CONSTRUCTION OF ASSOCIATION SCHEMES FROM FINITE GROUPS

by

I.M. Chakravarti
University of North Carolina

and

S. Ikeda
Nihon University

Institute of Statistics Mimeo Series No. 579

May 1968

This research was supported in part by the National Science Foundation Grant No. GP-5790 and the U.S. Army Research Office Grant No. DA-ARO-D-31-124-G910

DEPARTMENT OF STATISTICS

University of North Carolina

Chapel Hill, N. C.

CONTENTS

1. Introduction

A basic idea of constructing association schemes from permutation matrices has been presented by I.M. Chakravarti and W.C. Blackwelder [1], where they have proved an interesting theorem which is an analogue of H.B. Mann's theorem for symmetrical BIB designs [2]. We shall first reproduce their theorem with a modified proof.

Let us divide a given set of v distinct permutation matrices of order v,

$$\Pi = \{P_0 = I_v,\ P_1,\ \ldots,\ P_{v-1}\}\ , \tag{1.1}$$

into m + 1 non-empty subsets

$$\Pi_0 = \{P_0\}\ ,\quad \Pi_1,\ \ldots,\ \Pi_m, \tag{1.2}$$

and let us put

$$A_i = \Sigma_{\Pi_i} P_\alpha\ ,\ i = 0,1,\ldots,m, \tag{1.3}$$

where the summation is taken over all P_α belonging to Π_i. Then, m + 1 matrices $A_0 = I_v,\ A_1,\ldots,A_m$ are all vxv matrices.

Lemma 2.1 of [3] states that

LEMMA 1.1. A necessary and sufficient condition for a set of m + 1 matrices, $\{A_0 = I_v,\ A_1,\ldots,A_m\}$, of order v to be the set of association matrices of an m-class association scheme with parameters

$$v,\ p_{jk}^i,\ \ i,j,k = 0,1,\ldots,m, \tag{1.4}$$

is given by a set of conditions:

$$\begin{cases} \text{(i)} & \text{each } A_i \text{ is a symmetric (0,1)-matrix, } i = 0,1,\ldots,m, \\ \text{(ii)} & \sum_{i=0}^{m} A_i = J_v \text{ (the vxv matrix of 1's), and} \\ \text{(iii)} & A_jA_k = \sum_{i=0}^{m} p_{jk}^i A_i,\quad j,k = 0,1,\ldots,m. \end{cases} \tag{1.5}$$

By (1.3), the conditions given by (1.5) can be rewritten as

$$\text{(i)}\quad \Sigma_{\Pi_i} P_\alpha = \Sigma_{\Pi_i} P_\alpha^{-1}\ ,\quad i = 0,1,\ldots,m,$$

(1.6)
$$\text{(ii)}\quad \Sigma_{\Pi} P_\alpha = J_v\ ,\ \text{and}$$

$$\text{(iii)}\quad \Sigma_{\Pi_j} P_\beta \Sigma_{\Pi_k} P_\gamma = \sum_{i=0}^{m} p_{jk}^{i} \Sigma_{\Pi_i} P_\alpha\ ,\quad j,k = 0,1,\ldots,m,$$

where the summation of the right-hand side of (i) is taken over all P_α belonging to Π_i.

We shall say that two matrices, $R = (r_{ij})$ and $S = (s_{ij})$, are <u>disjoint</u> if the matrix $R \cdot S = (r_{ij}s_{ij})$ is the null-matrix. Then, the condition (ii) of (1.6) shows that Π given by (1.1) is a set of v mutually disjoint permutation matrices, from which the following lemma follows:

<u>LEMMA 1.2.</u> For P_α's satisfying the condition (ii) of (1.6) and for any given real numbers c_α's and d_α's, the condition

$$\text{(1.7)}\qquad \sum_{\alpha=0}^{v-1} c_\alpha P_\alpha = \sum_{\alpha=0}^{v-1} d_\alpha P_\alpha$$

implies that $c_\alpha = d_\alpha$, $\alpha = 0,1,\ldots,v-1$.

The proof of this lemma is easy and is omitted.

Let

$$\Pi_i = \{P_\alpha^{-1} \mid P_\alpha \in \Pi_i\}\ ,\quad i = 0,1,\ldots,m.$$

The following theorem due to Chakravarti and Blackwelder [1] is now easy to prove.

<u>THEOREM 1.1.</u> Suppose that the set Π of v permutation matrices of order v, given by (1.1), forms a group of order v. Then, the set of conditions given by (1.6) is equivalent to the following set of conditions:

(1.8) (i) $\Pi_i = \Pi_i^{-1}$, $i = 0,1,\ldots,m.$

(ii) $\Sigma_{\Pi} P_\alpha = J_v$, and

(iii) for any given P belonging to Π_i, the equation

$$P_\beta P_\gamma = P_\alpha$$

has exactly p_{jk}^i solutions (P_β, P_γ) such that $P_\beta \in \Pi_j$ and $P_\gamma \in \Pi_k$, for any j and k, $j,k = 0,1,\ldots,m$.

PROOF. It is evident that the conditions (1.8) are sufficient for (1.6). Since Π is a group, $\Pi^{-1} = \Pi$. For any given i, let us put

$$\Sigma_{\Pi i} P_\alpha = \sum_{\alpha=0}^{v-1} c_{i\alpha} P_\alpha \quad \text{and} \quad \Sigma_{\Pi_i} P_\alpha^{-1} = \sum_{\alpha=0}^{v-1} d_{i\alpha} P_\alpha .$$

Then, the condition (i) of (1.6) implies that

$$\sum_{\alpha=0}^{v-1} c_{i\alpha} P_\alpha = \sum_{\alpha=0}^{v-1} d_{i\alpha} P_\alpha , \quad i = 0,1,\ldots,m.$$

Hence it follows from Lemma 1.2 that $c_{i\alpha} = d_{i\alpha}$, $\alpha = 0,1,\ldots,v-1$; $i = 0,1,\ldots,m$, and therefore we have (i) of (1.8).

Let $p_{jk}(P_\alpha)$ be the number of solutions, (P_β, P_γ) with $P_\beta \in \Pi_j$ and $P_\gamma \in \Pi_k$, of the equation in (iii) of (1.8). Since Π is a group, $P_\beta P_\gamma$ is again in Π. Hence

$$\sum_{P_\beta \in \Pi_j} P_\beta \sum_{P_\gamma \in \Pi_k} P_\gamma = \sum_{\alpha=0}^{v-1} p_{jk}(P_\alpha) P_\alpha ,$$

and therefore, by the condition (iii) of (1.6), we have

$$\sum_{\alpha=0}^{v-1} p_{jk}(P_\alpha) P_\alpha = \sum_{i=0}^{m} p_{jk}^i \Sigma_i P_\alpha .$$

This implies, by Lemma 1.2, that

$$p_{jk}(P_\alpha) = p_{jk}^i ,$$

for any P_α belonging to Π_i, $i = 0, 1, \ldots, m$.

Thus, we have proved that the conditions (1.8) are necessary for those of (1.6).

This completes the proof of the theorem.

When the set $\mathfrak{N}$ of permutation matrices given by (1.1) forms a group, it can be regarded as a permutation group, whose elements being permutations on v objects: $\mathfrak{N}$ is isomorphic to a subgroup of the symmetric group of order v!. Since the order of $\mathfrak{N}$ is v, $\mathfrak{N}$ is isomorphic to a regular permutation group.

Group representation theory says that any finite group is represented as a regular permutation group, from which one can say that the construction problem of association schemes from permutation matrices, provided they form a group, is essentially equivalent to that from finite groups.

The present paper seeks for those association schemes which are constructed from finite groups.

In the following section, we shall introduce some operations on collections of group elements and state some of their properties.

In section 3, a pair-wise relation on group elements of a given finite group, which we intend to call <u>association relation</u>, is introduced, and the conditions under which the association relation results the usual association schemes are discussed. It comes out that the usual module theorem can be extended to the case where the group operation is not necessarily commutative.

Section 4 and subsequent sections are devoted to study some types of group structures which generate association schemes.

2. <u>Collections of group elements</u>

Let G be a group of finite order. By a <u>collection</u> of elements of G we mean a set of elements of G allowing the multiplicity of each element:

$$H = \{a,\ldots,a,b,\ldots,b,\ldots.\}, \quad a,b,\ldots \in G, \tag{2.1}$$

for which the multiplicities of the elements, a, b, ... are denoted by $f_a(H)$, $f_b(H)$, ..., respectively. Given a collection H, we shall define the multiplicity of any given element a of G relative to H in the following way: if a belongs to H, then $f_a(H)$ is defined to be the number of times a appears in H, and, if a does not belong to H, then $f_a(H) = 0$. Thus, for any given collection H, there corresponds a set of multiplicities of the group elements relative to H, $[f_a(H) \,|\, a \in G]$. This correspondence is one-to-one. A collection with the corresponding multiplicities $[f_a(H) = 0 \,|\, a \in G]$ is the empty collection.

According to the above definition, a subset H of G in the usual sense is a special type of collection for which $f_a(H)$ takes the value 0 or 1 for each $a \in G$.

It should be noted that the same kind of sets of group elements has been introduced, together with some operations which are stated below, and used extensively by M. Masuyama (see, for example, [4]).

Now, we shall define some operations on collections of group elements.

It is convenient to denote the collection H with the corresponding multiplicities $[f_a(H) \,|\, a \in G]$ by $H = H(G)[f_a(H)]$, where H(G) designates the subset of G which consists of all distinct elements belonging to H. For any two collections H and K, $H \subseteqq K$ means that $f_a(H) \leqq f_a(K)$ for each $a \in G$, with equality if and only if $f_a(H) = f_a(K)$ for all $a \in G$. Note that $H \subseteqq K$ implies that $H(G) \subseteqq K(G)$, while $H \subset K$ does not necessarily imply $H(G) \subset K(G)$.

We shall introduce some rules of calculation on collections:

(a) Inversion: $H^{-1} = K$ if and only if $f_a(K) = f_{a^{-1}}(H)$, and hence $K(G) = H(G)^{-1}$, where for any subset A of G,

$$A^{-1} = \{x^{-1} \mid x \in A\}.$$

(b) Scalar multiplication: For any non-negative integer λ, $K = \lambda H$ if

and only if $f_a(K) = \lambda f_a(H)$.

(c) Multiplication by group element: For any given element x of G, $K = xH$ if and only if $f_a(K) = f_{x^{-1}a}(H)$, and hence $K(G) = xH(G)$, where

$$xA = \{xa \mid a \in A\},$$

for any subset A of G and any $x \in G$. Right-multiplication, Hx, is also defined similarly.

(d) Addition: $H + K = L$ if and only if $f_a(L) = f_a(H) + f_a(K)$, and hence $L(G) = H(G) \cup K(G)$.

(e) Subtraction: For any H and K such that $H \supseteq K$, $H-K = L$ if and only if $f_a(L) = f_a(H) - f_a(K)$ for each $a \in G$.

(f) Union $H \cup K = L$ if and only if $f_a(L) = \max(f_a(H), f_a(K))$.

(g) Intersection: $H \cap K = L$ if and only if $f_a(L) = \min(f_a(H), f_a(K))$

(h) Product: $HK = L$ if and only if $f_a(L) = \sum_{xy=a} f_x(H)f_y(K)$, for each $a \in G$.

Some of the main properties of the operations defined above are listed in the following

LEMMA 2.1. Let H, K, L and M be any given collections of elements of a given finite group G, and λ, μ, ζ and η be any given integers such that both $\lambda H + \mu K$ and $\zeta L + \eta M$ are certain collections. Then, it holds that

(i) $(\lambda H+\mu K)(\zeta L+\eta M) = \lambda\zeta HL+\lambda\eta HM+\mu\zeta KL+\mu\eta KM$,

(ii) $(\lambda H+\mu K)^{-1} = \lambda H^{-1} + \mu K^{-1}$,

(iii) $(HK)^{-1} = K^{-1}H^{-1}$.

The proof of this lemma is easy and is omitted.

Let us define the cardinality of a collection of group elements, H, by

$$/H/ = \sum_{a \in G} f_a(H). \tag{2.2}$$

Then, we can see the following

LEMMA 2.2. For any given subsets, H and K, of G, the cardinality of $H \cap K$ is equal to the multiplicity of the unit element 1 in the product HK^{-1}, i.e.,

$$(2.3) \qquad / H \cap K / = f_1(HK^{-1}).$$

The product HK^{-1} can be replaced by any one of the products, $H^{-1}K$, KH^{-1} and $K^{-1}H$.

PROOF. By (2.2) and the definition of the intersection, we have

$$/ H \cap K / = \sum_{a \in G} \min(f_a(H), f_a(K)),$$

while, by the definition of the product,

$$f_1(HK^{-1}) = \sum_{xy=1} f_x(H)\, f_y(K^{-1}).$$

Since $f_y(K^{-1}) = f_{y^{-1}}(K)$, and $f_a(H)$ and $f_a(K)$ take the value 1 or 0, we get

$$f_1(HK^{-1}) = \sum_{x=y^{-1}} f_x(H)\, f_{y^{-1}}(K)$$

$$= \sum_{a \in G} f_a(H)\, f_a(K) = / H \cap K /,$$

which proves (2.3).

It is easy to see that HK^{-1} can be replaced by one of $H^{-1}K$, KH^{-1} and $K^{-1}H$.

This completes the proof of the lemma.

It is straightforward to extend this lemma to get

$$(2.4) \qquad / aH \cap bK / = f_{a^{-1}b}(HK^{-1}),$$

that is, the cardinality of the subset $aH \cap bK$ is equal to the multiplicity of the element $a^{-1}b$ in HK^{-1}, for any subsets H and K and any elements a and b of G.

Let us denote the subset of G consisting of the unit element only by G_0, i.e., $G_0 = \{1\}$.

LEMMA 2.3. (i) For any given subgroup H of G, and any given subset of H, it holds that

$$KH = HK = /K/H. \tag{2.5}$$

(ii) A necessary and sufficient condition for any given subset H of G to be a subgroup of G is that

$$H^2 = /H/\ H. \tag{2.6}$$

(iii) A subset $S = G_0 + T$ of G is a subgroup of G if and only if

$$T^2 = /T/\ G_0 + (/T/-1)T. \tag{2.7}$$

PROOF. (i): By definition,

$$f_a(KH) = \sum_{xy=a} f_x(K)\ f_y(H)$$

$$= \sum_{\substack{y=x^{-1}a \\ y\in H, x\in K}} 1 = \begin{cases} /K/, & \text{if } a \in H, \\ 0, & \text{otherwise.} \end{cases}$$

This proves (2.5).

(ii): Necessity follows from (i).

Suppose a subset H of G satisfies the condition (2.6).

Since $/\ H^2\ / = /\ nH\ /$ where $n = /H/$, the product of any two elements of H must be in H, i.e., if $x, y \in H$, then $xy \in H$.

Consider any element x in H. Then, there exist y, z in H such that $xy = z$, or equivalently, $x^{-1}z = y$. From (2.6) it follows that

$$(G-H)H=H(G-H) = HG - H^2 = nG - nH = n(G-H),$$

which implies that the equality $x^{-1}x = y$ given above is impossible unless

$x^{-1} \in H$. Hence, if $x \in H$ then $x^{-1} \in H$.

This completes the proof of (ii).

(iii): Put $/T/ = m$, then $/S/ = m + 1$.

Using (2.7) we have

$$S^2 = (G_0+T)^2 = G_0+2T+T^2$$
$$= G_0 + 2T + mG_0 + (m-1)T$$
$$= (m+1)(G_0+T) = (m+1)S,$$

and, conversely, if $S^2 = (m+1)S$, then we have (2.7).

Thus, (iii) follows from (ii), and the proof of the lemma is completed.

3. Association relation of group elements and an extension of the module theorem

Let G be any given finite group of order v, and let

$$G = G_0 + G_1 + \ldots + G_m \tag{3.1}$$

be a partition of G into (m+1) non-empty subsets, where, as before, $G_0 = \{1\}$, 1 being the unit element of G.

Let $\varphi(x,y)$ be a mapping from the direct product

$$G \times G = \{(x,y) \mid x, y \in G\},$$

onto the set of (m+1) integers, $\{0,1,\ldots,m\}$, defined by

$$\varphi(x,y) = i \text{ if and only if } x^{-1}y \in G_i,\ i = 0, 1, \ldots, m. \tag{3.2}$$

Note that $\varphi(x,y)$ is not necessarily symmetric with respect to x and y. We shall say that the element x is of the ith relation to y with respect to the partition (3.1), if x and y satisfy the condition (3.2).

The mapping defined above has the following properties:

(a) $\varphi(x,y)$ is defined for all (x,y) of $G \times G$,

(b) $\varphi(x,y) = 0$ if and only if $x = y$,

(c) for any element a of G, $\varphi(ax,ay) = \varphi(x,y)$,

(d) if G is abelian, then $\varphi(x,y) = \varphi(y^{-1},x^{-1})$, and

(e) for any given $a \in G$, the number of elements y such that $\varphi(a,y) = i$ is equal to the cardinality of G_i, $/G_i/$, $i = 0, 1, \ldots, m$.

We shall say that $\varphi(x,y)$ is symmetric, if and only if $\varphi(x,y) = \varphi(y,x)$ for all (x,y) of $G \times G$.

We then have the following

LEMMA 3.1. A necessary and sufficient condition for the mapping $\varphi(x,y)$, defined by (3.2), to be symmetric is that

$$G_i^{-1} = G_i, \quad i = 0, 1, \ldots, m. \tag{3.3}$$

PROOF. Suppose that $\varphi(x,y)$ is symmetric, and let c be any given element of G_i. Then, there exists at least one (x,y) of $G \times G$ such that $x^{-1}y = c$, and, of course, $\varphi(x,y) = i$.

Since, by assumption, $\varphi(x,y) = \varphi(y,x) = i$, it holds that $y^{-1}x = (x^{-1}y)^{-1} = c^{-1}$ belongs to G_i. This means that $G_i^{-1} \subseteq G_i$. Then, comparing the cardinalities of G_i and G_i^{-1}, we get (3.3), which proves the necessity.

It is quite easy to prove the sufficiency.

If every element of G is such that $a^2 = 1$, then for any partition of G in the form (3.1) satisfies the condition (3.3), and therefore $\varphi(x,y)$ is symmetric.

DEFINITION 3.1. The mapping $\varphi(x,y)$, given by (3.2), is said to define an m-class association scheme on the v elements of G, if it holds that

(i) $\varphi(x,y)$ is symmetric, and

(ii) for any given (x,y) of $G \times G$ such that $\varphi(x,y) = i$, the number p_{jk}^i, of such elements z that $\varphi(x,z) = j$ and at the same time $\varphi(y,z) = k$ is

independent of the initial (x,y), for any i, j and k; $i,j,k = 0,1,\ldots,m$.

Once we got an m-class association scheme on the v elements of G, it is considered as an m-class association scheme in the usual sense defined on v objects, regardless of the group operation among them.

It is well-known that the parameters, p_{jk}^{i}, satisfy the following conditions:

$$
\begin{aligned}
&\text{(a)} \quad \text{Putting } n_i = p_{ii}^{0}, \quad i = 0,1,\ldots,m, \\
&\qquad\qquad \sum_{i=0}^{m} n_i = v. \\
&\text{(b)} \quad p_{jk}^{0} = n_j \, \delta_{jk} \text{ and } p_{j0}^{i} = \delta_{ij}, \quad i,j,k = 0,1,\ldots,m. \\
&\text{(c)} \quad p_{jk}^{i} = p_{kj}^{i}, \quad i,j,k, = 0,1,\ldots,m. \\
&\text{(d)} \quad p_{jk}^{i} n_i = p_{ik}^{j} n_j = p_{ij}^{k} n_k, \quad i,j,k = 0,1,\ldots,m. \\
&\text{(e)} \quad \sum_{j=0}^{m} p_{jk}^{i} = n_k, \text{ independently of } i; \quad i,k = 0,1,\ldots,m.
\end{aligned}
\tag{3.4}
$$

The following is the main theorem of this section.

THEOREM 3.1. A necessary and sufficient condition for the mapping $\varphi(x,y)$ given by (3.2) to define an m-class association scheme on the v elements of G is given by a set of conditions

$$
\begin{cases}
\text{(i)} & G_i = G_i^{-1}, \quad i = 0, 1, \ldots, m, \\
\text{(ii)} & G_j G_k = \sum_{i=0}^{m} p_{jk}^{i} G_i, \quad j,k = 0, 1, \ldots, m,
\end{cases}
\tag{3.5}
$$

for some set of integers $\left\{p_{jk}^{i}\right\}$ $(i,j,k = 0,1,\ldots,m)$.

PROOF. (Necessity): Suppose that the two conditions of Definition 3.1 are satisfied.

Then, the parameters p_{jk}^{i} in the definition satisfy the conditions (a)

through (e) of (3.4).

First, the condition (i) of (3.5) follows from (i) in the definition by Lemma 3.1.

To prove (ii) of (3.5), let c be any given element of G_i. Then, there exists at least one (a,b) of $G \times G$ such that

$$a^{-1}b = c,$$

for which, of course, $\varphi(a,b) = i$. By the condition (ii) of Definition 3.1, there exist exactly p_{jk}^{i} such z that $\varphi(a,z) = j$ and at the same time $\varphi(b,z) = k$, that is,

$$a^{-1}z \in G_j \text{ and } z^{-1}b \in G_k.$$

Since $(a^{-1}z)(z^{-1}b) = a^{-1}b = c \in G_i$, there exist at least p_{jk}^{i} such (x,y) that $x \in G_j$, $y \in G_k$ and $xy = c$, which implies that

$$G_j G_k \supseteq \sum_{i=0}^{m} p_{jk}^{i} G_i, \quad (j,k = 0,1,\ldots,m). \tag{3.6}$$

The cardinalities of the collections on both sides of this implication relation are

$$/G_jG_k/ = /G_j//G_k/ = n_j n_k,$$

and

$$/\sum_{i=0}^{m} p_{jk}^{i}G_i/ = \sum_{i=0}^{m} p_{jk}^{i}n_i = \sum_{i=0}^{m} p_{ik}^{j}n_j = n_jn_k,$$

where we have used the fact that $n_i = /G_i/$ and the conditions (d) and (e) of (3.4). Hence, it follows from (3.6) that

$$G_j G_k = \sum_{i=0}^{m} p_{jk}^{i} G_i,$$

which proves (ii) of (3.5).

This completes the proof of necessity.

(Sufficiency): The condition (i) of Definition 3.1 follows from the condition (i) of (3.5) by Lemma 3.1.

We shall prove (ii) in the definition.

Let (x,y) be any given element of $G \times G$ satisfying the condition $\varphi(x,y) = i$. Then, it is easy to see that an element z of G satisfies the conditions $\varphi(x,z) = j$ and $\varphi(y,z) = k$ simultaneously if and only if

$$z \in xG_j \cap yG_k.$$

Thus, the number of such z that $\varphi(x,z) = j$ and $\varphi(y,z) = k$ for any given (x,y) satisfying $\varphi(x,y) = i$ is equal to the cardinality of the subset $xG_j \cap yG_k$, which is, by Lemma 2.2, identical with the multiplicity of the element $x^{-1}y$ in G_jG_k, provided that $x^{-1}y \in G_i$. This number is seen, by the condition (ii) of (3.5), to be equal to p_{jk}^i independently of (x,y).

This proves the sufficiency.

Thus the proof of the theorem is completed.

It should be remarked that the above theorem is a multiplicative group version of the usual module theorem (for example, [5]), when G is an abelian group. Since the group G of the theorem is not necessarily abelian, the theorem is regarded as an extension of the module theorem.

It is also noted that the condition (ii) of (3.5) does not require for the parameters p_{jk}^i to satisfy the conditions given by (3.4). The theorem says that p_{jk}^i in (ii) or (3.5) automatically satisfy the conditions (3.4). It is not so difficult to check that p_{jk}^i in (ii) of (3.5) satisfy (3.4) as will be shown in the following

LEMMA 3.2. For the parameters $\left\{p_{jk}^i\right\}$ $(i,j,k = 0,1,\ldots,m)$, the conditions (a) through (e) of (3.4) are all satisfied.

PROOF. The proof of this lemma will help to understand the structure of the partition (3.1) satisfying the conditions (3.5), expecially when G is not abelian.

(a): The condition (ii) of (3.5) means that p_{ii}^0 is the multiplicity of the unit element 1 in the collection G_i^2. Thus, by (i) of (3.5), we have $p_{ii}^0 = /G_i/$, $i = 0,1,\ldots,m$. Then, (a) of (3.4) follows from (3.1).

(b): From (ii) of (3.5) it follows that

$$G_j G_0 = G_j = \sum_{i=0}^{m} p_{j0}^i G_i,$$

which implies that $p_{j0}^i = \delta_{ij}$, where δ_{ij} designates the Kronecker delta.

Again from (ii) of (3.5) it follows that p_{jk}^0 is the multiplicity of the unit element 1 in the collection G_jG_k, which is equal to the cardinality of $G_j \cap G_k$. Since

$$/G_j \cap G_k/ = n_j\delta_{jk},$$

we have $p_{jk}^0 = n_j\delta_{jk}$.

(c): To prove (c) of (3.4), it suffices to show that

(3.7) $$G_jG_k = G_kG_j, \quad j,k = 0,1,\ldots,m.$$

Since $G_j = G_j^{-1}$ and $G_k = G_k^{-1}$, it holds that

$$(G_jG_k)^{-1} = G_kG_j.$$

But, from (i) and (ii) of (3.5) it follows that

$$(G_jG_k)^{-1} = \Big(\sum_{i=0}^{m} p_{jk}^i G_i\Big)^{-1} = \sum_{i=0}^{m} p_{jk}^i G_i^{-1} = \sum_{i=0}^{m} p_{jk}^i G_i$$

$$= G_j G_k.$$

Hence we have (3.7).

As we have used above, it holds that

(3.8) $$\sum_{i=0}^{m} \lambda_i G_i = \sum_{i=0}^{m} \mu_i G_i \quad \text{iff} \quad \lambda_i = \mu_i, \quad i = 0,1,\ldots,m,$$

for any non-negative integers λ_i and μ_i.

(d): (ii) of (3.5) shows that the total number of such (x,y) that

$x \in G_j$, $y \in G_k$ and $xy \in G_i$ is equal to the cardinality of the collection $p^i_{jk} G_i$, i.e., to $p^i_{jk} n_i$. Note that this is equal to the number of elements (x,y,z) of $G \times G \times G$ which satisfy the equation $xy = z$, $x \in G_j$, $y \in G_k$ and $z \in G_i$, and for each of such (x,y,z), we have an element (z,y^{-1},x) of $G \times G \times G$ which satisfies the conditions $zy^{-1} = x$, $z \in G_i$, $y^{-1} \in G_k$ and $x \in G_j$.

Thus, it holds that

$$p^i_{jk} n_i \leqq p^j_{ik} n_j,$$

and this relation is convertible, from which we have

$$p^i_{jk} n_i = p^j_{ik} n_j.$$

Analogously, we can prove that (d) holds true.

(e): Summing up both sides of (ii) of (3.5) with respect to j, we get

$$GG_k = \sum_{i=0}^{m} \Big(\sum_{j=0}^{m} p^i_{jk} \Big) G_i.$$

On the other hand, it follows from Lemma 2.3 that

$$GG_k = n_k G = n_k \sum_{i=0}^{m} G_i.$$

Hence, by (3.8), we have (e) of (3.4).

This completes the proof of the lemma.

Theorem 3.1 presents the conditions under which the association relation given by (3.2) becomes an m-class association in the usual sense: We can construct an m-class association scheme by finding out a finite group G with a partition in the form (3.1) satifying the conditions of (3.5).

The corresponding association matrices are then obtained by the following procedure.

Numbering the v elements of G in any way, let us put

$$G = \{a_0 = 1, a_1, \ldots, a_{v-1}\}.$$

There are two ways of representing the group G as a regular permutation group, that is, the left regular representation

$$\sigma(x) : \begin{pmatrix} a_0, & a_1, & \cdots, & a_{v-1} \\ xa_0, & xa_1, & \cdots, & xa_{v-1} \end{pmatrix} , \tag{3.9}$$

and the right regular permutation

$$\theta(x) : \begin{pmatrix} a_0 , & a_1 , & \cdots, & a_{v-1} \\ a_0x, & a_1x, & \cdots, & a_{v-1}x \end{pmatrix} . \tag{3.10}$$

For any one of these representations, the left regular representation say, let P(x) be the vxv permutation matrix corresponding to the permutation $\sigma(x)$. Then, the set of v permutation matrices,

$$\Pi = \{P(x) \mid x \in G\},$$

forms a group of order v isomorphic to G.

Suppose that G has a partition in the form (3.1) satisfying the two conditions of (3.5). For this partition, let us put

$$A_i = \sum_{x \in G_i} P(x), \quad i = 0,1,\ldots,m. \tag{3.11}$$

Then, $A_0 = I_v$, and it is easy to see that the (m+1) matrices satisfy all the conditions of Lemma 1.1, (1.5). Thus it is the set of association matrices of an m-class association scheme with the parameters (1.4).

4. Construction of association schemes from finite groups (1)

As we have seen in the preceding section, it is first necessary to find out a suitable partition of a given finite group, from which we construct an association scheme.

In the present section, we shall construct the so-called extended group divisible association scheme.

Let G be a finite group, and suppose that there exists a chain of m subgroups of G:

$$H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_{m-1} \subset H_m = G, \tag{4.1}$$

where H_{i-1} is a proper subgroup of H_i, $i = 1,\ldots,m$, and $H_0 = \{1\}$.

Let us put

$$/ H_i / = h_i, \quad i = 0,1,\ldots,m-1, \text{ and } / H_m / = /G/ = h_m, \tag{4.2}$$

and therefore $h_0 = 1$ and $h_m = v$. Then, there exists a set of positive integers, $\ell_1,\ldots,\ell_m$, such that

$$h_i = h_{i-1}\ell_i, \quad i = 1,\ldots, m. \tag{4.3}$$

Thus,

$$h_1 = \ell_1, \; h_2 = \ell_1\ell_2, \ldots, \; h_i = \ell_1\ldots\ell_i, \; \ldots, \text{ and} \tag{4.4}$$
$$v = h_m = \ell_1\ldots\ell_m.$$

Let us denote the complementary set of H_{i-1} relative to H_i by $\bar{H}_{i-1}$, $i = 1,\ldots,m$. Then,

$$\begin{aligned} H_1 &= H_0 + \bar{H}_0, \\ H_2 &= H_1 + \bar{H}_1, \\ &\cdots\cdots\cdots\cdots \\ H_{m-1} &= H_{m-2} + \bar{H}_{m-2}, \\ G &= H_{m-1} + \bar{H}_{m-1}. \end{aligned} \tag{4.5}$$

Putting $G_0 = H_0$, $G_1 = \bar{H}_0$, $G_2 = \bar{H}_1, \ldots, G_i = \bar{H}_{i-1}, \ldots, G_m = \bar{H}_{m-1}$, we have a partition

$$G = G_0 + G_1 + \ldots + G_m. \tag{4.6}$$

It is then clear that

$$G_i = G_i^{-1}, \quad i = 0,1,\ldots,m, \tag{4.7}$$

and

$$/\, G_i \,/ = h_i - h_{i-1} = \beta_0 \ldots \beta_{i-1}(\beta_i - 1), \quad i = 1,\ldots,m, \text{ where } \beta_0 = 1. \tag{4.8}$$

It is noted that the relations (4.5) can be rewritten as

$$H_i = G_0 + G_1 + \ldots + G_i, \quad i = 0,1,\ldots,m, \tag{4.9}$$

and conversely

$$G_i = H_i - H_{i-1}, \quad i = 0,1,\ldots,m, \tag{4.10}$$

where we have put $H_{-1} = \emptyset$ (empty).

It follows from (4.10) that, for $j < k$,

$$\begin{aligned} G_j G_k &= (H_j - H_{j-1})(H_k - H_{k-1}) \\ &= H_j H_k - H_j H_{k-1} - H_{j-1} H_k + H_{j-1} H_{k-1} \\ &= h_j H_k - h_j H_{k-1} - h_{j-1} H_k + h_{j-1} H_{k-1} \\ &= (h_j - h_{j-1})(H_k - H_{k-1}) = (h_j - h_{j-1})\, G_k, \end{aligned} \tag{4.11}$$

and for $j = k$,

$$\begin{aligned} G_j^2 &= (H_j - H_{j-1})^2 \\ &= H_j^2 - H_{j-1} H_j - H_j H_{j-1} + H_{j-1}^2 \\ &= h_j H_j - 2h_{j-1} H_j + h_{j-1} H_{j-1} \\ &= (h_j - h_{j-1}) H_j - h_{j-1}(H_j - H_{j-1}) \\ &= (h_j - h_{j-1})(G_0 + G_1 + \ldots + G_{j-1}) + (h_j - 2h_{j-1}) G_j, \end{aligned} \tag{4.12}$$

for $j,k = 1,\ldots,m$.

Thus, it holds that

$$(4.13) \qquad G_j G_k = \sum_{i=0}^{m} p_{jk}^{i} G_i, \quad j \leqq k, \ j,k = 0,1,\ldots,m.$$

where

$$(4.14) \qquad \begin{cases} p_{00}^{0} = 1, \quad p_{0k}^{i} = \delta_{ik}, \ i,k = 1,\ldots,m, \\ p_{jk}^{i} = p_{kj}^{i} = \delta_{ik}(h_j - h_{j-1}) = \delta_{ik}\ell_0\ell_1\cdots\ell_{j-1}(\ell_j - 1), \ j < k, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad j,k = 1,\ldots,m, \\ p_{jj}^{i} = \begin{cases} h_j - h_{j-1} = \ell_0\ell_1\cdots\ell_{j-1}(\ell_j - 1), \ 0 \leqq i < j, \\ h_j - 2h_{j-1} = \ell_0\ell_1\cdots\ell_{j-1}(\ell_j - 2), \quad i = j, \\ 0, \text{ otherwise.} \end{cases} \end{cases}$$

The m-class association scheme thus constructed is the so-called extended group divisible association scheme.

In the case $m = 2$, this gives a 2-class association scheme of the group divisible type : Putting $h_0 = \ell_0 = 1$, $h_1 = \ell_1 = n$, $h_2 = mn$, $\ell_2 = m$, as in the usual notation, it follows from (4.14) that

$$(4.15) \qquad \begin{cases} v = mn, \ n_1 = n-1, \ n_2 = n(m-1), \\ p_{11}^{1} = n-2, \ p_{12}^{1} = p_{21}^{1} = 0, \ p_{22}^{1} = n(m-1) \\ p_{11}^{2} = 0, \ p_{12}^{2} = p_{21}^{2} = n-1, \ p_{22}^{2} = n(m-2), \end{cases}$$

which gives the parameters of a 2-class association scheme of the group divisible type.

The above argument says that if a partition of a given group G

$$(4.16) \qquad G = G_0 + G_1 + \ldots + G_m$$

is such that the m+1 subsets of G defined by

$$(4.17) \qquad H_i = G_0 + G_1 + \ldots + G_i, \ H_m = G, \ i = 0,1,\ldots,m,$$

form a chain of subgroups of G:

$$(4.18) \qquad H_0 \subset H_1 \subset \ldots. \subset H_{m-1} \subset H_m = G$$

then, the partition (4.16) satisfies the two conditions of (3.5) and the resulting association scheme is of the extended group divisible type. Moreover, if we put, $\ell_0 = 1$, and

$$(4.19) \qquad /G_i/ = \ell_0 \ell_1 \cdots \ell_{i-1}(\ell_i - 1), \quad i = 0,1,\ldots,m,$$

then the parameters of the association are given by (4.14).

In the last half of this section, we shall prove that if the partition (4.16) gives an m-class association scheme of the extended group divisible type with the parameters (4.14), assuming that $/H_i/ = h_i$, $i = 0,1,\ldots,m$, then, the $m + 1$ subsets given by (4.17) form a chain of subgroups of G.

To prove this, it suffices, by Lemma 2.3 (ii), to show that

$$(4.20) \qquad H_i^2 = h_i H_i, \quad i = 0,1,\ldots,m.$$

From (4.13) and (4.14) it follows that

$$\begin{aligned} H_i^2 &= (G_0 + G_1 + \ldots + G_i)^2 \\ &= \sum_{j=0}^{i} G_j^2 + 2 \sum_{j<k}^{i} G_j G_k \\ &= \sum_{j=0}^{i} \sum_{s=0}^{m} p_{jj}^s G_s + 2 \sum_{j<k}^{i} \sum_{s=0}^{m} p_{jk}^s G_s , \end{aligned}$$

for $i = 1,\ldots,m-1$.

Here we have

$$\begin{aligned} \sum_{j=0}^{i} \sum_{s=0}^{m} p_{jj}^s G_s &= \sum_{s=0}^{m} p_{00}^s G_s + \sum_{j=1}^{i} \sum_{s=0}^{m} p_{jj}^s G_s \\ &= G_0 + \sum_{j=1}^{i} \Big(\sum_{s=0}^{j-1} (h_j - h_{j-1}) G_s + (h_j - 2h_{j-1}) G_j \Big), \end{aligned}$$

and also

$$\sum_{j<k}^{i} \sum_{s=0}^{m} p_{jk}^{s} G_s = \sum_{j<k}^{i} (h_j - h_{j-1}) G_k$$

$$= \sum_{k=1}^{i} G_k \sum_{j=0}^{k-1} (n_j - n_{j-1})$$

$$= \sum_{k=1}^{i} h_{k-1} G_k \ .$$

Hence, it follows that

$$H_i^2 = G_0 + \sum_{j=1}^{i} (h_j - h_{j-1})(G_0 + G_1 + \ldots + G_{j-1}) + \sum_{j=1}^{i} (h_j - 2h_{j-1}) G_j + 2 \sum_{k=1}^{i} h_{k-1} G_k$$

$$= h_i \sum_{j=0}^{i} G_j = h_i H_i,$$

which proves (4.20), and therefore H_i is a subgroup of G, $i = 1, \ldots, m$.

5. Construction of association schemes from finite groups (2)

In the present section, we shall consider a series of association schemes which are constructed from direct product of a finite group. The resulting schemes are seen to be of an extended L_2 type.

Let H be a group of order n, and let G be the m-fold firect product of H:

$$G = H \times H \times \ldots \times H, \tag{5.1}$$

whose elements being denoted by $(a_1, \ldots, a_m)$, $a_i \in H$, $i = 1, \ldots, m$. It is then clear that

$$/G/ = n^m , \tag{5.2}$$

and the unit element of G is $(1, \ldots, 1)$, 1 being the unit element of H.

Now, let us put

$$
(5.3)\qquad
\begin{cases}
G_0 = \{(1,\ldots,1)\}, \\
G_1 = \{(a_1,1,\ldots,1),\ldots,(1,\ldots,1,a_m) \mid a_i \in H,\ a_i \neq 1\ \}, \\
\quad\ldots\ldots\ldots\ldots \\
G_i = \text{the set of all elements of G whose i components are not} \\
\qquad \text{the unit element and the rest (m-i) components are the} \\
\qquad \text{unit element,} \\
\quad\ldots\ldots\ldots\ldots \\
G_m = \{(a_1,\ldots,a_m) \mid a_i \in H,\ a_i \neq 1,\ i = 1,\ldots,m\}.
\end{cases}
$$

It is obvious that

$$
(5.4)\qquad /G_i/ = \binom{m}{i} (n-1)^i,\quad i = 0,1,\ldots,m,
$$

and G is partitioned in the form

$$
(5.5)\qquad G = G_0 + G_1 + \ldots + G_m.
$$

It is also clear that

$$
(5.6)\qquad G_i^{-1} = G_i,\quad i = 0,1,\ldots,m.
$$

We shall check that the partition (5.5) satisfies the condition (ii) of (3.5) for some set of integers, p_{jk}^i.

Let us assume that $j \leq k$ and let $z = (z_1,\ldots,z_m)$ belong to G_i. Let, for z, N(z) and I(z) be the sets of all positions on which the component of z takes non-unity element and the unit element of H, respectively. Then, $/N(z)/ = i$ and $/I(z)/ = m-i$, and hence $/N(z)/ + /I(z)/ = m$.

Suppose that the equality

$$z = x\,y$$

holds for a pair $\{x,y\}$, $x = (x_1,\ldots,x_m) \in G_j$ and $y = (y_1,\ldots,y_m) \in G_k$. Then, N(z) can be divided into three parts:

$$N(z) = N_1(z) + N_2(z) + N_3(z),$$

where $N_1(z)$ is the set of positions on which z, x and y take non-unity elements (not all the same) of H, $N_2(z)$ the set of positions on which z and x take non-unity and y takes the unit element, and finally $N_3(z)$ the set of positions on which z and y take non-unity and x takes the unit element.

Likewise, I(z) can be divided into two parts:

$$I(z) = I_1(z) + I_2(z),$$

where $I_1(z)$ is the set of positions on which both x and y take non-unity and z takes the unit element, and $I_2(z)$ is the set of positions on which z, x and y take the unit element of H.

Let

$$/N_1(z)/ = s, \quad /N_2(z)/ = u \text{ and } /I_1(z)/ = t.$$

Then, it follows that

$$/N_3(z)/ = i-s-u, \text{ and } /I_2(z)/ = m-i-t.$$

The relations which must be satisfied by these numbers are

$$(5.7) \qquad \begin{cases} 0 \leqq s,\ u,\ t \leqq m, \\ s + u \leqq i, \\ s + u + t = j, \\ s + (i - s - u) + t = k, \end{cases}$$

from the last two of which we have

$$(5.8) \qquad \begin{cases} t = k - i + u, \\ s = (i + j - k) - 2u. \end{cases}$$

Since $s \geqq 0$ and $0 \leqq s + u \leqq i$, we have $0 \leqq i + j - k - u \leqq i$, or equivalently

$$(5.9) \qquad j-k \leqq u \leqq (i + j - k)/2.$$

On the other hand, $m - i \geqq t \geqq 0$ implies that

(5.10) $$m - i \geqq k - i + u \geqq 0, \text{ or } i - k \leqq u \leqq m - k.$$

Thus, it is seen from (5.9) and (5.10) that the number u should satisfy the following inequalities

(5.11) $$\alpha(i,j,k) \leqq u \leqq \beta(i,j,k),$$

where

(5.12) $$\begin{cases} \alpha(i,j,k) = \max(0, i-k), \\ \beta(i,j,k) = \min(i, m-k, \frac{i+j-k}{2}). \end{cases}$$

Now, we can see that, for any fixed $z \in G_i$, the number of pairs $\{x,y\}$, with $x \in G_j$, $y \in G_k$, such that $xy = z$ is given by

(5.13) $$\Sigma \frac{i!}{s!u!(i-s-u)!} \binom{m-i}{t} (n-2)^s (n-1)^t,$$

where the summation is taken over all integers, s, u, and t, satisfying the conditions (5.7). This can be rewritten as

(5.14) $$p_{jk}^i = \sum_{u=\alpha(i,j,k)}^{\beta(i,j,k)} \frac{i!}{(i+j-k-2u)!u!(k-j+u)!} \binom{m-i}{k-i+u} (n-2)^{i+j-k-2u} (n-1)^{k-i+u}$$

where $p_{jk}^i = 0$ if $\alpha(i,j,k) > \beta(i,j,k)$.

This gives us the values of p_{jk}^i for $j \leqq k$. Since $p_{jk}^i = p_{kj}^i$, the above exhausts all the cases.

Hence, for the group G given by (5.1), the partition (5.5) gives us an m-class association scheme whose parameters being $v = n^m$ and p_{jk}^i, $i,j,k = 0,1,\ldots,m$, given by (5.13). This is regarded as an extension of the usual L_2 type. In fact, in the special case m = 2, this gives us the 2-class association scheme of L_2 type, whose parameters being calculated by (5.13) as follows:

$$
\begin{aligned}
&p_{00}^0 = p_{10}^0 = p_{01}^0 = p_{20}^0 = p_{02}^0 = p_{12}^0 = p_{21}^0 = 0,\\
&p_{11}^0 = 2(n-1),\ p_{22}^0 = (n-1)^2,\ p_{10}^1 = p_{01}^1 = 1,\\
&p_{02}^1 = p_{20}^1 = 0,\ p_{11}^1 = (n-2),\ p_{12}^1 = p_{21}^1 = (n-1),\\
&p_{22}^1 = (n-1)(n-2),\ p_{00}^2 = p_{01}^2 = p_{10}^2 = 0\\
&p_{20}^2 = p_{02}^2 = 1,\ p_{11}^2 = 2,\ p_{12}^2 = p_{21}^2 = 2(n-2),\\
&p_{22}^2 = (n-2)^2.
\end{aligned}
\tag{5.15}
$$

In this case, the following method of calculation is more convenient: We shall write as (H,H) instead of $H \times H$, i.e., in general, Let

$$(H,K) = \{(x,y) \mid x \in H,\ y \in K\}.$$

Then, in the case m=2, the partition (5.5) becomes

$$G = G_0 + G_1 + G_2,$$

where $G = (H,H)$, $G_0 = (H_0,H_0)$, $G_1 = (H_1,H_0)+(H_0,H_1)$ and $G_2 = (H_1,H_1)$, with $H_0 = \{1\}$ and $H_1 = H - H_0$.

Bu using the relation

$$H_1^2 = (n-1)H_0 + (n-2)H_1,$$

we can obtain the following:

$$
\begin{aligned}
G_1^2 &= (H_1,H_0)^2 + 2(H_1,H_0)(H_0,H_1) + (H_0,H_1)^2\\
&= (H_1^2,H_0^2) + 2(H_1H_0,H_0H_1) + (H_0^2,H_1^2)\\
&= ((n-1)H_0+ (n-2)H_1,\ H_0) + 2(H_1,H_1)+(H_0,(n-1)H_0+(n-2)H_1)\\
&= 2(n-1)\ G_0 + (n-2)\ G_1 + 2\ G_2,
\end{aligned}
$$

$$
\begin{aligned}
G_1\ G_2 &= (H_1^2,H_1) + (H_1,H_1^2)\\
&= ((n-1)H_0+(n-2)H_1,H_1) + (H_1,(n-1)H_0+(n-2)H_1)\\
&= (n-1)G_1 + 2(n-2)G_2,
\end{aligned}
$$

and finally

$$G_2^2 = (H_1^2, H_1^2)$$
$$= ((n-1)H_0+(n-2)H_1,\ (n-1)H_0 + (n-2)H_1)$$
$$= (n-1)^2 G_0 + (n-1)(n-2) G_1 + (n-2)^2 G_2.$$

These equalities give the parameters (5.15).

It should be remarked that, for the general case,

$$G_1^2 = m(n-1)G_0 + (n-2) G_1 + 2 G_2 ,$$

and if we define the association in such a way that two elements, x, y, of G_1 are 1st associates if and only if $x^{-1} y \in G_1$ and 2nd associates if and only if $x^{-1}y \in G_2$, then we have a 2-class association shceme on the m(n-1) elements of G_1, induced from the original association scheme, and this turns out to be a 2-class association scheme of group divisible type.

6. Construction of association schemes from finite groups (3)

In the present section, we shall construct an association scheme of extended T_2 type, that is, an m-class association scheme from which a 2-class association scheme of triangular type is induced.

Let G be a finite group generated by the m generators

(6.1) $$a_1, a_2, \ldots, a_m,$$

subject to the generating relations

(6.2) $$a_i^2 = 1 \text{ and } a_i a_j = a_j a_i,\ i,j = 1,\ldots,m.$$

Let us define

(6.3)
$$\begin{cases} G_0 = 1, \\ G_1 = a_1, \ldots, a_m \\ \quad \ldots\ldots\ldots \\ G_i = \{a_{j_1} a_{j_2} \ldots a_{j_i} \mid \quad 1 \leq j_1 < \ldots < j_i \leq m \} \\ \quad \ldots\ldots\ldots \\ G_m = \{a_1 \ldots a_m\}. \end{cases}$$

Then, these subsets of G form a partition of G:

$$G = G_0 + G_1 + \ldots + G_m, \tag{6.4}$$

for which it is evident that

$$/G/ = 2^m, \quad /G_i/ = \binom{m}{i}, \quad i = 0,1,\ldots,m, \tag{6.5}$$

and

$$G_i = G_i^{-1}, \quad i = 0,1,\ldots,m. \tag{6.6}$$

The group thus defined is isomorphic to the additive group V_m, consisting of all binary m-vectors whose components are from the Galois field GF(2). Thus, if we denote V_m by G, then G_i given by (6.3) are

$$\begin{cases} G_0 = \{(0,\ldots,0)\}, \\ G_1 = \{(1,0,\ldots,0),\ldots,\ (0,\ldots,0,1)\} \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ G_i = \{(0,\ldots,0,\overbrace{1}^{j_1},0,\overbrace{1}^{j_2},0,\ldots,\overbrace{1}^{j_i},0,\ldots,0) \mid 1 \le j_1 \le \ldots \le j_m \le m\}, \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ G_m = \{(1,\ldots,1)\}. \end{cases} \tag{6.7}$$

Now, let z be any given element of G_i. We want to get the numbers of pairs x, y such that $x \in G_j$, $y \in G_k$ and

$$x + y = z. \tag{6.8}$$

It is seen that this relation holds true when and only when

(i) among the i positions on which z takes 1, ℓ positions are occupied by 1 of x and by 0 of y, and the rest $i - \ell$ positions are occupied by 1 of y and by 0 of x, and (ii) among the $m - i$ positions on which z takes $0, j - \ell$ positions are occupied by 1 of both x and y.

Then, the number ℓ must satisfy the following relations.

$$(6.9)\qquad \begin{cases} 0 \leqq \ell \leqq i, \\ i + j - 2\ell = k, \end{cases}$$

from which it follows that

$$(6.10)\qquad 0 \leqq \ell = \frac{i+j-k}{2} \leqq i.$$

Hence, the relation (6.8) holds for some pairs x, y only when the inequalities (6.10) are satisfied, and the number of such pairs is given by

$$(6.11)\qquad \binom{i}{\ell}\binom{m-i}{j-\ell} = \binom{i}{\frac{i+j-k}{2}} \binom{m-i}{\frac{j+k-i}{2}} .$$

Let us put

$$(6.12)\qquad p_{jk}^{i} = \begin{cases} \binom{i}{\frac{i+j-k}{2}}\binom{m-i}{\frac{j+k-i}{2}}, & \text{if } i+k-j \geq 0, \text{ and both } \frac{i+j-k}{2} \text{ and } \frac{j+k-i}{2} \\ & \text{are non-negative integers,} \\ 0, \text{ otherwise.} \end{cases}$$

Then, we have

$$(6.13)\qquad G_j G_k = \sum_{i=0}^{m} p_{jk}^{i} G_i, \quad j,k = 0,1,\ldots,m.$$

This condition, together with (6.6), gives us an m-class association scheme with parameters $v = 2^m$ and p_{jk}^{i} given by (6.12).

It is easy to see that

$$(6.14)\qquad \bar{G} = G_0 + G_2 + G_4 + \ldots + G_{2i} + \ldots + G_{2[m/2]},$$

[ ] being the usual Gauss symbol, is a subgroup of order 2^{m-1}. From (6.12) and (6.13) it follows that

$$(6.15)\qquad \begin{cases} G_{2j}^2 = \sum_{i=0}^{s} \binom{2i}{i}\binom{m-2i}{2j-i} G_{2i}, & j = 0,1,\ldots,s, \\ G_{2j}G_{2k} = \sum_{i=\max(0,j-k)}^{j+k} \binom{2i}{i+j-k}\binom{m-2i}{j+k-i} G_{2i}, & j,k=0,1,\ldots,s, \end{cases}$$

where we have put $s = [m/2]$. Since, putting $\bar{z} = 1-z$, 1 being the vector $(1,\ldots,1)$, we have $x+y = \bar{x}+\bar{y}$, it also follows that

$$G_i\, G_j = G_{m-i}\, G_{m-j},\quad i,j = 0,1,\ldots,m. \tag{6.16}$$

The relations (6.15) show that the partition (6.14) gives us an s-class association scheme with the parameters given by (6.15), which is defined on $\bar{G}$.

In the final place, we shall examine the association relation on G_2 induced from the association schemes given above.

From (6.15) we see that

$$G_2^2 = \binom{n}{2} G_0 + 2(n-2)\, G_2 + 6\, G_4\ . \tag{6.17}$$

We shall say that two elements x, y of G_2 are 1st associates or 2nd associates according respectively as $x^{-1}y \in G_2$ or as $x^{-1}y \in G_4$. Then, it is easy to check that the resulting association scheme is of the usual triangular type, whose parameters are

$$\begin{aligned} &v = \binom{n}{2},\ n_1 = 2(n-2),\ n_2 = \binom{n-2}{2}, \\ &p_{11}^1 = n-2,\ p_{12}^1 = p_{21}^1 = n-3,\ p_{22}^1 = \binom{n-3}{2}, \\ &p_{11}^2 = 4,\ p_{12}^2 = p_{21}^2 = 2(n-4),\ p_{22}^2 = \binom{n-4}{2}. \end{aligned} \tag{6.18}$$

7. Construction of association schemes from finite groups (4)

Let G be an abelian group of order v, and suppose that the partition

$$G = G_0 + G_1 + \ldots + G_m, \tag{7.1}$$

satisfies the following conditions:

(7.2) (i) $/G_i/ = n$, $i = 1,\ldots,m$,

(ii) $G_0 + G_i$ is a subgroup of G, $i = 1,\ldots,m$, and

(iii) for any given i and j ($i \neq j$), there exists n integers $k(i,j)_u$, $u = 1,\ldots,n$, such that

$$G_iG_j = \sum_{u=1}^{n} G_{k(i,j)_u} .$$

Then, it is clear that $v = nm + 1$, and $(n+1)^2$ divides v.

We first note that a sufficient condition for the condition (iii) in (7.2) to be satisfied under the other conditions is that each G_0+G_i has no proper subgroup other than G_0. This is shown easily as follows: Since $(G_0+G_i)(G_0+G_j)$ is a subgroup of G, containing G_i+G_j, it is true that, for any k ($\neq i,j$), the set

$$(G_0+G_i)(G_0+G_j) \cap (G_0+G_k) = G_0 + (G_iG_j \cap G_k)$$

is a subgroup of G, from which it follows that

$$G_iG_j \cap G_k = G_k, \text{ or } = \emptyset \text{ (empty)}.$$

This implies the condition (iii).

Since

$$(G_0+G_i)(G_0+G_j) = G_0+G_i+G_j+G_iG_j,$$

it is seen that, under the conditions given by (7.2), the subset of G,

$$H(i,j) = G_0 + G_i + G_j + \sum_{u=1}^{n} G_{k(i,j)_u} \tag{7.3}$$

forms a subgroup of G, for any i and j, $i \neq j$. It is also seen easily that H(i,j) is a minimal subgroup of G, which contains G_i+G_j, in the sense that there is no proper subgroup of H(i,j) which contains G_i+G_j.

The above condition is equivalent to the condition (iii) of (7.2), as will be stated in the following

LEMMA 7.1. Suppose, for the partition (7.1) of G, the conditions (i) and (ii) of (7.2) are satisfied. Then, for the condition (iii) of (7.2) it is necessary and sufficient that for any given i and j, $i \neq j$, there exist a set of n integers $k(i,j)_u$, $u = 1,\ldots,n$, such that the subset H(i,j) defined by (7.3) forms a subgroup of G.

In fact, if H(i,j) forms a subgroup of G, G_iG_j should be contained in H(i,j), but G_iG_j and G_i+G_j are disjoint. Hence, by comparing the cardinalities of G_iG_j and H(i,j), we have the sufficiency of the lemma.

We can show also that

LEMMA 7.2. Under the same situation as in the above lemma, suppose that for a set of (n+2)G_i's $\{G_{i_j}\}$, $j = 1,\ldots,n+2$,

$$G_0 + G_{i_1} + \ldots + G_{i_{n+2}} \tag{7.4}$$

forms a subgroup of G. Then, for any given j_1 and j_2 distinct, it holds that

$$G_{i_{j_1}} G_{i_{j_2}} = \sum_{j \neq j_1, j_2} G_{i_j} \quad . \tag{7.5}$$

The proof of this lemma is quite similar to that of the preceding lemma and will be omitted.

It is now evident that, under the conditions of (7.2), for any given i and j distinct there exists a unique set of n G_i's satisfying the equality given in (iii) of (7.2). Simplifying the notation of suffix, let them be

$$\mathfrak{M}(i,j) = \{G_i, G_j, G_{k_1}, \ldots, G_{k_n}\}. \tag{7.6}$$

Lemmas 7.1 and 7.2 say then that this set of G_i's is determined uniquely by giving any pair of G_i's in the set.

Let G_u be outside of the set $\mathfrak{M}(i,j)$ given by (7.6). Then, for any G_k

in $\mathfrak{H}(i,j)$ it is easy to see that

$$\mathfrak{H}(i,j) \cap \mathfrak{H}(k,u) = G_k, \tag{7.7}$$

and

$$G_u G_k \cap (G_0+G_i+G_j+G_{k_1}+\ldots+G_{k_n}) = \emptyset. \tag{7.8}$$

Hence, the family of all $\mathfrak{H}(i,j)$'s mutually distinct is a configuration satisfying the condition that

(7.9) $\mathfrak{H}(i,j)\cap \mathfrak{H}(s,t) = \emptyset$, or $= G_k$ for some k, that is, any pair of such $\mathfrak{H}(i,j)$'s do not possess more than one G_k's in common.

We shall prove the following

LEMMA 7.3. Under the conditions of (7.2), it holds that

$$\sum_{i<j} G_i G_j = \frac{n(m-1)}{2} \sum_{i=1}^{m} G_i. \tag{7.10}$$

PROOF. First it is noted that

$$\begin{cases} G_i^2 = nG_0 + (n-1)G_i, & i = 1,\ldots,m, \\ G^2 = vG = (nm+1)\,G. \end{cases} \tag{7.11}$$

Now,

$$\begin{aligned} G^2 &= \Big(\sum_{i=0}^{m} G_i\Big)^2 = \Big(G_0 + \sum_{i=1}^{m} G_i\Big)^2 \\ &= G_0^2 + 2G_0 \sum_{i=1}^{m} G_i + \Big(\sum_{i=1}^{m} G_i\Big)^2 \\ &= G_0 + 2\sum_{i=1}^{m} G_i + \sum_{i=1}^{m} G_i^2 + 2\sum_{i<j} G_i G_j \\ &= G_0 + 2\sum_{i=1}^{m} G_i + \sum_{i=1}^{m} (nG_0+(n-1)G_i) + 2\sum_{i<j} G_i G_j. \end{aligned}$$

Hence we have the identity

$$vG = G_0 + 2 \sum_{i=1}^{m} G_i + nmG_0 + (n-1) \sum_{i=1}^{m} G_i + 2 \sum_{i<j} G_iG_j,$$

from which it follows that

$$2 \sum_{i<j} G_iG_j = n(m-1) \sum_{i=1}^{m} G_i,$$

or equivalently (7.10).

This proves the lemma.

The identity (7.10) means that, for any fixed k, G_k is contained in exactly $n(m-1)/2$ of all $\binom{m}{2}$ $H(i,j)$'s, provided that $n(m-1)/2$ is a positive integer.

Let μ be the number of distinct $H(i,j)$'s which contain G_k. Then, since for each $H(i,j)$ containing G_k there are $\binom{n+1}{2}$ $H(i',j')$ which coincide with $H(i,j)$, it should be true that

$$\frac{n(m-1)}{2} = \mu \binom{n+1}{2},$$

from which we have

$$\mu = \frac{m-1}{n+1}, \tag{7.12}$$

and this value does not depend on any given G_k.

Thus we have seen that each G_k is contained in exactly $(m-1)/(n+1)$ distinct $H(i,j)$'s. It is also clear that any given pair G_k and G_u are contained in exactly one $H(i,j)$ belonging to $\mathfrak{B}$, the family of all distinct $H(i,j)$'s.

Thus we can state the following

THEOREM 7.1. Suppose that the conditions (i) through (iii) of (7.2) are satisfied for a partition (7.1) of an abelian group G of order nm+1, and that (a) $(n+1)^2$ divides nm+1, (b) n(m-1) is even and (c) (n+1)(n+2) divides m(m-1).

Then, the family $\mathfrak{B}$ is a (v,k,λ)-configuration ([5]), where

$$v = m,\ k = n+2,\ \lambda = 1, \tag{7.13}$$

and the other parameters are given by

$$b = \frac{m(m-1)}{(n+1)(n+2)},\quad r = \frac{m-1}{n+1}\ . \tag{7.14}$$

It should be remarked that the configuration of this theorem is a balanced incomplete block design with the parameters given above. It is also noted that the condition (a) in the theorem implies that n+1 divides m-1.

COROLLARY 7.1. If a partition (7.1) satisfying the conditions of (7.2) actually exists for some abelian group, and the conditions (a), (b) and (c) of the above theorem, then a BIB design with the parameters given by (7.13) and (7.14) can be constructed.

THEOREM 7.2. If there exists an abelian group G with the partition (7.1) satisfying the conditions of (7.2), then there can be found an m-class association scheme, whose parameters being given by

$$v = nm+1,\ n_i = n,\ i = 1,\ldots,m, \tag{7.15}$$

$$p_{jk}^{i} = \begin{cases} 1, & \text{if } G_i, G_j \text{ and } G_k \text{ belong to the same class} \\ & \text{in } \mathfrak{B}, \text{ and } j \neq k, \\ n-1, & \text{if } i = j = k, \\ 0, & \text{otherwise,} \end{cases} \qquad (i,j,k = 1,\ldots,m).$$

PROOF. By the preceding theorem, we can see that for any given j and k distinct there exists exactly one class, $\mathfrak{H}(t,u)$ say, in $\mathfrak{B}$ such that $\mathfrak{H}(j,k) = \mathfrak{H}(t,u)$.

Hence the theorem follows from Lemma 7.2.

In the case $n = s-1$ and $v = s^t$, where s is any prime power and t is any positive integer greater than 2, and hence $m = (s^t-1)/(s-1)$, the association scheme given in the above theorem is the geometrical association scheme given by Y. Fujii [6], basing upon the structure of finite projective geometty.

We shall give an algebraic derivation of this scheme.

Let s be a power of a prime. Then, there exists a finite field isomorphic to the Galois field GF(s).

Let us consider the vector space over GF(s):

$$V_{(t)} = \{(\alpha_1,\ldots,\alpha_t) \mid \alpha_i \in GF(s),\ i = 1,\ldots,t\ \}, \tag{7.16}$$

the cardinality of which is given by

$$s^t = \sum_{i=0}^{t} \binom{t}{i}(s-1)^i. \tag{7.17}$$

Thus, we have

$$m = \frac{s^t-1}{s-1} = \sum_{i=1}^{t} \binom{t}{i}(s-1)^{i-1}. \tag{7.18}$$

It is evident that $V_{(t)}$ is an abelian group of order $v = s^t$ with respect to the vector addition, whose unit is $\underline{0} = (0,\ldots,0)$.

Let us put $B_0 = \{\underline{0}\}$.

The expansion of m in the form (7.18) suggests us the following way of partitioning $V_{(t)}$.

Let U_i be the set of all vectors in $V_{(t)}$, i components of which are occupied by 1 and the rest t-i by 0. It is then clear that

$$/U_i/ = \binom{t}{i}, \quad i = 1,\ldots,t. \tag{7.19}$$

For any given vector

$$\underline{\epsilon} = (0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0),$$

let us put

$$W(\underline{\epsilon}) = \{(0,\ldots,0,1,0,\ldots,0,\alpha_1,0,\ldots,0,\alpha_2,0,\ldots,0,\alpha_{i-1},0,\ldots,0) \mid \alpha_j \in GF(s),\ \alpha_j \neq 0,\ j = 1,\ldots,i-1)\},$$

and

$$W(U_i) = \sum_{\underline{\epsilon} \in U_i} W(\underline{\epsilon}), \quad i = 1,\ldots,t.$$

Then it is clear that $W(U_i)$ contains $\binom{t}{i}(s-1)^{i-1}$ distinct vectors, $i=1,\ldots,t$.

Now, put

$$W = W(U_1) + \ldots + W(U_t). \tag{7.20}$$

Then, the cardinality of this set is equal to m. Let us number just for convenience the whole vectors in W in any way but once for each:

$$W = \{\underline{\alpha}_1,\ldots,\underline{\alpha}_m\}. \tag{7.21}$$

For each vector $\underline{\alpha}_u$ of W, let us define

$$V_u = \{\lambda\underline{\alpha}_u \mid \lambda \in GF(s),\ \lambda \neq 0\},\ u = 1,\ldots,m. \tag{7.22}$$

Writing $V_{(t)}$ simply as V, we then have the partition

$$V = V_0 + V_1 + \ldots + V_m, \tag{7.23}$$

for which it is seen that

$$/V_i/ = s-1,\ i = 1,\ldots,m, \tag{7.24}$$

and for each i, V_0+V_i forms a subgroup of V, $i = 1,\ldots,m$.

It is also shown that the condition (iii) of (7.2) is satisfied in the present case as follows: First it is easy to see that any two vectors in W are linearly independent. For any given j and k distinct, therefore,

$$V_jV_k = \{\lambda\underline{\alpha}_j + \mu\underline{\alpha}_k \mid \lambda, \mu \in GF(s),\ \lambda\mu \neq 0\},$$

has $(s-1)^2$ elements. Putting $\gamma = \mu/\lambda$, the above can be rewritten as

$$V_j V_k = \sum_{\substack{\gamma \in GF(s) \\ \gamma \neq 0}} \{\lambda \underline{\alpha}_j + \gamma \underline{\alpha}_k) \mid \lambda \in GF(s), \ \lambda \neq 0\}.$$

For any given γ ($\neq 0$), there exists exactly one V_u, to which $\underline{\alpha}_j + \gamma \underline{\alpha}_k$ belongs, and for this V_u, it holds that

$$V_u = \{\lambda(\underline{\alpha}_j + \gamma \underline{\alpha}_k) \mid \lambda \in GF(s), \ \lambda \neq 0\}.$$

It is also seen that if γ and γ' are distinct non-zero elements of GF(s), then $\underline{\alpha}_j + \gamma \underline{\alpha}_k$ and $\underline{\alpha}_j + \gamma' \underline{\alpha}_k$ do not belong to the same V_u. Thus, we have

$$V_j V_k = V_{u_1} + \ldots + V_{u_{s-1}}, \tag{7.25}$$

for some sets, $V_{u_1}, \ldots, V_{u_{s-1}}$.

Thus the partition (7.23) meets the three conditions of (7.2), and therefore we have an m-class association scheme equivalent to that of geometrical type.

REFERENCES

[1] I.M. Chakravarti and W.C. Blackwelder, "On some composition and extension methods in the construction of block designs from association matrices," (Read at Symposium on Combinatorial Mathematics, 1967, at Chapel Hill).

[2] H.B. Mann (1964), "Balanced incomplete block designs and Abelian difference sets", Illinois Jour. Math., 8, 252-261.

[3] W.A. Thompson, Jr. (1958), "A note on PBIB design matrices", Ann.Math. Statist., 29, 919-922.

[4] M. Masuyama, Calculus of blocks, Lecture note, 1965-1966, Dept. Statist., U.N.C.

[5] H.J. Ryser (1963), Combinatorial Mathematics, The Carus Math. Monographs, 14.

[6] Y. Fujii (1967), "Geometrical association schemes and fractional factorial designs", Jour. Scie. Hiroshima Univ., Japan, Ser.A-I, Vol.31, 195-209.