On Hadamard Matrices Constructible by Circulant Submatrices

By C. H. Yang

Abstract. Let \( V_{2n} \) be an \( H \)-matrix of order \( 2n \) constructible by using circulant \( n \times n \) submatrices. A recursive method has been found to construct \( V_{4n} \) by using circulant \( 2n \times 2n \) submatrices which are derived from \( n \times n \) submatrices of a given \( V_{2n} \). A similar method can be applied to a given \( W_{4n} \), an \( H \)-matrix of Williamson type with odd \( n \), to construct \( W_{8n} \). All \( V_{8n} \) constructible by the standard type, for \( 1 \leq n \leq 16 \), and some \( V_{2n} \), for \( n \geq 20 \), are listed and classified by this method.

Let \( H_n \) be an \( n \times n \) Hadamard matrix. Although it is conjectured that no circulant \( H_{4n} \)-matrix exists for \( n > 1 \) (see [3]), it is known that many \( H_{4n} \)-matrices can be constructed by using circulant submatrices of order \( n \) or \( 2n \). (For \( H \)-matrices of Williamson type, see [1], [2], [4].)

Let \( V_{2n} \) be an \( H_{2n} \)-matrix constructible by using circulant \( n \times n \) submatrices. Then \( V_{2n} \) can be constructed by the following standard type:

\[
(*) \quad M_{2n} = \begin{bmatrix} A & B \\ -B^T & A^T \end{bmatrix}, \quad \text{where } A, B \text{ are } n \times n \text{ circulant matrices}
\]

and \( C^T \) means the transposed matrix of \( C \).

A recursive method has been found to construct \( V_{4n} \) by circulant \( 2n \times 2n \) matrices which are derived by circulant \( n \times n \) submatrices of a given \( V_{2n} \). (See Theorem 1, below.) Likewise, let \( W_{4n} \) be an \( H_{4n} \)-matrix of Williamson type with odd \( n \); \( W_{8n} \) can be constructed by using \( 2n \times 2n \) symmetric circulant matrices which are derived from \( n \times n \) symmetric circulant submatrices of a given \( W_{4n} \). (See Theorem 2.)

Let \( S_n = ((e_i)) \) be the \( n \times n \) circulant matrix with the first row entries \( e_i \), \((0 \leq i \leq n - 1)\), all zero except for \( e_1 = 1 \). Then \( n \times n \) circulant matrices \( A, B \) of (*) can be written as polynomials in \( S \). (We shall omit the suffix \( n \) of \( S_n \) and others when there is no confusion.)

\[
A = A_n(S) = \sum_{i=0}^{n-1} a_i S^i, \quad B = B_n(S) = \sum_{i=0}^{n-1} b_i S^i,
\]

with coefficients \( a_i, b_i = 1 \) or \(-1\); where \( S^0 = I_n \) is the \( n \times n \) identity matrix.

A sufficient condition for the matrix \( M_{2n} \) of type (*) being an \( H \)-matrix is that \( M_{2n}M_{2n}^T = 2nI_{2n} \) which is equivalent to

\[
(1) \quad AA^T + BB^T = 2nI_n.
\]

Received March 31, 1970.

AMS 1970 subject classifications. Primary 05B20, 62K05, 05A19; Secondary 15A36, 05D4, 1504.
Key words and phrases. Construction of Hadamard matrices, circulant matrices, standard type \( H \)-matrices, Williamson type \( H \)-matrices, recursive method for \( H \)-matrices, table for some \( H \)-matrices.

Copyright © 1971, American Mathematical Society
Let $P = P_n(S)$, $Q = Q_n(S)$ be matrices obtained by replacing $-1$ by $0$ in $A$, $B$ respectively. Then the condition (1) is equivalent to

$$PP^T + QQ^T = (p_n + q_n - r_n)I + r_nJ,$$

where $J = J_n = \sum_{i=1}^{n-1} S^i$ and $p_n$, $q_n$ are, respectively, the numbers of 1's in each row of $P$, $Q$. Here, $p_n$, $q_n$ and $r_n$ must be solutions of the following necessary conditions for existence of $V_{2n}$.

$$n - 2p_n + (n - 2q_n)^2 = 2n,$$

$$p_n + q_n - r_n = \frac{1}{2}n.$$

Similarly, by taking $Q' = J - Q$, instead of $Q$ in (2), (3), and (4), which is possible since whenever $A$ and $B$ satisfy the condition (1), so do $A$ and $-B$, we obtain the corresponding conditions:

$$PP^T + Q'Q'^T = (p_n + q'_n - r'_n)I + r'_nJ,$$

$$n - 2p_n + (n - 2q'_n)^2 = 2n,$$

$$p_n + q'_n - r'_n = \frac{1}{2}n.$$

Since $q'_n = n - q_n$, we also obtain from (7) and (4),

$$r'_n = 2p_n - r_n.$$

**Theorem 1.** Let $M_{2m}$ be a given $V_{2m}$-matrix of type (*) satisfying the conditions (2), (3), and (4). Then $M_{4m}$, a $V_{4m}$-matrix of type (*), can be found as follows:

$$P_{2m}(s) = P_m(s^2) + s^kQ_m(s^2), \quad Q_{2m}(s) = P_m(s^2) + s^kQ'_m(s^2),$$

where $s = S_{2m}$, $Q'_m = J_m - Q_m$, and $k$ is any odd integer.

**Proof.** Since $p_{2m} = p_m + q_m$, $q_{2m} = p_m + (m - q_m)$, $r_{2m} = 2p_m$ are solutions of the conditions (3) and (4) for $n = 2m$ whenever $p_m$, $q_m$, $r_m$ are solutions of (3) and (4) for $n = m$, it is sufficient to show that $P_{2m}$ and $Q_{2m}$ satisfy the condition (2), i.e.

$$P_{2m}P_{2m}^T + Q_{2m}Q_{2m}^T = mI_{2m} + 2p_mJ_{2m}.$$

From (**), the left side of (5) equals, (since $P^T(s) = P(s^{-1}))$,

$$(P(s^2)P(s^{-2}) + Q(s^2)Q(s^{-2})) + (P(s^2)P(s^{-2}) + Q'(s^2)Q'(s^{-2}))$$

$$+ [s^kP(s^{-2}) + s^{-k}P(s^2)]J_m(s^2),$$

$$= \frac{1}{2} mI + r_m \sum_{i=0}^{m-1} s^{2i} + \frac{1}{2} mI + (2p_m - r_m) \sum_{i=0}^{m-1} s^{2i} + 2p_m \sum_{i=0}^{m-1} s^{2i+1}$$

$$= mI + 2p_mJ.$$

Let $N_{4n}$ be a $4n \times 4n$ matrix such that

$$N_{4n} = \begin{bmatrix}
A & B & C & D \\
-B & A & -D & C \\
-C & D & A & -B \\
-D & -C & B & A
\end{bmatrix}$$
where $A, B, C, D$ are $n \times n$ symmetric circulant $(+1, -1)$-matrices. Then a sufficient condition for $N_{4n}$ being a $W_{4n}$-matrix is that

$$N_{4n}^T N_{4n} = 4nI_{4n}.$$  

Let $P, Q, K,$ and $G$ be matrices obtained by replacing $-1$ by 0 in $A, B, C,$ and $D$, respectively. Then, corresponding to the conditions (2)-(4), we obtain

$$(2') \quad P^2 + Q^2 + K^2 + G^2 = (t_n - r_n)I + r_n J,$$

where $t_n = p + q + k + g; p, q, k,$ and $g$ are the numbers of 1's in each row of $A, B, C,$ and $D$, respectively.

$$(3') \quad (n - 2p)^2 + (n - 2q)^2 + (n - 2k)^2 + (n - 2g)^2 = 4n.$$  

$$(4') \quad t_n - r_n = n.$$  

Similarly, corresponding to the conditions (5)-(8), we obtain

$$(5') \quad P^2 + Q'^2 + K^2 + G'^2 = (t'_n - r'_n)I + r'_n J,$$

where $Q' = J - Q, G' = J - G,$ and $t'_n = p + q' + k + g'$; $q'$ and $g'$ are, respectively, the numbers of 1's in each row of $Q'$ and $G'$.

$$(6') \quad (n - 2p)^2 + (n - 2q')^2 + (n - 2k)^2 + (n - 2g')^2 = 4n.$$  

$$(7') \quad t'_n - r'_n = n.$$  

$$(8') \quad r'_n = 2(p + k) - r_n.$$  

**Theorem 2.** Let $N_{4m}$ be a given $W_{4m}$-matrix with odd $m$ satisfying the conditions (2'), (3') and (4'). Then $N_{8m},$ a $W_{8m}$-matrix, can be found as follows:

$$P_{2m}(s) = P(s^2) + s^mQ(s^2), \quad \quad Q_{2m}(s) = P(s^2) + s^mQ'(s^2),$$

$$K_{2m}(s) = K(s^2) + s^mG(s^2), \quad \quad G_{2m}(s) = K(s^2) + s^mG'(s^2);$$

where $s = S_{2m}, Q' = J_m - Q,$ and $G' = J_m - G.$

**Proof.** We know that $P_{2m}, Q_{2m}, K_{2m},$ and $G_{2m}$ are also symmetric circulant and, as in the proof of Theorem 1, that $p_{2m} = p + q,$ $q_{2m} = p + (n - q),$ $k_{2m} = k + g,$ and $g_{2m} = k + (n - g); r_{2m} = 2(p + k)$ are solutions of $(3')$ and $(4')$ for $n = 2m$ whenever $p, q, k,$ and $g$ are solutions of $(3')$ and $(4')$ for $n = m.$ Therefore, it is sufficient to prove that the condition $(2')$ is also satisfied, i.e.

$$(2'') \quad P_{2m}^2 + Q_{2m}^2 + K_{2m}^2 + G_{2m}^2 = 2mI + 2(p + k)J.$$  

The condition $(2'')$ can be checked easily since the process of proof is exactly similar to that of Theorem 1.

Let $\{u_i\}$ and $\{v_i\}$ be two finite sequences respectively of

$$PP^T = \sum_{i=0}^{n-1} u_i S^i \quad \text{and} \quad QQ^T = \sum_{i=0}^{n-1} v_i S^i,$$

where $P, Q$ are $n \times n$ circulant $(0, 1)$-matrices; in this case, we also obtain $w_{n-i} = w_i$ for $w = u$ or $v.$

The following Table I, of all constructible $V_{2n} (1 \leq n \leq 16)$ of type (*) with the restriction $p_\ast \leq q_\ast \leq \frac{1}{2}n,$ is obtained by matching two finite sequences $\{u_i\}$ and
\[ v_i \], respectively of \( PP^T \) and \( QQ^T \), such that \( u_i + v_i = r \) for \( 1 \leq i \leq \frac{1}{3}n \). Here, Theorem 1 serves as a tool of classifying these finite sequences.

Note. 1. \( s = S^k \), where \( k \) is any integer relatively prime to \( n \).
2. When \( q_n = \frac{1}{2}n \), \( Q_n(s) \) and \( Q_n(s) \) produce the same finite sequence.
3. \( * \) indicates the class of \( P_n(s) \) and \( Q_n(s) \) unobtainable by Theorem 1.

It should also be noted that for a given \( n \times n \) circulant matrix \( K(S) \), all matrices \( M(i, j) = S^iK(S^j) \), for any integers \( i \) and \( j \) with \( (n, j) = 1 \), produce the same finite sequence corresponding to \( M(i, j)M^T(i, j) \). Among all \( M(i, j) \) regarded as polynomials in \( S \), there is a polynomial, say \( R \), of least nonnegative degree; we list \( R \) as the representative of all matrices \( M(i, j) \) producing the same finite sequence, as \( R_n(s) \) in the Table I.

In Table I, Classes I and II of \( n = 16 \) are respectively derived from the corresponding classes of \( n = 8 \). Although \( P_n \) and \( Q_n \) of Class II cannot be derived from \( P_8 \) and \( Q_8 \), they produce \( P_{16} \) and \( Q_{16} \) of Class II, by Theorem 1. In this case, \( P_{16} \) and \( Q_{16} \) are interchangeable since \( p = q = 6 \), and we have

\[
\begin{array}{c|c|c}
\hline
n & P_n(s) & Q_n(s) \\
\hline
1 & 0 & 0 \\
\hline
2 & 0 & 1 \\
\hline
4 & & I \\
\hline
8-1 & I + s & I + s + s^8 + s^6 \\
\hline
II & I + s^2 & I + s + s^3 + s^4 \\
\hline
10 & I + s + s^3 & I + s + s^4 + s^6 \\
\hline
16-I & I + s + s^2 + s^3 + s^6 + s^{10} & I + s + s^3 + s^6 + s^8 + s^{12} \\
& I + s + s^2 + s^4 + s^7 + s^9 & I + s + s^3 + s^5 + s^7 + s^{11} \\
\hline
II & I + s + s^2 + s^4 + s^5 + s^{10} & I + s + s^3 + s^7 + s^9 + s^{12} \\
& I + s + s^2 + s^4 + s^6 + s^8 & I + s + s^3 + s^5 + s^7 + s^{11} \\
\hline
III & I + s + s^2 + s^4 + s^6 + s^9 & I + s + s^3 + s^5 + s^7 + s^{11} \\
& I + s^2 + s^3 + s^4 + s^5 + s^{11} & I + s + s^2 + s^6 + s^9 + s^{12} \\
& I + s + s^2 + s^5 + s^7 + s^8 & I + s + s^4 + s^5 + s^9 + s^{10} \\
\hline
\end{array}
\]
\[ P(s, k) = P_a(s^2) + s^k Q_a(s^2) = I + s^2 + s^4 + (I + s^2 + s^5 + s^8), \]
\[ Q(s, k) = P_a(s^2) + s^k Q_a(s^2) = I + s^4 + s^8 + (s^4 + s^{10} + s^{12} + s^{14}). \]

We obtain
\[ P_{14}(s) = I + s + s^2 + s^4 + s^5 + s^{10} = s Q(s, 5) \]
or
\[ = I + s + s^2 + s^4 + s^5 + s^8 = s P(s, -1), \]
since these two polynomials are of distinct type (in the sense of [5]) and of least positive degree in \( s = S \) producing the same finite sequence among all \( P(s, k) \) and \( Q(s, k) \) for this case.

When \( n = 20 \), we obtain two subclasses of matrices \( P \) and \( Q \) by Theorem 1. We have the following cases:

**Subclass-1:**

\[ P(s, k) = P_{10}(s^2) + s^{-k} Q_{10}(s^2) = I + s^2 + s^6 + s^{-k}(I + s^2 + s^8 + s^{12}) \]

and

\[ Q(s, k) = P_{10}(s^2) + s^{-k} Q_{10}(s^2) = I + s^2 + s^6 + s^{-k}(s^4 + s^6 + s^{10} + s^{14} + s^{16} + s^{18}); \]

**Subclass-2:**

\[ P(s, k) = P_{10}(s^2) + s^{-k} Q_{10}(s^2) = I + s^2 + s^6 + s^{-k}(I + s^{-2} + s^{-8} + s^{-12}) \]

and

\[ Q(s, k) = P_{10}(s^2) + s^{-k} Q_{10}(s^2) = I + s^2 + s^6 + s^{-k}(s^4 + s^6 + s^{10} + s^{14} + s^{16} + s^{18}); \]

Each one of the subclasses produces five distinct designs corresponding to \( k = 1, 3, 5, 7, \) and \( 9 \). For example, the finite sequence \( \{u_{2k+1}\} \) of odd components (since the even components \( u_{2i} = r = 2 \) for all \( i \), it is sufficient to consider only odd components of \( \{u_i\} \) corresponding to \( P(S, k) \) are: \( \{u_1, u_3, u_5, u_7, u_9\} = (4, 1, 3, 2, 2), (2, 4, 2, 2, 2), (2, 3, 3, 2, 2), (3, 1, 3, 3, 2), \) and \( (2, 3, 1, 3, 3) \) for Subclass-1 respectively of \( k = 1, 3, 5, 7, \) and \( 9 \); and \( (2, 2, 3, 2, 3), (1, 3, 3, 2, 3), (2, 2, 2, 4, 2), (3, 1, 3, 3, 2), (2, 4, 1, 2, 3) \) for Subclass-2.

The following Table II is obtained by taking \( s = S^k \) with \( k \), an integer relatively prime to \( n = 20 \) for \( P_{20} = P(s, 9) \) of Subclass-2, i.e. \( P_{20}(S^k) = I + S^{2k} + S^{3k} + S^{4k} + S^{9k} + S^{11k} + S^{13k} \).

Starting from \( P = Q = I \) for \( n = 4 \), and repeating applications of Theorem 1, we obtain, for example, the following \( P_n, Q_n \) for \( n = 32 \) and 64:

\[ P_{32} = \sum_{\alpha} s^\alpha, \quad \text{where} \quad \alpha \in \{0, 1, 2, 3, 4, 8, 9, 13, 14, 16, 17, 23\} \]

and

\[ Q_{32} = \sum_{\beta} s^\beta, \quad \text{where} \quad \beta \in \{0, 2, 4, 5, 7, 8, 11, 14, 15, 16, 19, 21, 25, 27, 29, 31\}; \]

\[ P_{64} = \sum_{\alpha} s^\alpha, \quad Q_{64} = \sum_{\beta} s^\beta; \]

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Table II

<table>
<thead>
<tr>
<th>$k$</th>
<th>$(+1, -1)$-matrix $A$ corresponding to $P_{20}$</th>
<th>${u_{21,1}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$+-+-++- -++-+ --++- -++-+-$</td>
<td>$2, 4, 1, 2, 3$</td>
</tr>
<tr>
<td>3</td>
<td>$+-+-++- -++-+ --++- -++-+-$</td>
<td>$2, 2, 1, 3, 4$</td>
</tr>
<tr>
<td>7</td>
<td>$+-+-++- -++-+ --++- -++-+-$</td>
<td>$4, 3, 1, 2, 2$</td>
</tr>
<tr>
<td>9</td>
<td>$+-+-++- -++-+ --++- -++-+-$</td>
<td>$3, 2, 1, 4, 2$</td>
</tr>
</tbody>
</table>

where $\alpha \in \{0, 1, 2, 4, 5, 6, 8, 9, 11, 15, 16, 17, 18, 23, 26, 28, 29, 31, 32, 33, 34, 39, 43, 46, 51, 55, 59, 63\}$ and $\beta \in \{0, 2, 3, 4, 6, 7, 8, 13, 16, 18, 19, 21, 25, 26, 27, 28, 32, 34, 35, 37, 41, 45, 46, 47, 49, 53, 57, 61\}$.

It should be noted that Theorem 3 of Williamson [4] produces Williamson type matrices of the same order, but of different construction, as given by Theorem 2 of this paper. When $n = 29$, we obtain a $W_{4n}$-matrix (see [7]) with submatrices

$$P_{29} = \sum_{\alpha} t_{\alpha}, \quad Q_{29} = \sum_{\beta} t_{\beta}, \quad K_{29} = \sum_{\gamma} t_{\gamma}, \quad G_{29} = \sum_{\delta} t_{\delta},$$

where $t_{\alpha} = S^{k} + S^{29-k}$; $\alpha \in \{2, 3, 5, 6, 8, 12\}$, $\beta \in \{4, 7, 9, 10, 11\}$, $\gamma \in \{3, 4, 5, 8, 9, 11, 13, 14\}$, and $\delta \in \{1, 3, 4, 5, 8, 9, 11\}$. By applying Theorem 2, we obtain $W_{s_{29}}$-matrix with submatrices

$$P_{s_{29}} = \sum_{\alpha} t_{\alpha}, \quad Q_{s_{29}} = \sum_{\beta} t_{\beta}, \quad K_{s_{29}} = \sum_{\gamma} t_{\gamma} \quad \text{and} \quad G_{s_{29}} = \sum_{\delta} t_{\delta},$$

where $t_{\alpha} = S^{k} + S^{s_{29}-k}$ for $k \neq 29$ and $t_{29} = S^{29}$; and $\alpha \in \{4, 6, 7, 9, 10, 11, 12, 15, 16, 21, 24\}$, $\beta \in \{1, 3, 4, 5, 6, 10, 12, 13, 16, 17, 19, 23, 24, 25, 27, 29\}$, $\gamma \in \{6, 7, 8, 10, 11, 13, 16, 18, 19, 21, 22, 23, 26, 27, 28\}$, and $\delta \in \{1, 3, 5, 6, 8, 9, 10, 15, 16, 17, 18, 22, 25, 26, 28, 29\}$.

State University College
Oneonta, New York 13820