

## 集中講義 応用数学特論Ⅱ

## Day 2 アダマール行列・BIB デザイン

担当：盧 曉南 (山梨大学)

[xnlu@yamanashi.ac.jp](mailto:xnlu@yamanashi.ac.jp)

2021 年 8 月 26 日

## — 本日の内容 —

本日は組合せデザイン理論において (ラテン方格とともに) 最も基本的な組合せ構造であるアダマール行列と BIB デザインを紹介する.

1. 天秤の秤量計画とアダマール行列, アダマール行列の D-最適性, アダマール行列の構成法 (Kronecker 積の構成法, Paley の構成法)
2. バネばかりの秤量計画と BIB デザイン, BIBD のパラメータにおける関係式, Fisher 不等式, 和デザインと補デザイン
3. シュタイナー三重系 (Steiner triple system; STS), 巡回 STS, 差集合族
4. Pairwise balanced design, group divisible design
5. 組合せ  $t$  デザイン, アダマール・デザイン

## 0 記号

- $A^T$ : 行列  $A$  の転置行列 (transpose)
- $\det(A)$ : 行列  $A$  の行列式 (determinant)
- $I_n$ :  $n$  次単位行列 (identity matrix)
- $J_n$ :  $n$  次全 1 行列 (all-one matrix)

## 1 アダマール行列

**定義 1.1.** 成分が  $\pm 1$  の  $n \times n$  行列  $H$  において,  $H^T H = nI_n$  を満たすとき,  $H$  はアダマール行列 (Hadamard matrix) という.

**例 1.2.**  $n = 1, 2, 4$  のアダマール行列  $H_n$ .

$$H_1 = \begin{bmatrix} 1 \end{bmatrix}, \quad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

**命題 1.3.**  $H$  がアダマール行列であるなら,  $H^T$  も  $-H$  もアダマール行列である.

**命題 1.4.**  $n$  次アダマール行列  $H_n$  において  $\det(H_n) = n^{n/2}$ .

**命題 1.5.** 任意の  $n$  次  $\{\pm 1\}$  行列  $A_n$  において  $\det(A_n) \leq n^{n/2}$ .

**定義 1.6.**  $n$  次  $\{\pm 1\}$  行列の集合  $\mathcal{A}_n$  において、行列式の値が最大になる行列  $A \in \mathcal{A}_n$ , つまり,  $\det(A) = \max\{\det(A) : A \in \mathcal{A}_n\}$  を満たす  $A \in \mathcal{A}_n$  は  $\mathcal{A}_n$  において  $D$ -最適 (D-optimal) という.

**注 1.7.**  $n$  次アダマール行列  $H_n$  は  $n$  次  $\{\pm 1\}$  行列全体の集合  $\mathcal{A}_n$  において  $D$ -最適である.

**定理 1.8.**  $n$  次 ( $n \geq 4$ ) アダマール行列  $H_n$  が存在するならば,  $n$  は必ず 4 の倍数である.

**定理 1.9.**  $H_n, H_k$  をそれぞれ  $n$  次と  $k$  次のアダマール行列とする.  $H_n$  と  $H_k$  のクロネッカー積 (Kronecker product)  $H_n \otimes H_k$  は  $nk$  次のアダマール行列である.

**系 1.10.** 任意の正整数  $m$  に対して  $2^m$  次のアダマール行列が存在する.

**予想 1.11** (アダマール予想). 任意の  $n \equiv 0 \pmod{4}$  に対して,  $n$  次のアダマール行列が存在する.

**定義 1.12.** 奇素数  $p$  において, 整数  $a$  が  $p$  を法とする完全平方と合同であるとき,  $a$  は法  $p$  の平方剰余 (quadratic residue) といい, そうでないとき, 法  $p$  の平方非剰余 (quadratic non-residue) という.

また,  $a$  と  $p$  におけるルジャンドル記号 (Legendre symbol) は次のように定義する.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ は法 } p \text{ の平方剰余,} \\ -1, & a \text{ は法 } p \text{ の平方非剰余,} \\ 0, & a \equiv 0 \pmod{p}. \end{cases}$$

**命題 1.13.** 任意の整数  $a, b$  において,

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

**定理 1.14.** 奇素数  $p \equiv 3 \pmod{4}$  において,  $M = (m_{i,j})$  を次に定義する.

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

次の  $p+1$  次行列  $H$  はアダマール行列である.

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & M - I_p & \\ 1 & & & \end{pmatrix}.$$

もし時間があれば Williamson の構成法 (1944) を用いた 92 次アダマール行列の例を紹介する.

## 2 BIB デザイン

**定義 2.1.** 有限集合  $V$  と  $V$  の部分集合族  $\mathcal{B}$  において, 以下の 3 つの条件がすべて満たされるとき,  $(V, \mathcal{B})$  は  $(v, k, \lambda)$  釣り合い型不完備ブロックデザイン (Balanced Incomplete Block Design; BIBD) という.

- (i)  $|V| = v$ ,
- (ii) 任意の  $B \in \mathcal{B}$  に対して  $|B| = k$ ,
- (iii) 任意の 2 点  $\{x, y\} \subseteq V$  に対して  $\{x, y\}$  を含む  $B \in \mathcal{B}$  がちょうど  $\lambda$  個ある.

$\mathcal{B}$  の要素をブロック (block) といい,  $v, k, \lambda$  をそれぞれ要素数 (number of elements) または点数 (number of points), ブロックサイズ (block size), 会合数 (index) と呼ぶ.

注 2.2.  $V$  の部分集合をなす集合は部分集合族 (family of subsets) という. つまり,  $\mathcal{B} \subseteq 2^V$ . ここで,  $2^V$  は  $V$  の部分集合全体の集合を表し,  $V$  の冪集合 (power set) という.

命題 2.3.  $(v, k, \lambda)$  BIB デザイン  $(V, \mathcal{B})$  において,  $b := |\mathcal{B}| = vr/k$ .

命題 2.4.  $(v, k, \lambda)$  BIB デザイン  $(V, \mathcal{B})$  において, 任意の頂点  $v$  に対して  $v$  を含むブロック数が一定であり,  $r = \lambda(v-1)/(k-1)$  で表す.

注 2.5. 命題 2.3 と命題 2.4 によって,  $(v, b, r, k, \lambda)$  の中に 3 つが分かれば, 残りの 2 つが確定する.

注 2.6. パラメータ  $(v, b, r, k, \lambda)$  が与えられたとき, そのパラメータを持つデザインが存在するかどうかを判断する問題が存在性問題 (existence problem) といい, 組合せデザイン理論における最も基本的な問題である. 命題 2.3 と命題 2.4 の 2 つの等式を満たす  $(v, b, r, k, \lambda)$  は admissible (正当な) という.

$$\begin{aligned} vr &= bk \\ r(k-1) &= \lambda(v-1) \end{aligned}$$

定理 2.7 (Fisher 不等式).  $v > k$  となる  $(v, k, \lambda)$  BIB デザインにおいて, ブロック数  $b$  は  $b \geq v$  が成り立つ.

定義 2.8.  $v = b$  となる  $(v, k, \lambda)$  BIB デザインは対称デザイン (symmetric design) という.

定理 2.9 (Bruck–Ryser–Chowla 定理, 1949–1950). 対称  $(v, k, \lambda)$  BIB デザインが存在するならば, 次が満たされる.

- (i)  $v$  が偶数であるとき,  $k - \lambda$  が平方数である.
- (ii)  $v$  が奇数であるとき,  $z^2 = (k - \lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$  となるような整数  $x, y, z$  が存在する.

Bruck–Ryser–Chowla 定理 2.9 の証明は詳しく説明しないが, 「有限射影幾何」の回に射影平面の Bruck–Ryser 定理 (BRC 定理はその拡張版) の証明を紹介する.

定理 2.10 (和デザイン; sum).  $(v, k, \lambda_1)$  BIB デザインと  $(v, k, \lambda_2)$  BIB デザインが存在するならば  $(v, k, \lambda_1 + \lambda_2)$  BIB デザインが存在する.

定理 2.11 (補デザイン; complementation).  $(v, b, r, k, \lambda)$  BIB デザイン ( $n \geq k + 2$ ) が存在するならば  $(v, b, b - r, v - k, b - 2r + \lambda)$  BIB デザインが存在する.

注 2.12.  $k \leq v/2$  のデザインを考えることは十分である.

### 3 巡回デザインと差集合族

定義 3.1. 点集合  $V = \mathbb{Z}_v$  上の  $(v, k, \lambda)$  BIB デザイン  $(\mathbb{Z}_v, \mathcal{B})$  において,  $\mathcal{B} + 1 = \mathcal{B}$  が成り立つとき,  $(\mathbb{Z}_v, \mathcal{B})$  は巡回デザイン (cyclic design) という. ここで,  $\mathcal{B} + 1 := \{B + 1 := \{x + 1, y + 1, z + 1\} : B = \{x, y, z\} \in \mathcal{B}\}$ .

定義 3.2. 点集合  $\mathbb{Z}_v$  上の集合族  $\mathcal{D} = \{D_1, \dots, D_s\}$  において, 以下の条件がすべて満たされるとき,  $\mathcal{D}$  は  $\mathbb{Z}_v$  の  $(v, k, \lambda)$  差集合族 (difference family; DF) または  $(v, k, \lambda)$  巡回差集合族 (cyclic difference family; CDF) という.

- (i)  $|D_i| = k$  ( $1 \leq i \leq s$ );

(ii) 多重集合として

$$\bigcup_{i=1}^s \Delta(D_i)$$

に  $\mathbb{Z}_n \setminus \{0\}$  の各要素がちょうど  $\lambda$  回現れる．ここで，

$$\Delta(D_i) = \{x - y : x, y \in D_i, x \neq y\}.$$

このとき， $D_1, \dots, D_s$  は基底ブロック (base block) という．

**定理 3.3.**  $(v, k, \lambda)$  差集合族の基底ブロック数は  $\frac{\lambda(v-1)}{k(k-1)}$  である．

**定理 3.4.**  $(v, k, \lambda)$  巡回差集合族が存在するならば  $(v, k, \lambda)$  巡回 BIB デザインが存在する． $\mathbb{Z}_v$  の  $(v, k, \lambda)$  差集合  $\mathcal{D}$  が与えられたとき， $\mathcal{B} = \{D_i + j : D_i \in \mathcal{D}, j \in \mathbb{Z}_v\}$  とし， $(\mathbb{Z}_v, \mathcal{B})$  は  $(v, k, \lambda)$  巡回 BIB デザインである．

## 4 シュタイナー三重系

**定義 4.1.**  $(v, k = 3, \lambda = 1)$  BIBD はシュタイナー三重系 (Steiner triple system; STS) といい， $\text{STS}(v)$  と書く．

**注 4.2.** 命題 2.3 と命題 2.4 によって， $\text{STS}(v)$  が存在するための必要条件は  $v \equiv 1, 3 \pmod{6}$ ．

**注 4.3.**  $v \leq k$  を満たすため， $v \geq 7$  とする．

**定理 4.4.** 任意の  $v \equiv 1, 3 \pmod{6}$  に対して  $\text{STS}(v)$  が存在する．

Bose の構成法や Skolem の構成法は STS の (標準的な) 直接構成法として良く知られているが，この講義では飛ばしておく．これから，差 (集合族) の方法 (difference methods) を用いたアプローチを 2 つ紹介する．

**注 4.5.** 定理 3.3 によって， $(v, 3, 1)$  差集合族が存在するための必要条件は  $v \equiv 1 \pmod{6}$ ．

**定義 4.6.**  $p$  を素数とする． $a \in \mathbb{Z}_p \setminus \{0\}$  に対して， $a^n \equiv 1 \pmod{p}$  となる最小の  $n$  ( $1 \leq n \leq p-1$ ) は  $a$  の位数 (order) という．また，位数  $p-1$  の要素は法  $p$  の原始根 (primitive root) という．

**定理 4.7.** 素数  $p = 6t + 1$  において， $\alpha$  を法  $p$  の原始根とする．

$$B_{i,j} = \{\alpha^i + j, \alpha^{2t+i} + j, \alpha^{4t+i} + j\}, \quad 0 \leq i \leq t-1, j \in \mathbb{Z}_p$$

とし，

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

とおく．このとき， $(\mathbb{Z}_p, \mathcal{B})$  は巡回  $\text{STS}(p)$  である．

**定義 4.8.**  $v$  を正の奇数とする．集合  $\{x, y, z\} \subset \{1, 2, \dots, (v-1)/2\}$  において，次のいずれかの条件が満たされるとき， $T = \{x, y, z\}$  は difference triple という．

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

このとき， $B(T) := \{0, x, x + y\}$  とし， $B(T)$  は  $T$  に対応する基底ブロックという．

**定義 4.9.**  $v \equiv 1, 3 \pmod{6}$  とし， $t = \lfloor t/6 \rfloor$  とする．Difference triple の集合  $\mathcal{T} = \{T_1, T_2, \dots, T_t\}$  において，以下の条件が満たされるとき， $\mathcal{T}$  は Heffter's Difference Problem (HDP) の解といい， $\text{HDP}(v)$  と書く．

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

**定理 4.10.**  $v \equiv 1, 3 \pmod{6}$  に対して, 巡回 STS( $v$ ) が存在する  $\iff$  HDP( $v$ ) が存在する.

**定理 4.11** (Pelteson, 1939).  $v \equiv 1, 3 \pmod{6}$ ,  $v \geq 7$ ,  $v \neq 9$  に対して, HDP( $v$ ) が存在する.

**系 4.12.**  $v \equiv 1, 3 \pmod{6}$ ,  $v \geq 7$ ,  $v \neq 9$  に対して, 巡回 STS( $v$ ) が存在する.

もし時間があれば STS に関する研究話題をいくつか紹介したい. 例えば,  $e$ -sparse STS, STS の parallel class に関する問題 (parallel class が存在しない STS) 等.

## 5 Pairwise balanced design, group divisible design

**定義 5.1.** 有限集合  $V$ ,  $V$  の部分集合族  $\mathcal{B}$  と正整数の集合  $K$  において, 次の条件がすべて満たされるとき,  $(V, \mathcal{B})$  は  $(v, K, \lambda)$  pairwise balanced design (PBD) という.

- (i)  $|V| = v$ ,
- (ii) 任意の  $B \in \mathcal{B}$  に対して  $|B| \in K$ . ここで,  $v > \max K$ .
- (iii) 任意の 2 点  $\{x, y\} \subseteq V$  に対して  $\{x, y\}$  を含む  $B \in \mathcal{B}$  がちょうど  $\lambda$  個ある.

特に,  $K = \{k\}$  のとき,  $(v, K, \lambda)$  PBD は単に  $(v, k, \lambda)$  BIBD になる.

**定義 5.2.** 有限集合  $V$ ,  $V$  の部分集合族  $\mathcal{B}, \mathcal{G}$  と正整数の集合  $K, G$  において, 次の条件がすべて満たされるとき,  $(V, \mathcal{G}, \mathcal{B})$  は  $(v, G, K, \lambda)$  group divisible design (GDD) という.

- (i)  $|V| = v$ ,
- (ii)  $\mathcal{G} = \{V_1, V_2, \dots, V_m\}$  は集合  $V$  の分割 (partition) となる. つまり  $V_i \cap V_j = \emptyset$  かつ  $\bigcup_{i=1}^m V_i = V$ . 部分集合  $V_i$  はグループ (group) と呼ぶ.
- (iii) 任意の  $V_i \in \mathcal{G}$  に対して  $|V_i| \in G$ . ここで,  $v > \max G$ .
- (iv) 任意の  $B \in \mathcal{B}$  に対して  $|B| \in K$ . ここで,  $v > \max K$ .  $B \in \mathcal{B}$  はブロック (block) と呼ぶ.
- (v) 任意の  $V_i \in \mathcal{G}$ ,  $B \in \mathcal{B}$  に対して  $|V_i \cap B| \leq 1$ .
- (vi) 異なるグループに属する任意の 2 点  $\{x, y\}$  に対して  $\{x, y\}$  を含む  $B \in \mathcal{B}$  がちょうど  $\lambda$  個ある.
- (vii) 同じグループに属する任意の 2 点  $\{x, y\}$  に対して  $\{x, y\}$  を含むブロックがない.

特に,  $G = \{1\}$  のとき,  $(v, G, K, \lambda)$  GDD は単に  $(v, K, \lambda)$  PBD になる.

**注 5.3.**  $G = \{g\}$ ,  $K = \{k\}$  のとき,  $(v, G, K, \lambda)$  GDD は横断デザイン (transversal design) といい, TD( $g, k, \lambda$ ) と書く.

**定理 5.4.** 以下の 3 つが同値である.

- (i) TD( $g, k, 1$ ),
- (ii) OA( $N = g^2, k, g, 2$ ) ( $\lambda = 1$ ),
- (iii)  $k - 2$  個 MOLS( $g$ ).

## 6 組合せ $t$ デザイン, アダマール・デザイン

**定義 6.1.** 有限集合  $V$  と  $V$  の部分集合族  $\mathcal{B}$  において, 次の条件がすべて満たされるとき,  $(V, \mathcal{B})$  は  $t$ -( $v, k, \lambda$ ) デザインという.

- (i)  $|V| = v$ ,
- (ii) 任意の  $B \in \mathcal{B}$  に対して  $|B| = k$ .
- (iii) 任意の  $t$  点部分集合  $T = \{x_1, x_2, \dots, x_t\} \subseteq V$  に対して  $T$  を含む  $B \in \mathcal{B}$  がちょうど  $\lambda$  個ある.

特に,  $2$ -( $v, k, \lambda$ ) デザインは単に  $(v, k, \lambda)$  BIBD になる.

**注 6.2.** PBD の「 $t$  デザイン」版として  $t$ -wise balanced design が定義できる.  $t \geq 3$  のとき, GDD の  $t$  デザイン類似もあるが, 拡張の仕方が唯一でないため, バリエーションがたくさんある.

**定理 6.3.**  $H = (h_{i,j})$  ( $i, j \in [4k]$ ) を  $4k$  次アダマール行列とする. ブロック  $B_{i,i'}, \overline{B_{i,i'}}$  を次に定義する.

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

また,  $\mathcal{B} = \{B_{i,i'}, \overline{B_{i,i'}} : i, i' \in [4k], i \neq i'\}$  とおく.  $(X = [4k], \mathcal{B})$  は  $3$ -( $4k, 2k, k-1$ ) デザインである.

**定理 6.4.**  $3$ -( $4k, 2k, k-1$ ) デザインが存在する  $\iff$   $4k$  次アダマール行列が存在する.

**注 6.5.** 定理 6.4 を証明するため, 対称デザイン (symmetric design) の概念が必要となり, もし時間があれば「有限射影幾何」の回に紹介する.

## レポート課題

**課題 1.** 定理 1.14 (Paley の構成法) を用いて  $n = 12$  のアダマール行列  $H_n$  を求めよ.

**課題 2.** 定理 4.7 (cyclotomic 構成法) を用いて巡回 STS(19), すなわち,  $(19, 3, 1)$  巡回差集合族を求めよ.

**注意:** プログラミングを用いて課題を完成するのは大歓迎. その場合, (可能な限り) プログラムのソースコードも PDF に添付して提出してください.

## 参考文献

- [1] S. T. Dougherty. *Combinatorics and Finite Geometry*. Springer, 2020.
- [2] C. C. Lindner and C. A. Rodger. *Design Theory*. Chapman and Hall/CRC, 2nd edition, 2008.
- [3] D. Raghavarao. *Constructions and Combinatorial Problems in Design of Experiments*. John Wiley & Sons, 1971.
- [4] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, 2nd edition, 2001.
- [5] Z.-X. Wan. *Design Theory*. World Scientific, 2009.