Two latin squares of the same size are said to be **orthogonal** if every possible ordered pair of symbols occurs exactly once when we overlay the two squares.

Example:

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

Overlaying these two matrices gives:

$$\begin{pmatrix} 11 & 22 & 33 & 44 \\ 23 & 14 & 41 & 32 \\ 34 & 43 & 12 & 21 \\ 42 & 31 & 24 & 13 \end{pmatrix}$$

Suppose $L_1 \perp L_2$.

Consider the n cells of L_2 which contain the same symbol, s say. The entries in the corresponding cells of L_1 must all be different, by orthogonality.

Since s occurs once in each row and column of L_2, the corresponding entries in L_1 form a transversal.

Thrm: A latin square of order n possesses an orthogonal mate iff it has n disjoint transversals.

A Cayley table of a group has an orthogonal mate iff it has a transversal.

A pair of orthogonal latin squares of order n is equivalent to an $n^2 \times 4$ orthogonal array.

$$\begin{pmatrix} 11 & 22 & 33 & 44 \\ 23 & 14 & 41 & 32 \\ 34 & 43 & 12 & 21 \\ 42 & 31 & 24 & 13 \end{pmatrix}$$

Each row of the array consists of
(i) row
(ii) column
(iii) symbol in first square
(iv) symbol in second square

$$\begin{pmatrix} \mathbf{11}\mathit{11} \\ \mathbf{12}\mathit{22} \\ \mathbf{13}\mathit{33} \\ \mathbf{14}\mathit{44} \\ \mathbf{21}\mathit{23} \\ \mathbf{22}\mathit{14} \\ \mathbf{23}\mathit{41} \\ \mathbf{24}\mathit{32} \\ \mathbf{31}\mathit{34} \\ \mathbf{32}\mathit{43} \\ \mathbf{33}\mathit{12} \\ \mathbf{34}\mathit{21} \\ \mathbf{41}\mathit{42} \\ \mathbf{42}\mathit{31} \\ \mathbf{43}\mathit{24} \\ \mathbf{44}\mathit{13} \end{pmatrix}$$

For each extra column we add to the orthogonal array, we add another latin square.

A set of mutually orthogonal latin squares (MOLS) is a set of latin squares each pair of which is orthogonal.

A set of m MOLS of order n is equivalent to an $n^2 \times (m+2)$ orthogonal array.

Thrm: Not more than $n-1$ mutually orthogonal latin squares of order n exist.

Proof: Wlog the symbols in the first rows of all the squares are $1, 2, \ldots, n$ in natural order.

The symbols occurring in the first cell of the second rows of the squares must then all be different by orthogonality.

No square can have 1 as the symbol in the first cell of the second row.

Thus, there are at most $n-1$ squares. $\square$

Complete sets of MOLS

Since no larger set is possible, a set of $n-1$ MOLS of order n is said to be **complete**.

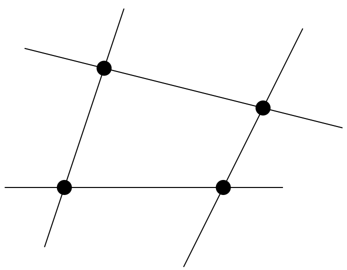
Example: A complete set of MOLS of order 4

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

Projective Planes

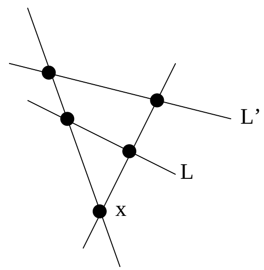
A projective plane is a set of "points" and "lines" such that every pair of lines meet in exactly one point and every pair of points are joined by a unique line.

To avoid degeneracy we also insist that there is some set of 4 points, no 3 of which are collinear.



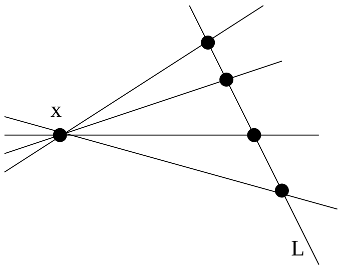
Thrm: Each line in a projective plane has the same number of points on it.

Proof: Consider two lines L and L' and a point x not on either line (Exercise: prove such a point exists, by using non-degeneracy).



There is a bijection from points on L to points on L'. Simply map $y \in L$ to the point on L' which is collinear with x and y. $\square$

Suppose there are $n+1$ points on every line



Choose a line L and a point x not on L.
Through each of the $n+1$ points on L there is a line to x.
These $n+1$ lines intersect only at x, so they contain
$(n+1)(n+1)-n = n^2+n+1$ points.

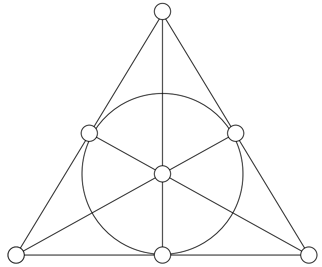
There are no other points in the plane. If there was another point z then there would be a line through x and z and this line must meet L.

This also shows that there are $n+1$ lines through every point.

The order of a plane

A finite projective plane, with $n+1$ points on each line is said to be of **order** n.
It will have n^2+n+1 lines, n^2+n+1 points and $n+1$ lines through every point.

Example:



The Fano plane has order 2. It has 7 lines and 7 points; 3 points per line and 3 lines through each point.

Duality

The definition of a projective plane P is symmetric between points and lines. So we can rename the points to be lines and vice versa! This gives a new projective plane, called the **dual** of P.

Some planes (eg. the Fano plane) are isomorphic to their dual. Others are not.

For each projective plane we can define a $(0,1)$ **incidence matrix**. The rows correspond to the points and the columns correspond to the lines.

We put a 1 if the point lies on the line and a 0 otherwise.

This matrix, P, belongs to $\Lambda^{n+1}_{n^2+n+1}$.
It satisfies the matrix equation $PP^T = P^TP = J + nI$.

To find the dual projective plane, we simply take the transpose.

Alternatively, we can think of a bipartite **incidence graph**. The two types of vertices correspond to points and lines, and the edges indicate that a point lies on a line. The dual is found by interchanging the roles of the two parts of the graph.

Thrm: There exists a finite projective plane of order n iff there exists a complete set of MOLS of order n.

Proof: We show how to build an $n^2 \times (n+1)$ orthogonal array O from a projective plane P of order n (and leave it as an exercise to show that the construction can be reversed).
Choose one line L of P. For each of the $n+1$ points $\{x_0, x_1, x_2, \ldots, x_n\}$ on L we will build one column of O. There are n^2 points not on L and for each we will build one row of O.
Consider a particular x_i. Label the lines, other than L, which pass through x_i as $\ell_1, \ell_2, \ldots, \ell_n$. Then in column i, the entry corresponding to a point y not on L is the index of the line ℓ_1, $\ell_2, \ldots$, or ℓ_n which contains y.
Now, since each ℓ_j contains n points other than x_j we see that each column of O contains n different symbols n times each. Also, since two points lie on a unique line the columns of O are orthogonal. $\square$

For what values of n does there exist a projective plane of order n?

Thrm: If n is a power of a prime then a plane exists.

Let $\mathbb{F}$ be a finite field of order n and let x generate the (cyclic) multiplicative group of $\mathbb{F}$. Define $\alpha_i = x^i$ for $i \in \{1, 2, \ldots, n-1\}$ and $\alpha_n = 0$.
For each $k \in \{1, 2, \ldots, n-1\}$ we construct a latin square L_k in which

$$(L_k)_{ij} = \alpha_i + \alpha_k \alpha_j$$

Exercise: Prove this construction works.

If $n \in \{6, 10\}$ then a plane does NOT exist.
The proof is by exhaustion.

Thrm: [Bruck-Ryser] If $n \equiv 1, 2 \bmod 4$ and a projective plane of order n exists then there exist integers a and b such that $n = a^2 + b^2$.

So, for example, there is no projective plane of order 14.

The smallest unresolved order is 12.

Exercise: For which orders below 50 does this theorem rule out the existence of a projective plane? For which orders below 50 are we still unsure about the existence of a projective plane?

The Euler conjecture

Thrm: The Cayley table of a cyclic group of order $n \equiv 2 \bmod 4$ has no orthogonal mate.

Proof: It has no transversals. $\square$

Euler famously conjectured that there are no orthogonal latin squares of order $n \equiv 2 \bmod 4$.
He knew this was true for $n = 2$ and $n = 6$.

Around 1960 Bose, Shrikhande and Parker showed that in every other case Euler was wrong!
In fact, Chowla, Erdös & Straus showed that the size of the largest set of MOLS of order n tends to ∞ as $n \to \infty$.