AN INNER ORTHOGONALITY OF HADAMARD MATRICES

K. A. BUSH

(Received 11 August 1968)

Communicated by G. B. Preston

1. Introduction

We say a matrix H of order $4t$ is Hadamard if each entry is 1 or -1, and the inner product of any two rows is zero. We shall consider only Hadamard matrices in normal form with the first row consisting solely of 1 while any two of the remaining rows have the property that $h_{ik} = h_{jk} \doteq 1$, $h_{ik} = -h_{jk} = 1$, $-h_{ik} = h_{jk} = 1$, and $-h_{ik} = -h_{jk} = 1$ each occur t times. We can induce a further normalization by choosing the second row of H to have the first $2t$ entries 1 and the last $2t$ entries -1, and this will be the standard form we consider. We now call $\tilde{H}$ the submatrix obtained by deleting the first two rows of H and the first $2t$ columns. $\tilde{H}$ therefore is of dimension $4t-2 \times 2t$. We prove the following theorem:

THEOREM. *$\tilde{H}\tilde{H}^T-(2t)I$ is orthogonal.*

It is interesting to note that this theorem has relevance for the problem of the existence of finite projective planes, and, although our methods lead to this theorem and thus prove to be inconclusive, it is possible that modification of our procedures would settle some of the questions concerning the existence of finite projective planes or lead to new theorems about Hadamard matrices. We therefore include the necessary background about finite projective planes in the next section.

2. Finite projective planes

By a finite projective plane of order $2t$ we mean a collection of $4t^2+2t+1$ objects called points divided into subclasses called lines such that each subclass contains $2t+1$ points, and any two subclasses have precisely one point in common. Thus two lines define a point, and the dual, two points determine a line, also holds. An extensive literature has grown up on this subject since the topic was first explored in (8).

The leading theorems about finite projective planes concern the question of existence of such planes. We have the classic result established in (1): if the order is a prime or a power of a prime, the geometry exists. We also have the now celebrated Bruck-Ryser theorem (5) stating that if the order $s \equiv 1$ or 2 (4) and if the

https://doi.org/10.1017/S1446788700009502 Published online by Cambridge University Press

decomposition of s contains a prime of the form $4k+3$ to an odd power, then the finite projective plane fails to exist. Despite strenuous efforts and much computer time, no further progress has been made with this fundamental question. As a result, two schools have arisen, one faction believing that finite projective planes exist in all cases not excluded by the Bruck-Ryser conditions while others conjecture that such planes exist only if s is a power of a prime or a prime. The former position was somewhat strengthened by the remarkable discovery of Bose, Shrikhande, and Parker that the Euler conjecture was false since they showed the existence of two orthogonal Latin squares of side $4k+2$ for $k > 1$ (3, 4) which we now proceed to define.

Let a set of s integers $0, 1, \cdots, s-1$ be arranged in an $s \times s$ square in such a way that every integer occurs s times. If each integer occurs once and only once in every row and column, the square is said to be a Latin square of side s. Two squares are said to be orthogonal to one another if, when one square is superimposed upon the other square, every number of the first occurs once and only once with every number of the second square. To the set of at most $s-1$ Latin squares which are mutually orthogonal, we may adjoin two other squares which are not Latin squares but which are orthogonal to each other and to every other Latin square in the orthogonal set. The first of these squares is constructed by taking each element of the first row as 0, each element of the second row as 1, and so on. The second square is the transpose of the first square. Conversely it may be noted that any square orthogonal to these two squares must be a Latin square. Thus a total of $s+1$ orthogonal squares is possible at best, and it is known that this bound is attainable when s is a prime or a power of a prime [1]. When this bound is attained, we say that we have a complete set of orthogonal squares. As an example of a complete set, we might choose $s = 3$ and write

$$\begin{array}{ccc} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

If we write in order the elements of each square in a line, we can display these squares in the following form:

$$\begin{array}{ccccccccc r} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & \text{[first square]} \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & \text{[second square]} \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 & \text{[third square]} \\ 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 & \text{[fourth square]} \end{array}$$

In this form we see that any two rows have the property that each one of the nine possible ordered pairs occurs exactly once when one row is superimposed on another row.

We call such an array an orthogonal array of index 1, strength 2, and level s. A classic result is that the maximum number of rows we can accommodate is $s+1$. We call the maximum number of rows we can construct the number of constraints.

https://doi.org/10.1017/S1446788700009502 Published online by Cambridge University Press

3. On the expansion of orthogonal arrays to a square matrix

We consider orthogonal arrays with $s = 2t$ of strength 2 and index 1. Then we assume that there are $2t+1$ constraints equivalent to the assumption that a finite projective plane of this order exists. We assume the array is written in standard form with the first two rows:

$$\begin{array}{llllll} 0 & 0\cdots 0 & 1 & 1\cdots 1\cdots & s-1 & s-1\cdots s-1 \\ 0 & 1\cdots s-1 & 0 & 1\cdots s-1\cdots & 0 & 1\ \cdots s-1 \end{array}$$

Let us suppose that the orthogonal array is repeated so that we now have $8t^2$ columns and $2t+1$ rows. We propose expanding this array to a square matrix of order $8t^2$ by replacing each element in the array by a vector. In fact, we set up a one-to-one correspondence between the elements of our array and vectors which are columns of a Hadamard matrix of order $4t$. Specifically, we assume this matrix exists, and we agree to choose the first row to consist only of positive entries. The second row is to contain $2t$ plus entries followed by $2t$ negative entries. We now delete these two rows from the Hadamard matrix and consider only the remaining $4t-2$ rows. We now replace 0 in the first half of the orthogonal array by the first column of our reduced Hadamard matrix where each element is multiplied by $\frac{1}{2}$. We replace 0 in the second half of our orthogonal array by the $2t+1$ column of our Hadamard matrix. Similarly we replace 1 in the first half of the array by the second column with each element multiplied by $\frac{1}{2}$ and 1 in the second half by the $2t+2$ column etc. To illustrate the process we have described, we append the details for the case $t = 1$. The array when duplicated becomes:

$$\begin{array}{cccccccc} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0. \end{array}$$

The Hadamard matrix is

$$\begin{array}{cccc} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & +. \end{array}$$

The replacements are:

$$\begin{array}{ll} \text{first half} & \text{second half} \\ 0\to\begin{matrix} 1/2 \\ 1/2 \end{matrix} & 0\to\pm \\ 1\to\begin{matrix} -1/2 \\ -1/2 \end{matrix} & 1\to\pm, \end{array}$$

and we secure:

$$\begin{array}{rrrrcrrrr}
1/2 & 1/2 & -1/2 & -1/2 & & + & + & - & - \\
1/2 & 1/2 & -1/2 & -1/2 & & - & - & + & + \\[6pt]
1/2 & -1/2 & 1/2 & -1/2 & & + & - & + & - \\
1/2 & -1/2 & 1/2 & -1/2 & & - & + & - & + \\[6pt]
1/2 & -1/2 & -1/2 & 1/2 & & + & - & - & + \\
1/2 & -1/2 & -1/2 & 1/2 & & - & + & + & -
\end{array}$$

In this way the original array now becomes a matrix with $(2t+1)(4t-2) = 8t^2-2$ rows. We now adjoin a row consisting of $\frac{1}{2}$ repeated $4t^2$ times followed by plus repeated $4t^2$ times. We adjoin a second row consisting of $\frac{1}{2}$ repeated $4t^2$ times and minus repeated $4t^2$ times to secure a square matrix. We call this matrix A. We claim that this matrix is orthogonal in the sense that the inner product of any two columns is zero.

Suppose we consider any two columns from the second half. From our construction we note that the portion of the inner product arising from two different symbols in the original array is the inner product of two columns of an Hadamard matrix with the first two rows deleted. The inner product contribution is therefore -2. If however the original symbols agree, the contribution is $4t-2$. We now note in the original array that any two columns have precisely one row in which the symbols agree, for if there were two such rows, then there would be a repeated pair. It is easily seen that any two columns have precisely one row in which the symbols agree. Recapitulating, the inner product is then:

$$\begin{array}{rl}
4t-2 & \text{(from repeated symbol)} \\
-2\ (2t) & \text{(from the remaining } 2t \text{ pairs)} \\
2 & \text{(from the adjoined rows).}
\end{array}$$

A precisely similar proof holds for the orthogonality of any two columns from the first half.

If we select one column from the first half and one from the second half, then there is no contribution to the inner product from the two adjoined rows. Since here we deleted the combination $\frac{1}{2}, \frac{1}{2}$ from the first two rows in the first half and the combination $+-$ from the first two rows in the second half, it is clear that the inner product attributable to any two symbols in the vector replacement process is zero. We thus have the result:

THEOREM. *The matrix A^TA is diagonal with the first $4t^2$ entries $2t^2$ and the last $4t^2$ entries $8t^2$.*

It follows that the eigenvalues of A^TA are $2t^2$ and $8t^2$ each of multiplicity $4t^2$. The matrix AA^T will have the same eigenvalues. We show that the inner product of any two rows of A arising from different rows in the original array is zero.

We note that each pair in the original array occurs once between any two rows. Thus 0 (say) is paired against $0, 1, \cdots, 2t-1$. In both the first half and the second half, the vector replacements have the property that the sum of the elements in any row is zero. Hence the contribution to the inner product arising from any fixed element (say) 0 in one of the rows is zero. Evidently the first two rows that we adjoined are orthogonal to all the remaining rows although not to each other. Nor are two rows that arise in the replacement process from a single row orthogonal. The matrix AA^T then consists of a direct sum of matrices $\oplus U$; $V, V, \cdots, V$ where U is 2×2 and each V is $(4t-2)\times(4t-2)$. Each of these matrices has $5t^2$ as a diagonal element, and U has $-3t^2$ as the off-diagonal element. The off-diagonal elements of V are not known unless we also describe the structure of the Hadamard matrix which generated them. We do know V is symmetric. Inspecting the U matrix, we easily verify that its eigenvalues are $8t^2$ and $2t^2$. Consequently each V has the same eigenvalues each repeated the same number of times.

We now set

$$C = (M+m)/(M-m)[I-2V/(M+m)].$$

Such a transformation has the effect of relocating all eigenvalues between -1 and 1 where M and m are the greatest and least eigenvalues of V. Since this theorem is not well-known, we append a short proof.

THEOREM. *If α and β are scalars and $E = \alpha I+\beta F$, then the eigenvalues of E are given by $\beta\lambda+\alpha$ where λ is an eigenvalue of F.*

PROOF. $|E-\mu I| = 0 \rightarrow |\alpha I+\beta F-\mu I| = 0 \rightarrow |F-[(\mu-\alpha)/\beta]I| = 0$. Setting $\lambda = (\mu-\alpha)/\beta$, we see that $\mu = \beta\lambda+\alpha$.

Identifying α and β in the transformation above yields our assertion. In the case at hand $M = 8t^2$ and $m = 2t^2$. Under this transformation we secure:

$$C = \tfrac{5}{3}I - V/3t^2.$$

Consequently the main diagonal of C consists solely of 0. Clearly C is symmetric, and its eigenvalues are ± 1. The eigenvalues of C^2 are therefore all 1 and C is symmetric. Hence there is an orthogonal matrix 0 such that $0C^2 0^T = I$ or $C^2 = 0^T I 0 = I$. Therefore C is orthogonal. The methods used here are similar to those introduced by the author in (7).

We now discuss the off-diagonal elements of C which arose from the original Hadamard matrix. Recalling how C was formed, we select the $4t$ distinct vectors in the H matrix with the proper weights: $\frac{1}{2}$ if the first half and 1 otherwise. We study the second half first. Here we can have the combinations listed below with the last line indicating the number of occurrences of each:

$$\begin{array}{cccc} + & + & - & - \\ + & - & + & - \\ a & t-a & t-a & a. \end{array}$$

https://doi.org/10.1017/S1446788700009502 Published online by Cambridge University Press

The contribution to the inner product is $4a-2t$ where $0 \leqq a \leqq t$. From the first half the same combinations weighted with $\frac{1}{2}$ occur with respective frequencies of $t-a$, a, a, $t-a$ so that the contribution to the inner product is $(2t-4a)/4$. In any case the total contribution is $\frac{3}{4}$ that of the portion arising from the second half. To within scaling factors

$$c_{ij} = \sum_{2t+1}^{4t} h_{ik} h_{jk}.$$

4. Proof of the Theorem

For orthogonality, we must have

$$\sum_{u \neq v} c_{uj} c_{vj} = 0.$$

We must therefore have

$$\sum_{\substack{j \neq u \\ j \neq v}} \sum_r h_{ur} h_{jr} \sum_s h_{vs} h_{js} = 0, \qquad u \neq v.$$

If we sum on j first, we must distinguish between the cases $r = s$ and $r \neq s$. We must also recall that the inner product of two columns is -2. We secure:

$$\sum_{r \neq s} (-2-h_{ur} h_{us} - h_{vr} h_{vs}) h_{ur} h_{vs} + \sum (4t-2-h_{ur}^2 - h_{vr}^2) h_{ur} h_{vr} = 0.$$

Since $h_{ur}^2 = h_{vr}^2 = 1$, the last sum reduces to

$$(4t-4) \sum h_{ur} h_{vr}.$$

We also note that

$$\sum_{r \neq s} h_{ur}^2 h_{us} h_{vs} = \sum_{s \neq 2t+1} h_{us} h_{vs} + \cdots + \sum_{s \neq 4t} h_{us} h_{vs}$$

$$= 2t \sum h_{us} h_{vs} - \sum h_{us} h_{vs} = (2t-1) \sum h_{us} h_{vs}.$$

We therefore finally secure

$$-2 \sum_{r,s} h_{ur} h_{vs}.$$

But $\sum_s h_{vs}$ is always zero establishing the theorem of the first section.

References

[1] R. C. Bose, 'On the application of the properties of Galois fields to the construction of hyper Graeco-Latin squares', *Sankhya* 3 (1938), 323–338.

[2] R. C. Bose and K. A. Bush, 'Orthogonal arrays of strength two and three', *Annals of Math. Stat.* 23 (1952), 508–524.

https://doi.org/10.1017/S1446788700009502 Published online by Cambridge University Press

[3] R. C. Bose and S. S. Shrikhande, 'On the falsity of Euler's conjecture about nonexistence of two orthogonal Latin squares of order $4t+2$', *Proc. N. A. S.* 45 (1959), 734—737.

[4] R. C. Bose, S. S. Shrikhande and E. T. Parker, 'Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture', *Canadian Jour. Math.* 12 (1960), 189—203.

[5] R. H. Bruck and H. J. Ryser, 'The nonexistence of certain finite projective planes', *Canadian Jour. Math.* 1 (1949), 88—94.

[6] K. A. Bush, 'Orthogonal arrays of index unity', *Annals of Math. Stat.* 23 (1952), 426—434.

[7] K. A. Bush, 'Unbalanced Hadamard matrices and finite projective planes of even order', *Jour. Comb. Theory* (to apepar).

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

Washington State University
and
The Australian National University

https://doi.org/10.1017/S1446788700009502 Published online by Cambridge University Press