Mathematics 366 **Latin Squares and Experimental Designs** A. Hulpke

A *latin square* is an n by n matrix $A = \left(a_{ij}\right)$, with entries $a_{ij} \in \{1,2,\ldots,n\}$, such that every row, and every column, each number occurs exactly once. (Thus the filled out sudoku is a 9×9 latin square with some extra conditions.) latin squares are used for example for agricultural experiments: suppose we want to test the efficiency of different types of seeds, as well as different amounts of fertilizers.

We could simply plant the seeds in different columns of a plot of land, and apply the fertilizer in rows as depicted here:

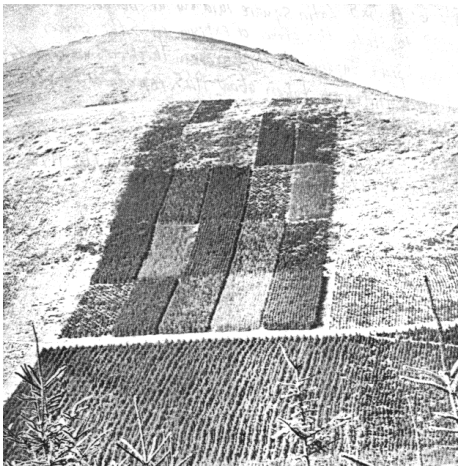
Fertilizer	Seed Type		
Low	A	B	C
Medium	A	B	C
High	A	B	C

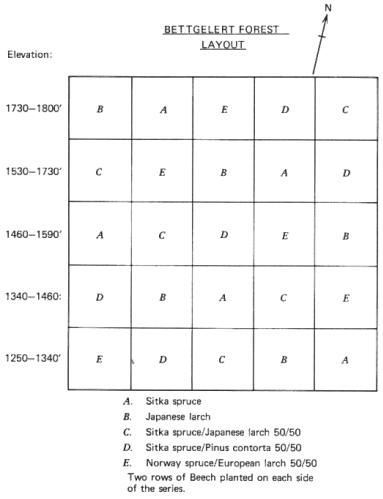
There is a problem with this approach. There might be an underlying variability of the land (a variation of soil, different amount of sun, difference in irrigation) which we don't know but which will skew our results. To neutralize such unknown effects, we plant the seeds instead to being form of a latin square. Now any difference of soil impacts the different experiments evenly, and can be canceled out in a statistical analysis. For example:

Fertilizer	Seed Type		
Low	A	B	C
Medium	C	A	B
High	B	C	A

(Note that in general it is not possible to obtain such a latin square by simple shifting of rows as in this example.)

This approach is used in practice. The following picture [1] shows a 5×5 latin square of trees planted on a hill in Wales in 1929 to determine the effect of elevation on different species of trees.





[1] from J F Box, *R. A. Fisher: The Life of a Scientist*

Now imagine we want to run a different experiment on the same plot of land. If we plant again in the same layout there is the danger that residues from the previous experiment impact the result. We therefore want to plant on a different latin square in which does not correlate with the first. This leads us to the following definition:

Definition: Two latin squares $A = (a_{ij})$ and $B = (b_{ij})$ are called *orthogonal* if for any pair k, l of numbers there is a unique position i, j such that $a_{i,j} = k$ and $b_{i,j} = l$. A set $\{A_1, \ldots, A_k\}$ of latin squares is called a set of *mutually orthogonal latin squares* (MOLS) if any pair of latin squares is orthogonal. The following is an example of two orthogonal latin squares:

Aa	Bb	Cc
Cb	Ac	Ba
Bc	Ca	Ab

Can we always find such orthogonal Latin squares, and if so what is the maximum size of a set of MOLS of order n?
We first observe that we cannot get more than $n-1$: Suppose $A_1, \ldots, A_r$ are MOLS. By permuting (relabelling) the entries (which will not affect latinicity or orthogonality) we can assume that all have entry 1 in position $1,1$. Each square must contain $n-1$ further 1s. None of these can be in the first row or in the first column, thus there are $(n-1)^2$ available positions. But – by orthogonality – no two squares may have any of these 1s in the same position. Thus each square "uses up" $n-1$ positions, which means there cannot be more than $n-1$ such squares.
If we have a finite field F with n elements (one can show that they exist for any prime power n) this best possible situation is in fact reached:
We will use the elements of F to index the rows and columns of each matrix. For each non-zero element m construct a matrix A_m for which the i, j-entry is $(A_m)_{i,j} := im + j$. For example, for $F = \mathbb{Z}_3 = \{0, 1, 2\}$ we get

$$A_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}.$$

Then each A_m is a latin square: If $im + j_1 = im + j_2$ (same entry in a row) we get $j_1 = j_2$, if $i_1 m + j = i_2 m + j$ (same entry in a column) we get $i_1 m = i_2 m$ from which we can deduce $i_1 = i_2$ **because m is invertible**. To show orthogonality, suppose we have two matrices A_m and A_n for $n \neq m$ and we want to find the positions for which $(A_m)_{i,j} = a$ and $(A_n)_{i,j} = n$. This yields the system:

$$\begin{aligned} im + j &= a \\ in + j &= b \end{aligned}$$

The corresponding matrix is $\begin{pmatrix} m & 1 \\ n & 1 \end{pmatrix}$ and has determinant $m - n \neq 0$, thus the system has a unique solution (i, j).