数理解析研究所講究録
第178巻 1973年 38-46

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

愛媛大 理　浜田 昇
愛媛大 理　大森博之

§1 序

釣合い型不完備計画（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]によって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$v-\mathrm{Rank}_q(N)$（ここに$\mathrm{Rank}_q(N)$）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$\mathrm{Rank}_q(N)$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 浜田[3,4]は有限射影幾何$PG(t,q)$（又はアフィン幾何$EG(t,q)$）を用い

て作られるBIB design $PG(t,q):\mu$ $(EG(t,q):\mu)$ は同じ parameters を持つBIB design の内では最小の q-rank を持つ事を予想した。ここでは，この予想が $q=2$ $\mu=t-1$ の場合には正しい事を示す。

§2 $PG(t,2):t-1$ の 2-rank の最小性

$PG(t,q)$ における点を処理に，μ-flat をブロックとみなす事によって出来る結合行列を $N(q:t,\mu)$ で表わすと，$N(q:t,\mu)$ は parameters:

$$v=(q^{t+1}-1)/(q-1), \quad b=\phi(t,\mu,q), \quad r=\phi(t-1,\mu-1,q),$$

$$k=(q^{\mu+1}-1)/(q-1), \quad \lambda=\phi(t-2,\mu-2,q)$$

をもつBIB design の結合行列である。ここに

$$\phi(t,\mu,q)=(q^{t+1}-1)(q^{t}-1)\cdots\cdots(q^{t-\mu+1}-1)\Big/(q^{\mu+1}-1)(q^{\mu}-1)\cdots\cdots(q-1)$$

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　$PG(t,p^m)$ における点と μ-flat からなる結合行列 $N(p^m:t,\mu)$ の p-rank は次式で与えられる。

$$R_\mu(t,p^m)=\sum_{(s_0,\cdots,s_m)\in S_{t,\mu}(p^m)}\ \prod_{j=0}^{m-1}\ \sum_{i=0}^{L(s_{j+1},s_j)}(-1)^i\binom{t+1}{i}\binom{t+s_{j+1}p-s_j-ip}{t}$$

ここに $L(s_{j+1},s_j)=\left[(s_{j+1}p-s_j)/p\right]$ で，$S_{t,\mu}(p^m)$ は $s_m=s_0$, $0\le s_j\le t-\mu$, $0\le s_{j+1}p-s_j\le(t+1)(p-1)$

$(j=0,1,\cdots,m)$ をみたす整数の組 $(s_0, s_1, \cdots, s_m)$ 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 Delsarte [2] 及び MacWilliams と Mann [6] によって得られたものである。

尚 parameters v, r, λ をもつ対称な BIB design を $D(v, r, \lambda)$ 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 $GF(2)$ 上での階数を $R_2(N)$, N の $GF(2)$ 上での列 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) 上での階数を表わす。

証明 $u=2^{t+1}-1$ $r=2^t-1$ $J_u'=(\overbrace{1,1,\cdots,1}^{u})$ とする。

このとき $NJ_u = rJ_u \equiv J_u \pmod 2$ ∴ $\mathcal{R}_2(N)\ni J_u$

一方，$J_u' N^* = 2^t J_u' \equiv (0,\cdots,0) \pmod 2$ …… (イ)

今 $\mathcal{R}_2(N^*)\ni J_u$ とすると $J_u'J_u = u \not\equiv 0 \pmod 2$ これは (イ)式に矛盾. ∴ $\mathcal{R}_2(N^*)\not\ni J_u$

又，$\mathcal{R}_2(N)=\mathcal{R}_2([N^*:J_u])$ は自明である。よって補助定理の結果を得る。

補助定理 2.5 $R_2(N^*)\ge t+1$

証明 $R_2(N^*)=r$ とし，$r<t+1$ とする。N^* の r 個の一次独立な列 Vector をとり，それらの GF(2) 上での相異る一次結合の総数は $2^r\ (<2^{t+1}-1)$。これは N^* に同一な列 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，この事はありえない。 証了

定理 2.3 の証明 補助定理 2.4，2.5 の結果により，$R_2(N)\ge t+2$。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の全体と一致しなくてはならない。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

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

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 $PG(t,2) : t-1$ による結合行列の2-rankは $t+2$ である。　　　　証了.

§3　$EG(t,2) : t-1$ の2-rankの最小性.

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

$u = q^t$　　$b = \phi(t,\mu,q) - \phi(t-1,\mu,q)$　　$r = \phi(t-1,\mu-1,q)$

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

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　$EG(t,q)$ 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 $q=p^m$）

$$r_\mu(t,p^m) = R_\mu(t,p^m) - R_\mu(t-1,p^m)$$

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

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

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 の結合行列を M とする。このとき　$R_2(M) \geq t+1$

特に等号が成立する場合は design が $EG(t,2): t-1$ 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, b, r, k, λ) をもつ BIB design の任意な2つのブロックの共通な処理の個数 λ' に対して

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

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ったものでなくてはならない。これより $d \geq t+1$ を得る。次に $R_2(M)=t+1$ とする。今 $\mathcal{R}_2(M) \ni J_{\hat{v}}$ (ただし $\hat{v}=2^t$)。この $J_{\hat{v}}$ と M の t 個の任意な一次独立な列 Vector をとっ

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の選び方によらず，行と行，列と列の入れかえによる違いを除けば一意的である。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の相異る一次結合全体から0 Vector及び J_{Ω} を取り除いたものでなくてはならない。この事は $R_2(M)=t+1$ のものが存在するときは一意的である事を示す。しかるに系3.2は $EG(t,2):t-1$ による結合行列の2-rankは $t+1$ である事を示す。証了

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

参考文献

[1] Connor, W. S. On the Structure of Balanced Incomplete Block Designs, Ann. Math. Statist. 23(1952), 57-71.

[2] Goethals, J. 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　有限幾何における結合行列のp-rankとその応用　日本数学会(1972年秋)統計数学分科会 特別講演要旨 (1972) 82-100.

[5] Hamada, N. and Ohmori, 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