

アダマール行列と有限群

イリノイ大 シカゴサークル 伊藤 昇

アダマール行列 n 次の正方行列 H は, その行ベクトル $\alpha_1, \dots, \alpha_n$ が (1) $(\alpha_i, \alpha_j) = 0$, $i \neq j$, (2) $\alpha_i = (\pm 1, \dots, \pm 1)$ を満足するときアダマール行列と呼ばれる。その存在, 構成, 分類問題を考察したい。アダマール (1893) は, $n > 2$ のとき n は 4 の倍数であることを示したが, この逆はアダマールの予想で, 今も未解決のままである。 $\{-1, 1\}$ 行列 H について (1), (2) は $HH^t = nI$ と等価, したがって $HH^t = H^tH$ であり上の行ベクトルによる定義は列ベクトルによってもよい。 n 次のアダマール行列 H, K について, K が H に等価とは, K が H から (イ) 行, 列の置換, (ロ) 行, 列に -1 をかける, ことにより得られることで, これは等価関係である。 $C(n)$ で n 次アダマール行列の等価類数を示す。また $K = H$ のときの (イ), (ロ) が H の自己同型, その全体が H の自己同型

群 $G = G(H)$ である. n 次アダマール行列 H には行 (又は列) 毎に (アダマール) $3 - (n, \frac{n}{2}, \frac{n}{4} - 1)$ デザイン, またその各 $3 -$ デザインには列 (又は行) 毎に (アダマール, 対称) $2 - (n-1, \frac{n}{2}-1, \frac{n}{4}-1)$ デザインが相伴する. これらのデザイン, それらの自己同型群と, H, G とを結び付けて考察するには H をデザイン化するのを便利である.

行列デザイン $M(H)$ 列点, 行ブロック式をとる. 列には 2 点 i, i^* を用意する. 行ベクトル α_j をつぎのようにブロックとする: α_j の i -座標が $+1$ の -1 の $i \in \alpha_j$ の $i^* \in \alpha_j$ とする. また $-\alpha_j = \alpha_j^*$ とおき, これもブロックとする. $M(H)$ の点集合 $P(H) = \{1, \dots, n, 1^*, \dots, n^*\}$, ブロック集合 $B(H) = \{\alpha_1, \dots, \alpha_n, \alpha_1^*, \dots, \alpha_n^*\}$ である. $\{i, i^*\}$ を含むブロックは存在しないが, それらを除外すると任意の点を含む $\frac{n}{4}$ 個のブロックがあり, $M(H)$ は概 $3 -$ デザインといえよう. また $G = G(H)$ の元 σ は, $P(H)$ 上の置換で, $B(H)$ を不変にし, さらに $i\sigma = j$ なら $i^*\sigma = j^*$ (ただし $i^{**} = i$ のようにする) を満足するものとなる.

$3 -$ デザイン $H(\alpha_j)$ $H(\alpha_j)$ の点集合は α_j , ブロックは $\alpha_j \cap \alpha_k, \alpha_j \cap \alpha_k^*, k \neq j, 1 \leq k \leq n$ である. これは $3 - (n, \frac{n}{2}, \frac{n}{4} - 1)$ デザインであること,

$H(\alpha_j)$ が与えられると H が構成されることは見易い。したがってアダマール予想は任意の4の倍数 n について 3-
 $(n, \frac{n}{2}, \frac{n}{4} - 1)$ デザインが存在すると述べられる。

2- デザイン $H(\alpha_j, i), i \in \alpha_j$ $H(\alpha_j, i)$ の真
 集合は $\alpha_j - \{i\}$, ブロックは $\alpha_j \cap \alpha_k - \{i\}, i \in$
 $\alpha_k, k \neq j, 1 \leq k \leq n$ である。これが対称 2-
 $(n-1, \frac{n}{2}-1, \frac{n}{4}-1)$ デザインであること, $H(\alpha_j, i)$ が
 与えられると $H(\alpha_j)$ が構成されることは見易い。したが
 ってアダマール予想は任意の4の倍数 n について 対称 2-
 $(n-1, \frac{n}{2}-1, \frac{n}{4}-1)$ デザインが存在すると述べられ
 る。

自己同型群間の関係 $H(\alpha_j), H(\alpha_j, i)$ の自己同
 型群を $G(\alpha_j), G(\alpha_j, i)$ とおく。これらに $\ast$ -コピ
 ーを付加し, 次数 $2n$ の置換群とみると, つぎの命題が成立
 する。

命題 (1) $G(\alpha_j)$ は α_j の G における安定部分群で
 ある。 $G(\alpha_j, i)$ は i の $G(\alpha_j)$ における安定部分群で
 ある。(2) G の $B(H)$ 上での可移域と $H(\alpha_j)$ の同型類
 とは自然に対応する。 $G(\alpha_j)$ の α_j 上での可移域と
 $H(\alpha_j, i)$ の同型類とは自然に対応する。

注意 (1) 証明は定義, 構成から直ちにわかると言って

よいと思う。(10) Norman [11] が n がいくらでも大きくて $G(\alpha_j) = 1$ という例を作っている。ここでは n 個の $H(\alpha_j, i)$ がすべて非同型であるので注目しよう。(11) 有限群を応用するが、アダマール予想に挑戦しようとするならば、2-, 3-デジタインではなく、行列(デジタイン)自体を考察すべきであることが暗示される。

群型のアダマール行列と平方剰余型のアダマール行列 アダマール行列は次山に存在するが、つぎの2つが代表的である。

1° 基本アーベル2群の指標行列は、指標の直交関係によりアダマール行列である。これが群型のアダマール行列 $H_g(n)$ であり、シルヴァエスター(1867)にまで遡れる。次数 n は2のべき、 $n = 2^m$ である。行 i が $j = (1, \dots, 1)$ 列 i が j^t のようにしておき、 $H_g(n)(\alpha(1), 1)$ をつくと、この2デジタインは $GF(2)$ 上の射影幾何で、超平面をブロックにしたものである。このように $H_g(n)$ はゆたかな構造を持っている。 $H_g(n)$ の自己同型群 $G_g(n)$ は Kantor [10] により決定されているが、木村-伊藤はつぎのように見る。 $GF(2)$ 上 $m+1$ 次元のベクトル空間を V , $(e_0, \dots, e_m)$ を V の基とする。点の集合を V , ブロックを e_0 を含まない超平面 M とその剰余類 $M + e_0$ (ここで M は動く)と

すると、これが $M(H_g(n))$ と同型であることは見易い。したがって位数 2^{m+1} の基本アーベル 2 群である平行移動群が、真上可移に働く。零ベクトルの安定部分群は e_0 も固定し、

線型変換群 $\begin{pmatrix} 1 & x \\ 0 & GL(m, 2) \end{pmatrix}$, x 任意, と同型である。 $G_g(n)$

は $H_g(n)$ の行, 列上それぞれに 2 重可移に働かせ, またそれぞれに正則可移正規部分群を含む。

2° q を $q \equiv 3 \pmod{4}$ なる素数べき, χ を $GF(q)$ の平方指標, または $R = (GF(q)^\times)^2$ とするとき, $\chi(a) = 1, a \in R; -1, 0 \neq a \notin R; 0, a = 0$ である。 (a, b) 成分は $\chi(b-a)$ である次数 q の行列を C , C を

$$S = \begin{pmatrix} 0 & J \\ -J^t & C \end{pmatrix} \text{ と拡大し, } H(q) = -I + S \text{ とおくと,}$$

χ の簡明な性質から, アダマール行列が得られる。これが平方剰余型のアダマール行列 $H(q)$ である。 $H(q)$ が雑誌に最初に登場したのはペイリー (1933) である。 $q \equiv 3 \pmod{4}$ から, S は歪対称行列で, そのような形のアダマール行列は歪アダマール行列と呼ばれる。 $H(q)$ はその代表的なものである。行 1 を $(-1, 1, \dots, 1)$, 列 1 を $-j^t$ のようにして, $H(q) (\alpha(1), 1)$ を作ると, この 2 デザインは, 点を $GF(q)$, ブロックを $R+a, a \in GF(q)$

とする周知の平イ剰余型 $\tilde{\Gamma}$ がインになる. $H(3)$, $H(7)$ はそれぞれ $H_g(4)$, $H_g(8)$ と等価であるので, ここでは $q > 7$ とする. $H(q)$ の自己同型群 $G(q)$ は Hall [3] Kantor [10] により決定されている. $H(11)$ はもっとも著名なものであり, Hall は $G(11)$ がマテュー-群 M_{12} の表現群であることを示している. $q \geq 19$ のとき $G(q)$ は $SL^*(2, q)$ ($SL(2, q)$ の体同型を付加したもの) を含むことは Hall によるが, それと一致することは Kantor により示された. Kantor の証明はあまり難解なもので, 簡明化が望まれる. $G(q)$ は $H(q)$ 上の行, 列上それぞれに 2 重可移に働らくが, 正則可移正規部分群は含まない.

列上 2 重可移な自己同型群を持つアダマール行列 アダマール行列を考察するのに, 群論的に強い条件を付しても, 群を具体的に与えない限り, それが困難であることは多くの組合せ構造について共通である現象のひとつである. ところで 2 重可移群の分類は, とくに正則可移正規部分群を含まないものは, 最近完成したことになっているので, したがって上のようなアダマール行列を分類することも可能になる.

命題 (Ito [6], Ito-Leon [8]) 列上 2 重可移, かつ正則可移正規部分群を含まない自己同型群を持つアダマール行列は平イ剰余型 ($q > 7$) の, $n = 36$ 通りのよう

に構成される。2デザインを与える。GF(2)上6次元のベクトル空間を V 、 $e_1, \dots, e_6$ を標準基とし、また V 上の2次形式 $X_1X_4 + X_2X_5 + X_3X_6$ を考察する。このとき35個の特異ベクトルがあるが、それら全体の集合 D を作る。またブロッツクのひとは $e_1, e_4, e_1+e_2, e_1+e_3, e_1+e_5, e_1+e_6, e_1+e_2+e_3, e_1+e_2+e_6, e_1+e_3+e_5, e_1+e_5+e_6, e_1+e_2+e_4+e_5, e_1+e_3+e_4+e_6, e_1+e_2+e_3+e_4+e_5, e_1+e_2+e_3+e_4+e_6, e_1+e_2+e_3+e_5+e_6, e_1+e_2+e_4+e_5+e_6, e_1+e_3+e_4+e_5+e_6$ であり、これに第一直交群 $O^+(6, 2)$ を作用させるとすべてのブロックが得られる。対応する行列の自己同型群は $S_p(6, 2)$ と位数2の巡回群との直積である。

正則可移正規部分群があるときは、Hering [5]の努力にもかかわらず2重可移群の分類は完全でないで、そのより高アダムール行列の分類もまた不完全である。

命題 (Ito - Kimura [7]) 列上2重可移、かつ正則可移正規部分群を含む自己同型群を持つアダムール行列について以下のことが成立する。次数 n は2のべき、 $n = 2^m$ であるが、 m が奇数ならば群型、また m が偶数でも列上3重可移ならば群型である。さらに $n = 16$ のときは群型である。

問題 列上ランク 3 を自己同型群を持つアダマール行列を考察せよ.

次数 n の任意のアダマール行列について $S = \prod_{i=1}^n (\delta_{ii} + i^*)$ は自己同型群の中心に入る. $G = \langle S \rangle$ であるようなアダマール行列の例は今のところ知られていない. 先にあげた Norman の例では自己同型群の位数は 4 で整除される.

$C(n)$ について n 次のアダマール行列全体に等価群が働いていて, その可移域の個数が $C(n)$ である. $n = 1, 2, 4, 8, 12$ のときは $C(n) = 1$, $C(16) = 5$, $C(20) = 3$ は Hall によって計算されている [2, 4]. これらの各アダマール行列は行 (列) 上可移な自己同型群を持っている.

命題 (Ito - Leon - Longyear [9]) $C(24) = 59$

注意 (i) $3 - (24, 12, 5)$ デザインの同型類の個数は 129 である. (ii) 自己同型群で区別できないのは 2 つだけ H, H^t の形になっている. (iii) 自己同型群の最小のものは位数 8 である.

アダマール予想は n が 4 で整除されるとき $C(n) > 0$ と述べられるが, $\lim_{n \rightarrow \infty} C(n) = \infty$ が成立して不思議でないように思われる. Gordon [1] は $\lim_{n \rightarrow \infty} C(2^n) = \infty$ を証明

している。したがって等価概念を広くして“等価”類の個数を小さくすることが望ましい。Seberry, Wallis [12] は (イ), (ロ) に (ハ) ある行, 列の整数倍を他の行, 列に加える: を付加することを提案している。すなわち2つのアダマール行列は単因子系が等しいとき“等価”とされる。これを左等価と呼び, 左等価類の個数を $E(n)$ で示そう。このとき $u = \frac{n}{4}$ が平方無縁ならば $E(n) = 1$ が成立する。したがってこれでは広すぎるといえよう。しかしながら $E(n)$ を一般に計算することも大きな課題のひとつである。

Q型のアダマール行列

$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ は次数2のアダマール行列

列であり, 2つのアダマール行列のクロネッカー積はアダマール行列だから (アダマール 1893), アダマール予想を考察するには, $n = 4u$, u 奇数の場合に限ってよい。このとき, つぎの3元で生成される次数 $2u$ の正則可移群 $\mathcal{Q}_n$ を Q型と呼ぼう: $A = (1 \dots u) \dots (3u+1 \dots 4u) (*)$, ここで $*$ はその前迄の $*$ コピーを付加することを示す, $B = (1, u+1, *) \dots (u, 2u, *) (2u+1, 3u+1, *) \dots (3u, 4u, *)$, $C = (1, 2u+1, *) (2, 3u, *) \dots (u, 2u+2, *) (u+1, (3u+1)^*, *) (u+2, (4u)^*, *) \dots (2u, (3u$

$+2)^*, *)$ さらに $\mathcal{Q}_n$ を自己同型群の部分群として含む
次数 n のアダマール行列を Q 型のアダマール行列と呼ぶ。

予想 任意の $n = 4u$, u 奇数 について n 次の Q 型のアダ
マール行列が存在する。

注意 講演者はこの予想の下でアダマール予想の考察を進
めている。

この予想の成立を支持するべきのことが示される。

1° 平方剰余型のアダマール行列は, $\frac{n}{4}$ が奇数のとき, Q
型である (正確には Q 型に等価であるというべきであろう。
以下同じ)。

2° 4つの対称巡回行列を用いて構成するウィリアムソン
型のアダマール行列は Q 型である。したがってウィリアムソ
ン型のアダマール行列は行, 列上可移な自己同型群を持つ。

注意 ウィリアムソン型のアダマール行列については山本
山田, 沢出 [13] により研究が進められている。

最後に, 沢山に知られているアダマール行列の系列では,
自己同型群の決定を待っているものが多いことを指摘してお
きたい。

文献

- [1] B. Gordon, A note on inequivalent Hadamard

matrices, JRAM (7 L L) 268 / 269, (1974),
427 - 433

[2] M. Hall, Jr., Hadamard matrices of order
16, JPL Research Summary 36-10, 1 (19
61), 21 - 26.

[3] 同, Note on the Mathieu group M_{12} ,
Arch Math. 13 (1962), 334 - 340.

[4] 同, Hadamard matrices of order 20, JPL
Technical Report No. 32-761.

[5] C. Hering, Transitive linear groups and linear
groups which contain irreducible subgroups of prime
order, GD 2 (1974) 425 - 460.

[6] N. Ito, Hadamard matrices with "doubly tran-
sitive" automorphism groups, Arch Math. 35 (198
0), 100 - 111.

[7] N. Ito - H. Kimura, Studies on Hadamard
matrices with "2-transitive" automorphism groups,
($\tau \parallel \tau^2 \parallel \dots \parallel \tau^{n-1}$)

[8] N. Ito - J. Leon, An Hadamard matrix of
order 36 ($\tau \parallel \tau^2 \parallel \dots \parallel \tau^{n-1}$)

[9] N. Ito - J. Leon - J. Longyear, Classifica-

tion of $3 - (24, 12, 5)$ designs and 24 -dimensional Hadamard matrices, to appear in JCTA.

[10] W. Kantor, Automorphism groups of Hadamard matrices, JCTG (1969) 279 - 281.

[11] C. Norman, Hadamard designs with no non-trivial automorphisms, GD 2 (1973) 201 - 204.

[12] W. D. Wallis - J. Seberry (Wallis), Equivalence of Hadamard matrices, Israel JM 7 (1969) 122 - 128.

[13] 本講義録 404 およびこれにあり文献.