

新しいアダマール行列の構成法

愛媛大学 理 宮本雅彦

アダマール行列とは、成分が 1 又は -1 だけから成る正方行列 H で各行が互に直交しているものをいう。(この様に各行がお互に直交している正方行列をこれから直交行列と呼ぶ。) 特に、 H が $n \times n$ 正方行列の時、この n をアダマール行列の次数と呼ぶ。この時 $HH^t = nI_n$ となる。ここで、 H^t は H の転置行列、 I_n は n 次の単位行列を表す。このアダマール行列は組合せ理論の色々な分野と関係しており興味ある性質をもっているが、此では、アダマール行列の存在についてのみ話を進めたい。アダマール行列が存在すれば、その次数は 1 か 2 か又は 4 の倍数となる事が分るが、この逆が成立つだろうというのが、アダマール行列についての最大の問題であり、アダマール予想と呼ばれている。もし n 次のアダマール行列が存在すれば $2n$ 次のアダマール行列も存在するので奇数の n に対して $4n$ 次のアダマール行列の存在を示せば充分である。今まで色々な系列の次数に対してアダマール行列が構成されているが、それらは非常に粗く等差数列的な次数に対するアダマール行列の構成

は見つかっていない。又、拡大という事に関しても、 $4s$ 次のアダマール行列と $4t$ 次のアダマール行列とから、 $4st$ 次のアダマール行列を構成する方法は現在のところ、 $4s$ 次の Bauert-Hall型と $4t$ 次の Williamson型から $4st$ 次のアダマール行列を構成する方法しかなく、それ以上の拡大を構成できない。

ここでは、かなり多くの新しい次数を持つアダマール行列を紹介します。此で紹介する構成法によって次数 $4n$ (n は奇数) で 8000 以下のものを調べると A. V. Germita と J. Seberry の本 "Orthogonal Designs" の中の表と最近の結果によれば、 215 個の次数に対してアダマール行列の存在が判っていなかったが、此では、このうち 89 個の次数に対してアダマール行列を構成した。これにより残りは 126 個となる。さらに、残りの次数に対しても $4n$ 次での存在は示せないが、多くの次数に対しては、 $8n$ 次のアダマール行列を構成した。これらの結果は最後に表にして載せた。

定理 1. q を奇素数巾とし、 $q \equiv 1 \pmod{4}$ とする。

もし $q-1$ 次のアダマール行列が存在すれば、 $4q$ 次のアダマール行列も存在する。

この定理の証明は複素アダマール行列や四元数アダマール行列に対しても有効なので次の結果を得た。

系 2 . q を奇素数巾とする。もし $2(q+1)$ 次の複素型のアダマール行列が存在すれば、 $8q$ 次のアダマール行列も存在する。又、もし、 $4(q-1)$ 次の Williamson 型のアダマール行列が存在すれば、 $16q$ 次のアダマール行列も存在する。

系 3 . q を奇素数巾とし、 $q \equiv 3 \pmod{4}$ とする。もし $2q-3$ 又は $q-2$ が素数巾なら、 $8q$ 次のアダマール行列が存在する。

ここで、複素型のアダマール行列とは、

$$H = \begin{bmatrix} A & B \\ -B & A \end{bmatrix}$$

の形を持つアダマール行列の事をいう。この時、

$AB^t = BA^t$ が成立つが、この性質を "A と B がアミカブル" と呼ぶ事にする。もし A, B ともに対称行列の時には、H を対称複素型と呼ぶ。 $2t$ 次の複素型のアダマール行列が存在する事と、 t 次の複素アダマール行列が存在する

こととは同値である。

次にこれから構成するアダマール行列は、一番最初に話したように拡大の時に重要な役割を果たす Williamson 型のアダマール行列である。

定理 4 . q を奇素数巾とし、 $q \equiv 1 \pmod{4}$ とする。
もし対称複素型の $q-1$ 次のアダマール行列が存在すれば、
 $4q$ 次の Williamson 型のアダマール行列が存在する。

系 5 . q を奇素数巾とし、 $q \equiv 1 \pmod{4}$ とする。

もし $\frac{1}{2}(q-3)$ が素数巾であるか又は、複素型の $q-1$
次のアダマール行列が存在すれば、 $4q$ 次の Williamson 型の
アダマール行列が存在する。

定理 6 . q を奇素数巾とし、 $q \equiv 1 \pmod{4}$ とする。
もし対称複素型の $q+1$ 次の C -行列と対称複素型の $q+3$
次の C_2 -行列が存在すれば、 $4(q+2)$ 次の Williamson 型
のアダマール行列が存在する。

ここで、 C -行列とは、対角成分がすべて 0 であり、

その他の成分が 1 又は -1 であるような直交行列の事をいう。又、 C_2 -行列とは、 $2t \times 2t$ 正方行列 $D = (d_{i,j})$ で対角成分で $d_{i,i+t}$ と $d_{i+t,i}$ とが $i = 1, \dots, t$ に対して 0 であり、その他の成分はすべて 1 又は -1 となっている直交行列のことをいう。

これらの結果によって 8000 までの次数に対して調べると以下の新しい次数 $4n$ に対してアダマール行列の存在を証明した。 $n =$

219, 249, 267, 269, 303, 373, 445, 509, 515, 519, 581,
 613, 623, 657, 699, 721, 723, 733, 757, 763, 773, 803,
 857, 865, 913, 941, 949, 959, 965, 979, 985, 1043, 1047,
 1059, 1079, 1109, 1133, 1157, 1165, 1199, 1205, 1211, 1213, 1227,
 1241, 1243, 1299, 1301, 1335, 1341, 1351, 1359, 1373, 1379, 1381,
 1385, 1387, 1397, 1411, 1433, 1465, 1469, 1493, 1507, 1513, 1527,
 1557, 1577, 1631, 1639, 1661, 1671, 1679, 1693, 1745, 1751, 1753,
 1781, 1869, 1903, 1909, 1913, 1921, 1937, 1957, 1963, 1973, 1985,
 1993

§ 2. この節で前節で述べた各結果の証明を与える。前節の結果はすべてこの節で示す主定理の系として出てくる。此では、アダマール行列の構成を考えるが、その前に、少しこれから使う記号の説明をしよう。

記号 $e = e_m$ で全成分が 1 である様な $1 \times m$ 行

列を表す。 $m \times m$ 行列 M に対して、 $e(M) = s$ は $Me_m^t = se_m$ と $e_m M = se_m$ の両方を意味する。 $J=J_m$ で全成分が 1 であるような $m \times m$ 行列を表す。 4 個の $k \times h$ 行列 A, B, C, D と 16 個の $k \times h$ 行列 X_{ij} ($i, j=1, \dots, 4$) に対して、 $W(A, B, C, D)$ と $W(X_{ij})$ とによって、

$$W(A, B, C, D) = \begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}$$

と

$$W(X_{ij}) = \begin{bmatrix} X_{11} & X_{12} & X_{13} & X_{14} \\ -X_{21} & X_{22} & X_{23} & -X_{24} \\ -X_{31} & -X_{32} & X_{33} & X_{34} \\ -X_{41} & X_{42} & -X_{43} & X_{44} \end{bmatrix}$$

とをそれぞれ表すことにする。

特に、 A, B, C, D がおたがいにアミカブルである様なときには、 $W(A, B, C, D)$ を "Williamson型" と呼ぶことにする。 さらに X_{ij} ($i=1, \dots, 4$) がお互にアミカブルで $W(X_{ij}) = W(X_{11}, X_{12}, X_{13}, X_{14})$ の時に、 $W(X_{ij})$ を "Williamson型" と呼ぶ。

さて、これから $4(2m+1)$ 次のアダマール行列の構成を目指す。 まず 2 組の 16 個づつからなる $m \times m$ 行列 U_{ij}, V_{ij} で以下の 3 条件を満足するものがあると仮定する。

1) U_{ij}, V_{ij} はすべて $(0, 1, -1)$ -行列である。

即ち、成分が全て 0 か 1 か -1 のいずれかである。

2) $U_{ij} \pm V_{ij}$ はすべて $(1, -1)$ -行列である。

3) すべての i に対して $e(U_{ii}) = 1$ であり、

$i \neq j$ に対しては $e(U_{ij}) = 0$ である。

次に、 $T_{ij} = U_{ij} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + V_{ij} \otimes \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$ と

$2m \times 2m$ 行列 T_{ij} を定義する。この時、条件 2) より行列 T_{ij} は、 $(1, -1)$ -行列となる。即ち、 T_{ij} の成分は

1 か -1 である。さらに、 $(2m+1) \times (2m+1)$ 行列

X_{ij} を次の様に構成する。

$$X_{ii} = \begin{bmatrix} 1 & -e_{2m} \\ -e_{2m}^t & T_{ii} \end{bmatrix}, \quad X_{ij} = \begin{bmatrix} 1 & e_{2m} \\ e_{2m}^t & T_{ij} \end{bmatrix}$$

前者は $i = j$ に対してであり、後者は $i \neq j$ に対して定義する。 T_{ij} と同様に X_{ij} も又 $(1, -1)$ -行列である。

16 個の $(2m+1) \times (2m+1)$ 行列が出来たので、最後

後に

$$H = W (X_{ij})$$

と置く。

H は $4(2m+1) \times 4(2m+1)$ 正方行列で、その成分は 1 か -1 である。主定理は U_{ij} と V_{ij} に対する簡単な

仮定のもとに、 H がアダマール行列となることを示す。

まず、 $U = W(U_{ij})$, $V = W(V_{ij})$ と置く。

主定理. もし $U U^t = (2m+1) I_{4m} - 2 I_4 \otimes J_m$

と $V V^t = (2m+1) I_{4m}$ が両方成立つなら、

$H = W(X_{ij})$ はアダマール行列となる。さらに、 U と V とが両方とも Williamson型なら、 H も又 Williamson型となる。

証明の概略. $H = W(X_{ij})$ の各行各列の内、各 X_{ij} の第1行と第1列とを前に取り出して、次の様に変形できる。

$$\left[\begin{array}{cc} W(1, 1, 1, 1) & W(-e, e, e, e) \\ W(-e^t, e^t, e^t, e^t) & W(T_{ij}) \end{array} \right]$$

行の交換と列の交換だけなので、これがアダマール行列であることを示せば良い。この行列の上の部分列

$$W(1, 1, 1, 1) \quad W(-e, e, e, e)$$

は実際には4列からなっている。又、簡単な計算によって、 $W(T_{ij})$ がWilliamson型であれば、 $W(X_{ij})$ も又Williamson型となることが分る。条件3)より、 $e(T_{ii}) = 2$, また $i \neq j$ に対しては、 $e(T_{ij}) = 0$ が成立つので、上の4列と

下の5列以降とはお互に直交している。又、上の4列も互に直交しているので、後は、

$$W(T_{ij})W(T_{ij})^t = (8m+4)I_{8m} - 4I_4 \otimes J_{2m}$$

を示せば良い。これは、主定理の仮定から単純な計算によってでてくる。

定理1の証明を例にとって示そう。

奇素数中 q で、 $q \equiv 1 \pmod{4}$ と成るものに対して $q+1$ 次 (即ち $2m+2 \times 2m+2$ の) C -行列

$$C = \begin{bmatrix} 0 & 1 & e & e \\ 1 & 0 & e & -e \\ e^t & e^t & -C_1 & C_2 \\ e^t & -e^t & C_3 & C_4 \end{bmatrix}$$

が存在する。 C_i は4つとも $m \times m$ 行列である。又、仮定より、 $2m$ 次のアダマール行列

$$K = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} \quad (K_i \text{ は } m \times m \text{ 行列})$$

が与えられているので、

$$U = \begin{bmatrix} C_1 & C_2 & 0 & 0 \\ -C_3 & C_4 & 0 & 0 \\ 0 & 0 & C_1 & C_2 \\ 0 & 0 & -C_3 & C_4 \end{bmatrix}$$

$$V = \begin{bmatrix} I & 0 & K_1 & K_2 \\ 0 & I & K_3 & -K_4 \\ -K_1^t & -K_3^t & I & 0 \\ -K_2^t & K_4^t & 0 & I \end{bmatrix}$$

と置くと主定理の仮定を満たしている。

定理 4 の証明は仮定より V が Williamson 型となり、又、体の性質から U も又、Williamson 型と取れるので、結局 H も Williamson 型となる。他の定理や系の証明も同様にして得られる。

知られているアダマール行列の表。

この表に載っていない 2000 まで奇素数 n に対しては、 $4n$ 次のアダマール行列がみつまっている。又、表の中の $n(s)$ は 2^n 次のアダマール行列が存在している事を意味する。

103 (3),	163 (3),	167 (3),	179 (3),	191 (3),
213 (3),	223 (3),	239 (4),	251 (3),	283 (3),
311 (3),	347 (3),	359 (4),	419 (4),	443 (3),
463 (3),	479 (12),	487 (3),	491 (4),	523 (3),
537 (4),	571 (3),	573 (3),	599 (4),	631 (3),
643 (3),	647 (3),	653 (3),	659 (17),	669 (3),
719 (4),	739 (4),	749 (4),	751 (3),	781 (3),
787 (3),	789 (3),	823 (3),	839 (8),	853 (3),

859 (3), 883 (3), 907 (3), 917 (3), 919 (3),
 933 (4), 947 (4), 955 (3), 971 (4), 991 (3),
 1019 (4), 1031 (4), 1039 (3), 1051 (3), 1063 (3),
 1087 (4), 1103 (3), 1115 (4), 1123 (3), 1169 (4),
 1177 (4), 1187 (3), 1223 (8), 1255 (3), 1257 (5),
 1259 (4), 1283 (3), 1291 (3), 1303 (3), 1315 (3),
 1319 (12), 1327 (4), 1349 (3), 1367 (3), 1423 (3),
 1427 (3), 1439 (12), 1441 (3), 1447 (4), 1451 (4),
 1471 (3), 1473 (3), 1483 (3), 1487 (3), 1491 (3),
 1499 (16), 1507 (3), 1509 (3), 1543 (3), 1559 (4),
 1567 (4), 1571 (4), 1579 (5), 1583 (3), 1589 (3),
 1619 (4), 1633 (3), 1663 (4), 1667 (3), 1689 (3),
 1699 (3), 1703 (3), 1713 (4), 1719 (3), 1723 (3),
 1747 (3), 1783 (4), 1787 (3), 1793 (4), 1795 (5),
 1823 (3), 1831 (3), 1841 (3), 1847 (3), 1871 (3),
 1879 (3), 1883 (4), 1893 (4), 1907 (3), 1915 (3),
 1929 (4), 1949 (4), 1969 (4), 1979 (4), 1981 (4),
 1987 (4),

参 考 文 献

1. A. V. Geramita and J. Seberry, "Orthogonal Designs,"
 Lecture Notes in Pure and Applied Math., 45,
 Marcel Dekker, New York-Basel, (1979).
2. M. Yamada, Some new series of Hadamard matrices,
 J. Australian Math. Soc., (to appear).