

幾何学的 BIBD の Construction について

海上保安大 福田 悌次郎

1. まえがき

p を素数とすると、ガロア体 $GF(m=p^n)$ 上の有限次元射影空間 $PG(t, m)$ における $d (< t)$ 次元線形部分空間 (d -flat) の全体を考えると $v = \phi(t, 0, m)$, $b = \phi(t, d, m)$, $k = \phi(d, 0, m)$, $r = \phi(t-1, d-1, m)$, $\lambda = \phi(t-2, d-2, m)$ を parameters とする BIBD (今後この design を $PG(t, m):d$ で表わす) が得られるが [2], 我々はこの design を組織的に構成するために, C. R. Rao [4] が導入した cycle の概念を用いて d -flats の構造を明らかにし, d -flats の全体を cycles によって類別した [5].

この小論では, これに関連してその後得られた一, 二の結果について報告する.

$\tilde{t} = n(t+1)-1$, $\tilde{d} = n(d+1)-1$ とおくと design $PG(t, m):d$ は, design $PG(\tilde{t}, p):\tilde{d}$ において cycle $\theta = \phi(t, 0, m)$ の $\tilde{d}$ -flats のみを blocks に, $GF(p^{\tilde{t}+1})$ の原始元 α のべきの指数が θ 未満の点のみを treatments にとることによっても得られるが [5], 直接構成するためには $GF(m^{t+1})$ の minimum function が必要である. しかしながら, $m=p^n$ の場合一般にはその minimum functions は知られてい

ないでその構成法について述べる。

次に, BIBD $PG(t, m):d$ において blocks の一部及び treatments の一部を除いて得られる designs の性質を考察する。

2. $GF(m^{t+1})$ の minimum functions

p を素数とすると, ガロア体 $GF(p^n)$ の minimum functions についても従来ごく僅かしか知られていなかった。ところが Alanen-Knuth [1] は $p < 50$, $p^n < 10^9$ の範囲内で $GF(p^n)$ の minimum functions をすべてリストした。一つの $GF(p^n)$ の minimum functions は後述するように $\varphi(p^n-1)/n$ 個存在するが, そのすべてを網羅した complete table は $p^n < 1024$ までの範囲で与えられ, それ以上の場合については代表的な一つずつが示されている。そこで $GF(p^n)$ の minimum functions が知られている場合にそれらを利用して $GF(m^{t+1})$ (ただし, $m=p^n$) の minimum functions を作る方法について述べる。

[Lemma 1] $GF(m^{t+1})$ の一つの minimum function $g(x)$ の一零点 $\in \alpha$ とすれば

$$g(x) = (x-\alpha)(x-\alpha^m)(x-\alpha^{m^2}) \cdots (x-\alpha^{m^t}). \quad (2.1)$$

(註) $m=p$ のときはよく知られている結果である。

(証) (i) $GF(m)$ を係数域とする任意の多項式を

$$G(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \quad (a_i \in GF(m)) \quad (2.2)$$

とすると

$$[G(x)]^p \equiv a_k^p x^{kp} + a_{k-1}^p x^{(k-1)p} + \cdots + a_1^p x^p + a_0^p \pmod{p}$$

$$[G(x)]^{p^2} = \{[G(x)]^p\}^p \\ \equiv a_k^{p^2} x^{kp^2} + a_{k-1}^{p^2} x^{(k-1)p^2} + \dots + a_1^{p^2} x^{p^2} + a_0^{p^2} \pmod{p}.$$

よって一般に

$$[G(x)]^{p^l} \equiv a_k^{p^l} x^{kp^l} + a_{k-1}^{p^l} x^{(k-1)p^l} + \dots + a_1^{p^l} x^{p^l} + a_0^{p^l} \pmod{p}.$$

特に $l=n$ のとき

$$[G(x)]^m \equiv a_k^m x^{km} + a_{k-1}^m x^{(k-1)m} + \dots + a_1^m x^m + a_0^m \pmod{p}.$$

一方, $a_i \in GF(m)$ for all i だから すべての a_i は, Fermat の定理

により $a_i^m = a_i$ をみたす. よって

$$[G(x)]^m \equiv a_k^m x^{km} + a_{k-1}^m x^{(k-1)m} + \dots + a_1^m x^m + a_0^m = G(x^m) \pmod{p}.$$

したがって一般に

$$[G(x)]^{m^s} \equiv G(x^{m^s}) \pmod{p} \text{ for all positive integer } s \quad (2.3)$$

が成立する.

(ii) $g(x) \in GF(m^{t+1})$ の一つの minimum function とし, $\alpha \in$ その零点の一つとすると, (2.3) から

$$g(\alpha^{m^s}) = p \text{ の倍数} \times [g(x)]^{m^s} = 0 \quad (s=1, 2, \dots, t).$$

即ち, $\alpha, \alpha^m, \alpha^{m^2}, \dots, \alpha^{m^t}$ は $g(x)=0$ の根ですべて異なる.

よって

$$g(x) = (x-\alpha)(x-\alpha^m)(x-\alpha^{m^2}) \dots (x-\alpha^{m^t}). \quad \text{Q.E.D.}$$

[Proposition 1] $f(x) \in GF(p^{n(t+1)})$ の minimum function とし, $\alpha \in$ その零点の一つとすると, $f(x)$ は $GF(m^{t+1})$ の n 個の minimum functions $g_1(x), g_2(x), \dots, g_n(x)$ の積

$$f(x) = g_1(x) g_2(x) \dots g_n(x) \quad (2.4)$$

に分解される。ここに

$$\begin{cases} g_1(x) = (x - \alpha)(x - \alpha^{p^n})(x - \alpha^{p^{2n}}) \cdots (x - \alpha^{p^{tn}}) \\ g_2(x) = (x - \alpha^p)(x - \alpha^{p^{n+1}})(x - \alpha^{p^{2n+1}}) \cdots (x - \alpha^{p^{tn+1}}) \\ \vdots \\ g_n(x) = (x - \alpha^{p^{n-1}})(x - \alpha^{p^{n+(n-1)}})(x - \alpha^{p^{2n+(n-1)}}) \cdots (x - \alpha^{p^{tn+(n-1)}}) \end{cases} \quad (2.5)$$

(証) α は $f(x)$ の零点だから Lemma 1 により, $f(x)$ は

$$f(x) = (x - \alpha)(x - \alpha^p)(x - \alpha^{p^2}) \cdots (x - \alpha^{p^n})(x - \alpha^{p^{n+1}}) \cdots (x - \alpha^{p^{n(t+1)-1}})$$

で与えられる。一方 α は $\text{GF}(p^{n(t+1)})$ の原始元, 即ち, $\alpha^y = 1$ とみれば最小の正整数 y が $y = p^{n(t+1)} - 1 = m^{t+1} - 1$ であるような元であるから, α は $\text{GF}(m^{t+1})$ の原始元でもある。よって α を零点にもつ $\text{GF}(m^{t+1})$

の minimum function を $g_1(x)$ とすると, Lemma 1 により

$$\begin{aligned} g_1(x) &= (x - \alpha)(x - \alpha^m)(x - \alpha^{m^2}) \cdots (x - \alpha^{m^t}) \\ &= (x - \alpha)(x - \alpha^{p^n})(x - \alpha^{p^{2n}}) \cdots (x - \alpha^{p^{tn}}) \end{aligned}$$

である。

同様に, $\text{GF}(p^{n(t+1)})$ の原始元 α^p は $\text{GF}(m^{t+1})$ の原始元でもあるから, α^p を零点にもつ $\text{GF}(m^{t+1})$ の minimum function $g_2(x)$ は

$$g_2(x) = (x - \alpha^p)(x - \alpha^{p^{n+1}})(x - \alpha^{p^{2n+1}}) \cdots (x - \alpha^{p^{tn+1}})$$

以下同様にして定理は証明される。

Q. E. D.

[Remark] $v = (m^{t+1} - 1) / (m - 1)$ とおくと, α^v は $\text{GF}(m)$ の原始元の一つであるから, α^v を零点とする $\text{GF}(m = p^n)$ の minimum function $h(x)$ は

$$h(x) = (x - \alpha^v)(x - \alpha^{p^v}) \cdots (x - \alpha^{p^{n-1}v}) \quad (2.6)$$

で与えられる。

$$\begin{array}{ccccc} & & \alpha: f(x) & & \\ & \nearrow & & \searrow & \\ GF(p) & \xrightarrow{\alpha^v: h(x)} & GF(m=p^n) & \xrightarrow{\alpha: g(x)} & GF(m^{t+1}) \end{array}$$

minimum function $g(x)$ を用いて $GF(m^{t+1})$ の元を, $GF(m)$ の $t+1$ 位の元の組として座標表現する際 $GF(m)$ の元の間の四則演算が問題になるが, その演算を規定するのが この $h(x)$ である。

[Proposition 2] (Aalen - Knuth の Proposition の拡張)

$GF(m^{t+1})$ の minimum functions の位数は $\varphi(m^{t+1}-1)/(t+1)$ である。

ここに $\varphi(m^{t+1}-1)$ は Euler's function で, $m^{t+1}-1 = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g}$ は $m^{t+1}-1$ の素因数分解とすると次式で与えられる。

$$\varphi(m^{t+1}-1) = (m^{t+1}-1) \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_g}\right) \quad (2.7)$$

(証) α を $GF(m^{t+1})$ の原始元のひとつとすると, 次のべき表現が得られる。

$$GF(m^{t+1}) = \{0, \alpha, \alpha^2, \dots, \alpha^{m^{t+1}-1} = 1\}.$$

すると, $\alpha^A \in GF(m^{t+1})$ が原始元であるための必要かつ十分条件は $(A, m^{t+1}-1) = 1$ であることが容易にわかる。よって, これから m^{t+1} 位の元の中で原始元の位数は $m^{t+1}-1$ と互に素であるような A の位数に等しく, それは $\varphi(m^{t+1}-1)$ で与えられる。

一方 β を $GF(m^{t+1})$ の任意の原始元とし, β を零点にもつ minimum function を $g(x)$ とすると Lemma 1 から

$$g(x) = (x-\beta)(x-\beta^m)(x-\beta^{m^2}) \cdots (x-\beta^{m^t}).$$

即ち, $t+1$ 位の原始元 $\beta, \beta^m, \beta^{m^2}, \dots, \beta^{m^t}$ は $g(x)$ の零点である。しか

がって $\varphi(m^{t+1}-1)$ 個の原始元の中の $t+1$ 個ずつは同じ minimum function の零点であるから, minimum functions の個数は $\varphi(m^{t+1})/(t+1)$ である.

Q. E. D

以上の考察により, $GF(p^{n(t+1)})$ の $\varphi(p^{n(t+1)}-1)/n(t+1) = \varphi(m^{t+1})/n(t+1)$ 個の minimum functions がすべて知られている場合には, $GF(m^{t+1})$ のすべての minimum functions を求めることができる.

(例1) $GF(9^2)$ の minimum functions

$f(x)$ として, x^4+x^3+2 をとると

$$f(x) = x^4 + x^3 + 2 \quad \text{in } GF(3^4)$$

$$= (x-\alpha)(x-\alpha^3)(x-\alpha^9)(x-\alpha^{27}),$$

$$g_1(x) = (x-\alpha)(x-\alpha^9) = x^2 - (\alpha + \alpha^9)x + \alpha^{10} \quad \text{in } GF(9^2)$$

$$= x^2 + \alpha^{30}x + \alpha^{10},$$

$$g_2(x) = (x-\alpha^3)(x-\alpha^{27}) = x^2 - (\alpha^3 + \alpha^{27})x + \alpha^{30} \quad \text{in } GF(9^2)$$

$$= x^2 + \alpha^{10}x + \alpha^{30},$$

$$h(x) = (x-\alpha^{10})(x-\alpha^{30}) = x^2 - (\alpha^{10} + \alpha^{30})x + \alpha^{40} \quad \text{in } GF(9^2)$$

$$= x^2 + 2x + 2.$$

よって, $GF(9)$ の元の演算は $\alpha^{20} + 2\alpha^{10} + 2 = 0$ という関係によって規定される.

(例2) $GF(4^4)$ のベキ表現と座標表現

$f(x)$ として, $x^8+x^4+x^3+x^2+1$ をとると

$$f(x) = x^8 + x^4 + x^3 + x^2 + 1 \quad \text{in } GF(2^8)$$

$$= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})(x-\alpha^{32})(x-\alpha^{64})(x-\alpha^{128}),$$

$$g_1(x) = (x-\alpha)(x-\alpha^4)(x-\alpha^{16})(x-\alpha^{64}) \quad \text{in GF}(4^4)$$

$$= x^4 + x^3 + \alpha^{85}x^2 + \alpha^{85}x + \alpha^{85},$$

$$g_2(x) = (x-\alpha^2)(x-\alpha^8)(x-\alpha^{32})(x-\alpha^{128}) \quad \text{in GF}(4^4)$$

$$= x^4 + x^3 + \alpha^{170}x^2 + \alpha^{170}x + \alpha^{170},$$

$$h(x) = (x-\alpha^{85})(x-\alpha^{170}) = x^2 + x + 1 \quad \text{in GF}(4^2)$$

よって $w_1 = \alpha^{85}$, $w_2 = \alpha^{170}$ とおくと

$$\begin{cases} g_1(x) = x^4 + x^3 + w_1x^2 + w_1x + w_1, \\ g_2(x) = x^4 + x^3 + w_2x^2 + w_2x + w_2 \end{cases} \quad \text{ただし, } w_1 + w_2 + 1 = 0.$$

今 $\text{GF}(4^4)$ の minimum function として, $g(x) = x^4 + x^3 + w_1x^2 + w_1x + w_1$ とおくと 次の table が得られる。

Table 1. $\text{GF}(4^4)$ のベキ表現と座標表現

power	x^3	x^2	x	1	power	x^3	x^2	x	1	power	x^3	x^2	x	1	power	x^3	x^2	x	1
①	0	0	0	1	22	w_2	w_2	w_1	w_1	44	w_2	w_1	w_1	w_1	⑥⑥	0	1	w_2	w_1
①	0	0	1	0	②③	0	w_2	w_2	1	45	1	w_2	w_2	1	67	1	w_2	w_1	0
②	0	1	0	0	24	w_2	w_2	1	0	46	w_1	1	w_2	w_1	68	w_1	0	w_1	w_1
3	1	0	0	0	②⑤	0	0	1	1	47	w_2	0	1	w_2	69	w_1	1	1	w_2
4	1	w_1	w_1	w_1	②⑥	0	1	1	0	48	w_2	0	w_1	1	70	w_2	w_1	0	w_2
5	w_2	0	0	w_1	27	1	1	0	0	49	w_2	w_2	0	1	71	1	1	w_1	1
6	w_2	1	w_2	1	②⑧	0	w_1	w_1	w_1	⑤⑩	0	1	0	1	⑦②	0	0	w_2	w_1
7	w_1	w_1	0	1	29	w_1	w_1	w_1	0	51	1	0	1	0	⑦③	0	w_2	w_1	0
⑧	0	w_2	w_1	w_2	③⑩	0	1	w_2	w_2	52	1	w_2	w_1	w_1	74	w_2	w_1	0	0

9	$w_2 w_1 w_2 0$	31	$1 w_2 w_2 0$	53	$w_1 0 0 w_1$	75	$1 1 1 1$
10	$1 w_1 1 1$	32	$w_1 1 w_1 w_1$	54	$w_1 w_2 1 w_2$	(76)	$0 w_2 w_2 w_1$
11	$w_2 w_2 w_2 w_1$	33	$w_2 1 1 w_2$	55	$1 w_1 0 w_2$	77	$w_2 w_2 w_1 0$
(12)	$0 w_1 w_2 1$	34	$w_1 0 w_1 1$	56	$w_2 w_1 1 w_1$	(78)	$0 w_2 1 1$
13	$w_1 w_2 1 0$	35	$w_1 1 w_1 w_2$	57	$1 0 w_2 1$	79	$w_2 1 1 0$
14	$1 w_1 w_2 w_2$	36	$w_2 1 0 w_2$	58	$1 1 w_2 w_1$	80	$w_1 0 1 1$
15	$w_2 1 1 w_1$	37	$w_1 1 w_1 1$	(59)	$0 1 0 w_1$	81	$w_1 w_1 w_1 w_2$
16	$w_1 0 w_2 1$	38	$w_2 1 w_1 w_2$	60	$1 0 w_1 0$	(82)	$0 1 0 w_2$
17	$w_1 0 w_1 w_2$	39	$w_1 w_2 w_1 1$	61	$1 0 w_1 w_1$	83	$1 0 w_2 0$
18	$w_1 1 0 w_2$	40	$1 1 w_1 w_2$	62	$1 0 0 w_1$	84	$1 1 w_1 w_1$
19	$w_2 w_2 0 w_2$	(41)	$0 0 1 w_1$	63	$1 w_1 0 w_1$	85	$0 0 0 w_1$
(20)	$0 1 w_1 1$	(42)	$0 1 w_1 0$	64	$w_2 w_1 0 w_1$	以下略	
21	$1 w_1 1 0$	43	$1 w_1 0 0$	65	$1 1 w_2 1$		

(例3) $v=b=85$, $k=r=21$, $\lambda=5$ の symmetrical BIBD

この design は $PG(3,4):2$ によって与えられる。

$(t+1, d+1)=(4, 3)=1$ だから cycle は $v=85$ だけである。また,

$\gamma=b/v=1$ だから initial 2-flat は k だけである。

そこで initial 2-flat として $V_2(0)=\{(a_0x^0+a_1x^1+a_2x^2)\}$

をとると, $V_2(0)$ 上の点を座標表現した場合 x^3 の係数は 0 であるから

(例2) の Table 1 において第一座標が 0 の点のみを拾えばよい。

かくしてこの design を生成する次の difference set を得る。

$$\{0, 1, 2, 8, 12, 20, 23, 25, 26, 28, 30, 41, 42, 50, 59, 66, 72, 73, 76, 78, 82\} \pmod{85}$$

3. BIBD $PG(t, m)$: d の blocks 及び treatments の一部を
 除いて得られる PBIBD

標記に戻する例として, 任意の一点及びこの点を通るすべての d -flats
 を取り除いて得られる PBIBD や, BIBD $EG(t, m)$: d において原点
 及び原点を通るすべての d -flats を取り除いて得られる PBIBD などが
 知られている [3].

ここでは, cycle の立場から問題を取り上げることとする.

我々は [5] において次の結果を得ている.

(i) 1° $(t+1, d+1) = 1$ ならば $PG(t, m)$ におけるすべての d -flats は
 m.c. ψ をもち, $\eta = \phi(t, d, m) / \psi$ 位の initial flats から生成され
 る.

2° $(t+1, d+1) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_e^{\alpha_e} (> 1)$ ならば $\prod_{i=1}^e (1 + \alpha_i)$ 位の異なる
 m.c. が存在する.

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

$$t[x_1, \dots, x_e] = (t+1) / (p_1^{x_1} \cdots p_e^{x_e}) - 1, \quad (3.1)$$

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

$$m[x_1, \dots, x_e] = m^{p_1^{x_1} \cdots p_e^{x_e}}$$

とあくと, $\theta[x_1, \dots, x_e]$ をそれぞれ cycle 及び m.c. とする d -flats
 の位数はそれぞれ

$$n(x_1, \dots, x_e) = \phi(t[x_1, \dots, x_e], d[x_1, \dots, x_e], m[x_1, \dots, x_e]), \quad (3.2)$$

$$n^*(x_1, \dots, x_e) = n(x_1, \dots, x_e), \quad (3.3)$$

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

である。

(ii) (i)の 2°) の条件の下で, 任意の 2 点 (α^a) と (α^b) とを通る cycle

$\theta[x_1, \dots, x_e]$ の d-flats の個数は

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

$$\lambda_1(x_1, \dots, x_e) = \phi(t[x_1, \dots, x_e]-1, d[x_1, \dots, x_e]-1, m[x_1, \dots, x_e]), \quad (3.4)$$

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

$$\lambda_2(x_1, \dots, x_e) = \phi(t[x_1, \dots, x_e]-2, d[x_1, \dots, x_e]-2, m[x_1, \dots, x_e]) \quad (3.5)$$

で与えられる。

以下, $(t+1, d+1) > 1$ と仮定する。

(1) $PG(t, m): d$ において cycle $\theta[x_1, \dots, x_e] \leq v$ の d-flats をすべて

除いて得られる PBIB D

任意の 2 点 (α^a) と (α^b) とに対して

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

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

任意の点はそれ自身と 0-th associate

の関係にあると定義すると, 次の parameters をもつ N_2 type の PBI

BD が得られる。

$$v = \phi(t, 0, m), \quad b = \phi(t, d, m) - \phi(t[x_1, \dots, x_e], d[x_1, \dots, x_e], m[x_1, \dots, x_e]),$$

$$r = \phi(d, 0, m), \quad r = \phi(t-1, d-1, m) - \lambda_1(x_1, \dots, x_e),$$

$$\lambda_1 = \phi(t-2, d-2, m) - \lambda_1(x_1, \dots, x_e), \quad \lambda_2 = \phi(t-2, d-2, m) - \lambda_2(x_1, \dots, x_e),$$

$$n_1 = r(x_1, \dots, x_e) - 1, \quad n_2 = r(x_1, \dots, x_e) \{ \theta[x_1, \dots, x_e] - 1 \}$$

$$k \nmid v \quad r(x_1, \dots, x_e) = v / \theta[x_1, \dots, x_e]$$

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

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

(2) $PG(t, m): d$ において m.c. $\theta[x_1, \dots, x_e] (< v)$ の d -flats を

blocks に, 原始元 x のべきの指数が $\theta[x_1, \dots, x_e]$ 未満の点を

treatments にとることによって得られる PBIBD

$PG(t, m): d$ において treatments はカットせずに m.c. $\theta[x_1, \dots, x_e]$ の d -flats を blocks とする design も考えられるが, これは標記の PBIBD を $r(x_1, \dots, x_e)$ に対して並べた design であり, $\alpha \equiv \beta \pmod{\theta[x_1, \dots, x_e]}$ のとき (x^α) と (x^β) とは 1st associate の関係にあると定義すると常に繰返し数は集合数 λ_1 に等しくなる. しかし以下 標記の design のみについて考察する.

しかしながら, この design も BIBD $PG(t[x_1, \dots, x_e], m[x_1, \dots, x_e]):$

$d[x_1, \dots, x_e] ([5])$ において m.c. $\tilde{v} = \theta[x_1, \dots, x_e]$ の $d[x_1, \dots, x_e]$ -flats

のみを blocks とする design であるから, 元の BIBD $PG(t, m): d$

において m.c. $v = (m^{t+1} - 1) / (m - 1)$ の d -flats のみを blocks とする

design について論議して一般性を失わない.

(a) $(t+1, d+1) = p^\alpha$ の場合

この場合 m.c.v の d-flats を blocks とする design は $PG(t, m):d$ から cycle $\theta[1] = (m^{t+1}-1)/(m^p-1)$ の d-flats を取り除いて得られるから, (1) の場合に帰着される.

(b) $(t+1, d+1) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell}$ の場合

この場合 異なる m.c. は $\prod_{i=1}^{\ell} (1+\alpha_i)$ 個存在し, これらの m.c. の間の約数関係は極めて複雑である. そこで一般論は別の機会に譲ることにして, ここでは最も簡単な一例をあげるに止める.

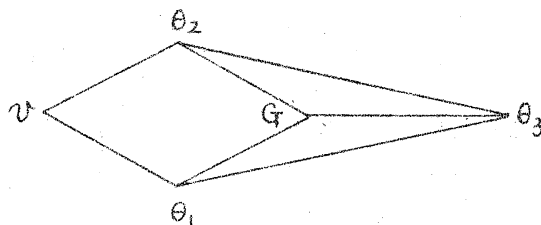
(例4) $(t+1, d+1) = p_1 p_2$ (p_1, p_2 は異なる素数) の場合

$v = (m^{t+1}-1)/(m-1)$, $\theta_1 \equiv \theta[1, 0] = (m^{t+1}-1)/(m^{p_1}-1)$, $\theta_2 \equiv \theta[0, 1] = (m^{t+1}-1)/(m^{p_2}-1)$, $\theta_3 \equiv \theta[1, 1] = (m^{t+1}-1)/(m^{p_1 p_2}-1)$ とおくと, d-flats の m.c. は $v, \theta_1, \theta_2, \theta_3$ の4個である.

これらの m.c. の間には次の関係がある.

θ_1, θ_2 の L.C.M. = v ,

θ_1, θ_2 の G.C.M. = $G = \frac{(m^{p_1 p_2}-1)(m-1)}{(m^{p_1}-1)(m^{p_2}-1)} \theta_3$.



[定義] 任意の2点 (x^α) と (x^β) に対して

$\alpha \equiv \beta \pmod{\theta_1}$

のとき (x^α) と (x^β) とは 1st associate,

$\alpha \equiv \beta \pmod{\theta_2}$

のとき " 2nd associate,

$\alpha \neq \beta \pmod{\theta_1, \theta_2}$, $\alpha \equiv \beta \pmod{G}$ のとき (α) と (β) とは 3rd associate,

$\alpha \neq \beta \pmod{G}$, $\alpha \equiv \beta \pmod{\theta_3}$ のとき " 4-th associate,

$\alpha \neq \beta \pmod{\theta_3}$ のとき " 5-th associate,

任意の点はそれ自身と 0-th associate

の関係にあると定義すると, この関係は association scheme のみたすべき条件を満足することがわかる.

よってこの design は 次の parameters をもつ 5 associate classes の PBIBD である.

$$(i) \quad v = \phi(t, 0, m),$$

$$b = \phi(t, d, m) - \phi(t[1, 0], d[1, 0], m[1, 0]) - \phi(t[0, 1], d[0, 1], m[0, 1]) + \phi(t[1, 1], d[1, 1], m[1, 1]),$$

$$r = \phi(t-1, d-1, m) - \lambda_1(1, 0) - \lambda_1(0, 1) + \lambda_1(1, 1),$$

$$\lambda_1 = \phi(t-2, d-2, m) - \lambda_1(1, 0) - \lambda_2(0, 1) + \lambda_1(1, 1),$$

$$\lambda_2 = \phi(t-2, d-2, m) - \lambda_2(1, 0) - \lambda_1(0, 1) + \lambda_1(1, 1),$$

$$\lambda_3 = \lambda_4 = \phi(t-2, d-2, m) - \lambda_2(1, 0) - \lambda_2(0, 1) + \lambda_1(1, 1),$$

$$\lambda_5 = \phi(t-2, d-2, m) - \lambda_2(1, 0) - \lambda_2(0, 1) + \lambda_2(1, 1),$$

$$n_1 = v/\theta_1 - 1, \quad n_2 = v/\theta_2 - 1, \quad n_3 = v/G - v/\theta_1 - v/\theta_2 + 1 = n_1 n_2,$$

$$n_4 = v/\theta_3 - v/G, \quad n_5 = v - v/\theta_3$$

$$(ii) \quad p_{11}^1 = n_1 - 1, \quad p_{12}^1 = 0, \quad p_{13}^1 = 0, \quad p_{14}^1 = 0, \quad p_{22}^1 = 0,$$

$$p_{11}^2 = 0, \quad p_{12}^2 = 0, \quad p_{13}^2 = n_1, \quad p_{14}^2 = 0, \quad p_{22}^2 = n_2 - 1,$$

$$p_{11}^3 = 0, \quad p_{12}^3 = 1, \quad p_{13}^3 = n_1 - 1, \quad p_{14}^3 = 0, \quad p_{22}^3 = 0,$$

$$p_{11}^4 = 0, \quad p_{12}^4 = 0, \quad p_{13}^4 = 0, \quad p_{14}^4 = n_1, \quad p_{22}^4 = 0,$$

$$\begin{array}{ccccc}
p_{11}^5 = 0, & p_{12}^5 = 0, & p_{13}^5 = 0, & p_{14}^5 = 0, & p_{22}^5 = 0, \\
p_{23}^1 = n_2, & p_{24}^1 = 0, & p_{33}^1 = n_3 - n_2, & p_{34}^1 = 0, & p_{44}^1 = n_4, \\
p_{23}^2 = 0, & p_{24}^2 = 0, & p_{33}^2 = n_3 - n_1, & p_{34}^2 = 0, & p_{44}^2 = n_4, \\
p_{23}^3 = n_2 - 1, & p_{24}^3 = 0, & p_{33}^3 = n_3 - n_2 - n_1 + 1, & p_{34}^3 = 0, & p_{44}^3 = n_4, \\
p_{23}^4 = 0, & p_{24}^4 = n_2, & p_{33}^4 = 0, & p_{34}^4 = n_3, & p_{44}^4 = n_4 - n_1 - n_2 - n_3 - 1, \\
p_{23}^5 = 0, & p_{24}^5 = 0, & p_{33}^5 = 0, & p_{34}^5 = 0, & p_{44}^5 = 0.
\end{array}$$

(註) 一般に, Association scheme の第三の条件(3) は次の条件:

- (3') $m \left[\binom{m-1}{2} + m - 1 \right]$ 個の p_{jrk}^i ($i=1, 2, \dots, m$; $j, k=1, 2, \dots, m-1$) が i -th associate の関係にある treatment pair (α, β) の選べ方に無関係で、かつ、 $j \neq k$ なる $m \binom{m-1}{2}$ 個の p_{jrk}^i について
- $$p_{jrk}^i = p_{rkj}^i \quad (i=1, 2, \dots, m) \text{ である.}$$

と同値であることが容易に示される。

(例4)において $p_{jrk}^i = p_{rkj}^i$ は定義より明らかであるから、第二種の parameters は上記のものについて調べれば十分である。

参考文献

- [1] Alanen, J.D. and Knuth, D.E. (1964). Tables of finite fields.
Sankhyā Ser.A 26 305-323.
- [2] Bose, R.C. (1939). On the construction of balanced incomplete
block designs. Ann. Eugenics 9 353-399.
- [3] Chakrabarti, M.C. (1962). Mathematics of design and analysis
of experiments. Asia publishing House, Bombay.
- [4] Rao, C.R. (1945). Finite geometries and certain derived resul-
ts in theory of numbers. Proc. Nat. Inst. Sci.
India 11 136-149.
- [5] Yamamoto, S., Fukuda, T. and Hamada, N. (1966). On finite geomet-
ries and cyclically generated incomplete block des-
igns. J. Sci. Hiroshima Univ. Ser.A-1 30 137-149.