conjecture stood until 1959-1960, when Bose, Shrikhande, and Parker (rather surprisingly!) disproved Euler's conjecture for every case of $n > 6$:

**Theorem 5** *There are mutually orthogonal latin squares for every $n \neq 2, 6$.*

In this class, we'll do some partial work on this theorem, and construct mutually orthogonal $n \times n$ latin squares for many values of $n$.

## 2.2 Partial Latin Squares

**Definition.** A **partial latin square** of order $n$ is a $n \times n$ array, filled with either blanks or symbols $\{1, \ldots n\}$, such that no symbol is repeated twice in any row or column.

**Example.** Here are a pair of partial $4 \times 4$ latin squares:

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

One natural question we can ask about partial latin squares is the following: when can we complete them into filled-in latin squares? There are trivially cases wherein we cannot complete a partial latin square: the second square above, for example, can't be completed to a full latin square. However, there are many conditions under which we can complete latin squares, as we'll show throughout this class (and, in particular, now:)

**Theorem 6** *Let $M$ be a partial $n \times n$ latin square in which the first $k$ rows are completely filled and the rest of $M$ is blank. Then $M$ can be completed to a $n \times n$ latin square.*

**Proof.** Recall Hall's marriage theorem (week 2, graph theory), which says the following:

**Theorem 7** *Suppose that $G = (A, B)$ is a bipartite graph that satisfies **Hall's property**:*

$$(\ddagger): \qquad \forall H \subset A \text{ or } H \subset B, |N(H)| \geq |H|.$$

*Then $G$ has a 1-factor.*

(HW: if you haven't proven this, do so!)

Create a graph $(A, B)$ as follows:

- $A = \{1 \ldots n\}$,
- $B = \{B_1 \ldots B_n\}$,
- $B_j =$ the collection of elements that don't occur in column $j$, and
- draw an edge from $i \in A$ to $B_j \in B$ iff $i \in B_j$.

By construction, the degree of any $B_j$ is just the number of elements that don't occur in a given column — i.e. n-k. As well, the degree of any $i \in A$ is just the number of columns that $i$ doesn't show up, which is *also* n-k; so this is a $n-k$ regular bipartite graph! As any such graph satisfies Hall's property, by Hall's marriage theorem, there is a 1-factor: i.e. a bijection between elements in $\{1, \ldots n\}$ and columns where they do not occur. Use this 1-factor to add a row to $M$, and repeat to complete $M$.

**Theorem 8** *(Ryser's theorem:) Suppose that $M$ is a $n \times n$ partial latin square with the elements $m_{ij}$ filled in iff $1 \leq i \leq r$, $1 \leq j \leq s$. Then $M$ can be completed.*

**Proof.** So: first consider the following useful lemma, which you're encouraged to prove:

**Lemma 9** *If $A$ is a $n \times n$ integral matrix, then for any $d$ there are matrices $B_1, \ldots B_d$ such that*

$$A = B_1 + \ldots + B_d,$$

*where the matrices $B_i$ are all integral $n \times n$ matrices that have the same entries, row and column sums, and sum over all entries as $\frac{1}{d}A$, up to rounding up or down.*

Given this lemma, our proof is in fact rather easy: let $B$ be the $0-1$ matrix defined by letting $b_{ij} = 1$ iff the element $j$ isn't in the $i$-th row in $A$. Then, the sum of the $i$-th row of $B$ is just the number of elements the $i$-th row is missing – i.e. $n-s$. Similarly, the sum of the $j$-th column of $B$ is just the number of times that $j$ goes missing in $A$, which is also bounded above by $n-s$ (as there are at most $s$ copies of $j$ in our matrix, as at most one $j$ can live in any row.)

Apply the lemma to write

$$B = L^{(s)} + \ldots + L^{(n)},$$

where the $L_i$ are 0-1 matrices with the same row/column sums as $\frac{1}{n-s}B$ – in other words, matrices where there is exactly 1 one in every row and at most 1 in every column.

What have we done? Well: the matrix $B$'s entries were a way of keeping track of which rows we could put certain elements in, and the splitting apart of $B$ into the $L_j$'s then gives us a way of dividing this data up into possible columns! Motivated by this, fill in all of the cells $(i,j) \in M$, $i \in \{1 \ldots n\}, j \in s+1 \ldots n\}$, by setting $(i,j) = k$ iff $l_{ik}^{(j)} = 1$. Because $l_{ik}^{(j)} = 1$ iff the element $k$ doesn't show up in row $i$, this will always work; thus, we can complete $M$ to a latin rectangle! By our earlier result, we can complete this to a latin square.