Hadamard Matrices, Finite Sequences, and Polynomials Defined on the Unit Circle

By C. H. Yang

Abstract. If a (*)-type Hadamard matrix of order 2n (i.e. a pair (A, B) of n x n circulant (1, -1) matrices satisfying AA' + BB' = 2nI) exists and a pair of Golay complementary sequences (or equivalently, two-symbol δ-code) of length m exists, then a (*)-type Hadamard matrix of order 2mn also exists. If a Williamson matrix of order 4n (i.e. a quadruple (W, X, Y, Z) of n x n symmetric circulant (1, -1) matrices satisfying W^2 + X^2 + Y^2 + Z^2 = 4nI) exists and a four-symbol δ-code of length m exists, then a Goethals-Seidel matrix of order 4mn (i.e. a quadruple (A, B, C, D) of mn x mn circulant (1, -1) matrices satisfying AA' + BB' + CC' + DD' = 4mnI) also exists. Other related topics are also discussed.

A sequence (c_k) is called a (d, e) sequence if each c_k = d or e. A finite (d, e) sequence C_n = (c_k)_n = (c_1, c_2, ..., c_n) can be associated with a polynomial C_n(z) = \sum_{k=1}^{n} c_kz^{k-1}, where z = exp(ix), x is a real number and i = \sqrt{-1}.

Definition. Two (1,-1) sequences A_n = (a_k)_n and B_n = (b_k)_n are said to be a pair of Golay complementary sequences of length n (abbreviated as GCL(n)), if their associated polynomials A_n(z) and B_n(z) satisfy

(1) \(|A_n(z)|^2 + |B_n(z)|^2 = 2n\) for any complex number z

on the unit circle K = \{z \in C: |z| = 1\} = \{z: z = \exp(ix), 0 \leq x \leq 2\pi\}, where C is the complex field.

Let c(j) = \sum_{k=1}^{n-1} c_kz^{k+j} for a given sequence (c_k)_n. The condition (1) is also equivalent to the following Golay definition of GCL(n) (see [2]),

(2) a(j) + b(j) = 0 \quad \text{for} \quad j \neq 0 \quad \text{(i.e. 1 \leq j \leq n - 1)}.

The above can be proved easily by observing that |C_n(z)|^2 = C_n(z)C_n(z^{-1}) = c(0) + \sum_{k=1}^{n-1} c(k)(z^k + z^{-k}), c(0) = \Sigma c_k^2 = n, and z^k + z^{-k} = 2 \cos kx for z = \exp(ix).

Definition. Two finite (1,-1) sequences A = (a_k)_n and B = (b_k)_n are said to be a pair of Hadamard sequences of length n (abbreviated as HL(n)), if their associated polynomials A(w) and B(w) satisfy

(3) \(|A(w)|^2 + |B(w)|^2 = 2n\) for any w \in K_n,

where K_n = \{w \in C: w^n = 1\} is the set of all n\textsuperscript{th} roots of unity. We shall omit the subscript n of C_n or (c_k)_n from now on if there is no confusion. Let c*(j) = c(j) + c(n - j) = \sum c_kz^{k+j}, where the subscript k + j is congruent modulo n. Then
\(|C(w)|^2 = C(w)C(w^{-1}) = \Sigma_{k=0}^{n-1} c^*(k)w^k\), where \(c^*(0) = n\), consequently the condition (3) is also equivalent to the following

\[ a^*(j) + b^*(j) = 0 \quad \text{for} \ j \neq 0 \quad \text{(i.e.} \ 1 \leq j \leq n/2) \].

We note here that \(c^*(n-j) = c^*(j)\). Since \(K_n \subseteq K\), we obtain

**Lemma 1.** If \((a_k)\) and \((b_k)\) are a pair of \(GCL(n)\), then they are also a pair of \(HL(n)\).

It should be noted that if \(A = (a_k)\) is a \(GCL(n)\) then \(-A = (-a_k) = (-a_1, -a_2, \ldots, -a_n)\) and \(A^r = (a^r_k) = (a_{n-k+1}) = (a_n, \ldots, a_2, a_1)\) are also \(GCL(n)\). Similarly, if \(A = (a_k)\) is an \(HL(n)\), then \(-A, A^r, \) and \(A^{(j)} = (a^{(j)}_k) = (a_k + j) = (a_{j+1}, \ldots, a_n, a_1, \ldots, a_j)\), for \(1 \leq j \leq n - 1\), are also \(HL(n)\). \(GCL(n)\) and \(HL(n)\) exist only if \(n = 1\) or \(n\) is even (see [2], [16], [17]).

When \((a_k)\) and \((b_k)\) are a pair of \(HL(n)\), they can be regarded as the first row entries of \(n \times n\) circulant matrices \(A\) and \(B\), respectively, such that

\[ M = \begin{pmatrix} A & B \\ -B & A^r \end{pmatrix} \]

is a Hadamard matrix of order \(2n\), i.e. \(MM' = 2nI\), since \(AA' + BB' = 2nI_n\), where \('\) indicates the transposed and \(I\) is the identity matrix. (See [16], [17].) Such a Hadamard matrix \(M\) is said to be of (*)-type.

**Definition.** A quadruple \((a_k)_n, (b_k)_n, (c_k)_n, \) and \((d_k)_n\) of \((1, -1)\) sequences is said to be a quad of Goethals-Seidel sequences of length \(n\) (abbreviated as \(GSS(n)\)), if their associated polynomials satisfy

\[ |A(w)|^2 + |B(w)|^2 + |C(w)|^2 + |D(w)|^2 = 4n \quad \text{for any} \ w \in K_n. \]

A sequence of vectors, \((v_k)_n\) is an \(m\)-symbol \(\delta\)-code of length \(n\) if

\[ \sum_{k=1}^{n-j} v_k \cdot v_{k+j} = 0 \quad \text{for each} \ j \neq 0, \]

where \(v_k\) is one of \(m\) orthonormal vectors \(i_1, \ldots, i_m\), or their negatives (see [7]).

**Definition.** A quadruple \((q_k)_n, (r_k)_n, (s_k)_n, \) and \((t_k)_n\) of \((0, \pm 1)\) sequences is said to be a quad of Turyn sequences (abbreviated as \(TS(n)\)) of length \(n\), if the sequence \((v_k)_n\) of vectors \(v_k = (q_k, r_k, s_k, t_k)\) forms a four-symbol \(\delta\)-code, where \(v_k\) is one of orthonormal vectors \((1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), \) and \((0, 0, 0, 1)\), or their negatives.

Let \(Q(z), R(z), S(z), \) and \(T(z)\) be the associated polynomials of a given quad of \(TS(n)\), \((q_k)_n, (r_k)_n, (s_k)_n, \) and \((t_k)_n\). Then we have

\[ |Q(z)|^2 + |R(z)|^2 + |S(z)|^2 + |T(z)|^2 = n \quad \text{for any} \ z \in K. \]

When \((a_k), (b_k), (c_k), \) and \((d_k)\) are a quad of \(GSS(n)\), they can be regarded, respectively, as the first row entries of \(n \times n\) circulant matrices \(A, B, C, \) and \(D\) such that \(AA' + BB' + CC' + DD' = 4nI\). Then a Goethals-Seidel (Hadamard) matrix \(H = (H_{ij}), 1 \leq i, j \leq 4,\) of order \(4n\) can be formed by the sixteen \(n \times n\) matrices \(H_{ij}\).
such that the first, second, third, and fourth rows of \( H \) are, respectively, \((A, BR, CR, DR)\), \((-BR, A, -D'R, C'R)\), \((-CR, D'R, A, -B'R)\), and \((-DR, -C'R, B'R, A)\), where \( R = (r_{ij}), 1 \leq i, j \leq n, \) is the \( n \times n \) symmetric matrix whose entries \( r_{ij} = 1 \) for \( i + j = n + 1 \) and \( r_{ij} = 0, \) otherwise. (See [1], [7].)

**Definition.** A quad of \( \text{GSS}(n) \), \((w_k), (x_k), (y_k), \) and \((z_k)\) is said to be a quad of Williamson sequences (abbreviated as \( \text{WS}(n) \)), if each sequence is symmetric, i.e. \( a_j = a_{n+2-j} \) for each \( j \) and each \((a_k)\) of \( \text{GSS}(n) \), or equivalently \( A(w^{-1}) = A(w) \) for each \( w \in K_n \) and each associated polynomial \( A(w) \) of \( \text{GSS}(n) \).

It is well known that when \((w_k), (x_k), (y_k), \) and \((z_k)\) are a quad of \( \text{WS}(n) \), they can be regarded as the first row entries of \( n \times n \) symmetric circulant matrices \( W, X, Y, \) and \( Z, \) respectively, such that \( W^2 + X^2 + Y^2 + Z^2 = 4nl \). Then a \( 4 \times 4 \) matrix \( H \) is a Williamson (Hadamard) matrix of order \( 4n \), where \((W, X, Y, Z), (-X, W, -Z, Y), (-Y, Z, W, -X), \) and \((-Z, -Y, X, W)\) are, respectively, the first, second, third, and fourth row blocks of \( H \). (See [14], [15], [16].)

The following three theorems (on Hadamard sequences) are derived from the known theorems (on Golay complementary sequences). (See [2], [7], and [10], respectively, for Theorems 2, 3, and 4.)

**Theorem 2.** Let \((a_k)\) and \((b_k)\) be a pair of \( \text{GCL}(m) \) and \((c_k), (d_k)\), a pair of \( \text{HL}(n) \). Then \((e_k)\) and \((f_k)\) is a pair of \( \text{HL}(2mn) \), where

\[
\begin{align*}
    e_{(2j-2)m+k} &= a_k c_j \quad e_{(2j-1)m+k} = b_k d_j \quad \text{and} \quad f_{(2j-2)m+k} = -a_k d_{n+1-j}, \\
    f_{(2j-1)m+k} &= b_k c_{n+1-j} \quad \text{for} \quad 1 \leq k \leq m \quad \text{and} \quad 1 \leq j \leq n.
\end{align*}
\]

**Proof.** Since

\[
E(w) = \sum_{k=1}^{2mn} e_k w^{k-1} = \sum_{j=1}^{n} (c_j w^{(2j-1)m} A(w) + d_j w^{(2j-1)m} B(w))
\]

\[
= A(w) C(w^{2m}) + B(w) D(w^{2m}) w^{m}
\]

and

\[
F(w) = -(A(w) D(w^{-2m}) + B(w) C(w^{-2m}) w^{-2m}) w^{-2m} \quad \text{for any} \quad w \in K_{2mn},
\]

consequently \( w^{2m} \in K_n \), we therefore obtain from (1) and (3),

\[
|E(w)|^2 + |F(w)|^2 = (|A(w)|^2 + |B(w)|^2)(|C(w^{2m})|^2 + |D(w^{2m})|^2) = 4mn.
\]

**Theorem 3.** Let \((a_k), (b_k)\) be a pair of \( \text{GCL}(m) \) and \((c_k), (d_k)\) be a pair of \( \text{HL}(n) \). Then \((e_k), (f_k)\) is a pair of \( \text{HL}(mn) \), where

\[
\begin{align*}
    e_{(j-1)m+k} &= \frac{[(a_k + b_k)c_j + (a_k - b_k)d_j]}{2} \\
    f_{(j-1)m+k} &= \frac{[(a_k - b_k)c_{n+1-j} - (a_k + b_k)d_{n+1-j}]}{2}
\end{align*}
\]

for \( 1 \leq k \leq m \) and \( 1 \leq j \leq n \).
Proof. Since
\[ E(w) = \frac{[A(w) + B(w))C(w^m) + (A(w) - B(w))D(w^m)]}{2} \]
and
\[ F(w) = \frac{[A(w) - B(w))C(w^{-m}) - (A(w) + B(w))D(w^{-m})]}{2} \]
consequently \( w^m \in K_n \), therefore, we have
\[ |E(w)|^2 + |F(w)|^2 = (|A(w)|^2 + |B(w)|^2)(|C(w^m)|^2 + |D(w^m)|^2)/2 = 2mn. \]

It should be noted that if \( (a_k) \) and \( (b_k) \) are a pair of \( GCL(m) \), then the sequence \( (v_k) \) of vectors \( v_k = \left(\frac{a_k + b_k}{2}, \frac{a_k - b_k}{2}\right) \), is a two-symbol \( \delta \)-code of length \( m \) with the two orthonormal vectors \( i_1 = (1,0) \) and \( i_2 = (0,1) \), and conversely.

**Theorem 4.** Let \( (a_k) \) and \( (b_k) \) be a pair of \( HL(n) \). Then \( (a_k^e), (b_k^e); (a_k^o), (b_k^o); (a_k^e), (b_k^o); \) and \( (a_k^o), (b_k^e) \) are also pairs of \( HL(n) \), where \( (c_k^e) \) is the sequence obtained from \( (c_k) \) by changing the sign of \( c_k \) if and only if the subscript \( k \) is even, i.e. \( c_k^e = (-1)^{k-1}c_k \), and \( c_k^o = (-1)^kc_k \) for \( c_k = a_k \) or \( b_k \).

Proof. Let \( A(w) = A_0(w^2) + wA_e(w^2) \) and \( B(w) = B_0(w^2) + wB_e(w^2) \) be, respectively, associated polynomials of \( (a_k) \) and \( (b_k) \). Then \( A^e(w) = A_0(w^2) - wA_e(w^2) \), \( B^e(w) = B_0(w^2) - wB_e(w^2) \), \( A^o(w) = -A_0(w^2) + wA_e(w^2) \), and \( B^o(w) = -B_0(w^2) + wB_e(w^2) \) are, respectively, associated polynomials of \( (a_k^e), (b_k^e), (a_k^o), \) and \( (b_k^o) \). Since
\[ |A(w)|^2 + |B(w)|^2 = |A_0(w^2) + wA_e(w^2)|^2 + |B_0(w^2) + wB_e(w^2)|^2 = 2n \]
for any \( w \in K_n \), which is equivalent to \[ |A_0(w^2)|^2 + |A_e(w^2)|^2 + |B_0(w^2)|^2 + |B_e(w^2)|^2 = 2n \]
and
\[ w(A_0(w^{-2})A_e(w^2) + B_0(w^{-2})B_e(w^2)) \]
\[ + w^{-1}(A_0(w^2)A_e(w^{-2}) + B_0(w^2)B_e(w^{-2})) = 0 \]
for any \( w \in K_n \).* Consequently, we have
\[ |A^e(w)|^2 + |B^e(w)|^2 = |A_0(w^2) - wA_e(w^2)|^2 + |B_0(w^2) - wB_e(w^2)|^2 \]
\[ = |A_0(w^2)|^2 + |A_e(w^2)|^2 + |B_0(w^2)|^2 + |B_e(w^2)|^2 = 2n. \]
Other cases can be proved similarly.

**Theorem 5.** Let \( (w_k), (x_k), (y_k), \) and \( (z_k) \) be a quad of \( WS(m) \) and \( (q_k), (r_k), (s_k), \) and \( (t_k) \) a quad of \( TS(n) \). Then \( (a_k), (b_k), (c_k), \) and \( (d_k) \) are a quad of \( GSS(mn) \), where
\[
\begin{align*}
a_{(h-1)n+j} &= w_hq_j + x_hr_j + y_hs_j + z_ht_j, \\
b_{(h-1)n+j} &= x_hq_j - w_hr_j + z_hs_j - y_ht_j, \\
c_{(h-1)n+j} &= y_hq_j - z_hr_j - w_hs_j + x_ht_j, \\
d_{(h-1)n+j} &= z_hq_j + y_hr_j - x_hs_j - w_ht_j \quad \text{for} \quad 1 \leq h \leq m \text{ and } 1 \leq j \leq n.
\end{align*}
\]

*We use the fact that \( w \in K_n \) implies \( -w \in K_n \) for even \( n \).
Proof. For any \( w \in K_{m^n} \), we have
\[
A(w) = \sum_{k=1}^{m^n} a_k w_k^{-1} = \sum_{j=1}^{n} \sum_{i=1}^{m} (w_n q_j + x_n r_j + y_n s_j + z_n t_{j}) w_i^{(n-1)i+1}
\]
\[
= \sum_{j=1}^{n} \sum_{i=1}^{m} (w_n q_j + x_n r_j + y_n s_j + z_n t_{j}) w_i^{(n-1)i+1}
\]
similarly,
\[
B(w) = \sum_{j=1}^{n} \sum_{i=1}^{m} (w_n q_j + x_n r_j + y_n s_j + z_n t_{j}) w_i^{(n-1)i+1}
\]
\[
C(w) = \sum_{j=1}^{n} \sum_{i=1}^{m} (w_n q_j + x_n r_j + y_n s_j + z_n t_{j}) w_i^{(n-1)i+1}
\]
and
\[
D(w) = \sum_{j=1}^{n} \sum_{i=1}^{m} (w_n q_j + x_n r_j + y_n s_j + z_n t_{j}) w_i^{(n-1)i+1}
\]
Since \( w^n \in K_m \) and \( U(w^{-n}) = U(w^n) \) for \( U = W, X, Y, \) and \( Z \), by replacing the right-hand sides of the above into the following sum and by rearrangements and simplifications, we obtain from (5) and (7),
\[
|A(w)|^2 + |B(w)|^2 + |C(w)|^2 + |D(w)|^2 = (W^2 + X^2 + Y^2 + Z^2)(|Q|^2 + |R|^2 + |S|^2 + |T|^2) = 4mn,
\]
where \( U = U(w^n) \) for \( U = W, X, Y, \) and \( Z; P = P(w) \) for \( P = Q, R, S, \) and \( T \).

It should be noted that a Hadamard matrix of order \( 4mn \) has been constructed by Turyn [7] using Baumert-Hall units if a Williamson matrix of order \( 4m \) and a four-symbol \( \delta \)-code of length \( n \) are known. Williamson matrices of order \( 4m \) exist for \( m \leq 31 \) or \( m = (q + 1)/2 \), where \( q \) (a prime power) \( \equiv 1 \) (mod 4), and others (see [4], [7], [8], [11], [13], [14], [15]).

Four-symbol \( \delta \)-codes (including two- and three-symbol codes) of length \( n \) exist for \( n \leq 61 \), or \( n = 2^a 10^b 26^c \) (two-symbol codes) and \( n = 2^a 10^b 26^c + 1 \) (three-symbol codes) for all \( a, b, c \geq 0 \) (see [7], [9], [11]), as well as for \( n = 2^a 10^b 26^c + 2^d 10^e 26^f \) (four-symbol codes) for all \( a, b, c, d, e, f \geq 0 \).

For example, in the two-symbol \( \delta \)-code \((1, i)\) of length 2, by letting \( 1 = (1, 0, 0, 0) \) and \( i = (0, 1, 0, 0) \), we obtain a quad of \( TS(2) \): \((q_k, r_k, s_k, t_k) = (1, 0, 0, 0)\). Similarly, by letting \( 1 = (0, 0, 1, 0) \) and \( j = (0, 0, 1, 0) \) in the three-symbol code \((1, i, j)\) of length 3, we obtain a quad of \( TS(3) \): \((q_k, r_k, s_k, t_k) = (0, 0, 1, 0)\). Thus, for the given quad of \( WS(3) \): \((w_k, x_k, y_k, z_k) = (1, 0, 0, 0)\), we obtain from Theorem 5 the following quads of \( GSS(n) \) for \( n = 6 \) and \( 9 \).
\[
\begin{align*}
n = 6: & \{a_k, b_k, c_k, d_k\} \text{ are, respectively, } (1, 1, 0, 0, 0, 0), (1, 0, 0, 0, 0, 0), (0, 0, 0, 1, 1, 1), \text{ and } (1, 1, 0, 0, 0, 0) \text{ for } n = 6. \\
n = 9: & \{a_k, b_k, c_k, d_k\} \text{ are, respectively, } (1, 1, 0, 0, 0, 0, 0, 0, 0), (1, 0, 0, 0, 0, 0, 0, 1, 1), \text{ and } (0, 0, 0, 1, 1, 1, 1, 1, 1) \text{ for } n = 9. 
\end{align*}
\]

The following new pairs \((a_k, b_k)\) of \( HL(26) \) have been found, which are listed as the following pairs of \( C \) and \( D \), respectively, where \( C = \{k: a_k = -1\} \) and \( D = \{k: b_k = -1\} \). \( C \) and \( D \) are: \{1, 2, 3, 7, 9, 11, 12, 14, 15, 17, 18\} and \{1, 2, 4, 8, 9, 11, 13, 16, 17, 21\}; \{1, 2, 3, 5, 6, 8, 12, 13, 15, 21\} and \{1, 2, 4, 5, 7, 11, 12, 13, 16, 19, 24\}; \{1, 2, 4, 6, 8, 9, 12, 13, 15, 22\} and \{1, 2, 3, 4, 8, 9, 13, 16, 17, 19, 25\}; and \{1, 2, 3, 5, 6, 10, 12, 13, 15, 23\} and \{1, 2, 3, 7, 9, 10, 12, 13, 16,
21, 23}, respectively. From Theorem 4, we also obtain the following pair corresponding to \((a^0_k)\) and \((b^0_k)\) of the first pair above, \{2, 5, 12, 13, 14, 18, 19, 21, 23, 25\} and \{2, 3, 4, 5, 7, 8, 15, 16, 19, 23, 25\}. Other pairs of HL(26) corresponding to \((a^0_k)\) and \((b^0_k)\), or \((a^0_k)\) and \((b^0_k)\), can be obtained from Theorem 4 in a similar way. We note here that \((c^0_k) = (-c^0_k)\) for \(c_k = a_k\) or \(b_k\).

In Theorem 3, for example, from the given pairs of GCL(10) and HL(4): \((a_k) = (1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, -1)\), \((b_k) = (1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1)\), and \((c_k) = (d_k) = \(-1, 1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1)\), we obtain the following \(E\) and \(F\) representing the pair \((e_k)\) and \((f_k)\) of HL(40):

\[
E = \{k: e_k = -1\} = \{1, 2, 3, 4, 6, 7, 10, 15, 18, 19, 25, 28, 29, 35, 38, 39\}
\]

and

\[
F = \{k: f_k = -1\} = \{1, 3, 5, 6, 7, 8, 11, 13, 15, 16, 17, 18, 21, 23, 25, 26, 27, 28, 32, 34, 39, 40\}.
\]

Department of Mathematical Sciences
State University of New York, College at Oneonta
Oneonta, New York 13820

4. E. SPENCE, "Hadamard matrices of order \(2q^2(q + 1)\) and \(q^2(q + 1)\)," Notices Amer. Math. Soc., v. 23, 1976, p. A-353.