GENERALIZED HADAMARD MATRICES

A. T. BUTSON

1. Introduction. A square matrix $H$ of order $h$ all of whose elements are $p$th 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 $h_1 \geq 2$ 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) $h = h_1h_2(q^k + 1)q^k$ where $h_1 \geq 2$, $h_2 \geq 2$ are orders of $H(2, h)$ matrices;
(1.8) $h = h_1h_2s(s + 3)$ where $h_1 \geq 2$, $h_2 \geq 2$ 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 $H(p, 2^mp^k)$ matrices where $p$ is a prime and $m \leq k$ 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 $H^CTH = hI$; 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 $p$th 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

$$\sum_{j=1}^{h} h_{ij} = \sum_{i=1}^{h} h_{ij} = 0, \quad i = 2, 3, \ldots, h;$$

$$\sum_{i=1}^{h} h_{ij} = \sum_{i=1}^{h} h_{ij} = 0, \quad j = 2, 3, \ldots, h.$$  

(2.5) If $H_1$ is an $H(p_1, h_1)$ matrix, $H_2$ is an $H(p_2, h_2)$ matrix, $h = h_1 h_2$, 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, $\gamma$ is a primitive $p_2$th root of unity, and $p = \text{l.c.m.}(p_1, p_2)$, then $\gamma H_1$ 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 $\gamma$ a fixed primitive $p$th 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 $1 = - \sum_{j=0}^{p-1} \gamma^{j}$, the condition becomes $\sum_{j=0}^{p-1} (k_{j} - k_{0}) \gamma^{j} = 0$, where $\sum_{j=0}^{p-1} k_{j} = h$. Since $\gamma, \gamma^{2}, \ldots$, $\gamma^{p-1}$ are independent over the rational field, it is necessary that $k_{j} = k_{0}$ for $j = 1, 2, \ldots, p - 1$. 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 $h = p^{2} t$ and $h = p$ or $h = 2 pt$. 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 $v_{ij} = \gamma^{ij}, \ i, j = 0, 1, \ldots, p - 1$. Then $\sum_{j=0}^{p-1} v_{ij}v_{ij}^{*} = \sum_{j=0}^{p-1} \gamma^{(i-k)j}$. When $i = k$, then $\sum_{j=0}^{p-1} \gamma^{(i-k)j} = p$. Suppose $i \neq k$. If $(i-k, p) = 1$, then $\gamma^{i-k}$ is a primitive $p$th root of
unity and $\sum_{k=0}^{p-1} \gamma^{(i-k)i}=0$. If $(i-k, p)=d$ where $d>1$, let $p=p_1d$ and $i-k=i_1d$. Then $(i-k)p_1=i_1dp_1=i_1p_1\equiv 0 \pmod{p}$, so that $\gamma^{i-k}$ is a $p_1$th root of unity. In this case $\sum_{k=0}^{p-1} \gamma^{(i-k)i}=d \sum_{k=0}^{p_1-1} \gamma^{(i-k)i}=0$. This establishes the following theorem.

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

If $p=p_1p_2\cdots p_r$, where the $p_i$ are distinct prime powers, $\gamma_j$ is a primitive $p_i$th 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, $V_j$ cannot 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 $w_{ij}=\gamma^{ni}$, $i, j=0, 1, \ldots, p-1$. Define the matrix $Q$ by $q_{ij}=0$ for $i\neq j$ and $q_{ii}=\gamma^{qi}$ for $i=0, 1, \ldots, p-1$. 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 $k=0, 1, \ldots, p-1$, so that $C$ and $B$ are cyclic matrices. Furthermore, $C$ and $B$ are symmetric matrices, and each contains at most $q+1$ distinct $p$th 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 $v^*_1$, $w_1=v_n$, and $w^*_1=v^*_n$, respectively. From this observation it easily follows that $D^kV=VT^k$ and $D^kW=WT^k$, where $D$ is the matrix defined by $d_{ij}=0$ for $i\neq j$, and $d_{ii}=\gamma^i$ for $i=0, 1, \ldots, p-1$, and $T$ is the permutation matrix defined by $t_{i+1, i}=1$ for $i=0, 1, \ldots, p-1$ and $t_{i, i}=0$ otherwise.

Let $Y=(1 \cdots 1)$ and $Z=(00 \cdots 0)$, both of length $p$. Then the $k$th column of $B$ can be written in the form $T^kQ^nY^T$, and the $k$th column of $CP$ in the form $T^kQ^nY^T$. 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
is an $H(p, 2p)$ matrix. First it is noted that $CY^T = (YQY^T)Y^T$ and $BY^T = (YQ^n Y^T)Y^T$. When $p = 2q + 1$ is prime, there are $q$ quadratic residues and $q$ quadratic nonresidues of $p$. Consequently,

$$YQY^T + YQ^n Y^T = \sum_{i=0}^{p-1} \gamma^{qi^2} + \sum_{i=0}^{p-1} \gamma^{qi^3} = 2 \sum_{j=0}^{p-1} \gamma^{qi} = 0.$$ 

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

$$\begin{pmatrix} (QV)(QV)^{CT} + (Q^n W)(Q^n W)^{CT} & (QV)(CP) + (Q^n W)B \\ (CP)^{CT}(QV)^{CT} + BCT(Q^n W)^{CT} & (CP)^{CT}(CP) + BCTB \end{pmatrix}.$$ 

By (2.2), $QV$, $Q^n W$, $CP$, and $B$ are all $H(p, p)$ matrices. Thus $(QV)(QV)^{CT} + (Q^n W)(Q^n W)^{CT} = (CP)^{CT}(CP) + BCTB = 2pI_p$.

Now consider $(QV)(CP) + (Q^n W)B$. Using the fact that the kth column of $CP$ and $B$ can be written as $T^k QY^T$ and $T^k Q^n Y^T$, respectively, the kth column of $(QV)(CP) + (Q^n W)B$ is then given by

$$QV T^k QY^T + Q^n W T^k Q^n Y^T = D^k QV QY^T + D^k Q^n W Q^n Y^T = D^k (CY^T + BY^T) = D^k Z^T = Z^T.$$ 

Hence, $(QV)(CP) + (Q^n W)B$ and its conjugate transpose $(CP)^{CT}(QV)^{CT} + BCT(Q^n W)^{CT}$ 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, $H(p, 2^m p^k)$ matrices can be constructed for any non-negative integers $m \leq k$.

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

**Theorem 3.6.** Let $p = 2^{k_1} p_1^{k_2} \cdots p_r^{k_r}$ be the factorization of $p$ into powers of distinct primes. If $k_0 = 0$, then $H(p, h_i)$ matrices can be constructed for $h_i = 2^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $j_i \geq 0$, $i = 0, 1, \cdots, r$; $j_i > 0$ for at least one $i > 0$; and $j_0 \leq \sum_{i=1}^{r} j_i$. If $k_0 \neq 0$, then $H(p, h_4)$ matrices can be constructed for $h_4 = h_0 h_3$, where $h_3$ is 1 or the order of any $H(2, h)$ matrix, and $h_4$ is 1 or any value of $h_4$.

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 $\pi$ be a primitive root of the prime $p$. Then there exists a permutation matrix $P$ such
A. T. BUTSON

that the core of \( PVP \) is the cyclic matrix whose rows are all the cyclic permutations of \( (\gamma^r \gamma^s \cdots \gamma^{r-1}) \). 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**


Boeing Airplane Company