DECOMPOSITION BY BILATERAL COSETS AND ITS GENERALIZATION

By MOTOSABURO MASUYAMA

Tokyo University

and

Indian Statistical Institute, Calcutta

SUMMARY. In previous papers the author (Masuyama, 1961a, 1961b, 1961c and 1961d) introduced (1) the factorial decomposition, (2) the hierarchic decomposition, (3) the symmetric decomposition and (4) the periodic decomposition of a finite module or a finite ring with unity. Each decomposition supplies a family of Partially Balanced Incomplete Block designs, if we make one element of a module or of a ring correspond to one variety and vice versa. As is proved by the author (Masuyama, 1961d) the periodic decomposition is a refinement of other decomposition. We shall generalize in Section 1 the concept of the periodic block in the sense that ordinary cosets are special cases of bilateral or double cosets in the theory of groups and shall generalize, further, from the viewpoint of mapping in Section 2 which was noticed by P. K. Menon.*

1. Suppose, $\mathcal{A}$ be a ring of order v with unity e. Let $\mathcal{G}$ and $\mathcal{H}$ be two multiplicative groups of order g and h respectively contained in this ring, e being the unity of $\mathcal{G}$ and $\mathcal{H}$. $\mathcal{G}$ and $\mathcal{H}$ are not necessarily distinct. a_i, G_j and H_l being an element of $\mathcal{A}$, $\mathcal{G}$ and $\mathcal{H}$ respectively, $G_j a_i H_l$ is an element of $\mathcal{A}$. We arrange this element in the row (a_i) and in the column (G_j, H_l), for $i = 1, 2, \ldots, v$, $j = 1, 2, \ldots, g$, $l = 1, 2, \ldots, h$. The order of arranging the heading (a_i) or (G_j, H_l) is immaterial, so far as all possible cases occur just once.

TABLE 1

	$(G_1, H_1) = (e, e)$	$\ldots$	(G_j, H_l)	$\ldots$	(G_g, H_h)
$(a_1) = (e)$	eee	$\ldots$	$G_j e H_l$	$\ldots$	$G_g e H_h$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
(a_i)	$e a_i e$	$\ldots$	$G_j a_i H_l$	$\ldots$	$G_g a_i H_h$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
(a_v)	$e a_v e$	$\ldots$	$G_j a_v H_l$	$\ldots$	$G_g a_v H_h$

*Dr. P. K. Menon, Director, Cypher Bureau, Ministry of Defence, Government of India, drew the author's attention to R. Vaidyanathaswamy's paper 'A remarkable property of the integers mod N, and its bearing on group theory,' published in *Proc. Ind. Acad. Sci.*, 5(1937), 63-75, in which Vaidyanathaswamy treated a special case of our periodic block, which corresponds to Fuchs' case with different notations. See L. Fuchs 'Ueber die Perioden usw', published in *Crelle's Journal*, 61(1863), 374-386 and P. Bachmann's *Lehre von der Kreistheilung*, Leipzig, 1872. Vaidyanathaswamy's method of determining coefficients which appear in a product of two periodic blocks, in our terminology, is new. However, these coefficients are easily determined by the remark given by Masuyama (1961d), at the end of Section 4 not only in the Fuchsian case but also in any case of periodic blocks generated by elements of a finite ring.

Then each column contains all elements of the ring exactly once, because if we have

$$G_j a H_l = G_j b H_l, \qquad \dots \quad (1)$$

then multiplying G_j^{-1} from the left and H_l^{-1} from the right we get

$$a = b. \qquad \dots \quad (2)$$

Identical elements of the ring may appear in the same row more than once. Suppose that there are exactly d elements contained in the row (a) which are equal to a, i.e.

$$a = G_{j_2} a H_{l_2} = G_{j_3} a H_{l_3} = \cdots = G_{j_d} a H_{l_d}. \qquad \dots \quad (3)$$

(i) If $d = gh$, we have $$a = G_j a H_l \qquad \dots \quad (4)$$

for $j = 1, 2, \dots, g$; $l = 1, 2, \dots, h$.

(ii) If $d < gh$, there are elements which are not equal to a. Let any one of them be GaH. Then multiplying G from the left and H from the right we have by (3)

$$GaH = GG_{j_2} a H_{l_2} H = \cdots = GG_{j_d} a H_{l_d} H, \qquad \dots \quad (5)$$

with $(G, H) \neq (GG_{j_m}, H_{l_m} H)$ for $m = 2, 3, \dots, d$. Thus GaH reduced to an element of $\mathscr{A}$ appears at least d times on the same row (a). If there were more than d elements which are equal to GaH, let $G_0 a H_0$ be any one of them.

Then we would have

$$a = G_{j_2} a H_{l_2} = \cdots = G_{j_d} a H_{l_d} = G^{-1} G_0 a H_0 H^{-1} \qquad \dots \quad (6)$$

with $(G_{j_m}, H_{l_m}) \neq (G^{-1}G_0, H_0 H^{-1})$ for $m = 2, 3, \dots, d$, which is contrary to our assumption. Thus each distinct element of $\mathscr{A}$ is contained exactly d times in the row (a), if it is contained in the row (a).*

A block which contains all elements of one row of Table 1 is called a bilateral coset block or in short BC block and a block which contains every different element in the same row exactly once is called a normalized BC block. Then two BC blocks obtained from different rows are either identical or disjoint.

If $$G_j a H_l = G_m b H_n, \quad \text{for} \quad a \neq b, \qquad \dots \quad (7)$$

we have $$GaH = GG_j^{-1} G_m b H_n H_l^{-1} H, \quad \text{for any } G \epsilon \mathscr{G} \text{ and } H \epsilon \mathscr{H}. \qquad \dots \quad (8)$$

Thus all elements GaH are contained in the row (b). Similarly, all elements GbH are contained in the row (a). Therefore, the sum of all possible non-identical normalized BC blocks contains all elements of the ring once and only once.

---

* The author wishes to express his thanks to Dr. P. K. Menon for kindly pointing out the mistake in the proof on this point in the first manuscript.

We shall now prove that a product of any two BC blocks is represented by a linear combination of BC blocks, coefficients being non-negative integers. In fact we have

$$G_jaH_l+G_mbH_n = G_j(a+G_j^{-1}G_mbH_nH_l^{-1})H_l$$
$$= G_j(a+G_pbH_q)H_l, \qquad \dots \quad (9)$$

in which the second term in the bracket runs through every element of the row (b) once and only once, for all combinations of m and n, whatever j and l may be so far as these two suffixes are fixed.

$$c_{pq} = a+G_pbH_q \qquad \dots \quad (10)$$

being an element of the ring $\mathscr{A}$, the block

$$\{G_1c_{pq}H_1, \dots, G_jc_{pq}H_l, \dots, G_gc_{pq}H_h\} \qquad \dots \quad (11)$$

for fixed values of p and q is a BC block. q.e.d.

The periodic block is a special case of our bilateral coset block in which one of $\mathscr{G}$ and $\mathscr{H}$ consists of only one element e.

2. The above result is easily generalized, if we realize that the essential features of the above proof are (i) the multiplicative group property of the transformations or mappings τ_{jl} of an element of a, i.e. G_jaH_l in this case, and (ii) the distributive property of the transformation or the isomorphism between a and $\tau_{jl}a$. The first property is used in getting the formulas, (2), (5), (6), and (8) and the second one is used in getting the formula (9). The existence of the unity in $\mathscr{A}$, which we have assumed in Section 1, is needed only when we utilize the group property of the mappings.

Now let $\mathscr{M}$ be a finite module of order v and $\tau_j\,a$ be a mapping of a in $\mathscr{M}$ into $\mathscr{M}$. Then all mappings τ_j constitute a semi-group $\mathscr{T}(\mathscr{M})$, of which an inversible element gives a bijective mapping. All the bijective mappings constitute a symmetric group, i.e. a substitution group $\mathfrak{S}(\mathscr{M})$, of which automorphic mappings constitute a subgroup $\mathfrak{A}(\mathscr{M})$ of $\mathfrak{S}(\mathscr{M})$. Any subgroup of $\mathfrak{A}(\mathscr{M})$ can be used for generating a Partially Balanced Incomplete Block design. Table 1 in Section 1 is replaced by the following table :

TABLE 2

	τ_1	$\dots$	τ_j	$\dots$	τ_g
(a_1)	τ_1a_1	$\dots$	τ_ja_1	$\dots$	τ_ga_1
$\vdots$	$\vdots$		$\vdots$		$\vdots$
(a_i)	τ_1a_i	$\dots$	τ_ja_i	$\dots$	τ_ga_i
$\vdots$	$\vdots$		$\vdots$		$\vdots$
(a_v)	τ_1a_v	$\dots$	τ_ja_v	$\dots$	τ_ga_v

The set of all elements in a row constitute a block, in which all distinct elements appear with the same frequency, say d-times. A block which is derived from one row and contains all distinct elements exactly once, is called a normalized block. The block thus obtained may be qualified by the specific mapping used.

3. We shall illustrate our method by one of the commonest transformations, i.e. by conjugation. Suppose that a is an element of a ring $\mathscr{A}$ of order v with unity and G_j is an element of a multiplicative group of order g contained in $\mathscr{A}$. Then the conjugated block

$$\{G_1 a G_1^{-1}, \ldots, G_j a G_j^{-1}, \ldots, G_g a G_g^{-1}\} \qquad \ldots \quad (12)$$

or its sum generates a Partially Balanced Incomplete Block design by multiplying $\{s\}$, s being every element of $\mathscr{A}$. The mapping 'conjugation' satisfies two conditions stated in Section 2.

Example : Consider the matrix ring of order 16 (see Appendix) which is quoted by (Masuyama, 1961d). Let $\mathscr{G}$ be (12, 23, 31, 32, 21, 13), of which (12, 23, 31), (12, 13), (12, 21) and (12) are its subgroups with regard to multiplication. The normalized conjugated blocks obtained by $\mathscr{G}$ are as follows :

$$E = \{00\},$$
$$A = \{12\},$$
$$B = \{23, 31\},$$
$$C = \{32, 21, 13\},$$
$$D = \{01, 20, 33\},$$
$$F = \{02, 03, 10, 11, 30, 22\}.$$

All these blocks are self-conjugate. The multiplication table of these blocks are given by Table 3.

TABLE 3

	E^*	A^*	B^*	C^*	D^*	F^*
E	E					
A	A	E				
B	B	B	$2E+2A$			
C	C	D	F	$3E+2C$		
D	D	C	F	$3A+2D$	$3E+2C$	
F	F	F	$2C+2D$	$3B+2F$	$3B+2F$	$6E+6A+4C+4D$

There are simple linear relations among these blocks and the periodic blocks (Masuyama, 1961d), i.e.

$$F_1 = A+B$$
$$F_2+F_3+F_4 = D+F$$

and

$$F_5 = C.$$

By setting

$$D_1 = A+C+F \quad \text{and} \quad D_2 = B+D$$

we obtain the following multiplication table :

TABLE 4

	E^{*}	D_1^{*}	D_2^{*}
E	E		
D_1	D_1	$10E+6(D_1+D_2)$	
D_2	D_2	$3D_1+4D_2$	$5E+2D_1$

The initial block D_1 and the initial block $(E+D_2)$ supply two Balanced Incomplete Block designs which are complementary. The initial block D_2 supplies a Partially Balanced Incomplete Block design with the following parameters of the first kind :

$$v = b = 16, \quad k = r = 5, \; n_1 = 10, \; n_2 = 5, \lambda_1 = 2 \text{ and } \lambda_2 = 0.$$

The parameters of the second kind are given in Table 4. A Partially Balanced Incomplete Block design with parameters of the same first and second kinds is given by Clatworthy (1956). However, his design is not cyclic.

Appendix : Matrix ring of order 16

THE ADDITION TABLE

00	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
01	01	00														
02	02	03	00													
03	03	02	01	00												
10	10	11	12	13	00											
11	11	10	13	12	01	00										
12	12	13	10	11	02	03	00									
13	13	12	11	10	03	02	01	00								
20	20	21	22	23	30	31	32	33	00							
21	21	20	23	22	31	30	33	32	01	00						
22	22	23	20	21	32	33	30	31	02	03	00					
23	23	22	21	20	33	32	31	30	03	02	01	00				
30	30	31	32	33	20	21	22	23	10	11	12	13	00			
31	31	30	33	32	21	20	23	22	11	10	13	12	01	00		
32	32	33	30	31	22	23	20	21	12	13	10	11	02	03	00	
33	33	32	31	30	23	22	21	20	13	12	11	10	03	02	01	00

THE MULTIPLICATION TABLE

R \ L	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
01	00	00	00	00	01	01	01	01	02	02	02	02	03	03	03	03
02	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03
03	00	01	02	03	01	00	03	02	02	03	00	01	03	02	01	00
10	00	00	00	00	10	10	10	10	20	20	20	20	30	30	30	30
11	00	00	00	00	11	11	11	11	22	22	22	22	33	33	33	33
12	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
13	00	01	02	03	11	10	13	12	22	23	20	21	33	32	31	30
20	00	10	20	30	00	10	20	30	00	10	20	30	00	10	20	30
21	00	10	20	30	01	11	21	31	02	12	22	32	03	13	23	33
22	00	11	22	33	00	11	22	33	00	11	22	33	00	11	22	33
23	00	11	22	33	01	10	23	32	02	13	20	31	03	12	21	30
30	00	10	20	30	10	00	30	20	20	30	00	10	30	20	10	00
31	00	10	20	30	11	01	31	21	22	32	02	12	33	23	13	03
32	00	11	22	33	10	01	32	23	20	31	02	13	30	21	12	03
33	00	11	22	33	11	00	33	22	22	33	00	11	33	32	11	00

(i, j) stands for $\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$ with $i = c_{11}+2c_{12}$ and $j = c_{21}+2c_{22}$, and c_{kl} is an element of the modulo to modulo 2, i. e. 0 or 1.

REFERENCES

BOURBAKI, N. (1936): *Eléments de Mathématique*, Hermann, Paris.

CLATWORTHY, W. H. (1956): Contributions on partially balanced incomplete block designs with two associate classes. N.B.S., Applied Mathematics Series, No. 47.

DUBREIL, P. (1954): *Algèbre*, Tome 1, Gauthier-Villars, Paris.

HALL, M. (1959): *The Theory of Groups*, MacMillan.

IYANAGA, S. and KODAIRA, K. (1961): *Survey of Modern Mathematics*, I, Iwanami., Tokyo.

LYAPIN, E. S. (1960): *Polugruppy*, Gos. Izd. Fiz.—Mat. Lit., Moskva.

MASUYAMA, M. (1961a): Calculus of blocks and a class of partially balanced incomplete block designs. *Rep. Stat. Appl. Res.*, 8, 56-69.

———— (1961b): On cyclic difference sets which generate orthogonal arrays, Part II. *Rep. Stat. Appl. Res.*, 8, 70-76.

———— (1961c): Le calcul des blocs et ses applications aux plans d'expérience, Colloques Internationaux de la Recherche Scientifique, Le Plan d'Expérience, 1-9.

———— (1961d): La décomposition périodique dans le calcul des blocs—le raffinement des décompositions, *Bulletin de l'Institut International de Statistique*, 33ᵉ, Session, Paris, 1-8.

Paper received: October, 1961.