# 離散数理工学　第 7 回

離散代数：ブロック・デザイン

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2023 年 11 月 28 日

最終更新：2023 年 11 月 19 日　23:52



## 今日の目標

**今日の目標**

ブロック・デザインに関して次ができるようになる

- 基本的な性質を証明できるようになる
- 組合せ配置に関する問題を解決できるようになる



## 復習：次の性質を満たす集合の集合は存在するか？

正整数 $m, q$，有限集合 $X$，$|X| = v$

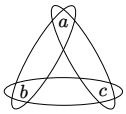
**問題**

$m$ 個の集合 $A_1, A_2, \ldots, A_m \subseteq X$ で次を満たすものは存在するか？

- $|A_1| = |A_2| = \cdots = |A_m| = q + 1$
- 任意の異なる $i, j \in \{1, 2, \ldots, m\}$ に対して
  $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- 任意の異なる $x, y \in X$ に対して
  $x, y \in A_i$ となる $i \in \{1, 2, \ldots, m\}$ が一意に存在する

例：$X = \{a, b, c\}$，$v = 3$，$m = 3$，$q = 1$

$A_1 = \{a, b\}, A_2 = \{a, c\}, A_3 = \{b, c\}$






## 復習：次の性質を満たす集合の集合は存在するか？ — 有限射影平面

正整数 $m, q$，有限集合 $X$，$|X| = v$

**問題**

$m$ 個の集合 $A_1, A_2, \ldots, A_m \subseteq X$ で次を満たすものは存在するか？

- $|A_1| = |A_2| = \cdots = |A_m| = q + 1$
- 任意の異なる $i, j \in \{1, 2, \ldots, m\}$ に対して
  $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- 任意の異なる $x, y \in X$ に対して
  $x, y \in A_i$ となる $i \in \{1, 2, \ldots, m\}$ が一意に存在する

**前回の復習**

$q$ が素数のべき，$v = m = q^2 + q + 1$ のときには存在する
(位数 $q$ の射影平面を考えればよい)





## 目次







## ブロック・デザイン

正整数 $v \geq 2, k \geq 2, \lambda \geq 1$

**定義：ブロック・デザイン**

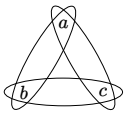
$(v, k, \lambda)$ **デザイン**とは，次を満たす $(X, \mathcal{D})$ という対

1. $|X| = v$
2. 任意の $B \in \mathcal{D}$ に対して，$|B| = k$
3. 異なる任意の $x, y \in X$ に対して，$x, y \in B$ を満たす $B \in \mathcal{D}$ の個数が $\lambda$

$$\lambda = |\{B \in \mathcal{D} \mid x, y \in B\}| \quad \forall\, x, y \in X, x \neq y$$

例：$X = \{a, b, c\}$，$v = 3$，$k = 2$，$\lambda = 1$

$\mathcal{D} = \{\{a, b\}, \{a, c\}, \{b, c\}\}$








## ブロック・デザイン：用語と記号

正整数 $v \geq 2, k \geq 2, \lambda \geq 1$

**定義：ブロック・デザイン**

$(v, k, \lambda)$ **デザイン**とは，次を満たす $(X, \mathcal{D})$ という対

1. $|X| = v$
2. 任意の $B \in \mathcal{D}$ に対して，$|B| = k$
3. 異なる任意の $x, y \in X$ に対して，$x, y \in B$ を満たす $B \in \mathcal{D}$ の個数が $\lambda$

$$\lambda = |\{B \in \mathcal{D} \mid x, y \in B\}| \quad \forall\, x, y \in X, x \neq y$$

- $b = |\mathcal{D}|$
- $X$ の要素を **点** と呼ぶ
- $\mathcal{D}$ の要素を **ブロック** と呼ぶ





## 有限射影平面とブロック・デザイン

位数 $q$ の有限射影平面から $(v, k, \lambda)$ デザインが得られる

$$v = q^2 + q + 1, \quad k = q + 1, \quad \lambda = 1$$

**復習：有限射影平面**

$m$ 個の集合 $A_1, A_2, \ldots, A_m \subseteq X$，$|X| = v$ で次を満たすものは存在するか？

- $|A_1| = |A_2| = \cdots = |A_m| = q + 1$
- 任意の異なる $i, j \in \{1, 2, \ldots, m\}$ に対して
  $x \in A_i \cap A_j$ となる $x \in X$ が一意に存在する
- 任意の異なる $x, y \in X$ に対して
  $x, y \in A_i$ となる $i \in \{1, 2, \ldots, m\}$ が一意に存在する

$v = m = q^2 + q + 1$ のとき，位数 $q$ の有限射影平面と呼ぶ

## ブロック・デザイン：応用例

7 種類のワインを 7 人の評価者で品評したい

**公平にするため，次を満たすようにしたい**

- どのワインも，3 人の評価者が品評する
- どの 2 つのワインも，ある評価者が同時に品評する

**問題**

このような品評の仕方は可能か？





## ブロック・デザイン：応用例 — 解答例

7 種類のワインを 7 人の評価者で品評したい

**公平にするため，次を満たすようにしたい**

- どのワインも，3 人の評価者が品評する
- どの 2 つのワインも，ある評価者が同時に品評する

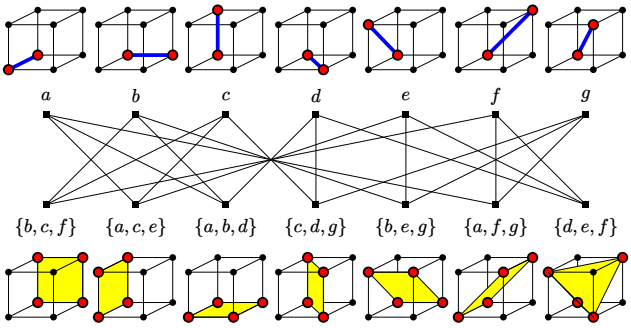
**解答例**

$(7,3,1)$ デザインを考えればよい (位数 $q=2$ の射影平面を考えればよい)





## 位数 2 の射影平面




対応

- 直線 $\leftrightarrow$ ワイン
- 平面 $\leftrightarrow$ 評価者





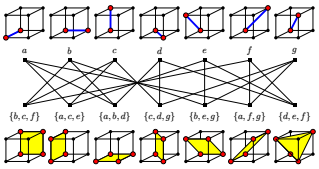
## ブロック・デザインの結合行列

$(v,k,\lambda)$ デザイン $(X,\mathcal{D})$

**定義：結合行列 (接続行列)**

$(X,\mathcal{D})$ の **結合行列** とは，次で定義される $X \times \mathcal{D}$ 行列 $N$

任意の $x \in X, B \in \mathcal{D}$ に対して，$n_{x,B} = \begin{cases} 1 & (x \in B \text{ のとき}), \\ 0 & (x \notin B \text{ のとき}) \end{cases}$



$$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$





## 目次







## 任意の点を含むブロックの数

$(v,k,\lambda)$ デザイン $(X,\mathcal{D})$，$b = |\mathcal{D}|$

**性質：任意の点を含むブロックの数**

任意の点 $x \in X$ に対して，
$x$ を含むブロックの数は $x$ に依らず一定で

$$\frac{(v-1)\lambda}{k-1}$$

である

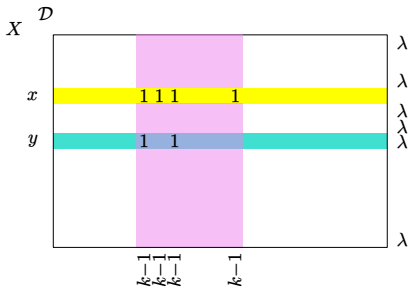
例：位数 $q$ の射影平面は $(q^2+q+1, q+1, 1)$ デザインで，

$\therefore$ 各点 $x \in X$ は $\dfrac{((q^2+q+1)-1)\cdot 1}{(q+1)-1} = q+1$ 個のブロックに含まれる





## 任意の点を含むブロックの数：証明のアイディア








## 任意の点を含むブロックの数：証明

証明：$x \in X$ を固定して，結合行列 $N$ を考える

$$\sum_{B \in \mathcal{D}: x \in B} \sum_{y \in X - \{x\}} n_{x,B} n_{y,B} = \sum_{B \in \mathcal{D}:\ x \in B} (k-1)$$
$$= (x \text{ を含むブロックの数}) \cdot (k-1),$$
$$\sum_{y \in X - \{x\}} \sum_{B \in \mathcal{D}: x \in B} n_{x,B} n_{y,B} = \sum_{y \in X - \{x\}} \lambda = (v-1)\lambda$$

この 2 つの和は等しいので，

$$(x \text{ を含むブロックの数}) = \frac{(v-1)\lambda}{k-1}$$

□

## ブロックの総数

$(v, k, \lambda)$ デザイン $(X, \mathcal{D})$，$b = |\mathcal{D}|$

**性質：ブロック・デザインにおけるブロックの総数**

$$b = \frac{v(v-1)\lambda}{k(k-1)}$$

証明：演習問題

例：位数 $q$ の射影平面は $(q^2+q+1, q+1, 1)$ デザインで，

$$\therefore \quad b = \frac{(q^2+q+1)((q^2+q+1)-1)\cdot 1}{(q+1)((q+1)-1)} = q^2+q+1$$





## ブロック・デザインの存在性

**問題**

$(v, k, \lambda)$ デザインが存在するような $v \geq 2, k \geq 2, \lambda \geq 1$ は何か？

先ほどの性質より，次が必要

- $k-1$ は $(v-1)\lambda$ の約数
- $k(k-1)$ は $v(v-1)\lambda$ の約数

**必要条件は満たすが，存在しない場合：例**

$v = 43, k = 7, \lambda = 1$ のとき (位数 6 の有限射影平面の存在性と等価)





## 目次







## 分解可能デザイン：例

ある $(9, 3, 1)$ デザイン

| $X$ | $\mathcal{D}$ | $\mathcal{D}_1$ | $\mathcal{D}_2$ | $\mathcal{D}_3$ | $\mathcal{D}_4$ |
|---|---|---|---|---|---|
| 1 | | 1 | 1 | 1 | 1 |
| 2 | | 1 | 2 | 2 | 2 |
| 3 | | 1 | 3 | 3 | 3 |
| 4 | | 2 | 1 | 3 | 2 |
| 5 | | 2 | 2 | 1 | 3 |
| 6 | | 2 | 3 | 2 | 1 |
| 7 | | 3 | 1 | 2 | 3 |
| 8 | | 3 | 2 | 3 | 1 |
| 9 | | 3 | 3 | 1 | 2 |





## 分解可能デザイン

**定義：分解可能デザイン**

$(v, k, \lambda)$ デザイン $(X, \mathcal{D})$ が **分解可能** であるとは，
次を満たす $\mathcal{D}$ の分解 $\{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_r\}$ が存在すること

- 任意の $i \in \{1, 2, \ldots, r\}$ と任意の $x \in X$ に対して
  ある $B \in \mathcal{D}_i$ が一意に存在して，$x \in B$

| $X$ | $\mathcal{D}$ | $\mathcal{D}_1$ | $\mathcal{D}_2$ | $\mathcal{D}_3$ | $\mathcal{D}_4$ |
|---|---|---|---|---|---|
| 1 | | 1 | 1 | 1 | 1 |
| 2 | | 1 | 2 | 2 | 2 |
| 3 | | 1 | 3 | 3 | 3 |
| 4 | | 2 | 1 | 3 | 2 |
| 5 | | 2 | 2 | 1 | 3 |
| 6 | | 2 | 3 | 2 | 1 |
| 7 | | 3 | 1 | 2 | 3 |
| 8 | | 3 | 2 | 3 | 1 |
| 9 | | 3 | 3 | 1 | 2 |





## 第 0 回講義より：カークマンの女学生問題 (1850 年)

**カークマンの女学生問題：設定**

- 15 人の女学生が 7 日間登校する
  - 必ず 3 人 1 組で登校する
  - 同じ 2 人が二度以上同じ組に入らない

**カークマンの女学生問題：問題**

このように登校させることはできるか？

分解可能 $(15, 3, 1)$ デザインの存在を尋ねている





## カークマンの女学生問題の類題

**設定**

- 9 人の女学生が 4 日間登校する
  - 必ず 3 人 1 組で登校する
  - 同じ 2 人が二度以上同じ組に入らない

**問題**

このように登校させることはできるか？

分解可能 $(9, 3, 1)$ デザインの存在を尋ねている

**今からの目標**

分解可能 $(9, 3, 1)$ デザインを構成する

(より一般的な構成の特殊な場合として)





## 有限アフィン平面

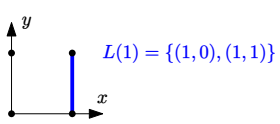
素数べき $q$

**定義：有限アフィン平面**

有限体 $\mathbb{F}_q$ 上の **アフィン平面** とは，次の点と直線の集合から成る

- 点の集合 $X = \mathbb{F}_q \times \mathbb{F}_q = \{(x, y) \mid x, y \in \mathbb{F}_q\}$
- 直線の集合 $\mathcal{L} = \{L(a, b) \mid a \in \mathbb{F}_q, b \in \mathbb{F}_q\} \cup \{L(c) \mid c \in \mathbb{F}_q\}$
  - $L(a, b) = \{(x, y) \mid x, y \in \mathbb{F}_q, y = ax + b\}$
  - $L(c) = \{(c, y) \mid y \in \mathbb{F}_q\}$

例：$q = 2$ のとき



## 有限アフィン平面における点の数

素数べき $q$

**定義：有限アフィン平面**

有限体 $\mathbb{F}_q$ 上の **アフィン平面** とは，次の点と直線の集合から成る

- 点の集合 $X = \mathbb{F}_q \times \mathbb{F}_q = \{(x, y) \mid x, y \in \mathbb{F}_q\}$
- 直線の集合 $\mathcal{L} = \{L(a, b) \mid a \in \mathbb{F}_q, b \in \mathbb{F}_q\} \cup \{L(c) \mid c \in \mathbb{F}_q\}$
  - $L(a, b) = \{(x, y) \mid x, y \in \mathbb{F}_q, y = ax + b\}$
  - $L(c) = \{(c, y) \mid y \in \mathbb{F}_q\}$

このとき，$|X| = |\mathbb{F}_q \times \mathbb{F}_q| = q^2$





## 有限アフィン平面における直線の数

素数べき $q$

**定義：有限アフィン平面**

有限体 $\mathbb{F}_q$ 上の **アフィン平面** とは，次の点と直線の集合から成る

- 点の集合 $X = \mathbb{F}_q \times \mathbb{F}_q = \{(x, y) \mid x, y \in \mathbb{F}_q\}$
- 直線の集合 $\mathcal{L} = \{L(a, b) \mid a \in \mathbb{F}_q, b \in \mathbb{F}_q\} \cup \{L(c) \mid c \in \mathbb{F}_q\}$
  - $L(a, b) = \{(x, y) \mid x, y \in \mathbb{F}_q, y = ax + b\}$
  - $L(c) = \{(c, y) \mid y \in \mathbb{F}_q\}$

**性質：有限アフィン平面における直線の数**

$|\mathcal{L}| = q^2 + q$

つまり，$L(a, b)$ や $L(c)$ は互いに異なる





## 有限アフィン平面における直線の数：証明

**証明すべきこと**

1. 異なる $(a, b)$ と $(a', b')$ に対して，$L(a, b) \neq L(a', b')$
2. 異なる $c$ と $c'$ に対して，$L(c) \neq L(c')$
3. 任意の $(a, b)$ と $c$ に対して，$L(a, b) \neq L(c)$

1 の証明：$L(a, b) = L(a', b')$ と仮定する

- $(x, y) \in L(a, b) = L(a', b')$ とすると，$y = ax + b$ かつ $y = a'x + b'$
- $\therefore ax + b = a'x + b'$ が任意の $x \in \mathbb{F}_q$ に対して成立
- $x = 0$ とすると，$b = b'$
- $x = 1$ とすると，$a + b = a' + b'$
- $\therefore (a, b) = (a', b')$ □

2 と 3 の証明：演習問題





## 有限アフィン平面からブロック・デザインへ

素数べき $q$

**性質：有限アフィン平面は分解可能デザインである**

有限体 $\mathbb{F}_q$ 上の有限アフィン平面 $(X, \mathcal{L})$ は
分解可能 $(q^2, q, 1)$ デザインである

証明すべきこと

1. $|X| = q^2$ $(v = q^2)$
2. 任意の直線 $L \in \mathcal{L}$ に含まれる点の数が $q$ である $(k = q)$
3. 任意の異なる 2 点 $(x, y), (x', y') \in X$ に対して，
   $(x, y)$ と $(x', y')$ を含む直線がちょうど 1 つある $(\lambda = 1)$
4. 分解可能である

「1 の証明」は済んでいる．「2 の証明」は簡単





## 2 点を通る直線が一意に存在：証明 (1)

3 の証明：異なる 2 点 $(x, y), (x', y')$ を考える

- $x = x'$ のとき，
  - $c = x = x'$ とおくと，この 2 点は $L(c)$ に含まれる
  - 一方で，$L(c')$ がこの 2 点を含むとすると，
    $c' = x = x' = c$ となり，$c' = c$ でなくてはならない
  - また，$L(a, b)$ がこの 2 点を含むとすると，
    $y = ax + b, y' = ax' + b$ なので，
    $y - y' = ax - ax' = 0$ となり，$y = y'$
    これは $(x, y)$ と $(x', y')$ が異なることに矛盾

**備忘録**

$L(a, b) = \{(x, y) \mid x, y \in \mathbb{F}_q, y = ax + b\}$，$L(c) = \{(c, y) \mid y \in \mathbb{F}_q\}$





## 2 点を通る直線が一意に存在：証明 (2)

3 の証明 (続き)：異なる 2 点 $(x, y), (x', y')$ を考える

- $x \neq x'$ のとき，
  - $(x, y), (x', y') \in L(a, b)$ とすると，$y = ax + b, y' = ax' + b$
  - このとき，$a = (y - y')(x - x')^{-1}, b = (x'y - xy')(x' - x)^{-1}$ と一意に決まる
  - 一方，$(x, y), (x', y') \in L(c)$ とすると，
    $x = x' = c$ だが $x \neq x'$ に矛盾 □

**備忘録**

$L(a, b) = \{(x, y) \mid x, y \in \mathbb{F}_q, y = ax + b\}$，$L(c) = \{(c, y) \mid y \in \mathbb{F}_q\}$





## 有限アフィン平面の分解可能性：証明 (1)

4 の証明：$\mathcal{L}$ を次の $q + 1$ 個の集合に分割する

- 任意の $i \in \mathbb{F}_q$ に対して，
  $\mathcal{L}_i = \{L(i, b) \mid b \in \mathbb{F}_q\}$
- $\mathcal{L}_q = \{L(c) \mid c \in \mathbb{F}_q\}$

**確認すべきこと**

任意の $i \in \{0, 1, \ldots, q - 1, q\}$ と任意の $(x, y) \in X$ に対して，
ある $L \in \mathcal{L}_i$ が一意に存在して，$(x, y) \in L$

$i \in \{0, 1, \ldots, q - 1\}$ の場合と $i = q$ の場合で分けて考える





## 有限アフィン平面の分解可能性：証明 (2)

$i \in \{0, 1, \ldots, q - 1\}$ のとき，

- 定義より，$\mathcal{L}_i = \{L(i, b) \mid b \in \mathbb{F}_q\}$
- 任意の $(x, y) \in X$ を考える
- $b = y - ix$ とすると，$(x, y) \in L(i, b)$
- 逆に，$(x, y) \in L(i, b)$ とすると，$y = ix + b$ より，$b = y - ix$

$i = q$ のとき，

- 定義より，$\mathcal{L}_q = \{L(c) \mid c \in \mathbb{F}_q\}$
- 任意の $(x, y)$ を考える
- $c = x$ とすると，$(x, y) \in L(c)$
- 逆に，$(x, y) \in L(c)$ とすると，$c = x$ □

## 有限アフィン平面：ここまでのまとめ

素数べき $q$

**定義：有限アフィン平面**

有限体 $\mathbb{F}_q$ 上の **アフィン平面** とは，次の点と直線の集合から成る

- 点の集合 $X = \mathbb{F}_q \times \mathbb{F}_q = \{(x, y) \mid x, y \in \mathbb{F}_q\}$
- 直線の集合 $\mathcal{L} = \{L(a, b) \mid a \in \mathbb{F}_q, b \in \mathbb{F}_q\} \cup \{L(c) \mid c \in \mathbb{F}_q\}$
  - $L(a, b) = \{(x, y) \mid x, y \in \mathbb{F}_q, y = ax + b\}$
  - $L(c) = \{(c, y) \mid y \in \mathbb{F}_q\}$

**性質：有限アフィン平面は分解可能デザインである**

有限体 $\mathbb{F}_q$ 上の有限アフィン平面 $(X, \mathcal{L})$ は
分解可能 $(q^2, q, 1)$ デザインである





## カークマンの女学生問題の類題：再掲

**問題**

- 9 人の女学生が 4 日間登校する
  - 必ず 3 人 1 組で登校する
  - 同じ 2 人が二度以上同じ組に入らない

**カークマンの女学生問題：問題**

このように登校させることはできるか？

分解可能 $(9, 3, 1)$ デザインの存在を尋ねている

**解答例**

有限体 $\mathbb{F}_3$ 上のアフィン平面を考えればよい





## $\mathbb{F}_3$ 上のアフィン平面

| $X$ \ $\mathcal{D}$ | | | | |
|---|---|---|---|---|
| | 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 | |





## 目次







## 今日のまとめ

**今日の目標**

ブロック・デザインに関して次ができるようになる

- 基本的な性質を証明できるようになる
- 組合せ配置に関する問題を解決できるようになる

有限体は離散数学，ブロック・デザインのみならず，
符号理論や暗号理論でも重要な役割を果たす