THE CONSTRUCTION OF HADAMARD MATRICES

E. C. Dade and K. Goldberg

An Hadamard matrix H is a (1, -1)-matrix of order 4n such that

$$HH^T = 4nI_{4n}, \tag{1}$$

where I_{4n} is the identity matrix of order 4n. The result of this paper is as follows.

THEOREM. *An Hadamard matrix of order* 4n *can be constructed if there exists a transitive permutation group of degree* 4n-- 1 *and odd order whose subgroups leaving one element fixed have three transitivity sets each.*

Suppose we can find a (0, 1)-matrix A of order 4n - 1 satisfying

$$AA^T = nI + (n - 1)J, \tag{2}$$

where I is the identity matrix, and J is the matrix with 1 in every position, of order 4n - 1. Then the bordered matrix

$$H = \begin{pmatrix} 1 & 1 \quad \cdots \quad 1 \\ 1 & \\ \cdot & \\ \cdot & 2A - J \\ \cdot & \\ 1 & \end{pmatrix}$$

satisfies (1). We shall prove that, given the permutation group of the theorem, we can construct a matrix A satisfying (2).

Let G be the permutation group of the theorem, and suppose it permutes the integers 1, 2, ⋯, 4n - 1. For each g in G, let P(g) be the permutation matrix of order 4n - 1 with 1 in the (i, j)-position if i = g(j).

Let $\mathscr{A}$ be the algebra of matrices of order 4n - 1 which commute with every P(g). If (x_{ij}) is any such matrix, then

$$(x_{ij}) = P(g)^{-1}(x_{ij})P(g) = (x_{g(i)g(j)}) \qquad (\text{all } g \in G),$$

and therefore (x_{ij}) is characterized by

$$x_{ij} = x_{g(i)g(j)} \qquad (\text{all } i, j = 1, 2, \cdots, 4n - 1 \text{ and all } g \in G). \tag{3}$$

The equivalence

Received July 18, 1958.

$$(i, j) \sim (i', j') \text{ if there is a } g \in G \text{ such that } i' = g(i),\ j' = g(j)$$

defines a partition of the set of ordered pairs formed from the integers $1, 2, \cdots, 4n - 1$. Denote the sets of this partition by $S_1, S_2, \cdots, S_m$.

For each $p = 1, 2, \cdots, m$, let $A_p = (a_{pij})$ be the incidence matrix of the set S_p. That is, let

$$a_{pij} = 1 \qquad \text{if } (i, j) \in S_p$$

and $a_{pij} = 0$ otherwise. By (3), each A_p is in $\mathscr{A}$. Suppose (x_{ij}) is in $\mathscr{A}$. Then, using equation (3), we can let

$$x_p = x_{ij} \qquad \text{if } (i, j) \in S_p$$

and obtain

$$(x_{ij}) = \sum_{p=1}^{m} x_p A_p .$$

Thus, since the A_p are clearly linearly independent, they form a basis for $\mathscr{A}$.

Since each pair (i, j) occurs in exactly one S_p, we have

$$\sum_{p=1}^{m} a_{pij} = 1 \qquad (i, j = 1, 2, \cdots, 4n - 1), \tag{4}$$

and therefore

$$A_1 + A_2 + \cdots + A_m = J .$$

Let $a_{pq}^{(r)}$ be the generic structure constant defined by

$$A_p A_q = \sum_{r=1}^{m} a_{pq}^{(r)} A_r .$$

The (i, j)-element on the right-hand side is $a_{pq}^{(r)}$, where r is defined by $a_{rij} = 1$. Thus

$$\sum_{k=1}^{4n-1} a_{pik} a_{qkj} = a_{pq}^{(r)} .$$

Summing over q we get, by (4),

$$\sum_{k=1}^{4n-1} a_{pik} = \sum_{q=1}^{m} a_{pq}^{(r)} . \tag{5}$$

This is the sum of the i-th row of A_p. The equation holds for all j, r such that $a_{rij} = 1$. Suppose $a_{pi_0j_0} = 1$. Then, because G is transitive, we can find a g in G

such that $i = g(i_0)$. Let $j = g(j_0)$, so that $a_{pij} = 1$. Then equation (5) becomes

$$\sum_{k=1}^{4n-1} a_{pik} = \sum_{q=1}^{m} a_{pq}^{(p)}.$$

The sum on the right is independent of i, and therefore all the row sums of A_p are equal. Denote this constant row sum by a_p.

Suppose $a_{111} = 1$. Then $a_{1ii} = 1$ for all i, since G is transitive. Moreover, $a_{1ij} = 1$ is possible only if $j = i$. That is, we can set

$$A_1 = I.$$

Let G_1 be the subgroup of G leaving 1 fixed, and denote its transitivity sets by $\{1\}$, U, V. Suppose $a_{212} = 1$ and 2 is in U. Then for every j in U there is a g in G_1 taking 2 into j, and therefore $a_{21j} = 1$. If k is in V, then $a_{21k} \neq 1$, and we let $a_{31k} = 1$. Then for each j in V we have $a_{31j} = 1$. That is, $A_1 + A_2 + A_3$ has 1 in every position of the first row. If there were any other A_p, it would have its first row a zero row, so that $a_p = 0$, which is impossible. Thus $m = 3$ and $A_1 + A_2 + A_3 = J$.

Suppose $a_{2ij} = a_{2ji} = 1$. Then there would be a g in G which transposes i and j, and the order of g would be even, which is impossible since G has odd order. Thus where A_2 has 1, A_3^T has 1, and conversely. That is, $A_3 = A_2^T$, and therefore $a_3 = a_2 = 2n - 1$.

Set $A = A_2$; then $A^T = A_3$. The constant row sum of A is $2n - 1$; therefore the diagonal elements of AA^T are equal to $2n - 1$ and the constant row sum of AA^T is $(2n - 1)^2$. Note that both A and A^T have zero diagonals, and that $A + A^T = J - I$.

Since $\{I, A, A^T\}$ is the basis of an algebra, we can write

$$AA^T = c_1 I + c_2 A + c_3 A^T$$

Comparing diagonal elements, we have $c_1 = 2n - 1$. Then symmetry and a comparison of row sums imply that $c_2 = c_3 = n - 1$. Thus

$$AA^T = (2n - 1)I + (n - 1)(A + A^T) = nI + (n - 1)J,$$

as desired.

If $4n - 1$ is a prime power, we can find a permutation group with properties satisfying the theorem from the Galois field $GF(4n - 1)$. The corresponding Hadamard matrices are constructable by other methods (see [1]).

However, this seems to be the first sufficient condition for the construction of the general Hadamard matrix which is not purely combinatorial. By appealing to the highly developed field of finite groups we may obtain more general results than have heretofore been possible.

REFERENCE

1. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys. 12 (1933), 311-320.

Added in proof. Professor Marshall Hall has pointed out that our groups are unlikely to exist when $4n - 1$ is not a prime power. For in this case, they would be insoluble because they are primitive. This is contrary to the classical conjecture that groups of odd order are soluble, a conjecture which has been verified for transitive permutation groups of degree ≤ 243.

Of course, the conjecture is not yet a theorem, and in those cases in which the matrix A is known to exist, the set of permutation matrices which commute with it may yield a counterexample. However, we consider this unlikely.

National Bureau of Standards
Washington, D. C.