

ある種の BIB design の non-isomorphic solution とその p -rank

愛媛大 理 矢 田 昇

愛媛大 理 大 森 博 之

§1 序

釣合・型不完備計画 (BIB design) [9] の結合行列 N を parity check matrix とする q 値線形符号 (以下, q 値 BIBD 符号という) は majority decoding [7] により比較的簡単に復号化が可能という利点をもつ。誤り訂正符号の立場からは, BIBD 符号の内では多くの誤りを訂正出来, かつ, 情報点の数が大きいものが望ましい。符号長 v の q 値線形符号の情報点の数は $u\text{-Rank}_q(N)$ (ここに $\text{Rank}_q(N)$ は有限体 $GF(q)$ 上での N の階数を表わす) であるから, 大きい情報点をもつ BIBD 符号を得るには $\text{Rank}_q(N)$ の値 (以下 q -rank) が小さい BIB design を求める必要がある。著者の一人 矢田 [3, 4] は有限射影幾何 $PG(t, q)$ (又は アフィン幾何 $AG(t, q)$) を用い

で作られる BIB design $P_G(t, g): M$ ($E_G(t, g): M$)
 は同じ parameters を持つ BIB design の内では最小の g -
 -rank を持つ事を予想した。:: では, この予想が $g \geq$
 $M = t-1$ の場合には正しい事を示す。

§2 $P_G(t, 2): t-1$ の 2-rank の最小性

$P_G(t, g)$ における点を処理に, M -flat をブロックとみな
 する事に g , 出来る結合行列を $N(g: t, M)$ で表わると,
 $N(g: t, M)$ は parameters:

$$u = (g^{t+1}-1)/(g-1), \quad t = \phi(t, M, g), \quad v = \phi(t+1, M-1, g), \\ k = (g^{M+1}-1)/(g-1), \quad \lambda = \phi(t+2, M-2, g)$$

をもつ BIB design の結合行列である。::

$$\phi(t, M, g) = (g^{t+1}-1)(g^t-1) \cdots (g^{t-M+1}-1) / (g^{M+1}-1)(g^M-1) \cdots (g-1)$$

定理 2.3 の証明に次の定理 (Hamada [3]) が本質的である。

定理 2.1 $P_G(t, p^m)$ における点と M -flat からなる
 結合行列 $N(p^m: t, M)$ の p -rank は次式で与えられる。

$$R_p(t, p^m) = \sum_{(\alpha_0, \dots, \alpha_m) \in S_{t, M}(p^m)} \prod_{j=0}^{m-1} \frac{L(\alpha_{j+1}, \alpha_j)}{\sum_{i=0}^{t-1} (-1)^i \binom{t+1}{i} \binom{t+\alpha_{j+1}p-\alpha_j-ip}{t}}$$

:: $L(\alpha_{j+1}, \alpha_j) = [(\alpha_{j+1}p - \alpha_j)/p]!$, $S_{t, M}(p^m)$ は
 $\alpha_m = \alpha_0$, $0 \leq \alpha_j \leq t-M$, $0 \leq \alpha_{j+1}p - \alpha_j \leq (t+1)(p-1)$

$(j = 0, 1, \dots, m)$ をみたす整数の組 $(\lambda_0, \lambda_1, \dots, \lambda_m)$ からなる集合を表わす。

系 2.2 $PG(t, p^m)$ における点と超平面 $(M=t-1)$ からなる結合行列 $N(p^m: t, t-1)$ の p -rank は

$R_{t-1}(t, p^m) = \binom{t+p-1}{t}^m + 1$ である。特に $p^m=2$ のとき $R_{t-1}(t, 2) = t+2$ である。

この結果 (系 2.2) は Smith [8] や Goethals と Delarte [2] 及び MacWilliams と Mann [6] によって得られたものである。

λ Parameters ν, γ, λ をもつ対称な BIB design を $D(\nu, \gamma, \lambda)$ で表わす。特に $D(2^{t+1}-1, 2^t-1, 2^{t-1}-1)$ の結合行列を N , その complement design の結合行列を N^* , N の $GF(2)$ 上の階数 $R_2(N)$, N の $GF(2)$ 上の列 vector の張る空間を $\mathcal{R}_2(N)$ で表わす事にする。

定理 2.3 $R_2(N) \geq t+2$

ここに等号が成立するのは N が $PG(t, 2): t-1$ の場合に限る。

証明は次の 2つの補助定理を用いて行う。

補助定理 2.4 $R_2(N) = R_2(N^*) + 1$

ただし $R_2(N^*)$ は N^* の $GF(2)$ 上の階数を表わす。

証明 $u = 2^{t+1} - 1$ $v = 2^t - 1$ $J'_u = (\overbrace{1, 1, \dots, 1}^u)$ とする。

このとき $N J_u = v J_u \equiv J_u \pmod{2}$ $\therefore R_2(N) \geq R_2(N^*)$

一方, $J'_u N^* = 2^t J'_u \equiv (0, \dots, 0) \pmod{2}$ (1)

よ $R_2(N^*) \geq R_2(N)$ とあると $J'_u J_u = u \not\equiv 0 \pmod{2}$: これは

(1) 式に矛盾. $\therefore R_2(N^*) \leq R_2(N)$

又, $R_2(N) = R_2([N^*; J_u])$ は自明である。よ。補助定理の結果を得る。

補助定理 2.5 $R_2(N^*) \geq t+1$

証明 $R_2(N^*) = r$ とし, $r < t+1$ とある。 N^* の r 個の一次独立な列 vector をとり, それらの $GF(2)$ 上の相異なる一次結合の総数は $2^r (< 2^{t+1})$ 。これは N^* に異なる列 vector が存在する事を示す。 N^* は対称な BIB design の結合行列であるから, この事はありえな。 証了

定理 2.3 の証明 補助定理 2.4, 2.5 の結果により,

$R_2(N) \geq t+2$ 。特に等号が成立するのは $R_2(N^*) = t+1$ の場合である。補助定理 2.5 と同様の論法により N^* の $(t+1)$ 個の独立な列 vector を任意にとり, それらの相異なる一次結合

全体 (但し 0-Vector は除く) は N^* の列 Vector の全体と一致してはならない。再び補助定理 2.5 と同様の論法により, 任意に選んだ $t+1$ 個の独立な列 Vector から成る行列の行全体は

$$\{(a_0, \dots, a_t) : a_i = 0 \text{ or } 1, i = 0, 1, \dots, t, (a_0, \dots, a_t) \neq (0, \dots, 0)\}$$

と一致せねばならない。この事は N^* の作り方が行と行, 列と列の入れかえを除けば, 一意的である事を示す。一方系 2.2 により $P(t, 2) : t-1$ による結合行列の 2-Rank は $t+2$ である。証了。

§ 3 $E(t, 2) : t-1$ の 2-Rank の最小性.

$E(t, 2)$ における点を処理に, μ -flat をブロックとみなす事によ, 出来る結合行列は parameters:

$$u = g^t \quad e = \phi(t, \mu, g) - \phi(t-1, \mu, g) \quad v = \phi(t-1, \mu-1, g)$$

$$k = g^\mu \quad \lambda = \phi(t-2, \mu-2, g)$$

をもつ BIB design の結合行列である。

定理 3.3 の証明に次の定理 (Hamada [3]) が本質的である。

定理 3.1 $E(t, g)$ における点と μ -flat から成る結合行列の P -Rank は次式で与えられる。 (ただし $g = P^\mu$)

$$V_\mu(t, P^\mu) = R_\mu(t, P^\mu) - R_\mu(t-1, P^\mu)$$

系 3.2 μ -flat の超平面の場合, 即ち $\mu = t-1$ のとき

$$V_{t-1}(t, p^m) = \binom{t+p-1}{t}^m$$

定理 3.3 Parameters $(2^t, 2^{t+1}-2, 2^t-1, 2^{t+1}, 2^{t+1}-1)$ をもつ一つの BIB design の結合行列 M とある。このとき

$$R_2(M) \geq t+1$$

特に等号が成立する場合 design が $E_4(t, 2): t-1$ の場合に限る。

証明は 次の補助定理を用いて行う。

補助定理 3.4 (Connor [17]) Parameters (v, u, r, k, λ) をもつ BIB design の任意は 2 つのブロックの共通な処理の回数 λ' に対し

$$-(r-\lambda-k) \leq \lambda' \leq \frac{1}{r} [2\lambda k + r(r-\lambda-k)]$$

定理 3.3 の証明 $R_2(M) = d$ とする。一般性を失う事なく M の最初の $2^t \times d$ 行列の列 vector は一次独立と仮定してよく, かつ この $2^t \times d$ 行列の行はすべて相異, たとの2つはくてもならない。よって $d \geq t+1$ を得る。次に $R_2(M) = t+1$ とする。今 $R_2(M) \ni J_{2^t}$ (ただし $u = 2^t$)。この J_{2^t} と M のその他の任意は一次独立な列 vector をと

て出来る $2^t \times (t+1)$ 行列を A とする。このとき $R_2(M) = R_2(A)$ 。
 更に A の作り方は, M の t 個の列 Vector の選ぶ方によらず,
 行と行, 列と列の入れかえによる違いを除けば一意である。
 一方, 補助定理 3.4 より M の列 Vector はすべて違っている
 事により, M の列 Vector は A の列 Vector の相異なる一次
 結合全体から 0 Vector 及び $\mathbf{J}$ を取り除いたものではなくては
 ならない。この事は $R_2(M) = t+1$ のものが存在するとき
 一意であることを示す。しかるに系 3.2 は $E(t, 2): t-1$
 による結合行列の 2-Rank は $t+1$ であることを示す。訂了

尚定理 2.1 及び定理 3.1, 及びこれらの系を除く諸命題
 の詳しい証明は参考文献 [5] にのっている。

参考文献

- [1] Conner, W. S. On the Structure of Balanced Incomplete Block Designs, Ann. Math. Statist. 23 (1952), 57-71.
- [2] Goethals, I. M. and Delsarte, P. On a class of Majority Logic Decodable Cyclic Codes, IEEE Trans. on Information Theory IT-14 (1968), 182-188.

- [3] Hamada, N. On the p -Rank of the Incidence Matrix of a Balanced or Partially Balanced Incomplete Block Design and its Applications to Error Correcting Codes, to appear in Hiroshima Math. J. 3 (1973).
- [4] 浜田 昇 有限差月における結合行列の p -rank とその応用 日本数学会 (1972 年秋) 統計数学会分科会 特別講演要旨 (1972) 82-100.
- [5] Hamada, N. and Ohmeri, H. On the BIB Design having the Minimum p -Rank Submitted to J. Combinatorial Theory (1973).
- [6] MacWilliams, J. and Mann, H. B. On the p -rank of the Design Matrix of a Difference Set, Mathematics Research Center, Technical Report, No. 803, Univ. of Wisconsin, 1967.
- [7] Massey, J. C. Threshold decoding. The M. I. T. Press, Cambridge, Massachusetts. (1963)
- [8] Smith, K. J. C. On the p -Rank of the Incidence Matrix of Points and Hyperplanes in a Finite Projective Geometry, J. Combinatorial Theory 7 (1969), 122-129.

[9] Yates, F. Incomplete Randomised Blocks,
Ann. Eugen. 7 (1936), 121-140