数理解析研究所講究録 1440 巻 2005 年 102-106

D-optimal designs and group divisible designs

田村宏樹 (Hiroki Tamura)
東北大学大学院情報科学研究科

1 Introduction

$\mathcal{X}_n$ 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。$md(n)$ の上限は Hadamard や Ehlich[4, 5] らによって、以下のように与えられている。

$n \mod 4$	$md(n)^2$ の上限	上限を満たす行列の Gram 行列
0	n^n	nI_n
1	$(2n-1)(n-1)^{n-1}$	$(n-1)I_n + J_n$
2	$(2n-2)^2(n-2)^{n-2}$	$((n-2)I_{n/2} + 2J_{n/2}) \otimes I_2$
3	$\det D_n(l)$	$D_n(l)$
	$(l = 6$ for $15 \leq n \leq 59$, $l = 7$ for $63 \leq n)$	

但し、 I_k は k 次の単位行列、 J_k は k 次の成分がすべて 1 の正方行列、 $D_n(l)$ は対角成分が n 、対角ブロックの非対角成分が 3 、その他の成分が -1 であり、各ブロックの大きさが、 $[n/l]$ または $[n/l]+1$ となる $l \times l$ のブロック構造をもった n 次の正方行列である。特に n が l の倍数であるときは、$n = kl$ とおくと $D_n(l) = [(n-3)I_k + 4J_k] \otimes I_l - J_n$ と表される。

$n \equiv 3 \pmod 4$ の場合、現在まで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 [3] 。

2 非存在定理と group divisible design との関連

Definition 1. (P, S, A) が group divisible design $\mathrm{GDD}(v, k, m, n, \lambda_1, \lambda_2)$ 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。

Group divisible design の存在に関する Bose と Connor の定理 [1, Theorem 9] の一般化として、次が成り立つ。

Theorem 1. $n = kl$ を奇数とし、a, b, c を 0 でない整数かつ、$a, a+bk, a+bk+cn$ がいずれも正とする。このとき $XX^T = (aI_k + bJ_k) \otimes I_l + cJ_n$ を満たす n 次の正方整数行列 X が存在する必要条件は、

(1) $a + bk + cn$ が平方数かつ、

(2) $(a, (-1)^{\frac{k-1}{2}}k)_p = (a + bk, (-1)^{\frac{l-1}{2}}l)_p$ がすべての奇素数 p に対し成り立つ。

$(\cdot,\cdot)_p$ は *Hilbert* 記号を表す。

ここで、 $a = n - 3,\ b = 4,\ c = -1$ とおくと

Cororally 2. $n = kl \equiv 3 \pmod 4$ とする。 $XX^T = D_n(l)$ を満たす n 次の正方整数行列 X が存在する必要条件は、

(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つ。

Cororally 2 の条件を満たす (k, l) の組は、n 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), $\cdots$ となる。特に、

Cororally 3. $XX^T = D_n(7)$ を満たす n 次の正方整数行列 X が存在するならば、$n \geq 511$ 。

$(k, l) = (3, 13)$ については $XX^T = D_n(l)$ を満たす $\mathcal{X}_n$ の元 X が、group divisible design より得られ、その行列式 $2^{50} \cdot 3^{33}$ はこれまでに知られている $md(39)$ の下限 $2^{38} \cdot 3^{34} \cdot 1241$ [6] よりも大きい。

一般に、square GDD$(n, \frac{n-t}{2}, k, l, \frac{n-2t+b+c}{4}, \frac{n-2t+c}{4})$ （但し、$t^2 = a + bk + cn$ ）が存在すれば、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、 $XX^T = (aI_k + bJ_k) \otimes I_l + cJ_n$ を満たす X が得られる。その逆が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 4. $n = kl = a+b+c$ とし、 $X \in \mathcal{X}_n$ が $XX^T = (aI_k + bJ_k) \otimes I_l + cJ_n$ 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 *square* $GDD(n, \frac{n-t}{2}, k, l, \frac{n-2t+b+c}{4}, \frac{n-2t+c}{4})$ （但し、$t^2 = a + bk + cn$ ）に由来する。

(1) $c, b + cl \neq 0$ かつ $XX^T = X^T X$

(2) $c \neq 0$ かつ X を $k \times k$ ずつの小行列に分割したとき、各行列の中で列の総和は一定

(3) n が奇数、 $b \neq 0$ で $(a,b) = 4$ かつ (ac, t^2) が平方因子を含まない

特に、*(1)* と *(3)* においては、 GDD は *symmetric* となる。

3 Ehlich ブロック行列

この節では、 $D_n(l)$ より一般的に、各ブロックの大きさが $k_1, \cdots, k_l$ である Ehlich ブロック行列 $D_n(k_1, \cdots, k_l)$ について述べる。$XX^T = Y := D_n(k_1, \cdots, k_l)$ を満たす $\mathcal{X}_n$ の元 X が存在する必要条件は、 $\det Y$ が平方数かつ、 Y が単位行列と有理同値となることである。また、v^T を X の列ベクトル、 $\hat{v} = (\hat{v}_1 \cdots \hat{v}_l)$ を v をサイズ $k_1, \cdots, k_l$ に分割して、各小ベクトルごとの成分の総和をとったものとすると、

Lemma 5. 正則行列 A が $AA^T = B$ を満たしているとき、 v^T を A の列ベクトルとすると、 $vB^{-1}v^T = 1$ が成り立つ。

から、 $\hat{v}$ の候補 $\{u^{(1)}, \cdots, u^{(s)}\}$ が求められ、

Lemma 6. ${v^{(1)}}^T, \cdots, {v^{(n)}}^T$ を X のすべての列ベクトルとすると、

$$\sum_{i=1}^{n} \hat{v^{(i)}}^T \hat{v^{(i)}} = Z := (Z_{ij})_{i,j=1,\cdots,l}$$

ここで $Z_{ii} = k_i(n + 3k_i - 3)$, $Z_{ij} = -k_i k_j$ $(i \neq j)$。

より、 Z は ${u^{(i)}}^T u^{(i)}$ たちの非負整数係数の一次結合で表されなければならない。これらの条件から、 $XX^T = D_n(k_1, \cdots, k_l)$ となる $X \in \mathcal{X}_n$ が存在する可能性のある $(k_1, \cdots, k_l)$ を列挙すると、

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,···,1	8	○	○
	4,3	7	○	○
	7	5	○	○
11	5,2,2,2	320	○	○
	1,···,1	243	○	○

n	$k_1, \cdots, k_l$	行列式 $/2^{n-1}$	存在	対称
15	4,4,4,3	25515	○	○
	1,⋯,1	16384	○	○
19	10,3,3,3	3211264	○	○
	1,⋯,1	1953125	○	○
23	1,⋯,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,⋯,1	96889010407	○	○
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	395824185999360000		×
	7,7,7,4,4,2,2,2	395824185999360000		×
	7,7,7,6,2,2,2,2	395824185999360000		×
	11,11,11,2	374361719025172480		
	4,4,4,4,4,1,⋯,1	346657985428193280		×
	1,⋯,1	166771816996665690	○	○

表中の「対称」は、$XX^T = X^TX$ なる X が存在するか否かを表す。$(k_1, \cdots, k_l) = (1, \cdots, 1)$ については $n+1$ 次の Hadamard 行列の存在と同値である。$(k_1, \cdots, k_l) = (2,2,2,1), (5,2,2,2), (4,4,4,3)$ はそれぞれ、$n = 7, 11, 15$ の D-optimal design に相当する [7] 。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 [6] よりも大きな行列式の値を与える。

参考文献

[1] R.C. Bose and W.S. Connor, Combinatorial properties of group divisible incomplete block designs, Ann. Math. Stat. **23** (1952), 367–383.

[2] W.S. Connor, Some relations among the blocks of symmetrical group divisible designs, Ann. Math. Stat. **23** (1952), 602–609.

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

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

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

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

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