

有限幾何と実験計画

広島大理 山本 純恭

海上保安大 福田 悌次郎

広島大理 浜田 昇

1. 序

C. R. Rao [2], [3] は R. C. Bose の Difference theorems [1] と呼ばれる定理を一般化し, BIBD を巡回的に生成する difference sets の構成法を発表した。一つのガロア体 $GF(m)$ 上の有限 t 次元射影空間 $PG(t, m)$ 及びユークリッド空間 $EG(t, m)$ において, 点の全体を treatments, $d \leq t$ 次元線形部分空間 (d -flat) の全体を blocks にとると BIBD が得られることは周知の通りであるが [1], Rao は一般化された difference theorems を用いてこれらの designs を組織的に作るために, d -flat に cycle という概念を導入して d -flats の全体を類別し, その構造定理を次のように述べた。

Proposition 1 (Rao)

$PG(t, m)$ において $r_1, r_2, \dots, r_p$ を次の条件をみたす正整数とする。

- (a) $0 < r_1 < r_2 < \dots < r_p < t$,
- (b) $(m^{d+1}-1)/(m^{r_i+1}-1) = \lambda_i$ は正整数,

$$(c) (d+1)/(r_i+1) = t_i \quad \text{は正整数,}$$

$$(d) (r_{i+1}+1)/(r_i+1) = l_i \quad \text{,}$$

$$(e) (m^{t_i}-1)/(m^{r_i+1}-1) = \theta_i \quad \text{,}$$

すると, $y_i = (n_i - n_{i+1})/\theta_i$ 個の cycle θ_i ($i=1, 2, \dots, p$) の initial flats と $\eta = (b - n_1)/v$ 個の cycle v の initial flats が存在し, d -flats の全体はこれらの initial flats から生成される. ここに, $n_i = \binom{\theta_i}{t_i} / \binom{\lambda_i}{t_i}$ であり, v と b はそれぞれ $PG(t, m)$ における点と d -flats の個数である.

Proposition 2 (Rao)

$EG(t, m)$ において $h = p_0 p_1^{i_1} p_2^{i_2} \dots$ ($p_0=1$, p_i は $p_i < p_{i+1}$ をみたす素数) を d と t との最大公約数とすると, 原点 (0) を通る d -flats は $\theta_{j,s} = (m^t - 1)/(m^{r_{j,s}} - 1)$ なる形の cycles をもち, cycle $\theta_{j,s}$ の initial flats の個数は

$$(n_{j,s} - n_{j+1, s+1}) / \theta_{j,s}$$

である. そして原点を通る d -flats の全体はこれらの initial flats から生成される. ここに $r_{j,s} = p_1^{i_1} p_2^{i_2} \dots p_j^{i_j}$ ($j=0, 1, \dots; s=0, 1, \dots, i_j$), $n_{j,s} = \binom{\theta_{j,s}}{d/r_{j,s}} / \binom{q_{j,s}}{d/r_{j,s}}$, $q_{j,s} = (m^d - 1)/(m^{r_{j,s}} - 1)$.

しかしながら, これらの Propositions は特別の場合を除いて一般には成立しない. この論説の目的の一つはこれらの構造定理を修正することである. 今一つの目的は より小さいある cycle θ の d -flats のみを blocks にとることにより一つの PBIBD が得られること, 更に,

cycle も d -flat 上の点の一部のみを treatments にとることにより一つの BIBD が得られることを示す。これらの考察から、 $PG(t, m=p^n)$ における d -flat の全体から作られる BIBD (今後これを $PG(t, m): d$ で表わす) は $PG(\tilde{t}, p)$ における $\tilde{d}$ -flat の全体から作られる BIBD $PG(\tilde{t}, p): \tilde{d}$ において、blocks の一部及び treatments の一部をカットすることによっても得られることがわかる。ここに、 $\tilde{t} = n(t+1)-1$, $\tilde{d} = n(d+1)-1$.

以下主要結果を述べる。詳細については [4] を参照されたい。

2. $PG(t, m)$ における d -flat

[定義] ガロア体 $GF(m=p^n)$ 上の t 次元射影空間 $PG(t, m)$ とは 次の条件をみたす点の集合である。

- (a) $GF(m^{t+1})$ の非零元 ν を点と考えて (ν) で表わす。
- (b) 2点 (ν) と (μ) とは $\mu = \sigma\nu$ なる $\sigma \neq 0 \in GF(m)$ が存在するときに限り同一点を表わす。
- (c) $(\nu_0), (\nu_1), \dots, (\nu_d)$ を係数体 $GF(m)$ に関して一次独立な点とすると、点 $(a_0\nu_0 + a_1\nu_1 + \dots + a_d\nu_d)$ の全体を d -flat という。ただし $a_i \in GF(m)$ であり、同時に 0 となることはないものとする。

特に 0-flat を点, 1-flat を直線, 2-flat を平面と呼ぶ。

[定義] α を $GF(m^{t+1})$ の原始元の一つとすると, α は $GF(m)$ を係数域とする $t+1$ 次の minimum function $f(x) = x^{t+1} + a_t x^t + \dots + a_1 x + a_0$ の零点であり, $GF(m^{t+1})$ の非零元は $\alpha^k (k=0, 1, 2, \dots, m^{t+1}-2)$ の形で

表わされる。これを x によるべき表現という [1], [2]。

$(t+1)/(i+1)$ が正整数のときは $\theta = (m^{t+1}-1)/(m^{i+1}-1)$ とおくと, x^θ は $GF(m^{i+1})$ の原始元であるから 次の表現を得る:

$$GF(m^{i+1}) = \{0, x^\theta, x^{2\theta}, \dots, x^{(m^{i+1}-2)\theta}\},$$

$$PG(i, m) = \{(x^0), (x^\theta), \dots, (x^{(\frac{m^{i+1}-1}{m-1}-1)\theta})\}.$$

特に $i=0$ のとき

$$GF(m) = \{0, x^0, x^v, \dots, x^{(m-2)v}\},$$

$$PG(t, m) = \{(x^0), (x^1), (x^2), \dots, (x^{v-1})\}. \quad \text{ただし, } v = \frac{m^{t+1}-1}{m-1}.$$

また, x^θ が $GF(m^{i+1})$ の原始元であることから $PG(i, m)$ の点の中で最初の $i+1$ 個の点 $(x^0), (x^\theta), \dots, (x^{i\theta})$ が 係数体 $GF(m)$ に関して一次独立であることがわかる。

[定義] 一次独立な $d+1$ 個の点 $(x^{b_0}), (x^{b_1}), \dots, (x^{b_d})$ を通る d -flat

$$V_d(0) = \{(a_0 x^{b_0} + a_1 x^{b_1} + \dots + a_d x^{b_d})\} \quad \text{及び} \quad \text{ある正整数 } c \text{ に対して}$$

$$V_d(c) = \{(a_0 x^{b_0+c} + a_1 x^{b_1+c} + \dots + a_d x^{b_d+c})\} \quad \text{なる } d\text{-flat を考える.}$$

$V_d(c) = V_d(0)$ なる正整数 c を initial flat $V_d(0)$ の cycle という [2].

$V_d(v) = V_d(0)$ であるから, v は常に任意の d -flat $V_d(0)$ の cycles の一つである. $V_d(0)$ の cycles の中で最小値を minimum cycle と呼び, m.c. と略記する.

$V_d(0)$ の m.c. を θ とすれば, $V_d(1), V_d(2), \dots, V_d(\theta-1)$ も m.c. θ をもつから これら θ 個の flats を m.c. θ の initial d -flat $V_d(0)$ から generate される d -flats という.

これらの定義と minimum cycles の性質 [2] から次の定理を得る.

[定理1] $\theta_i = (m^{t+1}-1)/(m^{i+1}-1)$ が正整数ならば, $V_i(0) = \{(a_0x^0 + a_1x^{e_1} + \dots + a_ix^{i\theta_i})\}$ は m.c. θ_i の i -flat である.

[定理2] 一つの d -flat V_d が必ずより小さい m.c. θ をもつならば, θ は $\theta = (m^{t+1}-1)/(m^{j+1}-1)$ の形である. ここに $j+1$ は $t+1$ と $d+1$ との公約数である. この場合 V_d は m.c. θ の j -flat $V_j(0) = \{(a_0x^0 + a_1x^{e_1} + \dots + a_jx^{j\theta})\}$ から generate される θ 個の j -flats の中の $(m^{d+1}-1)/(m^{j+1}-1)$ 個から成る.

[定義] $i+1$ を $t+1$ と $d+1$ との公約数の一つとすると, m.c. $\theta_i = (m^{t+1}-1)/(m^{i+1}-1)$ の i -flat $V_i(0) = \{(a_0x^0 + a_1x^{e_1} + \dots + a_ix^{i\theta_i})\}$ から generate される θ_i 個の flats の中から $d_i+1 = (d+1)/(i+1)$ 個の flats を選り出し, 各 flats 上の一次独立を $i+1$ 個ずつ合計 $d+1 = (i+1)(d_i+1)$ 個の点が一次独立となるようできる. これから $d+1$ 個の点によって張られる flat を d_i+1 個の一次独立な m.c. θ_i の i -flats から作られる d -flat と呼び, " $d(i)$ -flat" と書く. 特に, $i=0$ の場合, 即ち, d -flat V_d が $d+1$ 個の 0 -flats からできているとき, その flat も形式的に " $d(0)$ -flat" と書くことにする.

すると定義から, 定理2で述べた flat は一つの $d(j)$ -flat であることがわかる.

[定理3] (1) m.c. θ をもつ d -flat は常に存在する.

(2) $j+1$ が $t+1$ と $d+1$ との公約数であるような正整数 j が存在するならば, $\theta_j = (m^{t+1}-1)/(m^{j+1}-1)$ を m.c. とする d -flat が存在する.

[定理4] $j+1$ が $t+1$ と $d+1$ との公約数であり, かつ, V_d が $\theta_j = (m^{t+1}-1)/(m^{j+1}-1)$

$(m^{j+1}-1) \in m.c.$ にもつ d -flat をらば, V_d は一つの $d(j)$ -flat であるばかりでなく, $i+1$ が $j+1$ の約数であるような正整数 i または $i=0$ に対して $d(i)$ -flat とみなすことができる.

この定理から $d(i)$ -flats の全体は $m.c. \theta_i$ の d -flats のみならず, θ_i の約数であるような θ_j に対して $m.c. \theta_j$ の $d(j)$ -flats をも含むことがわかる. よって $m.c. \theta_i$ の $d(i)$ -flats の個数 n_i^* は $d(i)$ -flats の個数 n_i から, かかる $d(j)$ -flats の個数 n_j^* をすべて引くことによって求まる.

さて, n_i は次の定理によって計算される.

[定理5] $d(i)$ -flats の個数は $n_i = \phi(t_i, d_i, m^{i+1})$ である.

ここに $t_i = \frac{t+1}{i+1} - 1$, $d_i = \frac{d+1}{i+1} - 1$ であり, $\phi(t, d, m)$ は $PG(t, m)$ における d -flats の個数を表わす関数で次式で与えられる [1]:

$$\phi(t, d, m) = \frac{(m^{t+1}-1)(m^t-1) \cdots (m^{t-d+1}-1)}{(m^{d+1}-1)(m^d-1) \cdots (m-1)}.$$

以上をまとめて, Proposition 1 (Rao) に対応する次の general theorem を得る.

[定理6] (1) $t+1$ と $d+1$ とが互に素ならば, $PG(t, m)$ におけるすべての d -flats は $m.c. v$ をもち, $\eta = \phi(t, d, m)/v$ 個の initial d -flats から generate される.

(2) $(t+1, d+1) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_e^{\alpha_e}$ (>1 , p_i は $p_i < p_{i+1}$ をみたす素数) を $t+1$ と $d+1$ との最大公約数とすると, 異なる $m.c.$ の個数は $\prod_{i=1}^e (1 + \alpha_i)$ である. 今 .

$$\theta[x_1, \dots, x_e] = (m^{t+1} - 1) / (m^{p_1^{x_1} \dots p_e^{x_e}} - 1), \quad t[x_1, \dots, x_e] = (t+1) / (p_1^{x_1} \dots p_e^{x_e}) - 1,$$

$$d[x_1, \dots, x_e] = (d+1) / (p_1^{x_1} \dots p_e^{x_e} - 1), \quad m[x_1, \dots, x_e] = m^{p_1^{x_1} \dots p_e^{x_e}}$$

とおくと, $\theta[x_1, \dots, x_e] \in \text{cycle}$ 及び m.c. とする $d(p_1^{x_1} \dots p_e^{x_e} - 1)$ -flats の個数はそれぞれ

$$n(x_1, \dots, x_e) = \phi(t[x_1, \dots, x_e], d[x_1, \dots, x_e], m[x_1, \dots, x_e]),$$

$$n^*(x_1, \dots, x_e) = n(x_1, \dots, x_e),$$

$$n^*(x_1, \dots, x_e) = n(x_1, \dots, x_e) - \sum_{\substack{x_j \leq y_j \leq x_j; \exists j, x_j < y_j}} n^*(y_1, \dots, y_e)$$

で与えられる. よって m.c. $\theta[x_1, \dots, x_e]$ の initial d -flats の個

数は $n(x_1, \dots, x_e) = n^*(x_1, \dots, x_e) / \theta[x_1, \dots, x_e]$ であり, これから

m.c. $\theta[x_1, \dots, x_e]$ の d -flats の全体が generate される.

3. $EG(t, m)$ における d -flats

[定義] $GF(m)$ 上の t 次元ユークリッド空間 $EG(t, m)$ とは次の条件をみたす点の集合である.

(a) $GF(m^t)$ の各元を点と考えて (v) で表わす. 二点 (v) と (u) とは $v=u$ のときに限り同一点である.

(b) $(v_0), (v_1), \dots, (v_d) \in GF(m)$ に関して一次独立な点とすると, 点 $(a_0 v_0 + a_1 v_1 + \dots + a_d v_d)$ の全体を d -flat という. ただし, $a_i \in GF(m)$ は $\sum_{i=0}^d a_i = 1$ という制約条件をみたすものとする.

定義より, $EG(t, m)$ は $PG(t, m)$ から一つの超平面 $(t-1)$ -flat 上のすべての点を取り除いて得られる空間とみなすことができる. このことから $EG(t, m)$ における d -flats の個数は $b = \phi(t, d, m) - \phi(t-1, d, m)$

であることがわかる。

次に, $x \in \text{GF}(m^t)$ の原始元のひとつとすると, 次のような $\text{EG}(t, m)$ の x によるべき表現を得る:

$$\text{EG}(t, m) = \{(0), (x^0), (x^1), \dots, (x^{m^t-2})\}.$$

$\text{EG}(t, m)$ における d -flats の minimum cycles による類別に戻しては次の二つの場合が考えられる。

(1) 原点(0)を通らない d -flats

この場合の d -flats はすべて, m.c. $v^* = m^t - 1$ をもち, その位数は $b_1 = b - \phi(t-1, d-1, m) = \phi(t, d, m) - \phi(t-1, d, m) - \phi(t-1, d-1, m)$ 。

(2) 原点(0)を通る d -flats

原点を通る任意の d -flat は $\forall d(0) = \{(a_1 x^{b_1} + a_2 x^{b_2} + \dots + a_d x^{b_d})\}$ という形で表わされ, $\sum_{i=1}^d a_i = 1$ という制約条件は不用となる。さて, $\theta = (m^t - 1)/(m - 1)$ とおくと原点を通るすべての d -flats は cycles の一つとして θ をもつから, $\text{EG}(t, m)$ における原点を通る d -flats の全体は cycles に戻しては $\text{PG}(t-1, m)$ における $(d-1)$ -flats の全体と同じ構造をもつことがわかる。よって定理6の直接的結果として, Proposition 2(Rao)に対応する次の定理を得る。

[定理7] $(t, d) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_e^{\alpha_e}$ (> 1 , p_i は $p_i < p_{i+1}$ をみたす素数) を t と d との最大公約数とすると, 原点を通る d -flats の m.c. の位数は $\prod_{i=1}^e (1 + \alpha_i)$ である。今

$$\theta(x_1, \dots, x_e) = (m^t - 1) / (m^{p_1^{x_1} \dots p_e^{x_e}} - 1), \quad t(x_1, \dots, x_e) = t / (p_1^{x_1} \dots p_e^{x_e}),$$

$$d(x_1, \dots, x_e) = d / (p_1^{x_1} \dots p_e^{x_e}), \quad m(x_1, \dots, x_e) = m^{p_1^{x_1} \dots p_e^{x_e}}$$

とあくと, 原点を通り $\theta[x_1, \dots, x_e] \in \text{cycle}$ 及 α m.c. とする $d(p_1^{x_1} \dots p_e^{x_e}) - \text{flats}$ の個数はそれぞれ

$$n(x_1, \dots, x_e) = \phi(t[x_1, \dots, x_e] - 1, d[x_1, \dots, x_e] - 1, m[x_1, \dots, x_e]),$$

$$n^*(x_1, \dots, x_e) = n(x_1, \dots, x_e),$$

$$n^*(x_1, \dots, x_e) = n(x_1, \dots, x_e) - \sum_{x_j \neq y_j \leq x_j; \exists j, x_j < y_j} n^*(y_1, \dots, y_e)$$

で与えられる. よって m.c. $\theta[x_1, \dots, x_e]$ の initial d -flats の個数は

$$n(x_1, \dots, x_e) = n^*(x_1, \dots, x_e) / \theta[x_1, \dots, x_e] \text{ であり, これらから m.c. } \theta[x_1, \dots, x_e]$$

の d -flats の全体が generate される.

4. 巡回的に生成される不完備計画の Construction

designs の構成に関しては次の定理が必要である.

[定理8] 定理6の(2)の条件の下で, 2点 (x^α) と (x^β) とを通る cycle $\theta[x_1, \dots, x_e]$

の $d(p_1^{x_1} \dots p_e^{x_e} - 1)$ -flats の個数 $\lambda_i(x_1, \dots, x_e)$ は

$\alpha - \beta \equiv 0 \pmod{\theta[x_1, \dots, x_e]}$ のとき

$$\lambda_1(x_1, \dots, x_e) = \phi(t[x_1, \dots, x_e] - 1, d[x_1, \dots, x_e] - 1, m[x_1, \dots, x_e]),$$

$\alpha - \beta \not\equiv 0 \pmod{\theta[x_1, \dots, x_e]}$ のとき

$$\lambda_2(x_1, \dots, x_e) = \phi(t[x_1, \dots, x_e] - 2, d[x_1, \dots, x_e] - 2, m[x_1, \dots, x_e]).$$

[定義] $\theta[x_1, \dots, x_e] < v$ のとき, $PG(t, m)$ の任意の2点 (x^α) と (x^β) との間に関係を定義する.

$\alpha - \beta \equiv 0 \pmod{\theta[x_1, \dots, x_e]}$ のとき (x^α) と (x^β) とは 1st associate,

$\alpha - \beta \not\equiv 0 \pmod{\theta[x_1, \dots, x_e]}$ のとき (x^α) と (x^β) とは 2nd associate,

任意の点はそれ自身と 0-th associate である。

これらの点の間に定義されたこれらの関係は association scheme の満たすべき条件を満足する。これより次の定理を得る。

[定理 9] $PG(t, m)$ において一つの d -flat が v より小さい cycle $\theta[x_1, \dots, x_e]$ をもつならば, $PG(t, m)$ における点の全体を treatments, $d(p_1^{x_1} \dots p_e^{x_e} - 1)$ -flats の全体を blocks にとることにより N_2 type (GD type) の PBIBD が得られる。その parameters は次の通りである。

$$\begin{aligned} v &= \phi(t, 0, m), & b &= \phi(t[x_1, \dots, x_e], d[x_1, \dots, x_e], m[x_1, \dots, x_e]), \\ k &= \phi(d, 0, m), & r &= \lambda_1(x_1, \dots, x_e), \lambda_1 = \lambda_1(x_1, \dots, x_e), \lambda_2 = \lambda_2(x_1, \dots, x_e), \\ n_0 &= 1, & n_1 &= r(x_1, \dots, x_e) - 1, \quad n_2 = r(x_1, \dots, x_e) \{ \theta[x_1, \dots, x_e] - 1 \}, \end{aligned}$$

$$\text{ただし } r(x_1, \dots, x_e) = v / \theta[x_1, \dots, x_e]$$

$$\begin{bmatrix} p_{11}^1 & p_{12}^1 \\ p_{21}^1 & p_{22}^1 \end{bmatrix} = \begin{bmatrix} r(x_1, \dots, x_e) - 2 & 0 \\ 0 & r(x_1, \dots, x_e) \{ \theta[x_1, \dots, x_e] - 1 \} \end{bmatrix},$$

$$\begin{bmatrix} p_{11}^2 & p_{12}^2 \\ p_{21}^2 & p_{22}^2 \end{bmatrix} = \begin{bmatrix} 0 & r(x_1, \dots, x_e) - 1 \\ r(x_1, \dots, x_e) - 1 & r(x_1, \dots, x_e) \{ \theta[x_1, \dots, x_e] - 2 \} \end{bmatrix}.$$

[定理 10] 定理 9 で得られた design において, 原始元 s のべきの指数が $\theta[x_1, \dots, x_e]$ より小さい点のみを treatments にとれば, 次の parameters をもつ BIBD が得られる。

$$v^* = \theta[x_1, \dots, x_e] = \phi(t[x_1, \dots, x_e], 0, m[x_1, \dots, x_e]),$$

$$b^* = \phi(t[x_1, \dots, x_e], d[x_1, \dots, x_e], m[x_1, \dots, x_e]),$$

$$k^* = \phi(d[x_1, \dots, x_e], 0, m[x_1, \dots, x_e]),$$

$$r^* = \phi(t[x_1, \dots, x_e] - 1, d[x_1, \dots, x_e] - 1, m[x_1, \dots, x_e]),$$

$$\lambda^* = \phi(t[x_1, \dots, x_e] - 2, d[x_1, \dots, x_e] - 2, m[x_1, \dots, x_e]).$$

次の定理は定理10の系として得られる結果で、実際に幾何学的 BI
BDを作る際有力な方法を示すものである。

[定理11] $\tilde{t} = n(t+1)-1$, $\tilde{d} = n(d+1)-1$ とおくとき Design $PG(t, m=p^n):d$
は Design $PG(\tilde{t}, p): \tilde{d}$ において, $GF(p^{\tilde{t}+1})$ の原始元 α のべきの指数
が $\theta = \phi(t, 0, m)$ より小さい点のみを treatments に, cycle θ の $\tilde{d}$ -flats の
みを blocks にとることによって得られる。

幾何学的不完備計画を巡回的に生成する difference sets を実際に作る
には, m.c. $\theta[x_1, \dots, x_e]$ の $\eta(x_1, \dots, x_e)$ 個の initial d -flats 上の点
 $\{(x^{d_{ij}} \mid i=1, 2, \dots, \eta(x_1, \dots, x_e); j=1, 2, \dots, k)\}$ と各 $\theta[x_1, \dots, x_e]$ 毎に, α の
べきの指数 $\{d_{ij} \mid i=1, 2, \dots, \eta(x_1, \dots, x_e); j=1, 2, \dots, k\}$ で置きかえれば
よい。 $EG(t, m)$ においては $v = v^* + 1 = m^t$ 個の点があるから, 原点(0)
に対して若干の修正が必要である。即ち, 原点(0)には記号 ∞ を対応さ
せ $\infty + a = \infty$ ($a=0, 1, 2, \dots, v-2$) なる性質を持たせることにする。
すると, すべての $\theta[x_1, \dots, x_e]$ に対して得られた m.c. $\theta[x_1, \dots, x_e]$ の diffe-
rence sets $\{d_{ij}\}$ の全体は BIBD $PG(t, m):d$ 及び BIBD
 $EG(t, m):d$ を生成する[2]。

cycle $\theta[x_1, \dots, x_e]$ の difference sets のみを考えると定理9で述べた
PBIBDが得られるし, 更に, この difference sets で cycle $\theta[x_1, \dots, x_e]$
より小さい整数のみから成る部分集合の族を考えると 定理10で述べた
BIBD が得られる。

参考文献

- [1] Bose, R.C. (1939). On the construction of balanced incomplete block designs. Ann. Eugenics 9 353-399.
- [2] Rao, C.R. (1945). Finite geometries and certain derived results in theory of numbers. Proc. Nat. Inst. Sci. India 11 136-149.
- [3] Rao, C.R. (1946). Difference sets and combinatorial arrangements derivable from finite geometries. Proc. Nat. Inst. Sci. India 12 123-135.
- [4] Yamamoto, S., Fukuda, T. and Hamada, N. (1966). On finite geometries and cyclically generated incomplete block designs. J. Sci. Hiroshima Univ. Ser. A-1 30 137-149.