A Note of a Class of Hadamard Matrices

JENNIFER WALLIS

La Trobe University, Bundoora 3083, Victoria, Australia
Communicated by Marshall Hall, Jr.
Received September 9, 1968

An Hadamard matrix $H$ is a matrix of order $n$ all of whose elements are $+1$ or $-1$ and which satisfies $HH^T = nI_n$. $H = S + I_n$ is a skew-type Hadamard matrix if $S^T = -S$.

It is conjectured that an Hadamard matrix always exists for $n = 4t$, $t$ any integer. Many known matrices and classes of matrices can be found in [1].

In [1, p. 207] it is noted that an Hadamard matrix of order $h(h - 1)$ always exists when $h = 2(p^s + 1)$, $r, s$ integers and $p$ a prime such that $p^s + 1 \equiv 0 \pmod{4}$. We now consider cases $p^s \equiv 1 \pmod{4}$.

Let $p(\text{prime}) \equiv 1 \pmod{4}$ and let $A = (a_{ij})$, $B = (b_{ij})$, $D = (d_{ij})$, all $p \times p$ matrices, be given as follows where $\chi(i)$ is the Legendre symbol modulo $p$.

\[
d_{ij} = \begin{cases} 0 & i = j, \\ 1 & i \neq j, \end{cases} \chi(j - i)
\]

\[
A = D + I, \\
B = D - I.
\]

Further define $J$ to be the $p \times p$ matrix of all $+1$'s and $K = J - 2I$ where $I$ is the $p \times p$ unit matrix.

Since $J, K, A$ and $B$ are circulant and symmetric they commute in pairs.

Now

\[
JJ^T = pI_p,
KK^T = 4I_p + (p - 4)J_p,
DD^T = pI_p - J_p,
\]

so

\[
AA^T = (D + I_p)(D + I_p)^T = DD^T + 2D + I_p
= (p + 1)I_p - J_p + 2D,

BB^T = (D - I_p)(D - I_p)^T = DD^T - 2D + I_p
= (p + 1)I_p - J_p - 2D.
\]
Then, if
\[ M = \begin{bmatrix} J & K \\ -K & J \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} A & B \\ B & -A \end{bmatrix}, \]

\[ MMT^T = (4I_p + (2p - 4) J_p) \times I_2 \quad \text{and} \quad NNT^T = (2(p + 1) I_p - 2J_p) \times I_2. \]

Since \( A, B, J, K \) obey the condition above,

\[ MNT^T = \begin{bmatrix} JAT + KBT^T & JB - KAT \\ -KAT + JB^T & -KB - JAT \end{bmatrix} \]
\[ = \begin{bmatrix} AJT^T + BK^T & BJ^T - AK^T \\ -AK^T + BJ^T & -BK^T - AJ^T \end{bmatrix} = NMT^T. \]

**Theorem 1.** If there exists a skew-type Hadamard matrix \( H = S + I_{p-1} \)

of order \( p-1 \), where \( p \text{ (prime) } \equiv 1 \pmod{4} \), and if \( M \) and \( N \) are as defined above then \( H = S \times N + I_{p-1} \times M \) is an Hadamard matrix of order \( 2p(p - 1) \).

**Proof:**

\[ HHT^T = (S + I_{p-1})(ST^T + I_{p-1}) = SST^T + I_{p-1} \]
\[ = (p - 1) I_{p-1}, \]

so

\[ SST^T = (p - 2) I_{p-1}. \]

Then

\[ HHT^T = (S \times N + I_{p-1} \times M)(ST^T \times N^T + I_{p-1} \times MT^T) \]
\[ = SST^T \times NNT^T + S \times NMT^T + ST^T \times MNT^T + I_{p-1} \times MMT^T \]
\[ = I_{p-1} \times (4I_p + (2p - 4) J_p) \times I_2 \]
\[ + (p - 2) I_{p-1} \times (2(p + 1) I_p - 2J_p) \times I_2 \]
\[ = (4 + 2(p - 2)(p + 1)) I_{2p(p-1)} \]
\[ = 2p(p - 1) I_{2p(p-1)}. \]

If \( D \) is defined by the quadratic residues of \( GF(p^r) \), \( p^r \) a prime power, instead of by the Legendre symbol we have, similarly,

**Theorem 2.** If there exists a skew-type Hadamard matrix of order

\( p^r - 1 \), where \( p^r \text{ (prime power) } \equiv 1 \pmod{4} \), and if \( M \) and \( N \) are as defined above then \( H = S \times N + I \times M \) is an Hadamard matrix of order

\( 2p^r(p^r - 1) \).

**References**