数理解析研究所講究録 1465 巻 2006 年 65-70

Ehlich block matrices

田村宏樹 (Hiroki Tamura)
東北大学大学院情報科学研究科
Graduates School of Information Sciences, Tohoku University

1 Introduction

Ehlich ブロック行列とは次の形をした正方行列である。

$$D_n(k_1,\cdots,k_l) := (n-3)I_n - J_n + 4\begin{pmatrix} J_{k_1} & 0 & \cdots & 0 \\ 0 & J_{k_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{k_l} \end{pmatrix}$$

$$= \begin{pmatrix} n & & 3 & & & & \\ & \ddots & & & & -1 & \\ 3 & & n & & & & \\ & & & \ddots & & & \\ & & & & n & & 3 \\ & -1 & & & & \ddots & \\ & & & & 3 & & n \end{pmatrix}$$

但し、$\sum_{i=1}^{l} k_i = n$ で、I_k は k 次の単位行列、J_k は成分がすべて 1 の k 次の正方行列である。

このような行列を扱う理由は D-optimal design と深い関係にあるからである。$\mathcal{X}_n$ を成分が全て ± 1 である n 次正方行列の集合とし、その中で最大の行列式 $md(n)$ を持つものを n 次の D-optimal design と呼ぶ。n が 4 を法として 3 と合同な場合、

$$md(n)^2 \le \det D_n(k_1,\cdots,k_l) \text{ ここで、 } l = \begin{cases} 6 & 15 \le n \le 59 \\ 7 & 63 \le n \end{cases}$$

かつ全ての i, j に対し $|k_i - k_j| \le 1$

であることが、 Ehlich[2] によって示されている。

現在までこの上限を満たす行列の存在は知られていないが、存在するための n に関する必要条件として、n が 63 以上の 7 の倍数かつ $4n/7-3$ が平方数であることが、Cohn によって示された [1]。

2 Balanced case

Cohn の与えた条件下では、$k_1=k_2=\cdots=k_l$ となる。一般に、

Theorem 1. $n=kl$ として $XX^T=D_n(k,\cdots,k)$ を満たす行列 $X\in\mathcal{X}_n$ が存在するならば、

1. $4k-3$ が平方数かつ、
2. $(n-3)x^2+(-1)^{\frac{k-1}{2}}y^2=(n+4k-3)z^2$ が非自明な整数解を持たねばならない。

この定理の条件を満たす (k,l) の組は、kl が小さい方から、$(k,l)=$(3,13), (21,3), (7,13), (7,17), (3,49), (7,21), (7,25), (13,15), (73,3), (7,37), (3,109), (13,27), (7,53), (7,57), (13,31), (31,13), (7,61), (3,145), (7,73), (73,7), $\cdots$ となり、したがって Ehlich の上限を満たすためには、少なくとも kl が $73\cdot 7=511$ 以上でなければならない。

なお、このようなブロックの大きさが一定である場合は、group divisible design と深い関わりがある。

Definition 1. (P,S,A) が group divisible design GDD$(v,k,m,n,\lambda_1,\lambda_2)$ とは、

- P は点の集合で、$|P|=v=mn$
- S は P の、m 点ずつの部分集合（group）への分割
- A は P の、$k(\geq 2)$ 点部分集合（ブロック）のクラス
- 同一 group の異なる 2 点を共に含むブロックは丁度 λ_1 個
- 異なる group の 2 点を共に含むブロックは丁度 λ_2 個

$|P|=|A|$ のとき、group divisible design を square、さらに点とブロックを入れ替えても group divisible design であるとき、symmetric という。

GDD$(v,k,m,n,\lambda_1,\lambda_2)$ のインシデンス行列 B は、$BB^T=((r-\lambda_1)I_m+(\lambda_1-\lambda_2)J_m)\otimes I_n+\lambda_2 J_v$ を満たす。

もしも $t^2=4k-3$ として square GDD$(n,\frac{n-t}{2},k,l,\frac{n-2t+3}{4},\frac{n-2t-1}{4})$ が存在したとすれば、そのインシデンス行列中の 0 を -1 で置き換えることにより、$XX^T=D_n(k,\cdots,k)$ を満たす行列 $X\in\mathcal{X}_n$ が構成できる。その逆が必ず成り立つかどうかは分からないが、ある条件下では、そのような X が存在すれば group divisible design に由来していることが示される。

Theorem 2. $n = kl$ とし、 $X \in \mathcal{X}_n$ が $XX^T = D_n(k, \cdots, k)$ を満たすとする。このとき、 以下のいずれかを満たせば、 X は *symmetric* $GDD(n, \frac{n-t}{2}, k, l, \frac{n-2t+3}{4}, \frac{n-2t-1}{4})$ （但し、 $t^2 = 4k - 3$ ）に由来する。

1. $XX^T = X^T X$

2. $(n-3, 4k-3)$ が平方因子を含まない。

3 Imbalanced case

この節ではより一般的に、Ehlich ブロック行列のブロックの大きさが一定でない場合について扱う。Theorem 1 の拡張として、次が成り立つ。

Theorem 3. $n \equiv 3 \pmod 4$ とする。もしも $XX^T = D_n(k_1, \cdots, k_l)$ を満たす正方整数行列 X が存在するならば

1. $\det D_n(k_1, \cdots, k_l) = (n-3)^{n-l} \prod_{i=1}^{l} (n+4k_i-3) \cdot \left(1 - \sum_{i=1}^{l} \frac{k_i}{n+4k_i-3}\right)$
   が平方数かつ、

2. $c_p\left(\mathrm{diag}(n+4k_1-3, \cdots, n+4k_l-3) \oplus (n-3)I_{\bar{l}}\right) = 1$ *for all odd prime* p
   但し、$\bar{l}$ は $l+\bar{l}$ が 4 の倍数となる非負整数、 $c_p()$ は *Hasse-Minkowski invariant*

でなければならない。

$XX^T = D_n(k_1, \cdots, k_l)$ を満たす行列 X を構成するのに、以下は非常に有用である。

Theorem 4. $X \in \mathcal{X}_n$ が $XX^T = D_n(k_1, \cdots, k_l)$ を満たすとする。X の全ての列ベクトルを $v^{(1)}, \cdots, v^{(n)}$ とおくと、

1. $\widehat{v^{(i)}}^T Z \widehat{v^{(j)}} = \begin{cases} 3 & \mathit{if}\ i = j, \\ {v^{(i)}}^T v^{(j)} & \mathit{otherwise}, \end{cases}$ ここで $\widehat{v^{(i)}} = \begin{pmatrix} J_{1,k_1} & & 0 \\ & \ddots & \\ 0 & & J_{1,k_l} \end{pmatrix} v^{(i)}$,

$$Z = \left(\frac{4}{n+4k_i-3}\delta_{i,j} - \frac{n-3}{1 - \sum_{t=1}^{l} \frac{k_t}{n+4k_t-3}} \cdot \frac{1}{(n+4k_i-3)(n+4k_j-3)} \right)_{i,j=1,\cdots l}$$

2. $\sum_{i=1}^{n} \widehat{v^{(i)}} \widehat{v^{(i)}}^T = (W_{ij})_{i,j=1,\cdots,l}$ ここで $W_{ij} = k_i(n+4k_i-3)\delta_{i,j} - k_i k_j$

が成り立つ。したがって、$u^{(1)} = (u_1^{(1)} \cdots u_l^{(1)})^T, \cdots, u^{(\alpha)}$ を ${u^{(i)}}^T Z u^{(i)} = 3$, $u_t^{(i)} \equiv k_t \pmod 2$, $|u_t^{(i)}| \leq k_t$, $\sum_{t=1}^{l} u_t^{(i)} \equiv 3 \pmod 4$ を満たす全ての整数ベクトルとすれば、線型方程式

$$\begin{cases} \sum_{i=1}^{\alpha} c_i &= n, \\ \sum_{i=1}^{\alpha} c_i u^{(i)} {u^{(i)}}^T &= W \end{cases}$$

が $(c_1, \cdots, c_\alpha)$ に関する非負整数解を持たねばならない。

これにより、X が存在しうる $k_1, \cdots, k_l$ の値、その場合の列ベクトルの候補などが大幅に制限される。但し、$l \geq 4$ の場合には候補となりうる列ベクトルが多すぎて、特に $l \geq 5$ ではあまり有効ではない。これは Z が、$l = 4$ で半定値、$l \geq 5$ で不定値であるためと思われる。

4 Symmetric imbalanced case

そこで、行列 X の構成のために新たな制約を設ける。即ち、symmetric group divisible design と同様に $XX^T = X^T X$ を仮定する。すると次の補題より、様々な性質が導かれる。

Lemma 5. 正方行列 X が $XX^T = X^T X = Y$ を満たせば、任意の多項式 $f(x)$ に対し $Xf(Y)X^T = Yf(Y)$ が成り立つ。

Theorem 6. $n \equiv 3 \pmod 4$ とする。正方整数行列 X が $XX^T = X^T X = D_n(k_1, \cdots, k_l)$ を満たすならば、以下が成り立つ。

1. l が 4 以外ならば、$X = (X_{ij})_{i,j=1,\cdots,l}$, X_{ij} は $k_i \times k_j$ 小行列の形に分解したとき、各小行列内では行和・列和が等しくなる。

2. l が 4 以外の偶数ならば、$n - 3$ は平方数。

3. l が奇数ならば $(n-3)x^2 + (-1)^{\frac{l+1}{2}} \prod_{i=1}^{l} k_i \cdot y^2 = z^2$ は非自明な整数解を持つ。

また、この定理の 1 の系として

Cororally 7. l を 4 以外として、$X \in \mathcal{X}_n$ が $XX^T = X^T X = D_n(k_1, \cdots, k_l)$ を満たせば、任意の互いに素な k_i, k_j に対して $n + 3k_i - 3 \geq k_i k_j$ が成り立つ。

Theorem 8. $X \in \mathcal{X}_n$ が $XX^T = X^T X = D_n(k_1, \cdots, k_l)$ を満たすとする。$c(k) := \#\{i \mid k_i = k\}$ とおくと、

1. $c(k)$ が 2 以上の偶数ならば、 $n+4k-3$ は平方数。

2. $c(k)$ が奇数ならば、 $(n+4k-3)x^2+(-1)^{\frac{c(k)-1}{2}}c(k)y^2=z^2$ は非自明な整数解を持つ。

Theorem 9. $X \in \mathcal{X}_n$ が $XX^T = X^TX = D_n(k_1,\cdots,k_l)$ を満たすならば、$\det(D_n(k_1,\cdots,k_l)-x^2I_n)=g(x)g(-x)$ を満たす整多項式 $g(x)$ が存在する。

以下に $XX^T=D_n(k_1,\cdots,k_l)$ となる $X\in\mathcal{X}_n$ が存在しうる $(k_1,\cdots,k_l)$ $n\le 39$ を列挙する。

n	$k_1,\cdots,k_l$	行列式 $/2^{n-1}$	存在	対称
7	2,2,2,1	9	○	○
	3,3,1	8	○	○
	1,$\cdots$,1	8	○	○
	4,3	7	○	○
	7	5	○	○
11	5,2,2,2	320	○	○
	1,$\cdots$,1	243	○	○
15	4,4,4,3	25515	○	○
	1,$\cdots$,1	16384	○	○
19	10,3,3,3	3211264	○	○
	1,$\cdots$,1	1953125	○	○
23	1,$\cdots$,1	362797056	○	○
27	7,7,7,6	198087192576	○	○
	9,8,6,4	195910410240	○	○
	10,10,4,3	191556845568		
	11,10,3,3	189380063232		
	14,7,6	182849716224	○	○
	18,3,3,3	176319369216		
	1,$\cdots$,1	96889010407	○	○

n	$k_1,\cdots,k_l$	行列式 $/2^{n-1}$	存在	対称
31	9,9,9,4	75960984159088	○	○
	16,5,5,5	73248091867692		
	13,11,5,2	73248091867692		
	21,7,3	66465861139202	○	○
	31	52223176609373	○	○
	1,⋯,1	35184372088832	○	○
35	7,7,5,4,4,4,2,2	39582418599936000		×
	7,7,7,4,4,2,2,2	39582418599936000		×
	7,7,7,6,2,2,2,2	39582418599936000		×
	11,11,11,2	37436171902517248		
	4,4,4,4,4,1,⋯,1	34665798542819328		×
	1,⋯,1	16677181699666569	○	○

$(k_1,\cdots,k_l)=(2,2,2,1),(5,2,2,2),(4,4,4,3)$ はそれぞれ、$n=7,11,15$ の D-optimal design に相当する [4] 。また、$(k_1,\cdots,k_l)=(7,7,7,6),(9,9,9,4)$ はそれぞれ、$n=27,31$ のこれまでに知られている [3] よりも大きな行列式の値を与える。

予想としては、このような行列が存在すれば、全て symmetric であると思われるが、証明も反例もできていない。また、存在が期待される $k_1,\cdots,k_l$ の値には、l が 4 で、$k_1=k_2=k_3$ のものが多く、特に $k_1=k_2=k_3=k_4+1=(t^2+t+2)/2$ の場合、D-optimal design になるという予想がある。

参考文献

[1] J.H.E. Cohn, Almost D-optimal designs, Utilitas Math. **57** (2000), 121–128.

[2] H. Ehlich, Determinantenabschätzungen für binäre Matrizen mit $N\equiv 3 \pmod 4$, Math. Z. **84** (1964), 438–447.

[3] W. P. Orrick, B. Solomon, R. Dowdeswell, and W. D. Smith, New lower bounds for the maximal determinant problem, arXiv preprint math.CO/0304410.

[4] W. P. Orrick, The maximal {-1,1}-determinant of order 15, arXiv preprint math.CO/0401179.