Kim Ki-Hang Butler; Štefan Schwarz

The semigroup of circulant Boolean matrices

Czechoslovak Mathematical Journal, Vol. 26 (1976), No. 4, 632–635

Persistent URL: http://dml.cz/dmlcz/101434

Czechoslovak Mathematical Journal, 26 (101) 1976, Praha

THE SEMIGROUP OF CIRCULANT BOOLEAN MATRICES

KIM KI-HANG BUTLER*), Montgomery, and ŠTEFAN SCHWARZ, Bratislava

(Received February 25, 1975, in revised form August 4, 1975)

Let B_n be the semigroup of binary relations on a finite set X, with card $X = |X| = n$ represented as $n \times n$ matrices over the Boolean algebra $\{0, 1\}$.

A circulant is a Boolean matrix of the form

$$C = \begin{bmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-2} \\ \dots & \dots & \dots & \dots \\ c_1 & c_2 & \dots & c_0 \end{bmatrix}.$$

Denote

$$P = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}$$

and E the unit matrix of order n. Any circulant $\in B_n$ can be written in the form

$$C = c_0E + c_1P + c_2P^2 + \dots + c_{n-1}P^{n-1}, \quad c_i \in \{0, 1\}. \tag{1}$$

Hereby $P^n = E$. (See [1], [3].) We define also $P^0 = E$.

The set of all circulants (of order n) under multiplication forms a semigroup C_n with $|C_n| = 2^n$ (including the zero circulant Z). C_n contains the cyclic group $G_n = \{E, P, P^2, \dots, P^{n-1}\}$ of order n and we have $G_n \subset C_n \subset B_n$. Clearly every element $\in C_n$ has a unique representation in the form (1). (This will turn out to be essential.) Note that C_n is closed also under addition.

The purpose of this note is to give an explicit description of all idempotents $\in C_n$ and all maximal subgroups of C_n.

It will turn out that the set of all maximal subgroups of C_n is exactly the set of all cyclic groups of order d, d being a divisor of n. A remarkable feature of the results

*) The first named author was supported by NSF Grant No. HES 74-24502.

obtained bellow is the fact that an explicit description of maximal subgroups in a semigroup is only very rarely available.

Since C_n is finite and commutative, the relations $\mathfrak{L}$, $\mathfrak{R}$, $\mathfrak{D}$, $\mathfrak{H}$ in C_n coincide and the maximal subgroup $G(E^{(i)})$ belonging to the idempotent $E^{(i)}$ is the $\mathfrak{L}$-class containing $E^{(i)}$, i.e. the set $\{A \in C_n : SE^{(i)} = SA\}$. (See [2].) Clearly $G(E) = G_n$.

Lemma 1. *If $A, B \in C_n$, then $A \mathfrak{L} B$ iff there is an element $P^m \in G_n$ such that $A = P^m B$.*

Proof. (i) For any P^m $(m = 0, 1, 2, \ldots, n-1)$ we have $C_n P^m = C_n$. Hence $C_n A = C_n P^m B = C_n B$. Therefore $A = P^m B$ implies $A \mathfrak{L} B$.

(ii) Conversely $A \mathfrak{L} B$, $A \neq Z$, $B \neq Z$ implies that there are two elements $R, S \in C_n$ such that $A = RB$, $B = SA$. Write

$$R = P^{m_1} + P^{m_2} + \ldots + P^{m_r}, \quad S = P^{k_1} + P^{k_2} + \ldots + P^{k_s}.$$

Then

$$A = \left(P^{m_1} + P^{m_2} + \ldots + P^{m_r}\right) B, \quad B = \left(P^{k_1} + P^{k_2} + \ldots + P^{k_s}\right) A.$$

Hence (with $\subset$ denoting the usual ordering of Boolean matrices) $P^{m_1} B \subset A$, $P^{k_1} A \subset B$. This implies $B \supset P^{k_1} A \supset P^{k_1 + m_1} B$ and $B \supset P^{k_1 + m_1} B \supset P^{2(k_1 + m_1)} B \supset \ldots \supset P^{n(m_1 + k_1)} B = B$, whence $P^{k_1} A = B$. Analogously

$$A \supset P^{m_1} B \supset P^{m_1 + k_1} A \supset P^{2(m_1 + k_1)} A \supset \ldots \supset P^{n(m_1 + k_1)} A = A,$$

whence $A = P^{m_1} B$. This proves our lemma.

Remark. The element $P^m \in C_n$ in Lemma 1 is "in general" not uniquelly determined.

If $A \neq Z$ and $A = P^{m_1} + P^{m_2} + \ldots + P^{m_r}$ we shall call the subset $\{P^{m_1}, P^{m_2}, \ldots, P^{m_r}\}$ of G_n the *support* of A. Given A the support is uniquelly determined.

Lemma 2. *An element $A \in C_n$, $A \neq Z$, is an idempotent iff the support of A is a subgroup of G_n.*

Proof. (i) If $A^2 = A$, i.e.

$$\left(P^{m_1} + \ldots + P^{m_r}\right)\left(P^{m_1} + \ldots + P^{m_r}\right) = \left(P^{m_1} + \ldots + P^{m_r}\right),$$

then the subset $K = \{P^{m_1}, \ldots, P^{m_r}\}$ of G_n is closed under multiplication, i.e. $K^2 \subset K$. A subset K of a finite group G_n closed under multiplication is a subgroup of G_n.

Recall the following elementary result. All subgroups of G_n are obtained in the following manner. Let t be a divisor of n and $tn^* = n$. Then G_n contains a subgroup of order t which can be explicitly given in the form

$$G^* = \{P^{n^*}, P^{2n^*}, \ldots, P^{(t-1)n^*}, P^{tn^*} = E\}.$$

Though P^{n*}, as a generator of G^*, is not uniquelly determined, G^* as a whole is uniquelly determined. (For $t = 1$ we have $G^* = \{E\}$, for $t = n$ we have $G^* = G_n$.)

(ii) Let conversely

$$G^* = \{P^{n*}, P^{2n*}, \ldots, P^{tn*}\}, \quad n^*t = n,$$

be a subgroup of G_n. Direct computation shows that

$$A = P^{n*} + P^{2n*} + \ldots + E$$

is an idempotent $\in C_n$.

Let now $t_i \mid n$ and $t_i n_i = n$. To find the maximal subgroup $G(E^{(i)})$ belonging to the idempotent

$$E^{(i)} = P^{n_i} + P^{2n_i} + \ldots + P^{t_i n_i}$$

we use Lemma 1 and the fact that

$$G(E^{(i)}) = \{Y \in C_n : Y \,\mathfrak{Q}\, E^{(i)}\}.$$

We have $Y \,\mathfrak{Q}\, E^{(i)}$ iff there is an element $P^m \in G_n$ such that $Y = P^m E^{(i)}$. Hence

$$G(E^{(i)}) = \{E, P, P^2, \ldots, P^{n-1}\} E^{(i)}.$$

This set contains exactly n_i different elements, namely

$$E^{(i)}, PE^{(i)}, P^2E^{(i)}, \ldots, P^{n_i-1}E^{(i)}.$$

These are exactly those elements $\in C_n$ whose supports are the cosets of G_n modulo the cyclic group

$$\{P^{n_i}, P^{2n_i}, \ldots, P^{t_i n_i}\}.$$

We have proved:

Theorem 3. *Let t_i be a divisor of n and $t_i n_i = n$. Then*

$$E^{(i)} = P^{n_i} + P^{2n_i} + \ldots + P^{t_i n_i}$$

is an idempotent $\in C_n$. The maximal subgroup of C_n belonging to $E^{(i)}$ is the cylic group

$$\{E^{(i)}, PE^{(i)}, \ldots, P^{n_i-1}E^{(i)}\}.$$

All idempotents and all maximal subgroups of C_n are obtained in this manner.

Denote by $d(n)$ the number of divisors of n (including 1 and n) and by $\sigma(n)$ the sum of all divisors of n.

We have:

Corollary 4. *C_n contains $d(n)$ different idempotents $\neq Z$ and $\sigma(n)$ distinct regular elements $\neq Z$.*

Example. The semigroup C_6 contains (besides Z) the following four idempotents:

$$E^{(1)} = P^6 = E\,, \quad E^{(3)} = P^2 + P^4 + E\,,$$
$$E^{(2)} = P^3 + E\,, \quad E^{(4)} = P + P^2 + P^3 + P^4 + P^5 + E\,.$$

The corresponding maximal subgroups of C_6 are

$$G(E^{(1)}) = \{E, P, P^2, P^3, P^4, P^5\}\,, \quad G(E^{(3)}) = \{P^2 + P^4 + E,\ P^3 + P^5 + P\}\,,$$
$$G(E^{(2)}) = \{P^3 + E,\ P^4 + P,\ P^5 + P^2\}\,, \quad G(E^{(4)}) = E\,.$$

Remark 1. To avoid misunderstanding we note. The semigroup B_n may contain cyclic subgroups of order t which does not divide n and even cyclic subgroups of order $t > n$. To show this denote

$$Q_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Q_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

and consider the 5×5 matrix

$$A = \begin{bmatrix} Q_1 & 0 \\ 0 & Q_2 \end{bmatrix}.$$

It is immediately to seen that $\{A, A^2, A^3, A^4, A^5, E\}$ is a cyclic subgroup of B_5 of order $t = 6$. The cyclic subgroup $\{A^2, A^4, E\}$ is of order 3 though 3 does not divide 5.

Remark 2. In a "general" semigroup there may exist different idempotents with the corresponding maximal subgroups isomorphic one to the other. It is worth to mention that in C_n no two maximal subgroups are isomorphic one to the other.

References

[1] *Kim Ki-Hang Butler* and *J. R. Krabill:* Circulant Boolean relation matrices, Czech. Math. J,. *24 (99)* (1974), 247—251.

[2] *A. H. Clifford* and *G. B. Preston:* The algebraic theory of semigroups, Math. Surveys, No.7, Vol. 1, 1961, Amer. Math. Soc., Providence, R. I.

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

Authors' addresses: Kim Ki-Hang Buttler, Alabama State University, Montgomery 36101, U.S.A., Štefan Schwarz, 880 19 Bratislava, Gottwaldovo nám. 19, ČSSR (Slovenská vysoká škola technická).