

ある特殊な T-行列について

名工大 情報 沢出和江

1. Baumert-Hall 配列

最近の Hadamard 行列の構成と存在の問題には Baumert-Hall 配列 (array) と Williamson 行列の構成が重要な役割をなしていると思われる [1,3]. Williamson 行列については, 山田氏の論文 [4] に詳しく書かれているので, ここでは簡単に述べるに留める. t 次の Williamson 行列 A, B, C, D とは対称巡回 $(1, -1)$ -行列で, $A^2 + B^2 + C^2 + D^2 = 4tI_t$ を満足するものである. 従って, A, B, C, D は互いに可換であることに注意する.

n 次の Baumert-Hall 配列とは, Williamson 行列 A, B, C, D に対し, 次の 3 条件を満たすものである;

- (i) 行列 $\pm A, \pm B, \pm C, \pm D$ を成分に持つ n 行 n 列の配列である;
- (ii) 成分の符号を無視した時, どの行 (列) にも A, B, C, D が, n 個ずつ存在する;
- (iii) どの相異なる 2 行 (列) も形式的に直交している.

例えば, J. Williamson が Hadamard 行列の構成に使った四元数型配列

$$\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

は 1 次の Baumert-Hall 配列である. Baumert-Hall 配列は, 1965 年に L. Baumert と M. Hall が 3 次のこの配列を初めて構成し, これと 13 次の Williamson 行列によって 156 次の Hadamard 行列の構成に成功したことから, そう呼ばれているようである.

n 次の Baumert-Hall 配列と t 次の Williamson 行列が存在すれば, $4nt$ 次の Hadamard 行列が存在する.

2. T-行列

次の 3 つの条件を満たす行列 X_1, X_2, X_3, X_4 を T-行列と言う;

(I) すべて n 次巡回 $(1, 0, -1)$ -行列である;

(II) a_k, b_k, c_k, d_k ($k=0, 1, \dots, n-1$) をそれぞれ X_1, X_2, X_3, X_4 の第 1 行とすると, a_k, b_k, c_k, d_k のうちいずれか 1 つが $+1$ か -1 で, 他の 3 つは 0 である;

$$(III) X_1 X_1^T + X_2 X_2^T + X_3 X_3^T + X_4 X_4^T = nI_n \quad (1)$$

が成り立つ.

T-行列の重要性は次の定理から分かる.

定理 (Cooper-Wallis [3]) n 次の T -行列 X_1, X_2, X_3, X_4 が存在するならば, A, B, C, D を t 次の Williamson 行列とする時

$$\begin{aligned} X &= X_1 \otimes A + X_2 \otimes B + X_3 \otimes C + X_4 \otimes D, \\ Y &= X_1 \otimes (-B) + X_2 \otimes A + X_3 \otimes D + X_4 \otimes (-C), \\ Z &= X_1 \otimes (-C) + X_2 \otimes (-D) + X_3 \otimes A + X_4 \otimes B, \\ W &= X_1 \otimes (-D) + X_2 \otimes C + X_3 \otimes (-B) + X_4 \otimes A, \end{aligned} \quad (2)$$

と置き, Goethals-Seidel 配列

$$GS = \begin{pmatrix} X & YR & ZR & WR \\ -YR & X & -WR & Z'R \\ -ZR & WR & X & -YR \\ -WR & -Z'R & YR & X \end{pmatrix} \quad (3)$$

に代入すると, n 次の Baumert-Hall 配列が構成出来る。ここで, $\otimes$ はテンサー積; R は, n 次の基本的逆巡回行列と t 次の単位行列とのテンサー積である。

この定理は, n 次の T -行列と t 次の Williamson 行列が存在すれば, $4nt$ 次の Hadamard 行列が構成出来ることを意味する。更にその特殊な場合として, T -行列の次数が 1 の時に得られる Hadamard 行列は Williamson 型である。逆に, $t=1$ の時は, R が n 次基本的逆巡回行列, (2) 式の X, Y, Z, W が共に n 次の巡回 $(1, -1)$ -行列となり,

$$XX^T + YY^T + ZZ^T + WW^T = 4nI_n \quad (4)$$

を満足する。これは、(3)式が Goethals-Seidel 型 Hadamard 行列になる為の必要条件である。故に Williamson 行列の次数が 1 の時に得られる Hadamard 行列は Goethals-Seidel 型である。

3. T-行列と Goethals-Seidel 型 Hadamard 行列

n 次の T-行列が存在すれば、 $4n$ 次の Goethals-Seidel 型の Hadamard 行列が存在することが分かった。その時の (3) 式の X, Y, Z, W は、例えば $A=B=C=D=1$ の時には次の式から得る。

$$\begin{aligned} X &= X_1 + X_2 + X_3 + X_4, & Y &= -X_1 + X_2 + X_3 - X_4, \\ Z &= -X_1 - X_2 + X_3 + X_4, & W &= -X_1 + X_2 - X_3 + X_4. \end{aligned} \quad (5)$$

逆に、 n 次の X, Y, Z, W が存在するならば、それらは基本的巡回行列 U の多項式として次のように書ける：

$$X = \sum_{k=0}^{n-1} x_k U^k, \quad Y = \sum_{k=0}^{n-1} y_k U^k, \quad Z = \sum_{k=0}^{n-1} z_k U^k, \quad W = \sum_{k=0}^{n-1} w_k U^k.$$

但し x_k, y_k, z_k, w_k ($k=0, 1, \dots, n-1$) は X, Y, Z, W の第 1 行とする。

この時、行列 X_1, X_2, X_3, X_4 が (5) 式の逆変換

$$\begin{aligned} X_1 &= \frac{1}{4}(X - Y - Z - W), & X_2 &= \frac{1}{4}(X + Y - Z + W), \\ X_3 &= \frac{1}{4}(X + Y + Z - W), & X_4 &= \frac{1}{4}(X - Y + Z + W) \end{aligned}$$

で得られ、かつその成分 $a_k = \frac{1}{4}(x_k - y_k - z_k - w_k)$, $b_k = \frac{1}{4}(x_k + y_k - z_k + w_k)$, $c_k = \frac{1}{4}(x_k + y_k + z_k - w_k)$, $d_k = \frac{1}{4}(x_k - y_k + z_k + w_k)$ ($k=0, 1, \dots, n-1$) の全てが整数、すなわち 1 か 0 か -1 である場合には

$$X_1 = \sum_{k=0}^{n-1} a_k U^k, \quad X_2 = \sum_{k=0}^{n-1} b_k U^k, \quad X_3 = \sum_{k=0}^{n-1} c_k U^k, \quad X_4 = \sum_{k=0}^{n-1} d_k U^k \quad (6)$$

は n 次の T -行列となる。言い換えると x_k, y_k, z_k, w_k の中できっかり3つが同符号と言う条件が全ての k について成り立っている時に限り T -行列が得られる。その T -行列は (5) 式の X_1, X_2, X_3, X_4 である。同様のことを Williamson 行列 A, B, C, D が 1 次の時の一般の場合について調べると次が得られた。

Goethals-Seidel 型 Hadamard 行列において、行列 X, Y, Z, W の第 1 行を x_k, y_k, z_k, w_k ($k=0, 1, \dots, n-1$) とする時、全ての k について次の (i) または (ii) のいずれか一方を満足する時その時に限って、 X, Y, Z, W の存在と T -行列 X_1, X_2, X_3, X_4 の存在は同値である、

- (i) x_k, y_k, z_k, w_k の中で常に 3 つが同符号である、
- (ii) x_k, y_k, z_k, w_k の中で常に 2 つまたは 4 つが同符号である。

さて、(6) 式を対角化すると (1) 式は

$$F_1(\zeta) = \sum_{k=0}^{n-1} a_k \zeta^k, \quad F_2(\zeta) = \sum_{k=0}^{n-1} b_k \zeta^k, \quad F_3(\zeta) = \sum_{k=0}^{n-1} c_k \zeta^k, \quad F_4(\zeta) = \sum_{k=0}^{n-1} d_k \zeta^k, \quad (7)$$

$$F_1(\zeta)F_1(\zeta^{-1}) + F_2(\zeta)F_2(\zeta^{-1}) + F_3(\zeta)F_3(\zeta^{-1}) + F_4(\zeta)F_4(\zeta^{-1}) = n$$

と同値になる。ここで、 ζ は 1 の n 乗根とする。

Goethals-Seidel 型 Hadamard 行列では、 X, Y, Z, W からは必ずしも対応する T -行列が得られないが、その成分 x_k, y_k, z_k, w_k が先の条件 (i) または (ii) を満足する時には、 X, Y, Z, W と (7) 式の関

係が, Williamson 型 Hadamard 行列での, Williamson 行列 A, B, C, D と Williamson 等式の関係に似ている.

また一方, X, Y, Z, W には Williamson 行列に課せられている対称性は要求されていないかった. これは Williamson 行列よりも存在可能性が高いことを示していると思われる.

従って我々が考えたい特殊な形の Hadamard 行列に限定した場合, Williamson 型では存在しないが, Goethals-Seidel 型では存在する次数があるかも知れない. ここでは, この予想を肯定的にするデータを紹介する.

4. ある特殊な T-行列

以後, 次数が素数 $p \equiv 1 \pmod{3}$ で特殊な形の T-行列を考える. この時, $p = \alpha^2 + 3\beta^2$, $\alpha \equiv 1 \pmod{3}$, $\beta > 0$ の形に一意的に表わせる. 例えば, $7 = (-2)^2 + 3 \cdot 1^2$, $13 = 1^2 + 3 \cdot 2^2$, 等である. またそのような p について, $4p = u^2 + 3v^2$ の形に書ける (u, v) が 3 通りだけあり, u, v 共に奇数であるのはそのうちの 2 通りである. 即ち $(u, v) = (\alpha - 3\beta, \alpha + \beta), (\alpha + 3\beta, \alpha - \beta)$ である. 問題の T-行列と比較する Williamson 等式はこの 2 通りの中で更に $u \equiv 1 \pmod{12}$, $v \equiv 1 \pmod{4}$ を満たす場合である.

ζ : 1 の原始 p 乗根, γ : p の原始根,

w : 法 p の剰余類体 $\mathbb{F}_p$ の中で $w \neq 1, w^3 \equiv 1 \pmod{p}$ を満たすもの,

$F_1(x), F_2(x), F_3(x), F_4(x) : X_1, X_2, X_3, X_4$ の生成函数.

$\mathbb{Q}(\zeta)/\mathbb{Q}$ の生成的自己同型 $\sigma: \zeta \rightarrow \zeta^r$ とおくと, $\tau: \zeta \rightarrow \zeta^w$ について $H = \langle \tau \rangle$ は $G = \langle \sigma \rangle$ の位数 3 の部分群である.

さて, 我々は $F_1(\zeta) = \sum_{k=0}^{p-1} a_k \zeta^k$ は H で不変であって, しかも $F_2(\zeta) = \sum_{k=0}^{p-1} b_k \zeta^k$, $F_3(\zeta) = \sum_{k=0}^{p-1} c_k \zeta^k$, $F_4(\zeta) = \sum_{k=0}^{p-1} d_k \zeta^k$ は τ によって,

$$\tau: F_2(\zeta) \rightarrow F_3(\zeta), F_3(\zeta) \rightarrow F_4(\zeta), F_4(\zeta) \rightarrow F_2(\zeta)$$

と仮定したい. この時明らかに, $F_1(1) = \alpha$, $F_2(1) = F_3(1) = F_4(1) = \pm\beta$ を満足しなければならないが, $\pm X_1, \pm X_2, \pm X_3, \pm X_4$ も T -行列であるから, 後者の式は $\pm\beta$ と仮定出来る. すると $b_k = c_{kw} = d_{kw^2} = 1$ なる $1 \leq k \leq p-1$ が存在し, その k に対し $k = w^{\delta_\nu} r^\nu$, $0 \leq \delta_\nu \leq 2$, $0 \leq \nu \leq e-1$, $e = (p-1)/3$ を満たす (δ_ν, ν) が唯一組存在するから, $\mathbb{Q}(\zeta)/\mathbb{Q}$ の自己同型 $\sigma^{-\nu}$ と $\tau^{-\delta_\nu}$ の合成写像により $\zeta^k = \zeta^{w^{\delta_\nu} r^\nu}$ を ζ に移すことが出来る. この時勿論 $F_1(\zeta)$ の H のもとでの不変性は保存されている. 以上により, 我々が考える T -行列は, 自己同型によって次の様な形に出来る.

$$F_1(\zeta) = 1 + \sum_{\nu \in A_+} (\zeta^{r^\nu} + \zeta^{w r^\nu} + \zeta^{w^2 r^\nu}) - \sum_{\nu \in A_-} (\zeta^{r^\nu} + \zeta^{w r^\nu} + \zeta^{w^2 r^\nu}),$$

$$F_2(\zeta) = \zeta + \sum_{\nu \in B_+} \zeta^{w^{\delta_\nu} r^\nu} - \sum_{\nu \in B_-} \zeta^{w^{\delta_\nu} r^\nu},$$

(8)

$$F_3(\zeta) = \zeta^w + \sum_{\nu \in B_+} \zeta^{w^{(\delta_\nu+1)} r^\nu} - \sum_{\nu \in B_-} \zeta^{w^{(\delta_\nu+1)} r^\nu},$$

$$F_4(\zeta) = \zeta^{w^2} + \sum_{\nu \in B_+} \zeta^{w^{(\delta_\nu+2)} r^\nu} - \sum_{\nu \in B_-} \zeta^{w^{(\delta_\nu+2)} r^\nu},$$

但し, $e=(p-1)/3$; A_+, A_-, B_+, B_- は $\Omega=\{1, 2, \dots, e-1\}$ の分割; S_ν は ν に依存して 0, 1, 2 のいずれかの値を取るものとする.

そして, こゝらが

$$F_1(1) = \alpha \equiv 1 \pmod{3}, \quad F_2(1) = F_3(1) = F_4(1) = \beta \quad (9)$$

さらには

$$F_1(\zeta)F_1(\zeta^{-1}) + F_2(\zeta)F_2(\zeta^{-1}) + F_3(\zeta)F_3(\zeta^{-1}) + F_4(\zeta)F_4(\zeta^{-1}) = p \quad (10)$$

を満足するようにさせたい.

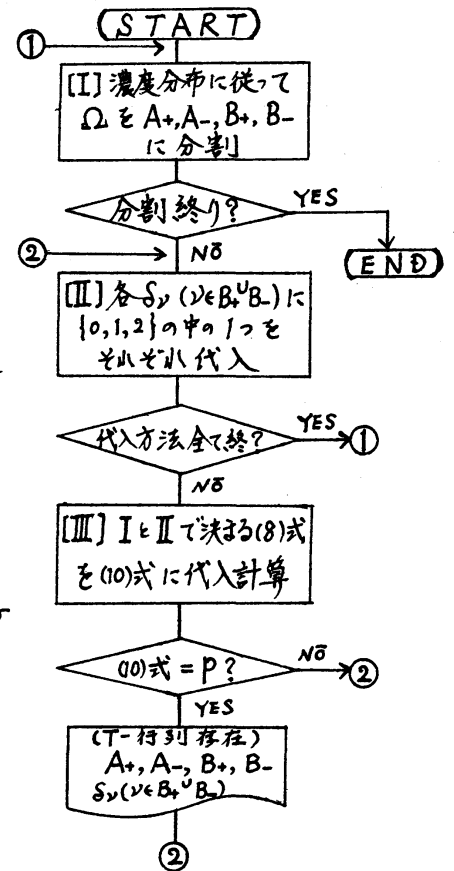
我々は, このような T-行列の存在を予想しその検索を行った.

5. 特殊な T-行列の検索方法 (その 1)

p 次 T-行列の実際の検索に当って
第 1 に, (9) 式を満たす $\#A_+, \#A_-, \#B_+, \#B_-$ の分布表を手作業により求め, その 1 つをそれぞれ r_1, r_2, r_3, r_4 とおく. この濃度分布に基づいた計算手順の概略は右のようである.

I の方法の数は, $\frac{(e-1)!}{r_1! r_2! r_3! r_4!}$ 通り,
II の方法の数は $3^{r_3+r_4}$ 通り, 従って総試行回数は $3^{r_3+r_4} \cdot \frac{(e-1)!}{r_1! r_2! r_3! r_4!}$.

ここで問題は III の計算方法であるが, 初めは次のように行なった.



$\eta_\nu = \zeta^{\gamma_\nu} + \zeta^{w\gamma_\nu} + \zeta^{w^2\gamma_\nu}$ ($\nu = 0, 1, \dots, e-1$) とおくと

$$\begin{aligned} F_1(\zeta)F_1(\zeta^{-1}) &= 1 + 3\left(\sum_{A_+} + \sum_{A_-}\right) + \sum_{\nu \in A_+} (\eta_\nu + \eta_{\nu+\frac{e}{2}}) - \sum_{\nu \in A_-} (\eta_\nu + \eta_{\nu+\frac{e}{2}}) \\ &\quad + \sum_{\substack{\nu \in A_+ \\ \nu \neq \mu}} \sum_{\substack{\mu \in A_- \\ \mu \neq \nu}} \sum_{k=0}^{e-1} (\mu-k, \nu-k) \eta_k + \sum_{\substack{\nu \in A_- \\ \nu \neq \mu}} \sum_{\substack{\mu \in A_+ \\ \mu \neq \nu}} \sum_{k=0}^{e-1} (\mu-k, \nu-k) \eta_k \\ &\quad - \sum_{\nu \in A_+} \sum_{\mu \in A_-} \sum_{k=0}^{e-1} \left\{ (\mu-k, \nu-k) + (\mu-k+\frac{e}{2}, \nu-k+\frac{e}{2}) \right\} \eta_k \end{aligned} \quad (11)$$

ここで (i, j) は $\mathcal{R}_p^*$ の e 乗剰余類 $L_k = \{\gamma^{es+k} \mid s=0, 1, 2\}$ ($k=0, \dots, e-1$) に関する円分数で, $l-m \in L_0$, $l \in L_j$, $m \in L_i$ を満たす対 (l, m) の数で定義されるものである.

さらに, $(1-w^{\delta_\nu}\gamma_\nu) \in L_{\phi(\nu)}$, $(w^{\delta_\nu}\gamma_\nu - w^{\delta_\mu}\gamma_\mu) \in L_{\psi(\nu, \mu)}$ とおくと

$$\begin{aligned} &F_2(\zeta)F_2(\zeta^{-1}) + F_3(\zeta)F_3(\zeta^{-1}) + F_4(\zeta)F_4(\zeta^{-1}) \\ &= 3\left(1 + \sum_{B_+} + \sum_{B_-}\right) + \sum_{\nu \in B_+} (\eta_{\phi(\nu)} + \eta_{-\phi(\nu)}) - \sum_{\nu \in B_-} (\eta_{\phi(\nu)} + \eta_{-\phi(\nu)}) \\ &\quad + \sum_{\substack{\nu \in B_+ \\ \nu \neq \mu}} \sum_{\substack{\mu \in B_+ \\ \mu \neq \nu}} \eta_{\psi(\nu, \mu)} + \sum_{\substack{\nu \in B_- \\ \nu \neq \mu}} \sum_{\substack{\mu \in B_- \\ \mu \neq \nu}} \eta_{\psi(\nu, \mu)} - \sum_{\nu \in B_+} \sum_{\mu \in B_-} (\eta_{\psi(\nu, \mu)} + \eta_{-\psi(\nu, \mu)}). \end{aligned} \quad (12)$$

$1 + 3\left(1 + \sum_{A_+} + \sum_{A_-} + \sum_{B_+} + \sum_{B_-}\right) = P$ であるから, (11)式と(12)式を加えてすべての η_k の係数が 0 になることが T-行列になる為の必要十分条件である. 明らかにそれは計算機にとって簡単な整数計算ではあるが, 計算時間の短縮化と言う目的からサブルーチン方式を避け, 先ず円分数表, $L_{\phi(\nu)}$ と $L_{\psi(\nu, \mu)}$ の表を全てストアしておき, 計算の都度テーブルサーチする方式を取ったが, それでも $L_{\psi(\nu, \mu)}$ を 4 次元配列にした為, 探索に時間が掛かり, あまり有効ではなかった. $P \leq 31$ については全てこの方法で検

索した。

6. 特殊な T-行列の検索方法 (その 2)

そこで $F_i(\zeta)F_i(\zeta^{-1}) = \{F_i(\zeta) \text{ の実部} \}^2 + \{F_i(\zeta) \text{ の虚部} \}^2$, $\zeta^k = \cos \frac{2\pi k}{p} + i \sin \frac{2\pi k}{p}$ を利用して, $F_i(\zeta)$ ($i=1,2,3,4$) を実部と虚部に分け, 直接 $\cos \frac{2\pi k}{p}$ と $\sin \frac{2\pi k}{p}$ を代入して近似計算をしてみた. しかしこの計算は倍精度演算でなければ, よい近似値が得られない. 浮動小数点計算をなるべく行わずに済むように, その前に整数計算の判定条件を入れることとする. それは次のようである.

体 $\mathbb{Q}(\zeta)$ における有理素数 p の素因子を ρ とし, $\mathbb{Q}(\zeta)$ の整数環の ρ 進完備の中に $\omega^{\rho-1} = -p$ を満たす ω が存在するが, その ω の中で, $\omega \equiv \zeta - 1 \pmod{\rho^2}$ を満たすものに固定して

$$\zeta^m \equiv \sum_{\nu=0}^{p-1} \frac{m^\nu}{\nu!} \omega^\nu \pmod{\rho^p}$$

と ρ 進近似出来る [2, 5]. 従って

$$\zeta^{\gamma^{\nu}} + \zeta^{\omega \gamma^{\nu}} + \zeta^{\omega^2 \gamma^{\nu}} \equiv 3 \left(1 + \frac{1}{3!} \gamma^{\nu} \omega^3 + \frac{1}{6!} \gamma^{\nu} \omega^6 \right) \pmod{\rho^7}$$

より

$$\begin{aligned} F(\zeta)F(\zeta^{-1}) &\equiv (1 + 3 \sum_{A_+} - 3 \sum_{A_-})^2 \\ &\quad + \left\{ \frac{6}{6!} (1 + 3 \sum_{A_+} - 3 \sum_{A_-}) \left(\sum_{A_+} \gamma^{\nu} - \sum_{A_-} \gamma^{\nu} \right) - \frac{3^2}{(3!)^2} \left(\sum_{A_+} \gamma^{\nu} - \sum_{A_-} \gamma^{\nu} \right)^2 \right\} \omega^6 \pmod{\rho^7}. \quad (13) \end{aligned}$$

$$E_k = 1 + \sum_{\nu \in B_+} w^{k\delta_\nu} \gamma^{k\nu} - \sum_{\nu \in B_-} w^{k\delta_\nu} \gamma^{k\nu} \quad (k=0,1,\dots,6)$$

とおくと

$$F_2(\zeta) \equiv \sum_{k=0}^6 \frac{E_k}{k!} \omega^k, \quad F_3(\zeta) \equiv \sum_{k=0}^6 \frac{w^k E_k}{k!} \omega^k, \quad F_4(\zeta) \equiv \sum_{k=0}^6 \frac{w^{2k} E_k}{k!} \omega^k \pmod{p^7}.$$

従って

$$\begin{aligned} & F_2(\zeta)F_2(\zeta^{-1}) + F_3(\zeta)F_3(\zeta^{-1}) + F_4(\zeta)F_4(\zeta^{-1}) \\ & \equiv 3E_0^2 + 3\left(\frac{2}{6!}E_0E_6 - \frac{2}{5!}E_1E_5 + \frac{2}{2!4!}E_2E_4 - \frac{1}{(3!)^2}E_3^2\right)\omega^6 \pmod{p^7}. \end{aligned} \quad (14)$$

今, $(1+3\sum_{A_+} - 3\sum_{A_-})^2 + 3E_0^2 = \alpha^2 + 3\beta^2 = p$ であるから, (10)式が $\text{mod } p^7$ で成り立つ為には, (13)式と(14)式を加えて ω^6 の係数が $\text{mod } p$ で 0 と合同になることが必要である. すなわち

$$\begin{aligned} & \alpha\left(\sum_{\nu \in A_+} \gamma^{\delta_\nu} - \sum_{\nu \in A_-} \gamma^{\delta_\nu}\right) - 30\left(\sum_{\nu \in A_+} \gamma^{2\delta_\nu} - \sum_{\nu \in A_-} \gamma^{2\delta_\nu}\right)^2 + \beta\left(1 + \sum_{\nu \in B_+} \gamma^{\delta_\nu} - \sum_{\nu \in B_-} \gamma^{\delta_\nu}\right) - 10\left(1 + \sum_{\nu \in B_+} \gamma^{2\delta_\nu} - \sum_{\nu \in B_-} \gamma^{2\delta_\nu}\right)^2 \\ & - 6\left(1 + \sum_{\nu \in B_+} w^{\delta_\nu} \gamma^{\delta_\nu} - \sum_{\nu \in B_-} w^{\delta_\nu} \gamma^{\delta_\nu}\right)\left(1 + \sum_{\nu \in B_+} w^{2\delta_\nu} \gamma^{2\delta_\nu} - \sum_{\nu \in B_-} w^{2\delta_\nu} \gamma^{2\delta_\nu}\right) \\ & + 15\left(1 + \sum_{\nu \in B_+} w^{2\delta_\nu} \gamma^{2\delta_\nu} - \sum_{\nu \in B_-} w^{2\delta_\nu} \gamma^{2\delta_\nu}\right)\left(1 + \sum_{\nu \in B_+} w^{\delta_\nu} \gamma^{4\delta_\nu} - \sum_{\nu \in B_-} w^{\delta_\nu} \gamma^{4\delta_\nu}\right) \equiv 0 \pmod{p} \end{aligned} \quad (15)$$

が判定条件である. この判定条件を用いた結果, $p=37$ の場合の計算時間は約 $1/3$ 短縮出来た. また, 上の方法で近似計算をした結果が真の T-行列であるのかどうかは, 5 の方法で組んだプログラムを使って確かめることが出来た.

現在, $p=37$ 迄については全て計算が完了している. その結果は表1のようであるが, 総当り計算では $p=37$ が限界と思われる.

一方, 同じ条件を満たす Williamson 等式は次のようになる.

$$\begin{aligned} & \left\{ 1 + 2 \sum_{\nu \in A_+} (\theta_{\nu} + \theta_{w\nu} + \theta_{w^2\nu}) - 2 \sum_{\nu \in A_-} (\theta_{\nu} + \theta_{w\nu} + \theta_{w^2\nu}) \right\}^2 \\ & + \left\{ 1 + 2 \sum_{\nu \in B_+} \theta_{w^{\delta\nu}\nu} - 2 \sum_{\nu \in B_-} \theta_{w^{\delta\nu}\nu} \right\}^2 + \left\{ 1 + 2 \sum_{\nu \in B'_+} \theta_{w^{(\delta\nu+1)}\nu} - 2 \sum_{\nu \in B'_-} \theta_{w^{(\delta\nu+1)}\nu} \right\}^2 \\ & + \left\{ 1 + 2 \sum_{\nu \in B''_+} \theta_{w^{(\delta\nu+2)}\nu} - 2 \sum_{\nu \in B''_-} \theta_{w^{(\delta\nu+2)}\nu} \right\}^2 = 4p, \end{aligned}$$

但し, $\theta_k = \zeta^k + \zeta^{-k}$; A_+, A_-, B_+, B_- は $\Omega = \{0, 1, \dots, \frac{p-1}{6}-1\}$ の分割である. 表2は, 上の形の $p \leq 37$ の Williamson 等式のすべてを表わしているが, 表1と表2を比較すると T-行列の方が存在性が高まるかに高いことがよく分かる.

7. 今後の課題

本稿では, 問題の T-行列の次数を素数に限定したが, 素数中への拡張も考えられる. 今後, 検索方法とプログラムの改良を重ねて $p=67$ についての検索を行ない, さらにこの特殊な T-行列が無限に存在するかどうかを調べることが大きな課題である.

表 1. $P(\leq 37)$ 次の特殊な T-行列

P	α	β	e	# Ω	#A+	#A-	#B+	#B-	ONE OF T-MATRICES				NO. OF T-MATRICES	NO. OF TRIALS	RUN TIME	MACHINE
									A+	A-	B+ (δ_v)	B- (δ_v)				
7	-2	1	2	1	0	1	0	0	$\emptyset$	1	$\emptyset$	$\emptyset$	1	1		
13	1	2	4	3	1	1	1	0	1	2	3 (1)	$\emptyset$	2	18	00:00:11	OKITAC 50
					0	0	2	1	$\emptyset$	$\emptyset$	1 (1), 2 (0)	3 (0)	18	81	00:00:01	HITAC 8450
19	4	1	6	5	3	2	0	0					NONE	10		
					2	1	1	1	2,4	3	5 (0)	1 (1)	50	540	00:00:12	OKITAC 50
31	-2	3	10	9	3	4	2	0	1	$\emptyset$	4 (0), 5 (1)	2 (0), 3 (2)	132	2430	00:00:05	HITAC 8450
					1	0	2	2					NONE	11340	00:00:53	HITAC 8450
					2	3	3	1					NONE	408240	00:15:05	HITAC 8450
					1	2	4	2	1	2,4	6 (1), 7 (2), 8 (2), 9 (1) 5 (1), 6 (0), 7 (1), 8 (1), 9 (1)	3 (0), 5 (0)	2670	2755620	02:44:50	HITAC 8450
					0	1	5	3	$\emptyset$	1		2 (2), 3 (1), 4 (2)	2674	3306744	05:14:56	HITAC 8450
37	-5	2	12	11	4	6	1	0					NONE	6930	00:00:20	OKITAC 50
					3	5	2	1	4,7,11	1,2,3,9,10	5 (0), 8 (2)	6 (0)	6	748440	00:06:37	HITAC 8450
					2	4	3	2	6,8	2,3,5,7	9 (0), 10 (2), 11 (2) 8 (1), 9 (0), 10 (2), 11 (2)	1 (2), 4 (0)	680	16839900	08:34:00	OKITAC 50
					1	3	4	3	6	2,3,7	1 (2), 2 (2), 3 (0), 4 (2), 10 (1)	1 (1), 4 (2), 5 (1)	9690	101039400	03:40:19	OKITAC 50
					0	2	5	4	$\emptyset$	8,11		5 (0), 6 (1), 7 (2), 9 (0)	11928	136403190	16:55:53	HITAC 8450
															03:07:01	OKITAC 50
															37:34:57	HITAC 8450

表 2. $p(\leq 37)$ 次の特殊な Williamson 等式

p	4p	u	v	# Ω^1	# A^+	# A^-	# B^+	# B^-	A^+	A^-	$B^+(\delta_v)$	$B^-(\delta_v)$
7	28	1	-3	1	0	0	0	1	$\emptyset$	$\emptyset$	$\emptyset$	0(0)
		-5	1	*								
13	52	7	1	*								
		-5	-3	*								
19	76	1	5	3	1	1	1	0	NONE			
					0	0	2	1	$\emptyset$	$\emptyset$	0(0), 2(0)	1(0)
									$\emptyset$	$\emptyset$	0(0), 2(1)	1(0)
		7	-3	*								
31	124	-11	1	5	2	3	0	0	NONE			
					1	2	1	1	NONE			
					0	1	2	2	NONE			
		7	5	*								
37	148	-11	-3	6	2	3	0	1	NONE			
					1	2	1	2	NONE			
					0	1	2	3	NONE			
		1	-7	6	2	2	0	2	NONE			
					1	1	1	3	NONE			
					0	0	2	4	$\emptyset$	$\emptyset$	2(2), 5(0)	0(0), 1(0), 3(1), 4(1)
									$\emptyset$	$\emptyset$	1(2), 4(0)	0(0), 2(1), 3(1), 5(2)

* : $u \equiv 1 \pmod{12}$ を満たしていない。

参考文献

1. A.V. Geramita and J. Seberry, Orthogonal designs, Lecture Notes in Pure and Applied Mathematics, vol. 45, Dekker, 1979.
2. K. Sawade, Hadamard matrices of order 100 and 108, Bull. of Nagoya Institute of Technology 29 (1977), 147-153.
3. W.D. Wallis, A.P. Street and J.S. Wallis, Combinatorics: Room squares, sum-free sets, Hadamard matrices, Lecture Notes in Math., vol. 292, Springer, New York, 1972.
4. 山田美枝子, Turyn 型 Williamson 行列について, 京都大学数理解析研究所講究録, 404 (1980), 101-116.
5. K. Yamamoto, An explicit formula of the norm residue symbol in a local number field, Science Reports of Tokyo Woman's Christian College, 24-28 (1972), 302-334.