数理解析研究所講究録
第671巻 1988年 66-80

Cayley の8元数と Orthogonal design, Hadamard行列

東女大・文理　山田美枝子 (Mieko Yamada)

1 1972年 J. Seberry は Baumert-Hall 配列の概念を拡張して直交配列 (Orthogonal design) を導入した。

定義　$x_0, x_1, \cdots x_l$ を互いに可換な変数、$s_0, \cdots, s_l$ を自然数とする。n 次正方行列 X は成分が $0, \pm x_0, \pm x_1, \cdots, \pm x_l$ で

$$XX^* = \left(\sum_{k=0}^{l} s_k x_k^2\right) I_n$$

をみたすとする。ただし X^* は X の転置行列、I_n は n 次単位行列とする。このとき X を n 次直交配列 (Orthogonal design) といい $OD(n; s_1, \cdots, s_l)$ とかく。

直交配列に行・列の入れかえ、行あるいは列に -1 をかけてできた配列も直交配列で、もとの直交配列と同値とみなす。

変数 x_k に $0, \pm 1$ を代入すると X は weighing 行列となる。さらに0を含まないとすると X は Hadamard 行列となる。

0を含まない2次直交配列 $OD(2; 1, 1)$, 4次直交配列 $OD(4; 1, 1, 1, 1)$ に

$$\begin{pmatrix} x_0 & x_1 \\ -x_1 & x_0 \end{pmatrix}, \quad \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ -x_1 & x_0 & -x_3 & x_2 \\ -x_2 & x_3 & x_0 & -x_1 \\ -x_3 & -x_2 & x_1 & x_0 \end{pmatrix}, \quad \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ -x_1 & x_0 & x_3 & -x_2 \\ -x_2 & -x_3 & x_0 & x_1 \\ -x_3 & x_2 & -x_1 & x_0 \end{pmatrix}$$

があるが、これらは複素数、四元数と変数の作る環の元の正則表現に他ならない。

次に変数x_kに行列を代入する。この場合に配列が直交するには成分行列の間に$AB^* = BA^*$という条件が必要である。そこで条件をできるだけへらして成分が行列である配列が直交するように、直交配列を変形することを考える。我々の目的は配列の構成原理をみいだし、符号配置を決定した後、配列の変数に行列を代入し、その配列をできるだけ少ない条件で直交させることである。

条件の少ない配列にはWilliamson行列、Goethals-Seidel行列などがあるが、特にGoethals-Seidel行列は条件が少なく、有効で重要な配列であるが、成分行列が巡回行列という条件を必要とする。成分行列が巡回行列という条件をはずして、できるだけ少ない条件でHadamard行列を構成することはHadamard行列の構成問題の今後の研究方向の一つであると考える。

ここではCayleyの8元数から作られる8次直交配列と、それを変形した配列を使ってHadamard行列の構成を行なう。

2 $\mathbf{C}=\{\pm i_k;\ 0\leqq k\leqq 7,\ i_0=1\}$ の乗法を $(7,3,1)$ デザインの各組 $(1,2,3),(1,4,5),(2,4,6),(3,4,7),(1,7,6),(7,2,5),(6,5,3)$ によって定義する。すなわち

$$(1,2,3)\to i_1i_2=i_3,\ i_2i_3=i_1,\ i_3i_1=i_2,\quad i_1^2=i_2^2=i_3^2=-1,$$
$$i_2i_1=-i_3,\ i_3i_2=-i_1,\ i_1i_3=-i_2,$$

とする。言いかえると $\{i_0=1,i_1,i_2,i_3\}$ は四元数単位であるとする。$(1,4,5)$ 以下についても同様。以上から $\mathbf{C}$ は Cayley の 8 元数で loop をなす。

$x_0,x_1,\cdots,x_7$ を互いに可換な変数で P を $x_0,\cdots,x_7$ を含む可換な変数の作る環とする。Z を有理整数環とし、多項式環 $Z[P]$ を考える。$\mathfrak{o}=Z[P]$ における自己同型写像 σ_k が

$$\sigma_k^2=1,\qquad \sigma_k\sigma_m=\sigma_{k+m}$$

を満足するものとする。ただし $k+m$ は有限体 $GF(8)$ での加法である。$\forall v\in\mathfrak{o}$ に対し

$$i_k v=v^{\sigma_k}i_k,\qquad i_k\in\mathbf{C}$$

であると仮定する。このとき $\{i_k:\sigma_k=1\}$ は $\mathbf{C}$ に等しいか、四元数部分群のいずれかである。

$\mathfrak{o}$ に $\mathbf{C}$ を添加し $\mathbf{R}$ とする。$\mathbf{R}$ の元 ξ は $\xi=\sum_{k=0}^{7}v_ki_k$ の形をしている。$\xi=\sum_{k=0}^{7}v_ki_k$, $\zeta=\sum_{k=0}^{7}u_ki_k\in\mathbf{R}$ の積 $\xi\zeta$ を σ_k を使って

$$\xi\zeta=\left(\sum_{k=0}^{7}v_ki_k\right)\left(\sum_{k=0}^{7}u_ki_k\right)=\sum_{k=0}^{7}\sum_{k=0}^{7}(v_ku_m^{\sigma_k})i_ki_m=\sum_{k=0}^{7}\sum_{k=0}^{7}v_ku_m^{\sigma_k}\delta_{k,m}i_{k+m}$$

で定義する。ただし $\delta_{k,m}$ は $\mathbf{C}$ の乗法に従い、1 か -1 をとり

$k+m$ は GF(8) での加法とする。

こうして $\mathbf{R}$ は積について閉じ、非可換非結合代数である。

$\xi = v_0 + \sum_{k=1}^{7} v_k i_k$ に対し、共役元 $\overline{\xi}$ を $\overline{\xi} = v_0 - \sum_{k=1}^{7} v_k \sigma_k i_k$ で定義し、ノルム $N(\xi)$ を $N(\xi) = \xi\overline{\xi}$ で定義する。

[I] $\{i_k : \sigma_k = 1\} = \mathbf{C}$ の場合

このとき

$$N(\xi) = \xi\overline{\xi} = \left(v_0 + \sum_{k=1}^{7} v_k i_k\right)\left(v_0 - \sum_{k=1}^{7} v_k i_k\right)$$
$$= v_0^2 - \sum_{k=1}^{7} v_k^2 i_k^2 - \sum_{k=1}^{7}\sum_{\substack{m=1 \\ m\neq k}}^{7} v_k v_m i_k i_m$$
$$= \sum_{k=0}^{7} v_k^2 - \frac{1}{2}\sum_{k=1}^{7}\sum_{\substack{m=1 \\ m\neq k}}^{7} (v_k v_m i_k i_m + v_m v_k i_m i_k) = \sum_{k=0}^{7} v_k^2$$

となり $N(\xi) \in \mathbb{R}$ である。

$\mathbf{R}$ は非可換非結合代数であるので正則表現は定義できないが正則表現に準じた行列を考える。すなわち $\mathbf{R}$ の元 $\xi = \sum_{k=0}^{7} v_k i_k$ の右正則表現に準じた行列 $R_0(\xi)$, $L_0(\xi)$ を

$$R_0(\xi) = \begin{pmatrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \\ -v_1 & v_0 & -v_3 & v_2 & -v_5 & v_4 & v_7 & -v_6 \\ -v_2 & v_3 & v_0 & -v_1 & -v_6 & -v_7 & v_4 & v_5 \\ -v_3 & -v_2 & v_1 & v_0 & -v_7 & v_6 & -v_5 & v_4 \\ -v_4 & v_5 & v_6 & v_7 & v_0 & -v_1 & -v_2 & -v_3 \\ -v_5 & -v_4 & v_7 & -v_6 & v_1 & v_0 & v_3 & -v_2 \\ -v_6 & -v_7 & -v_4 & v_5 & v_2 & -v_3 & v_0 & v_1 \\ -v_7 & v_6 & -v_5 & -v_4 & v_3 & v_2 & -v_1 & v_0 \end{pmatrix}, \quad L_0(\xi) = \begin{pmatrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \\ -v_1 & v_0 & v_3 & -v_2 & v_5 & -v_4 & -v_7 & v_6 \\ -v_2 & -v_3 & v_0 & v_1 & v_6 & v_7 & -v_4 & -v_5 \\ -v_3 & v_2 & -v_1 & v_0 & v_7 & -v_6 & v_5 & -v_4 \\ -v_4 & -v_5 & -v_6 & -v_7 & v_0 & v_1 & v_2 & v_3 \\ -v_5 & v_4 & -v_7 & v_6 & -v_1 & v_0 & -v_3 & v_2 \\ -v_6 & v_7 & v_4 & -v_5 & -v_2 & v_3 & v_0 & -v_1 \\ -v_7 & -v_6 & v_5 & v_4 & -v_3 & -v_2 & v_1 & v_0 \end{pmatrix}$$

で与える。

$$R_0(\overline{\xi}) = R_0(\xi)^*, \quad L_0(\overline{\xi}) = L_0(\xi)^*,$$

$$R_0(\xi\bar{\xi}) = R_0(\xi)R_0(\bar{\xi}) = R_0(\xi)R_0(\xi)^*,$$
$$L_0(\xi\bar{\xi}) = L_0(\xi)L_0(\bar{\xi}) = L_0(\xi)L_0(\xi)^*$$

が成りたつ。特に $\nu_k = \lambda_k$ の場合、$X = \sum_{k=0}^{7} \lambda_k i_k$ に対し

$$R_0(X)R_0(X)^* = R_0(X\bar{X}) = \left(\sum_{k=0}^{7} \lambda_k^2\right) I_8,$$
$$L_0(X)L_0(X)^* = L_0(X\bar{X}) = \left(\sum_{k=0}^{7} \lambda_k^2\right) I_8$$

が成りたち、$R_0(X)$, $L_0(X)$ は 8 次直交配列 $OD(8; 1,1,1,1,1,1,1,1)$ である。

[II] $\{i_k : \sigma_k = 1\}$ が四元数群 $\{i_0, i_2, i_4, i_6\}$ の場合

$\sigma_1, \sigma_2, \sigma_3$ を

$$i_1\nu = \nu^{-1}i_1, \quad i_2\nu = \nu i_2, \quad i_4\nu = \nu i_4$$

で定義する（ν^{-1} は ν^{σ_k}, $\sigma_k \neq 1$ を表わし、行列環では転置を意味する）と、関係式(1)からすべての σ_k, $0 \leq k \leq 7$ は決定される。$\{i_k : \sigma_k = 1\} = \{i_0 = 1, i_2, i_4, i_6\}$ である。

$X = \lambda_0 + \lambda_1 i_1 + \lambda_2 i_2 + \lambda_3 i_3 + \lambda_4 i_4 + \lambda_5 i_5 + \lambda_6 i_6 + \lambda_7 i_7$ の右正則表現に準じた行列を

$$R_1(X) = \begin{pmatrix}
\lambda_0 & \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 & \lambda_5 & \lambda_6 & \lambda_7 \\
-\lambda_1^{-1} & \lambda_0^{-1} & -\lambda_3^{-1} & \lambda_2^{-1} & -\lambda_5^{-1} & \lambda_4^{-1} & \lambda_7^{-1} & -\lambda_6^{-1} \\
-\lambda_2 & \lambda_3 & \lambda_0 & -\lambda_1 & -\lambda_6 & -\lambda_7 & \lambda_4 & \lambda_5 \\
-\lambda_3^{-1} & -\lambda_2^{-1} & \lambda_1^{-1} & \lambda_0^{-1} & -\lambda_7^{-1} & \lambda_6^{-1} & -\lambda_5^{-1} & \lambda_4^{-1} \\
-\lambda_4 & \lambda_5 & \lambda_6 & \lambda_7 & \lambda_0 & -\lambda_1 & -\lambda_2 & -\lambda_3 \\
-\lambda_5^{-1} & -\lambda_4^{-1} & \lambda_7^{-1} & -\lambda_6^{-1} & \lambda_1^{-1} & \lambda_0^{-1} & \lambda_3^{-1} & -\lambda_2^{-1} \\
-\lambda_6 & -\lambda_7 & -\lambda_4 & \lambda_5 & \lambda_2 & -\lambda_3 & \lambda_0 & \lambda_1 \\
-\lambda_7^{-1} & -\lambda_6^{-1} & -\lambda_5^{-1} & -\lambda_4^{-1} & \lambda_3^{-1} & \lambda_2^{-1} & -\lambda_1^{-1} & \lambda_0^{-1}
\end{pmatrix}$$

で与える。$R_1(\overline{X}) = R_1(X)^*$ である。しかし[I]の場合とは異なり $X\overline{X}$ も対であり、$R(X\overline{X}) = R(X)R(\overline{X}) = R(X)R(X)^*$ は一般には成りたたない。$R(X)R(X)^*$ が対角行列となるには

$x_0x_2^{-1} = x_2x_0^{-1}$, $x_1x_3^{-1} = x_3x_1^{-1}$, $x_4x_6^{-1} = x_6x_4^{-1}$, $x_5x_7^{-1} = x_7x_5^{-1}$, $x_0x_4^{-1} = x_4x_0^{-1}$, $x_1x_5^{-1} = x_5x_1^{-1}$,

$x_2x_6^{-1} = x_6x_2^{-1}$, $x_3x_7^{-1} = x_7x_3^{-1}$, $x_0x_6^{-1} = x_6x_0^{-1}$, $x_1x_7^{-1} = x_7x_1^{-1}$, $x_2x_4^{-1} = x_4x_2^{-1}$, $x_3x_5^{-1} = x_5x_3^{-1}$

が必要である。$\sigma_1, \sigma_2, \sigma_3$ の定義の仕方により異なる右正則表現に準じた行列が得られる。同じようにして左正則表現に準じた行列 $L_1(X)$ も得られる。

$R_0(X), L_0(X), R_1(X), L_1(X)$ の変数 x_k, $0 \le k \le 7$ に互いに可換な行列を代入した8次の配列から Hadamard 行列を構成することを考える。これまでに知られている、成分が行列である8次の配列のタイプは、こうして得られたものに一致する。

3 $R_1(X) = R_1(x_0, x_1, \cdots, x_7)$ を使った次の定理がある。

<u>定理1</u> n 次正規行列 A, B, C, D, E, F, G, H が次を満たすとする。

(i) 互いに可換で、成分は1または-1。

(ii) A, E の各行、各列の +1 の数は -1 の数より2多い。

B, C, D, F, G, H の各行、各列の +1 の数と -1 の数は等しい。

(iii) $AC^* = CA^*$, $BD^* = DB^*$, $CE^* = EC^*$, $DF^* = FD^*$, $EG^* = GE^*$, $FH^* = HF^*$,

$AE^* = EA^*$, $BF^* = FB^*$, $CG^* = GC^*$, $DH^* = HD^*$, $AG^* = GA^*$, $BH^* = HB^*$

(iv) $AA^* + BB^* + CC^* + DD^* + EE^* + FF^* + GG^* + HH^* = 8(n+1)I_n - 8J_n$

ただし J_n は成分がすべて1の n 次正方行列。

さらに4次正方行列L, M, Kを次のように定義する。

$$L=\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix},\quad M=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix},\quad K=-\frac{1}{2}LM.$$

このとき

$$H=\begin{pmatrix} 1\otimes L & -1\otimes L & e^*\otimes K & -e^*\otimes K \\ 1\otimes L & 1\otimes L & e^*\otimes K & e^*\otimes K \\ e\otimes M^* & e\otimes M^* & R_1(A,B,C,D,E,F,G,H) & \\ -e\otimes M^* & e\otimes M^* & & \end{pmatrix}$$

は$8(n+1)$次Cayley数型Hadamard行列になる。ただし$e=\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix}$, $\otimes$はテンサー積である。

(証明) 条件(i)-(iv)を使ってHH^*を計算する。

4 qを奇素数中、$F=GF(q)$を有限体、$K=GF(q^2)$をFの2次拡大体、γをKの生成元とする。χをKの指標で$\chi(\gamma)=\zeta_{q-1}$であるとする。ただしζ_{q-1}は1の原始$q-1$乗根である。Z_mを次で定義する。

$$\chi\left(\frac{S_{K/F}\,\gamma^m}{2\gamma^m}\right)=\zeta_{q-1}^{Z_m}\qquad 0\le m\le q,\ m\neq\frac{q+1}{2}$$

さらに多項式$f(x)$を

$$f(x)=\sum_{\substack{m=0\\ m\neq\frac{q+1}{2}}}^{q} x^{Z_m}\qquad (\bmod x^{q-1}-1)$$

で定義する。

補助定理1: $f(x)$について次が成りたつ。

(i) $f(x)$は$x^0=1$を除きx^{Z_m}を丁度2個含む。

(ii) $f(x)f(x^{-1})\equiv q+(q+1)J_{q-1}(x)-2J_{(q-1)/2}(x^2)\qquad (\bmod x^{q-1}-1)$

ただし $J_{q-1}(x) = 1 + x + \cdots + x^{q-2}$, $J_{(q-1)/2}(x^2) = 1 + x^2 + \cdots + x^{\frac{q-3}{2}x^2}$ である。

(証明) [7] 参照.

<u>補助定理2</u> $f(x) \equiv f_0(x^2) + x f_1(x^2) \pmod{x^{q-1}-1}$ とおく。$f_0(x^2)$, $f_1(x^2)$ の x^2 を x でおきかえて多項式

$$\psi_0(x) \equiv f_0(x) - J_{(q-1)/2}(x) \pmod{x^{\frac{q-1}{2}}-1}$$

$$\psi_1(x) \equiv f_1(x) - J_{(q-1)/2}(x) \pmod{x^{\frac{q-1}{2}}-1}$$

を定義する。このとき

$$\psi_0(x)\psi_0(x^{-1}) + \psi_1(x)\psi_1(x^{-1}) \equiv q - 2J_{(q-1)/2}(x) \pmod{x^{\frac{q-1}{2}}-1}$$

が成りたつ。

(証明) [7] 参照.

次に χ_2 を $F = GF(q)$ の平方剰余指標とする。C_m を

$$C_m = \chi_2(S_{K/F}\, \gamma^{m+\frac{q+1}{2}}) \qquad 0 \le m \le 2q+1$$

で定義する。C_m について

$$C_{m+q+1} = -C_m \qquad C_{-m} = (-1)^{m+1+\frac{q+1}{2}} C_m$$

が成りたつ。特に $q \equiv 1 \pmod 4$ とすると $\frac{q+1}{2}$ は奇数で

$$C_{-m} = C_m \quad m: \text{偶数のとき} \qquad C_{-m} = -C_m \quad m: \text{奇数のとき}$$

となる。C_m を使って多項式

$$G(x) \equiv \sum_{m=0}^{2q+1} C_m x^m \pmod{x^{2q+2}-1}$$

を定義すると $G(x)$ は

$$G(x) \equiv (1-x^{q-1})\, g(x) \pmod{x^{2q+2}-1}$$

$$g(x) \equiv \sum_{m=0}^{q} C_m x^m \pmod{x^{q+1}+1}$$

の形をしている。

補助定理3　$g(x)$について

$$g(x)g(x^{-1}) \equiv q \pmod{x^{\frac{q+1}{2}}+1}$$

が成りたつ。$q \equiv 1 \pmod 4$とする。$g(x) \equiv g_0(x^2) + xg_1(x^2) \pmod{x^{\frac{q+1}{2}}+1}$とおき、$g_0(x^2), g_1(x^2)$の$x^2$を$x$でおきかえると

$$g_0(x) \equiv g_0(x^{-1}) \pmod{x^{\frac{q+1}{4}}+1}$$

が成りたつ。

(証明) [7] 参照.

5 定義　W_1, W_2, W_3, W_4を成分が1または-1のn次行列で

(i) $\forall N, M \in \{W_1, W_2, W_3, W_4\}$に対し、$NM^* = MN^*$

(ii) $W_1W_1^* + W_2W_2^* + W_3W_3^* + W_4W_4^* = 4nI_n$

をみたすとする。このときW_1, W_2, W_3, W_4をn次Williamson-type行列という。

1944年にWilliamson [5]によってWilliamson型Hadamard行列が導入された。このとき成分行列W_iは巡回行列であることを必要とした。上記Williamson-type行列やGoethals-Seidel行列はこの拡張である。

6 以上を使いCayley数型Hadamard行列の構成を考える。

定理2　$q \equiv 3 \pmod 4$, $q-2$がともに素数中ならば$8q$次Cayley数型Hadamard行列が構成できる。

(証明) 行列A, B, C, D, E, F, G, Hを次のように定義する。

$$A=E=\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes\psi_1(T),\qquad B=F=\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes\psi_0(T)+\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes I,$$

$$C=G=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes g_1(T'),\qquad D=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes(g_0(T')+I),$$

$$H=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes(g_0(T')-I)$$

これらが定理1の条件(i)-(iv)を満足することを示す。ただしTは$\frac{q-1}{2}$次基本巡回行列、T'は$\frac{q-1}{2}$次基本negacyclic行列、Iは$\frac{q-1}{2}$次単位行列である。

(i) $\psi_0(T)$, $\psi_1(T)$は巡回行列、$g_0(T')$, $g_1(T')$はnegacyclic行列。行列$\begin{pmatrix}1&1\\1&1\end{pmatrix}$と行列$\begin{pmatrix}1&-1\\-1&1\end{pmatrix}$の積は0行列であることから、A, B, C, …, Hは正規行列で(i)をみたす。

(ii) mが偶数(奇数)ならばΣ_mも偶数(奇数)となることが言える。$\frac{q+1}{2}$は偶数である。

$$f_0(1)=\frac{q+1}{2}-1=\frac{q-1}{2},\qquad \psi_0(1)=\frac{q-1}{2}-\frac{q-1}{2}=0,$$

$$f_1(1)=\frac{q+1}{2},\qquad \psi_1(1)=\frac{q+1}{2}-\frac{q-1}{2}=1,$$

から$\psi_0(T)$の各行、各列の＋の数と－の数は等しく、$\psi_1(T)$の各行、各列の＋の数は－の数より1つ多い。従って$B=F$の各行、各列の＋の数と－の数は等しく、$A=E$の各行、各列の＋の数は－の数より2つ多い。定義からC, D, H, G, の各行の各行の＋の数と－の数は等しい。

(iii) $A=E$, $B=F$, $C=G$から条件(iii)は

$$AC^*=CA^*,\quad BD^*=DB^*,\quad BH^*=HB^*,\quad DH^*=HD^*$$

が成りたつか調べることに帰着する。行列$\begin{pmatrix}1&1\\1&1\end{pmatrix}$と$\begin{pmatrix}1&-1\\-1&1\end{pmatrix}$の積

が0行列になることから

$$AC^* = CA^*$$

が成りたつ。 $D^* = D$, $H^* = H$ から

$$DH^* = DH - HD = HD^*$$

が成りたつ。

$$BD^* = BD = DB^* = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes (g_0(T') + I),$$

$$BH^* = BH = HB^* = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes (g_0(T') - I).$$

となる。

(iv) $AA^* + BB^* + CC^* + DD^* + EE^* + FF^* + GG^* + HH^*$

$$= 2\left\{2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes (\psi_0(T)\psi_0(T') + \psi_1(T)\psi_1(T')) + 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\}$$

$$+ 4\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes (g_0(T)g_0(T') + g_1(T')g_1(T') + I)$$

$$= 4\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes (qI - 2J_{\frac{q-1}{2}}) + 4\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I + 4\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes (q-1)I$$

$$= 8qI_{q-1} - 8J_{q-1}$$

以上から $8q$ 次 Cayley 数型 Hadamard 行列が構成できる。

この定理は、Spence が $8q$ 次 Goethals-Seidel 配列を使って証明している[8]。ここでは Cayley 数型配列を使っても証明できることを示した。Spence の用いた8次の Goethals-Seidel 配列は、成分行列が巡回行列であるという条件を必要としている。Cayley 数型配列では行列 $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ と $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ の積が0行列になることを利用して成分行列は必ずしも巡回行列であることを必要としない。この例としてさらに2つの定理をあげる。

定理3 q: 奇素数中とする。$\frac{1}{2}(q-1)$次 Williamson-type 行列が存在し、互いに可換でそのうちの2つは対称行列であるとする。このとき $8q$次 Cayley 数型 Hadamard 行列が構成できる。

(証明) $q \equiv 1 \pmod 4$ のとき、行列 A, B, C, D, E, F, G, H, を

$$A = E = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \phi_0(T) + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I, \quad B = F = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \phi_1(T)$$

$$C = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_1, \quad D = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_2, \quad G = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_3, \quad H = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_4$$

で定義する。ただし W_1, W_2, W_3, W_4 は $\frac{1}{2}(q-1)$次 Williamson-type 行列で W_1, W_3 は対称行列とする。

$q \equiv 3 \pmod 4$ の場合には $q \equiv 1 \pmod 4$ の場合の A と B、E と F、C と D、G と H を入れかえて定義する。こうして定義された行列 A, B, C, D, E, F, G, H が定理1の条件をみたすことを示す。

(i) 行列 A, B, C, …, H は成分が 1 または -1 で互いに可換であることは明らか。

(ii) $q \equiv 1 \pmod 4$ のとき $\frac{q+1}{2}$ が奇数から $\phi_0(1) = 1$, $\phi_1(1) = 0$,

$q \equiv 3 \pmod 4$ のとき $\frac{q+1}{2}$ が偶数から $\phi_0(1) = 0$, $\phi_1(1) = 1$,

である。これより A, E の各行、各列の＋の数は－の数より2多く、B＝F の各行、各列の＋の数と－の数は等しい。定義から C, D, G, H の各行、各列の＋の数と－の数は等しい。

(iii) $q \equiv 1 \pmod 4$ の場合、A＝E、B＝F から

$$AC^* = CA^*, \quad BD^* = DB^*, \quad AG^* = GA^*, \quad BH^* = HB^*, \quad CG^* = GC^*, \quad DH^* = HD^*$$

が成りたつことを言えばよい。AとB, EとF, CとD, GとHを入れかえても同じ式が得られるので、$q \equiv 3 \pmod 4$ の場合は $q \equiv 1 \pmod 4$ の場合に帰着する。行列 $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ と行列 $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ の積が0行列になることから

$$BD^* = DB^* , \quad BH^* = HB^*$$

が成りたつ。$C^* = C$, $G^* = G$ から

$$AC^* = AC = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_1 = CA^*, \quad AG^* = AG = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_3 = GA^*$$

$$CG^* = CG = GC = GC^*$$

が成りたつ。

$$DH^* = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_2 W_4^* , \quad HD^* = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes W_4 W_2^*$$

において $W_2 W_4^* = W_4 W_2^*$ から $DH^* = HD^*$ を得る。

(iv) $AA^* + BB^* + CC^* + DD^* + EE^* + FF^* + GG^* + HH^*$

$$= 2\left\{2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \left(\psi_0(T)\psi_0(T^{-1}) + \psi_1(T)\psi_1(T^{-1})\right) + 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I\right\}$$

$$+ 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes (W_1 W_1^* + W_2 W_2^* + W_3 W_3^* + W_4 W_4^*)$$

$$= 4\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes (qI - 2J_{\frac{q-1}{2}}) + 4\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I + 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes 2(q-1)I$$

$$= 8qI_{q-1} - 8J_{q-1}$$

以上から $8q$ 次 Cayley 数型 Hadamard 行列が構成できる。

<u>定理4</u> $q \equiv 1 \pmod 4$ 素数中とする。$\frac{1}{4}(q-1)$ 次 Williamson-type 行列が存在し、互いに可換でそのうちの2つは対称行列とする。このとき $8q$ 次 Cayley 数型 Hadamard 行列が構成できる。

(証明) 行列 A, B, C, D, E, F, G, H を次で定義する。

$$A=E=\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes\psi_0(T)+\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes I$$

$$B=F=\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes\psi_1(T)$$

$$C=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes\begin{pmatrix}W_1&W_1\\W_1&-W_1\end{pmatrix},\quad D=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes\begin{pmatrix}W_2&W_2\\W_2&-W_2\end{pmatrix}$$

$$G=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes\begin{pmatrix}W_3&W_3\\W_3&-W_3\end{pmatrix},\quad H=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes\begin{pmatrix}W_4&W_4\\W_4&-W_4\end{pmatrix}$$

とおく。W_1, W_2, W_3, W_4 は $\frac{1}{4}(q-1)$ 次 Williamson-type 行列で W_1, W_3 は対称行列とする。$1\leq l$, $m\leq 4$ に対し

$$\begin{pmatrix}W_l&W_l\\W_l&-W_l\end{pmatrix}\begin{pmatrix}W_m&W_m\\W_m&-W_m\end{pmatrix}=\begin{pmatrix}2W_lW_m&0\\0&2W_lW_m\end{pmatrix},$$

$$\begin{pmatrix}W_m&W_m\\W_m&-W_m\end{pmatrix}\begin{pmatrix}W_l&W_l\\W_l&-W_l\end{pmatrix}=\begin{pmatrix}2W_mW_l&0\\0&2W_mW_l\end{pmatrix}=\begin{pmatrix}2W_lW_m&0\\0&2W_lW_m\end{pmatrix}$$

から C, D, G, H は互いに可換である。行列 A, B, C, …, H が定理1の条件を満足することが定理3と同じようにして証明できる。

7 Williamson-type の無限系列はいくつか知られている[1, 2, 3, 4, 6]。次の定理

定理5[4] $p\equiv 1 \pmod 4$ が素数中ならば $\frac{1}{2}p(p+1)$ 次 Williamson-type 行列が存在する。

で構成された Williamson-type 行列は互いに可換でかつ対称行列であるが巡回行列ではない。そしてこの Williamson-type 行列を使った行列 $\begin{pmatrix}W_l&W_l\\W_l&-W_l\end{pmatrix}$, $1\leq l\leq 4$ もまた巡回行列ではない。

参考文献

[1] R. J. Turyn, An infinite class of Williamson matrices, J. Comb. Theory (A) 12 (1972), 319-321.

[2] R. J. Turyn, A special class of Williamson matrices and difference sets, J. Comb. Theory (A) 36 (1984), 111-115.

[3] J. S. Wallis, Constructions of Williamson type matrices, Linear and Multilinear Algebra, 3 (1975), 197-207.

[4] J. S. Wallis, Some matrices of Williamson type, Utilitas Math., 4 (1973), 147-154.

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

[6] A. L. Whiteman, An infinite family of Hadamard matrices of Williamson type, J. Comb. Theory (A) 14 (1973), 334-340.

[7] M. Yamada, Hadamard matrices generated by an adaptation of generalized quaternion type array, Graphs and Combinatorics 2 (1986), 179-187.

[8] E. Spence, Hadamard matrices from relative difference sets, J. Comb. Theory (A) 19 (1975), 287-300.