数理解析研究所講究録
671巻 1988年 139-148

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

(1) $L = \bigcup_{J \subset D} Q^J$: 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.

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

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

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

定義2. $0 \leq t \leq k \leq d$ とする。

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

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

(2) $Y \subseteq L$ が $\{t\}$-$((d,q), \lambda_1, \cdots, \lambda_t)$-design. $(Y \neq \phi)$

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

但し. $i = 1, 2, \cdots, t$.

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

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

index λ である。 $\{t\}$-$((d,1), \lambda_1, \cdots, \lambda_t)$ 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 / Q とする。d は code の長さ、$M = |C|$、$t+1$ は minimal nonzero distance、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 $\Longleftrightarrow$ $D(\alpha) \cap D(\beta) = \phi$

・ $\alpha, \beta \in L$ が consistent $\Longleftrightarrow$ $\alpha \wedge \beta \in X_{|D(\alpha) \cap D(\beta)|}$

・ A, B を集合とするとき Mat(A, B) で、A, B を行列の

ラベル集合とする。奥行列全体をあらわすものとする。

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

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

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

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

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

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

補題 1 $\quad 0 \le i \le j \le t \le k \le d$ とする

(1) $Y \subseteq X_k$ に於て、$[t]\text{-}((d,q),k,\lambda)$ design $\Longleftrightarrow$ $N_t \mathbb{1}_Y = \lambda \mathbb{1}_t$

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

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

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

特に、$\{t\}\text{-}((d,q),\lambda_1,\cdots,\lambda_t)$ 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) からみちびかれる.

補題 2. $Y \subseteq L$ を $\{t\}$-$((d, q), \lambda_1, \cdots, \lambda_t)$ design とし. $(\alpha, \beta) \in X_i \times X_j$, $i+j \leq t$, α, β disjoint とする.

(1) $\lambda_i^j = |\{y \in Y \mid \alpha \leq y,\ \beta . y : \text{disjoint}\}|$ は上の α, β のとり方によらず一定.

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

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

(4) $\lambda_i^j = \binom{d-i-j}{k-i} q^{t-i} \lambda \Big/ \binom{d-t}{k-t}$ if Y: $[t]$-$((d, q), k, \lambda)$ 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 $\{t\}$-$((d, q), \lambda_1, \cdots, \lambda_t)$ design で $i+j \leq t$

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

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

$N_i (N_j^u)^T [\alpha, \beta] = |\{y \in Y \mid \alpha \leq y,\ \beta \wedge y \in X_u\ \ \beta . y : \text{consist.}\}|$

を数えることにより等式がえられる。

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

証明. $0 \leqq \lambda_s^j = \lambda_s^{j-1} - q\lambda_{s+1}^{j-1} \leqq \lambda_s^{j-1}$ より $\lambda_s^i \neq 0$ iss.
補題3の式を $i=j=s$ の場合に書き下すと.

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

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

$$\vdots$$

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

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

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

証明. 補題1(3) 及び 補題2(4) より 明らか.

系において $q=1$ 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. $q=1$ 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 を $[t]-((d,q),k,\lambda)$-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. $(\alpha,\beta) \in X_i \times X_j$ $\alpha \wedge \beta \in X_u$, 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} のごとくにふるまうことを示す. 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

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

(2) Y を $[2s]-((d,q),k,\lambda)$ 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) $|Y| \geq \operatorname{rank} N_{2s} \overset{①}{\geq} \operatorname{rank} N_s \overset{②}{=} \operatorname{rank}(N_s^T N_s) \overset{③}{=} \operatorname{rank}(N_s N_s^T)$

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

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.

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

$$X_{ji}^{\mu} = \{\alpha \in X_{ji} \mid \alpha \geqq \mu\} \qquad \mu \in X_{ii} \qquad \text{とする.}$$

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

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

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) $\operatorname{rank} W_{sk} = \binom{d}{s}$, if $s+k \leq d$.

(2) $\operatorname{rank} W_{sk} = \binom{d}{k}$, if $s+k \geqq d$.

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

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

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

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

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.

$x_0 \in X_d$ $\Delta = \Delta_{q,x_0} : H(d,q) \to H(d,q-1)$ 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

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

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

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

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

とすると $[t]-((d,q),k,\lambda_1\lambda_2)$ design が構成される。これを 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、

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

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、$wt(v)=k$ 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 からは $[2]-((q+1,q-1)q,1)$ 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。

<u>Question</u> tight $[2]-((d,2),k,\lambda)$ design からは Weighing matrix がつくれるか。

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