

有限幾何と実験計画

広島大理 山本 純恭
海上保安大 福田 勝次郎
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, $d < t$ 次元線形部分空間 (d -flat) の全体を blocks とするとき 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 は組織的に作るためには, d -flat (= 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 h_1, h_2, \dots, h_p を次の条件をみたす正整数とする。

- (a) $0 < h_1 < h_2 < \dots < h_p < t$,
- (b) $(m^{d+1}-1)/(m^{h_i+1}-1) = \lambda_i$ (は正整数),

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

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

$$(m^t-1)/(m^{r_i}-1) = \theta_i \quad \cdots.$$

すると, $y_i = (n_i - n_{i+1})/\theta_i$ は cycle θ_i ($i=1, 2, \dots, p$) の initial flats と $\eta = (b - n_1)/\eta$ は cycle η の initial flats が存在し, d -flats の全体はこれら initial flats から生成される。すなはち, $n_i = (\theta_i)/(t_i)$ であり, η 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 $p_i < p_{i+1}$ を満たす素数)を $d=t$ との最大公約数とするとき, 原点(0)を通る d -flats は $\theta_{j,0} = (m^t-1)/(m^{r_{j,0}}-1)$ なる形の cycles をもち, cycle $\theta_{j,0}$ の initial flats の個数は

$$(n_{j,0} - n_{j+1,0})/\theta_{j,0}$$

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

しかしながら, これら 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 ひより小さいある cycle θ の d -flats のみを blocks にとることにより一つの PBIBD が得られるここと, 更に,

cycle から blocks 上の点の一部のみを treatments にとることにより
一つの BIBD が得られるこことを示す。これらの方案から,
 $PG(t, m=p^n)$ 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{t} において, blocks の一部及び treatments の一部をカットするこによっても得られることがわかる。ミニに,
 $\tilde{t} = n(t+1)-1$, $\tilde{d} = n(d+1)-1$

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 γ を点と考えて (v) で表わす。
- (b) 2 点 (v) と (u) とは $\mu = \sigma\gamma$ すな $\sigma \neq 0 \in GF(m)$ が存在するとき
に限り同一点を表わす。
- (c) $(v_0), (v_1), \dots, (v_d)$ を素数体 $GF(m)$ に属して一次独立な点とするとき,
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
 $a_i \in GF(m)$ 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] x を $GF(m^{t+1})$ の原始元の一つとすると, x は $GF(m)$ の素数域とする $t+1$ 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 x^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:

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

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

特に $i=0$ のとき

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

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

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 像数体 $GF(m)$ に関する一次独立であることがわかる。

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

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

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

$V_d(c) = V_d(0)$ ある正整数 c を initial flat $V_d(0)$ の cycle といふ [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, $V_d(1), V_d(2), \dots, V_d(\theta-1)$ は m.c. θ をもつからこれら θ 個の flats は m.c. θ の initial d -flat $V_d(0)$ から generate される d -flats といふ。

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

[定理2] 一つの d -flat V_d が “より小さい” m.c. θ をもつならば,
 θ (\models $\theta = (m^{t+1})/(m^{t+1}-1)$ する形である. ここで $j+1$ は $t+1$ と $d+1$ の
 公約数である. この場合 V_d は m.c. θ の j -flat $V_j(0) = \{(a_0x^0 + a_1x^{e_i} + \dots + a_j x^{e_i})\}$ から generate される θ 12 の flats の中で $(m^{t+1})/(m^{t+1}-1)$ 12 から成る.

[定義] $i+1$ が $t+1$ と $d+1$ の公約数の一つとする. m.c. $\theta_i = (m^{t+1})/(m^{t+1}-1)$ の i -flat $V_i(0) = \{(a_0x^0 + a_1x^{e_i} + \dots + a_i x^{e_i})\}$ から generate される θ_i 12 の flats の中から $d_i+1 = (d+1)/(i+1)$ 12 の flats を選んで出し, 各 flats 上の一次独立を $i+1$ 12 ずつ合計 $d+1 = (i+1)(d_i+1)$ 12 の点が一次独立とすらようできる. これら $d+1$ 12 の点によって張られる flat は d_i+1 12 の一次独立を m.c. θ_i の i -flat 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 $d+1$ 12 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 $d+1$ の公約数であるような正整数 j が存在するならば, $\theta_j = (m^{t+1})/(m^{t+1}-1)$ を m.c. とする d -flat が存在する.

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

(m^{j+1}) が m.c. にもつ d -flat ならば、 ∇_d は一つの $d(j)$ -flat であるばかりでなく、 $i+1$ が $j+1$ の約数であるようす正整数 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. Θ_i の d -flats のみならず、 Θ_i の約数であるようす Θ_j に対して m.c. Θ_j の $d(j)$ -flats をも含むことがわかる。よって m.c. Θ_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 は次の定理によつて計算される。

[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] :

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

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 (す), $PG(t, m)$ におけるすべての d -flats は m.c. ∇ をもち、 $\eta = \phi(t, d, m) / \nabla$ は 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) と $t+1$ と $d+1$ との最大公約数とするとき、異なる m.c. の個数は $\prod_{i=1}^e (1 + \alpha_i)$ である。今

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

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

とおくと、 $\theta[x_1, \dots, x_e]$ が cycle かつ m.c. をする $d(p_1^{x_1} \cdots p_e^{x_e} - 1)$ -flats の個数はそれ

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

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

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

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 $\eta(x_1, \dots, x_e) = n^*(x_1, \dots, x_e) / \theta[x_1, \dots, x_e]$ 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。

3. $EG(t, m)$ における d -flats

[定義] $GF(m)$ 上の t 次元エーベリッド空間 $EG(t, m)$ 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。2 点 (v) と (u) とは $v=u$ のとき限り同一点である。

(b) $(v_0), (v_1), \dots, (v_d)$ を系数体 $GF(m)$ に関する一次独立な点とするとき、点 $(a_0 v_0 + a_1 v_1 + \cdots + a_d v_d)$ 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 を $\text{GF}(m^t)$ の原始元の一つとすると、次のようを $\text{EG}(t, m)$ 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 による類別に因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、その係数は
 $b_i = b - \phi(t-1, d-1, m) = \phi(t, d, m) - \phi(t-1, d, m) - \phi(t-1, d-1, m)$.

(2) 原点(0)を通る d -flats

原点を通る性質の d -flat (2) $V_d(0) = \{(a_1 x^{b_1} + a_2 x^{b_2} + \dots + a_d x^{b_d})\}$ という形で表わされ、 $\sum_{i=0}^d a_i = 1$ という制約条件は不要となる。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 → 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 に因しては $\text{PG}(t-1, m)$ 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] $(t, d) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_e^{\alpha_e} (> 1, p_i \text{ は } p_i < p_{i+1} \text{ をみたす素数})$ 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. の係数は $\prod_{i=1}^e (1 + \alpha_i)$ である。今

$$\begin{aligned} \theta[x_1, \dots, x_e] &= (m^t - 1)/(m^{p_1^{\alpha_1}} \cdots p_e^{\alpha_e} - 1), & t[x_1, \dots, x_e] &= t/(p_1^{\alpha_1} \cdots p_e^{\alpha_e}), \\ d[x_1, \dots, x_e] &= d/(p_1^{\alpha_1} \cdots p_e^{\alpha_e}), & m[x_1, \dots, x_e] &= m^{p_1^{\alpha_1}} \cdots p_e^{\alpha_e} \end{aligned}$$

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

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

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

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

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

$$\eta(x_1, \dots, x_e) = n^*(x_1, \dots, x_e) / \theta[x_1, \dots, x_e]$$
 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 の構成に関するに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] $\theta[x_1, \dots, x_e] < \nu$ のとき、 $\text{PG}(t, m)$ の任意の2点 (x^α) と (x^β) との
間に次の関係を定義する。

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

生産の点はそれが自身と 0-th associate である。

いゆう点の間に定義されたこれらの関係は association scheme のみ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 $\theta[x_1, \dots, x_e]$ をもつならば、 $PG(t, m)$ における点の全体を treatments, $d(p_1^{x_1} p_2^{x_2} \dots p_e^{x_e} - 1)$ -flats の全体を blocks にとおしては N_2 type (GD type) の PBIBD が得られる。その parameters は次の通りである。

$$v = \phi(t, 0, m), \quad b = \phi(t[x_1, \dots, x_e], d[x_1, \dots, x_e], m[x_1, \dots, x_e]), \\ k = \phi(d, 0, m), \quad r = \lambda_1(x_1, \dots, x_e), \quad \lambda_1 = \lambda_1(x_1, \dots, x_e), \quad \lambda_2 = \lambda_2(x_1, \dots, x_e), \\ n_0 = 1, \quad n_1 = r(x_1, \dots, x_e) - 1, \quad n_2 = r(x_1, \dots, x_e) \{ \theta[x_1, \dots, x_e] - 1 \}, \\ \text{ただし } r(x_1, \dots, x_e) = v / \theta[x_1, \dots, x_e]$$

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

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

[定理 10] 定理 9 で得られた design において、原始元とのべきの指数が $\theta[x_1, \dots, x_e]$ より小さい点のみ treatments (= すれば、) 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II] $\tilde{t} = n(t+1) - 1$, $\tilde{d} = n(d+1) - 1$ とおくとき Design PG($t, m=p^n$): d は Design PG(\tilde{t}, p): \tilde{d} において、 $\text{GF}(p^{\tilde{t}+1})$ の原始元 χ のべきの指數が $\theta = \phi(t, 0, m)$ 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 $\eta(x_1, \dots, x_e)$ による initial d -flats 上の点 $\{(x^{dij} | i=1, 2, \dots, \eta(x_1, \dots, x_e); j=1, 2, \dots, t\} \in \text{各 } \theta[x_1, \dots, x_e] \text{ 每に}$, χ のべきの指數 $\{dij | i=1, 2, \dots, \eta(x_1, \dots, x_e); j=1, 2, \dots, t\}$ で書きかえればよい。EG(t, m)においては $v=v^*+1=m^t$ による点があるから、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 $\infty + a = \infty$ ($a=0, 1, 2, \dots, v-2$) を持つ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 difference sets $\{dij\}$ 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 が 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.