

' t -designs' in $H(d, q)$

大阪教育大学・教養・数理科学

鈴木 寛 (Hiroshi SUZUKI)

以下において, ' t -designs' を少し拡張した形で定義し, その ' t -designs' について, Fisher 型の不等式を証明し, 不等式において, 等号をみたす例の構成等をのべる。

Fisher 型の不等式は, t -design における Ray-Chaudhuri - Wilson の不等式の拡張, 及び, orthogonal array of strength t の拡張になっている。

t -designs の概念の拡張については, Delsarte が, $\mathcal{Q}$ -polynomial association scheme 上での t -design, regular semilattice 上での t -design を定義し, 美しい理論を展開しているが, 以下でのべる semilattice $H(d, q) = L = L_d$ における t -design の定義される空間 $L_k(d, q)$ で, regular semilattice となるのは, $L_k(d, 1)$ 又は, $L_d(d, q)$ のみであり, Delsarte theory は適用できない。

1° 't - designs'

定義 1. d, g : 自然数. D : d -点集合 Q : g -点集合としたとき. semilattice $H(d, g) = (L, \leq)$ は次をみたすものである.

(1) $L = \bigcup_{J \subseteq D} Q^J$: the set of all partial mappings from D to Q .

(2) $(\alpha_1, J_1) \leq (\alpha_2, J_2) \iff J_1 \subseteq J_2$ かつ $\alpha_2|_{J_1} = \alpha_1$.

(3) $(\alpha, J) = (\alpha_1, J_1) \wedge (\alpha_2, J_2)$ とするとき.

$$J = \{j \in J_1 \cap J_2 \mid \alpha_1(j) = \alpha_2(j)\}, \quad \alpha = \alpha_1|_J$$

$(\alpha, J) \in L$ のとき $J = D(\alpha)$, $\alpha = (\alpha, J)$ であらわす.

$$X_i = \bigcup_{J \subseteq D, |J|=i} Q^J, \quad L_k = L_k(d, g) = \bigcup_{i=0}^k X_i,$$

定義 2. $0 \leq t \leq k \leq d$ とする.

(1) $Y \subseteq X_k$ が $[t]$ - $((d, g), k, \lambda)$ - design ($Y \neq \emptyset$)

$$\iff \lambda_t(\alpha) = |\{y \in Y \mid \alpha \leq y\}| = \lambda \quad \alpha \in X_t \text{ に依存せず一定}$$

(2) $Y \subseteq L$ が $\{t\}$ - $((d, g), \lambda, \dots, \lambda_t)$ - design ($Y \neq \emptyset$)

$$\iff \lambda_i(\alpha) = |\{y \in Y \mid \alpha \leq y\}| = \lambda_i \quad \alpha \in X_i \text{ に依存せず一定}$$

但し $i = 1, 2, \dots, t$.

$[t]$ - $((d, 1), k, \lambda)$ - design は 通常の t - (d, k, λ) - design ($S_\lambda(d, k, t)$ generalized Steiner system) のことであり.

$[t]$ - $((d, g), d, \lambda)$ - design は orthogonal array of strength t

index λ である。 $\{t\} - ((d, 1), \lambda_1, \dots, \lambda_t)$ design は t -design with multiple block sizes. である。

Orthogonal array of strength t についても数多くの研究がなされているが、以下によく知られた事を二点記す。

- C を $[d, r, t+1]$ linear code / $GF(q)$ とする。 d は code の長さ、 $r = \dim C$ 、 $t+1$ は minimal nonzero distance をあらわすものとする。すると $C^\perp$ は orthogonal array of strength t with index q^{d-r} (すなわち $\{t\} - ((d, q), d, q^{d-r})$ design) である。

- C を $(d, M, t+1)$ code / $\mathbb{Q}$ とする。 d は code の長さ、 $M = |C|$ 、 $t+1$ は minimal nonzero distance。 $\mathbb{Q}$ は q 点集合とする。この時 Singleton bound とよばれる簡単な不等式 $M \leq q^{d-t}$ が成立する。ここで等号が成り立つとき、MDS-code (maximum distance separable code) と呼ぶが、これは Orthogonal array of strength $d-t$ with index 1 (すなわち $[d-t] - ((d, q), d, 1)$ design) である。

以下に用語及び記号を定義する。

- $\alpha, \beta \in L$ が disjoint $\iff D(\alpha) \cap D(\beta) = \emptyset$
- $\alpha, \beta \in L$ が consistent $\iff \alpha \wedge \beta \in X_{|D(\alpha) \cap D(\beta)|}$
- A, B を集合とするとき $\text{Mat}(A, B)$ で A, B を行、列の

ラベル集合とする。実行列全体をあらわすものとする。

$$W_{ij} \in \text{Mat}(X_i, X_j) \quad W_{ij}[\alpha, \beta] = \begin{cases} 1 & \alpha \leq \beta \\ 0 & \text{otherwise.} \end{cases}$$

$$W_{ij}^u \in \text{Mat}(X_i, X_j) \quad W_{ij}^u[\alpha, \beta] = \begin{cases} 1 & \alpha \wedge \beta \in X_u, \alpha, \beta \text{ consist.} \\ 0 & \text{otherwise} \end{cases}$$

$$Y \subseteq L \quad N_i \in \text{Mat}(X_i, Y) \quad N_i[\alpha, \beta] = \begin{cases} 1 & \alpha \leq \beta \\ 0 & \text{otherwise} \end{cases}$$

$$N_i^u \in \text{Mat}(X_i, Y) \quad N_i^u[\alpha, \beta] = \begin{cases} 1 & \alpha \wedge \beta \in X_u, \alpha, \beta \text{ consist.} \\ 0 & \text{otherwise} \end{cases}$$

$$Y \subseteq X_k \quad C_{k,Y} \in \text{Mat}(X_k, Y) \quad C_Y[\alpha, \beta] = \begin{cases} 1 & \alpha = \beta \\ 0 & \text{otherwise} \end{cases}$$

特に $W_{ik} C_{k,Y} = N_i, \mathbb{1}_X, \mathbb{1}_Y$, all one vector on X_i, Y

補題 1. $0 \leq i \leq j \leq t \leq k \leq d$ とする

$$(1) \quad Y \subseteq X_k \text{ に対して, } [t] - ((d, g), k, \lambda) \text{ design} \iff N_t \mathbb{1}_Y = \lambda \mathbb{1}_t$$

$$(2) \quad W_{ij} W_{jk} = \binom{k-i}{j-i} W_{ik}$$

$$(3) \quad Y \subseteq X_k \text{ が, } [t] - ((d, g), k, \lambda) \text{-design}$$

$$\Rightarrow [i] - ((d, g), k, \lambda_i) \text{-design} \quad \text{with} \quad \lambda_i = \binom{d-i}{k-i} g^{t-i} \lambda / \binom{d-t}{k-t}$$

特に, $\{t\} - ((d, g), \lambda_1, \dots, \lambda_t) \text{ design}$ である。

証明. (1) は定義より明らか. (2) も明らか. (3) は (1) と (2) からみちみかれる.

補題 2. $Y \subseteq L$ を $\{t\} - ((d, g), \lambda_1, \dots, \lambda_t)$ design とし.

$(\alpha, \beta) \in X_i \times X_j$, $i+j \leq t$, α, β disjoint とする.

(1) $\lambda_i^j = |\{y \in Y \mid \alpha \leq y, \beta \cdot y : \text{disjoint}\}|$ は α, β のとりおちによらず一定.

(2) $\lambda_i^j + g \lambda_{i+1}^{j-1} = \lambda_i^{j-1}$, $\lambda_i^0 = \lambda_i$.

(3) $\lambda_i^j = \sum_{u=0}^j (-1)^u \binom{j}{u} g^u \lambda_{i+u}$.

(4) $\lambda_i^j = \binom{d-i-j}{k-i} g^{t-i} \lambda / \binom{d-t}{k-t}$ if $Y: [t] - ((d, g), k, \lambda)$ design

証明. (1) は (2) からの帰結. (2) は 簡単な counting argument
(2) から (3) がえられ (4) は 補題 1 の (3) と $H(d, 1)$ における λ_i^j の具体的計算からえられる.

補題 3. $Y \subseteq L$ を $\{t\} - ((d, g), \lambda_1, \dots, \lambda_t)$ design で $i+j \leq t$

$$\Rightarrow N_i(N_j^u)^T = \sum_{v=0}^{\min(i,j)} \binom{j-v}{u-v} \lambda_{i+u-v}^{j-u} W_{i,j}^v.$$

証明. $(\alpha, \beta) \in X_i \times X_j$, $\alpha \wedge \beta \in X_u$, α, β consistent とする.

$N_i(N_j^u)^T[\alpha, \beta] = |\{y \in Y \mid \alpha \leq y, \beta \wedge y \in X_u, \beta \cdot y : \text{consist.}\}|$
を数えることにより 等式がえられる.

定理 A. $Y \subseteq L$ を $\{2s\} - ((d, g), \lambda_1, \dots, \lambda_{2s})$ design とする.
 この時, $\lambda_s^s \neq 0 \Rightarrow |Y| \geq \text{rank } N_s = \binom{d}{s} g^s$.

証明. $0 \leq \lambda_s^j = \lambda_s^{j-1} - g \lambda_{s+1}^{j-1} \leq \lambda_s^{j-1}$ より $\lambda_s^i \neq 0 \quad i \leq s$.

補題 3 の式を $i = j = s$ の場合にかき下すと

$$N_s(N_s^0)^T = \lambda_s^s W_{ss}^0,$$

$$N_s(N_s^1)^T = s \lambda_{s+1}^{s-1} W_{ss}^0 + \lambda_s^{s-1} W_{ss}^1$$

$$\vdots$$

$$N_s(N_s^s)^T = \sum_{v=0}^{s-1} \binom{s-v}{u-v} \lambda_{2s-v}^0 W_{ss}^v + \lambda_s^0 W_{ss}^s, \quad W_{ss}^s = I_{|X_s| \times |X_s|}$$

よって $\text{Mat}(Y, X_s)$ の元 M で $I_{|X_s| \times |X_s|} = N_s M$ となるものが存在する. $|X_s| = \binom{d}{s} g^s$ であるから, 定理の主張がえられる.

系 (永尾 厚見) Y を $[2s] - ((d, g), k, \lambda)$ design とする.
 この時, $k+s \leq d \Rightarrow |Y| \geq \binom{d}{s} g^s$.

証明. 補題 1 (3) 及び 補題 2 (4) より 明らか.

系において $g=1$ の時は, Ray-Chaudhuri-Wilson の不等式そのままである. 定理 A は $\lambda_s^s \neq 0$ の条件のもとで $g=1$ の場合, multiple block sizes の t -design に関する Fisher 型の不等式がえられる. 但し orthogonal array の時は, $k=d$ であるから この系からは何も得られない.

補題4. Y は $[t]-(d, q, k, \lambda)$ -design とする. $i, j \leq k$

かつ $i+j \leq t$ であれば

$$N_i N_j^T = \sum_{u=0}^{\min(i,j)} \lambda_{i+j-u} W_{ij}^u = \frac{\lambda}{\binom{d-t}{k-t} q^{k-t}} W_{ik} W_{jk}^T$$

証明. $(\alpha, \beta) \in X_i \times X_j$, $\alpha, \beta \in X_u$, α, β consistent について $N_i N_j^T [\alpha, \beta]$ を計算すれば最初の等式が得られ 補題1 (3) と X_k 自身が $[t]-(d, q, k, \binom{d-t}{k-t} q^{k-t})$ design であることから 二番目の等式がえられる.

これは Y が $[t]$ -design の時 N_i が W_{ik} のごとくになるまうことを示す. 良く知られてはいるが, 重要な補題と思われる.

定理B. (1) $0 \leq s \leq k \leq d$ とすると

$$\text{rank } W_{sk} \geq \sum_{i=0}^{s+k-d-1} \binom{d-i}{k-i} \binom{d}{i} (q-1)^i + \sum_{i=s+k-d}^s \binom{d-i}{s-i} \binom{d}{i} (q-1)^i$$

(2) Y は $[2s]-(d, q, k, \lambda)$ design とすれば:

$$|Y| \geq \sum_{i=0}^{s+k-d-1} \binom{d-i}{k-i} \binom{d}{i} (q-1)^i + \sum_{i=s+k-d}^s \binom{d-i}{s-i} \binom{d}{i} (q-1)^i$$

証明. (2) $|Y| \geq \text{rank } N_{2s} \stackrel{\textcircled{1}}{\geq} \text{rank } N_s \stackrel{\textcircled{2}}{=} \text{rank } (N_s^T N_s) \stackrel{\textcircled{3}}{=} \text{rank } (N_s N_s^T)$

$$\stackrel{\textcircled{4}}{=} \text{rank} \left(\frac{\lambda}{\binom{d-t}{k-t} q^{k-t}} W_{sk} W_{sk}^T \right) = \text{rank} (W_{sk} W_{sk}^T) \stackrel{\textcircled{3}}{=} \text{rank} (W_{sk}^T W_{sk}) \stackrel{\textcircled{2}}{=} \text{rank } W_{sk}$$

- ① は補題 1 (2) ② は N_s が実行列であることより成立し。
 ③ は任意の行列について成立 ④ は補題 4. 従って, (2) は
 (1) より得られる.

(1). $A = W_{sk}$ とし. $x_0 \in X_d$ とする. さらに

$$X_{ji} = \{ \alpha \in X_j \mid \alpha \wedge x_0 \in X_{j-i} \}$$

$$X_{ji}^\mu = \{ \alpha \in X_{ji} \mid \alpha \succ \mu \}, \quad \mu \in X_{ii} \quad \text{とする}$$

A_{ij} を A の $X_{si} \times X_{rj}$ 上への制限. $A_i^{\mu\nu}$ を A の
 $X_{si}^\mu \times X_{ri}^\nu$ への制限とすると $A_{ij} = 0 \quad (i > j)$. かつ
 $A_i^{\mu\nu} = 0 \quad (\mu \neq \nu)$. 従って

$$\text{rank } A \geq \sum_{i=0}^s \text{rank } A_{ii} \geq \sum_{i=0}^s \sum_{\mu \in X_{ii}} \text{rank } A_i^{\mu\mu}$$

ところが, $A_i^{\mu\mu}$ は $H(d-i, 1)$ における $W_{s-i, k-i}$ と同
 じであるので, (1) は 次の補題から得られる.

補題 5. $0 \leq s \leq k \leq d$ とすると $H(d, 1)$ において

$$(1) \quad \text{rank } W_{sk} = \binom{d}{s}, \quad \text{if } s+k \leq d.$$

$$(2) \quad \text{rank } W_{sk} = \binom{d}{k}, \quad \text{if } s+k \geq d.$$

証明. (1) はよく知られている. (2) は (1) から得られる.

定理 B (1) において $s+k \leq d$ 又は $k=d$ のときは $=$ を
 示せるが, 一般の場合は不明. (2) において, $s+k \leq d$ の時

は、系がえられる。 $k=d$ の時は

$$|Y| \geq \sum_{i=0}^s \binom{d}{i} (q-1)^i$$

となり、これは Rao の不等式といわれるものである。 Θ が $GF(q)$ で、 Y が subspace のときは $|Y||Y^\perp| = q^d$ より

$$q^d \geq \left(\sum_{i=0}^s \binom{d}{i} (q-1)^i \right) |Y^\perp|$$

となり、 $Y^\perp$ が $[d, \log_q |Y^\perp|, 2s+1]$ code であることより Hamming bound に他ならない。

2° 例.

$x_0 \in X_d$ $\Delta = \Delta_{q, x_0} : H(d, q) \rightarrow H(d, q-1)$ を次のように定義する。 $D(\Delta\alpha) = \{s \in D(\alpha) \mid \alpha(s) \neq x_0(s)\}$, $\Delta\alpha = \alpha|_{D(\Delta\alpha)}$.

A) $Y \subset X_d$, $\bar{Y} \subset L_{q-1} = H(d, q-1)$, $\Delta(Y) = \bar{Y}$, $\Delta^{-1}(\bar{Y}) \cap X_d = Y$ とすると次が成り立つ

$$Y : [t]-(d, q), d, \lambda) \text{ design} \iff \bar{Y} : [t]-(d, q), \bar{\lambda}_1, \dots, \bar{\lambda}_t) \text{ design}$$

$$\bar{\lambda}_i = q^{-i} |Y|$$

B) $Y_1 : [t]-(d, 1), k, \lambda_1) \text{ design}$, $\{Y_\alpha\} : [t]-(k, q), k, \lambda_2) \text{ design}$
 $\alpha \in Y_1$ とする。 K を k -点集合とし、 $f_\alpha : \alpha \mapsto K$ 全単射。 $\alpha \in Y_1$ について固定する。

$$Y_1 \times \{Y_\alpha\} \ni (\alpha, \beta) \in D(\alpha, \beta) = \alpha \quad \beta(a) = \beta(f_\alpha(a)) \quad a \in \alpha$$

とすると, $[t]-(d, q), k, \lambda, \lambda_2$ design が構成される. これは product type という. Teirlink の結果より, 任意の k と, $(d-k+1)/(k!)^{2k-1} \in \mathbb{N}$ なる任意の d について $[k-1]-(d, 1), k, (k!)^{2k-1}$ design が存在する. 又,

$$q^{t-1} < \sum_{j=0}^t \binom{k}{j} (q-1)^j \Rightarrow \exists [t]-(k, q), k, q^{k-t} \text{ design}$$

が, Gilbert Varshamov bound からえられるので, 任意の t について, $[t]-(d, q), k, \lambda$ design が存在することがわかる.

しかし, 定理において 等号が (2) において成り立つ時, tight とよぶことにすると, product type は $s \geq 1$ のとき tight にはなりえないことがすぐわかる.

(C) C を $[d, m, t+1; q]$ linear code とし, $\text{wt}(v) = k$ for $\forall v \in C^\perp \setminus \{0\}$ とする. すると $\Delta(C^\perp \setminus \{0\})$ は $[t]-(d, q-1), k, \lambda$ design になる.

従って, $[q+1, q-1, 3; q]$ Hamming code から,

$[2]-(q+1, q-1, q, 1)$ design がつくれ. これは tight である. この他にも, $[2]-(7, 2), 4, 1$ design も構成できる.

Question tight $[2]-(d, 2), k, \lambda$ design が Weighing matrix かどうか.

参考文献: 't-designs' in $H(d, q)$. preprint.