Czechoslovak Mathematical Journal

Kim Ki-Hang Butler; James Richard Krabill

Circulant Boolean relation matrices

Czechoslovak Mathematical Journal, Vol. 24 (1974), No. 2, 247–251

Persistent URL: http://dml.cz/dmlcz/101235

Terms of use:

© Institute of Mathematics AS CR, 1974

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

Czechoslovak Mathematical Journal, 24 (99) 1974, Praha

CIRCULANT BOOLEAN RELATION MATRICES

KIM KI-HANG BUTLER and JAMES RICHARD KRABILL, Pembroke

(Received November 23, 1972)

Let $\mathscr{B}_n$ be the semigroup of all binary relations on a set of n elements. Let $\mathscr{C}_n$ be the subset of $\mathscr{B}_n$ consisting of all circulants. Then $\mathscr{C}_n$ is shown to be a maximal abelian subsemigroup of $\mathscr{B}_n$, and for $C \in \mathscr{C}_n$, necessary and sufficient conditions are obtained for the existence of a positive integer p such that $C^p = J_n$, all of whose entries are 1. Related problems are investigated by Š. SCHWARZ (see [7], [8], and [9]).

B. M. SCHEIN [6] asked in his sixth question for the maximal abelian subsemigroup of $\mathscr{B}_n$. We represent the elements of $\mathscr{B}_n$ as $n \times n$ matrices over the Boolean algebra of order 2. It is well known that $\mathscr{B}_n$ is a semigroup under matrix multiplication. Let $\mathscr{C}_n$ be the subset of $\mathscr{B}_n$ consisting of all the circulants. Thus for $C \in \mathscr{C}_n$, $c_{0,k} = c_{j,m}$ whenever $j + k \equiv m$ (modulo n) $(0 \leqq j, k, m \leqq n - 1)$. We have

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \dots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \dots & c_{n-3} & c_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c_1 & c_2 & c_3 & \dots & c_{n-1} & c_0 \end{bmatrix}_{n \times n}$$

and completely specify C by giving the first row. We now write $C = (c_0, \ldots, c_{n-1})$. $|X|$ denotes the cardinality of a set X.

Remark 1. $|C_n| = 2^n$.

We now give a partial solution to Schein's question in terms of $\mathscr{C}_n$. In this paper the term "maximal" as applied to an abelian subsemigroup of $\mathscr{B}_n$ means that the abelian subsemigroup is not properly contained in any abelian subsemigroup of $\mathscr{B}_n$.

Theorem 1. *$\mathscr{C}_n$ is a maximal abelian subsemigroup of $\mathscr{B}_n$.*

Proof. First, if $A, B \in \mathscr{C}_n$ and $A = (a_0, \ldots, a_{n-1})$ and $B = (b_0, \ldots, b_{n-1})$ then

$$AB = \Big(\sum_{\substack{i,j=0 \\ i+j \equiv 0 \pmod n}}^{n-1} a_i b_j, \sum_{\substack{i,j=0 \\ i+j \equiv 1 \pmod n}}^{n-1} a_i b_j, \ldots, \sum_{\substack{i,j=0 \\ i+j \equiv n-1 \pmod n}}^{n-1} a_i b_j \Big).$$

Thus, AB belongs to $\mathscr{C}_n$, and $AB = BA$ follows simply from commutativity of multiplication in the Boolean algebra. To show that $\mathscr{C}_n$ is not properly contained in any abelian subsemigroup $\mathscr{B}_n$, we let A be an arbitrary element of $\mathscr{B}_n \setminus \mathscr{C}_n$ and demonstrate a C in $\mathscr{C}_n$ such that $AC \neq CA$. Since $A \notin \mathscr{C}_n$, there exist j, k, $0 \leqq j, k \leqq n - 1$ such that $a_{0,k} \neq a_{j,m}$ where $m \equiv j + k \pmod n$ and $0 \leqq m \leqq n - 1$. Let $C = (c_0, \ldots$ $\ldots, c_{n-1})$ be such that $c_j = 1$ and $c_i = 0$ if $i \neq j$. Let $AC = D = (d_{ij})$ and $CA =$ $= F = (f_{ij})$. We have $d_{0,m} = a_{0,k}$ and $f_{0,m} = a_{j,m}$. Hence $AC \neq CA$ and the proof is completed.

Remark 2. *The $n \times n$ circulants whose entries belong to any commutative ring form an abelian semigroup under matrix multiplication.*

We now turn to the problem of determining which matrices A have the property $A^p = J_n$ for some positive integer p where J_n is the $n \times n$ matrix all of whose entries are 1. N. de Bruijn [3], I. Good [4], N. S. Mendelsohn [5] each described a specific class of graphs with the unique path property of order n. The incidence matrix A of a graph with this property satisfies the equation $A^p = J_n$ for some positive integer p. For the definition of unique path property and its graph theoretic significance, see Mendelsohn [5]. These authors obtained partial solutions with matrices over the real numbers while we obtain a partial solution in terms of $\mathscr{C}_n$ for Boolean relation matrices. The problem of finding Boolean relation matrices for which $A^p = J_n$ is related to a problem in matrices over the real field. Namely, if A is a matrix over the reals all of whose entries are nonnegative, then is there a positive integer p such that A^p has all entries strictly positive? The relationship is established by constructing a homomorphism from the nonegative real numbers to this Boolean algebra such that 0 is mapped to 0 and all positive real numbers are mapped to 1.

We now set up some notation and make a few remarks about certain circulants. We defined J_n in an earlier paragraph as $J_n = (1, \ldots, 1)$. We now define $P_n =$ $= (0, 1, 0, \ldots, 0)$, the permutation matrix with $p_1 = 1$ and $p_i = 0$ for $i \neq 1$. Let $\mathscr{G}_n = \{P_n^i, 0 \leqq i \leqq n - 1\}$, $\Delta(C) = \{i : c_{0,i} = 1, C \in \mathscr{C}_n\}$, and let $\sigma(C)$ be the greatest common divisor of the elements of $\Delta(C)$.

Remark 3. First, $\mathscr{G}_n$ is a cyclic subgroup of $\mathscr{C}_n$, and hence of $\mathscr{B}_n$. Next, $|\mathscr{G}_n| = n$. Finally, every circulant C can be written exactly one way as a sum of distinct elements of $\mathscr{G}_n$.

Remark 4. An element of $\mathscr{G}_n$, P_n^i, is a generator of $\mathscr{G}_n$ iff $(i, n) = 1$. In particular, P_n^i is a generator of $\mathscr{G}_n$ if n is prime and $i \neq 0$.

Remark 5. For every divisor d of n there is a cyclic subgroup of $\mathscr{C}_n$, and hence of $\mathscr{B}_n$, which is of order d. It consists of all $C \in \mathscr{C}_n$ for which $\Delta(C) = \{i : i \equiv k \pmod d\}$, $k = 0, 1, \ldots, d - 1$.

We now consider the theorem which gives a partial solution to the Mendelsohn problem.

Theorem 2. *Let $C \in \mathscr{C}_n$, $n > 1$. There exists a positive integer p such that $C^p = J_n$ iff $(\sigma(C), n) = 1$ and for every divisor d of n, $d > 1$, there exist $i, j \in \Delta(C)$ such that $i \not\equiv j \pmod{d}$. If p exists, then $p \leqq n - 1$.*

We need a lemma to establish the sufficiency.

Lemma. *If $C, D \in \mathscr{C}_n$, $C = (c_0, \ldots, c_{n-1})$, $D = (d_0, \ldots, d_{n-1})$, there exists a j, $0 \leqq j \leqq n - 1$ such that $d_r = c_i$ whenever $r \equiv i - j \pmod{n}$, $C^p = (a_0, \ldots, a_{n-1})$, and $D^p = (b_0, \ldots, b_{n-1})$, then $b_r = a_i$ whenever $r \equiv i - pj \pmod{n}$.*

Proof (of Lemma). Here $\Delta(C^p) = \{s \equiv i_0 + i_1 + \ldots + i_{p-1} \pmod{n} : i_m \in \Delta(C)\}$. Here and in the following i_m and i_n are not necessarily distinct. Also $\Delta(D^p) = \{s \equiv r_0 + r_1 + \ldots + r_{p-1} \pmod{n} : r_m \in \Delta(D)\}$. But $r_m \in \Delta(D)$ iff $i_m \in \Delta(C)$ where $r_m \equiv i_m - j \pmod{n}$. Thus $\Delta(D^p) = \{s \equiv r_0 + r_1 + \ldots + r_{p-1} - pj \pmod{n} : i_m \in \Delta(C)\}$. Therefore we have $b_r = a_i$ whenever $r \equiv i - pj \pmod{n}$ and the lemma is proved.

Proof (of Theorem 2). Necessity: The proof of the necessity is by contradiction. Let $C = (c_0, \ldots, c_{n-1})$ and $C^p = (b_0, \ldots, b_{n-1})$. If $(\sigma(C), n) = q > 1$, then for all p, $b_i = 0$ whenever $(i, q) = 1$. Hence, for all p, $C^p \neq J_n$. If $(\sigma(C), n) = 1$, but for some d a divisor of n, $d > 1$, we have $i, j \in \Delta(C)$, $m \equiv i \equiv j \pmod{d}$. Here $b_i = 0$ for each i such that $i \not\equiv pm \pmod{d}$, and for all p, $C^p \neq J_n$. This establishes the necessity of the conditions.

Sufficiency: If $|\Delta(C)| = 0$, then $C^p = C = (0, \ldots, 0)$ for all p. Also if $|\Delta(C)| = 1$ and $\{i\} = \Delta(C)$, then $\{j\} = \Delta(C^p)$ where $j \equiv pi \pmod{n}$. Thus, if p exists such that $C^p = J_n$, we must have $|\Delta(C)| \geqq 2$. We now assume $|\Delta(C)| \geqq 2$. When C and D satisfy the hypotheses of the lemma, the lemma shows $C^p = J_n$ iff $D^p = J_n$, and we may reduce the problem to that of finding all circulants D such that $D^p = J_n$ and $0 \in \Delta(D)$. The two hypotheses together for C are equivalent to the two hypotheses together for D. It should be noted however, that the common divisor condition alone for C does not imply the common divisor condition for D. Since $0 \in \Delta(D)$, we have the containment relation

$$\Delta(D) \subseteq \Delta(D^2) \subseteq \ldots \subseteq \Delta(D^p) \subseteq \Delta(D^{p+1}) \subseteq \ldots$$

Let $\{0, i_1, \ldots, i_s\} = \Delta(D)$. Then $(\sigma(D), n) = 1$ may be written $(i_1, i_2, \ldots, i_s, n) = 1$. It is well known that $(i_1, i_2, \ldots, i_s, n) = 1$ iff there is a solution in integers $x_1, x_2, \ldots \ldots, x_s, x_n$ of the equation

$$x_1 i_1 + x_2 i_2 + \ldots + x_s i_s + x_n n = 1 .$$

Let $x_i' \equiv x_i \pmod{n}$ and $0 \leqq x_i' \leqq n - 1$. Then we have

$$x_1' i_1 + x_2' i_2 + \ldots + x_s' i_s \equiv 1 \pmod{n}$$

Therefore,

$$p \geqq \sum_{i=1}^{s} x_i'$$

implies $1 \in \Delta(D^p)$. Since

$$\sum_{i=1}^{s} x_i' \leqq s(n-1),$$

we conclude $1 \in \Delta(D^{s(n-1)})$. Now 0 also belongs to $\Delta(D^{s(n-1)})$, and we obtain

$$\begin{aligned} &\{0, 1, 2\} \in \Delta(D^{2s(n-1)}), \\ &\{0, 1, 2, 3\} \in \Delta(D^{3s(n-1)}), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\{0, 1, \ldots, n-1\} \in \Delta(D^{s(n-1)^2}). \end{aligned}$$

This completes the proof of the sufficiency and we may write $\Delta(D^{s(n-1)^2}) = J_n$.

We now establish a smaller value of p, when it exists, since $p = s(n-1)^2$ is in general much larger then necessary. We observed earlier that for $0 \in \Delta(D)$,

$$\Delta(D) \subseteq \Delta(D^2) \subseteq \ldots \subseteq \Delta(D^p) \subseteq \ldots$$

Also

$$\Delta(D^k) = \Delta(D^{k+1})$$

implies

$$\Delta(D^k) = \Delta(D^{k+i})$$

for all positive integers i. If p is minimal such that $D^p = J_n$,

$$2 \leqq |\Delta(D)| < |\Delta(D^2)| < \ldots < |\Delta(D^p)| = n.$$

Hence $p \leqq n - 1$ whenever p exists, and the entire proof is complete.

Remark 6. An equivalent statement of Theorem 2 is obtained by replacing the word "divisor" with the phrase "prime divisor".

Remark 7. If $|\Delta(C)| = 2$ and there exists a p such that $C^p = J_n$, then $p = n - 1$. Thus, the upper bound on p in the theorem is best possible, when p exists.

Remark 8. Given $C \in \mathscr{C}_n$, there exists a positive integer p such that

$$\sum_{i=0}^{p} C^i = J_n$$

if and only if $(\sigma(C), n) = 1$. The incongruence condition of Theorem 2 does not apply.

Remark 9. Given $C \in \mathscr{C}_n$, the sequence $\{C^i\}$ becomes periodic with period greater than one eventually under two sets of conditions. That is, there exist positive integers m and k, k minimal and $k > 1$, such that $C^{j+ik} = C^j$ whenever $j > m$ and $i = 0$. First, from Remark 8, if $(\sigma(C), n) = 1$ but for some divisor d of n, $d > 1$, d maximal, $i \equiv j \pmod{d}$ whenever $i, j \in \Delta(C)$, the sequence has period d. Also, if $(\sigma(C), n) = q$ and for every $i, j \in \Delta(C)$, $i \equiv j \pmod{d}$, $q \mid d$, $q < d$, $d \mid n$, then the sequence is periodic with period d/q.

Added in proof: Recently the authors learned of a shorter proof of Theorem 2 by Professor Š. Schwarz [10].

References

[1] *K. K.-H. Butler,* On (0, 1)-matrix semigroups, Semigroup Forum, *3* (1971), 74—79.

[2] *A. H. Clifford* and *G. B. Preston,* The algebraic theory of semigroups, Mathematical surveys, No. 7, Vol *I,* 1961, Amer. Math. Society, Providence, R. I.

[3] *N. G. de Bruijn,* A combinatorial problems, Proc. Koninkl. Ned. Akad. Wetenschap, *49* (1946), 758—764.

[4] *I. J. Good,* Normal recurring decimals, J. London. Math. Society, *21* (1946), 167—169.

[5] *N. S. Mendelsohn,* Directed graphs with the unique path property, Colloquia Math. Societatis Janos Bolyai 4, Combinatorial theory, *2* (1970), 783—798.

[6] *B. M. Schein,* Semigroups of binary relations, to appear in the Proc. of Miniconference on Algebraic Semigroup Theory, J. Attila University, Szeged, Hungary, August—September, 1972.

[7] *Š. Schwarz,* On a sharp estimation in the theory of binary relations on a finite set, Czech. Math. J., *20 (95)* (1970), 703—714.

[8] *Š. Schwarz,* On idempotent binary relations on a finite set, Czech. Math. J., *20 (95)* (1970), 696—702.

[9] *Š. Schwarz,* On the semigroup of binary relations on a finite set, Czech. Math. J., *20 (95)* (1970), 632—679.

[10] *Š. Schwarz,* Circulant Boolean relation matrices, Czech. Math. J. *24 (99)* (1974), 252—253.

Authors' address: Pembroke State University, Pembroke, North Carolina 28372, U.S.A.