数理解析研究所講究録
第404巻 1980年 14-18

Hadamard 行列について

イリノイ大学　伊藤 昇
北大 理学部　木村 浩

H を $n(>2)$ 次の Hadamard 行列とする。すなわち $H=(h_{ij})=(\pm 1)$ で $H^t \cdot H = H \cdot H^t = nI$ をみたすものとする。$P=\{1,2,\cdots n\}$, $P^*=\{1^*,2^*,\cdots,n^*\}$ とし、$P\cup P^*$ の n 個からなる部分空間 α_i を次の様に定義する。

$$\alpha_i \ni j \longleftrightarrow h_{ij}=1,$$
$$\ni j^* \longleftrightarrow h_{ij}=-1.$$

さらに $\alpha_i^* = P\cup P^* - \alpha_i$ とおく。$B=\{\alpha_1,\cdots,\alpha_n\}$, $B^*=\{\alpha_1^*,\cdots,\alpha_n^*\}$. $P\cup P^*$ の元を点、$B\cup B^*$ の元を block と云う。このとき $M(H)=(P\cup P^*, B\cup B^*)$ を H の matrix design と呼ぶ。これは i, i^* を含む block は存在しないから 2-design ではない。又 $i, j\ (\neq i^*)$ を含む block の個数は $\frac{n}{2}$ 個である。

次に $i^{**}=i\ (1\leq i\leq n)$ と仮定しておく。G を次を満たす $P\cup P^*$ 上の置換全体の作る群とする。$\sigma(i)=j \longleftrightarrow$

$\sigma(i^*) = j^*$, $(B \cup B^*)^\sigma = B \cup B^*$. Gを$M(H)$の自己同型群と呼ぶ。これはHの自己同型群に同型である。

$\bar{P} = \{\bar{i} = \{i, i^*\} \mid 1 \le i \le n\}$, $\bar{B} = \{\bar{\alpha}_i = \{\alpha_i, \alpha_i^*\} \mid 1 \le i \le n\}$とおく。$\bar{G} = G/\langle \zeta \rangle$は$\bar{P}$, $\bar{B}$上の置換群と考えられる。ここで$\zeta = \pi(i, i^*) = \pi(\alpha_i, \alpha_i^*)$である。

[2]で伊藤は次の結果を得た。

「$\bar{G}$が$\bar{P}$上現在知られている2重可移群でregular normal subgroupを含まなければ次のいづれかである。(i) $n = q+1$, q =素数巾 $\equiv 3 \pmod 4$, Hはquadratic residue typeである。(ii) $n = 36$, $(\bar{G}, \bar{P}) \cong Sp(6, 2)$, Hは新しいものである。」

ここでは$\bar{G}$が$\bar{P}$上2重可移群でregular normal subgroupを含む場合を考える。次の予想の下にその性質をしらべた。

「上の仮定の下でHはelementary abelian group of order nのcharacter tableに相似である」

Kantor [3]の定理($\bar{G}$が$\bar{P}$上2重で,$\bar{B}$上faithfulでなければHは上のものに限る)によって以下$\bar{G}$は$\bar{B}$上faithfulとしてよい。

NをGの正規部分群($\ni \zeta$)で$N/\langle \zeta \rangle$が$\bar{G}$のregular normal subgroupとなるものとする。$n = 4$のときは良くわかっているから$n > 4$とする。置換論の一般的性質より$n = 2^m$

$(m>2)$ である。以下証明なしで性質を述べる。

Lemma 1. N は elementary abelian である。

Lemma 2. $\bar{G}$ は $\bar{B}$ 上 2 重可移である。

この lemma が以下の出発点である。Γ を ξ を含まない N の maximal subgroup の集合とする。$|\Gamma|=n$ で G は Γ 上に働く。

Lemma 3. Δ を $M\in\Gamma$ の $P\cup P^*$ 上の orbit とすれば任意の $\alpha\in B$ に対して $|\Delta\cap\alpha|=(n\pm\sqrt{n})/2$ が成り立つ。

この lemma より特に

Proposition 1. $\sqrt{n}$ は整数である。

Lemma 4. Γ は少なくとも 2 つ以上の G-conjugate class からなっている。

これよりただちに次を得る。

Proposition 2. G は可解ではない。

Lemma 5. p（素数）を $(|G|,(n-2)/2)$ の約数とすれば $i<m-1$ があって p は 2^i-1 の約数である。特に G は $\bar{P}$ 上 3 重可移ではない。

Lemma 6. G は $P\cup P^*$ 上の置換群として rank 4 である。

G の $P\cup P^*$ 上の permutation character $1_{G_a}^{G}$ $(a\in P)$ の irreducible character への分解を $1_G+\chi+\varphi_1+\varphi_2$ とす

3. ここでχは$(\bar{G}, \bar{P})$から出てくる次数$n-1$の character である。この character の性質より次を得る。

Lemma 7. Γは2つのG-conjugate class Γ_1, Γ_2からなっている。さらに$|G : N_G(M_i)| = |\Gamma_i| = \varphi_i(1)$としてよい。ただし$M_i \in \Gamma_i$.

Lemma 8. $\varphi_1(1) \geq \varphi_2(1)$とすれば$\varphi_1(1) = (n+\sqrt{n})/2$, $\varphi_2(1) = (n-\sqrt{n})/2$である。

NはP∨P*とregularであるからNの元とP∨P*の元を同一視できる。G_1はN上4つのorbitをもっているからそれを$\{1\}$, $\{\xi\}$, C_1, $C_2 = \xi C_1$とおく。$b \in C_1$に対して$u = |\{M \in \Gamma_1 \mid b \in M\}|$, $b \in C_2$に対して$v = |\{M \in \Gamma_1 \mid b \in M\}|$とおく。

Lemma 9. $u \neq v$.

C_1を$u > v$なる様に取っておく。

Proposition 3.

$$\bar{C_1}^2 = (n-1)\bar{1} + \frac{n-4}{2}\bar{C_1} + \frac{n}{2}\bar{C_2},$$

$$u = \frac{n+2\sqrt{n}}{4}, \quad v = \frac{n}{4}.$$

ここで$\bar{\ }$はNのgroup ringでのG_1-conjugateのclass sumである。

今後の問題としてelementary abelian group Nの部分集合C_1, C_2でProposition 3をみたすものがあるか、そしてそれはどんな性質をもっているかを知る必要がある。

References

1. M. Hall, Combinatorial theory, Blaisdell, 1967.

2. N. Ito, Hadamard matrices with doubly transitive automorphism groups, to appear.

3. W. M. Kantor, Automorphism groups of Hadamard matrices, J. Combinatorial Theory, 6 (1969), 279 – 281.