応用数学特論 II (集中講義)

Day 2 Hadamard matrices & BIB designs

盧 暁南 (山梨大学)
Xiao-Nan LU (University of Yamanashi)

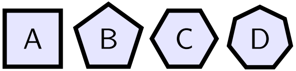
Aug. 26, 2021
Kobe University

Outline

Pan balance weighing designs (model 1)

y_1 $\qquad$ $a + \varepsilon_1$

- 4 objects

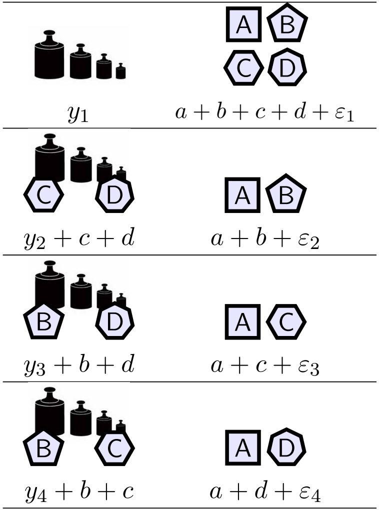


- Estimate of the weight $=$ weighing $=$ true weight $+$ error

$$\begin{cases} \hat{a} = y_1 = a + \varepsilon_1 \\ \hat{b} = y_2 = b + \varepsilon_2 \\ \hat{c} = y_3 = c + \varepsilon_3 \\ \hat{d} = y_4 = d + \varepsilon_4 \end{cases}$$

- 4 weighings

Pan balance weighing designs (model 2)



- Model 2:

$$\begin{cases} y_1 = a+b+c+d+\varepsilon_1 \\ y_2 = a+b-c-d+\varepsilon_2 \\ y_3 = a-b+c-d+\varepsilon_3 \\ y_4 = a-b-c+d+\varepsilon_4 \end{cases}$$

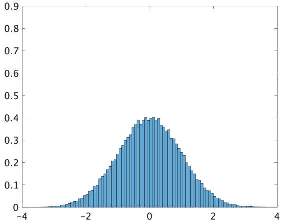
- The estimates of the weights

$$\begin{aligned} \hat{a} &= \tfrac{1}{4}(y_1+y_2+y_3+y_4) \\ &= a + \tfrac{1}{4}(\varepsilon_1+\varepsilon_2+\varepsilon_3+\varepsilon_4). \\ \hat{b} &= \tfrac{1}{4}(y_1+y_2-y_3-y_4) \\ &= b + \tfrac{1}{4}(\varepsilon_1+\varepsilon_2-\varepsilon_3-\varepsilon_4). \\ \hat{c} &= \dots \end{aligned}$$

Which model is better?

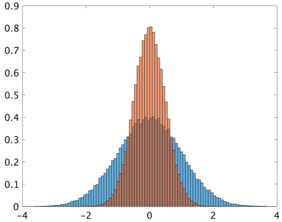
- $\varepsilon_i \sim N(0, \sigma^2)$ i.i.d. for $1 \le i \le 4$.
- Model 1:

$$\begin{aligned}\mathrm{Var}(\hat{a}) &= \mathrm{Var}(a + \varepsilon_1) \\ &= \mathrm{Var}(\varepsilon_i) = \sigma^2.\end{aligned}$$



- Model 2:

$$\begin{aligned}\mathrm{Var}(\hat{a}) &= \mathrm{Var}\left(a + \frac{1}{4}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4)\right) \\ &= \left(\frac{1}{4}\right)^2 \sum_{i=1}^{4} \underbrace{\mathrm{Var}(\varepsilon_i)}_{=\sigma^2} = \left(\frac{1}{2}\sigma\right)^2.\end{aligned}$$



Two models of matrix forms

- Model 1

$$\begin{cases} y_1 = a + \varepsilon_1 \\ y_2 = b + \varepsilon_2 \\ y_3 = c + \varepsilon_3 \\ y_4 = d + \varepsilon_4 \end{cases} \iff \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} + \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \end{bmatrix}$$

- Model 2

$$\begin{cases} y_1 = a + b + c + d + \varepsilon_1 \\ y_2 = a + b - c - d + \varepsilon_2 \\ y_3 = a - b + c - d + \varepsilon_3 \\ y_4 = a - b - c + d + \varepsilon_4 \end{cases} \iff \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} + \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \end{bmatrix}$$

- The design matrix is essential.

Least-squares estimation for linear model

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \boldsymbol{\varepsilon}$$

Multiply $\mathbf{H}^\top$ on both sides, we have

$$\mathbf{H}^\top \mathbf{y} = \mathbf{H}^\top \mathbf{H}\mathbf{x} + \mathbf{H}^\top \boldsymbol{\varepsilon} \quad \Longleftrightarrow \quad (\mathbf{H}^\top \mathbf{H})^{-1}\mathbf{H}^\top \mathbf{y} = \mathbf{x} + (\mathbf{H}^\top \mathbf{H})^{-1}\mathbf{H}^\top \boldsymbol{\varepsilon} = \hat{\mathbf{x}}$$

For model 2, $\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}$, $\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$, $\mathbf{x} = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$ (true), $\boldsymbol{\varepsilon} = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3 \\ \varepsilon_4 \end{bmatrix}$, $\hat{\mathbf{x}} = \begin{bmatrix} \hat{a} \\ \hat{b} \\ \hat{c} \\ \hat{d} \end{bmatrix}$ (estimated). Here, we want to minimize $\det(\mathbf{H}^\top \mathbf{H})^{-1}$ (or maximize det $(\mathbf{H}^\top \mathbf{H})$).

$$\mathbf{H}^\top \mathbf{H} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} \quad \longleftarrow \det(\mathbf{H}^\top \mathbf{H}) = 4^4 \text{ is max!}$$

Hadamard matrices

Definition

A square matrix $\mathbf{H} \in \{\pm 1\}^{n\times n}$ is an Hadamard matrix (アダマール行列) if

$$\mathbf{H}^\top \mathbf{H} = n\mathbf{I}_n.$$

In this case, $\det(\mathbf{H}^\top \mathbf{H}) = n^n$.

Example

$$\mathbf{H}^\top \mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4\mathbf{I}_4$$

Properties of Hadamard matrices

$I_n^T = I_n$

$(H^T)^T \cdot H^T = H \cdot H^T = nI_n$

Proposition HM-1

If $\mathbf{H}$ is an Hadamard matrix then $\mathbf{H}^\top$ and $-\mathbf{H}$ are also Hadamard matrices.

Proposition HM-2

- For an Hadamard matrix $\mathbf{H}$, $\det(\mathbf{H}) = n^{n/2}$.
- For any $n \times n$ $\{\pm 1\}$ matrix $\mathbf{A}$, $\det(\mathbf{A}) \leq n^{n/2}$.

Proof: Handwritten Notes

- $\mathcal{A}_n$: the set of all $n \times n$ $\{\pm 1\}$ matrices
- $\mathbf{H}$ is D-optimal over $\mathcal{A}_n$, i.e., $\mathbf{H} = \max\{\det(\mathbf{A}) : \mathbf{A} \in \mathcal{A}_n\}$.

Existence of Hadamard matrices

Proposition HM-3

For $n \geq 4$, if an Hadamard matrix of order n exists then $4 \mid n$.

Proof: Handwritten Notes

Kronecker Product Construction

Let $\mathbf{H}_n$ and $\mathbf{H}_k$ be Hadamard matrices of order n and k, respectively. Then $\mathbf{H}_n \otimes \mathbf{H}_k$ is an Hadamard matrix of order nk .

Proof: Handwritten Notes

Corollary

An Hadamard matrix of order 2^m exists.

Example: Jupyper Notebook

Hadamard conjecture

Hadamard conjecture

There exists an Hadamard matrix of order n for any $n \equiv 0 \pmod 4$.

- (1867) $n = 2^m$ ✓
- (1933) $n = q + 1$ ✓
  where $q \equiv 3 \pmod 4$ is a prime power $(q = 7, 11, 19, 23, 27, 31, \ldots)$
- (1962) $n = 92$ ✓ by computer search & combinatorial methods
- (2004) $n = 428$ ✓ by computer search & combinatorial methods
- The smallest unsolved case is $n = 668$. Have a try?

Quadratic residue

Quadratic residue

Let p be an odd prime. An integer a is called a quadratic residue (平方剰余) mod p if a is congruent (合同) to a square; otherwise, a is called a quadratic non-residue (平方非剰余) .

- The following notation is called Legendre symbol (ルジャンドル記号).

$$\chi_p(a) = \left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue mod } p, \\ -1, & \text{if } a \text{ is a quadratic non-residue mod } p, \\ 0, & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

- For any a, b,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Example: ▸▸ Jupyper Notebook

Paley's construction

Theorem (Paley's construction for Hadamard matrices)

For a prime $p \equiv 3 \pmod 4$, *define* $\mathbf{M}_p = (m_{i,j})$ *as follows:*

$$m_{i,j} = \left(\frac{j-i}{p}\right), \qquad i, j \in \mathbb{Z}_p.$$

Then, the following matrix $\mathbf{H}_{p+1}$ *is an Hadamard matrix of order* $p+1$.

$$\mathbf{H}_{p+1} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & \mathbf{M}_p - \mathbf{I}_p & \\ 1 & & & \end{pmatrix}.$$

Proof: Handwritten Notes

Example of $\mathbf{H}_8$ via Paley's construction

$$
\mathbf{M}_7 = \begin{array}{c}
\begin{matrix} \;0 & \;\;1 & \;\;2 & \;\;3 & \;\;4 & \;\;5 & \;\;6 \end{matrix} \\
\begin{pmatrix}
0 & 1 & 1 & -1 & 1 & -1 & -1 \\
-1 & 0 & 1 & 1 & -1 & 1 & -1 \\
-1 & -1 & 0 & 1 & 1 & -1 & 1 \\
1 & -1 & -1 & 0 & 1 & 1 & -1 \\
-1 & 1 & -1 & -1 & 0 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 0 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & 0
\end{pmatrix}
\end{array}.
$$

Circulant matrix

巡回行列

Then

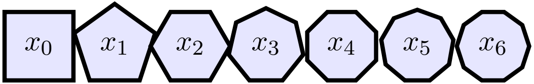
$$
\mathbf{H}_8 = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & & & \\
\vdots & & \mathbf{M}_7 - \mathbf{I}_7 & \\
1 & & &
\end{pmatrix}
= \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1
\end{pmatrix}.
$$

Outline

1. Pan balance weighing designs and Hadamard matrices
2. Spring balance weighing designs and BIB designs
3. Cyclic designs and difference families
4. Steiner triple systems
5. Pairwise balanced design, group divisible design
6. Combinatorial t-designs, Hadamard designs

Spring balance weighing designs (model 1)

- 7 objects



- Estimator = weighing = true weight + error

$$\hat{a}_i = y_i = x_i + \varepsilon_i$$

for $0 \leq i \leq 6$.

- 7 weighings

Spring balance weighing designs (model 2)

- Three objects in each weighing

$$
\begin{aligned}
y_0 &= x_0 + x_1 + x_3 + \varepsilon_0 \\
y_1 &= x_1 + x_2 + x_4 + \varepsilon_1 \\
y_2 &= x_2 + x_3 + x_5 + \varepsilon_2 \\
y_3 &= x_3 + x_4 + x_6 + \varepsilon_3 \\
y_4 &= x_4 + x_5 + x_0 + \varepsilon_4 \\
y_5 &= x_5 + x_6 + x_1 + \varepsilon_5 \\
y_6 &= x_6 + x_0 + x_2 + \varepsilon_6
\end{aligned}
$$

- 7 weighings

Design matrices for spring balance weighing designs

- $\mathbf{y} = [y_0, y_1, \ldots, y_6]^\top$, $\mathbf{x} = [x_0, x_1, \ldots, x_6]^\top$, $\boldsymbol{\varepsilon} = [\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_6]^\top$.
- Model 1: $\mathbf{y} = \mathbf{D}_1\mathbf{x} + \boldsymbol{\varepsilon}$
- Model 2: $\mathbf{y} = \mathbf{D}_2\mathbf{x} + \boldsymbol{\varepsilon}$

$$\mathbf{D}_1 = \mathbf{I}_7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{D}_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Least-squares estimation for spring balance weighing

- Model 2: $\mathbf{D}_2^\top \mathbf{y} = \mathbf{M}_2 \mathbf{x} + \mathbf{D}_2^\top \boldsymbol{\varepsilon} \quad \Longleftrightarrow \quad \mathbf{M}_2^{-1}\mathbf{D}_2^\top \mathbf{y} = \mathbf{x} + \mathbf{M}_2^{-1}\mathbf{D}_2^\top \boldsymbol{\varepsilon}$

$$\mathbf{M}_2 = \mathbf{D}_2^\top \mathbf{D}_2 = \begin{bmatrix} 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 3 \end{bmatrix}, \quad \mathbf{M}_2^{-1} = \frac{1}{18}\begin{bmatrix} 8 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 8 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 8 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 8 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 8 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & 8 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 8 \end{bmatrix}$$

Information matrix
情報行列

Estimate and variance for spring balance weighing

- Model 2:

$$\hat{\mathbf{x}} = \mathbf{M}_2^{-1}\mathbf{D}_2^\top (\mathbf{y} + \varepsilon) = \frac{1}{6}\begin{bmatrix} 2 & -1 & -1 & -1 & 2 & -1 & 2 \\ 2 & 2 & -1 & -1 & -1 & 2 & -1 \\ -1 & 2 & 2 & -1 & -1 & -1 & 2 \\ 2 & -1 & 2 & 2 & -1 & -1 & -1 \\ -1 & 2 & -1 & 2 & 2 & -1 & -1 \\ -1 & -1 & 2 & -1 & 2 & 2 & -1 \\ -1 & -1 & -1 & 2 & -1 & 2 & 2 \end{bmatrix} (\mathbf{y} + \varepsilon) \quad \begin{pmatrix} \varepsilon_0 \\ \vdots \\ \varepsilon_6 \end{pmatrix}$$

- $\varepsilon_i \sim N(0, \sigma^2)$ i.i.d. for $0 \le i \le 6$.
- Model 2: $\mathrm{Var}(\hat{x}_i) = \frac{4}{9}\sigma^2$
- Model 1: $\mathrm{Var}(\hat{x}_i) = \sigma^2$

$$\mathrm{Var}(\hat{x}_1) = \mathrm{Var}\left(\frac{1}{3}\varepsilon_0 - \frac{1}{6}\varepsilon_1 - \frac{1}{6}\varepsilon_2 \cdots\right)$$

$$= 3\cdot\left(\frac{1}{3}\right)^2\sigma^2 + 4\cdot\left(\frac{1}{6}\right)^2\sigma^2$$

$$= \frac{1}{3}\sigma^2 + \frac{1}{9}\sigma^2 = \frac{4}{9}\sigma^2.$$

不偏(unbiased)推定

Set system representation of design matrix

- Index the columns (for seven objects) of $\mathbf{D}_2$ by $0, 1, \ldots, 6$

$$\mathbf{D}_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- Rows (for seven weighings) of $\mathbf{D}_2$ can be represented by subsets of $\{0, 1, \ldots, 6\}$

$$B_0 = \{0,1,3\}, B_1 = \{1,2,4\}, B_2 = \{2,3,5\},$$
$$B_3 = \{3,4,6\}, B_4 = \{4,5,0\}, B_5 = \{5,6,1\}, B_6 = \{6,0,2\}.$$

BIB designs

Balanced Incomplete Block Design

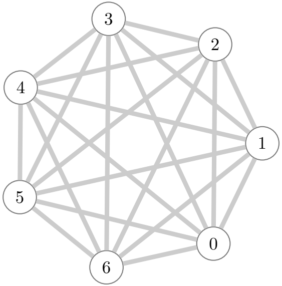
Let V be a finite set and $\mathcal{B}$ be a family of subsets of V. The pair $(V, \mathcal{B})$ is a (v, k, λ) balanced incomplete block design (釣合い型不完備ブロックデザイン; BIBD) if the all the following conditions hold.

i. $|V| = v$,
ii. For any $B \in \mathcal{B}$, $|B| = k$.
iii. For any pair of points $\{x, y\} \subseteq V$, there are exactly λ blocks (ブロック) $B \in \mathcal{B}$ containing $\{x, y\}$.

- v: number of elements (要素数) or number of points (点数)
- k: block size (ブロックサイズ)
- λ: index (会合数)

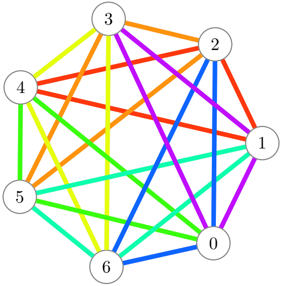
BIB designs and graph decomposition

- K_n: complete graph of order n, i.e., the graph with all $\binom{n}{2}$ possible edges on n vertices
- $(v, k, \lambda = 1)$ BIBD $\iff$ decomposition of K_n into K_k's.
- $(v, k = 3, \lambda = 1)$ BIBD $\iff$ decomposition of K_n into triangles.



BIB designs and graph decomposition

- K_n: complete graph of order n, i.e., the graph with all $\binom{n}{2}$ possible edges on n vertices
- $(v, k, \lambda = 1)$ BIBD $\iff$ decomposition of K_n into K_k's.
- $(v, k = 3, \lambda = 1)$ BIBD $\iff$ decomposition of K_n into triangles.



$$\{0,1,3\},\ \{1,2,4\},\ \{2,3,5\},\ \{3,4,6\},\ \{4,5,0\},\ \{5,6,1\},\ \{6,0,2\}.$$

Basic equalities between parameters of BIB designs

Proposition BIBD-1

$b := |\mathcal{B}| = vr/k$

Proposition BIBD-2

Let $(V, \mathcal{B})$ be a (v, k, λ) BIBD. For any $v \in V$, the number of blocks containing v is a constant, denoted by $r = \lambda(v-1)/(k-1)$.

- Any three parameters of (v, b, r, k, λ) implies the other two.
- (v, b, r, k, λ) is admissible if

$$vr = bk$$
$$r(k-1) = \lambda(v-1)$$

Example: Jupyper Notebook

Incidence matrix of BIB designs: revisit

- The incidence matrix is the transpose of "weighing design matrix".
- $\mathbf{1}_v$: all-one column vector of dimension v
- $\mathbf{J}_v = \mathbf{1}_v \mathbf{1}_v^\top$: all-one matrix of dimension v

Theorem

Let $\mathbf{N}$ *be a* $v \times b$ $\{0, 1\}$*-matrix. Then* $\mathbf{N}$ *is the incidence matrix of a* (v, b, r, k, λ) *BIBD iff*

$$\mathbf{N}^\top \mathbf{1}_v = k \mathbf{1}_b$$

and

$$NN^\top \quad \cancel{\mathbf{N}^\top \mathbf{N}} = \lambda \mathbf{J}_v + (r - \lambda) \mathbf{I}_v.$$

Proof: Handwritten Notes

Fisher's inequality

Theorem (Fisher's inequality)

For a (v, k, λ) BIBD with $v > k$, the number of blocks is not less than the number of points, that is, $b \geq v$.

Proof: Handwritten Notes

Symmetric BIBD

A (v, b, r, k, λ) BIBD with $b = v$ is called a symmetric design (対称デザイン).

Bruck–Ryser–Chowla theorem

Theorem (Bruck–Ryser–Chowla theorem, 1949–1950)

If a symmetric (v, k, λ) BIBD exists, then

1. *for v even, $k - \lambda$ must be a square.*
2. *for v odd, there exists integers x, y, z such that $z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$.*

$(x, y, z) \neq (0, 0, 0)$

- Bruck–Ryser–Chowla theorem is a generalization of Bruck–Ryser theorem for finite projective planes (in 3rd day).

Examples by Bruck–Ryser–Chowla theorem

$(22, 7, 2)$ SBIBD does not exist

- $r = \lambda(v-1)/(k-1) = 2 \times 21/6 = 7 \in \mathbb{Z}$, $\quad b = vr/k = 22 \times 7/7 = 22 \in \mathbb{Z}$.
- By BRC theorem, since $k - \lambda = 7 - 2 = 5$ is not a square, nonexistence.

$(43, 7, 1)$ SBIBD does not exist $\longleftrightarrow (6^2+6+1, 6+1, 1) \longleftrightarrow$ MOLS(6)

- $r = \lambda(v-1)/(k-1) = 1 \times 42/6 = 7 \in \mathbb{Z}$, $\quad b = vr/k = 43 \times 7/7 = 43 \in \mathbb{Z}$.
- By BRC theorem, consider the equation $z^2 = 6x^2 - y^2$.
- By modulo 3,

x	0	1	2
x^2	0	1	$4 \equiv 1$

$$z^2 \equiv -y^2 \equiv 2y^2 \pmod 3 \iff 2 \equiv (y^{-1}z)^2 \pmod 3 \iff \boxed{\left(\frac{2}{3}\right) = 1,}$$

where $\left(\frac{2}{3}\right)$ is the Legendre symbol. However, 2 is not a square mod 3.

New designs from the old designs

$(V, \mathcal{B}_1)$ $(V, \mathcal{B}_2)$ $(V, \mathcal{B}_1 \cup \mathcal{B}_2)$

Theorem (sum of BIBD)

If there exists a (v, k, λ_1) *BIBD and a* (v, k, λ_2) *BIBD, then a* $(v, k, \lambda_1 + \lambda_2)$ *BIBD exists.*

Theorem (complementation design)

A (v, b, r, k, λ) *BIBD* $(n \geq k + 2)$ *exists iff a* $(v, b, b - r, v - k, b - 2r + \lambda)$ *BIBD exists.*

Proof: Handwritten Notes $(V, \mathcal{B})$: (v, k, λ) BIBD $(V, \bar{\mathcal{B}})$

$\bar{\mathcal{B}} = \{ V \setminus B \mid B \in \mathcal{B} \}$ $\boxed{k \leq \frac{v}{2}}$

Outline

Cyclic BIB designs

$(\mathbb{Z}_v, +)$: cyclic group

$\mathbb{Z}_v = \{0, 1, \dots, v-1\} \pmod{v}$

Cyclic BIBD

Let $V = \mathbb{Z}_v$. For a (v, k, λ) BIBD $(\mathbb{Z}_v, \mathcal{B})$, if $\mathcal{B} + 1 = \mathcal{B}$ holds, then $(\mathbb{Z}_v, \mathcal{B})$ is called a cyclic design (巡回デザイン), where

$$\mathcal{B} + 1 := \{B + 1 : B \in \mathcal{B}\}.$$

and

$$B + 1 := \{x + 1, y + 1, z + 1\} \quad \text{for } B = \{x, y, z\}.$$

Example: ⏩ Jupyper Notebook

Difference families

- For $D \subset \mathbb{Z}_v$, as a multiset, $\Delta(D) = \{x - y : x, y \in D_i, x \neq y\}$.

Difference families; DF

The family $\mathcal{D} = \{D_1, \ldots, D_s\}$ of subsets of $\mathbb{Z}_v$ is called a (v, k, λ) difference family (差集合族; DF) over $\mathbb{Z}_v$, or a cyclic difference family (巡回差集合族; CDF), if all the following condition holds.

1. $|D_i| = k$ $(1 \leq i \leq s)$;
2. The multiset
$$\bigcup_{i=1}^{s} \Delta(D_i)$$
contains every element in $\mathbb{Z}_n \setminus \{0\}$ for exactly λ times.

The subsets $D_1, \ldots, D_s$ are called base block (基底ブロック).

Cyclic difference families $\implies$ cyclic BIBD

Proposition DF-1

The number of base blocks of a (v, k, λ) CDF is $\frac{\lambda(v-1)}{k(k-1)}$.

Proof: Handwritten Notes

Theorem

If there exists a (v, k, λ) CDF, then there exists a cyclic (v, k, λ) BIBD.
Explicitly, for a (v, k, λ) CDF $\mathcal{D}$, by denoting

$$\mathcal{B} = \{D_i + j : D_i \in \mathcal{D}, j \in \mathbb{Z}_v\},$$

$(\mathbb{Z}_v, \mathcal{B})$ is a cyclic (v, k, λ) BIBD.

Outline

Steiner triple systems

Steiner triple system; STS

A $(v, k = 3, \lambda = 1)$ BIBD is called a Steiner triple system (シュタイナー三重系; STS), denoted by STS(v).

- If there exits an STS(v), then $v \equiv 1, 3 \pmod 6$.
- Bose construction (for $v \equiv 3 \pmod 6$) and Skolem construction (for $v \equiv 1 \pmod 6$) are well-known direct constructions for STS(v).

Theorem

An STS(v) exists iff $v \equiv 1, 3 \pmod 6$.

Primitive root mod p

- Let p be a prime. For $a \in \mathbb{Z}_p \setminus \{0\}$, the smallest n $(1 \leq n \leq p-1)$ such that $a^n \equiv 1 \pmod{p}$ is the order (位数) of a.
- An element of order $p-1$ is called a primitive root (原始根) mod p.
- $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$ is a multiplicative cyclic group of order $p-1$. A primitive root mod p is a generator of the group $\mathbb{Z}_p^*$.

  $\mathbb{Z}_p^* = \{ g, g^2, \ldots, g^{p-2}, g^{p-1} = 1 \}$
- Let α be a generator of $\mathbb{Z}_p^*$. For any $f \mid p-1$, α^f generates a subgroup of $\mathbb{Z}_p^*$, which is of order $(p-1)/f$.

Example: Jupyper Notebook

Cyclotomic construction for STS

Theorem

Let $p = 6t + 1$ be a prime and let α be a primitive root mod p. Let

$$D_i = \{\alpha^i, \alpha^{2t+i}, \alpha^{4t+i}\} \quad \text{and} \quad B_{i,j} = D_i + j, \qquad \text{for } 0 \le i \le t-1, j \in \mathbb{Z}_p$$

$D_i = \alpha^i \cdot \{1, \omega, \omega^2\}$

and

$$\mathcal{B} = \{B_{i,j} : 0 \le i \le t-1, j \in \mathbb{Z}_p\}.$$

Then $(\mathbb{Z}_p, \mathcal{B})$ is a cyclic STS(p).
Moreover, $\mathcal{D} = \{D_i : 0 \le i \le t-1\}$ is a $(v, 3, 1)$ CDF. (Cyclic BIBD a base block)

- α^{2t} is a generator of the subgroup of $\mathbb{Z}_p^*$, which is of order 3.
- In other words, $\omega := \alpha^{2t}$ is a cubic root of unity in $\mathbb{Z}_p^*$, i.e., $\omega^3 = 1$.

$\omega^3 = (\alpha^{2t})^3 = \alpha^{6t} = \alpha^{p-1} = 1$

Example of STS(13) via cyclotomic construction

- $p = 6t + 1 = 13$, $t = 2$
- Take $\alpha = 2$, then $\omega = \alpha^{2t} = 16 \equiv 3 \pmod{13}$
- $D_0 = \{1, 3, 9\}$, $D_1 = \{2, 6, 5\}$

Example: Jupyper Notebook

Heffter's Difference Problem

difference triple

Let v be an odd integer. The triple $\{x, y, z\} \subset \{1, 2, \dots, (v-1)/2\}$ is a difference triple if

- $x + y = z$ $(x < y < z)$, or
- $x + y + z \equiv 0 \pmod{v}$.

Moreover, $B(T) := \{0, x, x+y\}$ is called the associated base block of T.

Heffter's Difference Problem

For $v \equiv 1, 3 \pmod 6$, let $t = \cancel{\lfloor t/6 \rfloor}$ $\lfloor \frac{v}{6} \rfloor$. Let $\mathcal{T} = \{T_1, T_2, \dots, T_t\}$ be a collection of difference triples. Then $\mathcal{T}$ is said to be a solution of Heffter's Difference Problem (HDP), denoted by HDP(v), if

- if $v \equiv 1 \pmod 6$, $\bigcup_{i=1}^{t} T_i = [1, \frac{v-1}{2}]$;
- if $v \equiv 3 \pmod 6$, $\bigcup_{i=1}^{t} T_i = [1, \frac{v-1}{2}] \setminus \{\frac{v}{3}\}$.

Heffter's Difference Problem $\iff$ Cyclic STS

Theorem

For any $v \equiv 1, 3 \pmod 6$, there exists a cyclic STS(v) iff there exists an HDP(v).

Theorem (Pelteson, 1939)

For any $v \equiv 1, 3 \pmod 6$ with $v \geq 7$, $v \neq 9$, there exists an HDP(v).

Theorem

For any $v \equiv 1, 3 \pmod 6$ with $v \geq 7$, $v \neq 9$, there exists a cyclic STS(v).

Outline

Pairwise balanced design

Pairwise balanced design

Let K be a finite set of positive integers. Let V be a finite set and $\mathcal{B}$ be a family of subsets of V. The pair $(V, \mathcal{B})$ is a (v, K, λ) pairwise balanced design (PBD) if the all the following conditions hold.

1. $|V| = v$,
2. For any $B \in \mathcal{B}$, $|B| \in K$, where $v \geq \max K$.
3. For any pair of points $\{x, y\} \subseteq V$, there are exactly λ blocks $B \in \mathcal{B}$ containing $\{x, y\}$.

- When $K = \{k\}$, a (v, K, λ) PBD is just a (v, k, λ) BIBD.
- E.g. $(v, \{3, 5\}, 1)$ PBD $\iff$ decomposition of K_v into K_3 and K_5.

Group divisible design

Group divisible design

Let K and G be finite sets of positive integers. Let V be a finite set and $\mathcal{B}$ be a family of subsets of V. The pair $(V, \mathcal{G}, \mathcal{B})$ is a (v, G, K, λ) group divisible design (GDD) if

i. $|V| = v$,
ii. $\mathcal{G} = \{V_1, V_2, \ldots, V_m\}$ is a partition of V, i.e., $V_i \cap V_j = \emptyset$ and $\bigcup_{i=1}^{m} V_i = V$. The subsets V_i are called groups (グループ).
iii. For any $V_i \in \mathcal{G}$, $|V_i| \in G$ where $v > \max G$.
iv. For any $B \in \mathcal{B}$, $|B| \in K$, where $v \geq \max K$.
v. For any $V_i \in \mathcal{G}$ and $B \in \mathcal{B}$, $|V_i \cap B| \leq 1$.
vi. For any pair of points x, y from difference groups, there are exactly λ blocks $B \in \mathcal{B}$ containing $\{x, y\}$.
vii. ~~For any pair of points x, y from the same group, no block contains $\{x, y\}$.~~ $(\Leftrightarrow (v))$

GDD and Transversal Designs

- When $G = \{1\}$, a (v, G, K, λ) GDD is just a (v, K, λ) PBD.
- When $G = \{g\}$, where $g \geq 2$, the GDD is said to be of type $g^{v/g}$.
- When $G = \{g\}$, $K = \{k\}$, a (v, G, K, λ) GDD is a transversal design (横断デザイン), denoted by TD(g, k, λ).

Theorem

The following are equivalent.

1. *TD*$(g, k, 1)$*,*
2. *OA*$(N = g^2, k, g, 2)$ *(*$\lambda = 1$*),*
3. $k - 2$ *MOLS(*g*).*

Latin square of order $n \iff \mathrm{TD}(3, n, 1)$

- $n = 7$
- $X = (x_{r,c}) =$

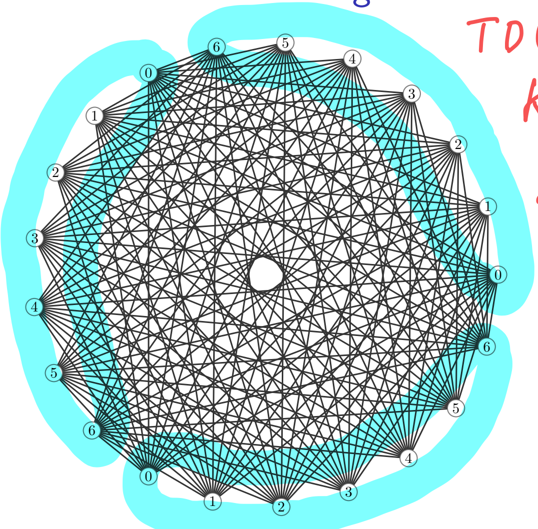
0	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

- $G_{\text{row}} = \{r_1 := (r, 1) \mid 0 \le r \le n-1\}$,
  $G_{\text{col}} = \{c_2 := (c, 2) \mid 0 \le c \le n-1\}$,
  $G_{\text{ele}} = \{e_3 := (e, 3) \mid 0 \le e \le n-1\}$,
- $V = G_{\text{row}} \cup G_{\text{col}} \cup G_{\text{ele}} = \mathbb{Z}_n \times \{1,2,3\}$
- $\mathcal{G} = \{G_{\text{row}}, G_{\text{col}}, G_{\text{ele}}\}$
- $\mathcal{B} = \{\{r_1, c_2, e_3\} \mid 0 \le r, c \le n-1, x_{r,c} = e\}$
- $(V, \mathcal{G}, \mathcal{B})$ is a $\mathrm{TD}(3, n, 1)$.

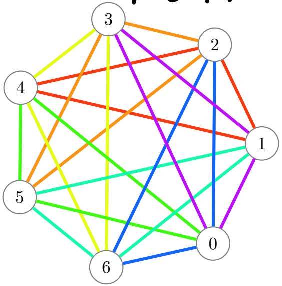
Construct new BIBD using GDD : recursive construction

$TD(3,n,1) \Leftrightarrow$ (divide and coquar)
分割統治法

$K_{n,n,n}$ の △ decomp.



Complete 3-partite graph $K_{7,7,7}$



Complete graph K_7

$\underset{K_{21}}{STS(21)} = TD(3,7,1) + STS(7)$

Outline

Combinatorial t-designs

Combinatorial t-design

Let V be a finite set and $\mathcal{B}$ be a family of subsets of V. Then $(V, \mathcal{B})$ is a t-(v, k, λ) design if

1. $|V| = v$,
2. For any $B \in \mathcal{B}$, $|B| = k$.
3. For any t-subset $T = \{x_1, x_2, \ldots, x_t\} \subseteq V$, there are exactly λ blocks containing T.

- When $t = 2$, a 2-(v, k, λ) design is just a (v, k, λ) BIBD.
- To construct t-(v, k, λ) designs with large t is quite difficult.
  - A t-$(v, k, \lambda = 1)$ design is also called a Steiner system.
  - For $\lambda = 1$ and $t \geq 4$, only finitely many examples.
  - For $\lambda = 1$ and $t \geq 6$, no known example.
- The notion of PBD can be generalized to t-wise balanced designs.
- The t-design version of GDD can also be defined. But there are many variations for $t \geq 3$.

Hadamard designs

Theorem

Let $H = (h_{i,j})$ $(i, j \in [4k])$ *be an Hadamard matrix of order* $4k$. *Let*

$$B_{i,i'} = \{j : h_{i,j} = h_{i',j}\}, \quad \overline{B_{i,i'}} = \{j : h_{i,j} \neq h_{i',j}\} \qquad (i \neq i').$$

and

$$\mathcal{B} = \{B_{i,i'}, \overline{B_{i,i'}} : i, i' \in [4k], i \neq i'\}.$$

Then $(X = [4k], \mathcal{B})$ *is a* 3-$(4k, 2k, k-1)$ *design.*

Theorem

There exists a 3-$(4k, 2k, k-1)$ *design* $\iff$ *there exists an Hadamard matrix of order* $4k$.

Homework assignments (レポート課題) for 2nd day

Exercise 1

Construct Hadamard matrix $\mathbf{H}_n$ for $n = 12$ using Paley's construction. $p=11$

$n=p+1$

Exercise 2

Construct a cyclic STS(19) (equivalently, a $(19, 3, 1)$-DF) using cyclotomic construction.

$p=19$

- You are encouraged to use computer programs for the assignments.
- If possible, please submit your program source codes together with the results of designs.
- Deadline: 6th Sept., 23:59:59