Štefan Schwarz

A counting theorem in the semigroup of circulant Boolean matrices

Czechoslovak Mathematical Journal, Vol. 27 (1977), No. 3, 504–510

Persistent URL: http://dml.cz/dmlcz/101485

Czechoslovak Mathematical Journal, 27 (102) 1977, Praha

A COUNTING THEOREM IN THE SEMIGROUP OF CIRCULANT BOOLEAN MATRICES

ŠTEFAN SCHWARZ, Bratislava

(Received August 25, 1975)

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

A circulant is a Boolean matrix of the form

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix}$$

Denote

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

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

$$(1) \qquad A = a_0E + a_1P + a_2P^2 + \dots + a_{n-1}P^{n-1}, \quad a_i \in \{0, 1\}.$$

Hereby $P^n = E$. For convenience we also define $P^0 = E$.

The set of all circulants of order n forms (under multiplication) a semigroup C_n with $|C_n| = 2^n$ (including the zero circulant Z).

The semigroup C_n contains the cyclic group $G_n = \{E, P, P^2, \dots, P^{n-1}\}$ and we have $G_n \subset C_n \subset B_n$.

If $A = (a_{ij})$ and $B = (b_{ij})$ are Boolean matrices $\in B_n$, we denote by $A \cap B$ the matrix $D = (d_{ij})$ with $d_{ij} = \min(a_{ij}, b_{ij})$. Clearly if $k \not\equiv l \pmod n$ we have $P^k \cap P^l = Z$. This implies that any element $\in C_n$ has a unique representation in the form (1).

The study of C_n has been iniciated in [1], where it is proved that C_n is a maximal abelian subsemigroup of B_n.

Denote by I_n the $n \times n$ Boolean matrix all elements of which are one's.

In [2] and [4] necessary and sufficient conditions are given in order that some power of an element $\in C_n$ is equal to I_n. In [1] a formula for the number of elements $\in C_n$ having this property is given. In the present paper this formula will appear as a special case of more general considerations.

In [3] we have proved the following results. Let d be any divisor of n, $n = dt$. Then

$$E^{(d)} = E + P^d + P^{2d} + \ldots + P^{(t-1)d} \tag{2}$$

is an idempotent $\in C_n$ and any idempotent $\in C_n$ is obtained in this manner. Also the maximal subgroup of C_n, which contains $E^{(d)}$ as the unit element, is the cyclic group $\{E^{(d)}, P \,.\, E^{(d)}, \ldots, P^{t-1} \,.\, E^{(d)}\}$ of order t.

Note for further purposes that in this notation $E^{(n)} = E$ and $E^{(1)} = I_n$.

The problem treated in this paper can be formulated for any finite semigroup S. If $a \in S$, then the sequence $\{a, a^2, a^3, \ldots\}$ contains one and only one idempotent, say e_α. We shall say that a belongs to the idempotent e_α. Denote by $K(e_\alpha)$ the set of all elements $\in S$ belonging to the idempotent e_α. If $\{e_\alpha, e_\beta, \ldots, e_\nu\}$ is the set of all idempotents $\in S$, then S can be written as a union of disjoint sets: $S = K(e_\alpha) \cup \cup K(e_\beta) \cup \ldots \cup K(e_\nu)$. If S is commutative, each $K(e_\mu)$ is a semigroup [the maximal subsemigroup of S containing the unique idempotent e_μ].

In the general case we can hardly expect to get some information concerning the cardinality of the sets $K(e_\mu)$. There are very few known non-trivial classes of semigroups where the cardinality of the sets $K(e_\mu)$ is known.

It is a remarkable feature of the semigroup C_n that in this case we are able

i) to give a reasonable description of all elements belonging to a given idempotent $E^{(d)}$,

ii) to give a smooth formula for the number $|K(E^{(d)})|$.

A

Lemma 1. *If $B \in C_n$, then B and $B \,.\, P^l$ $(0 \leqq l \leqq n - 1)$ belong to the same idempotent $\in C_n$.*

Proof. If $B^h = E'$, where E' is an idempotent, then $(BP^l)^{hn} = B^{hn} \,.\, P^{nlh} = E' \,.\, E = E'$.

If A, B are elements $\in B_n$, we shall write $A \leqq B$ iff $A \cap B = A$.

Lemma 2. *Let*

$$B = E + P^{j_1} + P^{j_2} + \ldots + P^{j_k}, \quad 1 \leqq j_1 < j_2 < \ldots < j_k \leqq n - 1 \,. \tag{3}$$

Then there is an integer h, $1 \leqq h \leqq n - 1$, such that B^h is an idempotent $\in C_n$.

Proof. The obvious "inequality" $B \leqq B^2$ implies

$$B \leqq B^2 \leqq B^3 \leqq \ldots \leqq B^{n-1} \leqq B^n \leqq \ldots$$

Since $j_1 \geqq 1$, the first row (and hence all rows) of B contains at least two non-zero elements. B^2 is either B or it contains at least three non-zero elements in all rows. Repeating this argument we obtain: There is an integer $h \leqq n - 1$ such that $B^h = B^{h+1}$. Now $B^h = B^{h+1} = \ldots = B^{2h}$ implies that B^h is an idempotent.

Corollary 2. *For any $A \in C_n$, A^n is an idempotent.*

Proof. If A is a permutation matrix or $A = Z$ the Corollary is trivially true. Otherwise write $A = P^l \,.\, B$, where B is of the form (3). We then have $A^n = P^{ln}B^n = E \,.\, B^n = B^n$ and by the proof of Lemma 2 B^n is an idempotent $\in C_n$.

Lemma 3. *Let d be a divisor of n, $d \neq n$, and $n = dt$. If an element B of the form (3) belongs to the idempotent $E^{(d)} = E + P^d + P^{2d} + \ldots + P^{(t-1)d}$, then $j_1 \equiv j_2 \equiv \ldots \equiv j_k \equiv 0 \pmod{d}$.*

Proof. It follows from Lemma 2 that there is an integer $h \leqq n - 1$ such that $B^h \,.\, B = B^h$ and B^h is an idempotent. Since $B^h = E^{(d)}$, we have

$$[E + P^d + P^{2d} + \ldots + P^{(t-1)d}]\,[E + P^{j_1} + P^{j_2} + \ldots + P^{j_k}] =$$
$$= [E + P^d + P^{2d} + \ldots + P^{(t-1)d}]\,.$$

This implies that the sets of integers

$$V_1 = \{0, d, 2d, \ldots, (t-1)\,d\}$$

and

$$V_2 = V_1 \cup [\bigcup_{l=1}^{k} \{j_l, j_l + d, j_l + 2d, \ldots, j_l + (t-1)\,d\}]$$

are $(\bmod\, n)$ identical. In particular, $\{j_1, j_2, \ldots, j_k\} \in V_1$, i.e. $j_l \equiv 0 \pmod{d}$ for any $l = 1, 2, \ldots, k$. This proves our Lemma.

Corollary 3. *Any element $\in C_n$ which belongs to the idempotent $E^{(d)}$, $d \neq n$, is necessarily of the form*

$$A = P^l(E + P^{u_1 d} + P^{u_2 d} + \ldots + P^{u_k d})\,, \tag{4}$$
$$1 \leqq u_1 < u_2 < \ldots < u_k \leqq t - 1\,,$$

with suitably chosen $u_1, \ldots, u_k$, and $0 \leqq l \leqq n - 1$.

Not all possible choices of $u_1, u_2, \dots, u_k$, give elements belonging to $E^{(d)}$. This is now clarified by the following theorem.

Theorem 1. *Let $n = dt$, $d \neq n$. An element*

$$A = P^l(E + P^{u_1 d} + P^{u_2 d} + \dots + P^{u_k d}), \quad 1 \leqq u_1 < u_2 < \dots < u_k \leqq t - 1$$

belongs to the idempotent $E^{(d)}$ iff g.c.d. $(u_1, u_2, \dots, u_k, t) = 1$.

Remark. This is a generalization of the result of [4], where the case $d = 1$ has been treated.

Proof. By Lemma 1 A belongs to $E^{(d)}$ iff $B = E + P^{u_1 d} + P^{u_2 d} + \dots + P^{u_k d}$ belongs to $E^{(d)}$.

Write for simplicity $P^d = Q$ and note that $Q^i \cap Q^j = Z$ if $i \not\equiv j \pmod t$ so that the representation of B in the form of a sum of powers of Q

$$B = E + Q^{u_1} + Q^{u_2} + \dots + Q^{u_k}$$

is uniquely determined.

It follows by Lemma 2 that B belongs to $E^{(d)}$ iff $B^{n-1} = E^{(d)}$ or (what is the same) iff $\sum_{l=n-1}^{N} B^l = E^{(d)}$ for any $N \geqq n - 1$. Hence B belongs to $E^{(d)}$ iff we have

$$(5) \qquad \sum_{l=n-1}^{N} (E + Q^{u_1} + \dots + Q^{u_k})^l = E + Q + Q^2 + \dots + Q^{t-1}\,.$$

[We use this formulation in order to avoid unnecessary restrictions concerning the choice of the integers x_{ij} needed below.]

Evaluate the left hand side of (5) as "polynomials in Q" by multiplying term by term the products $(E + Q^{u_1} + \dots + Q^{u_k})^l$. Using the idempotency of addition (i.e. $Q^i + Q^i = Q^i$) and $Q^t = E$, the left hand side of (5) becomes finally a sum of distinct powers of Q. Now (5) holds iff the left hand side of (5) contains as a summand every power Q^j, $j = 1, 2, \dots, t - 1$. Hence (5) holds iff to any integer $j = 1, 2, \dots$ $\dots, t - 1$ there exist non-negative integers $x_{1j}, x_{2j}, \dots, x_{kj}$ such that

$$(6) \qquad x_{1j}u_1 + x_{2j}u_2 + \dots + x_{kj}u_k \equiv j \pmod t\,.$$

Hereby $x_{1j} + x_{2j} + \dots + x_{kj} \leqq N$, where N is arbitrarily large.

Now the congruence

$$x_{11}u_1 + x_{21}u_2 + \dots + x_{k1}u_k \equiv 1 \pmod t$$

has a solution $x_{11}^0, x_{21}^0, \dots, x_{k1}^0$ iff g.c.d. $(u_1, u_2, \dots, u_k, t) = 1$. On the other hand if this condition is satisfied, then (6) has a solution for any $j \in \{2, 3, \dots, t - 1\}$. It is sufficient to put $x_{1j} = jx_{11}^0, x_{2j} = jx_{21}^0, \dots, x_{kj} = jx_{k1}^0$. This proves Theorem 1.

B

We now proceed to the problem to find the number of elements belonging to the idempotent $E^{(d)}$. Instead of $K(E^{(d)})$ we shall write simply $K^{(d)}$.

Suppose again $d < n$, hence $t > 1$. By Corollary 3 any element $\in K^{(d)}$ is a sum of properly chosen elements of one of these $d - 1$ sets:

$$T_0 = \{Q, Q^2, \dots, Q^t = E\},$$

$$T_1 = \{PQ, PQ^2, \dots, PQ^t = P\},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$T_{d-1} = \{P^{d-1}Q, P^{d-1}Q^2, \dots, P^{d-1}Q^t = P^{d-1}\}.$$

[We emphasise that any sum considered here and below consists of summands contained in one and only one "row".] With respect to the unicity of the representation of any $A \in C_n$ in the form (1) the various possible sums in each T_1 ($i = 0, 1, \dots \dots, d - 1$) are different one from the other.

Since we may exclude the zero matrix Z and $t > 1$, each of the sums which have to be in $K^{(d)}$ contains at least two summands. For each of the d classes $T_0, T_1, \dots, T_{d-1}$ we can construct $2^t - 1 - t$ different sums (each containing at least two summands). This gives together $d(2^t - 1 - t)$ different elements $\in C_n$.

Consider first the set $T_0 = \{Q, Q^2, \dots, Q^t = E\}$. To obtain the sums $\in T_0$ contained in $K^{(d)}$ we have (by Theorem 1) to exclude those elements $Q^{u_1} + Q^{u_2} + \dots \dots + Q^{u_k}$ for which g.c.d. $(u_1, u_2, \dots, u_k, t) \neq 1$. Analogously an element $P^lQ^{u_1} + P^lQ^{u_2} + \dots + P^lQ^{u_k}$ is to be excluded if g.c.d. $(u_1, u_2, \dots, u_k, t) \neq 1$.

Let $t = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_s^{\alpha_s}$ be the factorization of t into distinct primes.

Let us begin with the set T_0. Corresponding to the prime p_1 we have to exclude first all sums (containing at least two summands) obtained by summing elements of the set $\{Q^{p_1}, Q^{2p_1}, \dots, Q^{(t/p_1)p_1} = E\} \subset T_0$. This gives together $2^{t/p_1} - t/p_1 - 1$ elements. By Theorem 1 we have to exclude also all sums obtained by summing elements from the sets

$$\{Q^{p_1+v}, Q^{2p_1+v}, \dots, Q^v\} \subset T_0, \quad v = 1, 2, \dots, p_1 - 1$$

(each sum containing at least two summands). As far we have together $p_1(2^{t/p_1} - t/p_1 - 1)$ elements which must be excluded from all possible sums obtained by summing the elements $\in T_0$. Since the same holds for the sets T_1 $T_2, \dots, T_{a-1}$ we have: Corresponding to the prime p_1 we have to exclude $dp_1(2^{t/p_1} - t/p_1 - 1)$ elements which do not belong to $K^{(d)}$.

Next corresponding to any of the primes p_i ($i = 2, 3, \dots, s$) we have to exclude analogously $dp_i(2^{t/p_i} - t/p_i - 1)$ elements which do not belong to $K^{(d)}$.

At this stage we arrived to the number

$$d(2^t - t - 1) - d \sum_{p_i} p_i(2^{t/p_i} - t/p_i - 1).$$

Now by the principle of inclusion and exclusion we must add the sums excluded twice, i.e. those elements $P^l(E + Q^{u_1} + Q^{u_2} + \dots + Q^{u_k})$, $(l = 0, 1, \dots, d - 1)$ in which g.c.d. $(u_1, u_2, \dots, u_k)$ is divisible both by p_i and p_j $(i \neq j)$. This gives the number of elements

$$d \sum_{p_i, p_j} p_i p_j (2^{t/p_i p_j} - t/p_i p_j - 1)$$

to be included.

Repeating this argument in the usual manner we finally obtain

$$|K^{(d)}| = d(2^t - t - 1) - d \sum_{p_i} p_i (2^{t/p_i} - t/p_i - 1) +$$
$$+ d \sum_{p_i, p_j} p_i p_j (2^{t/p_i p_j} - t/p_i p_j - 1) + \dots$$
$$\dots + (-1)^s \, p_1 p_2 \dots p_s (2^{t/p_1 p_2 \dots p_s} - t/p_1 p_2 \dots p_s - 1) .$$

Now the sum of the second terms in all rows together is zero, since $-d[t - st + \binom{s}{2} t - \dots + (-1)^{s+1} t] = -dt(1 - 1)^s = 0$.

Hence we have:

$$|K^{(d)}| = d(2^t - 1) - d \sum_{p_i} p_i (2^{t/p_i} - 1) + d \sum_{p_i, p_j} p_i p_j (2^{t/p_i p_j} - 1) - \dots$$

Denoting by $\mu(l)$ the Möbius function we have the following final result:

Theorem 2. *Let be $n > 1$, d a divisor of n and $n = dt$. Then the number of elements $\in C_n$ belonging to the idempotent $E^{(d)}$ is given by the formula*:

$$|K^{(d)}| = d \sum_{l/t} l \, \mu(l) \, (2^{t/l} - 1) .$$

Remark 1. This result has been proved for $t > 1$. But it is true also for $t = 1$. In this case the formula gives $|K^{(n)}| = n$ and this is exactly the order of the maximal subgroup $G_n = \{E, P, \dots, P^{n-1}\}$ having $E = E^{(n)}$ as the unit element.

Remark 2. Theorem 2 is a wide generalization of Theorem 2 of the paper [1].

Remark 3. The formula in Theorem 2 has a form which enables easy computations for various n and d.

Introduce the following number-theoretical function (defined for all integers $t \geq 1$):

$$\Phi(t) = \frac{1}{t} \sum_{l/t} l \, \mu(l) \, (2^{t/l} - 1)$$

Then $|K^{(d)}| = n \, \Phi(t)$, where $t = n/d$.

The first ten values of $\Phi(t)$ are given by the table

t	$\Phi(t)$	t	$\Phi(t)$
1	1	6	46/6
2	1/2	7	120/7
3	4/3	8	226/8
4	9/4	9	490/9
5	26/5	10	956/10

Example 1. Let $n = 18$. C_{18} contains 6 non-zero idempotents:

$$E^{(18)} = E\,, \qquad E^{(3)} = E + P^3 + P^6 + \ldots + P^{15}\,,$$

$$E^{(9)} = E + P^9\,, \qquad E^{(2)} = E + P^2 + P^4 + \ldots + P^{16}\,,$$

$$E^{(6)} = E + P^6 + P^{12}\,, \qquad E^{(1)} = E + P + P^2 + \ldots + P^{17}\,.$$

We have:

$$|K^{(18)}| = 18\,\Phi(1) = 18\,, \qquad |K^{(3)}| = 18\,\Phi(6) = 138\,,$$

$$|K^{(9)}| = 18\,\Phi(2) = 9\,, \qquad |K^{(2)}| = 18\,\Phi(9) = 980\,,$$

$$|K^{(6)}| = 18\,\Phi(3) = 24\,, \qquad |K^{(1)}| = 18\,\Phi(18) = 260\,974\,.$$

Example 2. Our small table enables to make some computations even for large n. Let, e.g., $n = 100$. The number of elements $\in C_{100}$ belonging to the idempotent $E^{(20)} = E + P^{20} + \ldots + P^{80}$ is $|K^{(20)}| = 100\,\Phi(5) = 520$.

References

[1] *K. K.-Hang Butler* and *J. R. Krabill:* Abelian subsemigroups, enumeration and universal matrices, Duke Math. J. *40* (1973), 587—598.

[2] *K. K.-Hang Butler* and *J. R. Krabill:* Circulant Boolean relation matrices, Czechoslovak Math. J. *24* (*99*) (1974), 247—251.

[3] *K. K.-Hang Butler* and *Š. Schwarz:* The semigroup of circulant Boolean matrices, Czechoslovak Math. J. *26 (101),* (1976), 632—635.

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

Author's address: 801 00 Bratislava, Porubského 8, ČSSR.