Journal of Mathematical Research & Exposition
Vol.15, No.2, 173–178, May 1995

On Companion Boolean Relation Matrices *

Chao Chongyun
(Dept. of Math Univ of Pittsburgh Pittsburgh, PA 15260)

Wang Tianming
(Inst. of Math. Sciences Dalian Institute of Technology, Dalian, 116024)

Abstract We prove a theorem concerning the powers of a companion matrix over the Boolean algebra $B = (0, 1)$ by using elementary properties of directed graphs. The main results in [4], [1] and [2] are consequences of our theorem.

Keywords Boolean matrix, companion matrix, digraph

Classification AMS(1991) 05C50/CCL O153.2

Introduction

Let B be the Boolean algebra of 0 and 1, and $M_n(B)$ be the set of all $n \times n$ matrices over B with the usual matrix addition and multiplication. The following matrix

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & b_0 \\ 1 & 0 & 0 & \cdots & 0 & b_1 \\ 0 & 1 & 0 & \cdots & 0 & b_2 \\ \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_{n-1} \end{bmatrix}$$

is called the $n \times n$ (Boolean) companion matrix of the polynomial $x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1x + b_0$ where $b_0, b_1, \cdots, b_{n-1} \in B = \{0, 1\}$. when $b_0 = 1$ and $b_i = 0$ for $i = 1, 2, \cdots, n-1$, the matrix is a permutation matrix denoted by P^{-1}, corresponding to the permutation

$$\begin{pmatrix} 0 & 1 & \cdots & i & \cdots & n-1 \\ n-1 & 0 & \cdots & i-1 & \cdots & n-2 \end{pmatrix},$$

i.e., the permutation matrix P corresponds to the permutation

$$\begin{pmatrix} 0 & 1 & \cdots & i & \cdots & n-1 \\ 1 & 2 & \cdots & i+1 & \cdots & 0 \end{pmatrix} \tag{1}$$

*Received Feb.8, 1991.

We also let I and J denote the $n \times n$ identity matrix and the $n \times n$ matrix with all entries being 1 respectively. A matrix $C \in M_n(B)$ is said to be primitive, if there exists a positive integer N such that, for $m \geq N, C^m = J$. A matrix $C \in N_n(B)$ is said to be a t- periodic matrix, if there exist positive integers N and t such that, for $m \geq N, C^m = C^{m+t} = C^{m+2t} = \cdots = C^{m+kt} = \cdots$. P is an n-periodic matrix, and a primitive matrix is a 1-periodic matrix.

2. The Powers of Companion Matrices

Theorem 1 *Let*

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & b_1 \\ 0 & 1 & 0 & \cdots & 0 & b_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_{n-1} \end{bmatrix}$$

be an $n \times n$ matrix over the Boolean algebra $B = \{0,1\}, b_{j_1} = b_{j_2} = \cdots = b_{j_k} = 1$ where $1 \leq j_1 < j_2 < \cdots < j_k \leq n-1$ and all other $b_j's$ be 0 (if any), and t be the greatest common divisor of $j_1, j_2, \cdots, j_k$ and n (denoted by gcd $(j_1, j_2, \cdots, j_k, n) = t$).

(A) If $t > 1$, then we have:

(a) For a sufficiently large integer q,

$$C^{nq} = I + P^t + P^{2t} + \cdots + P^{(p-1)t},$$

where $n = pt$ and P is the $n \times n$ permutation matrix corresponding to the permutation (1).

(b) $C^{nq+i} = C^{nq+(i+t)} = \cdots = C^{nq+(i+ut)} = \cdots$ for $i = 0, 1, \cdots, t-1$.

(B) C is primitive, if and only if $t = 1$.

Proof (A) We consider C as the adjacency matrix of a directed graph G with loops. Thus, G has n vertices labelled as $0, 1, \cdots, n-1$. Let $C^n = (c_{ij})$. If c_{ij} in C^n is one (zero), it means that there is (is not) a directed path of length n from vertex i to vertex j. If $b_{j_t} = 1$ in $C, 1 \leq j_t \leq n-1$, then it means that, in G, there is a directed edge from the vertex j_t to the vertex $n-1$, and the directed edges

$$(j_t, n-1), (n-1, n-2), \cdots, (j_t+1, j_t)$$

constitute a directed cycle of length $n - j_t$ in G.

Let $C^{nq} = (e_{ij})$. We claim that if $0 < r < n$, and r is not a multiple of t, then

$$e_{0,r} = e_{1,r+1} = e_{2,r+2} = \cdots = e_{n-1,r+n-1} = 0$$

where the subscripts are taken modulo n. Suppose the contrary, i.e., $e_{s,r+s} = 1$ for some s such that $0 \leq s \leq n-1$. Then it means that there is a directed path of length nq from the vertex s to the vertex $r+s$ in the graph G whose adjacency matrix is C. Thus,

$$r + g_1(n - j_1) + g_2(n - j_2) + \cdots + g_k(n - j_k) + g_n n = nq \qquad (2)$$

where $g_1, g_2, \cdots, g_k$ and g_n are non-negative integers and $g_m(n - j_m)$ means the $(n - j_m)$-cycle in G is used g_m times for $m = 1, 2, \cdot, k$, and the n-cycle is used g_n times. (2) can be written as

$$r = g_1 j_1 + g_1 j_2 + \cdots + g_k j_k + n(q - g_1 - g_2 - \cdots - g_k - g_n). \tag{3}$$

Since $\gcd(j_1, j_2, \cdots, j_k, n) = t > 1$, the right side of (3) is divisible by t. But since r is not a multiple of t, we have a contradiction, and

$$e_{0,e} = e_{1,r+1} = e_{2,r+2} = \cdots = e_{n-1,r+n-1} = 0. \tag{4}$$

We claim that if s is a multiple of t, say, $s = ht$ for $h = 0, 1, \cdot \quad, p - 1$ where $n = pt$, then

$$e_{0,s} = e_{1,s+1} = e_{2,s+2} = \cdots = e_{n-1,s+n-1} = 1.$$

Since $\gcd(j_1, j_2, \cdots, j_k, n) = t > 1$, there exist integers $a_1, a_2, \cdots, a_k, a_n$ such that

$$a_1 j_1 + a_2 j_2 + \cdots + a_k j_k + a_n n = t. \tag{5}$$

Then, $t + a_1(n - j_1) + a_2(n - j_2) + \cdots + a_k(n - j_k) = n(a_1 + a_2 + \cdots + a_k + a_n)$, i.e.,

$$t + a_1(n - j_1) + a_2(n - j_2) + \cdots + a_k(n - j_k) \equiv 0 \mod n. \tag{6}$$

In (6), we replace a_i by d_i where d_i is non-negative and $d_i \equiv a_i \bmod n$ for $i = 1, 2, \cdots, k$. Then

$$t + d_1(n - j_1) + d_2(n - j_2) + \cdots + d_k(n - j_k) \equiv 0 \mod n \tag{7}$$

still holds, and

$$t + d_1(n - j_1) + d_2(n - j_2) + \cdots + d_k(n - j_k) = nq \tag{8}$$

holds for sufficiently large positive integers q. That means, in $C^{nq} = (e_{ij})$,

$$e_{0,s} = e_{1,s+1} = e_{2,s+2} = \cdots = e_{n-1,s+n-1} = 1 \tag{9}$$

for $s = ht, h = 0, 1, \cdots, p - 1$ where $n = pt$. Consequently, by (4) and (9), we have

$$C^{nq} = I + P^t + P^{2t} + \cdots + P^{(p-1)t}, \tag{10}$$

where P is the permutation matrix corresponding to the permutation (1), and the (a) part of (A) is proved.

(b) Let E_{ij} be the $n \times n$ matrix over B such that the i-th row and the j-th column is 1, and all other entries are 0. Then $C = P^{-1} + E_{j_1,n-1} + E_{j_2,n-1} + \cdots + E_{j_k,n-1}$.

We consider C^{qn+1}. By using (10), we have

$$C^{nq+1} = CC^{nq} = (P^{-1} + \sum_{s=1}^{k} E_{j_s,n} - 1)(\sum_{u=0}^{p-1} P^{ut}). \tag{11}$$

Since $\gcd(j_1, j_2, \cdots, j_k, n) = t > 1$, for $i = 1, 2, \cdots, k, j_i = d_i t$ for some positive integer d_i. Then we have

$$E_{j_i,n-1}P^{ut} = E_{d_i t,n-1}P^{ut} = E_{d_i t,ut-1}. \tag{12}$$

Also,

$$E_{d_it,ut-1} \leq P^{ut-1-d_it} = P^{(u-d_i)t-1}, \tag{13}$$

and

$$E_{d_it,n-1} \leq P^{d_it-1}. \tag{14}$$

By using (12), (13) and (14), we have (11) as

$$C^{nq+1} = \sum_{u=0}^{p-1} P^{ut-1}. \tag{15}$$

Assume that

$$C^{nq+v} = \sum_{u=0}^{p-1} P^{ut-v} \quad \text{for} \quad 1 \leq v \leq t. \tag{16}$$

We consider the case of C^{nq+v+1}. By using (16), we have

$$C^{nq+v+1} = CC^{nq+v} = (P^{-1} + \sum_{i=1}^{k} E_{d_it,n-1})(\sum_{u=0}^{p-1} P^{ut-v}). \tag{17}$$

Since $E_{d_it,n-1}P^{ut-v} = E_{d_it,ut-v-1} \leq P^{ut-v-1-d_it} = P^{(u-d_1)t-v-1}$ and $E_{d_it,n-1} \leq P^{d_it-v-1}$, (17) is

$$C^{nq+v+1} = \sum_{u=0}^{p-1} P^{ut-v-1} \tag{18}$$

By induction, we have $C^{nq+i} = C^{nq+(i+t)} = \cdots = C^{nq+(i+ut)} = \cdots$ for $i = 0, 1, \cdots, t-1$. That completes the proof of the (b) part of (A) in our Theorem 1.

(B) We shall show that C is primitive, if and only if $t = 1$.

If $\gcd(j_1, j_2, \cdots, j_k, n) = t = 1$, then there exist integers $a_1, a_2, \cdots, a_k$ and a such that

$$a_1j_1 + a_2j_2 + \cdots + a_kj_k + an = 1. \tag{19}$$

We can write (19) as

$$d_1j_1 + d_2j_2 + \cdots + d_kj_k \equiv 1 \mod n \tag{20}$$

where $d_1, d_2, \cdots, d_k$ are positive integers and $d_i \equiv a_i \mod n$ for $i = 1, 2, \cdots, k$.

If b_{j_t} in C is equal to 1 for $1 \leq j_t \leq n-1$, then in the graph G, there is a directed edge from the vertex j_t to the vertex $n-1$, and the directed edges

$$(j_t, n-1), (n-1, n-2), \cdots, (j_t+1, j_t)$$

constitute a directed cycle, Z_{j_t}, of length $n - j_t$ in G. Then, by using Z_{j_t}, in G, the following path from the vertex 0 to the vertex $n - j_t$ is of length n:

$$0 \text{—} (n-1) \text{—} (n-2) \text{—} \cdots \text{—} j_t \text{—} (n-1) \text{—} (n-2) \text{—} \cdots \text{—} (n-j_t).$$

That is ,in $C^n = (c_{ij}), c_{0,n-j_t} = 1$. Consequently,

$$c_{0,n-j_t} = c_{1,n-j_t-1} = c_{2,n-j_t-2} = \cdots = c_{n-1,n-j_t-(n-1)} = 1$$

where the subscripts are taken modulo n. Since $b_{j_1} = b_{j_2} = \cdots = b_{j_k} = 1$ where $1 \le j_1 < j_2 < \cdots < j_k \le n-1$,

$$C^n \ge I + P^{n-j_1} + P^{n-j_2} + \cdots + P^{n-j_k} = I + P^{-j_1} + P^{j_2} + \cdots + P^{-j_k}. \tag{21}$$

From (20), we know that $d_1 j_1 + d_2 j_2 + \cdots + d_k j_k = 1 + mn$ for some positive integer m. By using (21), we have

$$\begin{aligned} (C^n)^{1+mn} &\ge (I + P^{-j_1} + P^{-j_2} + \cdots + P^{-j_k})^{1+mn} \\ &= (I + P^{-j_1} + P^{-j_2} + \cdots + P^{-j_k})^{d_1 j_1 + d_2 j_2 + \cdots + d_k j_k} \\ &\ge I + P^{-j_1 d_1} + P^{-j_2 d_2} + \cdots + P^{-j_k d_k} = I + P^{-1} \end{aligned} \tag{22}$$

Since P^{-1} is a generator of the cyclic group $\{I, P, P^2, \cdots, P^{n-1}\}$, from (22) we have

$$((C^n)^{1+mn})^n \ge (I + P^{-1})^n = I + P^{-1} + P^{-2} + \cdots + P^{-n+1} = J.$$

Hence, C is primitive.

Conversely, if $\gcd(j_1, j_2, \cdots, j_k, n) = t > 1$, then by (A), C is not primitive. Hence, C is primitive, if and only if $t = 1$.

Corollary 1 *(Chao and Winograd [2]) Let*

$$A = C^{i_1} + C^{i_2} + \cdots + C^{i_s}$$

where C is the Boolean companion matrix in Theorem 1, and $i_1, i_2, \cdots, i_s$ are integers such that $0 \le i_1 < i_2 < \cdots < i_s \le n-1$ with $i_s > 0$. Then A is primitive, if and only if $\gcd(i_1 - i_1, i_2 - i_1, \cdots, i_s - i_1, j_1, j_2, \cdots, j_t, n) = 1$,

Proof If $\gcd(i_1 - i_1, i_2 - i_1, \cdots, i_s - i_1, j_1, j_2, \cdots, j_k, n) = 1$, then we have two cases to consider:

Case 1 $\gcd(j_1, j_2, \cdots, j_k, n) = 1$. Then by Theorem 1, C is primitive and A is also primitive.

Case 1 $\gcd(j_1, j_2, \cdots, j_k, n) = t > 1$. Since $\gcd(i_1 - i_1, i_2 - i_1, \cdots, i_s - i_1, t) = 1$, there exist integers $a_1, a_2, \cdots, a_s, a_{s+1}$ such that $a_1(i_1 - i_1) + a_2(i_2 - i_1) + \cdots + a_s(i_s - i_1) + a_{s+1}t = 1$, and there exist non-negative integers $d_1, d_2, \cdots, d_s, d_{s+1}$ such that

$$d_1(i_1 - i_1) + d_2(i_2 - i_1) + \cdots + d_s(i_s - i_1) + d_{s+1}t \equiv 1 \mod n. \tag{23}$$

By using the part (a) of (A) in Theorem 1, we have

$$\begin{aligned} A^{nq} &= (C^{i_1}(I + C^{i_2 - i_1} + \cdots + C^{i_s - i_1}))^{nq} \\ &= (I + P^t + P^{2t} + \cdots + P^{(p-1)t})^{i_1}(I + C^{i_2 - i_1} + \cdots + C^{i_s - i_1})^{nq} \\ &\ge (I + P^t + P^{2t} + \cdots + P^{(p-1)t})^{i_1}(I + (P^{-1})^{i_2 - i_1} + \cdots + (P^{-1})^{i_s - i_1})^{nq}. \end{aligned} \tag{24}$$

For sufficiently large nq, by (23) there is a term

$$I + P^{-1} = I + P^{-(d_1(i_1 - i_1) + d_2(i_2 - i_1) + \cdots + d_s(i_s - i_1) + d_{s+1}t)}$$

in the product of $(I+(P^{-1})^{i_2-i_1}+\cdots+(P^{-1})^{i_s-i_1})^{nq}$ in (24). Consequently,

$$(A^{nq})^n \geq ((I+P^t+P^{2t}+\cdots+P^{(p-1)t})^{i_1}(\cdots+I+P^{-1}+\cdots))^n = J,$$

and A is primitive.

If $\gcd(i_1-i_1, i_2-i_1, \cdots, i_s-i_1, j_1, j_2, \cdots, j_k, n) = d > 1$, then we show that A is not primitive. We claim that $f_{01}=0$ in $C^{md}=(f_{ij})$ for any non-negative integer m. Clearly, the entry $f_{01}=0$ in $C^0=I$. We suppose that $f_{01}=1$ in $C^{md}=(f_{ij})$ for some positive integer m. Then we would have a directed path of length md from vertex 0 to vertex 1 in the graph G whose adjacency matrix is C. Thus, $1+g_1(n-j_1)+g_2(n-j_2)+\cdots+g_k(n-j_k)+g_n n = md$, i.e.,

$$1 = g_1 j_1 + g_2 j_2 + \cdots + g_k j_k - n(g_1+g_2+\cdots+g_k+g_n) + md. \tag{25}$$

Since $j_1, j_2, \cdots, j_k$ and n are multiples of d, the right hand side of (25) is divisible by d, but 1 is not divisible by $d>1$. That is a contradiction.

Let $n=de$ for some positive integer e. We also let $i_r - i_1 = a_r d$ for some positive integer a_r, and $r=1,2,\cdots,s$. Then, for sufficiently large nq,

$$\begin{aligned} A^{nq} &= (C^{i_1}(I+C^{i_2-i_1}+\cdots+C^{i_s-i_1}))^{nq} = (C^{nq})^i (I+C^{a_2 d}+\cdots+C^{a_s d})^{nq} \\ &= C^{deqi}(I+C^{a_2 d}+\cdots+C^{a_s d})^{nq}. \end{aligned} \tag{26}$$

In the expansion of (26), every term is of the form C^{md} for some non-negative integer m. Since the (0,1)-entry $f_{10}=0$ in $C^{md}=(f_{ij})$ for any non-negative ingeger m, the (0,1)-entry of A^{nq} is 0 where nq is arbitrarily large, and A is not primitive.

Corollary 2 *(Butler and Krabil [1], and Schwarz [4]) The circulant Boolean relation $n \times n$ matrix in $P^{i_1}+P^{i_2}+\cdots+P^{i_k}$ where $0 \leq i_1 < i_2 < \cdots < i_k \leq n-1$, is primitive if and only if $\gcd(i_1-i_1, i_2-i_1, \cdots, i_k-i_1, n) = 1$.*

References

[1] K.K.H. Butler and J.K.Krabil, *Circulant Boolean Relation Matrices*, Czech. Math. J., Vol.24(1974), 247–251.

[2] C.Y.Chao and S.Winograd, *A Generalization of a Theorem of Boolean Relation Matrices*, Czech. Math. J., Vol.27(1977), 552-555.

[3] K.H.Kim, *Boolean Matrix Theory and Application*, Marcel Dekker, Inc., New York and Basel, 1982.

[4] S.Schwarz, *Circulant Boolean Relation Matrices*, Czech. Math. J., Vol.24(1974), 252–253.