8/26 応用数学特論II

Proposition HM-2

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

Proof:

①
$$\det(H^T \cdot H) = \det(nI_n) = n^n.$$
$$\det(H^T \cdot H) = (\det(H))^2$$
$$\Leftarrow \quad \det(H) = \sqrt{n^n} = n^{n/2}.$$

② The (i,j)-entry of

$$A^T \cdot A = \begin{pmatrix} a_1^T \cdot a_1, & a_1^T a_2 \cdots & a_1^T a_n \\ \vdots & & \vdots \\ a_n^T \cdot a_1, & a_n^T \cdot a_2, \ \cdots, & a_n^T \cdot a_n \end{pmatrix},$$

are $a_i^T \cdot a_j = \langle a_i, a_j \rangle$, where

$$A = (a_1\ a_2 \cdots a_n) \qquad a_i \in \{\pm 1\}^n.$$

$$\langle a_i, a_j \rangle \leq n,$$

(inner product)

Moreover, $\langle a_i, a_j \rangle = n$ iff

$$a_i = a_j$$

$$\Rightarrow \det(A^T \cdot A) \leq n^n.$$

det: (essentially vol)

体積

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_2 \otimes H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_2$$

$$= \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

is also an Hadamard matrix.

$(*)\quad (A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$

By $(*)$, $(H_n \otimes H_k)^T \cdot (H_n \otimes H_k)$

$$= (H_n^T \otimes H_k^T) \cdot (H_n \otimes H_k)$$

$$= (H_n^T \cdot H_n) \otimes (H_k^T \cdot H_k)$$

$$= (n I_n) \otimes (k I_k)$$

$$= (nk) \cdot I_{nk}. \quad \blacksquare$$

Proposition HM-3

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

Proof: $H = (h_1, h_2, \ldots, h_n)$

$(h_i \in \{\pm 1\}^n.)$

△ The diagonal of $H^T H$ are $h_i^T \cdot h_i = n$.

△ The off-diagonal of $H^T H$ are $h_i^T \cdot h_j$ $(i \neq j)$

$h_1 = [1 \ 1 \ \ldots \ 1]^T$

$h_i^T \cdot h_1 = 0 \iff \boxed{\#\text{ of "1" in } h_i = \#\text{ of "}-1\text{" in } h_i}$

$\iff n \equiv 0 \pmod 2$

$$h_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}^T$$

$$h_2 = \begin{bmatrix} 1 & 1 & 1 & -1 & -1 & -1 \end{bmatrix}^T$$

$$h_3 = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{bmatrix}$$

$x_i \in \{\pm 1\}$

In $\{x_1 \ldots x_6\}$, there are
$n/2$ ~~three~~ "1"
$n/2$ ~~three~~ "-1"

$a = \# \begin{bmatrix} h_2 \\ h_3 \end{bmatrix}$ の中に $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ の数

$b = \#$ 〃 $\begin{bmatrix} 1 \\ -1 \end{bmatrix}$ の数

$c = \#$ 〃 $\begin{bmatrix} -1 \\ 1 \end{bmatrix}$ の数

$d = \#$ 〃 $\begin{bmatrix} -1 \\ -1 \end{bmatrix}$ の数.

by counting "1" & "-1" in h_2 & h_3

$$\begin{cases} a+b=\frac{n}{2} \\ c+d=\frac{n}{2} \\ a+c=\frac{n}{2} \\ b+d=\frac{n}{2} \end{cases}$$

$$h_2^T \cdot h_3 = 0$$

$$\Leftrightarrow \#\text{"}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\text{"} + \#\text{"}\begin{pmatrix} -1 \\ -1 \end{pmatrix}\text{"}$$

$$= \#\text{"}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\text{"} + \#\text{"}\begin{pmatrix} -1 \\ 1 \end{pmatrix}\text{"}$$

$$\Leftrightarrow b+c=a+d=\frac{n}{2}$$

$$\Longrightarrow a=b=c=d=\frac{n}{4}$$

$$\Longrightarrow n \equiv 0 \pmod 4$$

(i) $vr = bk$

(ii) $r(k-1) = \lambda(v-1)$

Incidence matrix of BIBD

$v \times b$ $(0,1)$-matrix

$$N = \begin{array}{c} \\ 0 \\ 1 \\ \vdots \\ v-1 \end{array} \begin{array}{c} \begin{array}{cccc} B_0 & B_1 & \cdots & B_{b-1} \end{array} \\ \left[\begin{array}{cccc} & & & \\ & & & \\ & & & \\ & & & \end{array} \right] \end{array}$$

(i, B_j) entry $= 1 \iff i \in B_j$

" $= 0 \iff i \notin B_j$

Basic properties of inc. mat.

(1) each block contains k points

$\Longleftrightarrow$ column sum of N is k

(2) each point $v \in V$ is contained in r blocks

$\Longleftrightarrow$ row sum of $N = r$

(1) & (2) $\Rightarrow$ $b \cdot k = v \cdot r$

(the # of "1" in N)

$\boxed{/ / /}$

(ii)

$$\begin{array}{c|cccccccc}
 & B_0 & B_1 & \cdots & B_r & B_{r+1} & \cdots & B_{b-1} \\
\hline
0 & 1 & 1 & \cdots & 1 & 0 & \cdots & 0 \\
1 & & & & & & & \\
\vdots & & & & & & & \\
v-1 & & & & & & &
\end{array}$$

Fact

(1) Each pair $\{0, x\}$

$x \in \{1, \ldots, v-1\}$

appears in λ blocks.

$\Rightarrow$ $($\# "1" $= \lambda(v-1)$

(2) has r col. in each of which

there are $(k-1)$ "1"s

(1) & (2) $\Longrightarrow$ $\lambda(v-1) = r(k-1)$. $\blacksquare$

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

$$\boxed{\mathbf{N}^\top \mathbf{1}_v = k\mathbf{1}_b} \leftarrow (1)$$

and

$$NN^T \quad \cancel{\mathbf{N}^\top\mathbf{N}} = \lambda \mathbf{J}_v + (r-\lambda)\mathbf{I}_v. \quad (2) \qquad \mathbb{1}_v = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

(1)

$$\begin{array}{c|c} & B_0 \quad B_1 \quad \cdots \quad B_{b-1} \\ \begin{array}{c} 0 \\ \vdots \\ v-1 \end{array} & \left[\begin{array}{c} \\ \\ \\ \end{array} \right] \end{array}$$

- $\boxed{\text{col sum} = \text{block size} = k = \text{\# "1" in each col}}$
- $\boxed{\text{row sum} = r}$

(2)

$$NN^T = \begin{bmatrix} r & & \lambda \\ & \ddots & \\ \lambda & & r \end{bmatrix}_{v \times v}$$

Fisher's ineq. $(b \geq v)$

$N: v \times b$

$$NN^T = (r-\lambda) I_v + \lambda J_v$$

To show $\operatorname{rank}(NN^T) = v$.

$$\boxed{\begin{array}{l} \circledcirc\ NN^T = \begin{pmatrix} r & & \lambda \\ & \ddots & \\ \lambda & & r \end{pmatrix} \\ \text{eigenvalues of } NN^T \text{ are} \\ (v-1)\text{個の } (r-\lambda) \\ 1\text{個の } (r-\lambda)+\lambda v = r+(v-1)\lambda \\ \qquad = r + r(k-1) = rk \end{array}}$$

$$\det(NN^T) = (r-\lambda)^{v-1} \cdot rk$$

$(r > \lambda) \Rightarrow \det(NN^T) \neq 0 \Leftrightarrow \operatorname{rank}(NN^T) = v.$

$\Rightarrow b \geq v.$

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

例: $D = \{0, 1, 3\} \subseteq \mathbb{Z}_7$

$$\Delta(D) = \{0-1,\ 0-3,\ 1-3,\ 1-0,\ 3-0,\ 3-1\}$$

$$= \{\pm 1, \pm 3, \pm 2\} \bmod 7$$

$$= \{1, 2, 3, 4, 5, 6\}$$

mod 7

$-1 \equiv$	6
$-2 \equiv$	5
$-3 \equiv$	4

$\Rightarrow \mathcal{D} = \{D\}$ is a $(7, 3, 1)$-CDF.

△ (v, k, λ)-BIBD において.

$$b = |\mathcal{B}| = \frac{vr}{k} = \frac{v}{k} \cdot \frac{\lambda(v-1)}{(k-1)}$$

△ (v, k, λ)-DF ($\Leftrightarrow$ cyclic (v, k, λ)-BIBD (without short orbit)

~~例~~ $\{0, 5, 10\} \bmod 15$

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

$$b' = \frac{1 \cdot (7-1)}{3 \cdot (3-1)} = \frac{6}{6} = 1.$$

- If there exits an STS(v), then $v \equiv 1, 3 \pmod 6$.

- $r = \dfrac{\lambda(v-1)}{k-1}$ For STS, $k=3$, $\lambda=1$

- $b = \dfrac{vr}{k}$

$\Rightarrow \quad r = \dfrac{v-1}{2}, \quad b = \dfrac{v(v-1)}{6}$

$r, b \in \mathbb{Z} \iff v \equiv 1, 3 \pmod 6$

$\mathbb{Z}_{13}^* = \{2, 4, 8, \boxed{3}, 6, 12, 11, \boxed{9}, 5, 10, 7, \boxed{1}\}$

$(\alpha = 2)$ $\mathbb{Z}_{13}^* = \langle \alpha \rangle$

($\mathbb{Z}_{13}^*$ is generated by α)

- $p = 13$
- $p - 1 = 12$
- e.g. $f = 4$

$f \mid p-1$

- $\alpha^f = 2^4 = 3 \pmod{13}$

$\langle \alpha^f \rangle = \{3, 9, \underset{27}{\underset{\shortparallel}{1}}\}$ is a subgroup of $\mathbb{Z}_{13}^*$

部分群

- Remark: $(\alpha^4)^3 = (3^4)^3$

$$\boxed{\alpha^{p-1} = 1}$$

↑ Fermat's little theorem

$$\shortparallel$$

$$1 = \alpha^{12}$$

equation

- $x = \alpha^4$ は $x^3 = 1$ の solution になる
- x は primitive cubic root of unity mod p

(原始) 三乗根