J. Austral. Math. Soc. **22** (Series A) (1976), 469–475.

HADAMARD MATRICES AND SUBMATRICES

K. VIJAYAN

(Received 11 August 1975; revised 1 December 1975)

Abstract

Shrinkande and Bhagwan Das (1970) showed how to extend a $(4t-1,4t)$ row-orthogonal matrix with entries ± 1 to a Hadamard matrix of order $4t$. Using a slightly different approach we consider extensions of $(4t-k,4t)$ row-orthogonal matrix to a Hadamard matrix of order $4t$.

Introduction

An (m, n)-matrix $H_{m,n}$ with entries ± 1 is called a Hadamard submatrix if the rows of $H_{m,n}$ are orthogonal to one-another. If $m \geqq 3$, one can easily note that n is divisible by 4.

If $m = n$, we call the matrix a Hadamard matrix of order n.

In this note we investigate when and how one can extend a matrix $H_{m,n}$ to a matrix $H_{n,n}$ by adding $n-m$ rows to $H_{m,n}$. The particular case when $m = n-1$ is done by Shrikhande and Bhagwan Das (1970) using a different method.

Hereafter, weight of a vector means the sum of squares of the components of that vector.

2. General approach

From the general theory of linear algebra, there exists a row orthogonal matrix A of order $(n-m, n)$ such that the rows of A are orthogonal to the rows of $H_{m,n}$ and such that

$$AA' = n \cdot I_{n-m}$$

where I_{n-m} is the identity matrix of order $n-m$. If all the entries of A are ± 1, then if we augment the rows of A to $H_{m,n}$ we get an $H_{n,n}$. Hence, essentially what we have to look for is an A with these properties.

From the discussion, we have,

$$(1) \qquad \begin{pmatrix} H_{m,n} \\ \cdots \\ A \end{pmatrix} (H'_{m,n} \vdots A') = nI_n .$$

https://doi.org/10.1017/S1446788700016335 Published online by Cambridge University Press

From (1), it is immediate that

(2) $$(H'_{m,n} : A')\begin{pmatrix} H_{m,n} \\ \cdots \\ A \end{pmatrix} = nI_n.$$

From (2), we get

(3) $$A'A = nI_n - R,$$

where

$$R = (r_{ij}) = H'_{m,n}H_{m,n}$$

and

$$r_{ij} = m, \qquad i = 1, 2, \cdots, n.$$

If we denote the columns of A as $A_1, A_2, \cdots, A_n$, (3) means that the weight of A_i is $n - m$ and

(4) $$A'_iA_j = -r_{ij} \quad \text{if} \quad i \neq j, \qquad i, j = 1, 2, \cdots, n.$$

By retracing the steps, one notices that to extend $H_{m,n}$ to $H_{n,n}$ one need have to only construct n m-vectors $A_1, A_2, \cdots, A_n$ with entries ± 1 satisfying condition (4).

Since an A satisfying (1) always exists, from Schwartz inequality we have,

(5) $$|r_{ij}| \leqq n - m, \qquad i, j = 1 \cdots n$$

where

(6) $$r_{ij} = n - m \quad \text{iff} \quad A_i = -A_j$$

and $$-r_{ij} = n - m \quad \text{iff} \quad A_i = A_j \quad .$$

Hereafter we would say that two columns A_i and A_j are distinct if and only if $A_i \neq A_j$ and $A_i + A_j \neq 0$.

Obviously A_i and A_j are distinct if and only if

(7) $$|r_{ij}| < n - m,$$

and mainly we will be looking for distinct A_i's.

One can also notice that $n - m - r_{ij}$ is divisible by 2. This follows by observing that if ith and jth columns of H_{n-m} have a common entry, then

$$r_{ij} = a - (m - a) = 2a - m$$

which implies $r_{ij} + m$ is divisible by 2, and from a previous remark that n is a multiple of 4. So the possible values of r_{ij} are

(8) $$(n - m) - 2k, \qquad k = 0, 1, \cdots, (n - m).$$

https://doi.org/10.1017/S1446788700016335 Published online by Cambridge University Press

When $n-m=1$, from (6) and (8), we note that $H_{m,n}$ is uniquely extendable to $H_{n,n}$. In later sections, we use (6), (7) and (8) to extend $H_{m,n}$ to $H_{n,n}$.

3. Extension of $H_{n-2,n}$ to $H_{n,n}$

From (7) and (8) we note that any two distinct vectors A_i and A_j are orthogonal to one another. If a_{ik} is the kth component of A_i, this means that,

$$a_{i1}a_{j1}+a_{i2}a_{j2}=0. \tag{9}$$

At least one of a_{j1} and a_{j2} should be different from 0. Without loss of generality we may take a_{j1} to be different from 0. Then from (9), we have

$$a_{i1}=-a_{i2}\cdot\frac{a_{j2}}{a_{j1}}. \tag{10}$$

Remembering that the weights of A_i and A_j are 2, we get

$$2=a_{i1}^2+a_{i2}^2=a_{i2}^2\left(1+\frac{a_{j2}^2}{a_{j1}^2}\right)=\frac{a_{i2}^2}{a_{j1}^2}\cdot 2$$

and hence

$$a_{i2}=\pm a_{j1}. \tag{11}$$

Substituting in (10),

$$-a_{i1}=\pm a_{j2}. \tag{12}$$

Thus if we choose A_1, the remaining columns of A are determined from (6), (11) and (12). To preserve Hadamard property, we choose A_1 as $\binom{1}{1}$. For the first i such that $r_{1i}=0$, we might choose without any loss of generality

$$A_i=\begin{pmatrix}1\\-1\end{pmatrix},$$

as the other solution is obtained by interchanging the two rows of A. Thus we have:

THEOREM 1. *An $H_{n-2,n}$ can be extended to an $H_{n,n}$ essentially uniquely.*

4. Extension of $H_{n-3,n}$ to $H_{n,n}$

From (7) and (8) we find that any two distinct pair of columns A_i and A_j is such that

$$A_i'A_j=\pm 1. \tag{13}$$

https://doi.org/10.1017/S1446788700016335 Published online by Cambridge University Press

Consider all A_j's that are distinct from A_1. Without any loss of generality we can assume that if A_j is distinct from A_1, then

$$r_{1j} = 1\,.$$

If A_j and $A_{j'}$, are any two columns of A, that are distinct from A_1, one notices that

$$r_{jj'} = 1 \pmod 4 \qquad (14)$$
$$= 1 \quad \text{or} \quad -3.$$

Hence if A_j and $A_{j'}$ are distinct, then

$$r_{jj'} = 1\,.$$

Hence to determine the distinct columns of A, one is only to look for 3-vectors of weight 3, such that the inner product between any two vectors is -1. Now we show that there can be at most 4 distinct columns for A. If there are more than 4, let B_1, B_2, B_3, B_4 be any 4 of them. Then we note that

$$\left(\sum_{i=1}^{4} B_i\right)' B_j = 0 \quad j = 1,2,3,4. \qquad (15)$$

Since any three of the B's are easily seen to be independent, (15) implies that

$$\sum_{i=1}^{4} B_i = 0$$

i.e. any three of B's uniquely determine the fourth and hence there cannot be a fifth one.

For our purpose entries in B_i's should be ± 1. As usual, we choose B_1 with all entries $+1$. Then the other three B_i's are uniquely determined (except for permutation of suffixes) as

$$B_2 = \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \quad B_3 = \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}, \quad B_4 = \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}.$$

Now the construction of A is obvious. One can also see that A-matrix obtained by permutating the suffixes 2, 3, 4 of B-vectors, can also be obtained by permutating the rows of A. This is proved by noting that if there are r_i columns in A not distinct from B_i $(i = 1,2,3,4)$, then the orthogonality between rows of A implies that,

$$r_1 - r_2 - r_3 + r_4 = 0$$
$$r_1 - r_2 + r_3 - r_4 = 0 \qquad (16)$$

https://doi.org/10.1017/S1446788700016335 Published online by Cambridge University Press

and

$$r_1 + r_2 - r_3 - r_4 = 0\,,$$

and (16) implies that

$$r_1 = r_2 = r_3 = r_4\,.$$

Thus the A-matrix obtained is essentially unique. Hence we can state the theorem,

THEOREM 2. *An H_{n-3} can be extended to an $H_{n,n}$ essentially uniquely.*

5. Extension of $H_{n-4,n}$ to $H_{n,n}$

From (7) and (8), if any pair of columns of A are distinct then they are either mutually orthogonal or their inner product is ± 2.

REMARK 1. *If all distinct columns of A are orthogonal to one another then we could replace them by any set of orthogonal 4-vectors of weight 4 and hence in particular columns of an H_4 and the extension is trivially true.*

In view of the Remark 1, we hereafter only consider the case when there is a pair of non-orthogonal distinct columns.

REMARK 2. *If the two distinct columns A_i and A_j are not orthogonal to one another, then any columns A_k distinct from these two would be orthogonal to one of A_i and A_j, but not to both. This follows from the equation*

$$n - 4 + r_{ij} + r_{ik} + r_{jk} = 0\,(\mathrm{mod}\,4)\,.$$

It follows from Remark 2 that we could divide the columns of A into two sets, such that any pair of distinct columns from the same set are mutually orthogonal, while from different sets will have an inner product ± 2.

Let there be b distinct columns $B_1, \cdots, B_b$ in the first set and c distinct columns $C_1, \cdots, C_c$ in the second set. Without any loss of generality we assume that $b \geqq c$ and

$$B_i'C_1 = 2 \qquad i = 1, \cdots, b$$

and

$$B_1'C_j = 2 \qquad j = 1, \cdots, c\,.$$

To prove the extension we only have to show that B's and C's can be replaced by 4-vectors having components ± 1 without affecting the inner product properties.

Let $D = (d_{ij})$ be a $c \times b$ matrix with

$$d_{ij} = C_i'B_j\,.$$

https://doi.org/10.1017/S1446788700016335 Published online by Cambridge University Press

We first prove the following lemma.

LEMMA. *There exists a Hadamard matrix H_4 such that the first principal $c \times b$ submatrix of H_4 is $\frac{1}{2}D$.*

PROOF. If $b = 4$, D is a Hadamard submatrix and from previous sections we note that we can extend $\frac{1}{2}D$ to an H_4.

If $b = 3$, any 4-vector say B_4 having weight 4 and orthogonal to B_1, B_2 and B_3 should have inner product ± 2 with C's. This follows from the fact that C's should be in the space generated by B_1, B_2, B_3 and B_4 and hence could be written as

$$C_i = \sum_{j=1}^{4} l_{ij} B_j$$

where

$$l_{ij} = \frac{B_j' C_i}{B_j' B_j} = \frac{1}{4} B_j' C_i$$

and

$$\sum_j l_{ij}^2 = 1 .$$

Hence by adding a column to D of inner products of C's with B_4, we are in the same case as $b = 4$.

If $b = 2$, then c would have to be 2 and hence either the two rows of D are same as (11) or orthogonal to one another (remember that we have chosen B's such that $d_{11} = d_{21} = 1$).

If D is orthogonal then the matrix

$$\frac{1}{2}\begin{pmatrix} D & D \\ D & -D \end{pmatrix}$$

is an H_4.

If D has both rows the same, then we have

$$\begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{matrix}$$

as an H_4 with the required property. Hence the lemma.

Now we can show how to choose B's and C's having components ± 1 with the required inner product.

https://doi.org/10.1017/S1446788700016335 Published online by Cambridge University Press

For an H_4 defined as above, derive a matrix B by changing the sign of the last column. i.e. if u is the last column of H_4, then

$$B = H_2 - 2A$$

where A is a 4×4 matrix with last column same as u and the rest of the elements 0.

Note that the entries of B are ± 1 and is actually a Hadamard matrix.

Define $C = \frac{1}{2}B \cdot H_4'$. The entries of C also are ± 1 as

$$C = \tfrac{1}{2}B \cdot H_4' = \tfrac{1}{2}(H_4 - 2A)H_4' = \tfrac{1}{2}(H_4H_4' - 2AH_4') = \tfrac{1}{2}(4I - 2uu').$$

Hence if we take the first b columns of B as $B_1, \cdots, B_b$ and the first c columns of C as $C_1, \cdots, C_c$ we have the required result as we note that

$$B'C = \tfrac{1}{2}B'BH_4' = 2H_4'$$

which has D' as its principal $b \times c$ matrix.

Hence we have the theorem,

THEOREM 3. *We can extend an $H_{n-4,\,n}$ to an $H_{n,\,n}$.*

One can easily note that if $b = 4$, the extension is not essentially unique.

6. Concluding remarks

We have proved so far that we can always extend an $H_{n-k,\,n}$ to $H_{n,\,n}$ when $k \leqq 4$. The author feels that the result is true if $k \leqq n/2$, but this approach would obviously be very tedious to be of use to establish the result.

Reference

S. S. Shrikhande and Bhagwan Das (1970). *A note on embedding for Hadamard matrices,* (Essays in Probability and Statistics, University of North Carolina Press, Chapel Hill).

Department of Mathematics,
University of Western Australia,
Nedlands, W.A. 6009.

https://doi.org/10.1017/S1446788700016335 Published online by Cambridge University Press