

# t-デザインのブロック数の下界について

渡邊 悠太 (東北大学大学院情報科学研究科)

## 1 はじめに

ブロックデザインにおける主要な問題は、どんなパラメータ  $t, v, k, \lambda$  に対して  $t$ - $(v, k, \lambda)$  デザインが存在するかという存在問題であり、現在でもなお、多くのパラメータで未解決である。その存在問題に対する1つのアプローチとして、ここではブロック数に着目したい。

点の集合  $X$  とブロックの集合  $\mathcal{F}$  の組からなる  $t$ - $(v, k, \lambda)$  デザインに対して、そのブロック数  $|\mathcal{F}|$  はパラメータ  $t, v, k, \lambda$  を用いて  $\lambda \binom{v}{t} / \binom{k}{t}$  で与えられる。この公式は、 $X$  の  $t$  点部分集合とそれを含むブロックの組を2通りの方法で数えることから得られる。したがって、 $t$ -デザインのブロック数に関する不等式を見つけることは、 $t$ -デザインの存在性に関するパラメータの必要条件を見つけることに他ならない。

ブロック数に関する不等式はいくつか知られているが、ここでは以下の2つを紹介する。

**定理 1 (Fisher 型不等式).**  $(X, \mathcal{F})$  が  $t$ - $(v, k, \lambda)$  デザインならば、 $|\mathcal{F}| \geq \binom{v}{\lfloor t/2 \rfloor}$  が成り立つ。

この不等式が等号を満たすときにはある種の良い性質を持つことから、非常に重要視されており、tight な  $t$ -デザインとして研究されている。

2つ目は Delsarte によって association scheme の枠組みで証明された不等式である。 $t, v, k$  を正整数とし、 $f_j$  を Hahn 多項式と呼ばれる次のような  $j$  次多項式とする。

$$f_j(i) = \binom{v}{i} - \binom{v}{i-1} \sum_{n=0}^j \frac{(-j)_n \cdot (-i)_n \cdot (j-v-1)_n}{(k-v)_n \cdot (-k)_n \cdot n!} \quad \text{for } j = 0, 1, \dots, k.$$

ここで、 $(x)_n$  は Pochhammer 記号であり、 $(x)_0 = 1$ 、正整数  $n$  に対して  $(x)_n = \prod_{i=0}^{n-1} (x+i)$  と定められている。さらに、 $Q$  を  $(k+1)$  次正方行列とし、 $(i, j)$  成分が  $f_j(i)$  ( $0 \leq i, j \leq k$ ) で与えられるとする。ちなみに、association scheme の言葉で述べるならば  $Q$  は Johnson scheme  $J(v, k)$  の第2固有行列である。

2つ目のブロック数に関する不等式は、この  $Q$  を用いて次のように述べる事が出来る。

**定理 2 (Delsarte の線形計画限界).** 変数  $a = (a_0 \ a_1 \ \dots \ a_k) \in \mathbb{R}^{k+1}$  に対する線形計画問題

$$\begin{aligned} & \text{minimize} && a_* = (aQ)_0, \\ & \text{subject to} && \begin{cases} a_0 = 1, \\ a_i \geq 0 & 1 \leq i \leq k, \\ (aQ)_j = 0 & 1 \leq j \leq t, \\ (aQ)_j \geq 0 & t+1 \leq j \leq k. \end{cases} \end{aligned} \quad (1)$$

の最適値を  $a_*$  とする。 $(X, \mathcal{F})$  が  $t$ - $(v, k, \lambda)$  デザインならば、 $|\mathcal{F}| \geq a_*$  が成り立つ。

これは Fisher 型不等式よりも強力であるが、具体的なパラメータに対して計算機を用いて得られる下界のため、小さいパラメータでないと計算できないという欠点がある。本稿で述べる結果は、Delsarte の線形計画限界の欠点を補い、さらに Fisher 型不等式を改良したものである。

## 2 双対定理

本研究の鍵はこれから述べる双対定理と呼ばれる定理である。詳しくは [3] を参照。

**定理 3 (双対定理).**  $m \times n$  行列  $A$ ,  $m$  次列ベクトル  $\mathbf{b}, \mathbf{y}$ ,  $n$  次列ベクトル  $\mathbf{c}, \mathbf{x}$  に対して、

$$\text{Primary problem: maximize } z = \mathbf{c}'\mathbf{x}, \quad \text{subject to } A\mathbf{x} = \mathbf{b}, \mathbf{x} \geq 0.$$

$$\text{Dual problem: minimize } w = \mathbf{b}'\mathbf{y}, \quad \text{subject to } A'\mathbf{y} \geq \mathbf{c}.$$

このとき、Primary, Dual それぞれの最適解が存在するならば、最適値  $z, w$  は等しい。

この双対定理より前節で述べた線形計画問題 (1) と同じ最適値をもつ別の線形計画問題を構成することが出来る。したがって、定理 2 は次のように言い換えられる。

**定理 2' (Delsarte の線形計画限界).** 変数  $\mathbf{b} = (b_0 \ b_1 \ \dots \ b_k) \in \mathbb{R}^{k+1}$  に対する線形計画問題

$$\begin{aligned} & \text{maximize } b_0 = (bQ^T)_0, \\ & \text{subject to } \begin{cases} b_0 = 1, \\ b_j \leq 0 & 1 \leq j \leq k, \\ (bQ^T)_i \geq 0 & 1 \leq i \leq k. \end{cases} \end{aligned} \quad (2)$$

の最適値を  $b_0$  とする。  $(X, \mathcal{F})$  が  $t$ - $(v, k, \lambda)$  デザインならば、  $|\mathcal{F}| \geq b_0$  が成り立つ。

最大化問題 (2) の最適値がブロック数の下界となるため、任意の実行可能解から求められる値もまた下界となる。ただし、  $\mathbf{b} = (1 \ 0 \ \dots \ 0)$  のような実行可能解では自明な下界しか得られないため、“良い”実行可能解を構成することが出来るかが問題となる。

## 3 実行可能解

今回求めた“良い”実行可能解を述べるために記号を準備する。  $i, j, l$  を  $k$  以下の非負整数とし、  $q_{i,j}^l$  を次の式で定める。

$$f_i(x)f_j(x) \equiv \sum_{l=0}^k q_{i,j}^l f_l(x) \pmod{\prod_{n=0}^k (x-n)}.$$

ここで  $f_i$  は、前述の Hahn 多項式である。また、association scheme の言葉で述べるならば、  $q_{i,j}^l$  は Johnson scheme  $J(v, k)$  の Krein パラメータである。

$m$  を  $t$  以下の正整数とし、  $\mathbf{b} = (b_0 \ b_1 \ \dots \ b_k)$  を次のように定める。

$$b_j = \frac{1}{\mu_c^e} \sum_{l_1=0}^e \sum_{l_2=0}^e q_{l_1, l_2}^j + \frac{\delta_{j,m}}{\mu_c^e} \min \left\{ \frac{(\sum_{l=0}^e Q_{i,l})^2}{|Q_{i,m}|} \mid \begin{array}{l} 1 \leq i \leq k \\ Q_{i,m} < 0 \end{array} \right\} \quad \text{for } j = 0, 1, \dots, k.$$

ここで、  $e = \lfloor t/2 \rfloor$ ,  $\mu_c^e = \sum_{j=0}^e Q_{0,j}$  とする。

補題 1. 上で定めた  $b$  は最大化問題 (2) の実行可能解である。

証明には Krein パラメータの性質を用いる。実行可能解  $b$  において第 1 項だけからなるベクトルもまた最大化問題 (2) の実行可能解であり、その解に対する下界が Fisher 型不等式の下界と一致する。つまり、今回構成した実行可能解  $b$  は Fisher 型不等式の下界を与える実行可能解を改良したものとなっている。なお、改良に際して単体法と呼ばれるアルゴリズムを参考にしている。

## 4 主定理とその結果

前節の補題より次の定理を得る。ここで、 $e = \lfloor t/2 \rfloor$  である。

主定理.  $(X, \mathcal{F})$  が  $t$ - $(v, k, \lambda)$  デザインならば、 $t$  以下の正整数  $m$  に対して、次が成り立つ。

$$|\mathcal{F}| \geq \binom{v}{e} + \frac{Q_{0,m}}{\binom{v}{e}} \min \left\{ \frac{(\sum_{i=0}^e Q_{i,i})^2}{|Q_{i,m}|} \mid 1 \leq i \leq k, Q_{i,m} < 0 \right\}.$$

この下界は、第 1 項が Fisher 型の下界と一致していて、第 2 項が非負なので、Fisher 型不等式よりも強いことが分かる。また、計算機を用いた具体的なパラメータに対する下界は付録の表 2 に示した通りであり、表の範囲においては、次のパラメータに関して Fisher 型不等式を改良していることが分かる。

$$(t, v, k, \lambda) = (3, 22, 7, 1), (4, 12, 6, 2), (4, 17, 7, 2), (4, 23, 8, 2), (4, 38, 10, 2), \\ (4, 42, 16, 14), (4, 47, 11, 2), (4, 57, 12, 2), (6, 39, 18, 52), (6, 53, 17, 13).$$

さらに主定理では、線形計画法に依存しない下界を導いているため、計算速度が Delsarte の下界の計算よりも速いことが期待される。実際、上記のパラメータに関して確認した結果では一部において僅かな計算速度の向上が見られた。詳しい値は次の通りである。

表 1: 主定理と Delsarte の線形計画限界の計算時間の比較

$t$	$v$	$k$	$\lambda$	主定理	Delsarte
3	22	7	1	0.005208	0.008351
4	12	6	2	0.005716	0.003425
4	17	7	2	0.006833	0.005392
4	23	8	2	0.008737	0.005905
4	38	10	2	0.010823	0.009554
4	42	16	14	0.020263	0.029603
4	47	11	2	0.014043	0.013908
4	57	12	2	0.013319	0.013898
6	39	18	52	0.039330	0.054807
6	53	17	13	0.034076	0.037184

しかしながら、ある程度大きいパラメータに対して計算時間を比較すると十分差が開いていることが分かる。次の図は  $t = 4, v = 1000$  における計算機実験の結果である。

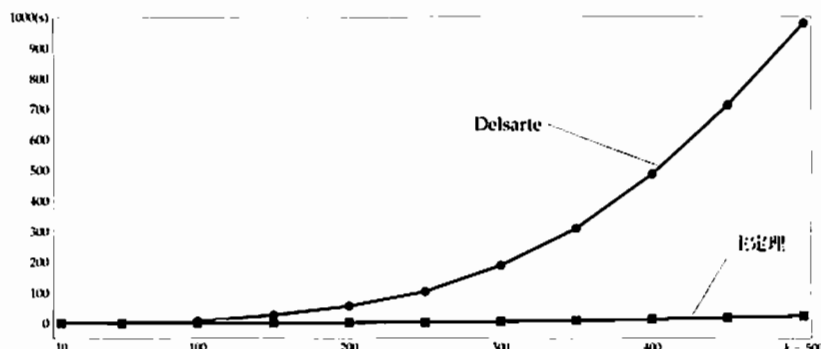


図 1:  $4-(1000, k, \lambda)$  デザインにおける主定理と Delsarte の線形計画限界の計算時間の比較

本稿に記載された数値は全て Mathematica 9.0 for Mac OS X x86 (64-bit)<sup>1</sup> を用いた計算機実験に依るものである。

## 5 主定理の系

主定理において、 $m$  の選び方には自由度がある。ここでは、その  $m$  やパラメータに制限を加えることで、主定理を簡潔に書き換えた結果を述べる。

系.  $e = \lfloor t/2 \rfloor$ , 方程式  $\sum_{i=0}^e f_i(x) = 0$  の解の最大値を  $\alpha_e$  とする.  $(X, \mathcal{F})$  が  $t-(v, k, \lambda)$  デザインならば,

1.  $v \geq k^2$  のとき,

$$|\mathcal{F}| \geq \binom{v}{e} + \frac{v-k}{\binom{v}{e}k} \left( \sum_{i=0}^e Q_{k,i} \right)^2.$$

2.  $v < k^2$  かつ  $e = 1, 2$  のとき,

$$|\mathcal{F}| \geq \binom{v}{e} + \frac{v-1}{\binom{v}{e}} \min \left\{ \frac{1}{|Q_{i,1}|} \left( \sum_{j=0}^e Q_{i,j} \right)^2 \mid \begin{array}{l} i = \lfloor \alpha_e \rfloor, \lfloor \alpha_e \rfloor \\ i > \frac{k(v-k)}{v} \end{array} \right\}.$$

3.  $t = 2, 3$  とする.

$$|\mathcal{F}| \geq v + \frac{v-3}{2} \min \left\{ \frac{(1+Q_{i,1})^2}{|Q_{i,2}|} \mid \begin{array}{l} i = \lfloor \alpha_1 \rfloor, \lfloor \alpha_1 \rfloor \\ i < \alpha' \end{array} \right\}.$$

ただし、 $\alpha'$  は  $f_2(x) = 0$  の解の最大値。

$v \geq k^2$  の場合は下界が Fisher 型よりも真に大きくなっているため、tight な  $t$ -デザインが存在しないことの証明になっている。

<sup>1</sup>CPU は Mac OS X 10.9 (1.6 GHz Intel Core i5) を使用。

## 6 今後の課題

今回の証明方法では, どんなに“良い”実行可能解を構成しても, Delsarte の線形計画限界より強い下界を作ることは出来ない. そのため今後は Terwilliger 代数などを用いて Delsarte 理論を拡張することが必要となる.

最近, Schrijver [4] が符号理論に限定して結果を出しているが, Delsarte 理論のように, 符号とデザインを統一的に扱える議論を構築したいと考えている. また, Delsarte 理論の拡張は, 他分野を含む研究の更なる発展につながると確信している.

## 謝辞

本研究を進めるにあたりご指導ご鞭撻を頂きました本学原田昌晃教授に心から感謝いたします. また, 本シンポジウムで発表の機会を与えていただいた世話人の先生方にお礼申し上げます.

## 参考文献

- [1] A. E. Brouwer and W. H. Haemers, *Association schemes*, Handbook of Combinatorics, Elsevier, Amsterdam, (1995), 747–771.
- [2] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. No. 10 (1973).
- [3] 今野 浩, *線形計画法*, 日科技連出版社, (1987).
- [4] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. Inform. Theory (2005), 2859–2866.

## A 付録

表 2: 主定理から非存在が分かるパラメータ ( $2 \leq t \leq 6, v \leq 70$ )

$t$	$v$	$k$	$\lambda$	$ \mathcal{F} $	Fisher	主定理	Delsarte
2	16	6	1	8	16	16	16
2	21	6	1	14	21	26	28
2	25	10	3	20	25	28	28
2	34	12	2	17	34	34	34
2	36	15	4	24	36	36	36
2	45	12	2	30	45	45	45
2	46	10	1	23	46	46	46
2	49	21	5	28	49	52	52
2	52	18	3	26	52	52	52
2	55	10	1	33	55	60	66
2	55	22	7	45	55	59	60
2	57	21	5	38	57	62	62
2	64	28	9	48	64	64	64
2	66	26	5	33	66	66	66
2	69	18	3	46	69	76	77
2	70	24	4	35	70	70	70
3	22	7	1	44	22	64	88
3	56	11	1	168	56	237	336
4	12	6	2	66	66	74	110
4	17	7	2	136	136	154	204
4	23	8	2	253	253	293	355
4	23	11	6	161	253	260	337
4	38	10	2	703	703	766	904
4	42	16	14	861	861	902	1062
4	47	11	2	1081	1081	1153	1352
4	47	23	35	705	1081	1109	1217
4	57	12	2	1596	1596	1679	1951
4	57	21	19	1254	1596	1629	1840
4	58	22	19	1102	1653	1663	1764
6	19	9	2	646	969	975	3553
6	39	18	52	9139	9139	9190	11001
6	49	24	133	13818	18424	19098	23602
6	53	17	13	24115	23426	24631	31832
6	59	29	260	24662	32509	32566	36905