Multi-Structured Designs and Their Applications

Ryoh Fuji-Hara
University of Tsukuba, Japan

Joint work with Ying Miao (University of Tsukuba)

Block Design $(V, \mathfrak{B})$

- V : a finite set (points)
- $\mathfrak{B}$: a collection of subsets (blocks) of V

$$\mathfrak{B} = \{\mathbf{B}_1, \mathbf{B}_2, ..., \mathbf{B}_b\} \ , \ \mathbf{B}_i \subseteq V$$

- some combinatorial conditions

Conditions

(C1) every block contains k points (regular)

(C2) every point of V is contained in r blocks (singleton balance)

(C3) every pair of distinct elements of V appears in exactly λ blocks (pair balance)

Classical designs

Pairwise Balanced Design (PBD) : when (C3) is satisfied

(r, λ)-design : when (C2) and (C3) are

Balanced Incomplete Block Design (BIBD) or 2-design: when (C1), (C2) and (C3) are

Multi-Structured Design

- A block design
- Each block has further structure
- additional combinatorial conditions

Block Forms

Each block $\mathbf{B}_i$ has sub-blocks

$$\mathbf{B}_i = \{C_{i1}, C_{i2}, ..., C_{in_i}\} \ , \ C_{ij} \subseteq \mathbf{B}_i$$

I) $\{C_{i1}, C_{i2}, ..., C_{in_i}\}$ is a partition of $\mathbf{B}_i$

II) $C_{ij} \subseteq \mathbf{B}_i$ and $\mathbf{B}_i = \bigcup_{1 \leq j \leq n_i} C_{ij}$

Unordered

Each block $\mathbf{B}_i$ is a set of disjoint $n_i$sub-blocks

$$\tilde{\mathbf{B}}_i = \{C_{i1}, C_{i2}, ..., C_{in_i}\} \ , \ C_{ij} \subseteq \mathbf{B}_i$$

Ordered

Each block $\mathbf{B}_i$ is an ordered set of disjoint n sub-blocks (some of them can be empty)

$$\vec{\mathbf{B}}_i = (C_{i1}, C_{i2}, ..., C_{in}) \ , \ C_{ij} \subseteq \mathbf{B}_i$$

App. I (Designs of Experiments)

$(V, \mathfrak{B})$ super design

$$\mathfrak{B} = \{\mathbf{B}_1, \mathbf{B}_2, ..., \mathbf{B}_b\} \ , \ \mathbf{B}_i \subseteq V$$

$(V, \mathfrak{C})$ sub-design (nested design)

$$\tilde{\mathbf{B}}_i = \{C_{i1}, C_{i2}, ..., C_{in_i}\} \ , \ C_{ij} \subseteq \mathbf{B}_i$$

$$\mathfrak{C} = \{C_{ij} \mid 1 \leq i \leq b, \ 1 \leq j \leq n_i\}$$

Note: $\{ \ \}$ is a multi-set

Multi-Structured Design (MSD) with a 2-design

Conditions on $(V, \mathfrak{B})$ $S_\lambda(2; v, k)$

(1) block size is constant (regular) k

(2) every element of V appears in the same number of the blocks (singleton balance) r

(3) every pair of distinct elements of V appears in the same number of blocks (pair balance) λ

Conditions on $(V, \mathfrak{C})$ $S_{\lambda'}(2; v, k')$

(1) regular

(2) singleton balance

(3) pair balance

Federer(1972),Preece(1967) (Nested Design)

Example V={0,1,2,3,4} S3(2;5,4)

B_1= { {0, 1} ,{2, 4} }

B_2= { {1, 2} ,{3, 0} }

B_3= { {2, 3} ,{4, 1} }

B_4= { {3, 4} ,{0, 2} }

B_5= { {4, 0} ,{1, 3} }

Standard Block Experiments

7 fertilizers

j

7 wheat varieties i

x		x				x
x	x				x	
	x			x		x
x			x	x		
	x	x	x			
		x		x	x	
			x		x	x

21 experiments

$$y_{ij} = \mu + \alpha_i + \beta_j + \epsilon_{ij} \qquad \sum_{i=1}^{7} \alpha_i = \sum_{j=1}^{7} \beta_j = 0$$

the total combinations of i and j are 49

Merits

- Less experiments
- All effects are estimable easily
- Good precision of estimations
- Equal precisions of estimations

Nested Blocks

10 fertilizers (5 kinds X 2 types)
{0-0, 0-1, 1-0, 1-1, 2-0, 2-1, 3-0, 3-1, 4-0, 4-1}

5 wheat varieties

0	x	o	o		x
1	x	o	x	o	
2		x	x	o	o
3	o	x		x	o
4	o		o	x	x

$$y_{ijk} = \mu + \alpha_i + \beta_j + \gamma_k + \epsilon_{ijk}$$

γ_k , $k = 0, 1$: sub-block effect

$$\gamma_0 + \gamma_1 = 0$$

App. 2 (Rows and Columns)

$(V, \mathfrak{B})$ the points of each block are arranged in an nXm array

$$\mathbf{B}_i = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{pmatrix}$$

(1) pair balance

(2) for any distinct two points x,y of V, there are exactly λ_R blocks which contain x,y in a row (row pair balance)

(3) (column pair balance) λ_C

Experiments

Srivastava (1978)

Singh and Dey (1978)

$$y_{ijkl} = \mu + \alpha_i + \beta_j + \gamma_k + \delta_l + \epsilon_{ijkl}$$

α_i : variety effect

β_j : block effect

γ_k : row effect

δ_l : column effect

$(V, \mathfrak{B})$

$\mathfrak{B} = \{\mathbf{B}_1, \mathbf{B}_2, ..., \mathbf{B}_b\}$, $\mathbf{B}_i \subseteq V$

$|\mathbf{B}_i| = nm$

For each block $\mathbf{B}_i$,

$$\tilde{\mathbf{B}}_i^{(R)} = \{C_{i1}, C_{i2}, ..., C_{in}\} \ , \ C_{ij} \subseteq \mathbf{B}_i$$

$$\tilde{\mathbf{B}}_i^{(C)} = \{D_{i1}, D_{i2}, ..., D_{im}\} \ , \ D_{ij} \subseteq \mathbf{B}_i$$

Orthogonal MSDs

Two "MSD with a 2-design"s with the conditions

1. $(V, \mathfrak{C})$ $\mathfrak{C} = \{C_{ij} \mid 1 \le i \le b, \ 1 \le j \le n\}$
   (1) regular
   (2) pair balance
2. $(V, \mathfrak{D})$ $\mathfrak{D} = \{D_{ij} \mid 1 \le i \le b, \ 1 \le j \le m\}$
   (1) regular
   (2) pair balance
3. For each i ,
   $|C_{ij} \cap D_{ik}| = 1$, $1 \le j \le n$, $1 \le k \le m$

Example v=9 k=3X3

∞	0	4
1	2	7
5	3	6

∞	2	6
3	4	1
7	5	0

∞	1	5
0	2	3
4	7	6

∞	3	7
2	4	5
6	1	0

App. 3 (Authentication Code)

E : common encryption function set

$e : S \rightarrow M$, $e \in E$

S : source set , M : message set

$\kappa(e) = (e(s_1), e(s_2), ...)$: the images of e

Transformer $\xleftrightarrow{\text{select } e \in E}$ Receiver

for some $s_1, s_2, ... \in S$ $\xrightarrow{(s_i, e(s_i)) \in M}$ Check: uniquely determined ? $\kappa(e)$

sources

encryption functions

	s_0	s_1	s_2
e_0	0	0	0
e_1	1	1	2
e_2	2	2	1
e_3	0	1	1
e_4	1	2	0
e_5	2	0	2
e_6	0	2	2
e_7	1	0	1
e_8	2	1	0

There are no two images including $e_i(s_j), e_i(s_k), j \neq k$

M= {0,1,2}

MSD with External Packing

Each block $\mathbf{B}_i$consists of a set of disjoint n_i sub-blocks

$$\tilde{\mathbf{B}}_i = \{C_{i1}, C_{i2}, ..., C_{in_i}\}\ ,\ C_{ij} \subseteq \mathbf{B}_i$$

Conditions

(1) For any $x, y \in V$, there is at most one super block which contains x, y in distinct sub-blocks

(2) $|C_{ij}| \geq 1,\ n_i = n\ ,\ \text{for any } i = 1, 2, ..., b$

Splitting Authentication

W. Ogata, K. Kurosawa, D. R. Stinson and H. Saido (2004)

Encryption function

$$e(s, r),\ e \in E,\ s \in S$$

$$r\ :\ \text{a random number}$$

Transformer $\xleftrightarrow{\text{select } e \in E}$ Receiver

for some $s_1, s_2, ... \in S$
Get random numbers $r_1, r_2, ...$

$\xrightarrow{(s_i, e(s_i, r_i)) \in M}$

Check: uniquely determined ?

$\kappa(e)$

---

	s_0	s_1	s_2
e_0	0, 1	2, 4	12, 20
e_1	7, 8	9, 11	19, 2
e_2	5, 6	7, 9	17, 0
e_3	3, 4	5, 7	15
e_4	9, 10	11	21, 4
e_5	2, 3	4, 6	14, 22
e_6	10, 11	12, 14	5
e_7	4, 5	6, 8	16
e_8	6, 7	8, 10	18, 1
e_9	1, 2	3, 5	13, 21
e_{10}	8, 9	10, 12	20, 3
e_{11}	11, 12	13, 15	23, 6

There are no two rows which contain $e_i(s_j, r), e_i(s_k, r'), j \neq k$ in different columns

M={0,1,2,..., 24}

---

c-splitting: $|e(s)| = c$ for any $e \in E$ and any $s \in S$. (regular)

Optimality Theorem

W. Ogata, K. Kurosawa, D. R. Stinson and H. Saido (2004)

(1) For any c-splitting authentication code, the following inequalities always hold:

$$|E| \geq |M|(|M| - 1) / (c^2|S|(|S| - 1)).$$

A c-splitting authentication code is said to be *optimal* if it satisfies all the equalities in the Theorem.

(2) If there exists an MSD with an externally balanced ($\lambda = 1$) sub-design (*u sub-blocks of size c*) then there exists an optimal c-splitting authentication code such that

(1) $|M|=v$, $|S|=u$;

(2) each source state occurs with equal probability.

App. 4 **(Balanced and Orthogonal Arrays)**

Ordered Form

Each block $\mathbf{B}_i$ is partitioned into n sub-blocks and they are placed in an order (some of them can be empty)

$$\vec{\mathbf{B}}_i = (C_{i1}, C_{i2}, ..., C_{in})\ ,\ C_{ij} \subseteq \mathbf{B}_i$$

$\mathfrak{C}_j$: the set of *j*-th sub-blocks $1 \leq j \leq n$

Correspondence between multi-structured blocks and vectors of length v

Ordered multi-structured block $V = \{0,1,2,...,v-1\}$

$$\vec{\mathbf{B}}_i = (C_{i1}, C_{i2}, ..., C_{in})\ ,\ C_{ij} \subseteq \mathbf{B}_i$$

(n+1)-ary vector of length v

$$\mathbf{x}_i = (x_0, x_1, x_2, ..., x_{v-1})$$

$$x_t = \begin{cases} j & \text{if } t \in C_{ij} \\ 0 & \text{otherwise} \end{cases}$$

Example

$V = \{0,1,2,...,6\}$

$$\vec{\mathbf{B}}_1 = (\{0,1\},\{2,5\}) \qquad \mathbf{x}_1 = \overset{\begin{array}{ccccccc}0&1&2&3&4&5&6\end{array}}{(1,1,2,0,0,2,0)}$$

$$\vec{\mathbf{B}}_2 = (\{0,4\},\{3,6\}) \qquad \mathbf{x}_2 = (1,0,0,2,1,0,2)$$

$$\vdots \qquad\qquad \vdots$$

Balanced Array Chakravarti (1956,1961)

As a generalization of orthogonal array
In order to use in orthogonal experiments

$b \times v$ array , entries are from *F={0,1,2,...,n}*

(1) In any two columns, a pair $(x, y) \in F^2$ occurs exactly μ_{xy} times.

(2) $\mu_{xy} = \mu_{yx}$ for any $x, y \in F$

If $\mu_{xy} = \mu$ for any $x, y \in F$, the array is called *orthogonal array*

Example 20 X 6 BA

	1	2	3	4	5	6
1	1	2	1	0	0	0
2	1	1	0	0	1	0
3	2	0	2	0	0	1
4	2	0	0	0	1	2
5	0	2	2	2	0	0
6	0	1	0	1	2	0
7	0	0	1	1	0	2
8	0	0	0	2	2	1
9	2	1	0	2	0	0
10	2	2	0	1	0	0

11	1	0	2	0	2	0
12	2	0	1	0	2	0
13	1	0	0	1	0	1
14	1	0	0	2	0	2
15	0	1	1	0	0	1
16	0	1	2	0	0	2
17	0	2	0	0	1	1
18	0	2	0	0	2	2
19	0	0	1	2	1	0
20	0	0	2	1	1	0

μ_{00} =4, μ_{01} =μ_{02} =3 and μ_{11} =μ_{12} =μ_{22} =1.

Ordered MSD with Mutually Balanced (r,λ)-designs

[1] $(V, \mathfrak{B})$ (1) singleton balance (r)
(2) pair balance (λ)

[2] $(V, \mathfrak{C}_j)$ (1) singleton balance (r_j)
(2) pair balance (λ_j)
for j=1,2,...,n

[3] External Balance :

For any distinct $x, y \in V$, there are exactly μ_{ij} super blocks, each of which contains x in the i-th and y in the j-th sub-block.

Let $\mathfrak{C}_0 = \{V \setminus \mathbf{B}_i \mid 1 \leq i \leq b\}$

Lemma

If the conditions [1] and [2] are satisfied then $(V, \mathfrak{C}_0)$ holds singleton and pair balance property

$$r_0 = b - r$$
$$\lambda_0 = b - 2r + \lambda$$

Lemma

Further, if the condition [3] is satisfied for i,j = 1,2,...n then it works for $0 \leq i, j \leq n$

$$\mu_{i0} = \mu_{0i} = r_i - \sum_{j=1}^{n} \mu_{ij}$$

Theorem (S.Kuriki and R.Fuji-Hara,1994)

There exists an ordered multi-structured design which satisfies [1],[2] and [3] if and only if there exists a $b \times v$ balanced array with entries from F={0,1,...,n} and parameters $\mu_{xy},\ 0 \le x, y \le n$

Example V={1,2,3,4,5,6}

(1 , 3 | 2)
(1, 2, 5 | ∅)
(6 | 1, 3)
(5 | 1, 6)
(∅ | 2, 3, 4)
(2, 4 | 5)
(3, 4 | 6)
(6 | 4, 5)
(2 | 1 , 4)
(4 | 1 , 2)
(1 | 3 , 5)

(3 | 1, 5)
(1 , 4 , 6 | ∅)
(1 | 4 , 6)
(2, 3, 6 | ∅)
(2 | 3 , 6)
(5 , 6 | 2)
(∅ | 2, 5, 6)
(3, 5 | 4)
(4, 5 | 3)

The Intermission

休憩