BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 14, Number 3, September 1986

EXISTENCE AND NON-EXISTENCE OF ASSOCIATION SCHEMES*

BY

GERARD J. CHANG (張鎮華)

Abstract. A $(v, n+1)$-association scheme is a set $S=\{A_0=I, A_1, \ldots, A_n\}$ of $n+1$ symmetric (0, 1)-matrices of order $v\times v$ such that (i) $\sum_{i=0}^{n} A_i = J$ (the all-ones matrix), (ii) $A_i A_j = \sum_{k=0}^{n} a_{ijk} A_k$ for $0\leq i, j\leq n$, where a_{ijk} are non-negative integers. The main purpose of this paper is to study the existence or non-existence of a $(v, n+1)$-association scheme for certain parameters v and n, especially for the case of v is a power of two.

1. Introduction. An *association scheme with n classes* (or relations) consists of a finite set X of $v\geq 2$ elements together with $n+1$ non-empty relations $R_0, R_1, \cdots, R_n$ defined on X which satisfy conditions (R1) to (R4).

(R1) Each R_i is symmetric, i.e. $(x, y)\in R_i$ implies $(y, x)\in R_i$.

(R2) For every $x, y\in X$, $(x, y)\in R_i$ for exactly one i.

(R3) $R_0=\{(x, x) : x\in X\}$ is the identity relation.

(R4) If $(x, y)\in R_k$, the number of $z\in X$ such that $(x, z)\in R_i$ and $(y, z)\in R_j$ is a constant a_{ijk} depending on i, j, k but not on the particular choice of x and y.

Association schemes were first introduced by statisticians in connection with the design of experiments ([5], [6], [12], [14], [15], [16], [19]), and have since proved very useful in the study of permutation groups ([7], [10], [11], [18]), graphs ([1], [2], [3], [8]), and coding theory ([9], [13]).

In this paper we call an association scheme with n classes on

Received by the editors June 23, 1984 and revised May 23, 1985.
* This research was supported by National Science Council of Republic of China under Grant NSC73-0208-M008-08
Key words: association scheme, adjacency matrix, group, Kronecker product.
AMS subject classification. 05B30.

a set of v elements a $(v, n+1)$-*association scheme* or simply a $(v, n+1)$-*scheme*. We describe the relations by their *adjacency matrices* A_i which are the $v \times v$ matrices with rows and columns labeled by the elements of X and defined by

$$(A_i)_{xy} = \begin{cases} 1 & \text{if } (x, y) \in R_i, \\ 0 & \text{otherwise.} \end{cases}$$

The definition of an association scheme is equivalent to saying that the A_i are non-zero $v \times v$ (0, 1)-matrices which satisfy conditions (A1) to (A4). (We often use the set $\mathcal{S} = \{A_0, \cdots, A_n\}$ to denote the association scheme.)

(A1) Each A_i is symmetric, i.e. $A_i = A_i^t$.

(A2) $\sum_{i=0}^n A_i = J$ (the all-ones matrix).

(A3) $A_0 = I$.

(A4) $A_i A_j = \sum_{k=0}^n a_{ijk} A_k, \quad i, j = 0, 1, \cdots, n$.

(A1), (A2), and (A4) together imply

(A5) $A_i A_j = A_j A_i, \quad i, j = 0, 1, \cdots, n$.

Summing up the equalities in (A5) for all j, we can see that every A_i has a constant row sums and column sums v_i i.e.

(A6) $A_i J = J A_i = v_i J, \quad i = 0, 1, \cdots, n$.

Other relations on a_{ijk} are listed below (see [13]).

(A7)
$$a_{ii0} = v_i, \quad a_{ijk} = a_{jik}, \quad a_{0jk} = \delta_{jk},$$
$$v_k a_{ijk} = v_i a_{kji}, \quad \sum_{j=0}^n a_{ijk} = v_i,$$
$$\sum_{r=0}^n a_{ijr} a_{rkm} = \sum_{s=0}^n a_{ism} a_{jks}.$$

The existence of special association schemes, such as Hamming schemes, spectral schemes, cyclotomic schemes, Lee schemes, have been extensively studied, see section 2.5 of [9], for some recent results see [20, 21].

The main purpose of this paper is to study conditions on the parameters v and n for which a $(v, n+1)$-scheme exists or does not exist. In section 2, we prove some theorems on association schemes. Section 3 discusses constructions of association schemes from association schemes with smaller parameters v and n. Finally, in section 4, we use these results to study the existence and non-existence of $(v, n+1)$-schemes for certain parameters v and n, especially for the case of v is a power of two.

2. **Some theorems on association schemes.** Suppose $\mathscr{S} = \{A_0, A_1, \cdots, A_n\}$ is a $(v, n+1)$-scheme, Let $\mathscr{S}_i$ denote the set of all A_j with $v_j = i$. The following two equalities are important in this paper.

$$|\mathscr{S}_1| + 2|\mathscr{S}_2| + \cdots + v|\mathscr{S}_v| = v. \tag{2.1}$$

$$|\mathscr{S}_1| + |\mathscr{S}_2| + \cdots + |\mathscr{S}_v| = n+1. \tag{2.2}$$

Note that some $\mathscr{S}_i$ may be empty.

$A_0 = I \in \mathscr{S}_1$. For any $A_i \in \mathscr{S}$, $A_i \in \mathscr{S}_1$ if and only if A_i is a permutation matrix; in this case $A_i = A_i^t = A_i^{-1}$. Moreover, we have the following theorems.

THEOREM 2.1 *$\mathscr{S}_1$ is an abelian group under matrix multiplication. In fact, $\mathscr{S}_1$ is isomorphic to $(Z_2)^m$ for some non-negative integer m, and so $|\mathscr{S}_1| = 2^m$.*

Proof. For any pair $A_i, A_j \in \mathscr{S}_1$, $A_i A_j = \sum_{k=0}^{n} a_{ijk} A_k$ implies that $A_i A_j$ has a constant row sums and column sums $\sum_{k=0}^{n} a_{ijk} v_k$. Since A_i and A_j are permutation matrices, so is $A_i A_j$. These imply that $1 = \sum_{k=0}^{n} a_{ijk} v_k$, and so all $a_{ijk} = 0$ except $a_{ijh} = v_h = 1$ for exactly one h, i. e. $A_i A_j = A_h \in \mathscr{S}_1$. This proves that $\mathscr{S}_1$ is closed under matrix multiplication. Also, the identity matrix $I = A_0 \in \mathscr{S}_1$. And for each $A_i \in \mathscr{S}_1$, $A_i^{-1} = A_i \in \mathscr{S}_1$. So $\mathscr{S}_1$ is a group under martix multiplication. By (A5), $\mathscr{S}_1$ is abelian.

The fact that $A_i = A_i^{-1}$ implies that every element of $\mathscr{S}_1$ is of order 2 except $A_0 = I$. By the Basic Theorem of Abelian Group (see [17], Theorem 4.6), $\mathscr{S}_1$ is isomorphic to $(Z_2)^m$ for some non-negative integer m.

THEOREM 2.2 *If $A_i \in \mathscr{S}_1$ and $A_j \in \mathscr{S}_h$, then $A_i A_j \in \mathscr{S}_h$.*

Proof. We will prove the theorem by induction on h. By Theorem 2.1, the theorem is true for the case of $h = 1$. Suppose the theorem holds for all $h' < h \geq 2$. Similar to the proof of

Theorem 2.1, $A_i A_j = \sum_{k=0}^{n} a_{ijk} A_k$ implies that $h = v_j = \sum_{k=0}^{n} a_{ijk} v_k$. Suppose $a_{ijk} = 0$ for all A_k with $v_k \geq h$. Then, by $A_i = A_i^{-1}$,

$$A_j = \sum_{v_k<h} a_{ijk}(A_i A_k). \tag{2.3}$$

By the induction hypothesis, $A_i A_k \in \mathcal{S}_{v_k}$ for all $v_k < h$. (2.3) is impossible since $A_j \in \mathcal{S}_h$ and (A2). Thus $a_{ijk} \geq 1$ for some A_k with $v_k \geq h$. This implies that all $a_{ijk} = 0$ except $a_{ijm} = 1$ and $v_m = h$ for exactly one m, i.e. $A_i A_j = A_m \in \mathcal{S}_h$.

For any $\mathcal{S}_h$, consider the relation $\overset{h}{\sim}$ on $\mathcal{S}_h$ defined by: $A_j \overset{h}{\sim} A_k$ if and only if $A_i A_j = A_k$ for some $A_i \in \mathcal{S}_1$. Using Theorem 2.1, it is easy to check that $\overset{h}{\sim}$ is an equivalence relation on $\mathcal{S}_h$. So $\mathcal{S}_h$ is the disjoint union of equivalence classes $[A_j]$. For each $A_j \in \mathcal{S}_h$, denote $F(A_j) = \{A_i \in \mathcal{S}_1 : A_i A_j = A_j\}$.

THEOREM 2.3 *Suppose $A_j \in \mathcal{S}_h$ and $|\mathcal{S}_1| = 2^m$ as shown in Theorem 2.1. The following statements hold.*

(i) *$F(A_j)$ is a subgroup of $\mathcal{S}_1$, and so $F(A_j) \simeq (Z_1)^{m'}$ for some $m' \leq m$.*

(ii) $|[A_j]| = 2^{m-m'}$.

(iii) $|F(A_j)| \leq h$.

(iv) *$|[A_j])|$ is a multiple of $2^{m-m''}$, where $m'' = \lfloor \log_2 h \rfloor$.*

(v) *$|\mathcal{S}_h| = a\, 2^{m-m''}$ and $h|\mathcal{S}_h| \geq a\, 2^m$ for some positive integer a.*

Proof. (i) Suppose $A_i, A_k \in F(A_j)$, i.e. A_i, $A_k \in \mathcal{S}_1$ and $A_i A_j = A_k A_j = A_j$. Since $A_i^{-1} = A_i \in \mathcal{S}_1$ and $A_i^{-1} A_j = A_i A_j = A_j$, $A_i^{-1} \in F(A_j)$. $A_i A_k \in \mathcal{S}_1$ by Theorem 2.1 and $(A_i A_k) A_j = A_i(A_k A_j) = A_i A_j = A_j$, so $A_i A_k \in F(A_j)$. Also $I = A_0 \in F(A_j)$. These prove that $F(A_j)$ is a subgroup of $\mathcal{S}_1$. $\mathcal{S}_1 = (Z_2)^m$ implies $\mathcal{S}(A_j) \simeq (Z_2)^{m'}$ for some $m' \leq m$.

(ii) Note that $[A_j] = \{A_i A_j : A_i \in \mathcal{S}_1\}$. $A_i A_j = A_k A_j$ if and only if $(A_k A_i) A_j = A_j$ or $A_k A_i \in F(A_j)$. So $|[A_j]| = |\mathcal{S}_1| / |F(A_j)| = 2^{m-m'}$.

(iii) By (A6) and (A4),

$$\begin{aligned} v_j J = J A_j = \sum_{i=0}^{n} A_i A_j &= \sum_{A_i \in F(A_j)} A_i A_j + \sum_{A_i \notin F(A_j)} A_i A_j \\ &= |F(A_j)| A_j + N, \end{aligned}$$

where N is a non-negative matrix. Compare the entries which are ones in A_j, then $h = v_j \geq |F(A_j)|$.

(iv) By (ii) and (iii), $2^{m'} = |F(A_j)| \leq h$, so $m' \leq \log_2 h$. Then $m' \leq m''$ and $|[A_j]| = 2^{m-m'}$ is a multiple of $2^{m-m''}$.

(v) $|\mathcal{S}_h| = a\ 2^{m-m''}$ follows from (iv) and the fact that $\mathcal{S}_h$ is the disjoint union of equivalence classes $[A_j]$. $h \geq 2^{m''}$ implies $h|\mathcal{S}_h| \geq a\ 2^m$.

THEOREM 2.4 *Suppose* $E \subseteq \{1,\cdots, v\}$. *If*

$$\sum_{j \in E} |\mathcal{S}_j| = p = 2^{u_s} + \cdots + 2^{u_1},$$

where $u_s > u_{s-1} > \cdots > u_1 \geq 0$ *are integers, then* $\sum_{j \in E} j|\mathcal{S}_j| \geq s\ 2^m$, *where* $2^m = |\mathcal{S}_1|$.

Proof. We will prove the theorem by induction on p. Suppose $p = 1$, then $p = 2^0$ and there is some $h \in E$ such that $\mathcal{S}_h = \emptyset$. By Theorem 2.3 (v), $h|\mathcal{S}_h| \geq 2^m$. So the theorem holds.

Suppose the theorem holds for all $p' < p = 2^{u_s} + \cdots + 2^{u_1} \geq 2$. Since $u_1 \geq m$ would imply $\sum_{j \in E} j|\mathcal{S}_j| \geq \sum_{j \in E}|\mathcal{S}_j| \geq s\ 2^m$, without loss of generality we assume that $u_1 < m$. Suppose $j < 2^{m-u_1}$ for all $j \in E$. By Theorem 2.3 (v), each $|\mathcal{S}_j|$ is a multiple of $2^{m-m''}$, where $m'' = \lfloor \log_2 j \rfloor < m - u_1$, i. e. $m - m'' \geq u_1 + 1$. Thus $p = \sum_{j \in E}|\mathcal{S}_j|$ is a multiple of 2^{u_1+1} which contradicts $p = 2^{u_s} + \cdots + 2^{u_2} + 2^{u_1}$ and $u_s > \cdots > u_2 \geq u_1 + 1 > u_1$. So there is some $h \in E$ with $h \geq 2^{m-u_1}$. By Theorem 2.3(v), $|\mathcal{S}_h| = a\ 2^{m-m''}$ and $h|\mathcal{S}_h| \geq a\ 2^m$, where a is a positive integer and $m'' = \lfloor \log_2 h \rfloor \geq m - u_1$, i. e. $2^{m-m''} \leq 2^{u_1}$.

Consider $E' = E \backslash \{h\}$, then $p' = p - |\mathcal{S}_h|$, where $|\mathcal{S}_h| \leq a\ 2^{u_1} \leq 2^{u_a} + 2^{u_{a-1}} + \cdots + 2^{u_1}$. So $p' = 2^{u_s} + \cdots + 2^{u_{a+1}} + 2^{w_r} + \cdots + 2^{w_1}$ where $r \geq 0$ and $u_s > \cdots > u_{a+1} > w_r > \cdots > w_1 \geq 0$. By the induction hypothesis, $\sum_{j \in E'} j|\mathcal{S}_j| \geq (s - a + r)\ 2^m \geq (s - a)\ 2^m$. So $\sum_{j \in E} j|\mathcal{S}_j| \geq a\ 2^m + (s - a)\ 2^m = s\ 2^m$.

Hence the theorem holds by induction.

THEOREM 2.5 $|\mathcal{S}_1|$ *is a divisor of* v.

Proof. Consider the binary relation $\sim$ on X defined by: $i \sim j$ if and only if there is a matrix $A_k = (a_{xy}^{(k)}) \in \mathcal{S}_1$ such that $a_{ij}^{(k)} = 1$. $\sim$ is an equivalent relation as shown below.

(i) $i \sim i$ since $A_0 = I = (\delta_{ij})$ with $\delta_{ii} = 1$.

(ii) $i \sim j$ implies $j \sim i$ follows from the fact that each A_k is symmetric.

(iii) Suppose $i \sim j$ and $j \sim k$, i.e. there are $A_p, A_q \in \mathcal{S}_1$ with $a_{ij}^{(p)} = a_{jk}^{(q)} = 1$. Note that $A_r = A_p A_q \in \mathcal{S}_1$ and $a_{ik}^{(r)} \geq a_{ij}^{(p)} a_{jk}^{(q)} = 1$. So $a_{ik}^{(r)} = 1$ and then $i \sim k$.

The equivalence relation $\sim$ partitions X into equivalence classes. For each $i \in X$ and $A_k \in \mathcal{S}_1$, there exists one $j \in [i]$ such that $a_{ij}^{(k)} = 1$. The correspondence between A_k and j is one to one. Thus each class $[i]$ is of size $|\mathcal{S}_1|$. Then $v = |\mathcal{S}_1| \cdot$ #(equivalence classes), i.e. $|\mathcal{S}_1|$ is a divisor of v.

3. Constructions of new association schemes from given association schemes.

In coding therory, *extension* of an association scheme is a very common way to get new association schemes (see [9], section 2.5). In this section, we introduce other constructions of new association schemes from given association schemes by means of Kronecker product of two matrices.

Suppose $A = (a_{ij})$ is a $u \times v$ matrix and B a $r \times s$ matrix. The *Kronecker product* $A \otimes B$ of A and B is the following $(ur) \times (vs)$ matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \cdots a_{1v}B \\ a_{21}B & a_{22}B \cdots a_{2v}B \\ \\ a_{u1}B & a_{u2}B \cdots a_{uv}B \end{pmatrix}.$$

The following equalities are frequently used in this paper.

$$a(A \otimes B) = (aA) \otimes B = A \otimes (aB). \tag{3.1}$$

$$(A_1 + A_2) \otimes B = (A_1 \otimes B) + (A_2 \otimes B). \tag{3.2}$$

$$A \otimes (B_1 + B_2) = (A \otimes B_1) + (A \otimes B_2). \tag{3.3}$$

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD). \tag{3.4}$$

$$(A \otimes B)^t = A^t \otimes B^t. \tag{3.5}$$

THEOREM 3.1 *Suppose* $\mathcal{S}=\{A_0,\cdots,A_n\}$ *is a* $(v, n+1)$*-scheme* $\mathcal{S}'=\{A_0',\cdots,A_m'\}$ *is a set of* $m+1$ $v\times v$ $(0,1)$*-matrices such that* (i) *each* A_j' *is the sum of some matrices in* $\mathcal{S}$, (ii) *all* A_j' *sum up to* J, (iii) $A_i A_j'=\sum_{k=0}^{m} a_{ijk}' A_k'$ *for* $0\le i\le n$ *and* $0\le j\le m$, *where* a_{ijk}' *are non-negative integers.* $\mathcal{G}=\{B_0,\cdots,B_p\}$ *is a* $(u, p+1)$*-scheme.* $\mathcal{G}'\subseteq\mathcal{G}$ *satisfies* $B_0\in\mathcal{G}'$ *and* $B_iB_j=\sum_{B_k\in\mathcal{G}'} b_{ijk}' B_k$ *for* $B_i, B_j\in\mathcal{G}'$, *where* b_{ijk}' *are non-negative integers. Construct the set*

$$\begin{aligned}\mathcal{U}=\{A_i\otimes B_j : A_i\in\mathcal{S} \text{ and } B_j\in\mathcal{G}'\}\,\cup\\ \{A_i'\otimes B_j : A_i'\in\mathcal{S}' \text{ and } B_j\in\mathcal{G}\backslash\mathcal{G}'\}.\end{aligned}$$

Then $\mathcal{U}$ *is an association scheme.*

Proof. We shall prove that (A1) to (A4) hold for $\mathcal{U}$.

(A1) Since all matrices in $\mathcal{S}$, $\mathcal{S}'$, $\mathcal{G}$, $\mathcal{G}'$ are symmetric nonzero (0, 1)-matrices, so are all matrices in $\mathcal{U}$.

(A2)
$$\begin{aligned}&\sum\{A_i\otimes B_j : A_i\in\mathcal{S} \text{ and } B_j\in\mathcal{G}'\}\\ &\quad+\sum\{A_i'\otimes B_j : A_i'\in\mathcal{S}' \text{ and } B_j\in\mathcal{G}\backslash\mathcal{G}'\}\\ &=\sum_{A_i\in\mathcal{S}} A_i\otimes\sum_{B_j\in\mathcal{G}'} B_j+\sum_{A_i'\in\mathcal{S}'} A_i'\otimes\sum_{B_j\in\mathcal{G}\backslash\mathcal{G}'} B_j\\ &=J_v\otimes\sum_{B_j\in\mathcal{G}'} B_j+J_v\otimes\sum_{B_j\in\mathcal{G}\backslash\mathcal{G}'} B_j\\ &=J_v\otimes\Big(\sum_{B_j\in\mathcal{G}'} B_j+\sum_{B_j\in\mathcal{G}\backslash\mathcal{G}'} B_j\Big)\\ &=J_v\otimes J_u\\ &=J_{vu}.\end{aligned}$$

(A3) $I_{vu}=I_v\otimes I_u=A_0\otimes B_0\in\mathcal{U}$.

(A4) For $A_i\in\mathcal{S}$, $B_j\in\mathcal{G}'$, $A_r\in\mathcal{S}$, $B_s\in\mathcal{G}'$,

$$\begin{aligned}&(A_i\otimes B_j)(A_r\otimes B_s)\\ &\quad=(A_iA_r)\otimes(B_jB_s)\\ &\quad=\sum_{A_k\in\mathcal{S}} a_{irk}A_k\otimes\sum_{B_h\in\mathcal{G}'} b_{jsh}'B_h\\ &\quad=\sum\{a_{irk}b_{jsh}'A_k\otimes B_h : A_k\in\mathcal{S} \text{ and } B_h\in\mathcal{G}'\}.\end{aligned}$$

For $A_i \in \mathcal{S}$, $B_j \in \mathcal{G}'$, $A'_r \in \mathcal{S}'$, $B_s \in \mathcal{G}\backslash\mathcal{G}'$,

$$\begin{aligned}(A_i \otimes B_j)(A'_r \otimes B_s) &= (A_i A'_r) \otimes (B_j B_s)\\ &= \sum_{A'_k \in \mathcal{S}'} a'_{irk} A'_k \otimes \sum_{B_h \in \mathcal{G}} b_{jsh} B_h\\ &= \sum \{a'_{irk} b_{jsh} A'_k \otimes B_h : A'_k \in \mathcal{S}' \text{ and } B_h \in \mathcal{G} \setminus \mathcal{G}'\}\\ &\qquad + \sum \{a'_{irk} b_{jsh} c_{kt} A_t \otimes B_h : A_t \in \mathcal{S} \text{ and } B_h \in \mathcal{G}'\}\end{aligned}$$

where $A'_k = \sum_{t=0}^{n} c_{kt} A_t$ by assumption (i) of the theorem.

For $A'_i \in \mathcal{S}'$, $B_j \in \mathcal{G}\setminus\mathcal{G}'$, $A'_r \in \mathcal{S}'$, $B_s \in \mathcal{G}\backslash\mathcal{G}'$, we can similarly prove that $(A'_i \otimes B_j)(A'_r \otimes B_s)$ is a non-negative integer combination of matrices in $\mathcal{U}$.

COROLLARY 3.2 *Suppose* $\mathcal{S} = \{A_0, \cdots, A_n\}$ *is a* $(v, n+1)$*-scheme and* $\mathcal{G} = \{B_0, \cdots, B_p\}$ *is a* $(u, p+1)$*-scheme. Then* $\mathcal{S} \otimes \mathcal{G} = \{A_i \otimes B_j : 0 \le i \le n \text{ and } 0 \le j \le p\}$ *is a* $(vu, (n+1)(p+1))$*-scheme.*

Proof. Choose $\mathcal{S}' = \mathcal{S}$ and $\mathcal{G}' = \{B_0\}$. Apply Theorem 3.1.

$\mathcal{S} \otimes \mathcal{G}$ is called the *type I product* of $\mathcal{S}$ and $\mathcal{G}$. Note that Hamming scheme of length 3 is in fact equivalent to $\{I_4, J_4 - I_4\} \otimes \{I_2, J_2 - I_2\}$.

COROLLARY 3.3 *Suppose* $\mathcal{S} = \{A_0, \cdots, A_n\}$ *is a* $(v, n+1)$*-scheme and* $\mathcal{G} = \{B_0, \cdots, B_p\}$ *is a* $(u, p+1)$*-scheme.* $\mathcal{S}' = \{J_v\}$ *and* $\mathcal{G}'$ *is a subgroup of* $\mathcal{G}_1 = \{B_j : \text{row sum of } B_j \text{ is } 1\}$. *Then* $\{A_i \otimes B_j : A_i \in \mathcal{S} \text{ and } B_j \in \mathcal{G}'\} \cup \{J_v \otimes B_j : B_j \in \mathcal{G}\backslash\mathcal{G}'\}$ *is a* $(vn, n|\mathcal{G}'| + p + 1)$*-scheme. (This new scheme is called the type II product of* $\mathcal{S}$ *and* $\mathcal{G}$ *with respect to* $\mathcal{G}'$.)

4. Existence or non-existence of association schemes with certain parameters v and n. The main purpose of this section is to prove the existence or non-existence of schemes with certain parameters v and n. In other word, we want to determine N_v, the set of integers $n+1$ for which there exists a $(v, n+1)$-scheme. It is easy to see that $2 \le \min N_v \le \max N_v \le v$. The only $(v, 2)$-scheme is $\{I, J-I\}$. so $\min N_v = 2$.

A $(v, 3)$-scheme $\{A_0, A_1, A_2\}$ is equivalent to a *strongly regular* graph whose adjacence matrix is A_1 (see [4]). For v a composite integer or a prime of $4s+1$ type, there always exists a $(v, 3)$-scheme. But it is unsolved for the case of v is a prime of $4s+3$ type. We know that there is no $(3, 3)$-scheme or $(7, 3)$-scheme.

If $v=rs$, with $r, s \geq 2$ are integers, then $\{I_v, (J_r - I_r) \otimes I_s, J_r \otimes (J_s - I_s)\}$ is a $(v, 3)$-scheme. In fact this scheme is the type II product of $\{I_r, J_r - I_r\}$ and $\{I_s, J_s - I_s\}$ with respect to $\{I_s\}$. If v is a prime of $4s+1$ type, we can use the fact that Z_v has $2s$ quadratic residue to construct a (v, s)-scheme.

Next question is to determine max N_v in term of v.

THEOREM 4.1 *If $v = 2^r u$, where r is a non-negative integer and u an odd integer, then* $\max N_v = 2^{r-1}(u+1)$.

Proof. Suppose $\mathcal{S}$ is a $(v, n+1)$-scheme. By Theorems 2.1 and 2.5, $|\mathcal{S}_1| = 2^m$ with $m \leq r$. By (2.1) and (2.2),

$$v \geq |\mathcal{S}_1| + 2\sum_{j=2}^{v} |\mathcal{S}_j| = 2^m + 2(n+1-2^m) = 2(n+1) - 2^m.$$

Then

$$n+1 \leq (2^r u + 2^m)/2 \leq (2^r u + 2^r)/2 = 2^{r-1}(u+1).$$

So max $N_v \leq 2^{r-1}(u+1)$.

Conversely, we will construct a $(v, 2^{r-1}(u+1))$-scheme and conclude that max $N_v = 2^{r-1}(u+1)$.

Consider the following $u \times u$ permutation matrices $P_k = (t_{ij}^{(k)})$, $0 \leq k \leq u-1$, defined by $t_{ij}^{(k)} = 1$ if $j = i+k$ and $t_{ij}^{(k)} = 0$ otherwise, where the addition of indices are taken modulo u.

let $A_0 = P_0$ and $A_i = P_i + P_{u-i}$ for $1 \leq i \leq (u-1)/2$. It is straight forward to check that $\mathcal{S} = \{A_0, A_1, \cdots, A_{(u-1)/2}\}$ is a $(u, (u+1)/2)$-scheme by using the fact that $P_k P_h = P_{k+h}$. Consider the $(2, 2)$-scheme $\mathcal{G} = \{I_2, J_2 - I_2\}$. Then $\mathcal{S} \otimes \mathcal{G} \otimes \cdots \otimes \mathcal{G}$ (with r terms of $\mathcal{G}$) is a $(v, 2^{r-1}(u+1))$-scheme.

In the rest of this section, we will concentrate on the case of $v = 2^u$.

THEOREM 4.2 *Suppose $v = 2^u$ and $n+1 = 2^{u_0} + 2^{u_1} + \cdots + 2^{u_r} \geq 2$, where $u_0 > u_1 > \cdots > u_r \geq 0$ are integers. If $u \geq r + u_0$, then there exists a $(v, n+1)$-scheme.*

Proof. We will prove the theorem by induction on u. The case of $u=1$ is clear since $v=n+1=2$. Suppose the theorem holds for all $u'<u\geq 2$. Without loss of generality we can assume that $n+1\geq 3$, since $\{I_v, J_v-I_v\}$ is a $(v, 2)$-scheme.

Suppose $u_r\geq 1$, i.e. $n+1$ is even. Consider $v'=2^{u-1}$ and $n'+1=(n+1)/2$. Note that $n'+1=2^{u_0-1}+2^{u_1-1}+\cdots+2^{u_r-1}\geq 2$. Since $u>r+u_0$ implies $u-1\geq r+(u_0-1)$, by the induction hypothesis, there is a $(v', n'+1)$-scheme $\mathscr{S}$. Consider the $(2, 2)$-scheme $\mathscr{G}=\{I_2, J_2-I_2\}$. By corollary 3.2, $\mathscr{S}\otimes\mathscr{G}$ is a $(v, n+1)$-scheme.

Suppose $u_r=0$, i.e. $n+1$ is odd. for the case of $n+1=3$, a $(v, 3)$-scheme exists as shown in the 3rd paragraph of this section. For the case of $n+1\geq 5$, consider $v'=2^{u-2}$ and $n'+1=n/2$. Note that $n'+1=2^{u_0-1}+2^{u_1-1}+\cdots+2^{u_{r-1}-1}\geq 2$. Since $u>r+u_0$ implies $u-2\geq(r-1)+(u_0-1)$, by the induction hypothesis, there is a $(v', n'+1)$-scheme $\mathscr{S}$. Next consider the $(4, 3)$-scheme. $\mathscr{G}=\{I_4, (J_2-I_2)\times I_2, J_2\otimes(J_2-I_2)\}$. Let $\mathscr{G}'=\{I_4, (J_2-I_2)\otimes I_2\}$. By Corollary 3.3, the type II product of $\mathscr{S}$ and $\mathscr{G}$ with respect to $\mathscr{G}'$ is a $(v, n+1)$-scheme.

Thus the theorem holds by induction.

Although Theorem 4.2 is proved by induction, we can in fact construct the corresponding $(v,n+1)$-scheme in the proof. For convenience, we use the following notation.

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad J=\begin{pmatrix}1&1\\1&1\end{pmatrix},\quad K=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$
$$\langle M_1,\cdots,M_u\rangle=M_1\otimes\cdots\otimes M_u.$$

Suppose $v=2^u$ and $n+1=2^{u_0}+2^{u_1}+\cdots+2^{u_r}\geq 2$, where $u_0>u_1>\cdots>u_r=0$ are integers and $u\geq r+u_0$. (If $u_r>0$, we can consider $v'=2^{u-u_r}$ and $n'+1=(n+1)/2^{u_r}$. Then use type I product of schemes.) Let $u_i=0$ for $i>r$. Define

$$\begin{aligned}\mathscr{S}^{(0)}=\{\langle M_1,\cdots,M_u\rangle:&\\ &M_j=I \text{ or } K \text{ for } 1\leq j\leq u_0,\ M_j=I \text{ for } j\geq u_0+1\},\\ \mathscr{S}^{(i)}=\{\langle M_1,\cdots,M_u\rangle:&\ M_j=J \text{ for } 1\leq j\leq u_0+i-u_i-1,\\ &M_j=I \text{ or } K \text{ for } u_0+i-u_i\leq j\leq u_0+i-1,\\ &M_{u_0+1}=K,\ M_j=I \text{ for } j\geq u_0+i+1\},\\ &\text{for } i=1,2,\cdots,u-u_0.\end{aligned}$$

Then $\mathcal{S} = (\bigcup_{0\leq i\leq r-1}\mathcal{S}^{(i)}) \cup \{A_n\}$ is the scheme given in the proof of Theorem 4.2, where $A_n = \sum\{M : \mathcal{S}^{(i)} = \{M\}, r \leq i \leq u - u_0\}$.

For example, $v = 2^5$ and $n + 1 = 2^4 + 2^2 + 2^1 + 2^0$. Then $\mathcal{S}$ contains the following $n + 1$ matrices.

$$\begin{array}{ll} \langle K^{c_1}, K^{c_2}, K^{c_3}, K^{c_4}, I, I, I, I\rangle, & c_1, c_2, c_3, c_4 = 1 \text{ or } 2, \\ \langle J, J, K^{c_5}, K^{c_6}, K, I, I, I\rangle, & c_5, c_6 = 1 \text{ or } 2, \\ \langle J, J, J, J, K^{c_7}, K, I, I\rangle, & c_7 = 1 \text{ or } 2, \\ \langle J, J, J, J, J, J, K, I\rangle + \langle J, J, J, J, J, J, J, K\rangle, & \end{array}$$

where $K^1 = K$ and $K^2 = I$.

COROLLARY 4.3 *Suppose* $v = 2^u$ *and* $2 \leq n + 1 \leq 2^{1+[u/2]}$, *then there exists a* $(v, n + 1)$*-scheme.*

THEOREM 4.4 *Suppose* $\mathcal{S}$ *is a* $(v, n + 1)$*-scheme with* $2^{u-1} < n + 1 < v = 2^u$, *then* $n + 1 = 2^{u-1} + 2^w$ *for some* $0 \leq w \leq u - 2$.

Proof. Suppose the theorem is not true, then $n+1=2^{u-1}+2^w+z$, where $0 \leq w \leq u - 2$ and $1 \leq z \leq 2^w - 1$. By (2.1) and (2.2),

$$\begin{aligned} v &\geq |\mathcal{S}_1| + 2\sum_{j=2}^{v} |\mathcal{S}_j| \\ &= |\mathcal{S}_1| + 2(n + 1 - |\mathcal{S}_1|) = 2(n + 1) - |\mathcal{S}_1|. \end{aligned}$$

Then

$$|\mathcal{S}_1| \geq 2(n + 1) - v = 2^{w+1} + 2z > 2^{w+1}.$$

By Theorem 2.1, $|\mathcal{S}_1| = 2^m$ for some non-negative integer m. $2^u = v > n + 1 \geq 2^m > 2^{w+1}$ implies $u - 1 \geq m \geq w + 2$. Again, by (2.1) and (2.2),

$$\begin{aligned} 2^u = v &\geq |\mathcal{S}_1| + 2|\mathcal{S}_2| + 3\sum_{j=3}^{v} |\mathcal{S}_j| \\ &= |\mathcal{S}_1| + 2|\mathcal{S}_2| + 3(n + 1 - |\mathcal{S}_1| - |\mathcal{S}_2|) \\ &= 3\cdot 2^{u-1} + 3\cdot 2^w + 3z - 2^{m+1} - |\mathcal{S}_2|. \end{aligned}$$

Then

$$|\mathcal{S}_2| \geq 2^{u-1} - 2^{m+1} + 3\cdot 2^w + 3z.$$

By Theorem 2.3(v), $|\mathcal{S}_2|$ is a multiple of 2^{m-1}. Therefore, $|\mathcal{S}_2| = 2^{u-1} - 2^{m+1} + t\,2^{m-1}$, where $t \geq 1$ is an integer. So

$$\sum_{j=3}^{v} |\mathscr{S}_j| = n + 1 - |\mathscr{S}_1| - |\mathscr{S}_2| \tag{4.1}$$
$$= 2^w + z + (2-t)\, 2^{m-1} \geq 0$$

and

$$\sum_{j=3}^{v} j|\mathscr{S}_j| = v - |\mathscr{S}_1| - 2|\mathscr{S}_2| = (3-t)2^m. \tag{4.2}$$

(4.1) and the fact that $m \geq w+2$ imply $2-t \geq 0$, i.e. $2-t=0$ or 1. Then

$$\sum_{j=3}^{v} |\mathscr{S}_j| = (2-t)\, 2^{m-1} + 2^w + 2^{u_s} + \cdots + 2^{u_1},$$

where $m-1 > w > u_s > \cdots > u_1 \geq 0$ and $s \geq 1$. (Note that $(2-t)\ 2^{m-1}$ is either 2^{m-1} or nothing.) By Theorem 2.4,

$$\sum_{j=3}^{v} j|\mathscr{S}_j| \geq (2-t+1+s)2^m \geq (4-t)2^m.$$

This contradicts (4.2). Thus the theorem holds.

By Corollary 4.3 and Theorem 4.4, we have

$$N_2 = \{2\},$$
$$N_4 = \{2, 3, 4\},$$
$$N_8 = \{2, 3, 4, 5, 6, 8\},$$
$$N_{16} = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 16\}.$$

However, for $v=32$, the only $n+1$ for which we can not use Theorems 4.2 and 4.4 to determine if $n+1 \in N_v$ is $n+1=15$. But there exists (4, 3)-scheme and (8, 5)-scheme. Their type I product is a (32, 15)-scheme. So we have

$$N_{32} = \{2, 3, \cdots, 16, 17, 18, 24, 32\}.$$

Similary, for $v = 2^6$, we have difficulty when $n+1 = 23, 27, 29, 30, 31$. Since there exist (4, 3)-scheme, (16, 9)-scheme, (8, 5)-scheme, (8.6)-scheme, by using type I product, there exist (32, 27)-scheme and (32, 30)-scheme. Also the following is a (32, 23)-scheme:

$$\begin{array}{ll} \mathscr{S} = \{\langle K^{c_1}, K^{c_2}, K^{c_3}, K^{c_4}, I, I\rangle, & c_1, c_2, c_3, c_4 = 1 \text{ or } 2, \\ \quad\langle J, J, K^{c_5}, K^{c_6}, K, I\rangle, & c_5\ c_6 = 1 \text{ or } 2, \\ \quad\langle K^{c_7}, J, J, J, I, K\rangle, & c_7 = 1 \text{ or } 2, \\ \quad\langle J, J, J, J, K, K\rangle\}. & \end{array}$$

so only the cases of $n+1=29, 31$ are unknown.

$$N_{64}=\{2\cdots 28, (29?), 30, (31?)\ 32, 33, 34, 36, 40, 48, 64\}.$$

In general, we still can not determine N_v. In order to get more results on N_v, we believe that we should understand more structures on $\mathscr{S}_j$ for an association scheme $\mathscr{S}$.

Acknowledgment. The author wishs to express his gratitude to Hua-Min Huang for his introducing the topic of association schemes.

References

1. N. L. Biggs, *Perfect codes and distance-transtive graphs*, Combinatorics (Proc. British Combinatorial Conf., Univ. Coll. Wales, Aberystwyth.) 1-8, (1973).
2. ———, *Algebraic Graph Theory*, Cambridge Univ. Press, London (1974).
3. N. L. Biggs, R. M. Damerell and D. A. Sands, *Recursive families of graphs*, J. Combinatorial Theory Ser. *B*, 12 (1972), 123-131.
4. R. C. Bose, *On some connections between the design of experiments and information theory*, Bull. Intern. Stat. Inst., 38 (1963), 257-271.
5. R. C. Bose and D. M. Mesner, *On linear association algebras corresponding to association schemes of partially balanced designs*, Ann. Math. Stat., 30 (1959), 21-38.
6. R. C. Bose and T. Shimamota, *Classification and analysis of partially balanced incomplete block designs with two associate classes.*, J. Amer. Stat. Assoc., 47 (1952) 151-184.
7. P. J. Cameron, *Suborbits in transitve permutation groups*, in: M. Hall, Jr. and J. H. van Lint, eds., *Combinatorics*, (Reidel, Dordrecht), 419-450, (1975).
8. R. M. Damerell, *On Moore graphs*, Proc. Cambridge Philis Soc., 74 (1973), 227-236.
9. P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements, No. 10 (1973).
10. M. D. Hestenes, *On the use of graphs in group theory, in:* F. Harary, ed., New Directions in the Theory of Graphs, (Academic Press, New York), 97-128, (1973).
11. D. G. Higman, *Combinatorial Considerations about Permutation Groups*, Lecture Note, Math. Inst., Oxford (1972).
12. A. T. James, *The relationship of an experimental design*, Ann, Math. Stat., 28 (1957), 993-1002.
13. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Part I and II, North-Holland, Amsterdam (1977).
14. M. Ogasawara, *A necessary condition for the existence of regular and symmetrical PBIB designs of T_m type*, Inst. of Stat. Mimeo. Ser. No. 418 (Univ. of North Carolina, Chapel Hill, NC) (1965).
15. J. Ogawa, *The theory of the association algebra and relationship algebra of a partially balanced imcomplete block design*, Inst. Stat. Mimeo. Ser. No. 224 (Univ. of North Carolina, Chapel Hill, NC) (1959).
16. D. Raghavarao, *Constructions and Combinatorial Problems in Design of Experiments*, Wiley, New York (1971).
17. J. J. Rotman, *The Theory of Graphs: An Introduction*, Allyn and Bacon, Boston, Mass. (1965).
18. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York (1964).

19. S. Yamamots, Y. Fujii and N. Hamada, *Composition of some series of association algebras*, J. Sci. Hiroshima Univ., Ser A-I, **29** (1965), 181–125.

20. E. Bannai, P. J. Cameron and J. Kahn, *Nonexistence of certain distance-transitive digraphs*, J. Comb. Theory Series B, **31** (1981), 105–110.

21. E. Yoshimi, *Characterization of $H(n, q)$ by parameters*, J. Comb. Theory, Series A, **31** (1981), 108–125

Department of Mathematics
National Central University
Chung-Li, Taiwan 32054
Republic of China