GENERALIZED HADAMARD MATRICES

A. T. BUTSON

1. **Introduction.** A square matrix H of order h all of whose elements are pth roots of unity is called a *Hadamard matrix* ($H(p, h)$ *matrix*) if $HH^{CT} = hI$. It is known [**4**] that $H(2, h)$ matrices can exist only for values $h = 2$ and $h = 4t$, where t is a positive integer. Although it has been conjectured that $H(2, 4t)$ matrices exist for all positive integers t, their existence has been established [**1**; **3**; **4**; **5**; **6**; **7**] for only the following values of h, where q denotes an odd prime:

(1.1) $h = 2^k$;

(1.2) $h = q^k + 1 \equiv 0 \pmod 4$;

(1.3) $h = h_1(q^k + 1)$ where $h_1 \geqq 2$ is the order of an $H(2, h)$ matrix;

(1.4) $h = h^*(h^* - 1)$ where h^* is a product of numbers of forms (1.1) and (1.2);

(1.5) $h = 172$;

(1.6) $h = h^*(h^* + 3)$ where h^* and $h^* + 4$ both are products of numbers of forms (1.1) and (1.2);

(1.7) $h = h_1 h_2 (q^k + 1) q^k$ where $h_1 \geqq 2$, $h_2 \geqq 2$ are orders of $H(2, h)$ matrices;

(1.8) $h = h_1 h_2 s(s + 3)$ where $h_1 \geqq 2$, $h_2 \geqq 2$ are orders of $H(2, h)$ matrices and where s and $s + 4$ both are of the form $q^k + 1$;

(1.9) $h = (r + 1)^2$ where both r and $r + 2$ are prime or prime powers;

(1.10) h is a product of numbers of the forms (1.1)–(1.9).

This list is taken from [**2**].

This paper is concerned with $H(p, h)$ matrices when $p > 2$. The main result is the construction of $H(p, 2^m p^k)$ matrices where p is a prime and $m \leqq k$ are non-negative integers.

2. **Elementary properties.** Some easily established results concerning $H(p, h)$ matrices which will be used in the sequel are the following:

(2.1) The requirement that $HH^{CT} = hI$ is equivalent to the requirement that $H^{CT}H = hI$; i.e., the orthogonality of any two rows of H is equivalent to the orthogonality of any two columns of H.

(2.2) A permutation of the rows (columns) and multiplication of the elements of a row (column) by a fixed pth root of unity are elementary operations which leave invariant the Hadamard property.

(2.3) An $H(p, h)$ matrix can always be reduced to the standard form in which the initial row and column contain only the root 1.

Presented to the Society January 24, 1961; received by the editors June 9, 1961.

[1] It was noted by the referee that this result is known, and may be found in R. E. Bellman's *Introduction to matrix analysis*, McGraw-Hill, 1960, p. 27, problem 13.

(2.4) If $H=(h_{ij})$ is an $H(p, h)$ matrix in standard form, then

$$\sum_{j=1}^{h} h_{ij} = \sum_{j=1}^{h} h_{ij}^{C} = 0, \qquad i = 2, 3, \cdots, h;$$

$$\sum_{i=1}^{h} h_{ij} = \sum_{i=1}^{h} h_{ij}^{C} = 0, \qquad j = 2, 3, \cdots, h.$$

(2.5) If H_1 is an $H(p_1, h_1)$ matrix, H_2 is an $H(p_2, h_2)$ matrix, $h=h_1h_2$, and $p=\text{l.c.m.}(p_1, p_2)$, then $H_1 \otimes H_2$ is an $H(p, h)$ matrix.

(2.6) If H_1 is an $H(p_1, h)$ matrix, γ is a primitive p_2th root of unity, and $p=\text{l.c.m.}(p_1, p_2)$, then γH_1 is an $H(p, h)$ matrix.

3. **Construction of $H(p, h)$ matrices.** Throughout the remainder of this paper H will denote an $H(p, h)$ matrix in standard form and γ a fixed primitive pth root of unity.

When p is a prime, the requirement (2.4) that $\sum_{j=1}^{h} h_{2j}=0$ can be written in the form $\sum_{j=0}^{p-1} k_j\gamma^j=0$, where the k_j are non-negative integers satisfying $\sum_{j=0}^{p-1} k_j=h$. Using $1=-\sum_{j=1}^{p-1}\gamma^j$, the condition becomes $\sum_{j=1}^{p-1} (k_j-k_0)\gamma^j=0$, where $\sum_{j=0}^{p-1} k_j=h$. Since $\gamma, \gamma^2, \cdots, \gamma^{p-1}$ are independent over the rational field, it is necessary that $k_j=k_0$ for $j=1, 2, \cdots, p-1$. Hence $pk_0=h$ and the following result has been established.

Theorem 3.1. *When p is a prime, an $H(p, h)$ matrix can exist only for values $h=pt$, where t is a positive integer.*

The necessary condition that $h=2$ or $h=4t$ for $H(2, h)$ matrices has two obvious possible analogues for $H(p, h)$ matrices when p is a prime; namely, $h=p$ or $h=p^2t$ and $h=p$ or $h=2pt$. Results to follow in this section show that neither of these is necessary. The condition in the above theorem is the most stringent that has been obtained; and when p is not a prime, even this is not necessary as the following immediate consequence of (2.6) shows.

Theorem 3.2. *It is possible to construct $H(2p, h)$ matrices for p arbitrary and h any value described in* (1.1)–(1.10).

By using (2.6) an $H(p, h)$ matrix can be constructed from an $H(p_1, h)$ matrix, where p_1 is a divisor of p. Such an $H(p, h)$ matrix can obviously be reduced by the elementary operations (2.2) to an $H(p_1, h)$ matrix; and, consequently, is considered as trivial.

Now let V be the matrix defined by $v_{ij}=\gamma^{ij}$, $i, j=0, 1, \cdots, p-1$. Then $\sum_{j=0}^{p-1} v_{ij}v_{kj}^{C}=\sum_{j=0}^{p-1}\gamma^{(i-k)j}$. When $i=k$, then $\sum_{j=0}^{p-1}\gamma^{(i-k)j}=p$. Suppose $i\neq k$. If $(i-k, p)=1$, then γ^{i-k} is a primitive pth root of unity and $\sum_{j=0}^{p-1}\gamma^{(i-k)j}=0$. If $(i-k,\ p)=d$ where $d>1$, let $p=p_1d$ and $i-k=i_1d$. Then $(i-k)p_1=i_1dp_1=i_1p\equiv 0 \pmod p$, so that γ^{i-k} is a p_1th root of unity. In this case $\sum_{j=0}^{p-1}\gamma^{(i-k)j}=d\sum_{j=0}^{p_1-1}\gamma^{(i-k)j}=0$. This establishes the following theorem.

THEOREM 3.3. *The Vandermonde matrix V defined by $v_{ij}=\gamma^{ij}$, $i, j=0, 1, \cdots, p-1$, is a symmetric $H(p, p)$ matrix.*[1]

If $p=p_1p_2\cdots p_r$, where the p_j are distinct prime powers, γ_j is a primitive p_jth root of unity, and V_j the corresponding Vandermonde matrix, then permutation matrices P and Q exist such that $V=P(V_1\otimes V_2\otimes\cdots\otimes V_r)Q$. However, V_j can not be so decomposed, so it would not have been sufficient to have proven the above theorem for p a prime.

Suppose p is odd, say $p=2q+1$, and let n be the smallest quadratic nonresidue of p. Denote by U that permutation matrix such that $W=VU$ has elements $w_{ij}=\gamma^{nij}$, $i, j=0, 1, \cdots, p-1$. Define the matrix Q by $q_{ij}=0$ for $i\neq j$ and $q_{ii}=\gamma^{qi^2}$ for $i=0, 1, \cdots, p-1$. Then $C=QVQ$ and $B=Q^nWQ^n$ are, by (2.2), $H(p, p)$ matrices. Using $-2q\equiv 1 \pmod p$, it is easy to see that $c_{ij}=\gamma^{q(i-j)^2}$ and $b_{ij}=\gamma^{nq(i-j)^2}$. Obviously now, $c_{ij}=c_{i+k,j+k}$ and $b_{ij}=b_{i+k,j+k}$ for $k=0, 1, \cdots, p-1$, so that C and B are cyclic matrices. Furthermore, C and B are symmetric matrices, and each contains at most $q+1$ distinct pth roots of unity.

Defining the product of two rows v_i and v_j of V to be that vector obtained by multiplying (mod p) the corresponding components of the two rows, it is noted that $v_iv_j=v_{i+j}$, so that the rows of V form a cyclic group with generator v_1. Similarly, the columns of V, the rows of W, and the columns of W all form cyclic groups with generators v_1^T, $w_1=v_n$, and $w_1^T=v_n^T$, respectively. From this observation it easily follows that $D^kV=VT^k$ and $D^{nk}W=WT^k$, where D is the matrix defined by $d_{ij}=0$ for $i\neq j$, and $d_{ii}=\gamma^i$ for $i=0, 1, \cdots, p-1$, and T is the permutation matrix defined by $t_{i+1,i}=1$ for $i=0, 1, \cdots, p-1$ and $t_{ij}=0$ otherwise.

Let $Y=(11\cdots 1)$ and $Z=(00\cdots 0)$, both of length p. Then the kth column of B can be written in the form $T^kQ^nY^T$, and the kth column of CP in the form $T^{kn}QY^T$. It will now be easy to prove the following construction theorem.

THEOREM 3.4. *When p is a prime, an $H(p, 2p)$ matrix can be constructed.*

The procedure will be to show that the matrix

$$K = \left(\frac{QV}{(CP)^{CT}} \middle| \frac{Q^n W}{B^{CT}} \right)$$

is an $H(p, 2p)$ matrix. First it is noted that $CY^T = (YQY^T)Y^T$ and $BY^T = (YQ^nY^T)Y^T$. When $p = 2q+1$ is prime, there are q quadratic residues and q quadratic nonresidues of p. Consequently,

$$YQY^T + YQ^nY^T = \sum_{i=0}^{p-1} \gamma^{qi^2} + \sum_{i=0}^{p-1} \gamma^{nqi^2} = 2 \sum_{j=0}^{p-1} \gamma^{qj} = 0.$$

Thus $CY^T + BY^T = Z^T$. Now KK^{CT} in block form is

$$\left(\frac{(QV)(QV)^{CT} + (Q^nW)(Q^nW)^{CT}}{(CP)^{CT}(QV)^{CT} + B^{CT}(Q^nW)^{CT}} \middle| \frac{(QV)(CP) + (Q^nW)B}{(CP)^{CT}(CP) + B^{CT}B} \right).$$

By (2.2), QV, Q^nW, CP, and B are all $H(p, p)$ matrices. Thus $(QV)(QV)^{CT} + (Q^nW)(Q^nW)^{CT} = (CP)^{CT}(CP) + B^{CT}B = 2pI_p$. Now consider $(QV)(CP) + (Q^nW)B$. Using the fact that the kth columns of CP and B can be written as $T^{kn}QY^T$ and $T^kQ^nY^T$, respectively, the kth column of $(QV)(CP) + (Q^nW)B$ is then given by

$$\begin{aligned} QVT^{kn}QY^T + Q^nWT^kQ^nY^T &= D^{kn}QVQY^T + D^{kn}Q^nWQ^nY^T \\ &= D^{kn}(CY^T + BY^T) = D^{kn}Z^T = Z^T. \end{aligned}$$

Hence, $(QV)(CP) + (Q^nW)B$ and its conjugate transpose $(CP)^{CT}(QV)^{CT} + B^{CT}(Q^nW)^{CT}$ are both 0. Thus $KK^{CT} = 2pI_{2p}$ and the theorem is proven. An immediate consequence of this theorem and (2.5) is now stated.

THEOREM 3.5. *When p is a prime, $H(p, 2^mp^k)$ matrices can be constructed for any non-negative integers $m \leqq k$.*

All the preceding results on the construction of $H(p, h)$ matrices are summarized in the following theorem.

THEOREM 3.6. *Let $p = 2^{k_0}p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$ be the factorization of p into powers of distinct primes. If $k_0 = 0$, then $H(p, h_1)$ matrices can be constructed for $h_1 = 2^{j_0}p_1^{j_1}p_2^{j_2} \cdots p_r^{j_r}$, where $j_i \geqq 0$, $i = 0, 1, \cdots, r$; $j_i > 0$ for at least one $i > 0$; and $j_0 \leqq \sum_{i=1}^{r} j_i$. If $k_0 \neq 0$, then $H(p, h_4)$ matrices can be constructed for $h_4 = h_2h_3$, where h_2 is 1 or the order of any $H(2, h)$ matrix, and h_3 is 1 or any value of h_1.*

4. Remarks. Let the matrix obtained from H by deleting the initial row and column of 1's be called the core of H. Let π be a primitive root of the prime p. Then there exists a permutation matrix P such that the core of PVP is the cyclic matrix whose rows are all the cyclic permutations of $(\gamma^{\pi}\gamma^{\pi^2}\cdots\gamma^{\pi^{p-1}})$. The rows of PVP obviously form a group. In a subsequent paper the connection between an $H(p, p^n)$ matrix whose rows form a group and whose core is cyclic, a maximal length linear recurring sequence with elements in $GF(p)$, and a "relative" difference set will be shown. One consequence of this connection is the following theorem.

THEOREM 4.1. *For any prime p and any positive integer n, an $H(p, p^n)$ matrix whose rows form a group and whose core is cyclic can be constructed.*

REFERENCES

1. R. C. Bose, *On the construction of balanced incomplete block designs*, Annals of Eugenics **9** (1939), 353–399.

2. R. C. Bose and S. S. Shrikhande, *A note on a result in the theory of code construction*, Information and Control **2** (1959), 183–194.

3. A. Brauer, *On a new class of Hadamard determinants*, Math. Z. **58** (1953), 219–225.

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

5. R. G. Stanton and D. A. Sprott, *A family of difference sets*, Canad. J. Math. **10** (1958), 73–77.

6. J. Williamson, *Hadamard determinant theorem and sum of four squares*, Duke Math. J. **11** (1944), 65–81.

7. ———, *Note on Hadamard's determinantal problem*, Bull. Amer. Math. Soc. **53** (1947), 608–613.

BOEING AIRPLANE COMPANY