Štefan Schwarz
Circulant Boolean relation matrices

Czechoslovak Mathematical Journal, Vol. 24 (1974), No. 2, 252–253

Persistent URL: http://dml.cz/dmlcz/101236

Czechoslovak Mathematical Journal, 24 (99) 1974, Praha

CIRCULANT BOOLEAN RELATION MATRICES

(A note to the foregoing paper of K. K. Hang Butler and J. R. Krabill)

ŠTEFAN SCHWARZ, Bratislava

(Received June 19, 1973)

The purpose of this note is to give a new proof of Theorem 2 of the foregoing paper [1] and to modify its statement in a way which seems to be more adequate.

We briefly recall some necessary preliminaries and notations. All matrices in this note are $n \times n$ Boolean relation matrices with the usual addition and multiplication. We denote $E = \text{diag}\,[1, 1, \ldots, 1]$. Further, J denotes the $n \times n$ matrix in which all patterns are ones.

If $A = (a_{ik})$, $B = (b_{ik})$, we shall write $A \leqq B$ if $a_{ik} = 1$ implies $b_{ik} = 1$. If A is any $n \times n$ matrix it is known (see e.g. [2]) that $A^t \leqq A + A^2 + \ldots + A^n$ for any $t > 0$.

A matrix A is called irreducible if $A + A^2 + \ldots + A^n = J$. It is called primitive if there is an integer $p > 0$ such that $A^p = J$. A primitive matrix is irreducible. The converse need not be true. Nevertheless, if $E \leqq A$, then A is primitive iff A is irreducible. Indeed, $E \leqq A$ implies $E \leqq A \leqq A^2 \leqq \ldots \leqq A^n$, hence $A + A^2 + \ldots + A^n = A^n$ and $A + A^2 + \ldots + A^n = J$ iff $A^n = J$.

Let P be the $n \times n$ permutation matrix

$$P = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}.$$

Then $P^n = E$, and every circulant (Boolean relation) matrix can be written in the form

$$C = c_0 E + c_1 P + c_2 P^2 + \ldots + c_{n-1} P^{n-1}\,.$$

Omitting those c_i which are zeros and defining $P^0 = E$, we have

$$C = P^{i_1} + P^{i_2} + \ldots + P^{i_l}\,, \tag{1}$$

where $0 \leqq i_1 < i_2 < i_3 < \ldots < i_l \leqq n - 1$. Suppose $l > 1$.

The problem treated in [1] can be formulated as follows. We have to find necessary and sufficient conditions under which C is primitive. We prove:

Theorem. *The circulant Boolean relation matrix* (1) *is primitive iff*

$$\text{g.c.d.}\ (i_2 - i_1, i_3 - i_1, \ldots, i_l - i_1, n) = 1\,.$$

Proof. Write

$$C = P^{i_1}[E + P^{i_2 - i_1} + \ldots + P^{i_l - i_1}] = P^{i_1} \, . \, T\,,$$

where T has the obvious meaning. We have $C^p = P^{pi_1} \, . \, T^p$. Since the permutation matrix P^{pi_1} rearranges only the rows and columns in T^p, we conclude that $C^p = J$ holds iff $T^p = J$ holds.

Since $E \leqq T$, T is primitive iff it is irreducible, i.e. iff

$$T + T^2 + \ldots + T^n = J\,. \tag{2}$$

It is advantageous to write instead of (2) $\sum_{j=1}^{N} T^j = J$ for any integer $N \geqq n$. Hence T is primitive iff for any $N \geqq n$ we have

$$\sum_{j=1}^{N} (E + P^{i_2 - i_1} + \ldots + P^{i_l - i_1})^j = J\,. \tag{3}$$

Note that $E + P + P^2 + \ldots + P^{n-1} = J$ and each summand on the left hand side is essential, i.e., omitting any P^i $(0 \leqq i \leqq n - 1)$ the sum becomes $\neq J$.

Multiply term by term the products $(E + P^{i_2 - i_1} + \ldots + P^{i_l - i_1})^j$. Using the idempotency of addition (i.e. $P^l + P^l = P^l$) and $P^n = E$, the left hand side of (3) finally becomes a sum of distinct powers of P. Now (3) holds iff the left hand side of (3) contains as a summand every power P^j for $j = 0, 1, \ldots, n - 1$. Since this expression certainly contains E, we can state that (3) holds iff to any integer $k = 1, 2, \ldots, n - 1$ there exist nonnegative integers $x_{2k}, x_{3k}, \ldots, x_{lk}$ such that

$$x_{2k}(i_2 - i_1) + x_{3k}(i_3 - i_1) + \ldots + x_{lk}(i_l - i_1) \equiv k \pmod{n}\,.$$

Now the congruence

$$x_2(i_2 - i_1) + x_3(i_3 - i_1) + \ldots + x_l(i_l - i_1) \equiv 1 \pmod{n}$$

has a solution $x_{21}, x_{31}, \ldots, x_{l1}$ iff g.c.d. $(i_2 - i_1, i_3 - i_1, \ldots, i_l - i_1, n) = 1$. On the other hand if this condition is satisfied, then for any $k = 2, 3, \ldots, n - 1$ the congruence

$$y_2(i_2 - i_1) + y_3(i_3 - i_1) + \ldots + y_l(i_l - i_1) \equiv k \pmod{n}$$

has a solution $y_{2k}, y_{3k}, \ldots, y_{lk}$. [It is sufficient to put $y_{2k} = kx_{21}, \ldots, y_{lk} = kx_{l1}$.] This proves our statement.

References

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

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

Author's address: 880 31 Bratislava, Gottwaldovo nám. 2, ČSSR (SVŠT).