Latin squares

R. A. Bailey
r.a.bailey@qmul.ac.uk

G. C. Steward lecture,
Gonville and Caius College, Cambridge

7 March 2013

A stained glass window in Caius

photograph by
J. P. Morgan

And on the opposite side of the hall

R. A. Fisher promoted the use of Latin squares in experiments while at Rothamsted (1919–1933) and his 1935 book *The Design of Experiments*.

What is a Latin square?

Definition
Let n be a positive integer. A Latin square of order n is an $n \times n$ array of cells in which n symbols are placed, one per cell, in such a way that each symbol occurs once in each row and once in each column.

The symbols may be letters, numbers, colours, . . .

A Latin square of order 7

This Latin square was on the cover of the first edition of *The Design of Experiments*.

Why this one?
It does not appear in the book. It does not match any known experiment designed by Fisher.

Why is it called 'Latin'?

What are Latin squares used for?

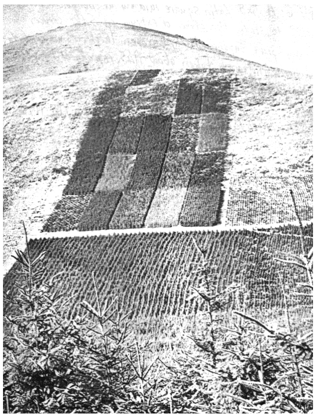
Agricultural field trials, with rows and columns corresponding to actual rows and columns on the ground (possibly the width of rows is different from the width of columns).

"...on any given field agricultural operations, at least for centuries, have followed one of two directions, which are usually those of the rows and columns; consequently streaks of fertility, weed infestation, etc., do, in fact, occur predominantly in those two directions."

R. A. Fisher,
letter to H. Jeffreys,
30 May 1938
(selected correspondence edited by J. H. Bennett)

This assumption is dubious for field trials in Australia.

A forestry experiment



Experiment on a hillside near Beddgelert Forest, designed by Fisher and laid out in 1929

Other sorts of rows and columns: animals

An experiment on 16 sheep carried out by François Cretté de Palluel, reported in *Annals of Agriculture* in 1790. They were fattened on the given diet, and slaughtered on the date shown.

slaughter date	Breed: Ile de France	Beauce	Champagne	Picardy
20 Feb	potatoes	turnips	beets	oats & peas
20 Mar	turnips	beets	oats & peas	potatoes
20 Apr	beets	oats & peas	potatoes	turnips
20 May	oats & peas	potatoes	turnips	beets

Other sorts of rows and columns: plants in pots

An experiment where treatments can be applied to individual leaves of plants in pots.

height	plant 1	2	3	4
1	*A*	*B*	*C*	*D*
2	*B*	*A*	*D*	*C*
3	*C*	*D*	*A*	*B*
4	*D*	*C*	*B*	*A*

Other designs related to Latin squares

Another experiment where treatments can be applied to individual leaves of plants in pots.

height	plant 1	2	3	4	5	6	7	8
1	*A*	*B*	*C*	*D*	*A*	*B*	*D*	*C*
2	*B*	*A*	*D*	*C*	*C*	*A*	*B*	*D*
3	*C*	*D*	*A*	*B*	*D*	*C*	*A*	*B*
4	*D*	*C*	*B*	*A*	*B*	*D*	*C*	*A*

Unequal replication

X	*P*	*D*	*M*	*G*	*X*
M	*X*	*P*	*G*	*X*	*D*
D	*G*	*M*	*P*	*X*	*X*
G	*D*	*X*	*X*	*M*	*P*
X	*M*	*X*	*D*	*P*	*G*
P	*X*	*G*	*X*	*D*	*M*

Unequal replication on the ground

Latin squares with another system of blocks

Behrens introduced 'gerechte' designs in 1956.

A	B	C	E	D	F
D	E	F	B	C	A
B	C	E	F	A	D
F	D	A	C	B	E
C	F	D	A	E	B
E	A	B	D	F	C

Sudoku puzzle

8			9	1				
3		7	6			9		1
	9							
5				3		7		9
	3	4		8		2	6	
9		2		7				4
							5	
1		3			2	4		7
				9	1			3

Fill the grid with the numbers 1 to 9 so that each row, column and 3 × 3 block contains the numbers 1 to 9.

Ciphers

Vigenère used this method for spies at court in 16th century; so did various air forces in WWII.

key	A	C	E	H	K	N	T
	plain text						
A	A	T	K	N	E	H	C
C	T	C	N	K	H	E	A
E	K	N	E	T	A	C	H
H	N	K	T	H	C	A	E
K	E	H	A	C	K	T	N
N	H	E	C	A	T	N	K
T	C	A	H	E	N	K	T

key 'word': KEN CAN CHEAT

plain	A T T A C K T H E T E C H A T T E N
key	K E N C A N C H E A T K E N C A N C
send	E H K T T T A H E C H H T H A C C E

How to construct a Latin square: cyclic method

1. Choose an integer m with $1 \leq m < n$ and m coprime to n.
2. Put the symbols in the first row in any order.
3. In each successive row, move all symbols m places to the right (pretending that the first column is immediately to the right of the last column).

Example ($n = 7$ and $m = 2$)

F	C	A	G	D	E	B
E	B	F	C	A	G	D
G	D	E	B	F	C	A
C	A	G	D	E	B	F
B	F	C	A	G	D	E
D	E	B	F	C	A	G
A	G	D	E	B	F	C

How to construct a Latin square: group method

1. Let G be a group of order n.
2. Label the rows by the elements of G, in any order.
3. Label the columns by the elements of G, in any order (it does not have to be the same as the row order).
4. In the cell in row g and column h put symbol gh.

The cyclic method is a special case of the group method, using the cyclic group C_n of order n.

Example ($n = 6$ and $G = S_3$)

	(123)	(13)	1	(23)	(132)	(12)
1	(123)	(13)	1	(23)	(132)	(12)
(12)	(13)	(123)	(12)	(132)	(23)	1
(23)	(12)	(132)	(23)	1	(13)	(123)
(132)	1	(23)	(132)	(12)	(123)	(13)
(123)	(132)	(12)	(123)	(13)	1	(23)
(13)	(23)	1	(13)	(23)	(12)	(132)

How to construct a Latin square: product method

Suppose that $n = rs$ where $r \neq 1$ and $s \neq 1$.

1. Let L be a Latin square of order r with letters $A_1, \ldots, A_r$.
2. For $i = 1, \ldots, r$, replace each occurrence of A_i by a Latin square of order s with letters $s(i-1)+1, \ldots, s(i-1)+s$.

If you always use the same Latin square M of order s, replacing its letter B_j by $s(i-1)+j$ for $j = 1, \ldots, s$, this is called $L \otimes M$.

Example ($r = 2$ and $s = 3$)

A_1	A_2
A_2	A_1

1	2	3	4	5	6
2	3	1	5	6	4
3	1	2	6	4	5
4	6	5	1	2	3
6	5	4	3	1	2
5	4	6	2	3	1

Steiner triple systems

Definition
A Steiner triple system of order n is a set of size n together with some subsets of size three (called triples) such that if i and j are distinct elements of the set then there is exactly one triple containing both i and j.

Example ($n = 7$)

{1,2,4} {2,3,5} {3,4,6} {4,5,7} {1,5,6} {2,6,7} {1,3,7}

Homework
Prove that, if there exists a Steiner triple system of order n, then n is congruent to 1 or 3 modulo 6.

Constructing a Latin square from a Steiner triple system

1. In row i and column i put symbol i.
2. If $i \neq j$ and $\{i,j,k\}$ is a triple then put symbol k in row i and column j.

Example ($n = 7$)

{1,2,4} {2,3,5} {3,4,6} {4,5,7} {1,5,6} {2,6,7} {1,3,7}

	1	2	3	4	5	6	7
1	1	4	7	2	6	5	3
2	4	2	5	1	3	7	6
3	7	5	3	6	2	4	1
4	2	1	6	4	7	3	5
5	6	3	2	7	5	1	4
6	5	7	4	3	1	6	2
7	3	6	1	5	4	2	7

How many different Latin squares of order n are there?

Are these two Latin squares the same?

A	B	C
C	A	B
B	C	A

1	2	3
3	1	2
2	3	1

To answer this question, we will have to insist that all the Latin squares use the same symbols, such as $1, 2, \dots, n$.

Reduced Latin squares, and equivalence

Definition
A Latin square is reduced if the symbols in the first row and first column are $1, 2, \dots, n$ in natural order.

Definition
Latin squares L and M are equivalent if there is a permutation f of the rows, a permutation g of the columns and permutation h of the symbols such that

symbol s is in row r and column c of L
$\iff$
symbol $h(s)$ is in row $f(r)$ and column $g(c)$ of M.

Theorem
If there are m reduced squares in an equivalence class of Latin squares of order n, then the total number of Latin squares in the equivalence class in $m \times n! \times (n-1)!$.

Order 3

There is only one reduced Latin square of order 3.

1	2	3
2	3	1
3	1	2

Order 4

There are two equivalence classes of Latin squares of order 4.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

cyclic

3 reduced squares

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

non-cylic group

more 2×2 Latin subsquares

1 reduced square

MacMahon's counting

"... problem of the Latin square. I have given the mathematical solution and you will find it in my *Combinatory Analysis*, Vol. 1, p. 250.

For $n = 2$,	no.	of	arrangements is	2
3,	″	″	″	12
4,	″	″	″	576
5,	″	″	″	149 760

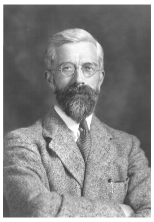
and I have not calculated the numbers any further."

P. A. MacMahon
letter to R. A. Fisher,
30 July 1924
(selected correspondence edited by J. H. Bennett)

Correction

Fisher divided by $n! \times (n-1)!$ to obtain the number of reduced Latin squares, which he pencilled in.

				all	reduced
For $n = 2$,	no.	of	arrangements is	2	1
3,	″	″	″	12	1
4,	″	″	″	576	4
5,	″	″	″	149 760	52



By September 1924 they had agreed that the number of reduced Latin squares of order 5 was 56, not 52.

Euler had already published this result in 1782; and so had Cayley in a 1890 paper called 'On Latin squares'.

Order 5

There are two equivalence classes of Latin squares of order 5.

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

cyclic

no 2×2 Latin subsquare

6 reduced squares

1	2	3	4	5
2	1	4	5	3
3	4	5	1	2
4	5	2	3	1
5	3	1	2	4

not from a group

has a 2×2 Latin subsquare

50 reduced squares

Numbers of reduced Latin squares

order	cyclic	non-cyclic group	non-group	all	equivalence classes
2	1	0	0	1	1
3	1	0	0	1	2
4	3	1	0	4	2
5	6	0	50	56	2
6	60	80	9268	9408	22
7	120	0	16941960	16942080	564
8	1260	1500	$> 10^{12}$	$> 10^{12}$	1676267
9	6720	840	$> 10^{15}$	$> 10^{15}$	$> 10^{12}$
10	90720	36288	$> 10^{25}$	$> 10^{25}$	$> 10^{18}$
11	36288	0	$> 10^{34}$	$> 10^{34}$	$> 10^{26}$

6: Frolov, 1890; Tarry, 1900; Fisher and Yates, 1934
7: Frolov (wrong); Norton, 1939 (incomplete); Sade, 1948; Saxena, 1951
8: Wells, 1967   9: Baumel and Rothstein, 1975
10: McKay and Rogoyski, 1995   11: McKay and Wanless, 2005

Leonhard Euler, Swiss mathematician

Euler's problem of the 36 officers

There are 36 officers, from

- 6 regiments
- 6 ranks,

one officer from each rank in each regiment.

Can the officers be paraded in a 6×6 square in such a way that

- there is one officer of each regiment in each row
- there is one officer of each regiment in each column
- there is one officer of each rank in each row
- there is one officer of each rank in each column?

Euler watches the officers trying to arrange themselves

Cartoon by Neill Cameron

An easier problem: 9 officers

regiments

A	B	C
C	A	B
B	C	A

ranks

α	β	γ
β	γ	α
γ	α	β

When the two Latin squares are superposed,
each Latin letter occurs exactly once with each Greek letter.

$A\ \alpha$	$B\ \beta$	$C\ \gamma$
$C\ \beta$	$A\ \gamma$	$B\ \alpha$
$B\ \gamma$	$C\ \alpha$	$A\ \beta$

Euler called such a square a 'Graeco-Latin square'.
The name 'Latin square' seems to be a back-formation from this.

Pairs of orthogonal Latin squares

Definition
A pair of Latin squares of order n are orthogonal to each other if, when they are superposed, each letter of one occurs exactly once with each letter of the other.

We have just seen a pair of orthogonal Latin squares of order 3.

Question (Euler, 1782)
For which values of n does there exist a pair of orthogonal Latin squares of order n?

Theorem
If n is odd, or if n is divisible by 4, then there is a pair of orthogonal Latin squares of order n.

Proof of theorem: (i)

Proof. (i) n is odd.
If n is odd, consider the following cyclic Latin squares L_1 and L_2, whose symbols are $1, \dots, n$ considered as integers modulo n.

row	column	letter in L_1	letter in L_2
i	j	$i+j$	$i-j$

Suppose that cells (i_1, j_1) and (i_2, j_2) have the same letter in L_1 and the same letter in L_2. Then

$$i_1 + j_1 = i_2 + j_2 \quad \text{and} \quad i_1 - j_1 = i_2 - j_2.$$

Hence $\quad i_1 - i_2 = j_2 - j_1 = j_1 - j_2,$

so $\quad 2(j_1 - j_2) = 0 \text{ modulo } n,$

so $j_1 - j_2 = 0$ modulo n, because n is odd,
so $j_1 = j_2$ and $i_1 = i_2$. Hence L_1 is orthogonal to L_2. □

Proof of theorem: (ii)

Proof. (ii) $n = 4$ or $n = 8$.

$A\alpha$	$B\beta$	$C\gamma$	$D\delta$
$B\gamma$	$A\delta$	$D\alpha$	$C\beta$
$C\delta$	$D\gamma$	$A\beta$	$B\alpha$
$D\beta$	$C\alpha$	$B\delta$	$A\gamma$

$A\alpha$	$B\beta$	$C\gamma$	$D\delta$	$E\varepsilon$	$F\zeta$	$G\eta$	$H\theta$
$B\gamma$	$A\delta$	$D\alpha$	$C\beta$	$F\eta$	$E\theta$	$H\varepsilon$	$G\zeta$
$C\varepsilon$	$D\zeta$	$A\eta$	$B\theta$	$G\alpha$	$H\beta$	$E\gamma$	$F\delta$
$D\eta$	$C\theta$	$B\varepsilon$	$A\zeta$	$H\gamma$	$G\delta$	$F\alpha$	$E\beta$
$E\delta$	$F\gamma$	$G\beta$	$H\alpha$	$A\theta$	$B\eta$	$C\zeta$	$D\varepsilon$
$F\beta$	$E\alpha$	$H\delta$	$G\gamma$	$B\zeta$	$A\varepsilon$	$D\theta$	$C\eta$
$G\theta$	$H\eta$	$E\zeta$	$F\varepsilon$	$C\delta$	$D\gamma$	$A\beta$	$B\alpha$
$H\zeta$	$G\varepsilon$	$F\theta$	$E\eta$	$D\beta$	$C\alpha$	$B\delta$	$A\gamma$

□

Proof of theorem: (iii)

(iii) n is divisible by 4.
If n is divisible by 4 then $n = 4^r \times 8^s \times m$ where m is odd, $r \geq 0$, $s \geq 0$ and $r + s > 0$.

If L_1 is orthogonal to L_2 and M_1 is orthogonal to M_2, then $L_1 \otimes M_1$ is orthogonal to $L_2 \otimes M_2$. □

Euler's conjecture

Conjecture
If n is even but not divisible by 4, then there is no pair of orthogonal Latin squares of order n.

This is true when $n = 2$, because the two letters on the main diagonal must be the same.

Euler was unable to find a pair of orthogonal Latin squares of order 6.

Theorem (Tarry, 1900)
There is no pair of orthogonal Latin squares of order 6.

Proof.
Exhaustive enumeration by hand. □

The end of the conjecture

Theorem (Bose and Shrikhande, 1959)
There is a pair of orthogonal Latin squares of order 22.

Theorem (Parker, 1959)
If $n = (3q-1)/2$ and $q-3$ is divisible by 4 and q is a power of an odd prime, then there is a pair of orthogonal Latin squares of order n. In particular, there are pairs of orthogonal Latin squares of orders 10, 34, 46 and 70.

Theorem (Bose, Shrikhande and Parker, 1960)
If n is not equal to 2 or 6, then there exists a pair of orthogonal Latin squares of order n.

Mutually orthogonal Latin squares

Definition
A collection of Latin squares of the same order is mutually orthogonal if every pair is orthogonal.

Example ($n = 4$)

$A\alpha 1$	$B\beta 2$	$C\gamma 3$	$D\delta 4$
$B\gamma 4$	$A\delta 3$	$D\alpha 2$	$C\beta 1$
$C\delta 2$	$D\gamma 1$	$A\beta 4$	$B\alpha 3$
$D\beta 3$	$C\alpha 4$	$B\delta 1$	$A\gamma 2$

How many mutually orthogonal Latin squares?

Theorem
If there exist k mutually orthogonal Latin squares $L_1, \ldots, L_k$ of order n, then $k \leq n-1$.

Proof.
For $i = 1, \ldots, k$, let m_i be the column in the second row of L_i that has the same letter as the first column of the first row.
Then $m_i \neq 1$, because L_i is a Latin square.
If $i \neq j$, then $m_i \neq m_j$, because L_i is orthogonal to L_j.
So $1, m_1, \ldots, m_k$ are all different, and so $1 + k \leq n$. □

When is the maximum achieved?

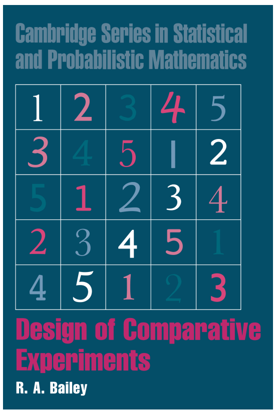
Theorem
If n is a power of a prime number then there exist $n-1$ mutually orthogonal Latin squares of order n.

For example, $n = 2, 3, 4, 5, 7, 8, 9, 11, 13, \ldots$.

Theorem (Lam, Thiel and Swiercz, 1989)
There is no set of 9 mutually orthogonal Latin squares of order 10.

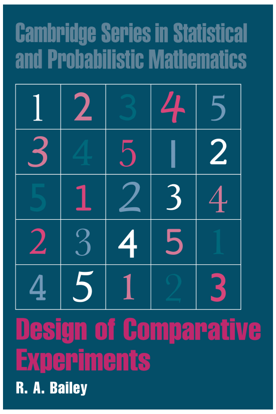
Question
Does there exist a set of 3 mutually orthogonal Latin squares of order 10?

The cover of a book



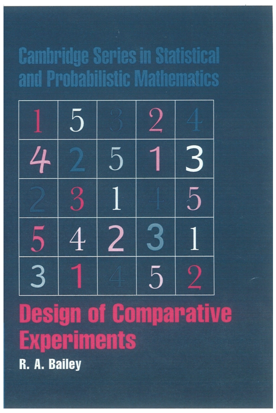
There are 3 mutually orthogonal Latin squares of order 5:
one on 1, 2, 3, 4, 5;
one on colours;
one on fonts.

Who designed the cover?



This was designed by someone in the art department at C.U.P. It is a lovely idea, but . . .

Who designed the cover? —Not me!



. . .
their original version had been randomized in such a way that the cells no longer formed Latin squares.
I had to correct it at a very late stage.

Who designed the cover of Fisher's book?

My theory is that the cover was designed by someone in the art department at Oliver and Boyd . . .
who had read enough to know what a Latin square was but did not know any of the standard methods of constructing Latin squares,
and so made this one by trial and error.