J. Sci. Hiroshima Univ. Ser. A-I
30 (1966), 137-149

On Finite Geometries and Cyclically Generated Incomplete Block Designs

Sumiyasu Yamamoto, Teijiro Fukuda and Noboru Hamada

(Received September 20, 1966)

1. Introduction

C. R. Rao [3], [4] generalized certain theorems known as the difference theorems of R. C. Bose [1] and derived a method of constructing difference sets which cyclically generate balanced incomplete block (BIB) designs. The main results were derived with the help of a compact representation of d dimensional linear subspaces (flats) in a $t(>d)$ dimensional finite projective space and also in Euclidean space. The notion of the cycle of a flat was introduced there in order to investigate the structure of the family of flats and the following general propositions were conjectured:

Proposition 1 (Rao) *In* PG(t, m), *if* $r_1, r_2, \cdots, r_p$ *are integers such that*

(a) $0<r_1<r_2<\cdots<r_p<t$,

(b) $(m^{d+1}-1)/(m^{r_i+1}-1)=s_i$ *integral for all* i,

(c) $(d+1)/(r_i+1)=t_i$ *integral for all* i,

(d) $(r_{i+1}+1)/(r_i+1)=l_i$ *integral for all* i,

(e) $(m^{t+1}-1)/(m^{r_i+1}-1)=\theta_i$ *integral for all* i,

then there are

$$y_i=(n_i-n_{i+1})/\theta_i \quad where \quad n_i=\binom{\theta_i}{t_i}\Big/\binom{s_i}{t_i}$$

initial flats of cycle θ_i $(i=1, 2, \cdots, p)$ *and*

$$\eta=(b-n_1)/v$$

initial flats of cycle v *from which the totality of the* d*-flats can be generated.*

Proposition 2 (Rao) *In* EG(t, m), *if* $h=p_0p_1^{i_1}p_2^{i_2}\cdots$ $(p_0=1$ *and* p*'s are primes such that* $p_i<p_{i+1})$ *is the highest common factor* (H.C.F.) *of* d *and* t, *then the* d*-flats passing through the origin* (0) *will have cycles of the form* $\theta_{js}=(m^t-1)/(m^{r_{js}}-1)$ *where*

$$r_{js}=p_1^{i_1}p_2^{i_2}\cdots p_j^s \qquad (j=0, 1, \cdots;\ s=0, 1, \cdots, i_j).$$

The number of initial flats from which all flats of cycle θ_{js} can be generated is given by

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

where n_{js} is the number of d-flats that can be generated from θ_{js} flats of dimensions having

$$n_{js}=\binom{\theta_{js}}{d/r_{js}}\Big/\binom{q_{js}}{d/r_{js}}$$

where $q_{js}=(m^d-1)/(m^{r_{js}}-1)$.

These conjectures, however, are not valid except some special cases. One of the purposes of this paper is to correct these general conjectures. Another is to show that we can obtain a PBIB design by considering only a sub-family of all d-flats having a cycle θ and that we can obtain a BIB design by taking up a part of points in each of the d-flats having the cycle θ. These considerations show that any BIB design constructed by all d-flats in PG$(t, m=p^n)$ can be obtained by considering a certain sub-family of $\tilde{d}$-flats in PG$(\tilde{t}, p)$ and taking up a part of points in each of these $\tilde{d}$-flats, where $\tilde{t}=n(t+1)-1$ and $\tilde{d}=n(d+1)-1$.

2. *d*-flats in PG(*t*, *m*)

With the help of the Galois field GF(m) where m is an integer of the form p^n (p being a prime), we can define a finite projective geometry PG(t, m) of t-dimensions as a set of points satisfying the following conditions (a), (b) and (c):

(a) A point in PG(t, m) is represented by (ν) where ν is a non-zero element of GF(m^{t+1}).

(b) Two points (ν) and (μ) represent the same point when and only when there exists an element $\sigma(\neq 0)$ of GF(m) such that $\mu=\sigma\nu$.

(c) A d-flat in PG(t, m) is defined as a set of points

$$\{(a_0\nu_0+a_1\nu_1+\cdots+a_d\nu_d)\}$$

where a's run independently over the elements of GF(m) and are not all simultaneously zero and $(\nu_0), (\nu_1), \cdots, (\nu_d)$ are linearly independent over the coefficient field GF(m), that is, they do not lie on a $(d-1)$-flat.

It is known that the geometry defined above satisfies the postulates of Veblen and Bussey for a finite projective geometry [6].

In GF(m^{t+1}), there exists an element x called primitive such that every non-zero element of GF(m^{t+1}) can be represented by x^k $(k=0, 1, \cdots, m^{t+1}-2)$. It satisfies an irreducible equation of the $(t+1)$st degree in GF(m):

$$x^{t+1}+a_tx^t+\cdots+a_1x+a_0=0. \tag{2.1}$$

The function $f(x)=x^{t+1}+a_t x^t+\cdots+a_1 x+a_0$ is called a minimum function [1], [3]. Each element of $\mathrm{GF}(m^{t+1})$ can also be represented by a polynomial over $\mathrm{GF}(m) \bmod f(x)$. Thus any element of $\mathrm{GF}(m^{t+1})$ can be represented either as a power of the primitive element x or a polynomial of degree less than $t+1$. If

$$x^k \equiv b_t x^t + b_{t-1}x^{t-1}+\cdots+b_0 \qquad (\bmod f(x))$$

then, the correspondence (x^k) as a point represented by a power of x and $(b_t, b_{t-1}, \cdots, b_0)$ as a point represented by an ordered set of the elements of $\mathrm{GF}(m)$ is unique.

When $(t+1)/(i+1)$ is integral for some non-negative integer i, $m^{i+1}-1$ is the least integer u satisfying $(x^\theta)^u=1$ where $\theta=(m^{t+1}-1)/(m^{i+1}-1)$. Thus, x^θ is one of the primitive elements of $\mathrm{GF}(m^{i+1})$. $\mathrm{GF}(m^{i+1})$ can, therefore, be represented as

$$\mathrm{GF}(m^{i+1})=\{0,\ x^0,\ x^\theta,\ \cdots,\ x^{(m^{i+1}-2)\theta}\}. \tag{2.2}$$

Thus, we have

$$\mathrm{PG}(i,\ m)=\{(x^0),\ (x^\theta),\ \cdots,\ (x^{[(m^{i+1}-1)/(m-1)-1]\theta})\}. \tag{2.3}$$

In particular,

$$\mathrm{GF}(m)=\{0,\ x^0,\ x^v,\ \cdots,\ x^{(m-2)v}\}, \tag{2.2$'$}$$

$$\mathrm{PG}(t,\ m)=\{(x^0),\ (x^1),\ (x^2),\ \cdots,\ (x^{v-1})\} \tag{2.3$'$}$$

where $v=(m^{t+1}-1)/(m-1)$.

Among the points in $\mathrm{PG}(i,\ m)$, the beginning $i+1$ points (x^0), (x^θ), $\cdots$, $(x^{i\theta})$ are linearly independent over the coefficient field $\mathrm{GF}(m)$ and the totality of linear combinations of these points is $\mathrm{PG}(i,\ m)$.

Let us consider a d-flat $\mathrm{V}_d(0)$ in $\mathrm{PG}(t,\ m)$ passing through a set of linearly independent $d+1$ points (x^{b_0}), (x^{b_1}), $\cdots$, (x^{b_d}):

$$\mathrm{V}_d(0)=\{(a_0 x^{b_0}+a_1 x^{b_1}+\cdots+a_d x^{b_d})\}$$

and a d-flat

$$\mathrm{V}_d(c)=\{(a_0 x^{b_0+c}+a_1 x^{b_1+c}+\cdots+a_d x^{b_d+c})\}$$

for an integer c. For some positive integer c, $\mathrm{V}_d(c)$ coincides with $\mathrm{V}_d(0)$. Such an integer c is called a cycle of the initial flat $\mathrm{V}_d(0)$ by Rao. Since $\mathrm{V}_d(v)=\mathrm{V}_d(0)$, v is a cycle of any d-flat $\mathrm{V}_d(0)$. To secure the clarity of description we call the minimum value of these cycles the minimum cycle (*m.c.*) of $\mathrm{V}_d(0)$.

The following properties are known as the immediate consequences of the definition of the cycle [3].

(i) If θ is the *m.c.*, then it is a factor of any cycle c and therefore a factor of v.

(ii) All points on a d-flat of the $m.c.$ θ are given by (recording only powers of x's)

$$\begin{matrix} c_0, & c_0+\theta, & \cdots, & c_0+(r-1)\theta, \\ c_1, & c_1+\theta, & \cdots, & c_1+(r-1)\theta, \\ \vdots & \vdots & & \vdots \\ c_q, & c_q+\theta, & \cdots, & c_q+(r-1)\theta \end{matrix} \tag{2.4}$$

where $c_i-c_j \not\equiv 0 \pmod{\theta}$ $(i\neq j;\ i, j=0, 1, 2, \cdots, q)$, $r=v/\theta$.

(iii) A necessary condition for the existence of a d-flat having the $m.c.$ $\theta(<v)$ is that $v=\phi(t, 0, m)$, the number of points in $\mathrm{PG}(t, m)$, and $\phi(d, 0, m)$, the number of points on a d-flat, are not relatively prime, where

$$\phi(t, d, m)=\frac{(m^{t+1}-1)(m^t-1)\cdots(m^{t-d+1}-1)}{(m^{d+1}-1)(m^d-1)\cdots(m-1)} \tag{2.5}$$

is the number of d-flats in $\mathrm{PG}(t, m)$ [1].

(iv) If θ is the $m.c.$ of a d-flat, a d-flat with the points obtained by adding an integer $k(k=1, 2, \cdots, \theta-1)$ to all the powers of x's in (2.4) has the same $m.c.$ θ. Accordingly, we assume in the following that $c_0=0$ in the initial flat from which θ different flats $\mathrm{V}_d(0)$, $\mathrm{V}_d(1)$, $\cdots$, $\mathrm{V}_d(\theta-1)$ can be generated.

THEOREM 2.1 *If* $\theta_i=(m^{t+1}-1)/(m^{i+1}-1)$ *is integral, then* $\mathrm{V}_i(0)=\{(a_0x^0+a_1x^{\theta_i}+\cdots+a_ix^{i\theta_i})\}$ *is an i-flat of the m.c.* θ_i.

Note that $(m^{t+1}-1)/(m^{i+1}-1)$ is integral if and only if $(t+1)/(i+1)$ is integral.

PROOF Since θ_i is integral, x^{θ_i} is a primitive element of $\mathrm{GF}(m^{i+1})$. Hence

$$\mathrm{PG}(i, m)=\{(x^0), (x^{\theta_i}), \cdots, (x^{i\theta_i}), \cdots, (x^{[(m^{i+1}-1)/(m-1)-1]\theta_i})\}.$$

As mentioned earlier, the beginning $i+1$ points $(x^0), (x^{\theta_i}), \cdots, (x^{i\theta_i})$ are linearly independent over the coefficient field $\mathrm{GF}(m)$ and the totality of linear combinations of these points is $\mathrm{PG}(i, m)$. This shows that $\mathrm{V}_i(0)=\{(a_0x^0+a_1x^{\theta_i}+\cdots+a_ix^{i\theta_i})\}$ is an i-flat of the $m.c.$ θ_i in $\mathrm{PG}(t, m)$.

THEOREM 2.2 *If a d-flat* V_d *has a cycle less than v, then there exists a positive integer j such that* $j+1$ *is a common factor of* $t+1$ *and* $d+1$ *and that* $\theta=(m^{t+1}-1)/(m^{j+1}-1)$ *is the m.c. of* V_d.

In this case, the flat V_d *is composed of* $(m^{d+1}-1)/(m^{j+1}-1)$ *flats each of which belongs to a set of* θ *j-flats* $\mathrm{V}_j(0)$, $\mathrm{V}_j(1)$, $\cdots$, $\mathrm{V}_j(\theta-1)$ *generated from the initial j-flat* $\mathrm{V}_j(0)=\{(a_0x^0+a_1x^{\theta}+\cdots+a_jx^{j\theta})\}$ *of the m.c.* θ.

PROOF. Let the $m.c.$ of V_d be θ. By the property (ii) of the cycle, all powers of points on V_d are given by

$$\begin{array}{cccc} 0, & \theta, \cdots, & j\theta, \cdots, & (r-1)\theta, \\ c_1, & c_1+\theta, \cdots, & c_1+j\theta, \cdots, & c_1+(r-1)\theta, \\ \vdots & \vdots & \vdots & \vdots \\ c_q, & c_q+\theta, \cdots, & c_q+j\theta, \cdots, & c_q+(r-1)\theta \end{array}$$

where $r=v/\theta$. There exists some integer j such that $(x^0), (x^\theta), \cdots, (x^{j\theta})$ are linearly independent and that $(x^{(j+1)\theta})$ is represented by a linear combination of these $j+1$ points. Then, $V_j(0)=\{(a_0x^0+a_1x^\theta+\cdots+a_jx^{j\theta})\}$ is a j-flat and θ is one of the cycles of $V_j(0)$. If (x^c) belongs to $V_j(0)$, $(x^{c+k\theta})$ does for any integer k. If (x^b) is any point on V_d, it follows that (x^{c+b}) is also a point on V_d. Hence, if $(x^0), (x^\theta), \cdots, (x^{j\theta}), (x^{b_1}), \cdots, (x^{b_{d-j}})$ are basis points of V_d, then (x^c), $(x^{c+\theta}), \cdots, (x^{c+j\theta}), (x^{c+b_1}), \cdots, (x^{c+b_{d-j}})$ are also basis points of V_d. This shows that c is a cycle of V_d. Since θ is the *m.c.* of V_d, c must be a multiple of θ and all points on $V_j(0)$ are represented by $(x^0), (x^\theta), \cdots, (x^{j\theta}), \cdots, (x^{(r-1)\theta})$. As the number of points on $V_j(0)$ is $(m^{j+1}-1)/(m-1)$, $\theta=v/r=(m^{t+1}-1)/(m^{j+1}-1)$ and $j+1$ is a factor of $t+1$. Since the flat V_d is composed of $q+1$ j-flats $V_j(0)$, $V_j(c_1), \cdots, V_j(c_q)$ having the *m.c.* θ, $q+1=\phi(d, 0, m)/\phi(j, 0, m)=(m^{d+1}-1)/(m^{j+1}-1)$ is integral and $j+1$ is a factor of $d+1$.

When $i+1$ is a common factor of $t+1$ and $d+1$, the flat $V_i(0)=\{(a_0x^0+a_1x^{\theta_i}+\cdots+a_ix^{i\theta_i})\}$ is an i-flat of the *m.c.* $\theta_i=(m^{t+1}-1)/(m^{i+1}-1)$ from which i-flats $V_i(0), V_i(1), \cdots, V_i(\theta_i-1)$ having the same *m.c.* θ_i are generated. Among these θ_i flats, we can choose $d_i+1=\dfrac{d+1}{i+1}$ flats such that all basis points of these i-flats i.e., $d+1=(i+1)(d_i+1)$ points, are linearly independent. The linear combinations of these $d+1$ points generate a d-flat having the cycle θ_i. We denote such a d-flat by a '$d(i)$-flat' and call it a d-flat which is generated by d_i+1 linearly independent i-flats of the *m.c.* θ_i. When the generating flats degenerate into $d+1$ points in PG(t, m), i.e., $i=0$, we denote the d-flat by a $d(0)$-flat.

The following corollary can easily be proved.

Corollary. *A d-flat having the minimum cycle θ less than v is a $d(j)$-flat for some positive integer j.*

Theorem 2.3 (1) *A d-flat having the minimum cycle v always exists.*

(2) *If there exists a positive integer j such that $j+1$ is a common factor of $t+1$ and $d+1$, there exists a d-flat having the m.c. $\theta_j=(m^{t+1}-1)/(m^{j+1}-1)$ less than v.*

Proof. (1) Since $t+1$ points $(x^0), (x^1), \cdots, (x^t)$ are linearly independent, $V_d=\{(a_0x^0+a_1x^1+\cdots+a_dx^d)\}$ is a d-flat. It can be shown that the *m.c.* of the flat is not less than v.

(2) Let $t_j+1=\dfrac{t+1}{j+1}$ and $d_j+1=\dfrac{d+1}{j+1}$. If x is one of the primitive elements of $\mathrm{GF}(m^{t+1})$, it is also a primitive element of $\mathrm{GF}((m^{j+1})^{t_j+1})$ and the beginning t_j+1 points $(x^0), (x^1), (x^2), \cdots, (x^{t_j})$ in $\mathrm{PG}(t_j, m^{j+1})$ are linearly independent over the coefficient field $\mathrm{GF}(m^{j+1})$. Thus, if we choose a special set of d_j+1 flats $\mathrm{V}_j(0), \mathrm{V}_j(1), \cdots, \mathrm{V}_j(d_j)$ from θ_j j-flats of the *m.c.* θ_j, we can verify that these d_j+1 flats are linearly independent and that the $d(j)$-flat generated by these has the *m.c.* θ_j.

THEOREM 2.4 *If $j+1$ is a common factor of $t+1$ and $d+1$, and if a d-flat V_d has the m.c. $\theta_j=(m^{t+1}-1)/(m^{j+1}-1)$, then the d-flat V_d is regarded to be not only a $d(j)$-flat but also a $d(i)$-flat for any non-negative integer i such that either $i+1$ is a factor of $j+1$ or $i=0$.*

PROOF. As mentioned in the corollary to the Theorem 2.2, V_d is a $d(j)$-flat generated by linearly independent d_j+1 j-flats $\mathrm{V}_j(c_0), \mathrm{V}_j(c_1), \cdots, \mathrm{V}_j(c_{d_j})$. All points on any component j-flat $\mathrm{V}_j(c_l)$ are given by (recording only powers of x's)

$$c_l,\ c_l+\theta_j,\ \cdots,\ c_l+(r_j-1)\theta_j$$

where $r_j=(m^{j+1}-1)/(m-1)$.
These points can be decomposed into k groups as:

$$\begin{array}{llll}
1) & c_l, & c_l+\theta_i, & \cdots,\ c_l+(r_i-1)\theta_i \\
2) & c_l+\theta_j, & c_l+\theta_i+\theta_j, & \cdots,\ c_l+(r_i-1)\theta_i+\theta_j \\
\vdots & \vdots & \vdots & \vdots \\
k) & c_l+(k-1)\theta_j, & c_l+\theta_i+(k-1)\theta_j, & \cdots,\ c_l+(r_i-1)\theta_i+(k-1)\theta_j
\end{array}$$

for any i satisfying the assumption, where $\theta_i=(m^{t+1}-1)/(m^{i+1}-1)=k\theta_j$, $k=(m^{j+1}-1)/(m^{i+1}-1)$ and $r_i=(m^{i+1}-1)/(m-1)$.

Since each group is an i-flat having the *m.c.* θ_i, $\mathrm{V}_j(c_l)$ is decomposed into k i-flats of the *m.c.* θ_i, $\mathrm{V}_i(c_l), \mathrm{V}_i(c_l+\theta_j), \cdots, \mathrm{V}_i(c_l+(k-1)\theta_j)$. Thus the d-flat V_d is a $d(i)$-flat for any i satisfying the assumption.

These theorems show that the totality of $d(i)$-flats contains not only $d(i)$-flats of the *m.c.* θ_i but also $d(j)$-flats of the *m.c.* θ_j for any integer j such that θ_j is a factor of θ_i.

Hence, the number n_i^* of $d(i)$-flats having the *m.c.* θ_i is given by subtracting all the numbers n_j^* of such $d(j)$-flats from the number n_i of $d(i)$-flats.

The number n_i is given by the following theorem.

THEOREM 2.5 *The number of $d(i)$-flats is*

$$n_i=\phi(t_i, d_i, m^{i+1}) \tag{2.6}$$

where $t_i=\dfrac{t+1}{i+1}-1$ *and* $d_i=\dfrac{d+1}{i+1}-1.$

Proof. The number of such d-flats can be enumerated as follows. The first i-flat can be chosen in θ_i ways, the second in θ_i-1 ways, the third in $\theta_i-\dfrac{m^{2(i+1)}-1}{m^{i+1}-1}$ ways and so on. The total number of ways of choosing d_i+1 linearly independent i-flats is

$$\psi(\theta_i)=\theta_i(\theta_i-1)\left(\theta_i-\frac{m^{2(i+1)}-1}{m^{i+1}-1}\right)\cdots\left(\theta_i-\frac{m^{d_i(i+1)}-1}{m^{i+1}-1}\right).$$

While, each d-flat is composed of $s_i=(m^{d+1}-1)/(m^{i+1}-1)$ i-flats and can be generated by any one of $\psi(s_i)=s_i(s_i-1)\left(s_i-\dfrac{m^{2(i+1)}-1}{m^{i+1}-1}\right)\cdots\left(s_i-\dfrac{m^{d_i(i+1)}-1}{m^{i+1}-1}\right)$ sets of d_i+1 independent i-flats. Hence the number of $d(i)$-flats having the cycle θ_i is given by

$$\begin{aligned} n_i&=\frac{\psi(\theta_i)}{\psi(s_i)}=\frac{(M_i^{t_i+1}-1)(M_i^{t_i}-1)\cdots(M_i^{t_i-d_i+1}-1)}{(M_i^{d_i+1}-1)(M_i^{d_i}-1)\cdots(M_i-1)}\\ &=\phi(t_i,\ d_i,\ M_i)\end{aligned}$$

where $M_i=m^{i+1}$.

Now we have the following general theorem.

Theorem 2.6

(1) *If* $t+1$ *and* $d+1$ *are relatively prime, then all* d*-flats in* PG(t, m) *have the minimum cycle* v *and can be generated from* $\eta=\phi(t,\ d,\ m)/v$ *initial* d*-flats.*

(2) *If* $(t+1,\ d+1)=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_l^{\alpha_l}(>1,$ *p's are primes such that* $p_i<p_{i+1})$ *is the* H.C.F. *of* $t+1$ *and* $d+1$, *then the number of different minimum cycles is* $\prod_{i=1}^{l}(1+\alpha_i)$. *Let*

$$\begin{aligned} &\theta[x_1,\ \cdots,\ x_l]=(m^{t+1}-1)/(m^{p_1^{x_1}\cdots p_l^{x_l}}-1),\\ &t[x_1,\ \cdots,\ x_l]=(t+1)/(p_1^{x_1}\cdots p_l^{x_l})-1,\\ &d[x_1,\ \cdots,\ x_l]=(d+1)/(p_1^{x_1}\cdots p_l^{x_l})-1,\\ &m[x_1,\cdots,\ x_l]=m^{p_1^{x_1}\cdots p_l^{x_l}}.\end{aligned}\tag{2.7}$$

Then the numbers of $d(p_1^{x_1}\cdots p_l^{x_l}-1)$*-flats having the the cycle* $\theta[x_1,\ \cdots,\ x_l]$ *and the m.c.* $\theta[x_1,\ \cdots,\ x_l]$ *are respectively*

$$n(x_1,\ \cdots,\ x_l)=\phi(t[x_1,\ \cdots,\ x_l],\ d[x_1,\ \cdots,\ x_l],\ m[x_1,\ \cdots,\ x_l]),\tag{2.8}$$

$$\begin{aligned} &n^*(\alpha_1,\ \cdots,\ \alpha_l)=n(\alpha_1,\ \cdots,\ \alpha_l),\\ &n^*(x_1,\ \cdots,\ x_l)=n(x_1,\ \cdots,\ x_l)\ -\sum_{x_j\le y_j\le\alpha_j;\ \exists j,\, x_j<y_j} n^*(y_1,\ \cdots,\ y_l).\end{aligned}\tag{2.9}$$

The number of initial d-flats of any m.c. $\theta[x_1, \cdots, x_l]$ *is*

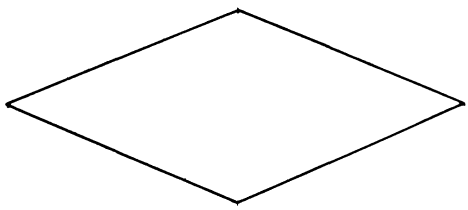
$$\eta(x_1, \cdots, x_l)=n^*(x_1, \cdots, x_l)/\theta[x_1, \cdots, x_l], \tag{2.10}$$

from which the totality of d-flats having the m.c. $\theta[x_1, \cdots, x_l]$ *can be generated.*
The following is an example of our results.

EXAMPLE 1 Let us consider 5-flats in PG(11, m). There are 4 *m.c.* $\theta[0, 0]$ $(=v)$, $\theta[1, 0]$, $\theta[0, 1]$ and $\theta[1, 1]$. The relation between these is as follows.

$$\theta[1, 0]=\frac{m^{12}-1}{m^2-1}$$

$$v=\frac{m^{12}-1}{m-1}$$



$$\theta[1, 1]=\frac{m^{12}-1}{m^6-1}$$

$$\theta[0, 1]=\frac{m^{12}-1}{m^3-1}$$

The number of initial 5-flats of the *m.c.* $\theta[x_1, x_2]$ is as follows:

(1) $n^*(1, 1)=\phi(1, 0, m^6)=m^6+1$, $\theta[1, 1]=m^6+1$,
$\eta(1, 1)=n^*(1, 1)/\theta[1, 1]=1$.

(2) $n^*(0, 1)=\phi(3, 1, m^3)-n^*(1, 1)=m^3(m^6+1)(m^3+1)$, $\theta[0, 1]=(m^6+1)(m^3+1)$,
$\eta(0, 1)=n^*(0, 1)/\theta[0, 1]=m^3$.

(3) $n^*(1, 0)=\phi(5, 2, m^2)-n^*(1, 1)=m^2(m^6+m^2+1)(m^6+1)(m^4+m^2+1)$,
$\theta[1, 0]=(m^6+1)(m^4+m^2+1)$,
$\eta(1, 0)=n^*(1, 0)/\theta[1, 0]=m^2(m^6+m^2+1)$.

(4)
$$\begin{aligned} n^*(0, 0)&=\phi(11, 5, m)-n^*(1, 0)-n^*(0, 1)-n^*(1, 1)\\ &=m(m^{24}+m^{22}+m^{21}+2m^{20}+2m^{19}+4m^{18}+2m^{17}+5m^{16}+4m^{15}+6m^{14}\\ &\quad+4m^{13}+8m^{12}+3m^{11}+7m^{10}+4m^9+6m^8+2m^7+6m^6+4m^4+m^3\\ &\quad+m^2+1)(m^{11}+m^{10}+\cdots+m+1), \end{aligned}$$
$\theta[0, 0]=m^{11}+m^{10}+\cdots+m+1$,
$\eta(0, 0)=n^*(0, 0)/\theta[0, 0]=m(m^{24}+m^{22}+m^{21}+2m^{20}+\cdots+4m^4+m^3+m^2+1)$.

3. *d*-flats in EG(t, m)

The Euclidean geometry of t-dimensions, denoted by EG(t, m), is a set of points which satisfy the following two conditions:

(a) A point is represented by (ν) where ν is an element of $GF(m^t)$, each element representing a unique point.

(b) A d-flat is defined as a set of points

$$\{(a_0\nu_0+a_1\nu_1+\cdots+a_d\nu_d)\}$$

where (ν_0), (ν_1), $\cdots$, (ν_d) are linearly independent over the coefficient field $GF(m)$ and a's run over the elements of $GF(m)$ subject to the restriction $\sum_{i=0}^{d} a_i=1$.

$EG(t, m)$ is derivable from $PG(t, m)$ by cutting out one $(t-1)$-flat and all points lying on it. From this, the number of d-flats in $EG(t, m)$ is given by

$$b=\phi(t, d, m)-\phi(t-1, d, m). \tag{3.1}$$

If x is a primitive element of $GF(m^t)$, then we have the following representation of $EG(t, m)$ by the power cycle of x:

$$EG(t, m)=\{(0), (x^0), (x^1), \cdots, (x^{m^t-2})\}. \tag{3.2}$$

In $EG(t, m)$, $v^*=m^t-1$ is a cycle of any d-flat. As to the classification of d-flats in $EG(t, m)$ with respect to their minimum cycles, the following two cases must be considered.

(1) The d-flats not passing through the origin (0).

The number of such d-flats is given by

$$\begin{aligned} b_1&=b-\phi(t-1, d-1, m)\\ &=\phi(t, d, m)-\phi(t-1, d, m)-\phi(t-1, d-1, m). \end{aligned} \tag{3.3}$$

Furthermore, it is easy to see that any flat not passing through the point (0) has the cycle $v^*=m^t-1$ and has no cycles less than v^*.

(2) The d-flats passing through the origin (0).

Any d-flat is given in the form

$$V_d(0)=\{(a_1x^{b_1}+a_2x^{b_2}+\cdots+a_dx^{b_d})\} \tag{3.4}$$

and the restriction $\sum_{i=0}^{d} a_i=1$ need not be imposed. Let $\theta=(m^t-1)/(m-1)$, then all d-flats passing through (0) have θ as one of their cycles. A set of d-flats passing through (0) in $EG(t, m)$ has, therefore, the same structure as a set of $(d-1)$-flats in $PG(t-1, m)$.

The following theorem is an immediate consequence of the Theorem 2.6.

THEOREM 3.1 *If* $(t, d)=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_l^{\alpha_l}$ $(>1$, *p's are primes such that* $p_i<p_{i+1})$ *is the* H.C.F. *of* t *and* d, *then the number of different minimum cycles of d-flats passing through the origin* (0) *is* $\prod_{i=1}^{l}(1+\alpha_i)$.

Let

$$\begin{aligned} &\theta[x_1, \cdots, x_l]=(m^t-1)/(m^{p_1^{x_1}\cdots p_l^{x_l}}-1), \\ &t[x_1, \cdots, x_l]=t/(p_1^{x_1}\cdots p_l^{x_l}), \\ &d[x_1, \cdots, x_l]=d/(p_1^{x_1}\cdots p_l^{x_l}), \\ &m[x_1, \cdots, x_l]=m^{p_1^{x_1}\cdots p_l^{x_l}}. \end{aligned} \tag{3.5}$$

Then the number of $d(p_1^{x_1}\cdots p_l^{x_l})$-flats having the cycle $\theta[x_1, \cdots, x_l]$ and the minimum cycle $\theta[x_1, \cdots, x_l]$ are respectively

$$n(x_1, \cdots, x_l)=\phi(t[x_1, \cdots, x_l]-1,\ d[x_1, \cdots, x_l]-1,\ m[x_1, \cdots, x_l]), \tag{3.6}$$

$$\begin{aligned} &n^*(\alpha_1, \cdots, \alpha_l)=n(\alpha_1, \cdots, \alpha_l), \\ &n^*(x_1, \cdots, x_l)=n(x_1, \cdots, x_l)\ -\sum_{x_j\le y_j\le\alpha_j;\ \exists j, x_j<y_j} n^*(y_1, \cdots, y_l). \end{aligned} \tag{3.7}$$

The number of initial d-flats of the m.c. $\theta[x_1, \cdots, x_l]$ is

$$\eta(x_1, \cdots, x_l)=n^*(x_1, \cdots, x_l)/\theta[x_1, \cdots, x_l] \tag{3.8}$$

from which the totality of d-flats having the m.c. $\theta[x_1, \cdots, x_l]$ in EG(t, m) *can be generated.*

4. Construction of cyclically generated designs

The following theorems concerning the construction of cyclically generated designs can be derived from the cyclic structure of d-flats in PG(t, m).

THEOREM 4.1 *Under the assumption* (2) *of Theorem* 2.6, *the number of $d(p_1^{x_1}\cdots p_l^{x_l}-1)$-flat of the cycle $\theta[x_1, \cdots, x_l]$ passing through a given point pair (x^α) and (x^β) is*

$$\begin{aligned} &\lambda_1(x_1, \cdots, x_l)=\phi(t[x_1, \cdots, x_l]-1,\ d[x_1, \cdots, x_l]-1,\ m[x_1, \cdots, x_l]) \\ &\qquad\qquad \textit{when}\quad \alpha-\beta\equiv 0 \pmod{\theta[x_1, \cdots, x_l]}, \end{aligned} \tag{4.1}$$

$$\begin{aligned} &\lambda_2(x_1, \cdots, x_l)=\phi(t[x_1, \cdots, x_l]-2,\ d[x_1, \cdots, x_l]-2,\ m[x_1, \cdots, x_l]) \\ &\qquad\qquad \textit{when}\quad \alpha-\beta\not\equiv 0 \pmod{\theta[x_1, \cdots, x_l]}. \end{aligned} \tag{4.2}$$

PROOF. Any $d(p_1^{x_1}\cdots p_{l_x}^{x_l}-1)$-flat is generated by $d[x_1, \cdots, x_l]+1$ linearly independent $(p_1^{x_1}\cdots p_l^{x_l}-1)$-flats of the *m.c.* $\theta[x_1, \cdots, x_l]$ and composed of $s(x_1, \cdots, x_l)=(m^{d+1}-1)/(m^{p_1^{x_1}\cdots p_l^{x_l}}-1)$, $(p_1^{x_1}\cdots p_l^{x_l}-1)$-flats of the same *m.c.*.

When $\alpha-\beta\equiv 0 \pmod{\theta[x_1, \cdots, x_l]}$, the pair of points (x^α) and (x^β) occur together in the same $(p_1^{x_1}\cdots p_l^{x_l}-1)$-flat. Hence We have (4.1) by choosing a set of $d[x_1, \cdots, x_l]+1$ independent flats including the $(p_1^{x_1}\cdots p_l^{x_l}-1)$-flat.

On the other hand, when $\alpha-\beta\not\equiv 0 (\bmod\, \theta[x_1, \cdots, x_l])$, the points (x^α) and (x^β) are on different $(p_1^{x_1}\cdots p_l^{x_l}-1)$-flats. Hence we have (4.2).

When $\theta[x_1, \cdots, x_l]<v$, if we consider all points in PG(t, m) as v different treatments and all $d(p_1^{x_1}\cdots p_l^{x_l}-1)$-flats as $\phi(t[x_1, \cdots, x_l], d[x_1, \cdots, x_l], m[x_1, \cdots, x_l])$ blocks and define a relation of association between a pair of points (x^α) and (x^β) as 1st associates when $\alpha-\beta\equiv 0$ $(\bmod\, \theta[x_1, \cdots, x_l])$ and 2nd associates when $\alpha-\beta\not\equiv 0$ $(\bmod\, \theta[x_1, \cdots, x_l])$, we have the following theorem.

THEOREM 4.2 *When a d-flat in* PG(t, m) *has a cycle* $\theta[x_1, \cdots, x_l]$ *less than* v, *if we consider all* $d(p_1^{x_1}\cdots p_l^{x_l}-1)$-*flats in* PG$(t, m)$, *we have a* PBIB *design of* N_2-*type* (*group divisible*), *its parameters being as follows*:

(i) *Paratemeters of the first kind*:

$$v=\phi(t, 0, m),\ b=\phi(t[x_1, \cdots, x_l], d[x_1, \cdots, x_l], m[x_1, \cdots, x_l]),$$

$$k=\phi(d, 0, m),\ r=\lambda_1(x_1, \cdots, x_l),\ \lambda_1=\lambda_1(x_1, \cdots, x_l),$$

$$\lambda_2=\lambda_2(x_1, \cdots, x_l),\ n_0=1,\ n_1=r(x_1, \cdots, x_l)-1,$$

$$n_2=r(x_1, \cdots, x_l)\{\theta[x_1, \cdots, x_l]-1\},$$

$$\textit{where}\quad r(x_1, \cdots, x_l)=v/\theta[x_1, \cdots, x_l].$$

(ii) *Parameters of the second kind*:

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

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

THEOREM 4.3 *In a design treated in the Theorem* 4.2, *if we consider only those points having the powers of x's less than* $\theta[x_1, \cdots, x_l]$ *as treatments, we have a* BIB *design with parameters*

$$v^*=\theta[\theta_1, \cdots, x_l]=\phi(t[x_1, \cdots, x_l], 0, m[x_1, \cdots, x_l]),$$

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

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

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

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

A useful method of construction stated in the following theorem can be derived as a corollary to the Theorem 4.3.

THEOREM 4.4 *A* BIB *design constructed by the totality of d-flats in* PG$(t, m=p^n)$ *can be obtained by considering all $\tilde{d}$-flats of the cycle $\theta=\phi(t, 0, m)$ in* PG$(\tilde{t}, p)$ *as blocks, and those points whose powers of x's are less than θ as treatments where $\tilde{t}=n(t+1)-1$, $\tilde{d}=n(d+1)-1$ and x is a primitive element of* GF$(p^{\tilde{t}+1})$.

In order to construct actually the difference sets generating cyclically a design, we replace the points $\{(x^{d_{ij}})\,|\,i=1, 2, \cdots, \eta(x_1, \cdots, x_l);\ j=1, 2, \cdots, k\}$ on $\eta(x_1, \cdots, x_l)$ initial d-flats of the *m.c.* $\theta[x_1, \cdots, x_l]$ by the powers of x's for all $\theta[x_1, \cdots, x_l]$:

$$\{d_{ij}\,|\,i=1, 2, \cdots, \eta(x_1, \cdots, x_l);\ j=1, 2, \cdots, k\}. \tag{4.3}$$

In EG(t, m), since there are $v=v^*+1=m^t$ points, slight modification is necessary for the origin (0). We usually replace (0) by the symbol ∞ satisfying the property $\infty+a=\infty$ for any $a=0, 1, 2, \cdots, v-2$. Then the sets of integers (4.3) are the difference sets of the *m.c.* $\theta[x_1, \cdots, x_l]$. The totality of the difference sets of the *m.c.* $\theta[x_1, \cdots, x_l]$ for all $\theta[x_1, \cdots, x_l]$ generates a BIB design [3].

If we consider only the difference sets of the cycle $\theta[x_1, \cdots, x_l]$, we have a PBIB design mentioned in the Theorem 4.2. If we consider a family of the partial sets consisting of the powers of x's less than $\theta[x_1, \cdots, x_l]$ in the difference sets of the cycle $\theta[x_1, \cdots, x_l]$, we have a BIB design mentioned in the Theorem 4.3.

EXAMPLE 2 If we consider 2-flats in PG(3, 4), we can construct on paper a symmetrical BIB design with the following parameters:

$$v=b=85,\quad k=r=21,\quad \lambda=5.$$

The difference sets generating the design, however, have not yet been obtained [5]. Our Theorem 4.4 provides a solution as is obtained in the following.

In this case, as $\tilde{t}=7$, $\tilde{d}=5$ and $p=2$, we consider the PG(7, 2). The only *m.c.* less than 255 is $(2^8-1)/(2^2-1)=85$. The number of 5-flats of the *m.c.* 85 is $\phi(3, 2, 2^2)=85$.

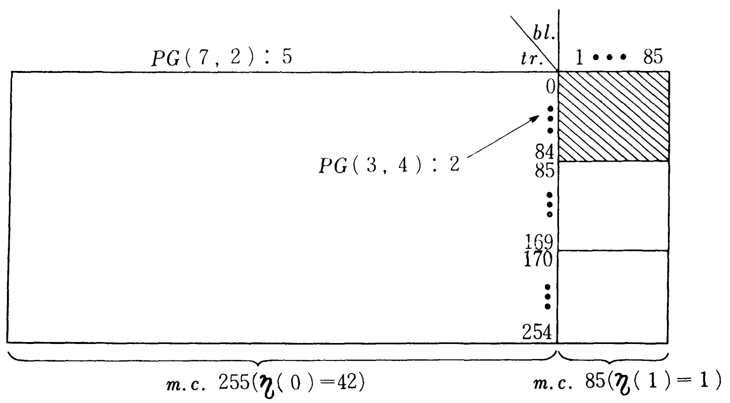


Fig. 1. Figure illustrating the relation between 5-flats in PG(7, 2) and 2-flats in PG(3, 4).

Since a minimum function of GF(2^8) is $f(x)=x^8+x^4+x^3+x^2+1$ [2], three lines $V_1(0)=\{(a_{00}x^0+a_{01}x^{85})\}$, $V_1(1)=\{(a_{10}x^1+a_{11}x^{86})\}$ and $V_1(2)=\{(a_{20}x^2+a_{21}x^{87})\}$ of the *m.c.* 85 are linearly independent. So we have an initial 5-flat of the *m.c.* 85

$$V_5(0)=\{(a_0x^0+a_1x^1+a_2x^2+a_3x^{85}+a_4x^{86}+a_5x^{87})\}.$$

Hence we have after some calculation the following difference set generating the BIB design mentioned above by taking up those points on $V_5(0)$ which have the powers of x's less than 85:

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

The following two BIB designs can be derived by the processes of block section and block intersection:

$$v=64,\ b=84,\ r=21,\ k=16,\ \lambda=5;$$

$$v=21,\ b=84,\ r=20,\ k=5,\ \lambda=4.$$

References

[1] Bose, R.C. (1939). On the construction of balanced incomplete block designs. *Ann. Eugenics* **9** 353-399.

[2] Carmichael, R.D. (1937). *Introduction to the theory of groups of finite order*. Ginn and Company, Boston.

[3] Rao, C.R. (1945). Finite geometries and certain derived results in theory of numbers. *Proc. Nat. Inst. Sci. India* **11** 136-149.

[4] Rao, C.R. (1946). Difference sets and combinatorial arrangements derivable from finite geometries. *Proc. Nat. Inst. Sci. India* **12** 123-135.

[5] Takeuchi, K. (1962). A table of difference sets generating balanced incomplete block designs. *Rev. Inst. Internat. Statist.* **30** 361-366.

[6] Veblen, O. and Bussey, W.H. (1906). Finite projective geometries. *Trans. Amer. Math. Soc.* **7** 241-259.

Department of Mathematics,
Faculty of Science,
Hiroshima University;
Maritime Safety Academy, Kure
and
Department of Mathematics,
Faculty of Science,
Hiroshima University