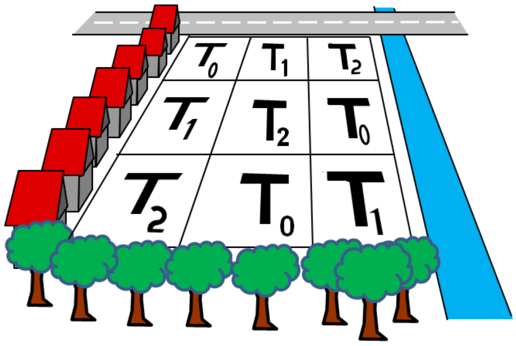
Chapter 10. Section 4



Latin Squares

We are given three crop treatments (fertilisers, pesticides or whatever) called T_0, T_1 and T_2. We want to test their effectiveness on crops experimentally. Rather than just growing one field for each treatment, we grow three for each, arranged so that each treatment is tried in different positions relative to external sources of variance. In the illustration on the right these outside influences are: road, river, wood and village.

This is an example of a kind of experimental design called a **combinatorial design**. What we achieved in the illustration is formalised as follows:

A **Latin square** of order n is an $n \times n$ matrix with entries in an n-letter **alphabet** (usually $\{0, 1, \ldots, n-1\}$ but it could be any collection of n symbols) in which every letter appears in every row and every column.

0	1	2
1	2	0
2	0	1

The illustration above shows a Latin square of order 3. Written down as a mathematical object we have the matrix shown on the right (although it is a matrix it is customary to write Latin squares down as $n \times n$ tables). It is in **standard form** meaning it has been arranged so that the first row and column are in ascending order.

Latin squares exist and can be constructed for all orders. To see this, observe that the multiplication table of a group of order n (otherwise known as its **Cayley table** is a Latin square.

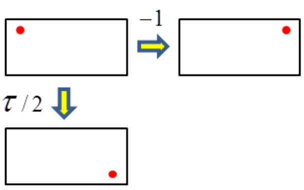
Examples (1) The Latin square of order 3 given above is the Cayley table of C_3, the rotational symmetries of an equilateral triangle, under the mapping $0 \rightarrow 0$, $\tau/3 \rightarrow 1$, $2\tau/3 \rightarrow 2$, from rotations by zero, $\tau/3$ and $2\tau/3$ radians, respectively.[1] It is worth writing the Cayley table out explicitly as shown above right. Of course multiplication for rotational symmetries means 'followed by': the operation is commutative and is usually written as +. Thus $0 + \tau/3 = \tau/3$ because rotation by zero radians followed by a 1-third turn ($\tau/3$ radians) gives a total rotation of ... $\tau/3$ radians.

+	0	$\tau/3$	$2\tau/3$
0	0	$\tau/3$	$2\tau/3$
$\tau/3$	$\tau/3$	$2\tau/3$	0
$2\tau/3$	$2\tau/3$	0	$\tau/3$

(2) The rotational group, C_4, of the square, is isomorphic to addition modulo 4. This additive group, usually denoted by $\mathbb{Z}_4$ has the Cayley table shown on the right (again the group is abelian, so its operation is written + rather than $\times$) and this directly supplies a standard form Latin square on $\{0, 1, 2, 3\}$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(3) The Klien-4 group, consisting of the symmetries of a non-square rectangle under rotation and reflection, gives an order 4 Latin square. If we represent rotation and reflection as $\tau/2$ and -1, respectively, as shown below left, then the Cayley table (again abelian) is as shown below right, together with the matching standard form Latin square on $\{0, 1, 2, 3\}$.



+	0	-1	$\tau/2$	$-\tau/2$
0	0	-1	$\tau/2$	$-\tau/2$
-1	-1	0	$-\tau/2$	$\tau/2$
$\tau/2$	$\tau/2$	$-\tau/2$	0	-1
$-\tau/2$	$-\tau/2$	$\tau/2$	-1	0

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

Note that the red spot on the rectangle above left is there to show how the reflection and rotation operations act: the rectangle itself is, by definition, invariant under these symmetries.

[1]With τ=1 turn; I cannot bring myself to refer to a one-third turn as two-thirds π, since I learnt that it is quite respectable not to - see www.theoremoftheday.org/Annex/taumanifesto.html.

Turning to the usual combinatorial question: can we count Latin squares? The answer is No: this is an unsolved problem. Any Latin square can be transformed into a standard form Latin square by reordering the rows and columns independently: this does not affect which letters appear in each row and column. So we can ask how many $n \times n$ standard form Latin squares there are. For small n we get:

n	1	2	3	4	5	6	7	8
#	1	1	1	4	56	9408	16942080	$\approx 5 \times 10^{11}$

We observe that the 3×3 square on page 1 was the *only* possible square. The two order 4 groups we gave in examples 2 and 3 on page 1 are the only order 4 groups, whereas the above table says there are four standard form Latin squares of order 4. However three of these are obtained by relabelling the Cayley table of the group C_4.

For instance, if we apply the permutation (1 2) (in disjoint cycle notation) to the elements of $\mathbb{Z}_4$ then we get the multiplication table shown near right. Now mapping $0, 1, 2, 3$ to a, c, b, d, respectively gives the 4×4 Latin square shown far right which is a different standard form Latin square from the two on page 1.

+	0	2	1	3
0	0	2	1	3
2	2	1	3	0
1	1	3	0	2
3	3	0	2	1

$\longrightarrow$

a	b	c	d
b	a	d	c
c	d	b	a
d	c	a	b

Note that we have used actual alphabet letters instead of numbers which is perfectly legitimate since it does not affect the defining property of Latin squares (each letter in each row and each column). And standard form is still well-defined, but in terms of alphabetical order instead of numerical order. By the way, the name 'Latin square' comes from the fact that their original definition, in the 17th century, used the Latin alphabet as entries.

So there are two groups of order 4 and two standard form Latin squares or order 4, up to permutations of the n-letter alphabet: these are called **isometries**. Perhaps, up to isometry, Latin squares are the *same* as Cayley tables?

In fact they are not: the multiplication table shown on the right cannot be the Cayley table of a group because it does not obey the **associative law**. For example, $(a \times b) \times d = c \times d = a$ which is not equal to $a \times (b \times d) = a \times c = d$. In fact Latin squares are the multiplication tables of a more general structure than a group: a **quasigroup** (usually pronounced 'kwarzy-group') is a group except that it need not be associative and may lack an identity element; a **loop** is a group except it need not be associative. Latin squares are multiplication tables of quasigroups; Latin squares in standard form are multiplication tables of loops. The multiplication table above right is an example of a loop.

$\times$	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	d	1	a	c
c	c	b	d	1	a
d	d	c	a	b	1

Orthogonal Latin Squares and Transversals

We return to our original crop treatment example. Suppose we want to re-run our experiment in the same 3×3 plot layout. A new source of variance arises: what if treatment T_0 remains in the soil and 'contaminates' future treatments? The solution is to find a new Latin square which, combined with the original one, offers every ordered pair (T_i, T_j). Now we can control for each possible way in which one previous treatment may contaminate a following treatment.

A pair of $n \times n$ Latin squares L_1 and L_2 with alphabet $\{0, \ldots, n-1\}$ are said to be **orthogonal** if, when they are superimposed, every ordered pair from the alphabet appears in some entry. More formally, for each of the n^2 ordered pairs (i, j), $0 \leq i, j \leq n-1$, there is a row r_i and column c_j such that L_1 has i in row r_i and column c_j and L_2 has j in row r_i and column c_j.

This is illustrated below at (a) where our original Latin square is given an orthogonal mate. At (b)

0	1	2
1	2	0
2	0	1

1	0	2
2	1	0
0	2	1

01	10	22
12	21	00
20	02	11

(a)

0		
	2	
		1

	1	
		0
2		

		2
1		
	0	

(b)

this original Latin square is **decomposed** into three **transversals**: each transversal has three non-empty cells which together contain the whole alphabet; together the three transversals make up the complete Latin square.

Lemma An $n \times n$ Latin square L has an orthogonal mate if and only if it has a decomposition into n transversals.

Proof. Assume without loss of generality that the alphabet of L is $\{0, \ldots, n-1\}$.

$\Leftarrow$: replace the entries in the i-th transversal with copies of i. Then together the resulting squares make up a Latin square and this is necessarily orthogonal to L.

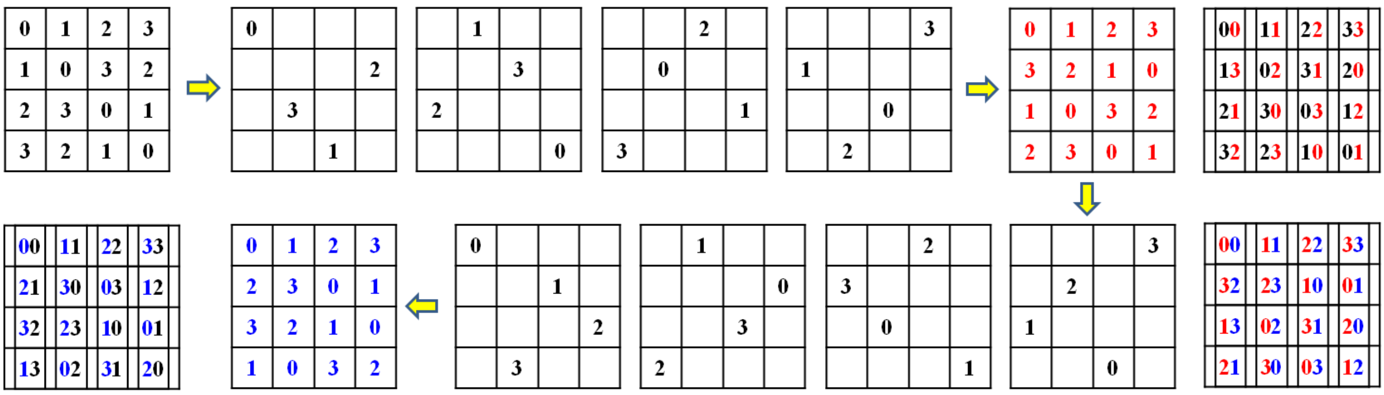
$\Rightarrow$: suppose L has an orthogonal mate L'. Fix j, $0 \leq j \leq n-1$ and identify the collection of row-column pairs which give all ordered pairs (i, j), $0 \leq i \leq n-1$. The corresponding entries in L are necessarily a transversal. $\square$

As usual in combinatorics we ask: does an orthogonal mate always exist? And then we ask: if one does exist, how many can there be?

The answer to the first question is NO. Indeed a Latin square need not have even *one* transversal, let alone n of them. In fact the addition table of $\mathbb{Z}_n$ is a Latin square for all $n \geq 1$ and this has no transversal when n is even. You may check the table of $\mathbb{Z}_4$ on page 1 and convince yourself this is true for $n = 4$. For odd values of n counterexamples are harder to find and it has only recently been proved that Latin squares having no orthogonal mate exist for all orders except 1 and 3.

When an orthogonal mate *does* exist for a Latin square we can ask how many mates there can be. One specific form this question can take is to ask for the largest collection of **mutually orthogonal Latin squares** or **MOLS** for short, meaning that each pair in the collection is orthogonal.

We show below that the Cayley table of the Klein-4 group forms part of a collection of three MOLS, by first finding a decomposition of K_4 into transversals to build it an orthogonal mate and then finding a decomposition of the mate into transversals *which simultaneously correspond to a different transversal decomposition for K_4*.



Certainly this construction is not obvious! Nevertheless, if n is a prime power there is a systematic way to achieve a set of $n-1$ MOLS. In our example $n = 2^2$ and we found $4 - 1 = 3$ MOLS. One of the most famous conjectures in combinatorics asserts that for all other n the maximum possible number of MOLS is less than $n-1$. Currently this is not even confirmed for $n = 12$. Certainly we cannot find *more* than $n-1$:

Lemma A set of MOLS of order n can have size at most $n-1$.

Proof. Suppose the first Latin square is in standard form, using the alphabet $\{0, \ldots, n-1\}$. Put the first row of all the other Latin squares into ascending order by permutating their alphabets: this cannot affect orthogonality. Consider the first entry of row 2: none of the squares can have 0 in this position by definition; and only the first square can have 1 in this position because the pair $(1, 1)$ is already found in the first rows from each pair of squares. So there are only $n-2$ possible values that can be taken by the squares other than the first. $\square$