

ある特殊な Goethals-Seidel 行列について

東女大 文理 山田美枝子

1. 序.

1976年に Whiteman は次の定理を証明した。

定理1 [Whiteman, 7] p 素数で $q=2p-1$ が素数中のとき
 $4(2p+1)$ 次 Hadamard 行列が存在する。

この定理で、 $p=19$, $q=37$ とするとき 156 次の Hadamard 行列が構成できる。156 次の Hadamard 行列を最初に構成したのは Baumert と Hall [1] であるが、これら二つの Hadamard 行列が同値であるかどうかはまだわかっていない。しかし、構成法は全く異なっている。 $p=439$, $q=877$ とすると、3516 次の Hadamard 行列が求まるが、これは新しく発見された次数のようである。このようは p, q の組が無限に存在するほう、Hadamard 行列の無限系列が存在することにはなるが、どうも

そのような P, q は無限に存在するようである。

Whiteman は、ある特殊な Goethals-Seidel 行列の存在条件に合致する Supplementary difference sets を構成して定理 1 を証明した。ここでは、有限体の理論を用いてこの構成を解説する。

2. Goethals-Seidel 行列.

1970 年に Goethals と Seidel は新しい Hadamard 行列を構成した。この行列を Goethals-Seidel 行列という。すなわち、

定理 2 [Goethals-Seidel, 2] A, B, C, D は成分が $1, -1$ の n 次巡回行列, I は n 次単位行列, $A-I$ は交代行列, $R = (r_{st})$ は $r_{s, n-s+1} = 1, s = 1, \dots, n$, でその他の成分は 0 で定義される行列とする。このとき

$$A^t A + B^t B + C^t C + D^t D = 4nI,$$

が成り立つとすれば

$$H = \begin{pmatrix} A & BR & CR & DR \\ -BR & A & -{}^t DR & {}^t CR \\ -CR & {}^t DR & A & -{}^t BR \\ -DR & -{}^t CR & {}^t BR & A \end{pmatrix}$$

は $4n$ 次交代 Hadamard 行列となる。

この定理では $A-I$ を交代行列としているが、この条件がなくても Hadamard 行列となる。ただし、必ずしも交代 Hadamard 行列ではない。

3. 定理1の証明.

次の定理が重要である。

定理3 [Whiteman, 7] A, B, C, D は成分が $1, -1$ の $2n$ 次巡回行列, A の各行、各列の 1 の数は $n-1$ 個, B, C, D の各行、各列の 1 の数は n , とする。しかも

$$A^t A + B^t B + C^t C + D^t D = 4(2n+1)I - 4J, \quad (1)$$

が成り立つとすれば

$$H = \begin{pmatrix} A & BR & CR & DR & X \\ -BR & A & -{}^t DR & {}^t CR & Y \\ -CR & {}^t DR & A & -{}^t BR & Z \\ -DR & -{}^t CR & {}^t BR & A & W \\ -{}^t X & {}^t Y & {}^t Z & {}^t W & K \end{pmatrix}$$

は $4(2n+1)$ 次 Hadamard 行列である。ただし J は成分がすべて 1 の $2n$ 次正方行列, R は定理2と同じように定義された $2n$ 次正方行列, ω を成分がすべて 1 の $2n$ 次列ベクトルとすると
 $X = (\omega, \omega, \omega, \omega)$, $Y = (\omega, \omega, -\omega, -\omega)$, $Z = (\omega, -\omega, \omega, -\omega)$,

$W = (-\omega, \omega, \omega, -\omega)$, K は第1行が $(1, -1, -1, -1)$ である4次の巡回行列である。

Whiteman は、ある Supplementary difference sets を構成し、その生成行列が定理3の A, B, C, D の条件を満足することを示し、定理1を証明したのである。

我々は次のように行列 A, B, C, D を定義する。

$$A = -(I_2 + T) \otimes I_p + (I_2 - T) \otimes \sum_{r=1}^{p-1} a_{4r} T_p^r,$$

$$B = (I_2 - T) \otimes \sum_{r=0}^{p-1} b_{4r} T_p^r,$$

$$C = D = (I_2 + T) \otimes \sum_{r=1}^{p-1} \psi(r) T_p^r + (I_2 - T) \otimes I_p.$$

ここで、 p, q は定理1に同じ、 I_2, I_p は2次、 p 次の単位行列、 T, T_p は2次、 p 次の基本的巡回行列、 ξ は $GF(q^2)$ の原始根、 χ は $GF(q)$ の Legendre 指標、 S は $GF(q^2)$ から $GF(q)$ へのスワール、 $a_r = \chi(2) \cdot \chi(S\xi^{r-p})$, $b_r = \chi(2) \cdot \chi(S\xi^r)$, ψ は $\text{mod } p$ の平方剰余指標とする。

さらに、

$$Q = B + i^{-p} A,$$

$$U = C + i C,$$

と定義する。

Q を詳しく計算すると、

$$Q = (I_2 - T) \otimes \sum_{r=0}^{p-1} (b_{4r} + i^{-p} a_{4r}) T_p^r - i^{-p} (I_2 + T) \otimes I_p$$

$$= (I_2 - T) \otimes \chi(2) \sum_{r=0}^{p-1} \{ i^{4r} \chi(S\xi^{4r}) + i^{4r-p} \chi(S\xi^{4r-p}) \} T_p^r \\ - i^{-p} (I_2 + T) \otimes I_p .$$

$i^r \chi(S\xi^r)$ は r について周期 $2p$ をもつ偶函数である。そこで

$$Q = (I_2 - T) \otimes \chi(2) \sum_{r=0}^{p-1} (-1)^r \{ \chi(S\xi^{2r}) + i^p \chi(S\xi^{2r+p}) \} T_p^r \\ - i^{-p} (I_2 + T) \otimes I_p .$$

を得る。 U については

$$U = (1+i)(I_2 + T) \otimes \sum_{r=0}^{p-1} \psi(r) T_p^r + (1+i)(I_2 - T) \otimes I_p ,$$

を得る。定理3の(1)式の左辺は $QQ^* + UU^*$ で表わされることから、 QQ^* , UU^* を求めると。

$$QQ^* = (I_2 - T)^2 \otimes \sum_{r=0}^{p-1} (b_{4r} + i^{-p} a_{4r}) T_p^r \cdot \sum_{r=0}^{p-1} (b_{4r} - i^{-p} a_{4r}) T_p^{p-r} \\ - i^{-2p} (I_2 + T)^2 \otimes I_p \\ = 2(I_2 - T) \otimes \sum_{k=0}^{p-1} \left\{ \sum_{r=0}^{p-1} (b_{4k} b_{4k+4r} + a_{4k} a_{4k+4r}) \right\} T_p^{p-r} \\ + 2(I_2 + T) \otimes I_p .$$

ここで、 a_r, b_r について次の直交関係がある。

$$b_r = a_{r+p}, \quad \sum_{k=0}^{2p-1} b_{4k} b_{4k+4r} = \begin{cases} 2 & (r=0), \\ 0 & (r \neq 0). \end{cases}$$

従って

$$QQ^* = 2(I_2 - T) \otimes \left(\sum_{r=0}^{p-1} b_{4r}^2 I_p + \sum_{r=0}^{p-1} a_{4r}^2 I_p \right) + 2(I_2 + T) \otimes I_p \\ = 2(2p-1)(I_2 - T) \otimes I_p + 2(I_2 + T) \otimes I_p ,$$

を得る。

$$UU^* = (1+i)(1-i)(I_2 - T)^2 \otimes \sum_{r=1}^{p-1} \psi(r) T_p^r \cdot \sum_{r=1}^{p-1} \psi(r) T_p^{p-r} \\ + (1+i)(1-i)(I_2 + T)^2 \otimes I_p$$

$$= 4(I_2 + T) \otimes \left\{ \sum_{r=1}^{p-1} \psi^2(r) I_p + \sum_{r=1}^{p-1} \left(\sum_{k=1}^{p-1} \psi(k) \cdot \psi(k+r) \right) T_p^{r-r} \right\} \\ + 4(I_2 - T) \otimes I_p.$$

Jacobstahl の和 $\sum_{k=1}^{p-1} \psi(k) \cdot \psi(k+r) = -1 \quad (r \neq 0)$ から

$$UU^* = 4(I_2 + T) \otimes (pI_p - J_p) + 4(I_2 - T) \otimes I_p$$

を得る。 J_p は成分がすべて 1 の p 次正方行列である。従って定理 3 の (1) 式

$$QQ^* + UU^* = 4(2p+1)I_{2p} - 4J_{2p},$$

が成り立つ。 I_{2p} , J_{2p} は $2p$ 次の単位行列と $2p$ 次の成分がすべて 1 の正方行列を表わす。このことから Q , U は問題の Hadamard 行列を構成する上で大きな意味をもつことがわかる。

4. Q , U の考察.

3 の Q , U は問題の Hadamard 行列と与えることがわかったが、 Q , U の整数論的な意味を考察する。

まず、 Q , U を対角化する。

$$Q \sim \tilde{Q}$$

$$= \begin{pmatrix} 2 & \\ & 0 \end{pmatrix} \otimes \begin{pmatrix} \chi(2) \sum_{r=0}^{p-1} (-1)^r \left\{ \chi(s\xi^{2r}) + i^p \chi(s\xi^{2r+p}) \right\} \\ \chi(2) \sum_{r=0}^{p-1} (-1)^r \left\{ \chi(s\xi^{2r}) + i^p \chi(s\xi^{2r+p}) \right\} \zeta_p^r \\ \vdots \\ \chi(2) \sum_{r=0}^{p-1} (-1)^r \left\{ \chi(s\xi^{2r}) + i^p \chi(s\xi^{2r+p}) \right\} \zeta_p^{r(p-1)} \end{pmatrix}$$

$$-i^{-p} \begin{pmatrix} 0 & \\ & 2 \end{pmatrix} \otimes \begin{pmatrix} 1 & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix},$$

$$U \sim \tilde{U}$$

$$= (1+i) \begin{pmatrix} 0 & \\ & 2 \end{pmatrix} \otimes \begin{pmatrix} \sum_{r=1}^{p-1} \psi(r) & & \\ & \sum_{r=1}^{p-1} \psi(r) \zeta_p^r & \\ & & \ddots \\ & & & 1 \end{pmatrix}$$

$$+ (1+i) \begin{pmatrix} 2 & \\ & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix},$$

となる。ただし ζ_p は 1 の p 乗根である。 Q, U を対角化した行列 $\tilde{Q}, \tilde{U}$ について $\tilde{Q}\tilde{Q}^*, \tilde{U}\tilde{U}^*$ をとると

(1) T の固有値 1 に対しては

$\tilde{Q}\tilde{Q}^*$ の対角成分は 4δ , $\tilde{U}\tilde{U}^*$ の対角成分は δ ,

(2) T の固有値 -1 に対しては

$\tilde{Q}\tilde{Q}^*$ の対角成分は 4 , $\hat{U}\hat{U}^*$ の対角成分は $8p$,
 とはる。しかし $\tilde{Q}\tilde{Q}^* + \hat{U}\hat{U}^*$ の対角成分は、 T の固有値 1 に対
 しては、 $4q+8$, T の固有値 -1 に対しては、 $8p+4$ とはり
 一致するのである。言い換えれば、 p, q の条件は $\tilde{Q}\tilde{Q}^* + \hat{U}\hat{U}^*$
 の対角成分が T の固有値によらず $4(2p+1)$ と一定値をとる
 よう決めてあるのである。ただし第1成分は除く。

次に、 θ を対角化した時に生じた数

$$\theta = \sum_{r=0}^{p-1} (-1)^r \left\{ \chi(S\xi^{2r}) + i^p \chi(S\xi^{2r+p}) \right\} \zeta_p^r.$$

について考える。 θ は有限体 $GF(q^2)$, $GF(q)$ の Gauss の和。

$$G_\Phi = \sum_{\alpha \in GF(q^2)} \phi(\alpha) \zeta_{p'}^{S'(\alpha)}, \quad G_\Phi^{(0)} = \sum_{\alpha \in GF(q)} \phi(\alpha) \zeta_{p'}^{S''(\alpha)},$$

の比 θ_Φ である[8]。

$$\theta = \theta_\Phi = \frac{G_\Phi}{G_\Phi^{(0)}}.$$

ただし、 ϕ は $GF(q^2)$ の指標で $GF(q)$ で Legendre 指標とはるもの、
 p' は $GF(q^2)$, $GF(q)$ の標数、 S', S'' は $GF(q^2)$, $GF(q)$ からの
 絶対スプールである。

U を対角化した時に生ずる

$$\gamma = \sum_{r=1}^{p-1} \psi(r) \zeta_p^r,$$

は $GF(p)$ の Gauss の和である。

以上から、 $GF(p)$, $GF(q)$, $GF(q^2)$ の Gauss の和、および Gauss
 の和の比が定理1の Hadamard 行列の生成に大きな役割を果たし

ていることがわかる。Gauss の和の比 θ は $q^2-1/q-1$ の位数の巡回群上に定義された ± 1 をとる函数に対する指標和であり、Gauss の和 η は、位数 p の巡回群上で定義された ± 1 をとる函数に対する指標和である。従って定理 1 の構成は有限体の理論ですべて統制できる。

参考文献

1. L. D. BAUMERT, M. HALL, JR., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* **71** (1965), 169-170.
2. J. M. GOETHALS, J. J. SEIDEL, A skew Hadamard matrix of order 36, *J. Austral. Math. Soc.* **11** (1970), 343-344.
3. S. LANG. *Cyclotomic Fields*, Springer, New York, 1978.
4. 沢出和江, ある特殊な T -行列について, 京都大学数理解析研究所講究録, 本号.
5. 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.
6. A. L. WHITEMAN, An infinite family of Hadamard matrices of Williamson type, *J. Combinatorial Theory Ser. A* **14** (1973), 334-340.
7. A. L. WHITEMAN, Hadamard matrices of order $4(2p+1)$.

J. Number Theory **8** (1976), 1-11.

8. 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.