On Designs of Maximal (+1, -1) -Matrices of Order $n \equiv 2 \pmod{4}$

By C. H. Yang

When $n \equiv 2 \pmod{4}$, it is known that the absolute value α_n of the determinant of n th order (+1, -1)-matrices satisfies the following inequalities:

$$\alpha_n^2 \leq 4(n-1)^2(n-2)^{n-2} = \mu_n \quad (\text{see [1]})$$

and

$$\alpha_n = \mu_n^{1/2}, \quad \text{for } n \leq 54, \quad \text{except } n = 22, 34 \quad (\text{see [1], [2] and [3]}).$$

Let M_n be a maximal (+1, -1)-matrix of order $n \equiv 2 \pmod{4}$. Then such a maximal matrix M_n can be constructed by the following standard form:

$$M_n = \begin{pmatrix} A & B \\ -B^T & A^T \end{pmatrix},$$

where A, B are circulant matrices of order $n/2$. T indicates the transposed matrix. In this case, the gramian matrix $G(M_n)$ of M_n has the following form:

$$G(M_n) = M_n M_n^T = \begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix},$$

where

$$P = AA^T + BB^T = \begin{pmatrix} n & & 2 \\ & \ddots & \\ 2 & & n \end{pmatrix}.$$

More precisely, we have

$$G(A) = AA^T = (a_{ij}), \quad G(B) = BB^T = (b_{ij}),$$

$1 \leq i, j \leq n/2$; where $a_{ij} = b_{ij} = n/2$, for $1 \leq i \leq n/2$, and $a_{ij} + b_{ij} = 2$ for $i \neq j$. Since A, B are circulant (+1, -1)-matrices, it can be shown easily that $G(A), G(B)$ are not only circulant but also symmetric, namely, $a_{ij} = a_{|i-j|}$ and $b_{ij} = b_{|i-j|}$. It follows that construction of M_n is reduced to finding two finite sequences $\{a_k\}$ and $\{b_k\}$, $1 \leq k \leq (n-2)/4$, such that $a_k + b_k = 2$.

Let $C = (c_{ij})$ be an m th order circulant (+1, -1)-matrix, then $G(C) = G(C^T) = G(C_{pq})$, where $C_{pq} = (c_{kl})$, $k \equiv p + i$, $l \equiv q + j \pmod{m}$ for fixed integers p and q . Consequently, the finite sequences of C, C^T and C_{pq} are identical; therefore, matrices C, C^T and C_{pq} are regarded as of the same type.

In the following table, all M_n , constructible by all distinct types of A and B with the restriction that $N(A) \leq N(B) < n/4$, where $N(C)$ means the number of -1's in each row of C , are listed for $n \leq 38$.

The following methods and theorems are helpful for constructions of M_n .

Let $S = (s_{ij})$ be the m th order circulant matrix such that

Received April 3, 1967.

$$s_{ij} = 1, \text{ if } j - i \equiv 1 \pmod{m}, \\ = 0, \text{ otherwise.}$$

Then the m th order circulant matrices C, D whose first row vectors are respectively $U = (u_1, \dots, u_m), V = (v_1, \dots, v_m)$ can be represented as

$$C = \sum_{k=1}^m u_k S^{k-1} \quad \text{and} \quad D = \sum_{k=1}^m v_k S^{k-1}$$

where $S^0 = I =$ the m th order identity matrix.

THEOREM 1. *Let*

$$M = \begin{pmatrix} C & D \\ -D^T & C^T \end{pmatrix},$$

then the gramian matrix $G(M)$ becomes

$$(1) \quad G(M) = MM^T = \begin{pmatrix} G & 0 \\ 0 & G \end{pmatrix},$$

where $G = (g_{ij}) = CC^T + DD^T$. And

$$(2) \quad g_{ij} = c_{ij} + d_{ij} = c_k + d_k = g_k = g_{m-k},$$

if $k = |i - j|$, where $(c_{ij}) = CC^T, (d_{ij}) = DD^T; c_{ij} = c_k = c_{m-k}$ and $d_{ij} = d_k = d_{m-k}$, if $k = |i - j|$.

THEOREM 2. *Let p and q be respectively the number of 1's in the first row vectors U, V of C and D when u_k, v_k are 0 or 1. Then*

$$(3) \quad \sum_{k=1}^{m-1} c_k = p(p-1) \quad \text{and} \quad \sum_{k=1}^{m-1} d_k = q(q-1).$$

And

$$(4) \quad c_k + d_k = r, \quad \text{for } 1 \leq k \leq m-1,$$

implies

$$(5) \quad r(m-1) = p(p-1) + q(q-1).$$

THEOREM 3. *Let A and B be the matrices obtained by substituting -1 's for 1 's and 1 's for 0 's in C and D respectively. Then the elements g_k of G become*

$$(6) \quad g_k = 2m, \quad \text{if } k = 0, \\ = 2m - 4(p + q - c_k - d_k), \quad \text{otherwise.}$$

And

$$(7) \quad g_k = 2, \quad \text{for } 1 \leq k \leq \frac{1}{2}(m-1),$$

if and only if

$$(8) \quad p + q - r = \frac{1}{2}(m-1).$$

Sketch of the proofs for Theorems 1, 2, and 3. Since the i th row vector and j th column vector of C can be expressed as US^{i-1} and $(US^{j-1})^T$, respectively, we have

The first row of A or B

n	$\{a_k\}$ or $\{b_k\}$					
6	3	-1	+++			
			-++			
10	1	1	-++			
	1	1	-++			
14	3	3	-++			
	-1	-1	-++			
18	5	1	-++			
	-3	1	-++			
	1	5	-++			
	1	-3	-++			
	1	1	-++			
	1	1	-++			
26	1	1	-++			
	1	1	-++			
	1	1	-++			
	5	1	-++			
	-3	1	-++			
	1	5	-++			
	1	-3	-++			
30	3	3	-++			
	-1	-1	-++			
	3	3	-++			
	-1	-1	-++			
	3	3	-++			
	-1	-1	-++			
	3	3	-++			
	-1	-1	-++			

$3, -1, 3, 3, 3, 3, 3$ $-1, 3, -1, -1, -1, -1$	$--++--$ $--++--$ $--++--$	$+++-$ $+++-$ $+++-$	$+++-$ $+++-$ $+++-$	$+++-$ $+++-$ $+++-$
$-1, 3, 3, 3, 3, 3$ $3, -1, -1, -1, -1, -1$	$-+--++$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, -1, 3, 3, 3, 7, -1$ $-1, 3, -1, -1, -1, -5, 3$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$-1, 3, 7, -1, 3, 3, 3$ $3, -1, -5, 3, -1, -1, -1$	$-+--++$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, 3, 3, 3, 3, -1, -1, 3, -1, 3$ $-1, -1, -1, -1, -1, 3, 3, -1, 3$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, 3, 3, -1, 3, -1, 3, -1, 3$ $-1, -1, -1, 3, -1, 3, -1, 3, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, 3, 3, -1, 3, -1, 3, 3, -1$ $-1, -1, -1, 3, -1, 3, -1, -1, 3$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, 3, -1, 3, -1, -1, 3, 3, -1$ $-1, -1, 3, -1, -1, 3, 3, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, 3, -1, 3, -1, -1, 3, 3, 3$ $-1, -1, 3, -1, 3, -1, -1, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, -1, 3, 3, -1, 3, 3, 3, -1$ $-1, 3, -1, -1, 3, -1, -1, 3$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, -1, -1, 3, -1, 3, 3, 3, 3$ $-1, 3, -1, -1, 3, -1, -1, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, -1, -1, 3, -1, 3, 3, 3, 3$ $-1, 3, -1, -1, 3, -1, -1, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, -1, -1, 3, -1, 3, 3, 3, 3$ $-1, 3, -1, -1, 3, -1, -1, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, -1, -1, 3, -1, 3, 3, 3, 3$ $-1, 3, -1, -1, 3, -1, -1, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$
$3, -1, -1, 3, -1, 3, 3, 3, 3$ $-1, 3, -1, -1, 3, -1, -1, -1$	$--++--$ $--++--$ $--++--$	$-++-$ $-++-$ $-++-$	$-++-$ $-++-$ $-++-$	$+++-$ $+++-$ $+++-$

[illegible]

$$\begin{aligned}
c_{ij} &= (US^{i-1})(US^{j-1})^T = (US^{i-1})(S^{j-1})^T U^T \\
&= US^{i-1} S^{m-j+1} U^T \quad [\cdots (S^k)^T = S^{m-k}] \\
&= (US^{m+i-j}) U^T = c_{(m+i-j+1)1}, \quad \text{if } j > i, \\
&= (US^{i-j}) U^T = c_{(i-j+1)1}, \quad \text{if } i \geq j \quad [\cdots S^m = I] \\
&= U(US^{j-1})^T = c_{1(j-i+1)}, \quad \text{if } j \geq i.
\end{aligned}$$

Since the gramian matrix is symmetric, i.e., $c_{ij} = c_{ji}$, by defining $c_k \equiv c_{1(k+1)} = c_{(k+1)1}$, we have

$$\begin{aligned}
c_k &= c_{|i-j|} = c_{1(j-i+1)} = c_{ij} \\
&= c_{(m+i-j+1)1} = c_{|m-(j-i)|} = c_{m-k}, \quad \text{if } k = |i-j|.
\end{aligned}$$

Similarly we have $d_k = d_{|i-j|} = d_{ij} = d_{m-k}$ if $k = |i-j|$.

The equalities (3) can be proved by mathematical induction. When $p = 1$, obviously they are true. Assuming that they are true for $p = N < m$, we have $\sum_{k=1}^{m-1} c_k = N(N-1)$ and N 1's in U . Without loss of generality, let us assume $u_j = 0$. Then by replacing $u_j = 0$ by $u_j = 1$ in U , which corresponds to $p = N+1$, we observe that $2(m-1)$ terms $u_j u_k, u_k u_j$ ($k \neq j, 1 \leq k \leq m$), in $\sum_{k=1}^{m-1} c_k = \sum_{k=1}^{m-1} U(US^k)^T = \sum_{k=1}^{m-1} \sum_{l=1}^m u_i u_l$ [$l \equiv i-k \pmod{m}$], may be affected by this change. Among these $2(m-1)$ terms, exactly $2N$ terms change the value from 0 to 1, for there are N 1's among u_k ($k \neq j, 1 \leq k \leq m$). Therefore, $\sum_{k=1}^{m-1} c_k = N(N-1) + 2N = (N+1)N$, thus they are also true for $p = N+1$.

For proof of Theorem 3, let $AA^T = (a_{ij})$ and $a_k = a_{|i-j|} = a_{ij}$, if $k = |i-j|$. Since $a_k = U(US^k)^T = \sum_{l=1}^m u_i u_l$ [$l \equiv i-k \pmod{m}$], by observing that there are $c_k, 2(p-c_k)$, and $m-c_k-2(p-c_k)$ terms of $u_i u_l$ respectively with $u_i = u_l = -1, u_i = -u_l = 1$ (or -1), and $u_i = u_l = 1$, we have $a_k = m - 4(p-c_k)$, for $1 \leq k \leq m-1$. Similarly, $b_k = m - 4(q-d_k)$, where $b_k = b_{|i-j|} = b_{ij}$, if $k = |i-j|$ and $(b_{ij}) = BB^T$. Consequently, we have

$$g_k = a_k + b_k = 2m - 4(p+q-c_k-d_k), \quad \text{for } 1 \leq k \leq m-1.$$

The equality (8) can be derived easily from (3), (5), (6), and (7).

From (5) and (8), and for a given m and preassigned r , solutions for p and q can be obtained. When $m = 11, 17, \dots$, there is no solution for p and q . (See [1] and the table of [2].) For constructions of M_n , it is noticed that finding two sequences $\{c_k\}$ and $\{d_k\}$ satisfying (4) is usually easier than finding two sequences $\{a_k\}$ and $\{b_k\}$ satisfying (7).

4 Gunnison Park Boulevard
Oneonta, New York

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

2. C. H. YANG, "Some designs for maximal $(+1, -1)$ -determinant of order $n = 2 \pmod{4}$," *Math. Comp.*, v. 20, 1966, pp. 147-148. MR 32 #5534.

3. C. H. YANG, "A construction for maximal $(+1, -1)$ -matrix of order 54," *Bull. Amer. Math. Soc.*, v. 72, 1966, p. 293. MR 32 #5678.