数理解析研究所講究録
第 471 巻 1982 年 117-122

Orthogonal arrays について

鹿児島大理　厚見寅司
Tsuyoshi Atsumi

F 有限集合 $|F|=q$, $X=F^n=\overbrace{F\times\cdots\times F}^{n\text{コ}}$. X に Hamming distance d を入れる。$Y(\subseteq X)$ を F 上の長さ n の code といい, Y の元を codewords と云う。

定義 Y code とする。Y の元 (i.e. codewords) を上から下へならべて array を作る。t, λ 整数 $t\leqq n$. もし array の任意の t 列の各 t 項ベクトルの中にすべての t 項ベクトル (成分は F の元) が丁度各々 λ 回起こるとき Y を strength t, index λ の orthogonal array と云う。Y を (N, n, q, t) と表わす。$|Y|=\lambda q^t=N$.

Delsarte, Enomoto Ito Noda, 及び Noda の結果にヒントを得て, t-デザインについて成立するいくつかの結果が Orthogonal arrays にも成立するのではないかと予想しいくつかの結果を得た。次の定理は Steiner systems についての Noda-Gross の定理に対応するものである。

定理1. $Y=(N, n, q, t)$ で index 1 とする。もし Y のどの2つの codewords 間の Hamming distance $\leqq n-1$ のとき、次の(1)か(2)が成立する。

(1) $(N, n, q, t) = (q^2, q+1, q, 2)$
or
(2) $(N, n, q, t) = (2^t, t+1, 2, t)$ かつ t は偶数.

次の Bush の定理はここでの方法で見ると分りやすい。

定理2. $Y=(N, n, q, t)$ で index 1 とする。もし $q \leqq t$ ならば $n \leqq t+1$.

この定理は Steiner system $S(t, k, v)$ に関する Cameron の不等式 $v \geqq (t+1)(k-t+1)$ に"ある意味で"対応する。ここでの証明はもとの Bush の証明よりたいへん簡単である。

以下 $F=\{0, 1\}$ とする。Y を F 上の長さ n の code とする $|F|=2$ より $\forall A \in Y$ に対して、$\exists_1 A' \in X = F^n$ such that $d(A, A')=n$. $Y' \stackrel{\text{def}}{=} \{A' \mid A \in Y\}$. 又た Y の各元に第 $n+1$ 座標に 0 をつけ F 上の長さ $n+1$ の code を作れる。この code を Y^- と表わす. 次の定理はオーデザインの拡張についての Alltop の定理に対応する。

定理3 Y を $F=\{0, 1\}$ 上の code とする。$Y=(N, n, 2, t)$
$t=\text{even} \Rightarrow Y^- \cup (Y^-)' = (2N, n+1, 2, t+1)$

定理の証明には次の命題が重要である。

$Y \subseteq F^n$. $Y = (N, n, q, t)$ とする。$L = (j_1, \cdots, j_s)$

s-tuple で j_i は異なった整数 $n \geq j_i \geq 1$

$S = (\alpha_1 \cdots \alpha_s) \in F^s$ $\alpha_i \in F$.

$c_i(S, L)$: the number of codewords B such that

$d(B_L\ S) = s - i$. ただし B_L は B の L 座標成分をとりだして作った s-tuple.

命題 1. $E_q(s, r)$ $\displaystyle\sum_{i=r}^{s} \binom{i}{r} c_i(S, L) = \binom{s}{r} \lambda_r$

$\lambda_r = \lambda q^{t-r}$ $0 \leq r \leq \min(s, t)$

注意 この命題は Delsarte が Regular Semilattices の中で t-Designs を定義しましたが、この t-Designs で成立します。

上の命題の証明は次の pair を2通りに数えることで

$(S'\ B)$ $S' \in F^r$, $B \in Y$

$S' \overset{t}{\subseteq} B_L \cap S$ (S' は $B_L \cap S$ という tuple の一部分からなる tuple)

命題 2 (Bush) $Y = (N, n, q, t)$ で index 1

$\Longrightarrow$ $n \leq q + t - 1$.

定理1を証明するためには次のlemmaは重要である。

Lemma 1. $Y=(N, n, q, t)$ で index 1.

$(\alpha_1 \cdots \alpha_i) \in F^i$, $(\beta_1 \cdots \beta_j) \in F^j$, $L=(n_1 \cdots n_i, n_{i+1}, \cdots n_{i+j})$

$\alpha_l \in F$ $\beta_m \in F$

n_mは異なった整数 $1 \leqq n_m \leqq n$. 次のような C codewordsが存在するとする

$$C_L=(\alpha_1 \cdots \alpha_i, \beta_1 \cdots \beta_j),$$

そのとき次のような codewords D の数は i, j と orthogonal array のパラメーターで決まる。

$$D=(\delta_1 \cdots \delta_n) \text{ such that } \delta_{n_1}=\alpha_1, \cdots \delta_{n_i}=\alpha_i$$

$$\delta_{n_{i+1}} \neq \beta_1 \cdots \delta_{n_{i+j}} \neq \beta_j.$$

この数を $\lambda_{i,j}$ と書く.

Lemma 2.

$$\lambda_{i,j}=\sum_{r=0}^{t-i-1}(-1)^r (q-1)^{t-i-r}\binom{i+j-t+r-1}{r}$$

$$0 \leqq i \lneqq t \qquad t < i+j \leqq n$$

$$\lambda_{i,j}=\delta_{j,0} \qquad t \leqq i \leqq n \qquad t \leqq i+j \leqq n.$$

$c_0=\lambda_{0,n}$に注意してGrossと同じく証明すればよい。

定理3を証明するには命題1の特別な場合である次のLemmaが必要である。

Lemma 3. $E_q(t+1)$ $\quad C_0(S, L) + (-1)^t C_{t+1}(S, L)$

$$= \sum_{r=0}^{t} (-1)^r \binom{t+1}{r} \lambda_r .$$

$S \in F^{t+1}$, $L = (i_1 \cdots i_{t+1})$ $\quad i_\ell$ 異なった整数 $1 \leq i_\ell \leq n$. $\mu = \sum_{r=0}^{t} (-1)^r \binom{t+1}{r} \lambda_r$, $C_0 = C_0(S, L)$

$C_{t+1} = C_{t+1}(S, L)$ とおく。 t 偶数

$C_0 + C_{t+1} = \mu$ それゆえ、$B_L = S$ なる codewords の数は C_{t+1}

$B'_L = S$ なる codewords $B' \in Y^-$ の数も C_{t+1} である。 また $B''_L = S$ なる codewords $B'' \in Y'$ の number は $\mu - C_{t+1} = C_0$ である。

$B_L = S$ なる $B \in Y^- \cup (Y^-)'$ の個数は μ である。 注意 この μ は S と L の選択に関係がない!!

$L' = (j_1 \cdots j_t, n+1)$ $\quad j_\ell$: 異なっている整数 $\quad 1 \leq j_\ell \leq n$

この場合 $B_{L'} = S$ なる codewords $B \in Y^- \cup (Y^-)'$ の個数は λ である。

(S, B) such that $S \in F^{t+1}$ $B \in Y^- \cup (Y^-)'$, $B_L = S$

for some $L = (i_1 \cdots i_{t+1})$ $\quad 1 \leq i_\ell \leq n+1$: 異なった整数

を2通りに数えると

$\mu = \lambda$ が証明できる

References

1. Allton Extending t-Designs J. Comb. Th(A) 18 (1975) 177-186.

2. Delsarte An algebraic approach to the association schemes of coding theory Philips Research Reports Supplements 1973 No 10.

3. Delsarte Association Schemes and t-Designs in Regular Semilattices J. Comb. Th(A) 20 (1976) 230-243.

4. Enomoto, Ito, Noda Tight 4-design Osaka J. Math 16 (1979) 39-43.

5. Noda On orthogonal arrays of strength 4 achieving Rao's Bound J. London Math Soc. (2) 19 (1979) 385-390.