A construction for Hadamard matrices

H. Kharaghani

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alta., Canada T1K 3M4

Received 11 March 1991

Abstract


Let $2^m$ be the order of an Hadamard matrix. Using block Golay sequences, a class of Hadamard matrices of order $(r + 4^n + 1)4^n + 1$ is constructed, where $r$ is the length of a Golay sequence.

A matrix $H$ of order $n$ with entries in $\{1, -1\}$ and distinct rows orthogonal is called an Hadamard matrix. For the matrices $A = [a_{ij}]$, $B$, the Kronecker product of $A$, $B$, denoted $A \times B$, is the matrix $[a_{ij}B]$. Let $A = \{a_1, a_2, \ldots, a_n\}$ be a sequence of commuting variables of length $n$. The nonperiodic auto-correlation function of the sequence $A$ is defined by

$$N_A(j) = \sum_{i=1}^{n-j} a_i a_{i+j} \quad j = 1, 2, \ldots, n-1,$$

$$0 \quad j \geq n,$$

Two sequences $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_n\}$ are called Golay sequences of length $n$ if all the entries are $\pm 1$ and $N_A(j) + N_B(j) = 0$ for all $j \geq 1$. Golay sequences exist for orders $2^a10^b26^c$, $a$, $b$, $c$, nonnegative integers. See Turyn [8] and [1] for details.

Turyn [8] used Golay sequences to construct Hadamard matrices of order $4(1+r)$, where $r$ is the length of a Golay sequence. Koukouvinos and Kounias [7] used Golay sequences to construct Hadamard matrices of order $r_1 + r_2$ where $r_1$ and $r_2$ are the lengths of Golay sequences. The author introduced block Golay sequences in [5] and used them to construct Hadamard matrices of order $(r + 4^n + 1)4^n + 1$ for each positive integer $n$, where $r$ is the length of a Golay sequence.

Correspondence to: H. Kharaghani, Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alta., Canada T1K 3M4.
Wallis [9] demonstrated that for a given integer \( q \), there exists an Hadamard matrix \( 2^q \) for every \( s \geq \lfloor 2 \log_2(q - 3) \rfloor \).

In this paper by using block Golay sequences, we construct a class of Hadamard matrices of order \((r + 4^m + 1)4^m \), where \( 2^m \) is the order of an Hadamard matrix and \( r \) is the length of a Golay sequence. This extends our earlier result, provides many new regular complex Hadamard matrices and Hadamard matrices of new order. We begin with our definition of block Golay sequences.

Two sequences \( A = \{A_1, A_2, \ldots, A_n\} \), \( B = \{B_1, B_2, \ldots, B_n\} \), where \( A_i \) and \( B_i \) are commuting symmetric \((1, -1)\)-matrices of order \( m \), are called block Golay sequences of length \( n \) and block size \( m \) if

1. \[ \sum_{i=1}^{n} (A_i^2 + B_i^2) = 2nmI_m \]
2. \[ N_A(j) + N_B(j) = \begin{cases} \sum_{i=1}^{n-j} A_iA_{i+j} + \sum_{i=1}^{n-j} B_iB_{i+j} = 0 & \text{for } j = 1, 2, \ldots, n-1, \\ 0 & \text{for } j > n. \end{cases} \]

Let \( A_1, A_2 \) be two symmetric matrices of the same order. Let

\[
L_2(A_1, A_2) = \begin{pmatrix} A_1 & A_2 \\ A_2 & A_1 \end{pmatrix}.
\]

In general, for symmetric matrices \( A_1, A_2, \ldots, A_{2^n} \) all of the same order, let

\[
L_{2^n}(A_1, A_2, \ldots, A_{2^n}) =
L_2(L_{2^{n-1}}(A_1, A_2, \ldots, A_{2^{n-1}}), L_{2^{n-1}}(A_{2^{n-1}+1}, A_{2^{n-1}+2}, \ldots, A_{2^n})).
\]

We call such matrices \( L \)-matrices. \( L \)-matrices are symmetric and if the entries of two \( L \)-matrices commute, then the \( L \)-matrices commute.

We need the following two lemmas.

**Lemma 1.** For each positive integer \( k \), there are \( 2^k \) \((1, -1)\), \( L \)-matrices, say, \( kD_1, kD_2, \ldots, kD_{2^k} \), all of order \( 2^k \) such that

1. \( kD_l \neq kD_m \), \( l \neq m \),
2. \( \sum_{l=1}^{k} kD_l^2 = 2^{2k} I_{2^k} \)

**Proof.** For \( k = 1 \), let

\[
kD_1 = \begin{pmatrix} + & + \\ + & + \end{pmatrix}, \quad kD_2 = \begin{pmatrix} + & - \\ - & + \end{pmatrix}.
\]

Assuming the existence of \( k-1D_i, 1 \leq i \leq 2^{k-1} \), satisfying (i), (ii), let

\[
kD_i = L_2(k-1D_{i+k-1}D_i), \quad kD_{i+2^{k-1}} = L_2(k-1D_{i+k-1}, -k-1D_i)
\]
for \(i = 1, 2, \ldots, 2^{k-1}\). Using induction hypothesis it is easy to show that \(sD_i\)s satisfy (i), (ii). By induction, the construction is complete. \(\Box\)

For simplicity we will drop the left indices when we apply this lemma.

**Lemma 2** (Kharaghani [4]). Let \(n\) be the order of an Hadamard matrix. Then there are \(n\) symmetric \((1, -1)\)-matrices, say, \(C_1, C_2, \ldots, C_n\) of order \(n\) such that:

(i) \(C_iC_m = 0\) if \(i \neq m\).

(ii) \(\sum_{i=1}^{n} C_i^2 = n^2 I_n\).

For simplicity let \((A_1, A_2, \ldots, A_n)\) denote the back circulant matrix with first row \((A_1, A_2, \ldots, A_n)\). e.g.

\[
(A_1, A_2, A_3) = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_2 & A_3 & A_1 \\ A_3 & A_1 & A_2 \end{pmatrix}
\]

**Theorem 3.** Let \(2^nm\) be the order of an Hadamard matrix. Then there are \(4^nm\) symmetric \((1, -1)\)-matrices, \(F_1, F_2, \ldots, F_{4^nm}\) and a symmetric Hadamard matrix \(H\), all of order \(4^nm^2\) such that:

(i) \(F_iF_m = 0, \ l \neq m\)

(ii) \(\sum_{i=1}^{4^nm} F_i^2 = 4^{2nm^2} l_{4^nm^2}\)

(iii) \(\{H, F_1, F_2, \ldots, F_{4^nm}\}\) is a commuting family of matrices.

**Proof.** Let \(C_1, C_2, \ldots, C_{2^nm}\) be the matrices of Lemma 2. Let \(H_i = (C_{i(-1)m+1}, C_{i(-1)m+2}, \ldots, C_{i(m)}), i = 1, 2, \ldots, 2^n\) be \(2^n\) (symmetric) \((1, -1)\) back circulant matrices (of order \(2^nm^2\)). Then

\[
(*) \quad H_iH_m = 0 \text{ for } l \neq m \text{ and}
\]

\[
(**) \quad \sum_{i=1}^{4^nm} H_i^2 = 4^{n^2m^2} l_{4^nm^2}
\]

by Lemma 2.

Let \(D_i, i = 1, 2, \ldots, 2^n\) be the matrices of Lemma 1. Let \(F_{i+2^n(j-1)} = D_i \times H_j, 1 \leq i \leq 2^n, 1 \leq j \leq 2^n\). Then \(F_is\) are \((1, -1)\)-matrices of order \(4^nm^2\).

Furthermore,

\[
F_{i+2^n(j-1)} = (D_i \times H_j)^l = D_i^l \times H_j = D_i \times H_j = F_{i+2^n(l-1)}
\]

by Lemmas 1, 2. Let \(l \neq m\), then \(F_iF_m = (D_i \times H_j)(D_i \times H_j)\) for some \(i \neq i'\) or \(j \neq j'\). Thus, \(F_iF_m = D_iD_i' \times H_jH_j', 0\), by Lemmas 1, 2.

\[
\sum_{i=1}^{n} F_i^2 = \sum_{j=1}^{2^n} \sum_{i=1}^{2^n} (D_i \times H_j)^2 = \sum_{i=1}^{2^n} D_i^2 \times \sum_{i=1}^{2^n} H_j^2 = 4^n l_{2nm^2} \times 4^n m^2 l_{2nm^2}
\]

\[
= 4^{2nm^2} l_{4^nm^2}
\]

by Lemma 1, and (**)?

It remains to construct the Hadamard matrix \(H\). Let \(H = L_{2^n}(H_1, H_2, \ldots, H_{2^n})\). It is easy to see that \(H\) is a symmetric Hadamard matrix of order \(4^nm^2\). Now \(F_is\) and \(H\) are
$L$-matrices with commuting block entries by $(\ast)$ and thus $\{H, F_1, \ldots, F_{4n}\}$ is a commuting family of matrices. $\Box$

**Example 4.** Let $n = 2$ and $m = 3$ in Theorem 3 and note that there is an Hadamard matrix of order 12, then

\[
D_1 = L_2 \left( \begin{pmatrix} + & + \\ + & + \end{pmatrix}, \begin{pmatrix} + & + \\ + & + \end{pmatrix} \right) = \begin{pmatrix} + & + & + \\ + & + & + \\ + & + & + \end{pmatrix},
\]

\[
D_2 = L_2 \left( \begin{pmatrix} + & + \\ + & + \end{pmatrix}, \begin{pmatrix} + & - \\ - & + \end{pmatrix} \right) = \begin{pmatrix} + & - & + \\ - & + & + \\ + & - & + \end{pmatrix},
\]

\[
D_3 = L_2 \left( \begin{pmatrix} + & + \\ + & + \end{pmatrix}, - \begin{pmatrix} + & + \\ + & + \end{pmatrix} \right) = \begin{pmatrix} + & + & - \\ - & + & + \\ - & + & + \end{pmatrix},
\]

\[
D_4 = L_2 \left( \begin{pmatrix} + & - \\ - & + \end{pmatrix}, - \begin{pmatrix} + & + \\ + & + \end{pmatrix} \right) = \begin{pmatrix} + & - & - \\ - & + & + \\ - & + & + \end{pmatrix},
\]

$H_1 = (C_1, C_2, C_3), \quad H_2 = (C_4, C_5, C_6), \quad H_3 = (C_7, C_8, C_9), \quad H_4 = (C_{10}, C_{11}, C_{12})$,

\[
F_i = \begin{cases} 
D_i \times H_1, & i = 1, 2, 3, 4, \\
D_i \times H_2, & i = 5, 6, 7, 8, \\
D_i \times H_3, & i = 9, 10, 11, 12, \\
D_i \times H_4, & i = 13, 14, 15, 16,
\end{cases}
\]

$H = L_2(\left( H_1, H_2, H_3, H_4 \right)) = L_2 \left( L_2(H_1, H_2), L_2(H_3, H_4) \right) = \begin{pmatrix}
H_1 & H_2 & H_3 & H_4 \\
H_2 & H_1 & H_4 & H_3 \\
H_3 & H_4 & H_1 & H_2 \\
H_4 & H_3 & H_2 & H_1
\end{pmatrix}$
Remark. Note that in the previous example we let $12 = 2^2 \cdot 3$. If we let $12 = 2.6$, then Theorem 3 provides the following matrices:

\[ D_1 = \begin{pmatrix} + & + \\ + & + \end{pmatrix}, \quad D_2 = \begin{pmatrix} + & - \\ - & + \end{pmatrix}, \]

\[ H_1 = (C_1, C_2, C_3, C_4, C_5, C_6), \quad H_2 = (C_7, C_8, C_9, C_{10}, C_{11}, C_{12}), \]

\[ F_1 = D_1 \times H_2 = \begin{pmatrix} H_1 & H_1 \\ H_1 & H_1 \end{pmatrix}, \quad F_2 = D_2 \times H_1 = \begin{pmatrix} H_1 & -H_1 \\ -H_1 & H_1 \end{pmatrix}, \]

\[ F_3 = D_1 \times H_2 = \begin{pmatrix} H_2 & H_2 \\ H_2 & H_2 \end{pmatrix}, \quad F_4 = D_2 \times H_2 = \begin{pmatrix} H_2 & -H_2 \\ -H_2 & H_2 \end{pmatrix}, \]

\[ H = L_2 (H_1, H_2) = \begin{pmatrix} H_1 & H_2 \\ H_2 & H_1 \end{pmatrix}. \]

As a first application, we will construct a huge number of block Golay sequences.

**Theorem 5.** Let $2^m n$ be the order of an Hadamard matrix, then there is a block Golay sequence of length $4^n + 1$ and block size $4^n m^2$.

**Proof.** Let $H, F_1, F_2, \ldots, F_{4^n}$ be the matrices of Theorem 3. Let $A = \{ A_1 = H, A_2 = F_1, \ldots, A_{4^n+1} = F_{4^n}\}$, $B = \{ B_1 = -H, B_2 = F_1, \ldots, B_{4^n+1} = F_{4^n}\}$. Then $N_A(j) + N_B(j) = H F_j - H F_j = 0$. The rest follows from (i), (ii), and (iii) of Theorem 3. \(\square\)

**Example 6.** For $n = 2$ and $m = 3$, we get from Example 4 the following block Golay sequence of length 17 and block size 122.

\[ H F_1 F_2 \cdots F_{16}, -H F_1 F_2 \cdots F_{16}. \]

**Theorem 7.** Let $2^m n$ be the order of an Hadamard matrix. Then there are Hadamard matrices of order $(r + 4^n + 1)4^n m^2$, where $r$ is the length of a Golay sequence.

**Proof.** Let $F, G$ be Golay sequences of length $r$. Let $H$ be the Hadamard matrix of Theorem 3. Let $C = E \times H$ and $D = G \times H$. Then $C, D$ is a block Golay sequence of length $r$ and block size $4^n m^2$. Let $A, B$ be the block Golay sequences of Theorem 5 and let $X = (A, C)$, $Y = (A, -C)$, $Z = (B, D)$, $U = (B, -D)$. Then $(N_A + N_B + N_C + N_D)(j) = 2(N_A + N_B + N_C + N_D)(j) = 0$ for each integer $j \geq 1$.

Now let $X', Y', Z', U'$ be the block circulant matrices whose first rows are $X, Y, Z, U$ respectively. It is easy to see that $X' X'' + Y' Y'' + Z' Z'' + U' U'' = (r + 4^n + 1)4^n m^2 I_{4^n m^2}$ and thus these matrices can be used in a Goethals and Seidel [3] array to construct Hadamard matrices of order $(r + 4^n + 1)4^n m^2$. \(\square\)

**Corollary 8** (Kharaghani [5]). For each positive integer $n$ there is a class of Hadamard matrices of order $(r + 4^n + 1)4^n + 1$, where $r$ is the length of a Golay sequence.
Proof. Let \( m = 1 \) in Theorem 7.

Remark. Let \( n = 2 \) in Corollary 8, then the corollary provides Hadamard matrices of order \( 64(2^2m^2 + 17) \), \( a, b, c \) nonnegative integers. This is a large class of Hadamard matrices which includes many new orders. This shows the power of Theorem 7.

Corollary 9. Let \( 2^m \) be the order of an Hadamard matrix. Then there is a complex Hadamard matrix of order \( (4^m + 1)4^m \) with sum of each row \( 4^m + 2^m \).

Proof. Let \( A, B \) be the block circulant matrices constructed from the Golay sequences of Theorem 5. Let \( R \) be the back identity matrix. Let \( C = \frac{1}{2}(A + BR) + \frac{1}{2}(A - BR) \). Then \( C \) is a complex Hadamard matrix. The sum of each row of \( C \) is \( 4^m + 2^m \).

Hadamard matrices with constant row sums are called regular in [6]. Corollary 9 provides a large class of regular complex Hadamard matrices.

Acknowledgement

The research is supported by NSERC grant 4972.

References