A GENERALIZATION OF A THEOREM OF BOOLEAN RELATION MATRICES

CHONG-YUN CHAO*), Pittsburgh, and SHMUEL WINograd, New York

(Received July 21, 1975)

The purpose of this note is to prove a theorem concerning Boolean relation matrices which is a generalization of a theorem in [2] and [1]. Let \( B = \{0, 1\} \) with the usual Boolean addition and multiplication. The matrices which we consider here are \( n \times n \) (Boolean relation) matrices over \( B \) with the usual matrix addition and multiplication. A \( n \times n \) matrix \( A \) is said to be primitive if there is a positive integer \( k \) such that \( A^k = J \) where \( J \) is the \( n \times n \) matrix with every entry being 1. Let \( A = (a_{ij}) \) and \( C = (c_{ij}) \) be two \( n \times n \) matrices over \( B \), we shall write \( A \preceq C \) if \( a_{ij} = 1 \) implies \( c_{ij} = 1 \). Let \( P \) be the following \( n \times n \) permutation matrix:

\[
P = \begin{bmatrix}
0 & 0 & 0 & \ldots & 0 & 1 \\
1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & 0 & \ldots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & 0
\end{bmatrix},
\]

(1)

then \( P^n \) is the identity matrix \( I \), and any \( n \times n \) circulant (Boolean relation) matrix over \( B \) is in the form

\[
a_0 I + a_1 P + a_2 P^2 + \ldots + a_{n-1} P^{n-1}.
\]

(2)

Omitting those \( a_i \)'s which are zeros, and defining \( P^0 = I \), the circulant matrix can be written as

\[
P^{i_1} + P^{i_2} + \ldots + P^{i_k}
\]

(3)

where \( 0 \leq i_1 < i_2 < \ldots < i_k \leq n - 1 \). The following was proved in [2] and [1]:

**Theorem.** The circulant Boolean relation matrix (3) is primitive if and only if

\[
\text{g.c.d.} \ (i_1 - i_1, i_2 - i_1, i_3 - i_1, \ldots, i_k - i_1, n) = 1.
\]

*) This work was done while the author was a visitor at the IBM Watson Research Center.
It is well known that the \( n \times n \) circulants are closely related to the polynomial \( x^n - 1 \), e.g., the algebra of \( n \times n \) circulants over a field \( F \) is isomorphic to the algebra, \( F[x]/\langle x^n - 1 \rangle \), of polynomials modulo \( x^n - 1 \) over \( F \). The companion matrix for the polynomial \( x^n - 1 \) is \( P \). It leads us to define

\[
C = \begin{bmatrix}
0 & 0 & 0 & \ldots & 0 & b_0 \\
1 & 0 & 0 & \ldots & 0 & b_1 \\
0 & 1 & 0 & \ldots & 0 & b_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & b_{n-1}
\end{bmatrix}
\]

as the (Boolean relation) companion matrix for the polynomial \( f(x) = x^n - b_{n-1}x^{n-1} - b_{n-2}x^{n-2} - \ldots - b_1x - b_0 \), where \( b_i \in \{0, 1\} \) for \( i = 0, 1, \ldots, n - 1 \). We will assume from now on that \( b_i \in \{0, 1\} \) for \( i = 0, 1, \ldots, n - 1 \). Omitting those \( b_i \)'s which are 0, we will write \( x^n = g(x) = x^{j_1} + x^{j_2} + \ldots + x^{j_t} \), where \( 0 \leq j_1 < j_2 < \ldots < j_t \leq n - 1 \), instead of \( f(x) = 0 \).

We will consider (Boolean relation) matrices of the form

\[
A = a_0 C^0 + a_1 C^1 + a_2 C^2 + \ldots + a_{n-1} C^{n-1}
\]

where \( a_i \in B, i = 0, 1, \ldots, n - 1 \), and \( A \neq I \). Omitting those \( a_i \)'s which are 0, we have

\[
A = C^{i_1} + C^{i_2} + \ldots + C^{i_k}
\]

where \( 0 \leq i_1 < i_2 < \ldots < i_k \leq n - 1 \), and \( i_k > 0 \).

**Theorem.** Let \( C \) be as in (4) and \( A \) as in (6). Then \( A \) is primitive if and only if

1) \( j_1 = 0 \), and
2) \( \gcd(i_1 - i_1, i_2 - i_1, \ldots, i_k - i_1, j_1, j_2, \ldots, j_t, n) = 1 \).

The first condition of the theorem is obvious, for if \( j_1 > 0 \) (i.e., \( b_0 = 0 \)), then all the entries in the first row of \( C^l \) are 0 for all \( l > 0 \). So we will assume \( j_1 = 0 \).

In order to prove the rest of the theorem we need the following lemmas.

**Lemma 1.** Let \( C \) be as in (4), then

\[ C^n = g(C) = C^{j_1} + C^{j_2} + \ldots + C^{j_t}. \]

**Proof.** Consider the polynomial \( f(x) = x^n - x^{j_1} - x^{j_2} - \ldots - x^{j_t} \), over the reals \( \mathbb{R} \), and let \( \bar{C} \) be its companion matrix. Then, by Cayley-Hamilton's theorem, we have

\[ C^n = \bar{C}^{j_1} + \bar{C}^{j_2} + \ldots + \bar{C}^{j_t}. \]
Let \( \chi \) be the map from the set of all non-negative numbers \( \mathbb{R}^+ \) into \( B \) defined by
\[
\chi(x) = \begin{cases} 
0 & \text{if } x = 0, \\
1 & \text{if } x > 0,
\end{cases}
\]
then \( \chi \) can be extended to a map from the set of all \( n \times n \) matrices \( M_n(\mathbb{R}^+) \) over \( \mathbb{R}^+ \) to the set \( M_n(B) \) of all \( n \times n \) matrices over \( B \). Moreover, if \( U, V \in M_n(\mathbb{R}^+) \) then
\[
\chi(UV) = \chi(U) \chi(V) \quad \text{and} \quad \chi(U + V) = \chi(U) + \chi(V).
\]
Consequently, \( C^n = (\chi(C))^n = \chi(C^n) = \sum_{i=1}^t C^{ji} = \sum_{i=1}^t (\chi(C))^{ji} = \sum_{i=1}^t C^{ji} = g(C) \).

**Lemma 2.** Let \( A \) be as in (6). Then \( A \) is primitive if and only if there is a positive integer \( m \) such that \( A^m \geq C^q \) for all \( q = 0, 1, \ldots, n - 1 \).

**Proof.** If \( A \) is primitive then there exist \( m \) such that \( A^m = J \geq C^q \) for all \( q = 0, 1, \ldots, n - 1 \). Conversely, if \( A^m \geq C^q \) for all \( q = 0, 1, \ldots, n - 1 \), then, since \( C \geq P \), it follows that \( A^m \geq \sum_{i=0}^{n-1} P^i = J \).

**Lemma 3.** Let \( A \) be as in (6) with \( i_1 = 0 \), \( a = \text{g.c.d.} \left(i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_l, n\right) \) and
\[
J_a = C^0 + C^a + C^{2a} + \ldots + C^{\left(n-1\right)a}.
\]
Then there exists a positive integer \( m_0 \) such that \( A^m = J_a \) for all \( m \geq m_0 \).

**Proof.** Since \( A = C^{i_1} + C^{i_2} + \ldots + C^{i_k} \) where \( 0 = i_1 < i_2 < \ldots < i_k \leq n - 1 \) and \( i_k > 0 \), \( A \geq I \) and \( A^t \geq I \) for all positive integers \( l \).

Let \( l \) be any positive integer and \( A^t = C^{l_1} + C^{l_2} + \ldots + C^{l_p} \) where \( 0 = l_1 < l_2 < \ldots < l_p \). Since each \( l_q \) is in the form
\[
\sum_{s=2}^{k} r_s i_s + \sum_{\beta=2}^{t} s_{\beta} j_{\beta} + vn
\]
for some integers \( r_s, s_{\beta} \) and \( v \), each \( l_q \) is divisible by \( a \) for \( q = 1, 2, \ldots, p \). Consequently, \( J_a \geq C^{l_q} \) for \( q = 1, 2, \ldots, p \), and \( J_a \geq A^t \) for any positive integer \( l \).

Since \( a \) is the g.c.d., there exist integers \( r_2, r_3, \ldots, r_k \) and \( s_2, s_3, \ldots, s_t \) and \( v \) such that
\[
a = \sum_{s=2}^{k} r_s i_s + \sum_{\beta=2}^{t} s_{\beta} j_{\beta} - vn,
\]
i.e.,
\[
\sum_{s=2}^{k} r_s i_s = a - \sum_{\beta=2}^{t} s_{\beta} j_{\beta} + vn
\]
where \( v \) is positive, and where, without loss of generality, we can assume that each of \( r_s \) and \( s_{\beta} \) is non-negative, for otherwise, we can replace each \( r_s \) by \( r_s + w_s n \),
each $s_\beta$ by $s_\beta + w_\beta n$, and $v$ by $v + \sum_{\alpha=2}^{k} w_\alpha' \lambda_\alpha + \sum_{\beta=2}^{t} w_\beta' f_\beta$. Also, we may assume that

$$v = \sum_{\beta=2}^{t} s_\beta + v'$$

where $v'n \geq \sum_{\beta=2}^{t} s_\beta f_\beta$, for if not, in (8), after we replace $r_2$ by $r_2 + wn$ and $v$ by $v + w_2$, we choose $w$ so that $v + w_2 = \sum_{\alpha=2}^{k} s_\alpha + v'$ and $v'n \geq \sum_{\beta=2}^{t} s_\beta f_\beta$.

Let $h_0 = \sum_{\alpha=2}^{k} \rho_\alpha$. Then, by using (8) and Lemma 1, we have

$$A^{h_0} = A^{\sum_{\alpha=2}^{k} \rho_\alpha} \geq A^{\sum_{\alpha=2}^{k} \rho_\alpha i_\alpha} = A^{\sum_{\alpha=2}^{k} \rho_\alpha} \cdot C^{n} = A^{\rho_\alpha} \cdot C^{n} \cdot C^{v'n} = A^{\rho_\alpha} \cdot C^{n} \cdot C^{v'n} = A^{\rho_\alpha} \cdot C^{n} \cdot C^{v'n} = A^{\rho_\alpha} \cdot C^{n} \cdot C^{v'n} \geq A^{\rho_\alpha}.$$

Hence, $A^{h_0} \geq A^a$. Since $A^l \geq I$ for all positive integer $l$, $A^{h_0} \geq I + A^a$. Now we can choose $m_0 = h_0 \cdot (n/a)$, and we have $A^{m_0} = A^{h_0(n/a)} \geq (I + A^a)^{(n/a)} \geq J_a$. Hence, $A^m = J_a$ for all $m \geq m_0$.

Now the proof of our Theorem: We consider the cases of $k = 1$ and $k > 1$.

For the case of $k = 1$, $A$ can be written as

$$A = C^{i_1}(C^{i_1-i_1} + C^{i_2-i_1} + \ldots + C^{i_k-i_1}).$$

Let $a = \text{g.c.d.} (i_1 - i_1, i_2 - i_1, \ldots, i_k - i_1, j_2, \ldots, j_n)$. Then, by Lemma 3, we have $A^m = C^{i_1m} J_a$ for sufficiently large $m$. By Lemma 2, $A$ is primitive if and only if $a = 1$.

For the case $k = 1$. Let $a = \text{g.c.d.} (i_1 - i_1, j_1, j_2, \ldots, j_n) = \text{g.c.d.} (j_1, j_2, \ldots, j_n)$. Then, by Lemma 1, we have $A^n = C^{i_1n} = (g(C))^{i_1}$. So $A$ is primitive if and only if $A^n$ is primitive, i.e., if and only if $g(C)$ is primitive. But, by Lemma 3, $(g(C))^m = J_a$, and $g(C)$ is primitive if and only if $a = 1$.

References


Authors’ addresses: Chong-Yun Chao, University of Pittsburgh, Pittsburgh, Pennsylvania 15260, U.S.A.; Shmuel Winograd, IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598, U.S.A.