数理解析研究所講究録 第2086巻 2018年 105-110

On the Smith normal form of a skew-symmetric D-optimal design of order $n \equiv 2 \pmod 4$

愛知教育大　須田庄 (Sho Suda)
Aichi University of Education

1　はじめに

位数が n の正方行列で成分を $1, -1$ とする行列のうち、最大の行列式を持つ行列を D-optimal design と呼ぶ。本講究録では $n \equiv 2 \pmod 4$ のとき、歪対称となる D-optimal design の Smith nomrla form を決定する。 本研究は Gary Greaves 氏 (Nanyang Technological University) との共同研究である。省略された証明については [7] を参照されたい。

M を階数が r の $n \times n$ の整数行列とする。このとき、ある $n \times n$ ユニモジュラー行列 P, Q が存在し、

$$PMQ = \mathrm{diag}[m_1, m_2, \ldots, m_r, m_{r+1}, \ldots, m_n]$$

となる。ただし、対角成分 $m_1, \ldots, m_n$ は非負整数であり、$m_i | m_{i+1}$ $(1 \leq i \leq n-1)$ かつ $m_{r+1} = 0$ を満たす。このような対角行列は一意的に定まる。この対角行列を M の Smith normal form といい、その対角成分を M の invariant factors という。invariant factors に関する次の補題は基本的である。

Lemma 1.1 (Corollary 1.20 of [13]). *M を階数が r の $n \times n$ の整数行列とし、M の invariant factors を $m_1, \ldots, m_n$ としたとき、$m_i = d_i(M)/d_{i-1}(M)$ $(i = 1, \ldots, r)$ が成り立つ。* ここで、$d_i(M)$ は M のすべての $i \times i$ 小行列式の最大公約数を表し、$d_0(M) = 1$ とする。

2　D-optimal designs

位数が n の正方行列で成分を $1, -1$ とする M の行列式に対して次の不等式が知られている [9]：

$$|\det(M)| \leqslant n^{n/2}. \tag{2.1}$$

(2.1) において等号成立することと、$MM^\top = nI$ が成り立つことが同値である。このような行列 M をアダマール行列という。アダマール行列が存在するとき、位数は $1, 2$ もしくは 4 の倍数でなければならないことは容易にわかる。

4 の倍数でない位数 n に対して、不等式 (2.1) は [5, 15] において改善されている。本講究録では $n \equiv 2 \pmod 4$ の場合に焦点を当てる。$n \equiv 2 \pmod 4$ となる n に対して、

$$|\det(X)| \leqslant 2(n-1)(n-2)^{(n-2)/2} \tag{2.2}$$

が成り立つ。(2.2) において等号成立することと、次の行列等式を満たす位数 n の正方行列 B が存在することが同値である:

$$BB^\top = B^\top B = \begin{pmatrix} (n-2)I + 2J & O_{n/2} \\ O_{n/2} & (n-2)I + 2J \end{pmatrix}. \tag{2.3}$$

(2.3) を満たす位数 n の正方行列 B を EW 行列と呼ぶ。ただし、J は成分がすべて 1 の正方行列を表す。

用語の乱用であるが、成分が $1, -1$ である位数が n の正方行列 M が歪対称（skew-symmetric）であるとは、$M + M^\top = 2I$ が成り立つことと定義する。この条件は、$M - I$ が通常の意味で歪対称であることと同値である。

一般にアダマール行列の Smith normal form は位数により一意的に決まらないが、歪対称の条件を課すと一意的に決まることが知られている。

Theorem 2.1 ([12, 8])**.** 位数が $4t$ の歪対称アダマール行列の *Smith normal form* は次の通り一意的に決まる*:*

$$\mathrm{diag}[1, \underbrace{2, \ldots, 2}_{2t-1}, \underbrace{2t, \ldots, 2t}_{2t-1}, 4t].$$

一般に EW 行列の Smith normal form も位数から一意的に決まらない [11]。歪対称 EW 行列の Smith normal form は Armario により、部分的に決定されていた [4]。さらに歪対称 EW 行列の Smith normal form は位数により明示的に決まるであろうという予想がされていた。本講究録では、Armario の予想を肯定的に解決したことを報告する。主結果は以下の通りである。

Theorem 2.2. 位数が $4t+2$ の歪対称 *EW* 行列の *Smith normal form* は次の通り一意的に決まる*:*

$$\mathrm{diag}[1, \underbrace{2, \ldots, 2}_{2t+1}, \underbrace{2t, \ldots, 2t}_{2t-1}, 2t(4t+1)].$$

3 Theorem 2.2の証明の方針

位数が $4t+2$ の $\{1,-1\}$-行列 S を歪対称 EW 行列とし、その invariant factors を $s_1, s_2, \ldots, s_{4t+2}$ とする。S は $\{1,-1\}$-行列であるので、Lemma 1.1 により $s_1 = 1$ が従う。s_{2t+2}, s_{4t+2} が決定できれば残りの invariant factors は決定されるという次の補題は、初等整数論的な議論で証明される。

Lemma 3.1. 位数が $4t+2$ の $\{1,-1\}$-行列 S を歪対称 *EW* 行列とし、その *invariant factors* を $s_1, s_2, \ldots, s_{4t+2}$ とする。$s_{2t+2} = 2$, $s_{4t+2} = 2t(4t+1)$ が成り立つと仮定する。このとき、$s_2 = \cdots = s_{2t-1} = 2$, $s_{2t+3} = \cdots = s_{4t+1} = 2t$ が成り立つ。

以下では、$s_{2t+2} = 2$ と $s_{4t+1} = 2t$ を示す方針について述べる。

3.1 $s_{2t+2} = 2$

S を位数が $4t+2$ の歪対称 EW 行列とする。このとき、EW トーナメント行列と呼ばれるある有向グラフの隣接行列 A が以下の通り対応する [2, 6]:

$$S = \begin{pmatrix} 1 & \mathbf{1}^\top \\ -\mathbf{1} & I + A - A^\top \end{pmatrix}. \tag{3.1}$$

このとき、$A+I$ と S の invariant factors には以下の関係がある。

Lemma 3.2. [4, Lemma 2,2, Corollary 2.3] S を位数が $4t+2$ の歪対称 *EW* 行列、A を (3.1) により S から得られる *EW* トーナメント行列とする。$s_1, \ldots, s_{4t+2}$ を S の *invariant factors*、$b_1, \ldots, b_{4t+1}$ を $A+I$ の *invariant factors* とする。このとき、次が成り立つ。

(1) $s_{i+1} = 2b_i$, $i = 1, \ldots, 4t+1$.

(2) $\det(A+I) = t^{2t}(4t+1)$.

Lemma 3.2 により、$b_{2t+1} = 1$ を示せばよい。

以下の等式が示す通り、invariant factors と整数行列の p-rank は密接に関係している。

$$\mathrm{rank}_p(A+I) = \max\{i \mid p \text{ does not divide } b_i\}$$

$A+I$ の p-rank については、p が t を割り切るときに明示的に計算できる。証明には、EW トーナメント行列が満たす行列等式を用いる [2]。

Lemma 3.3. A を位数が $4t+1$ の *EW* トーナメント行列とし、p を t を割り切る素数とする。このとき、$\mathrm{rank}_p(A+I) = 2t+1$ が成り立つ。

($b_{2t+1}=1$ の証明). b_{2t+1} を割り切る素数 p が存在したと仮定する。 Lemma 1.1, Lemma 3.2 により $b_1\cdots b_{4t+1}=\det(A+I)=t^{2t}(4t+1)$ がわかる。このとき、以下のいずれかが成り立つ。

(1) p は t を割り切る。

(2) p は t を割り切らず、かつ p は $4t+1$ を割り切る。

(1) のとき、$p|b_{2t+1}$ より

$$\mathrm{rank}_p(A+I)=\max\{i \mid p \text{ does not divide } b_i\}\leqslant 2t.$$

となるが、これは Lemma 3.3 に反する。

(2) のとき、$i=2t+2,\dots,4t+1$ に対して p は b_i を割り切るので、p^{2t+1} は $b_1\cdots b_{4t+1}=t^{2t}(4t+1)$ を割り切る。ここで、p は t を割り切らないので、p^{2t+1} は $4t+1$ を割り切る。一方、p は奇数でなければならないので、$p\geq 3$ である。このとき $p^{2t+1}>4t+1$ となるが、これは先ほどの p^{2t+1} は $4t+1$ を割り切ることに反する。

(1), (2) のいずれの場合も矛盾が導かれたので、b_{2t+1} を割り切る素数が存在しないこと、すなわち $b_{2t+1}=1$ が示された。 □

3.2 $s_{4t+2}=2t(4t+1)$

Lemma 1.1 により、$d_{4t-1}(S)$ を決定すれば s_{4t+2} も決定できる。ここでは次の補題を用いる。位数 n の正方行列 M と行列の添え字の集合 I,J に対して、行と列をそれぞれ I,J に制限した M の部分行列を $M_{I,J}$ と記す。また、$I=\{i\},J=\{j\}$ のときは $M_{I,J}=M_{i,j}$ とし、$[n]=\{1,2,\dots,n\}$ とする。

Lemma 3.4 (Page 21 of [10]). M を正則な $n\times n$ 行列とする。このとき次が成り立つ。

$$\det(M_{[n]\setminus\{i\},[n]\setminus\{j\}})=\pm\det(M)\det((M^{-1})_{j,i}).$$

この補題により S の逆行列の成分が明示的にわかれば、S の $(4t+1)\times(4t+1)$ 小行列式が計算できる。

式 (2.3) より

$$S^{-1}=S^{\top}\left(\frac{1}{4t}I-\frac{1}{4t(4t+1)}\begin{pmatrix}J & O\\ O & J\end{pmatrix}\right). \tag{3.2}$$

となる。ここで、次の補題を用いる。

Lemma 3.5 ([14]). S を $S=\left(\begin{smallmatrix}S_{11} & S_{12}\\ S_{21} & S_{22}\end{smallmatrix}\right)$ のようにブロック分けする。ただし、各 S_{ij} は $(2t+1)\times(2t+1)$ 行列である。このとき $S_{11}J=S_{22}J=J$, $S_{12}J=-S_{21}J=\pm\sqrt{8t+1}J$ が成り立つ。

Lemma 3.5 と $\det(S) = (8t+2)(4t)^{2t}$ とより

$$\det(S)S^{-1} = 2(4t)^{2t-1}\left((4t+1)(2I-S) - \begin{pmatrix} J & \mp\sqrt{8t+1}J \\ \pm\sqrt{8t+1}J & J \end{pmatrix}\right).$$

したがって $\det(S)S^{-1}$ の成分は、符号を除いて

$$2(4t)^{2t-1} \times 4t, \quad 2(4t)^{2t-1} \times (4t+2), \quad 2(4t)^{2t-1} \times (4t+1 \pm \sqrt{8t+1}) \tag{3.3}$$

となる。ここで $\sqrt{8t+1}$ は奇数であることが [3] で示されているので、(3.3) の値の最大公約数は $4(4t)^{2t-1}$ となることが示された。したがって $d_{4t+1}(S) = 4(4t)^{2t-1}$ となる。$d_{4t+2}(S) = \det(S) = (8t+2)(4t)^{2t}$ を用いると、Lemma 1.1 より $s_{4t+2} = d_{4t+2}(S)/d_{4t+1}(S) = 2t(4t+1)$ を得る。

4 おわりに

歪対称 EW 行列の Smith normal form を決定するために、付随する EW トーナメント行列を A としたとき、$A+I$ の Smith normal form を部分的に決定することが重要であった。S の Smith normal form を決定するためには必要はないが、Greaves 氏との共同研究をさらに進めて以下の結果を得た。

Theorem 4.1. 位数が $4t+1$ の *EW* トーナメント行列の *Smith normal form* は次の通り一意的に決まる:

$$\mathrm{diag}[\underbrace{1,\ldots,1}_{2t+2},\underbrace{t,\ldots,t}_{2t-2},t^2(4t+1)].$$

歪対称な EW 行列の例は、位数が $6, 14, 26, 42, 62$ のときに知られている [1]。いずれも supplementary difference set から構成されている。最後に以下の問題を提示し本講究録を終える。

Problem 4.2. 歪対称 *EW* 行列の無限系列の例を構成せよ。

参考文献

[1] M Araya, M. Harada and S. Suda, Supplementary difference sets related to a certain class of complex spherical 2-codes, *Australas. J. Combin.*, **65** (2016), 71–83.

[2] J. A. Armario, On $(-1,1)$-matrices of skew type with the maximal determinant and tournaments, *Algebraic design theory and Hadamard matrices*, 1–11, **Springer Proc. Math. Stat.**, 133, Springer, Cham, 2015.

[3] J. A. Armario and M. D. Frau, On skew E-W matrices, *J. Combin. Des.* **24** (2016), 461–472.

[4] J. A. Armario, On the Smith normal form of skew E-W matrices, *Linear Multilinear Algebra* **65** (2017), no. 2, 375–380.

[5] H. Ehlich, Determinantenabschätzungen für binäre Matrizen, *Math. Z.* **83** (1964) 123–132.

[6] G. Greaves and S. Suda, Symmetric and skew-symmetric $\{0, \pm 1\}$-matrices with large determinants, *J. Combin. Des.* **25** (2017), 507–522.

[7] G. Greaves and S. Suda, On the Smith normal form of a skew-symmetric D-optimal design of order $n \equiv 2 \pmod 4$, submitted, arXiv:1801.07516.

[8] I. Hacioğlu and A. Keman, A shorter proof of the Smith normal form of skew-Hadamard matrices and their designs, *Hacet. J. Math. Stat.* **43** (2014), 227–230.

[9] J. Hadamard, Resolution d'une question relative aux determinants, *Bull. Sciences Mathematiques* **17** (1893) 240–246.

[10] R. A. Horn, C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1990.

[11] C. Koukouvinos, M. Mitrouli and J. Seberry, On the Smith normal form of D-optimal designs, *Linear Algebra Appl.* **247** (1996), 277–295.

[12] T. S. Michael and W. D. Wallis, Skew-Hadamard matrices and the Smith normal form, *Des. Codes Cryptogr.* **13** (1998), 173–176.

[13] C. Norman, *Finitely Generated Abelian Groups and Similarity of Matrices over a Field*, Springer-Verlag, London, 2012.

[14] H. Nozaki and S. Suda, Complex spherical codes with two inner products, *European J. Combin.* **51** (2016), 511–518.

[15] M. Wojtas, On Hadamard's inequality for the determinants of order non-divisible by 4, *Colloq. Math.* **12** (1964) 73–83.