数理解析研究所講究録
第853巻 1993年 183-186

アダマール行列を群から作る

名城大理工 伊藤 昇 (Noboru Ito)

こんなことが出来たらいいなと思って付けた夢のようなタイトルです。位数$2n$の群から位数nのアダマール行列を作ろうとするのですが，その様な群はある条件を満足しないとなりません。群Gがその条件を満足するときアダマール群と呼ぶ。Gがアダマール群とは，Gがn-部分集合Dと元e^*でつぎの2条件を満足するものをふくむことです。

(1) $D \cap De^* = \emptyset$，e，e^*と異なるGの任意の元aについて$|D \cap Da| = n/2$，

(2) Gの任意の2元a，bについて$|Da \cap \{b, be^*\}| = 1$。

命題1．e^*はGの中心にふくまれ，位数2を持つ。

このときアダマール行列はつぎの様に作ります。Gをe^*-対にわけ，任意に番号付ける：$\{a_1, a_1e^*\}$，…，$\{a_n, a_ne^*\}$。各e^*-対からひとつの元b_iを任意にえらび，

$Db_1, \cdots, Db_n$を作る。各Db_iは第j e^*-対の元c_{ij}をひとつだけふくむ($j=1,\cdots,n$)。そこでGの元を成分とする位数nの行列(c_{ij})を作る。そして$c_{ij}=a_j$のとき1, $c_{ij}=a_je^*$のとき-1とおくと，位数nの(-1, 1)行列Hが得られる。HがGから作られるアダマール行列である。

位数の小さなものについては，比較的容易です。

例1．$G=C_4=\langle a\rangle$，位数4の巡回群では，$e^*=a^2$, $D=\{e, ae^*\}$とおくとよい。±で±1を示すことにすると，$H=\begin{pmatrix}+&-\\+&+\end{pmatrix}$のように$e^*$-対を番号付けられる。

例2．$G=C_4\times C_2=\langle a\rangle\times\langle b\rangle$では，$e^*=b$, $D=\{e, ae^*, a^2, a^3\}$とおけます($e^*=a^2$というようなえらび方も出来る。そのときDは同じでありません。)

$H=\begin{pmatrix}+&-&+&+\\+&+&-&+\\+&+&+&-\\-&+&+&+\end{pmatrix}$と巡回型アダマール行列が得られるように$e^*$-対が番号付けられる。一般につぎのことが成立する。

命題2．Eが群Hにふくまれるアダマール差集合なら，$G=H\times\langle e^*\rangle$を作り，$D=E\cup(H-E)e^*$とおくことにより，アダマール群$G$が得られる。逆に，アダマール群$G$について，$G=H\times\langle e^*\rangle$となっていると，$E=D\cap H$

は H にふくまれるアダマール差集合である。

尚，アダマール差集合とは (v, k, λ) 差集合で，$v = 4(k-\lambda)$ となるものです。例2では $\{e, a^2, a^3\}$ が C_4 にふくまれるアダマール差集合です。アダマール差集合については最近もいろいろ面白い結果が得られていますが，私達の考えていることの特別の場合であるというのは，過言でしょうか。

例3．$G = Q$，四元数群；$a^4 = b^4 = e$，$b^{-1}ab = a^{-1}$，$a^2 = b^2$ では，$e^* = a^2$ は自明ですが，$D = \{e^*, a, b, ab\}$ とえらべます。このとき
$$H = \begin{pmatrix} - & + & + & + \\ - & - & + & - \\ - & - & - & + \\ - & + & - & - \end{pmatrix}$$
と所謂 skew になるように e^*-対が番号付けられる．

命題3．G がアダマール群で，H が skew になるように e^*-対が番号付けられると，e^* は D の唯一つの位数2の元となる。したがって $|G| \geqq 8$ のとき，G のシロー2-群は一般四元数群である．

これは魅力的であるが，$n = 4m$ とおくとき，すべての m について G が存在するというわけにはいかないようである。命題3はまたアダマール群のシロー2群にはなんらかの制限があることを示唆するが実際つぎのことが成立する。

命題4．位数 $\geqq 8$ の巡回群，二面体群はアダマール群のシ

ロー2ー群になれない。

さらに表現論を使うとつぎの結果が得られる。

命題5. RをGの既約表現で，単位表現でないものとする，e^*がRの核に入るか入らないかにより，$R(D^{-1}D)=0$かnI（Iは単位行列）になる。n－部分集合Dと中心にふくまれる位数2の元e^*について，これが成立つとGはアダマール群になる．

また既知のアダマール群から，直積のようなやり方でアダマール群の無限系列を作ることも出来る。さらに平方剰余型とかペイリー型とかのアダマール行列にたいしては，それらを作るアダマール群を作ることも出来るが，群論的とは言えそうもない。

何時かタイトルが夢でなくなる時が来ることを願っている。

文献

N. Ito, On Hadamard groups I, II
to appear in Journal of Algebra

Note on Hadamard groups of quadratic residue type
to appear in Hokkaido Math. Journal

Note on Hadamard groups and difference sets