数理解析研究所講究録
第 285 巻 1976 年 67-75



# 100次および108次のHadamard行列

東女大 文理 山本 幸一
沢出 和江

## 1. はじめに

Hadamard行列の構成において，近年のその発展は、1944年に発表されたWilliamson型のHadamard行列[4]に負う所が多い。実際，92次，116次，172次は，他のどの分類からも存在の判らなかった次数である。

$4n$次のWilliamson型のHadamard行列とは，

$n$次で対称な$(1,-1)$-行列$A_1, A_2, A_3, A_4$が存在して，

$$A_iA_j = A_jA_i \qquad (i,j=1,\cdots,4)$$

$$A_1^2+A_2^2+A_3^2+A_4^2=4nI_n \qquad (I;\text{単位行列})$$

を満足する時の

$$H=\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{pmatrix}$$

である。

以下略して，H-行列，W型のH-行列と書く。

この型に関しては，これまでにL. Baumertが92次までの，すべてのW型のH-行列を発見し，表にしているが，100次以上については完全でない。　今回は，幾つかの新しい結果も含めて100次及び108次の(同値なものは省いた)すべてのW型のH-行列を見付け出した事を報告したい。

## 2. WilliamsonによるHadamard行列の構成

W型のH-行列を構成するには，4つの行列$A_1, \cdots, A_4$を与える，1の巾根に関する多項式

$$\mu_i = 1 + 2\left\{\sum_{j=1}^{\frac{n-1}{2}} t_{ij}(\omega^j + \omega^{-j})\right\} \qquad (i=1,\cdots,4) \qquad \text{-----}(1)$$

を考え，それらが

$$\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2 = 4n \qquad \text{-----}(2)$$

を満足する解$t_{ij}\,(i=1,\cdots,4;\ j=1,\cdots,\frac{n-1}{2})$を持つならば$4n$次のW型のH-行列は存在するわけである[2, 5]。

理論的に言えば以上のようであるが，実際に構成するには次のような順である。

(i)　$4n$次のW型のH-行列が存在すれば，$8n$次のそれも存在する事は明白だから，$n$が奇数の場合のみ考えればよい。また，$\omega$が1自身の時も考慮に入れると，その時の全ての$\mu_i$ $(i=1,\cdots,4)$が奇数となる。

従って，オ1に

$4n$ を可能なすべての場合の4つの奇数の平方の和に表わす。

これは Lagrange の定理[3]より常に可能で，その場合の数は Jacobi の定理[1]に従い $16\sigma(n)$ ($\sigma(n)$；$n$ の約数の和）と正確に出る。

(ii) さて，$t_{ij}$ は Williamson の定理[2,5]により，$j$ を固定した時，4つの $t_{ij}$ $(i=1,\cdots,4)$ のうち唯1つが $+1$ または $-1$ で，他は $0$

となる性質を持つ。即ち $0$ でない $t_{ij}$ は全部で $\frac{n-1}{2}$ 個ある。問題は，(1)のどの $t_{ij}$ に $+1$ or $-1$ を代入すれば(2)を満足するかと言う事になる。しかも，その $t_{ij}$ は $\omega=1$ を代入した時，(i)の4つの平方の和に表わした時の形になっていなければならない。　以上の条件から $(t_{ij})$ の $i$ 行，$j$ 列，それぞれに制限が出来，解の候補が縮小される。

(iii) その先は，独自の計算により解を求めて行くのであるが，その際，計算時間を出来るだけ短かく済ませる為に，$\omega$ を如何に取扱うかが問題となる。　そこで，$\omega$ を円周等分体における素イデアルに関する合同条件でもって近似計算を行なって，簡単な整数の問題に還元する事により計算時間を極力減らす事が出来た。

即ち，次の「1の巾根に関する定理」を使う。

**3.** 1の巾根に関する定理を使って

$\boxed{\text{定理}}$ [6]

$p$；奇素数

$\omega$；1の原始$p$乗根

$\mathbb{Q}_p(\omega)$；有理$p$進数体$\mathbb{Q}_p$に$\omega$を付加した体

$\mathfrak{p}$；体$\mathbb{Q}_p(\omega)$の整数環の素イデアル

$\varpi$；$\omega \equiv 1+\varpi \pmod{\mathfrak{p}^2}$，かつ

体$\mathbb{Q}_p(\omega)$上，$\varpi^{p-1}=-p$の解

以上のように仮定した時，

$$A(\varpi)=\exp\left(\sum_{n=0}^{\infty}\frac{\varpi^{p^n}}{p^n}\right)\equiv\omega \qquad \pmod{\mathfrak{p}^{p+1}}。$$

（AはArtin-Hasse級数を意味する。）

上の定理を使って，

$$\omega\equiv 1+\frac{\varpi}{1!}+\frac{\varpi^2}{2!}+\cdots\cdots+\frac{\varpi^{p-1}}{(p-1)!} \qquad \pmod{\mathfrak{p}^p}$$

を得る。更に有理整数$\alpha$に対し，$\omega^{\alpha}\equiv 1+\frac{\alpha\varpi}{1!}+\frac{\alpha^2\varpi^2}{2!}+\cdots+\frac{\alpha^{p-1}\varpi^{p-1}}{(p-1)!}$ $\pmod{\mathfrak{p}^p}$であるから，

$$\omega^{\alpha}+\omega^{-\alpha}\equiv 2\left(1+\frac{\alpha^2\varpi^2}{2!}+\frac{\alpha^4\varpi^4}{4!}+\cdots\cdots+\frac{\alpha^{p-1}\varpi^{p-1}}{(p-1)!}\right) \quad \pmod{\mathfrak{p}^p}。$$

今，$n=p$（奇素数）の場合に限定し，上式を法$\mathfrak{p}^3$で考えて**2**の(1)に適用すれば，

$$\mu_i\equiv 1+4\left\{\sum_{j=1}^{\frac{n-1}{2}}t_{ij}\left(1+\frac{j^2\varpi^2}{2}\right)\right\} \quad (i=1,\cdots,4) \quad \pmod{\mathfrak{p}^3}。$$

各$\mu_i$は$\bmod\ \mathfrak{p}^3$で$\varpi^2$に関する簡単な有理整係数の多項式になっ

ている事に注意する。そこで $\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2\equiv 4n \pmod{p^3}$
を満足するためには、

$$\left[(\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2)\text{の}\varpi^2\text{の係数}\right]\equiv 0 \qquad \pmod{n}$$

となる事が必要である。
これは解の候補 $t_{ij}$ の組が真の解である為の必要条件であり、この条件により解の候補は一挙に $1/n$ に縮小され、更に必要とあれば（可能な場合）、mod $p^5$ で近似計算を行ない、合わせて $1/n^2$ に縮小可能である。　そうして最終段階として、$\omega$ を実際に代入して(2)を満足するか否かをみる。

ここで、$n$ が奇素数の場合に限定したが、素数巾、合成数の場合も以上を応用する事により、勿論近似計算可能である。
但し、注意すべき事は、$A(\varpi)$ の性質上、高々 mod $p^p$ までしか近似出来ないと言う点である。
この事は、$n\geqq 27$ の3の巾の時に非常に影響を与える。
実際、数十種に類別しても少なくとも10！以上もある解の候補を $1/3$ にしか減らせないのであるから、時間的には大型の電算機でもパンク状態になり、この場合無意味と言わねばならない。　しかし、$n$ が5以上の素数巾であれば、この方法はかなり有効である。

## 4. 100次のWilliamson型のHadamard行列

以上の構成法に基づき $n=25$ の場合を考える。

100を4つの奇数の平方の和に表わす方法は4通りで，詳細は以下の通りである。

$$\left.\begin{array}{l} 5^2+5^2+5^2+5^2 \\ 1^2+1^2+7^2+7^2 \\ 1^2+3^2+3^2+9^2 \\ 1^2+5^2+5^2+7^2 \end{array}\right\}$$

100次のすべての解を出す為に掛かった時間 ―― 約146時間

by TOSBAC 3400 model 31

結果は，1962年にL. Baumertが発見している4つの解に加えて，新たに4つの解が発見出来，以下の8つの解が100次のW型のH-行列を与える全てである事が判った。

以下，それらを明記する。（注：＊は新しい解を意味する）

$(5^2+5^2+5^2+5^2)$

$$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_1+2w_9-2w_6)^2+(1+2w_7-2w_8+2w_{12})^2+(1+2w_2-2w_4+2w_5)^2+(1-2w_3+2w_{10}+2w_{11})^2$$

$(1^2+1^2+7^2+7^2)$

$$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=1^2+1^2+(1-2w_2-2w_3-2w_5+2w_6-2w_7+2w_{12})^2+(1-2w_1-2w_4+2w_8+2w_9-2w_{10}-2w_{11})^2$$

$$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_3-2w_7)^2+(1-2w_1+2w_4)^2+(1+2w_8-2w_9-2w_{10}-2w_{11})^2+(1-2w_2-2w_5+2w_6-2w_{12})^2$$

＊ $$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_3-2w_9)^2+(1+2w_4-2w_{12})^2+(1-2w_1-2w_7)^2+(1+2w_6+2w_8-2w_{11}-2w_{10}-2w_5-2w_2)^2$$

$(1^2+3^2+3^2+9^2)$

$$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_6-2w_{11})^2+(1-2w_1+2w_3-2w_{12})^2+(1+2w_4-2w_7-2w_9)^2+(1+2w_2+2w_5-2w_8+2w_{10})^2$$

＊ $$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_2+2w_{10}-2w_1-2w_8)^2+(1-2w_5)^2+(1+2w_9+2w_{11}-2w_7-2w_4-2w_3)^2+(1+2w_6+2w_{12})^2$$

＊ $$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=1^2+(1+2w_1+2w_2-2w_3-2w_8-2w_9)^2+(1+2w_7+2w_{11}-2w_{12}-2w_6-2w_4)^2+(1+2w_5+2w_{10})^2$$

$(1^2+5^2+5^2+7^2)$

$$*\ \mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2W_5-2W_{10})^2+(1+2W_6+2W_{11}-2W_2)^2+(1+2W_{12}+2W_9+2W_4-2W_7-2W_8)^2+(1-2W_1-2W_3)^2$$

## 5. 108次のWilliamson型のHadamard行列

$n=27$の場合，**3**の方法に代わるものとして，部分体の性質を使う方法が上げられる。円周27等分体は部分体として，円周3等分体及び円周9等分体をもつ。ち，$\nu$，$\omega$をそれぞれ1の3乗根，9乗根，27乗根とおく。

ある$t_{ij}$ $(i=1,\cdots,4\,;\,j=1,\cdots,13)$の組が，$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=108$を満たす$\mu_i=1+2\left\{\sum_{j=1}^{13}t_{ij}(\omega^j+\omega^{27-j})\right\}$ $(i=1,\cdots,4)$の解である為の必要条件として，

$\mu_1'^2+\mu_2'^2+\mu_3'^2+\mu_4'^2=108$を満たす$\mu_i'=1+2\left\{\sum_{j=1}^{13}t_{ij}(\text{ち}^j+\text{ち}^{27-j})\right\}$

$(i=1,\cdots,4)$の解であること

さらにそれらが

$\mu_1''^2+\mu_2''^2+\mu_3''^2+\mu_4''^2=108$を満たす$\mu_i''=1+2\left\{\sum_{j=1}^{13}t_{ij}(\nu^i+\nu^{27-i})\right\}$

$(i=1,\cdots,4)$の解であること

が考えられる。　この2条件により，解の候補が非常に細かく分類されるので，時間に合わせてDATAを適当に組合わせる事が出来，限定された時間内での計算処理に向いている。

詳細は次のようである。

$$\left.\begin{array}{l} 1^2+1^2+5^2+9^2 \\ 1^2+3^2+7^2+7^2 \\ 3^2+3^2+3^2+9^2 \\ 3^2+5^2+5^2+7^2 \end{array}\right\}$$

108次のすべての解を出すのに掛かった時間
═ 約90時間50分＋約9時間49分
(by TOSBAC 3400)　(by HITAC $\frac{8800}{8700}$)

計算時間は，108次の場合約1/3をTOSBAC 3400で行なったが，後は時間の関係で東大のHITAC $\frac{8800}{8700}$に依頼した為である。

以下，108次の解をすべて列挙する。

$(1^2+1^2+5^2+9^2)$

$$\mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=1^2+1^2+(1-2w_1-2w_2+2w_6+2w_8+2w_{10}-2w_{11}+2w_{13})^2+(1-2w_3+2w_4+2w_7+2w_5-2w_9+2w_{12})^2$$

$$*\ \mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_3+2w_1-2w_9-2w_4)^2+(1+2w_{12}+2w_2-2w_{10}-2w_{11})^2+(1+2w_7+2w_8-2w_6)^2+(1+2w_{13}+2w_5)^2$$

$$*\ \mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_9+2w_{13}-2w_5-2w_8)^2+(1+2w_3-2w_{10})^2+(1+2w_2)^2+(1+2w_6+2w_{11}+2w_7+2w_1-2w_{12}-2w_4)^2$$

$(1^2+3^2+7^2+7^2)$

$$*\ \mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_5+2w_2-2w_8-2w_7)^2+(1+2w_9-2w_{10}-2w_{11})^2+(1+2w_3-2w_4-2w_{13}-2w_6)^2+(1-2w_1-2w_{12})^2$$

$$*\ \mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_9-2w_4)^2+(1+2w_{11}-2w_5-2w_7)^2+(1+2w_8+2w_{13}-2w_3-2w_6-2w_{10}-2w_1)^2+(1-2w_{12}-2w_2)^2$$

$(3^2+3^2+3^2+9^2)$ ----- 解なし

$(3^2+5^2+5^2+7^2)$

$$*\ \mu_1^2+\mu_2^2+\mu_3^2+\mu_4^2=(1+2w_1-2w_4-2w_6)^2+(1+2w_{10}+2w_{13}-2w_{11})^2+(1+2w_5+2w_2-2w_{12})^2+(1+2w_7-2w_8-2w_3-2w_9)^2$$

## 参考文献

[1] M. Gaston Benneton, Arithmétique des Quaternions; Bulletin de la Société Mathematique de France, Tome 71, (1943), 78-111.

[2] M. Hall, Jr., "Combinatorial Theory," Blaisdell, Waltham, Mass., (1967).

[3] G. H. Hardy & E. M. Wright, An Introduction to the Theory of Numbers, Oxford: Clarendon Press 1938.

[4] J. Williamson, Hadamard's determinant theorem and the sum of four squares, Duke Math. J. 11 (1944), 65-81.

[5] W. D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis, Combinatorics: Room squares, sum-free sets, Hadamard matrices, Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

[6] K. Yamamoto, An explicit formula of the Norm residue symbol in a local number field, Science Reports of Tokyo Woman's Christian College, Nos. 24-28, (1972), 302-334.