

応用数学特論 II (集中講義)

DAY 1 LATIN SQUARES & ORTHOGONAL ARRAYS

盧 曉南 (山梨大学)

Xiao-Nan LU (University of Yamanashi)

Aug. 25, 2021

Kobe University

Outline

- ① Latin squares, quasigroups, groups
- ② Completion of Latin rectangles
- ③ Mutually orthogonal Latin squares (MOLS)
- ④ Transversals of Latin squares
- ⑤ Orthogonal arrays and applications to designs of experiments

Definition of Latin squares

Latin squares

An $n \times n$ array A with entries in $[n] = \{1, 2, \dots, n\}$ is a **Latin square** (ラテン方格) if

- In each row, each column, every symbol in $[n]$ appears once.

The integer n is called the **order** (位数) of A .

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

A Latin square of order 4

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

A Latin square of order 5

Groupoid and quasigroup

Groupoid

- X : a nonempty set
- $(x, y) \mapsto z = x \circ y, x, y, z \in X$.
- \circ : binary operator on X .

The operator is **closed** under \circ . (X, \circ) is a **groupoid** (厝群).

Quasigroup

A groupoid (X, \circ) is a **quasigroup** (擬群) if

- for any $a, b \in X$, there exists unique $x, y \in X$ such that

$$a \circ x = b \quad \text{as well as} \quad y \circ a = b$$

Quasigroups defined by Latin squares

- $A = (a_{i,j})$: Latin square
- Define \circ by $i \circ j = a_{i,j}$, $i, j \in [n]$.
- $([n], \circ)$ is a quasigroup.

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

A Latin square of order 4

- Latin square (in combinatorics) \iff quasigroup (in algebra)

Loops and groups (in algebra)

- **identity** (單位元) e : $x \circ e = x$ and $e \circ x = x$ for any $x \in X$.
- **loop** \iff quasigroup + identity
- **associative law** (結合律): $(x \circ y) \circ z = x \circ (y \circ z)$ for any $x, y, z \in X$.
- **group** (群) \iff loop + associative law

groupoid $\xrightarrow{+\text{Latin property}}$ quasigroup $\xrightarrow{+\text{identity}}$ loop $\xrightarrow{+\text{associative law}}$ group

Cyclic group (under addition)

(Additive) cyclic group

A finite **cyclic group** (巡回群) of **order** (位数) n is

- The set of additions of “1” (**generator**; 生成元), where 0 is the identity.

$$C_n = \{e = 0(\text{~~=1 \times 0~~}), 1, 1 + 1, 1 + 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{n-1}\}$$

- $\underbrace{1 + 1 + \dots + 1}_n = e = 0$ (identity)

• $(C_n, +)$ is a cyclic group.

• $(\mathbb{Z}_n, +) \simeq (C_n, +)$

Cyclic group (under multiplication)

(Multiplicative) cyclic group

A finite **cyclic group** (巡回群) of **order** (位数) n is

- The set of multiplications of g (**generator**; 生成元), where $g^0 = 1$ is the identity.

$$C_n = \{e = g^0 (= 1), g^1, g^2, g^3, \dots, g^{n-1}\}$$

- $g^n = e = 1$ (identity)

Examples of cyclic groups: [Jupyter Notebook](#)

Permutations and symmetric group

Permutation

A **permutation** (置換) σ on a set $X = [n]$ is defined as a bijection from X to itself.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1^\sigma & 2^\sigma & \cdots & n^\sigma \end{pmatrix}$$

We say σ **acts on** $x \in X$.

#permutation = $n!$

Symmetric group

- The set of all permutations of $[n]$ form a group called the **symmetric group** (对称群).
- The group operation is the **composition**, say $x^{\sigma\tau} = (x^\sigma)^\tau$ for $\sigma, \tau \in S_n$, $x \in [n]$.

Example of symmetric group

Example ($S_3 = \{\sigma_0, \sigma_1, \dots, \sigma_5\}$, i.e., all the permutations on $X = [3]$)

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = () = \text{id.}$$

$$|S_3| = 3! = 6$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \ 2) \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \ 3) \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \ 3)$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3) \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \ 3 \ 2)$$

E.g., the operator between permutations is performed as:

$$\sigma_1 \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5, \quad \text{whereas} \quad \sigma_2 \sigma_1 = \sigma_4.$$

Outline

- ① Latin squares, quasigroups, groups
- ② Completion of Latin rectangles
- ③ Mutually orthogonal Latin squares (MOLS)
- ④ Transversals of Latin squares
- ⑤ Orthogonal arrays and applications to designs of experiments

Latin rectangles

Latin rectangles

A $k \times n$ ($k < n$) array A with entries in $[n] = \{1, 2, \dots, n\}$ is a **Latin rectangles** (ラテン長方形) if in each row, each column, every symbol in $[n]$ appears at most once.

1	2	3	4
2	1	4	3

A Latin square of size 2×4

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

A Latin square of size 4×5

Completion of Latin rectangles

Theorem

Any $k \times n$ Latin rectangle can be extended to a $(k + 1) \times n$ Latin rectangle.

Proof: Let S_i denote the set of symbols not occurring in the i -th columns of the Latin rectangle. Let $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$. Then, the proof completes if we can choose $s_i \in S_i$ such that s_i ($1 \leq i \leq n$) are pairwise distinct.

Corollary

Any $k \times n$ Latin rectangle can be extended to a Latin square.

Examples: [Jupyter Notebook](#)

Example of Latin rectangle completion

1	2	3	4	5
2	1	4	5	3

$$S_1 = \{3, 4, 5\}$$

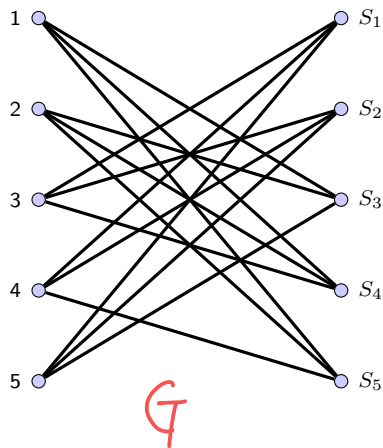
$$S_2 = \{3, 4, 5\}$$

$$S_3 = \{1, 2, 5\}$$

$$S_4 = \{1, 2, 3\}$$

$$S_5 = \{1, 2, 4\}$$

二部グラフ
bipartite graph



Example of Latin rectangle completion

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

$$S_1 = \{3, 4, 5\}$$

$$S_2 = \{3, 4, 5\}$$

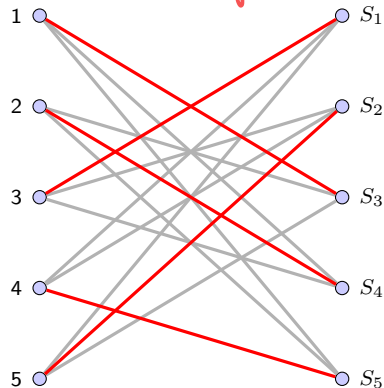
$$S_3 = \{1, 2, 5\}$$

$$S_4 = \{1, 2, 3\}$$

$$S_5 = \{1, 2, 4\}$$

G の
完全
2-4-5

red edges: perfect
matching of G



Example of Latin rectangle completion

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

$$S_1 = \{4, 5\}$$

$$S_2 = \{3, 4\}$$

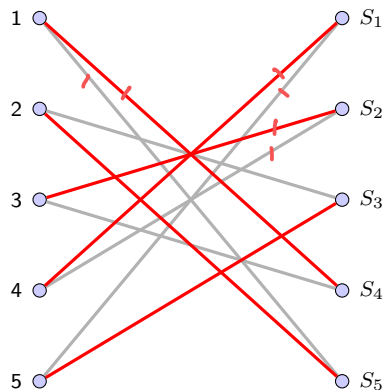
$$S_3 = \{2, 5\}$$

$$S_4 = \{1, 3\}$$

$$S_5 = \{1, 2\}$$

$$N_G(\{S_1, S_2\}) = \{4, 5, 3\}$$

$$N_G(\{1\}) = \{S_4, S_5\}$$



Hall's marriage theorem

- \mathcal{S} : a family of subsets of a finite set X
- \mathcal{S} satisfies **Hall's condition** (ホール条件) if for any $\mathcal{W} \subseteq \mathcal{S}$,

$$\left| \bigcup_{A \in \mathcal{W}} A \right| \geq |\mathcal{W}|.$$

- A set T of size $|T| = |\mathcal{S}|$ that intersects each $S \in \mathcal{S}$ in exactly one point is called a **System of Distinct Representatives** (SDR). 相互代表系.

Hall's marriage theorem (ホールの結婚定理), 1935

\mathcal{S} has an SDR iff \mathcal{S} satisfies Hall's condition.

Corollary

If $|S| = k$ for each $S \in \mathcal{S}$, then \mathcal{S} (said to be **k -uniform**) has an SDR.

Graph theoretic formulation for Hall's marriage theorem

- V and U are vertex sets such that $V \cap U = \emptyset$.
- A **bipartite graph** $G = (V \cup U, E)$ is a graph with no edge within V or U .
- A **matching** M is a subset of E such that no two edges in M have common endpoints.
- A **V -perfect matching** is a matching covering all the vertices in V .
- If $|V| = |U| = n$, a V -perfect matching is simply a **perfect matching** which has n edges.
- For $W \subseteq V$, let $N_G(W)$ denote the **neighborhood** of W in G , i.e., the set of all vertices in U adjacent to some vertex in W .

Hall's marriage theorem (ホールの結婚定理) for graph matching

There is a V -perfect matching iff for each subset W of V ,

$$|N_G(W)| \geq |W|.$$

Outline

- 1 Latin squares, quasigroups, groups
- 2 Completion of Latin rectangles
- 3 Mutually orthogonal Latin squares (MOLS)**
- 4 Transversals of Latin squares
- 5 Orthogonal arrays and applications to designs of experiments

Orthogonality of two Latin squares

$$L_1 =$$

<i>A</i>	<i>K</i>	<i>Q</i>	<i>J</i>
<i>K</i>	<i>A</i>	<i>J</i>	<i>Q</i>
<i>Q</i>	<i>J</i>	<i>A</i>	<i>K</i>
<i>J</i>	<i>Q</i>	<i>K</i>	<i>A</i>

$$L_2 =$$

♠	♦	♥	♣
♥	♣	♠	♦
♣	♥	♦	♠
♦	♠	♣	♥

$$L_1 \boxplus L_2 =$$

<i>A</i> ♠	<i>K</i> ♦	<i>Q</i> ♥	<i>J</i> ♣
<i>K</i> ♥	<i>A</i> ♣	<i>J</i> ♠	<i>Q</i> ♦
<i>Q</i> ♣	<i>J</i> ♥	<i>A</i> ♦	<i>K</i> ♠
<i>J</i> ♦	<i>Q</i> ♠	<i>K</i> ♣	<i>A</i> ♥

where $L_1 \boxplus L_2$ denotes the superposition of L_1 and L_2 .

Orthogonality

Two Latin squares L_1 and L_2 are **orthogonal** if each possible pair appears once in $L_1 \boxplus L_2$.



Mutually orthogonal Latin squares (MOLS)

MOLS

Latin squares L_1, \dots, L_k are **mutually orthogonal** if each pair of them are orthogonal.

- $N(n) := \max\{k \in \mathbb{N} : \text{there exists } k \text{ MOLS of order } n\}$

Theorem

$$N(n) \leq n - 1.$$

Proof: [» Handwritten Notes](#)

Theorem

For any prime power q , $N(q) = q - 1$.

Proof will be given after the notion of “finite fields” being proposed.

Product construction for MOLS

Theorem

- A_1, A_2 : MOLS of order n
- B_1, B_2 : MOLS of order m

Then $A_1 \otimes B_1$ and $A_2 \otimes B_2$ are MOLS of order mn , where \otimes denotes Kronecker product.

Proof: [▶ Handwritten Notes](#)

- In general, $N(mn) \geq \min\{N(n), N(m)\}$.

Theorem

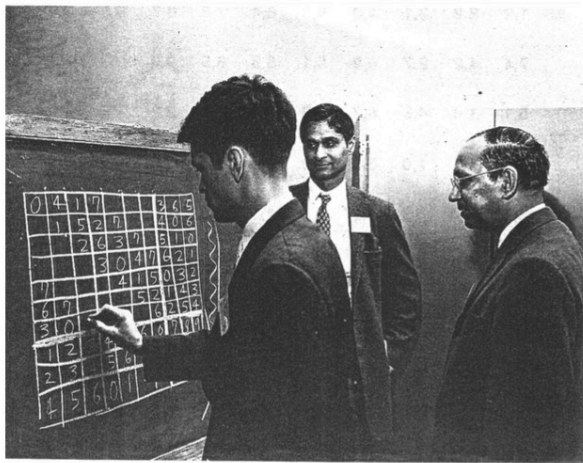
For any $n \equiv 0, 1, 3 \pmod{4}$, $N(n) \geq 2$.

Euler's conjecture on MOLS

Euler's conjecture (1782)

For $n = 4k + 2$, there does **not** exist MOLS of order n .

- In 1901, nonexistence for $n = 6$ was proved.
- In 1959, Parker, Shrikhande, and Bose proved that for all $n = 4k + 2$ except $n = 2, 6$, there **does** exist MOLS of order n .



The End of the Euler Conjecture:
Dr. E. T. Parker, Prof. S. S. Shrikhande and Prof. R. C. Bose.
 (Reprinted from *The New York Times*, April 26, 1959, with
 permission from New York Times Pictures.)

1,2	2,3	3,1	4,6	5,9	6,4	7,8	8,7	9,5	0,0
7,4	4,2	2,7	0,9	6,1	5,8	8,5	9,0	3,3	1,6
5,1	1,4	4,5	6,7	0,8	8,0	9,3	2,2	7,6	3,9
0,7	7,1	1,0	3,8	8,3	9,2	4,4	5,6	1,2	6,5
3,5	5,7	7,3	8,2	9,4	1,1	0,6	4,9	6,0	2,8
2,0	0,5	5,2	9,1	7,7	3,6	1,9	6,3	4,8	8,4
4,3	3,0	0,4	5,5	2,6	7,9	6,2	1,8	8,1	9,7
8,9	9,8	6,6	2,4	3,2	0,3	5,0	7,5	1,7	4,1
6,8	8,6	9,9	7,0	1,5	4,7	2,1	3,4	0,2	5,3
9,6	6,9	8,8	1,3	4,0	2,5	3,7	0,1	5,4	7,2

A counterexample to Euler's conjecture: 2 MOLS of order 10. This corresponds to the pair on the cover of *Scientific American*, November 1959.

Recursive constructions for MOLS

Theorem

For any $0 \leq u \leq t$,

$$N(mt + s) \geq \min\{N(m), N(m + 1), N(t) - 1, N(\textcolor{red}{s})\}.$$

Proof: [» Handwritten Notes](#) (if times permits)

Theorem

For any $n \geq 3$, $n \neq 6$, we have $N(n) \geq 2$.

Proof: [» Handwritten Notes](#)

Results and problems on $N(n)$

- (Bruck–Ryser, 1949) $N(n) \neq n - 1$ for infinitely many n . E.g. $n = 6, 14, 21, 22, 30, \dots$
- (Parker, Shrikhande, Bose, 1959) For any $n \notin \{2^*, 6^*\}$, $N(n) \geq 2$.
- (Wallis, 1986) For any $n \notin \{2^*, 3^*, 6^*, 10, 14\}$, $N(n) \geq 3$.
- (Shrikhande, 1961) For $n \geq 4$, if $N(n) \geq n - 3$ then $N(n - 3) \geq n - 1$.

Prime power conjecture

$N(n) = n - 1$ if and only if n is a prime power.

- (Lam, Thiel, Swiercz, 1989; Bright, et. al, 2019–2020) $N(10) < 9$. $\implies 2 \leq N(10) \leq 6$
- For large enough n , using analytic number theory (sieve methods),
 - ▶ (Chowla, Erdős, Strauss, 1960) $N(n) > \frac{1}{3}n^{1/91} > \frac{1}{3}n^{0.01}$
 - ▶ (Wilson, 1974) $N(n) > n^{1/17} - 2 > n^{0.058} - 2$
 - ▶ (Lu, 1985) $N(n) > n^{1/14.3} - 2 > n^{0.069} - 2$

Latest records of $N(n)$ for small n

n	$N(n) \geq ?$	Reference
10	2	Parker, Shrikhande, Bose, 1959
12	5	Johnson, Dulmage, Mendelsohn, 1961
14	4	Todorov, 2012
15	4	Schellenberg, van Rees, Vanstone, 1978
18	5	Abel, 2015
20	4	Wang, 1978
21	5	Nazarok, 1991
22	3	Abel, Zhang, Zhang, 1996 (idempotent MOLS)
24	7	Abel, Colbourn, Wojtas, 2004
26	4	Colbourn, 1995
28	5	Abel, 2006
30	4	Abel, Todorov, 1994

Magic squares

Magic squares

A **magic square** (魔法陣) is an arrangement of $\{0, 1, \dots, n^2 - 1\}$ in an $n \times n$ array, such that the sum of number in each row, each column, and each diagonal (diagonal and back-diagonal) is equal.

A♠	K♦	Q♥	J♣
K♥	A♣	J♠	Q♦
Q♣	J♥	A♦	K♠
J♦	Q♠	K♣	A♥

$$\begin{array}{c} (A \ K \ Q \ J) \\ (0 \ 1 \ 2 \ 3) \\ \hline (\spadesuit \ \diamondsuit \ \heartsuit \ \clubsuit) \\ (0 \ 1 \ 2 \ 3) \end{array} \rightarrow$$

00	11	22	33
12	03	30	21
23	32	01	10
31	20	13	02

4-ary numbers to decimal numbers \rightarrow

0	5	10	15
6	3	12	9
11	14	1	4
13	8	7	2

Outline

- ① Latin squares, quasigroups, groups
- ② Completion of Latin rectangles
- ③ Mutually orthogonal Latin squares (MOLS)
- ④ Transversals of Latin squares
- ⑤ Orthogonal arrays and applications to designs of experiments

Transversals of Latin squares

Transversal

A **transversal** (横断集合) of a Latin square is a set of entries which includes exactly one entry from each row and column and one of each symbol.

















Partial transversal

A **partial transversal** (部分横断集合) of a Latin square is a set of entries which includes at most one entry from each row and column and at most one of each symbol.

$$L_1 =$$

A	K	Q	<i>J</i>
K	<i>A</i>	J	Q
<i>Q</i>	J	A	K
J	Q	<i>K</i>	A

$$L_2 =$$

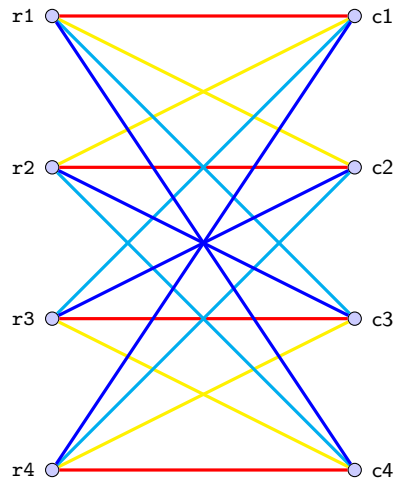
Transversal = perfect rainbow matching in complete bipartite graphs

	c1	c2	c3	c4
r1	A	K	Q	J
r2	K	A	J	Q
r3	Q	J	A	K
r4	J	Q	K	A

edge-
coloring
边染色

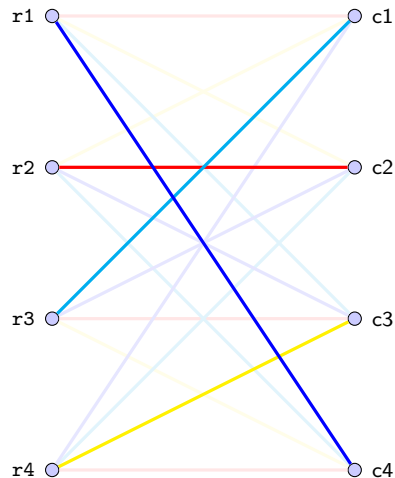


彩虹



Transversal = perfect rainbow matching in complete bipartite graphs

	c1	c2	c3	c4
r1				<i>J</i>
r2		<i>A</i>		
r3	<i>Q</i>			
r4			<i>K</i>	



Ryser's original conjecture

$$\# \text{ transversals} \equiv n \pmod{2}$$

Ryser's original conjecture, 1967

For every Latin square of order n , the number of transversals is congruent to n modulo 2.

- (Balasubramanian, 1990) For every Latin square of even order, the number of transversals is even.
- There are many counterexamples of odd order to Ryser's original conjecture.
- There is no known example of a Latin square of odd order which has no transversal.

Conjecture

Each Latin square of odd order has a transversal.

An infinite family of Latin squares without transversal

- x : row index, y : column index, z : symbol ($= L(x, y)$)
- $\Delta(x, y, z) := x + y - z \pmod n$

Lemma

The sum $\pmod n$ of the Δ values over the elements of a transversal T is 0 if n is odd, and $n/2$ if n is even.

Proof:

$$\sum_{e \in T} \Delta(e) = \sum_{x=0}^{n-1} x + \sum_{y=0}^{n-1} y - \sum_{z=0}^{n-1} z = \frac{n(n-1)}{2}.$$

Theorem (Wanless, Webb, 2006)

The Latin square generated by the cyclic group \mathbb{Z}_n has no transversal if n is even.

Proof: [▶▶ Handwritten Notes](#)

Ryser–Brualdi–Stein's conjecture

Ryser–Brualdi–Stein's conjecture

Every Latin square of order n has a partial transversal of length $n - 1$.

- (Brouwer, et al., 1978; Woolbright, 1978) Every Latin square of order n has a partial transversals of length at least $n - \sqrt{n}$.
- (Shor, 1982; Hatami–Shor, 2008) ... at least $n - O(\log^2 n)$. ($n - 11.053 \log^2 n$)
- (Keevash, Pokrovskiy, Sudakov, Yepremyan, 2020+) [arXiv:2005.00526] ... at least $n - O(\log n / \log \log n)$.

An illustration for the basic idea of Hatami–Shor's theorem

Every Latin square of order 6 has a partial transversal of length 5.

Proof: [» Handwritten Notes](#)

Outline

- ① Latin squares, quasigroups, groups
- ② Completion of Latin rectangles
- ③ Mutually orthogonal Latin squares (MOLS)
- ④ Transversals of Latin squares
- ⑤ Orthogonal arrays and applications to designs of experiments

Statistical designs of experiments

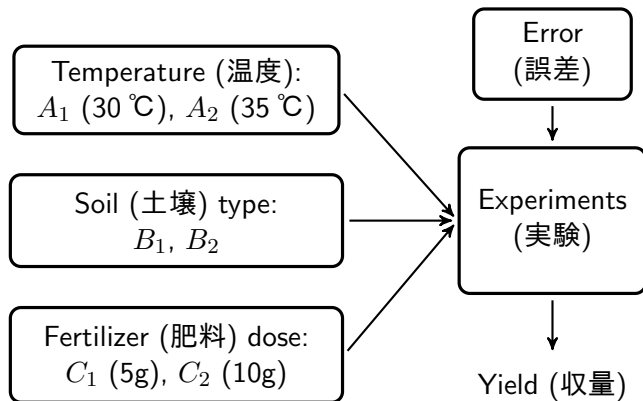
- The **Design of Experiments** (DoE, 実験計画法) is a field of applied statistics that aims to design efficient experiments and to analyze experimental data with high accuracy.
- DoE was pioneered by R. A. Fisher in 1920s for agricultural experiments.
- In 1950, W. G. Cochran and G. M. Cox published *Experimental Designs*.
- DoE has been broadly adapted in biological, psychological, and agricultural experiments.
- In 1970s, Taguchi methods (aka 品質工学) was developed to improve the quality of manufactured goods, and more recently also applied to engineering, marketing, etc.



Sir Ronald Aylmer Fisher (1890 – 1962)

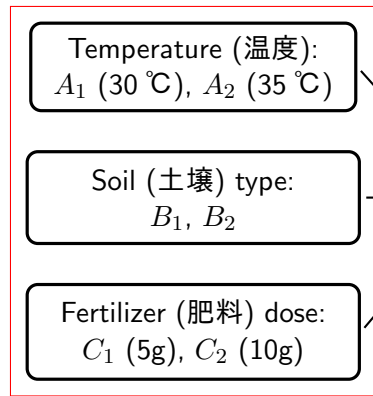


Designs of experiments: Fisher's idea for agricultural experiments



Designs of experiments: Fisher's idea for agricultural experiments

Factors (要因) and their levels (水準)



Error
(誤差)

Experiments
(実験)

Yield (収量)

Full factorial design
(完全実施要因計画)

A_1, B_1, C_1 ;

A_1, B_1, C_2 ;

A_1, B_2, C_1 ;

A_1, B_2, C_2 ;

A_2, B_1, C_1 ;

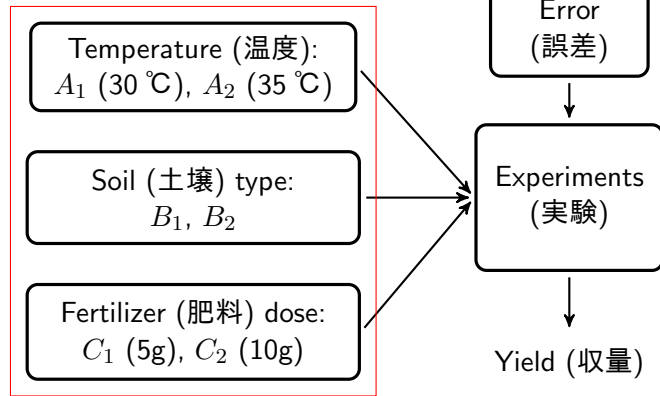
A_2, B_1, C_2 ;

A_2, B_2, C_1 ;

A_2, B_2, C_2 ;

Designs of experiments: Fisher's idea for agricultural experiments

Factors (要因) and their levels (水準)



Fractional factorial design
(一部実施要因計画)

$A_1, B_1, C_1;$

$A_1, B_1, C_2;$

$A_1, B_2, C_1;$

$A_1, B_2, C_2;$

$A_2, B_1, C_1;$

$A_2, B_1, C_2;$

$A_2, B_2, C_1;$

$A_2, B_2, C_2;$

Fractional factorial design and orthogonal arrays

- Choose 4 combinations from the full factorial design.

<i>A</i>	<i>B</i>	<i>C</i>
1	1	1
1	1	2
1	2	1
1	2	2
2	1	1
2	1	2
2	2	1
2	2	2

<i>A</i>	<i>B</i>	<i>C</i>
1	1	2
1	2	1
2	1	1
2	2	2

OA with
 $v = 2, \lambda = 1$

<i>A</i>	<i>B</i>	<i>A</i>	<i>C</i>	<i>B</i>	<i>C</i>
1	1	1	2	1	2
1	2	1	1	2	1
2	1	2	1	1	1
2	2	2	2	2	2

Most important property

Restricting on any two columns, the occurrence number of each combination of levels is equal to λ .

Which combination is the best?

No.	Temp. (°C)	Soil type	Fertilizer (g)	Yield (kg)
1	30	B1	10	67
2	30	B2	5	86
3	35	B1	5	54
4	35	B2	10	79

- $y_{f,v}$: average yield when factor = f and level = v .
 - ① $y_{1,1} = (67 + 86)/2 = 76.5$ (Temp = 30 is better), $y_{1,2} = (54 + 79)/2 = 66.5$
 - ② $y_{2,1} = 60.5$, $y_{2,2} = 82.5$ (Soil B2 is better)
 - ③ $y_{3,1} = 70$, $y_{3,2} = 73$ (Fertilizer 10g is better)
- (Temp., Soil type, Fertilizer) at (level 1, level 2, level 2), i.e. (Temp. 30, Soil B2, Fertilizer 10g) is the best combination.
- Notice: Here interactions (交互作用) between factors are not considered.

Orthogonal arrays

Orthogonal arrays (OA)

An $N \times k$ array with symbols in S is an **orthogonal array** (直交配列; OA) if in any $N \times t$ subarray, each t -dimensional row vector in S^t appears exactly λ times, denoted by $\text{OA}(N, k, s, t)$.

- ① $t \geq 2$: strength (強さ)
- ② $s = |S| \geq 2$: number of levels (水準数)
- ③ λ : index (会合数)

Proposition OA-1

$$N = \lambda s^t.$$

Proof: [▶ Handwritten Notes](#)

Properties of orthogonal arrays

$$N = \lambda \cdot s^t \quad \Leftrightarrow \quad N = (\lambda \cdot s) \cdot s^{t-1}$$

Proposition OA-2

An $\text{OA}(N, k, s, t)$ with index λ is also an $\text{OA}(N, k, s, t-1)$ with index λs .

Proof: [» Handwritten Notes](#)

Proposition OA-3

Any $N \times k'$ subarray of an $\text{OA}(N, k, s, t)$ is an $\text{OA}(N, k', s, t')$ where $t' = \min\{t, k'\}$.

Proof: [» Handwritten Notes](#)

Upper bound on number of factors

Theorem (Rao's inequality)

For $\text{OA}(N, k, s, t)$,

$$N \geq \sum_{i=0}^u \binom{k}{i} (s-1)^i, \quad \text{if } t = 2u,$$

$$N \geq \sum_{i=0}^u \binom{k}{i} (s-1)^i + \binom{k-1}{u} (s-1)^{u+1}. \quad \text{if } t = 2u + 1,$$

Find optimal OAs

For given k, s, t , find the smallest $N = \lambda s^t$ such that $\text{OA}(N, k, s, t)$ exists.

Most known constructions are based on linear codes (in 4th day).

Construct OA via MOLS

Theorem

There is an $OA(s^2, k, s, 2)$ (with $\lambda = 1$) \iff there exist $k - 2$ MOLS(s).

$OA(s^2, s-1, s, 2)$ \iff (max) $s-1$ MOLS(s)
 \uparrow
 optimal on k

	α	β	γ	δ
1	A♠	K♦	Q♥	J♣
2	K♥	A♣	J♠	Q♦
3	Q♣	J♥	A♦	K♠
4	J♦	Q♠	K♣	A♥

→

row idx	col idx	1st LS	2nd LS
1	α	A	♠
1	β	K	♦
1	γ	Q	♥
1	δ	J	♣
2	α	K	♥
2	β	A	♣
2	γ	J	♠
2	δ	Q	♦
⋮	⋮	⋮	⋮

$OA(16, 4,$
 $4, 2)$

16×4

$2\text{-MOLS}(4)$ 4×4

Secret sharing schemes

- Aim: protect secret information K
- The dealer divides K into w pieces (shares) and contribute shares to w participants s.t.
 - ▶ by combining any t ($t \leq w$) shares K can be recovered
 - ▶ any combination of less than t shares cannot retrieve K

$(t, n, v; m)$ -threshold secret sharing scheme

Let $\mathcal{K} = \{K_1, \dots, K_m\}$ be the set of secret keys and $\mathcal{S} = \{s_1, \dots, s_v\}$ be the set of shares. Each $K \in \mathcal{K}$ can be divided into shares $k_1, \dots, k_w \subseteq \mathcal{S}$ such that any t shares can retrieve K and any $t - 1$ or less cannot. This is called a $(t, w, v; m)$ -**threshold secret sharing scheme** (閾值秘密分散法). Moreover, if any $t - 1$ or less participants cannot obtain any information about K , then it is called a **perfect** threshold scheme.

even partial information

Application of OAs to secret sharing schemes

- s : total number of secret keys
- w : number of shares for a given secret key
- t : threshold for key recovery

Theorem

An $OA(s^t, w + 1, s, t) \implies$ a perfect $(t, w, s; s)$ -threshold secret sharing scheme

- Column 1 of OA: secret keys $K \in \mathcal{K}$ (totally s different keys)
- For any $K \in \mathcal{K}$, let $C_K = \{i \in [s^t] : a_{i,w+1} = K\}$.
- The dealer randomly choose $i \in C_K$ and distribute $a_{i,j}$ ($2 \leq j \leq w + 1$) to participant j .

$OA(27, 4, 3, 3)$

K_0	s_0	s_0	s_0
K_0	s_0	s_1	s_2
K_0	s_0	s_2	s_1
K_0	s_1	s_0	s_2
K_0	s_1	s_1	s_1
K_0	s_1	s_2	s_0
K_0	s_2	s_0	s_1
K_0	s_2	s_1	s_0
K_0	s_2	s_2	s_2
K_1	s_0	s_0	s_2
K_1	s_0	s_1	s_1
K_1	s_0	s_2	s_0
K_1	s_1	s_0	s_1
K_1	s_1	s_1	s_0
K_1	s_1	s_2	s_2
K_1	s_2	s_0	s_0
K_1	s_2	s_1	s_2
K_1	s_2	s_2	s_1
K_2	s_0	s_0	s_1
K_2	s_0	s_1	s_0
K_2	s_0	s_2	s_2
K_2	s_1	s_0	s_0
K_2	s_1	s_1	s_2
K_2	s_1	s_2	s_1
K_2	s_2	s_0	s_2
K_2	s_2	s_1	s_1
K_2	s_2	s_2	s_0

key P_1, P_2, P_3

Homework assignments (レポート課題) for 1st day (1/2)

Exercise 1

- ① Create the Cayley table of the cyclic group \mathbb{Z}_6 and the symmetric group S_3 .
- ② Briefly state the reason why the above two Latin squares are not orthogonal.

Hint: Both \mathbb{Z}_6 and S_3 are of order 6. So their Cayley tables should be 6×6 Latin squares.

Homework assignments (レポート課題) for 1st day (2/2)

Exercise 2

Consider an experiment for industrial products with three factors, each of which has three levels: temperature (温度), processing time (処理時間), catalyst (触媒). Suppose that the effect on production (生産量) of each factor is independent.

According to the experimental results by using an $OA(9, k=3, s=3, t=2)$ shown as follows, which combination of levels for the three factors is the best?

No.	temp. (°C)	time (min)	catalyst (g)	production (kg)
1	80	90	5	31
2	80	120	6	54
3	80	150	7	38
4	85	90	6	53
5	85	120	7	49
6	85	150	5	42
7	90	90	7	57
8	90	120	5	62
9	90	150	6	64

$OA(9, 3, 3, 2)$