

Orthogonal arrays について

鹿野島大理 厚見寅司
Tsuyoshi Atsumi

F 有限集合 $|F| = q$, $X = F^m = \overbrace{F \times \cdots \times F}^m$. X に Hamming distance d を入れる. $Y (\subseteq X)$ を F 上の長さ m 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) を上の j 下 i 列 i 行 array と作る. t, λ 整数 $t \leq m$. t (array の任意の t 列の各 t 項ベクトルの中に t 項ベクトル (成分は F の元) が λ 度各々 λ 回起こるとき Y は strength t , index λ の orthogonal array と云う. Y は (N, m, 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 にも成立するのでないかと予想 (いくつかの結果を得た. 次の定理は Steiner systems についての Noda - Gronn の定理に対応するものである.

定理 1. $\mathcal{Y} = (N, n, q, t)$ で index 1 とする。もし $\mathcal{Y}$ のどの 2 つの codewords 間の Hamming distance $\leq n-1$ のとき、次の (1) か (2) が成り立つ。

$$(1) (N, n, q, t) = (q^2, q+1, q, 2)$$

or

$$(2) (N, n, q, t) = (q^t, t+1, 2, t) \text{ かつ } t \text{ は偶数.}$$

次の Bush の定理をここでの方法で見ると分かりやすい。

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

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

以下 $F = \{0, 1\}$ とする。 $\mathcal{Y}$ を F 上の長さ n の code とする $|\mathcal{Y}| = 2$ より $\forall A \in \mathcal{Y}$ に対して, $\exists A' \in X = F^n$ such that $d(A, A') = n$. $\mathcal{Y}' \triangleq \{A' \mid A \in \mathcal{Y}\}$. また $\mathcal{Y}$ の各元に $n+1$ 座標に 0 をつけ F 上の長さ $n+1$ の code を作る。この code を $\mathcal{Y}^-$ と表す。次の定理は オーデガイン の拡張についての Alltop の定理に対応する。

定理 3 $\mathcal{Y}$ を $F = \{0, 1\}$ 上の code とする。 $\mathcal{Y} = (N, n, 2, t)$

$$t = \text{even} \Rightarrow \mathcal{Y}^- \cup (\mathcal{Y}^-)' = (2N, n+1, 2, t+1)$$

定理の証明には次の命題が重要である。

$$Y \subseteq F^m, Y = (N, m, q, t) \text{ とする。 } L = (j_1, \dots, j_n)$$

n -tuple で j_i は異なり、 t 整数 $m \geq j_i \geq 1$

$$S = (\alpha_1, \dots, \alpha_n) \in F^n \quad \alpha_i \in F$$

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

$d(B, S) = n - i$. $F^L(B)$ は B の L 座標成分をとり

F^L 上での n -tuple .

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

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

注意 この命題は Delsarte が Regular Semilattices の中で t -Designs を定義したことが、この t -Designs になります。

上の命題の証明は次の pairs を 2 通りに数え、とて

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

$$S' \subseteq B \cap S \quad \left(\begin{array}{l} S' \text{ は } B \cap S \text{ の } r \text{-tuple の} \\ \text{一部分が } j \text{ の } j \text{-tuple} \end{array} \right)$$

$$\text{命題 2 (Bush)} \quad Y = (N, m, q, t) \text{ の index 1}$$

$$\Rightarrow m \leq q + t - 1.$$

定理1 を証明する ために は 次の lemma は 重要である。

Lemma 1. $Y = (N, n, g, t)$ を index 1.

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

$\alpha_i \in F \quad \beta_j \in F$

$\dots n_{i+j})$ n_m は 異 1, ..., t : 整数 $1 \leq n_m \leq n$, 次の δ_j

に C code words が存在する。

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

このとき 次の δ_j の code words D の数は i, j の orthogonal array の パラメータで決まる。

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

$$\delta_{n_{i+1}} = \beta_1, \dots, \delta_{n_{i+j}} = \beta_j.$$

この数を $\lambda_{i,j}$ と書く。

Lemma 2.

$$\lambda_{i,j} = \sum_{r=0}^{t-i-1} (-1)^r (2-1)^{t-i-r} \binom{i+j-t+r-1}{r}$$

$$0 \leq i \leq t \quad t < i+j \leq n$$

$$\lambda_{i,j} = \delta_{j,0} \quad t \leq i \leq n \quad t \leq i+j \leq n,$$

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

定理3を証明する際には命題1の特別な場合である次の Lemmaが必要である。

$$\text{Lemma 3. } E_2(t+1) = C_0(S, L) + (-1)^t C_{t+1}(S, L) \\ = \sum_{r=0}^t (-1)^r \binom{t+1}{r} \lambda_r.$$

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

$$C_{t+1} = C_{t+1}(S, L) \text{ とおく. } t \text{ 偶数}$$

$$C_0 + C_{t+1} = \mu \quad \text{すなわち. } B_L = S \text{ 上の code words の数は } C_{t+1}$$

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

$B_L = S$ 上の $B \in Y^- \cup (Y^-)'$ 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!!

$L' = (j_1, \dots, j_t, n+1) \quad j_\ell: \text{異なり, } t \text{ 整数} \quad 1 \leq j_\ell \leq n$
この場合 $B_{L'} = S$ 上の code words $B \in Y^- \cup (Y^-)'$ の個数は λ である。

(S, B) such that $S \in F^{t+1} \quad B \in Y^- \cup (Y^-)', B_L = S$
for some $L = (i_1, \dots, i_{t+1}) \quad 1 \leq i_\ell \leq n+1; \text{異なり, } t \text{ 整数}$
を2通りに数えたと

$$\mu = \lambda \text{ が証明できる}$$

References

1. Allton Extending t -Designs J. Comb. Th(A) 18 (1975) 177-186.
2. Delorme An algebraic approach to the association schemes of coding theory Philips Research Reports Supplements 1973 No 10.
3. Delorme 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.