MATHEMATICS OF COMPUTATION, VOLUME 33, NUMBER 146
APRIL 1979, PAGES 688–693

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 $n \times n$ 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 $n \times n$ 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 $mn \times mn$ 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 $C_n = (c_k)_n = (c_1, c_2, \ldots, c_n)$ can be associated with a polynomial $C_n(z) = \Sigma_1^n c_k z^{k-1}$, 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

$$(1) \qquad |A_n(z)|^2 + |B_n(z)|^2 = 2n \quad \text{for any complex number } z$$

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

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

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

The above can be proved easily by observing that $|C_n(z)|^2 = C_n(z)C_n(z^{-1}) = c(0) + \Sigma_1^{n-1} c(k)(z^k + z^{-k})$, $c(0) = \Sigma c_k^2 = n$, 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

$$(3) \qquad |A(w)|^2 + |B(w)|^2 = 2n \quad \text{for any } w \in K_n,$$

where $K_n = \{w \in \mathbf{C}: w^n = 1\}$ is the set of all nth 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 $c^*(j) = c(j) + c(n-j) = \Sigma_1^n c_k c_{k+j}$, where the subscript $k + j$ is congruent modulo n. Then

Received August 30, 1976.
AMS (MOS) subject classifications (1970). Primary 05B20, 05A19, 62K05.

$|C(w)|^2 = C(w)C(w^{-1}) = \Sigma_0^{n-1} c^*(k)w^k$, where $c^*(0) = n$, consequently the condition (3) is also equivalent to the following

$$(4) \qquad a^*(j) + b^*(j) = 0 \quad \text{for } j \neq 0 \text{ (i.e. } 1 \leqslant j \leqslant n/2).$$

We note here that $c^*(n-j) = c^*(j)$. Since $K_n \subset K$, 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 $A^r = (a_k^r) = (a_{n-k+1}) = (a_n, \ldots, a_2, a_1)$ are also GCL(n). Similarly, if $A = (a_k)$ is an HL(n), then $-A$, A^r, and $A^{(j)} = (a_k^{(j)}) = (a_{k+j}) = (a_{j+1}, \ldots, a_n, a_1, \ldots, a_j)$, for $1 \leqslant j \leqslant n-1$, 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

$$M = \begin{pmatrix} A & B \\ -B' & A' \end{pmatrix}$$

is an 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

$$(5) \qquad |A(w)|^2 + |B(w)|^2 + |C(w)|^2 + |D(w)|^2 = 4n \quad \text{for any } w \in K_n.$$

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

$$(6) \qquad \sum_{k=1}^{n-j} v_k \cdot v_{k+j} = 0 \quad \text{for each } j \neq 0,$$

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

Definition. A quadruple (q_k), (r_k), (s_k), and (t_k) 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 δ-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), (r_k), (s_k), and (t_k). Then we have

$$(7) \qquad |Q(z)|^2 + |R(z)|^2 + |S(z)|^2 + |T(z)|^2 = n \quad \text{for any } z \in K.$$

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 $H = (H_{ij})$, $1 \leqslant i, j \leqslant 4$, 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 $R = (r_{ij})$, $1 \leqslant i, j \leqslant n$, 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 GSS(n), (w_k), (x_k), (y_k), and (z_k) is said to be a quad of Williamson sequences (abbreviated as WS(n)), if each sequence is symmetric, i.e. $a_j = a_{n+2-j}$ for each j and each (a_k) of GSS(n), or equivalently $A(w^{-1}) = A(w)$ for each $w \in K_n$ and each associated polynomial $A(w)$ of GSS(n).

It is well known that when (w_k), (x_k), (y_k), and (z_k) are a quad of 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 $W^2 + X^2 + Y^2 + Z^2 = 4nI$. Then a 4×4 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* GCL(m) *and (c_k), (d_k), a pair of* HL(n). *Then (e_k) and (f_k) is a pair of* HL($2mn$), *where*

$$e_{(2j-2)m+k} = a_k c_j, \quad e_{(2j-1)m+k} = b_k d_j \quad \text{and} \quad f_{(2j-2)m+k} = -a_k d_{n+1-j},$$
$$f_{(2j-1)m+k} = b_k c_{n+1-j} \quad \text{for } 1 \leqslant k \leqslant m \text{ and } 1 \leqslant j \leqslant n.$$

Proof. Since

$$E(w) = \sum_1^{2mn} e_k w^{k-1} = \sum_1^{n} (c_j w^{2(j-1)m} A(w) + d_j w^{(2j-1)m} B(w))$$
$$= A(w)C(w^{2m}) + B(w)D(w^{2m})w^m$$

and

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

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* GCL(m) *and (c_k), (d_k) be a pair of* HL(n). *Then (e_k), (f_k) is a pair of* HL(mn), *where*

$$e_{(j-1)m+k} = [(a_k + b_k)c_j + (a_k - b_k)d_j]/2$$

and

$$f_{(j-1)m+k} = [(a_k - b_k)c_{n+1-j} - (a_k + b_k)d_{n+1-j}]/2$$
$$\text{for } 1 \leqslant k \leqslant m \text{ and } 1 \leqslant j \leqslant n.$$

Proof. Since

$$E(w) = [(A(w) + B(w))C(w^m) + (A(w) - B(w))D(w^m)]/2$$

and

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

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 $v_k = (x_k, y_k)$, where $x_k = (a_k + b_k)/2$ and $y_k = (a_k - b_k)/2$, is a two-symbol δ-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^e), (b_k^0); (a_k^0), (b_k^e); and (a_k^0), (b_k^0) 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 $c_k^0 = (-1)^k c_k$ 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 $A^e(w) = A_0(w^2) - wA_e(w^2)$, $B^e(w) = B_0(w^2) - wB_e(w^2)$, $A^0(w) = -A_0(w^2) + wA_e(w^2)$, and $B^0(w) = -B_0(w^2) + wB_e(w^2)$ are, respectively, associated polynomials of (a_k^e), (b_k^e), (a_k^0), and (b_k^0). 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

$$\begin{aligned} |A^e(w)|^2 + |B^e(w)|^2 &= |A_0(w^2) - wA_e(w^2)|^2 + |B_0(w^2) - wB_e(w^2)|^2 \\ &= |A_0(w^2)|^2 + |A_e(w^2)|^2 + |B_0(w^2)|^2 + |B_e(w^2)|^2 = 2n. \end{aligned}$$

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*

$$\begin{aligned} a_{(h-1)n+j} &= w_h q_j + x_h r_j + y_h s_j + z_h t_j, \\ b_{(h-1)n+j} &= x_h q_j - w_h r_j + z_h s_j - y_h t_j, \\ c_{(h-1)n+j} &= y_h q_j - z_h r_j - w_h s_j + x_h t_j, \\ d_{(h-1)n+j} &= z_h q_j + y_h r_j - x_h s_j - w_h t_j \quad \text{for } 1 \leqslant h \leqslant m \text{ and } 1 \leqslant j \leqslant n. \end{aligned}$$

*We use the fact that $w \in K_n$ implies $-w \in K_n$ for even n.

Proof. For any $w \in K_{mn}$, we have

$$A(w) = \sum_{1}^{mn} a_k w^{k-1} = \sum_{1}^{m}\sum_{1}^{n} (w_h q_j + x_h r_j + y_h s_j + z_h t_j) w^{(h-1)n+j-1}$$

$$= W(w^n)Q(w) + X(w^n)R(w) + Y(w^n)S(w) + Z(w^n)T(w),$$

similarly,

$$B(w) = X(w^n)Q(w) - W(w^n)R(w) + Z(w^n)S(w) - Y(w^n)T(w),$$

$$C(w) = Y(w^n)Q(w) - Z(w^n)R(w) - W(w^n)S(w) + X(w^n)T(w),$$

and

$$D(w) = Z(w^n)Q(w) + Y(w^n)R(w) - X(w^n)S(w) - W(w^n)T(w).$$

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 δ-code of length n are known. Williamson matrices of order $4m$ exist for $m \leqslant 31$ or $m = (q + 1)/2$, where q (a prime power) $\equiv 1 \pmod 4$, and others (see [4], [7], [8], [11], [13], [14], [15]).

Four-symbol δ-codes (including two- and three-symbol codes) of length n exist for $n \leqslant 61$, 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 $a, b, c \geqslant 0$ (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 $a, b, c, d, e,$ and $f \geqslant 0$.

For example, in the two-symbol δ-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): $(q_k) = (1, 0)$, $(r_k) = (0, 1)$, and $(s_k) = (t_k) = (0, 0)$. Similarly, by letting 1 and i as above and $j = (0, 0, 1, 0)$ in the three-symbol code $(1, i, j)$ of length 3, we obtain a quad of TS(3): $(q_k) = (1, 0, 0)$, $(r_k) = (0, 1, 0)$, $(s_k) = (0, 0, 1)$, and $(t_k) = (0, 0, 0)$. Thus, for the given quad of WS(3): $(w_k) = (x_k) = (y_k) = (-, 1, 1)$ and $(z_k) = (1, 1, 1)$, where $-$ stands for -1, we obtain from Theorem 5 the following quads of GSS(n) for $n = 6$ and 9. $n = 6$: (a_k), (b_k), (c_k), and (d_k) are, respectively, $(-, -, 1, 1, 1, 1)$, $(-, 1, 1, -, 1, -)$, $(-, -, 1, -, 1, -)$, and $(1, -, 1, 1, 1, 1)$; $n = 9$: $(-, -, -, 1, 1, 1, 1, 1, 1)$, $(-, 1, 1, 1, -, 1, 1, -, 1)$, $(-, -, 1, 1, -, -, 1, -, -)$, and $(1, -, 1, 1, 1, -, 1, 1, -)$.

The following new pairs (a_k) and (b_k) of HL(26) have been found, which are listed as the following pairs of C and D, respectively, where $C = \{k\colon a_k = -1\}$ and $D = \{k\colon b_k = -1\}$. 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 $\{1, 2, 3, 5, 7, 11, 12, 13, 16, 19, 24\}$; $\{1, 2, 4, 6, 8, 9, 12, 13, 15, 22\}$ 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_k^0) and (b_k^0) 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_k^0) and (b_k^0), or (a_k^e) and (b_k^e), can be obtained from Theorem 4 in a similar way. We note here that $(c_k^e) = (-c_k^0)$ for $c_k = a_k$ or b_k.

In Theorem 3, for example, from the given pairs of GCL(10) and HL(4): $(a_k) = (1, 1, 1, 1, -, 1, 1, -, -, 1)$, $(b_k) = (1, -, 1, -, 1, 1, 1, 1, -, -)$ and $(c_k) = (d_k) = (-, 1, 1, 1)$, 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

1. J. M. GOETHALS & J. J. SEIDEL, "A skew Hadamard matrix of order 36," *J. Austral. Math. Soc.*, v. 11, 1970, pp. 343–344.

2. M. J. E. GOLAY, "Complementary series," *IRE Trans. Information Theory*, v. IT-7, 1961, pp. 82–87.

3. M. J. E. GOLAY, "Note on complementary series," *Proc. IRE*, v. 50, 1962, p. 84.

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

5. E. SPENCE, "Hadamard matrices of the Goethals-Seidel type," *Canad. J. Math.*, v. 27, 1975, pp. 555–560.

6. E. SPENCE, "Skew-Hadamard matrices of order $2(q + 1)$," *Notices Amer. Math. Soc.*, v. 22, 1975, p. A-303.

7. R. J. TURYN, "Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings," *J. Combinatorial Theory Ser. A*, v. 16, 1974, pp. 313–333.

8. R. J. TURYN, "An infinite class of Williamson matrices," *J. Combinatorial Theory Ser. A*, v. 12, 1972, pp. 319–321.

9. R. J. TURYN, "Computation of certain Hadamard matrices," *Notices Amer. Math. Soc.*, v. 20, 1973, p. A-1.

10. Y. TAKI et al., "Even-shift orthogonal sequences," *IEEE Trans. Information Theory*, v. IT-15, 1969, pp. 295–300.

11. J. S. WALLIS, "On Hadamard matrices," *J. Combinatorial Theory Ser. A*, v. 18, 1975, pp. 149–164.

12. A. L. WHITEMAN, "Skew Hadamard matrices of Goethals-Seidel type," *Discrete Math.*, v. 2, 1972, pp. 397–405.

13. A. L. WHITEMAN, "Williamson type matrices of order $2q(q + 1)$," *Notices Amer. Math. Soc.*, v. 21, 1974, p. A-623.

14. A. L. WHITEMAN, "An infinite family of Hadamard matrices of Williamson type," *J. Combinatorial Theory Ser. A*, v. 14, 1973, pp. 334–340.

15. J. WILLIAMSON, "Hadamard's determinant theorem and sum of four squares," *Duke Math. J.*, v. 11, 1944, pp. 65–81.

16. C. H. YANG, "On Hadamard matrices constructible by circulant submatrices," *Math. Comp.*, v. 25, 1971, pp. 181–186.

17. C. H. YANG, "Maximal binary matrices and sum of two squares," *Math. Comp.*, v. 30, 1976, pp. 148–153.