8/26 応用数学特論||

Proposition HM-2

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

Proof:

$$det(H^{T}\cdot H) = det(nI_{n}) = n^{n}$$
.
 $(det(H))^{2}$
 $det(H) = \sqrt{n^{n}} = n^{n}$.

The
$$(i,j)$$
 -entry of

$$A^{T} \cdot A = \begin{pmatrix} \alpha_{1}^{T} \cdot \alpha_{1}^{T} \cdot \alpha_{2}^{T} \cdot \alpha_{1}^{T} \cdot \alpha_{2}^{T} \cdot \alpha_{1}^{T} \cdot \alpha_{2}^{T} \cdot \alpha_{1}^{T} \cdot \alpha_{2}^{T} \cdot \alpha_{$$

$$A = (\alpha_1 \alpha_2 \cdots \alpha_n) \qquad \alpha_i \in \{\pm 1\}^h$$
.

 $\langle \alpha_i, \alpha_j \rangle \leq \eta$ (ihner product) Morever, <ai, a; >= n ac = a; \Rightarrow det $(A^{T} \cdot A) \leq h^{n}$. det: (essentially vol) 体精

$$H_{2}=\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_2 \otimes H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_1$$

$$= \begin{pmatrix} H_{\nu} & H_{\nu} \\ H_{\nu} & -H_{\nu} \end{pmatrix}$$

is also an Hadamand matrix.

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

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

$$= (nI_n) \otimes (kI_k)$$

$$\otimes (R \perp_k)$$

Proposition HM-3

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

Proof:
$$H = (k_1, k_2, ..., k_n)$$

 $(k_i \in \{\pm 1\}^n)$

the off-diagonal of HTH are his his (1'+j)

$$h_{i} = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}^{T}$$

$$h_{i} \cdot f_{i} = 0 \qquad \Rightarrow \qquad f '' 1'' \text{ in } h_{i}'$$

$$= \# \text{ of } '' - 1'' \text{ in } h_{i}'$$

$$\Rightarrow \qquad N \equiv 0 \pmod{2}$$

$$\Leftrightarrow$$
 $N \equiv 0 \pmod{2}$

1/2 three "-1" $Q = \# \begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix} \circ \# \begin{bmatrix} 1 \\ 1 \end{bmatrix} \circ \not b$ 门间车 d = 4 ,

[-1] a \$ 2.

$$C+d=\frac{n}{2}$$

$$a+c=\frac{h}{2}$$

$$b+d=\frac{h}{2}$$

by
$$a+b=\frac{n}{2}$$
 $h_2^Th_3=0$
Counting $c+d=\frac{n}{2}$ $f''(a) + f''(a)$
in h_2 $a+c=\frac{h}{2}$ $f''(a) + f''(a)$
 $h_2^Th_3=0$
 $f''(a) + f''(a)$
 $f''(a) + f''(a)$

n = 0 (md 4)

 $\Rightarrow a=b=c=d=\frac{h}{4}$

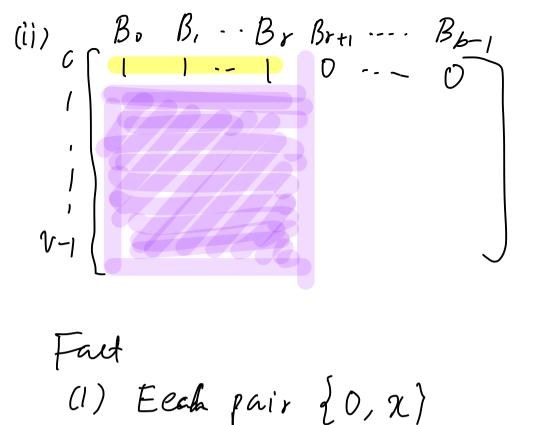
(i)
$$vr = bk$$

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

Incidence matrix of BIBD Vxb(0,1)-matrix

$$(i, B_j)$$
 entry = $| \Leftrightarrow i \in B_j$
 $| = o \Leftrightarrow i \notin B_j$

Basic properties of inc. mat. (1) each block contains k points Column cum of Nisk (2) each point NEV is contained in r blocks (=) YOW Sum of N = Y (1) & (2) => b.k=v.r (the # of "1" in N)



appears in λ blocks. $\Rightarrow \frac{1}{2} \left(\frac{1}{2} \right)^{n} = \lambda(\nu-1)$ (2) has γ col, in which there are $(k-1)^{n} 1^{n} 5$

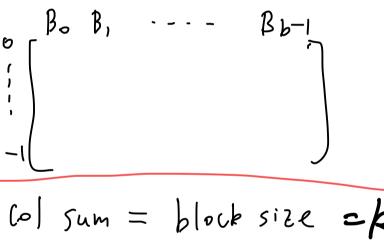
$$\chi = \chi(V-1) = \chi(k-1).$$

Theorem

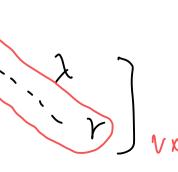
Let
$${f N}$$
 be a $v imes b$ $\{0,1\}$ -matrix. Then ${f N}$ is the incidence matrix of a (v,b,r,k,λ) BIBD iff

$$\mathbf{N}^{\mathsf{T}}\mathbf{1}_v=k\mathbf{1}_b$$
 \longleftarrow \bigcirc

 $\mathbf{N} \mathbf{N}^{\mathsf{T}} = \lambda \mathbf{J}_v + (r - \lambda) \mathbf{I}_v.$ 2 and



col sum = block size = #1" in each col



Fisher's ineq.
$$(b \ge v)$$
 $N: v \times b$
 $N N^{T} = (r - \lambda) I_{v} + \lambda J_{v}$

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

eigenvalues of NNT are

$$(v-1)(E \circ (r-\lambda))$$
 $(v-1)(E \circ (r-\lambda))$
 $(v-1)(E \circ (r-\lambda))$

⇒ b2v.

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

$$(3^i): \quad D = \{0, 1, 3\} \subseteq \mathbb{Z}_7$$

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

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

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

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

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

 $b = |B| = \frac{VV}{k} = \frac{V}{k}, \frac{\lambda(V-1)}{(k-1)}$

(V, k, λ) - OF (=) Cyclic (v, k, λ)-B10D (vithout short orbit)

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

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

\$ 0,5,10) mid (5)



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

$$0 \quad \gamma = \frac{\lambda(\nu-1)}{k-1} \qquad For STS, \\ k=3, \quad \lambda=1$$

$$0 \quad b = \frac{vr}{k}$$

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

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

$$2_{13}^{*} = \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, (\alpha = 2) \ 2_{13}^{*} = (\alpha) \ (2_{13}^{*} \text{ is generated by } \alpha)$$
 $p = 13$ o $p - 1 = 12$ o e.g., $f = 4$

• $d^{f} = 2^{q} = 3$ (mod 13)

($d^{f} > = \{3, 9, 1\}$ is a subgroup of 2_{13}^{*}

• Remark: $(d^{4})^{3} = (3^{4})^{3}$

• Remark: $(d^{4})^{3} = (3^{4})^{3}$

Fermat's $1 = \alpha^{12}$ equation

Fermat's $1 = \alpha^{12}$ equation

Fermat's $1 = \alpha^{12}$ equation

(Extensity mod p)

(Extensity mod p)