A Class of Hadamard Matrices

JENNIFER WALLIS

Department of Mathematics, Melbourne University, Melbourne,
and
La Trobe University, Melbourne, Australia

Communicated by Marshall Hall

ABSTRACT

Whenever there exists a quasi-skew Hadamard matrix of order $4n$ and $(4n - 1, k, m - n + k)$ and $(4n - 1, u, v - n)$ configurations with circulant incidence matrices, then there exists an Hadamard matrix of order $4m(4n - 1)$.

An Hadamard matrix is a square matrix of ones and minus ones whose row (and hence column) vectors are orthogonal. The order $n$ of an Hadamard matrix is necessarily $1, 2$ or $4t$ with $t = 1, 2, 3, \ldots$. It has been conjectured that this condition $(n = 1, 2, or 4t)$ also ensures the existence of an Hadamard matrix. Constructions have been given for particular values of $n$ and even for various infinite classes of values. While other constructions exist, those given in the bibliography of [2] and in [1] and [2] themselves exhaust all the previously known values of $n$. The only value for $n = 4t \leq 232$ which has not been decided is 188.

A matrix $Q$ will be called quasi-skew if $Q = S - I$, that is $Q - Q^T = 2I$, where $S$ is skew-symmetric. Williamson [5] has shown that a quasi-skew Hadamard matrix of order $N$ exists for

$$N = 2^r k_1 k_2 \cdots k_r,$$

where $k_i = p_i^{i+1} + 1 \equiv 0 \pmod{4}$, $p_i$ being an odd prime. We note that a quasi-skew matrix, $Q = (q_{ij})$ of order $4n - 1$, may be found by choosing

$$-q_{ij} = \left( \frac{j - i}{4n - 1} \right),$$

where $(\cdot)$ is the Legendre symbol [4, p. 81]. So if $e$ is a $1 \times (4n - 1)$ matrix comprising all $-1$'s, then

$$H = \begin{bmatrix} 1 & e^T \\ -e^T & Q \end{bmatrix}$$

is a quasi-skew matrix of order $4n$. 40
$B$ will stand for a matrix satisfying

$$BB^T = 4nI - J,$$

(2)

where $J$ is the matrix comprising all $+1$'s and $I$ is the identity matrix.

One such $B$ is the matrix obtained by rearranging an Hadamard matrix of order $4n$ to

$$H = \begin{bmatrix} 1 & e \\ e^T & B \end{bmatrix}$$

with $e$ as before. $(B = (b_{jk})$ is a $(1, -1)$ matrix corresponding to a $(4n - 1, 2n, n)$ configuration, as defined on p. 102 of [3]. We note that any $(1, -1)$ matrix corresponding to a $(4n - 1, u, u - n)$ configuration will satisfy (2).

We shall write $A = (a_{ij})$ for a $(4n - 1) \times (4n - 1)$ $(1, -1)$ matrix corresponding to a $(4n - 1, v, m - n + v)$ configuration. Then $A$ satisfies

$$AA^T = 4(n - m)I - (4m - 1)J,$$

(3)

where $I$ and $J$ are as before.

For our subsequent discussion we will require $A$ and $B$ to have circulant incidence matrices. These do exist, in at least two cases, because difference sets $(v, k, \lambda)$ configurations with $k = 0$ or 1 and $\lambda = 0$ give circulant matrices.

We will now show that if there exists such an $A$ and $B$ then we can define $C = (c_{ij})$ such that $AC^T$ is symmetric.

Let $X = \{x_1, x_2, \ldots, x_v\}$ be the positions of the elements corresponding to a $(4n - 1, v, m - n + v)$ configuration and $Y = \{y_1, y_2, \ldots, y_u\}$ similarly correspond to a $(4n - 1, u, u - n)$ configuration where both $X$ and $Y$ generate circulant incidence matrices. Write

$$a_{ij} = \begin{cases} -1 & \text{if } i + j \equiv X \pmod{4n - 1}, \\ +1 & \text{otherwise}, \end{cases}$$

and

$$b_{ij} = \begin{cases} +1 & \text{if } i + j \in Y, \\ -1 & \text{otherwise}, \end{cases}$$

$$c_{ij} = b_{4n-1-i,j}.$$

(It is easily verified that $C$ is of the form (2).)

**Theorem 1.** $AC^T$ is symmetric.
PROOF: The \((i, j)\) element of \(AC^T\) is
\[
\sum_k a_{ik}c_{kj} = \sum_k a_{ik}b_{km-j,k} = -\sum_{i+k\in X} b_{km-j,k} + \sum_{i+k\notin X} b_{km-j,k}.
\]

\(X\) has \(v\) elements, so there are \(v\) terms in the first summation and \(4n - 1 - v\) in the other. \(Y\) has \(u\) elements, so \(u\) of the \(b_{km-j,k}\) are positive. Suppose \(p\) of them occur in the first summation. The line becomes
\[
- (+ \cdots + - - \cdots - -) + (+ \cdots + - - \cdots - -)
\]
\[
p \quad v - p \quad u - p \quad 4n - 1 - v - u + p
\]
\[
= 2v + 2u - 4n + 1 - 4p.
\]

Where \(p\) is the number of choices of \(k\) such that \(i + k \in X\) and \(4n - j + k \in Y\), that is the number of pairs \(x_a\) and \(y_b\) such that \(j + i - 4n \equiv x_a - y_b \pmod{4n - 1}\).

By a similar argument the \((j, i)\) element of \(AC^T\) is \(2v + 2u - 4n + 1 - 4s\), where \(s\) is the number of pairs \(x_a\) and \(y_b\) such that \(j + i - 4n \equiv x_a - y_b \pmod{4n - 1}\). So \(s = p\) and the matrix is symmetric. Q.E.D.

**Theorem 2.** With \(A, C,\) and \(Q\) as above \(K = C \times S + A \times I_{4m}\) is an Hadamard matrix of order \(4M = 4m(4n - 1)\).

**Proof:** Since \(Q = S + I_{4m}\) is a quasi-skew Hadamard matrix of order \(4m\),
\[
4mI_{4m} = QQ^T = (S + I_{4m})(S^T + I_{4m})
\]
\[
= SS^T + I_{4m} + (S + S^T)I_{4m}
\]
\[
= SS^T + I_{4m}.
\]

So
\[
KK^T = (C \times S + A \times I_{4m})(C^T \times S^T + A^T \times I_{4m})
\]
\[
= CCT \times SS^T + A^T \times S^T + CAT \times S + AAT \times I_{4m}
\]
\[
= (4n - 1)I_{4m} \times (SS^T + I_{4m}) + AC^T \times S + CAT \times S
\]
by (2) and (3)
\[
= (4n - 1)4mI_{4m} \quad \text{by Theorem 1.} \quad \text{Q.E.D.}
\]

**Theorem 3.** There exists an Hadamard matrix of order \(4M = 4h_1(4h_2 - 1)\) whenever there exist \((4h_2 - 1, k, h_1 - h_2 + k)\) and \((4h_2 - 1, u, u - h_2)\) configurations with circulant incidence matrices and a quasi-skew matrix of order \(4h_1\).
COROLLARY 4. If there exist \((1, -1)\) matrices \(A\) and \(C\) such that \(AA^T = 4(n - m)I + (4m - 1)J\), \(CC^T = 4nI - J\) (as in (2)) and \(AC^T = CA^T\), and a quasi-skew Hadamard matrix of order \(4m\), then there exists an Hadamard matrix of order \(4m(4n - 1)\).

It is known [3, pp. 104 and 132] that a \((q^2 + q + 1, q + 1, 1)\) configuration always exists when \(q = p^\alpha, p\) a prime and \(\alpha\) a positive integer. These configurations correspond with cyclic projective planes and planar difference sets. Now difference sets satisfy our condition of yielding circulant matrices so \(A\) exists for \(4h_1 - 1 = q^2 + q + 1, v = q + 1, h_1 - h_2 + v = 1\), that is, \(4h_1 = (q - 2)(q - 1)\) and \(4M = (q - 2)(q - 1)\).

COROLLARY 5. There exist Hadamard matrices of order \((q - 2)(q - 1)\) where \(q = p^\alpha\) as before, whenever a quasi-skew Hadamard matrix of order \((q - 2)(q - 1)\) and a circulant

\[
\begin{pmatrix}
q^2 + q + 1, u, u - \frac{q^2 + q + 2}{4}
\end{pmatrix}
\]

configuration exist.

COROLLARY 6. An Hadamard matrix of order \(4M = 4h(4h - 1)\) exists whenever a quasi-skew Hadamard matrix of order \(4h\) and a \((4h - 1, 2h, h)\) configuration with circulant incidence matrix exist.

This follows from putting \(h = h_1 = h_2\). Obviously a \((4h - 1, 0, 0)\) configuration always exists and so we obtain the class of [5, pp. 65–68].

COROLLARY 7. An Hadamard matrix of order \(4M = 4h(4h + 3)\) exists whenever a quasi-skew Hadamard matrix of order \(4h\) and a \((4h - 1, 2h, h)\) configuration with a circulant incidence matrix exist.

We obtain this result by putting \(h = h_1 = h_2 - 1\) in Theorem 3, and clearly a \((4h - 1, 1, 0)\) configuration always exists. This is the class of [6].

In particular if \(4h = p^\alpha - 1\) \((p\) prime \(\alpha\) a positive integer) we have the classes \(p^\alpha(p^\alpha + 1)\) and \((p^\alpha + 1)(p^\alpha + 4)\).

REFERENCES

