MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 133
JANUARY 1976, PAGES 148–153

Maximal Binary Matrices and Sum of Two Squares

By C. H. Yang

Abstract. A maximal $(+1, -1)$-matrix of order 66 is constructed by a method of matching two finite sequences. This method also produced many new designs for maximal $(+1, -1)$-matrices of order 42 and new designs for a family of H-matrices of order 26.2^n. A nonexistence proof for a $(*)$-type H-matrix of order 36, consequently for Golay complementary sequences of length 18, is also given.

Let M be a $2n \times 2n$ $(+1, -1)$-matrix, then the absolute value of det M is equal to or less than μ_{2n}, where $\mu_{2n} = (2n)^n$, if n is even; and $\mu_{2n} = 2^n(2n-1)(n-1)^{n-1}$, if n is odd (see [1], [2] and their references).

When n is even and the absolute value of det M is equal to μ_{2n}, then the matrix M is called a nontrivial Hadamard matrix or H-matrix. Another characterization of an H-matrix M of order m is that it satisfies $MM^T = mI_m$, where I_m is the $m \times m$ identity matrix, T indicates the transposed matrix. (m must be equal to 1, 2, or $4n$.)

A sufficient condition for $(+1, -1)$-matrix M of order $2n$ being maximal is that the following condition holds:

$$MM^T = \begin{bmatrix} P_n & 0 \\ 0 & P_n \end{bmatrix}, \tag{1}$$

where $P_n = 2nI_n$, when n is even (i.e. when M is an H-matrix); and $P_n = (2n-2)I_n + 2J_n$, when n is odd, J_n is the $n \times n$ matrix whose every entry is 1.

When n is odd, such maximal $(+1, -1)$-matrices M_{2n} satisfying the condition (1) have been known for $1 \leqslant n \leqslant 31$, except $n = 11$, 17, and 29 (see [1], [2], and [4]). Such maximal matrices M_{2n} can be constructed by the following standard form:

$$M_{2n} = \begin{bmatrix} A & B \\ -B^T & A^T \end{bmatrix}, \tag{$*$}$$

where A and B are $n \times n$ circulant matrices with entries 1 or -1.

For maximal matrices M_{2n} of type $(*)$, the condition (1) is equivalent to

$$AA^T + BB^T = P_n. \tag{2}$$

Let (a_k) and (b_k), $0 \leqslant k \leqslant n-1$, be, respectively, the first row entries of matrices A and B, then the condition (2) is also equivalent to each of the following conditions (3) and (4) (see [4], [5]).

Received February 25, 1974; revised March 18, 1974 and February 25, 1975.
AMS (MOS) subject classifications (1970). Primary 05B20, 05A19, 62K05.

(3) $$|A(w)|^2 + |B(w)|^2 = P_n(w),$$

where $A(w) = \Sigma_{k=0}^{n-1} a_k w^k$, $B(w) = \Sigma_{k=0}^{n-1} b_k w^k$, w is any nth root of unity; and a_k, b_k are either 1 or -1. $P_n(w) = 2n$, for even n; and $P_n(w) = 2(n + \Sigma_{k=1}^{n-1} w^k)$, for odd n.

(4) $$|C(s)|^2 + |D(s)|^2 = [n/2],$$

where $C(s) = \Sigma_{k=0}^{n-1} c_k s^k$, $D(s) = \Sigma_{k=0}^{n-1} d_k s^k$, s is any nontrivial nth root of unity (i.e. $s \neq 1$), $c_k = 1$ whenever $a_k = 1$, and $c_k = 0$ whenever $a_k = -1$, d_k is similarly defined by b_k, and $[r]$ means the integral part of r.

Let $|C(s)|^2 = \Sigma_{k=0}^{n-1} p_k s^k$, $|D(s)|^2 = \Sigma_{k=0}^{n-1} q_k s^k$. Then

(5) $$|C(s)|^2 + |D(s)|^2 = \sum_{k=0}^{n-1} (p_k + q_k) s^k.$$

Consequently, the right-hand side of (5) is equal to $[n/2]$, if $p_k + q_k = r_n$, for each k, $1 \leqslant k \leqslant [n/2]$, where $r_n = (p^2 + q^2 - p - q)/(n-1)$, $p = p_0$ and $q = q_0$ are, respectively, the number of $+1$'s in each row of matrices A and B.

The following maximal matrices M_{2n} with the corresponding $C(s)$ and $D(s)$ have been obtained for $n = 21$, 33, and 26, by matching two finite sequences (p_k) and (q_k) such that $p_k + q_k = r_n$, for each k, $1 \leqslant k \leqslant [n/2]$. Let $C(s) = \Sigma_k s^k$, $k \in C$, and $D(s) = \Sigma_k s^k$, $k \in D$; $s^n = 1$, where s is a nontrivial nth root of unity. Then we have the following C and D in Table I for $n = 21$.

TABLE I

C	D
0, 1, 3, 6, 8, 12	0, 1, 2, 3, 4, 8, 11, 12, 16, 18
0, 1, 2, 4, 11, 17	0, 1, 2, 3, 6, 8, 10, 11, 15, 18
0, 1, 4, 10, 15, 17	0, 1, 2, 3, 4, 5, 9, 11, 14, 17
0, 1, 5, 10, 13, 15	0, 1, 2, 3, 4, 5, 8, 11, 15, 17 or 0, 1, 2, 3, 4, 6, 7, 10, 14, 16
0, 1, 3, 7, 10, 15 or 0, 1, 4, 7, 14, 16	0, 1, 2, 3, 4, 6, 8, 11, 12, 16
0, 1, 4, 8, 14, 16	0, 1, 2, 3, 4, 6, 7, 11, 13, 16
0, 1, 4, 8, 10, 16	0, 1, 2, 3, 4, 6, 7, 11, 14, 16

For example, $(+1, -1)$ matrices A, corresponding to $C(s)$ with $C = \{0, 1, 3, 6, 8, 12\}$, can be obtained for $s = w^k$, $w = \exp(2\pi i/21)$, if k is relatively prime to 21. These matrices A are listed in Table II, where $+$ stands for $+1$ and $-$ for -1.

TABLE II

k	First row of $(+1, -1)$-matrix A
1	++−+− −+−+− −−+−− −−−−− −
2	+−++− −+−−− −−+−− −+−−− −
4	+−−++ −+−−− −++−− −−−−− −
5	+−−−− +−−−+ −−−−− +−−++ −
8	++−+− −+−+− −−+−− −−−−− −
10	+−−−− −−−−+ +−−−− +−++− −

For $n = 33$, we have $C = \{0, 1, 2, 3, 7, 8, 11, 13, 15, 18, 27, 30\}$ and $D = \{0, 1, 2, 3, 5, 8, 12, 15, 16, 17, 21, 25, 27\}$.

When n is even, M_{2n} is an H-matrix and for $n = 26$, we have $C = \{0, 1, 2, 5, 7, 8, 11, 16, 19, 21\}$ and $D = \{0, 1, 2, 3, 4, 5, 9, 12, 16, 18, 22\}$. By applying Theorem 1 of [5] once, we obtain $(*)$-type H-matrices of order 104, i.e. for $n = 52$, we have $C = \{0, 1, 2, 3, 4, 5, 7, 9, 10, 11, 14, 16, 19, 22, 25, 32, 33, 37, 38, 42, 45\}$ and $D = \{0, 2, 4, 10, 13, 14, 15, 16, 17, 21, 22, 23, 27, 29, 31, 32, 35, 38, 39, 41, 42, 43, 47, 49, 51\}$; or $C = \{0, 1, 2, 4, 9, 10, 14, 16, 17, 21, 22, 29, 32, 35, 38, 42, 43, 45, 47, 49, 51\}$ and $D = \{0, 2, 3, 4, 5, 7, 10, 11, 13, 14, 15, 16, 19, 22, 23, 25, 27, 31, 32, 33, 37, 38, 39, 41, 42\}$. By applying the above theorem n times, we obtain $(*)$-type H-matrices of order 52.2^n.

Other $(*)$-type H-matrices M_{52} with the corresponding C and D are found as follows:

$$C = \{0, 1, 2, 3, 4, 7, 10, 15, 17, 21\}, \quad D = \{0, 1, 2, 4, 6, 7, 10, 11, 15, 18, 20\};$$

or

$$C = \{0, 1, 2, 3, 4, 7, 9, 12, 16, 20\}, \quad D = \{0, 1, 2, 4, 6, 12, 13, 17, 18, 20, 23\};$$

or

$$C = \{0, 1, 2, 3, 5, 8, 12, 13, 16, 22\}, \quad D = \{0, 1, 3, 4, 6, 8, 10, 12, 13, 18, 19\}.$$

A complex H-matrix of order n is an $n \times n$ matrix γ whose entries are ± 1 or $\pm i$ such that $\gamma\bar{\gamma}^T = nI_n$, where $\bar{\gamma}$ is the complex conjugate of γ. It should be noted that existence of a $(*)$-type H-matrix of order $2n$ with symmetric circulant $n \times n$ submatrices A and B implies existence of a complex symmetric circulant $n \times n$ H-matrix $\gamma = \alpha + i\beta$, where $\alpha = (A + B)/2$ and $\beta = (A - B)/2$. Consequently, no $(*)$-type H-matrices of order $2n$ with symmetric submatrices A and B exist when $n = 2p^m$ or $n = 2^k$ for $k > 4$, where p is an odd prime; m and k positive integers (see Theorem 1 of [3]).

Also we have

THEOREM. *No $(*)$-type H-matrix of order* 36 *exists regardless of symmetry in submatrices A and B.*

Suppose on the contrary such a $(*)$-type H-matrix exists. Let $C(s) = C_0(s^2) + sC_1(s^2)$ and $D(s) = D_0(s^2) + sD_1(s^2)$ be the corresponding polynomials of the H-matrix satisfying the condition (4). Then $-s$ is also an 18th root of unity and $C(-s) = C_0(s^2) - sC_1(s^2)$ and $D(-s) = D_0(s^2) - sD_1(s^2)$.

Since $|B(s)|^2 = B(s)B(s^{-1})$ and $|B(-s)|^2 = B(-s)B(-s^{-1})$ for $B(s) = C(s)$ or $D(s)$, we have for $s \neq \pm 1$,

$$18 = |C(s)|^2 + |D(s)|^2 + |C(-s)|^2 + |D(-s)|^2$$
$$= 2(|C_0(t)|^2 + |C_1(t)|^2 + |D_0(t)|^2 + |D_1(t)|^2),$$

where $t = s^2$, a nontrivial 9th root of unity. Consequently, we have

(6) $$|C_0(t)|^2 + |C_1(t)|^2 + |D_0(t)|^2 + |D_1(t)|^2 = 9.$$

By setting $s = -1$ in (4), we have

(7) $$C(-1)^2 + D(-1)^2 = 9.$$

Since $C(-1) = C_0(1) - C_1(1)$ and $D(-1) = D_0(1) - D_1(1)$ are integers, without loss of generality, we can assume that $C(-1)^2 = 0$ and $D(-1)^2 = 9$, from the condition (7). Consequently, $C_0(t)$ and $C_1(t)$ must each have three nonvanishing terms in t, and one of $D_k(t)$ must have three terms in t and the other $D_j(t)$ six terms, where $k = 0$ or $1, j \neq k$. And $D_j'(t) = -D_j(t) = \Sigma_0^8 t^k - D_j(t)$ must have three terms in t.

When $t = \mathrm{w}^k$, $\mathrm{w} = \exp(2\pi i/3)$, $k = 1$ or 2: $|B_k(\mathrm{w})|$, where $B = C$ or D, $k = 1$ or 0, can only take the value 0, $\sqrt{3}$, or 3. This is because $B_k(\mathrm{w})$ is of the form: $1 + \mathrm{w} + \mathrm{w}^2$, or $\pm(2 + \mathrm{w}^n)\mathrm{w}^m$, where $n, m = 0, 1$, or 2 and only $D_j(\mathrm{w}) = -D_j'(\mathrm{w})$ has $-$ sign.

There are only two possibilities for $|B_k(\mathrm{w})|$'s to satisfy the condition (6): *Case* 1, three of them must be equal to $\sqrt{3}$ and the other one 0; or *Case* 2, one of them must be 3 and the other three 0.

For Case 1, without loss of generality, let $|C_k(\mathrm{w})| = 0$, then $|C(\mathrm{w})| = |C_j(\mathrm{w}^2)| = |D_h(\mathrm{w})| = \sqrt{3}$, where $k = 0$ or 1; $j \neq k$; and $j, h = 0$ or 1. Also,

$$|D(\mathrm{w})| = |D_0(\mathrm{w}^2) + \mathrm{w}D_1(\mathrm{w}^2)|$$
$$= |\mp(2 + \mathrm{w}^{2k})\mathrm{w}^{2h} \pm \mathrm{w}(2 + \mathrm{w}^{2m})\mathrm{w}^{2n}| = |2 + \mathrm{w}^{2k} - (2 + \mathrm{w}^{2m})\mathrm{w}^{2q+1}|,$$

where $k, m = 1$ or 2; $h, n = 0, 1$, or 2; and $q = n - h$, can only take the value 0, $\sqrt{3}$, or 3.* This is because $2 + \mathrm{w}^{2k} - (2 + \mathrm{w}^{2m})\mathrm{w}^{2q+1}$ can be reduced to 0 or $\pm(2 + \mathrm{w}^n)\mathrm{w}^m$, where $n, m = 0, 1$, or 2.* Consequently, the condition (4) cannot be satisfied. When $|D_h(\mathrm{w})| = 0$, $|D(\mathrm{w})| = |D_m(\mathrm{w}^2)| = |C_n(\mathrm{w})| = \sqrt{3}$, where $h = 0$ or 1; $h \neq m$; and $m, n = 0$ or 1. Also, $|C(\mathrm{w})| = |C_0(\mathrm{w}^2) + \mathrm{w}C_1(\mathrm{w}^2)| = |2 + \mathrm{w}^{2k} + (2 + \mathrm{w}^{2m})\mathrm{w}^{2q+1}|$ can only take the value 0, $\sqrt{3}$ or 3. Therefore, the condition (4) cannot be satisfied.

For Case 2, without loss of generality, let $|C_k(\mathrm{w})| = 3$ then $|C_j(\mathrm{w})| = |D_h(\mathrm{w})| = 0$, where $k = 0$ or 1; $j \neq k$; and $j, h = 0$ or 1. Consequently, for $t \neq \mathrm{w}^r$ $(r = 0, 1$, or 2) $C_k(t)$ must be of the form $t^n(1 + t^3 + t^6)$ and the other three of the form $\pm t^m u(t^q)$, where $u(t) = 1 + t + t^2$, $q \not\equiv 3 \pmod 9$.

For nonnegative integers a, b, c, such that $a + b + c = 3$,

*Excluding the case $|D(\mathrm{w})| > 3$.

$$a|u(t)|^2 + b|u(t^2)|^2 + c|u(t^4)|^2 \tag{8}$$
$$= 3(a + b + c) + (2a + c)t_1 + (2b + a)t_2 + (2c + b)t_4,$$

where $t_k = t^k + t^{-k}$, the condition (8) holds for any t, a 9th root of unity which is not a 3rd root of unity. From now on let t be such a 9th root of unity, i.e. $t \neq \mathbf{w}^k$.

Since there are only three distinct $|u(t^r)|$'s for $r \not\equiv 3 \pmod 9$, i.e. $|u(t)|$, $|u(t^2)|$, and $|u(t^4)|$, from the conditions (6) and (8), one of $|C_j(t)|$ and $|D_h(t)|$ must be equal to $|u(t)|$ and the other two $|u(t^2)|$ and $|u(t^4)|$. Let $|C_j(t)| = |u(t)|$; then $|C(t)| = |C_j(t^2)| = |u(t^2)|$ and $|D(t)| = |D_0(t^2) + tD_1(t^2)| = |u(t^{2n}) - t^k u(t^{2m})|$, where $n \neq m$; $n, m = \pm 2$ or ± 4; k an integer $\pmod 9$. Consequently, we have

$$|C(t)|^2 + |D(t)|^2 = 9 - P(n, m, k; t), \tag{9}$$

where

$$P(n, m, k; t) = t^k u(t^{2m})u(t^{-2n}) + t^{-k}u(t^{-2m})u(t^{2n})$$
$$= \sum_\alpha t_\alpha, \quad \alpha \in \{k, k - 2n, k - 4n, k + 2m, k + 4m, k + 2(m - n),$$
$$k + 4(m - n), k + 2m - 4n, k + 4m - 2n\}.$$

By using identities $P(n, m, k; t) = P(m, n, -k; t) = P(-m, -n, k; t) = P(-n, -m, -k; t)$ and performing computations and simplifications, $P(n, m, k; t)$ is found to take the value $t_2 - t_4, t_4 - t_1, 3 + t_1 - t_2, -3 + t_2 - t_4$, or $2(t_4 - t_2)$ for $n \neq m$; $n, m = \pm 2$ or ± 4; $0 \leqslant k \leqslant 8$. Thus, the condition (4) cannot be satisfied since $P(n, m, k; t) \neq 0$ for t, any primitive 9th root of unity. Similarly, when $|D_h(\mathbf{w})| = 3$, we obtain $|C(t)|^2 + |D(t)|^2 = 9 + P(n, m, k; t)$. Consequently, the condition (4) cannot be satisfied; and hence, no such $(*)$-type H-matrix of order 36 exists.

Since existence of Golay complementary sequences $(a_k), (b_k)$, $0 \leqslant k \leqslant n - 1$, of length n (see [6]) implies existence of a $(*)$-type H-matrix of order $2n$ with the corresponding $A(w) = \Sigma a_k w^k$ and $B(w) = \Sigma b_k w^k$ satisfying the condition (3), nonexistence of Golay complementary sequences of length 18 is derived from nonexistence of a $(*)$-type H-matrix of order 36.

Acknowledgment. I wish to thank the referee for comments and recommendations concerning nonexistence proof of a $(*)$-type H-matrix of order 36 and references to Golay complementary sequences.

Department of Mathematics
SUNY, College at Oneonta
Oneonta, New York 13820

1. H. EHLICH, "Determinantenabschätzungen für binäre Matrizen," *Math. Z.*, v. 83, 1964, pp. 123–132. MR **28** #4003.

2. J. BRENNER & L. CUMMINGS, "The Hadamard maximum determinant problem," *Amer. Math. Monthly*, v. 79, 1972, pp. 626–630. MR **46** #190.

3. R. J. TURYN, "Complex Hadamard matrices," in *Combinatorial Structures and Their Applications* (Proc. Calgary Internat. Conf., Calgary, Alta., 1969), Gordon and Breach, New York, 1970, pp. 435–437. MR **42** #5821.

4. C. H. YANG, "On designs of maximal (+1, −1)-matrices of order $n \equiv 2 \pmod 4$. II," *Math. Comp.*, v. 23, 1969, pp. 201–205.

5. C. H. YANG, "On Hadamard matrices constructible by circulant submatrices," *Math. Comp.*, v. 25, 1971, pp. 181–186. MR **44** #5235.

6. M. J. E. GOLAY, "Complementary series," *IRE Trans. Information Theory*, v. IT-7, 1961, pp. 82–87. MR **23** #A3096.

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

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

9. S. JAUREGUI, JR., "Complementary sequences of length 26," *IRE Trans. Information Theory*, v. IT-8, 1962, p. 323.