139. A Note on the Powers of Boolean Matrices

By Shinnosuke ÔHARU
Waseda University, Tokyo

(Comm. by Kinjirô KUNUGI, M.J.A., Sept. 12, 1967)

1. Let $\mathfrak{A}$ be the set of all $n\times n$-matrices each element of which is 1 or 0. For any $A=(a_{ij})$ and $B=(b_{ij})$ of $\mathfrak{A}$, we define multiplication by

$$A\cdot B=\left(\sum_{k=1}^{n}\oplus a_{ik}b_{kj}\right)$$

where $1\oplus 1=1$, $1\oplus 0=0\oplus 1=1$, $0\oplus 0=0$. It is readily seen that this multiplication is associative and we can consider the m-th power $\underbrace{A\cdot A\cdot\cdots\cdot A}_{m}$ of any element $A\in\mathfrak{A}$. We denote it by A^m. In this paper we shall treat the powers of elements of $\mathfrak{A}$ under this multiplication.

Definitions, Notations, and Preliminary Notes. For any $A=(a_{ij})$ and $B=(b_{ij})$ of $\mathfrak{A}$, we difine operations

$$A\vee B=(a_{ij}\oplus b_{ij}) \text{ and } A\wedge B=(a_{ij}b_{ij}).$$

Then it is easily seen that $\mathfrak{A}$ is a Boolean algebra under these operations. And we can define the ordering $\leqq$ by the usual manner. This definition is equivalent to the proposition that $A\leqq B$ if and only if $a_{ij}=0$ whenever $b_{ij}=0$, and we use also the ordering $<$ defined in such a way that $A<B$ if and only if $A\leqq B$ and $A\neq B$.

E_{st} is the $s\times t$-matrix whose elements are all 1 and O_{st} is the $s\times t$-matrix whose elements are all 0. Particularly if $s=t=n$, we denote them by E and O respectively. Under the above orderings, we can prove that $O\leqq D\leqq E$ for any $D\in\mathfrak{A}$ and that $A\leqq B$ implies $D\cdot A\leqq D\cdot B$ and $A\cdot D\leqq B\cdot D$ for any $D\in\mathfrak{A}$. And $I=(\delta_{ij})$ is the matrix such that $\delta_{ij}=1$ only if $i=j$. For any $A\in\mathfrak{A}$, $I\cdot A=A\cdot I=A$. Further, for each $A\in\mathfrak{A}$, we put $A^k=(a_{ij}^{(k)})$ for each integer $k\geqq 1$. Let $P=(p_{ij})$ be the permutation matrix corresponding to a permutation σ in such a way that only the $p_{i\sigma(i)}$ is 1 in the i-th row and $P^{\top}=(p'_{ij})$ be its transpose. Then P and $P^{\top}$ are the elements of $\mathfrak{A}$ and for each $A\in\mathfrak{A}$ the (i,j)-element of $P\cdot A\cdot P^{\top}$ is

$$\sum_{l=1}^{n}\oplus\left(\sum_{k=1}^{n}\oplus p_{ik}a_{kl}\right)p'_{lj}=\sum_{l=1}^{n}\oplus a_{\sigma(i)l}p_{jl}=a_{\sigma(i)\sigma(j)}.$$

Thus the operation $P\cdot A\cdot P^{\top}$ is equivalent to the operation $PAP^{\top}$ by means of the usual matrix multiplication. In particular, $P\cdot P^{\top}=P^{\top}\cdot P=I$. By virtue of this fact, we can apply the well known theorem for the reducibility of the matrix [1; p 45], and use the term "irreducible matrix" in the usual manner. That is, we can find a permutation matrix P such that $P.A.P^{\top}(=PAP^{\top})$ is of the form

$$\begin{pmatrix} A_{11}, & \cdots, & A_{1N} \\ \vdots & & \vdots \\ A_{N1}, & \cdots, & A_{NN} \end{pmatrix} \tag{1}$$

where each block submatrix A_{ij} is an $n_i \times n_j$-matrix $\left(\sum_{k=1}^{N} n_k = n\right)$, $A_{ij} = O_{n_i n_j}$ for $i>j$ and A_{ii} are irreducible for all $i=1, \cdots, N$.

The main result is the following

Theorem. *Let $A \in \mathfrak{A}$ be such that $a_{ii}=1$ for all i. Then there exists an integer $m \leqq n-1$ such that*

$$A < A^2 < A^3 < \cdots < A^m = A^{m+1} \tag{2}$$

and such that for the permutation matrix P such that $P \cdot A \cdot P^{\top}$ is of the form (1), *the matrix $P \cdot A^m \cdot P^{\top}$ has the form*

$$\begin{pmatrix} G_{11}, & \cdots, & G_{1N} \\ \vdots & & \vdots \\ G_{N1}, & \cdots, & G_{NN} \end{pmatrix} \tag{3}$$

which is the same partition as that of $P \cdot A \cdot P^{\top}$, where $G_{ij} = O_{n_i n_j}$ for $i>j$, $G_{ii} = E_{n_i n_j}$ for all i and for $i<j$, each G_{ij} is either $E_{n_i n_j}$ or $O_{n_i n_j}$.

Here if $P \cdot A \cdot P^{\top}$ is the direct sum of its submatrices, then m can be strictly smaller than the maximum of the degrees of the submatrices.

Conversely, if a matrix $G \in \mathfrak{A}$ is such that $G^2 = G$ and $g_{ii}=1$ for all i, then for some permutation matrix P, the matrix $P \cdot G \cdot P^{\top}$ is of the abovementioned form (3) *and we can find matrices A of $\mathfrak{A}$ such that $a_{ii}=1$ for all i,*

$$A < A^2 < \cdots < A^m = A^{m+1} = G$$

for some $m \leqq n-1$ and such that for any A' with $A' < A$, $A'^k \neq G$ for all integer $k \geqq 1$.

Moreover, such an A is irreducible iff $A^m = E$ for some $m \leqq n-1$.

This research is originally arisen from the problem of the circuit theory, but its application will be published elsewhere, in addition to the details of proofs.

And the author expresses his sincere thanks to Prof. H. Sunouchi for many useful advices.

2. We shall prove the theorem mentioned above by the following successive lemmas: Throughout the lemmas we assume that the matrix A is such that $a_{ii}=1$ for all i.

Lemma 1. *There exists an $m \leqq n-1$, for which* (2) *holds. And A is irreducible iff $A^m = E$ for some $m \leqq n-1$.*

Proof. We note that $a_{ij}^{(k)}=\sum_{l_{k-1}=1}^{n}\oplus\cdots\sum_{l_1=1}^{n}\oplus a_{il_1}a_{l_1l_2}\cdots a_{l_{k-1}j}=1$ iff for some combination of suffices $\{l_1, l_2, \cdots, l_{k-1}\}$ we have $a_{il_1}a_{l_1l_2}\cdots a_{l_{k-1}j}=1$. Thus $a_{ii}=1$ implies $A^k \leqq A^{k+1}$.

Since $A^k \leqq E$ and $E\cdot A \leqq E$, there always exists an m such that $A^{m+1}=A^m$. In order to prove that such an m is smaller than $n-1$, it suffices to show that if $a_{ij}^{(n-1)}=0$ $(i\neq j)$ then $a_{ij}^{(m)}=0$ for any $m\geqq n$, by noting that the total number of the suffices is n. The equality $A^m=E$ means that for any pair (i, j) there exists a product of the form $a_{il_1}a_{l_1l_2}\cdots a_{l_{m-1}j}=1$, which is equivalent to the fact that A is irreducible. [1; p 20, Th. 1.6]. Q.E.D.

We note that the above proof shows that if $a_{ij}^{(m)}=1$ for some $m\geqq n$, then $a_{ij}^{(k)}=1$ for some $k<n$. And clearly if A is the direct sum of its submatrices $A_1, \cdots, A_d$, then A^k is also the direct sum of the submatrices $A_1^k, \cdots, A_d^k$. Thus $m \leqq \max_{1\leqq v\leqq d}(n_v)-1$, where each n_v is the degree of A_v. Generally, m can not be smaller than this bound.

Lemma 2. *There exists a permutation matrix P for which $P\cdot A^m\cdot P^{\top}$ has the form* (3), *where m is that of lemma* 1.

Proof. Let P be the permutation matrix such that $P\cdot A\cdot P^{\top}$ is of the form (1). Then from the direct computation it follows that $P\cdot A^m\cdot P^{\top}=(P\cdot A\cdot P^{\top})^m=(PAP^{\top})^m$ is of the form

$$\begin{pmatrix} A_{11}^m, & A_{12}^{(m)}, & \cdots, & A_{1N}^{(m)} \\ & A_{22}^m, & \cdots, & A_{2N}^{(m)} \\ & & \ddots & \vdots \\ & & & A_{NN}^m \end{pmatrix}.$$

From the proof of lemma 1, for each i, $A_{ii}^m=E_{n_in_i}$ for some sufficiently large m. And by using this fact we can prove that if $A_{ij}^{(m)}\neq O_{n_in_j}$, then $A_{ij}^{(m)}=E_{n_in_j}$. Q.E.D.

We note that if $A_{ij}\neq O_{n_in_j}$, then $A_{ij}^{(m)}\neq O_{n_in_j}$ from lemma 1, which implies $A_{ij}^{(m)}=E_{n_in_j}$ from the above proof.

Lemma 3. *Let $\tilde{G}$ be an $N\times N$ matrix of the form*

$$\begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \cdots & * \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix} \tag{4}$$

If $\tilde{G}^2=\tilde{G}$, then we can find a matrix $\tilde{A}$ with $\tilde{a}_{ii}=1$ for all i, such that $\tilde{A}^m=\tilde{G}$ for some m and such that for any $\tilde{A}'$ with $\tilde{A}'<\tilde{A}$, $\tilde{A}'^k\neq\tilde{G}$ for all integer $k\geqq 1$.

Proof. If the successive k superdiagonal elements $(k\geqq 2)$ are equal to 1 in such a way as

$$\begin{pmatrix} \ddots & & & & & & \\ & 1 & 0 & & & & \\ & & \boxed{\begin{matrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{matrix}} & & & & \\ & & & 0 & & & \\ & & & 1 & & & \\ & & & & \ddots & & \end{pmatrix}$$

then, because of the identity $\widetilde{G}^2=\widetilde{G}$, the submatrix surrounded by dotted line must be of the form

$$(5)\qquad \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & 1 & \cdots & 1 \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix}$$

Thus we get the partition of $\widetilde{G}$ of the form

$$\begin{pmatrix} \widetilde{G}_{11}, & \widetilde{G}_{12}, & \cdots, & \widetilde{G}_{1r} \\ & \widetilde{G}_{22}, & \cdots, & \widetilde{G}_{2r} \\ & & \ddots & \vdots \\ & & & \widetilde{G}_{rr} \end{pmatrix}$$

where each $\widetilde{G}_{ii}$ is an $N_i\times N_i$-submatrix of the form (5) $\left(\sum_{i=1}^{r} N_i=N\right)$ and there are no submatrices of the form (5), which contain entirely a $\widetilde{G}_{ii}(i=1,\cdots,r)$.

Set $\mathfrak{J}_1=\{(s,l);\ \widetilde{g}_{sl}=1,\ s=l, \ \text{or}\ \ s+1=l\}$ and $\mathfrak{J}_2=\bigcup_{i<j}\mathfrak{J}_{ij}$ where $\mathfrak{J}_{ij}=\left\{(s,l)\in\mathfrak{J}^0_{ij};\ s+1<l,\ \sum_{s<l_1\leq l_2\leq\cdots\leq l_{l-s-1}<l}\oplus\widetilde{g}_{sl_1}\widetilde{g}_{l_1l_2}\cdots\widetilde{g}_{l_{l-s-1}l}=0\right\}$ and $\mathfrak{J}^0_{ij}=\{(s,l);\ \widetilde{g}_{sl}=1$ is in the submatrix $\widetilde{G}_{ij}$ and $\widetilde{g}_{s,l-1}=0$, and $\widetilde{g}_{s+1,l}=0$ if they are elements of the $\widetilde{G}_{ij}\}$.

Put $\mathfrak{J}=\mathfrak{J}_1\cup\mathfrak{J}_2$ and construct a matrix $\widetilde{A}$ so that $\widetilde{a}_{ij}=1$ only for $(i,j)\in\mathfrak{J}$. Then we can prove that this $\widetilde{A}$ is the desired matrix in the lemma. Q.E.D.

3. Proof of the Theorem. The first half of the theorem and the last assertion follow from lemma 1 and 2. Thus we prove the second half of the main theorem. First, we shall show that there exists a permutation matrix P such that $P\cdot G\cdot P^{\mathrm{T}}$ is of the form (3). As is mentioned in the preliminary notes, there exists a permutation matrix P such that $P\cdot G\cdot P^{\mathrm{T}}$ is of the form (1), i.e.,

$$\begin{pmatrix} G_{11}, & \cdots, & G_{1N} \\ \vdots & & \vdots \\ G_{N1}, & \cdots, & G_{NN} \end{pmatrix}.$$

From $G^2=G$, lemma 1 and 2, it follows that $G_{ii}=E_{n_i n_i}$ for each i and $G_{ij}=E_{n_i n_j}$ whenever $G_{ij}\neq O_{n_i n_j}$, which shows that the above matrix $P.G.P^{\top}$ is of the form (3). For this $P\cdot G\cdot P^{\top}$, we define an $N\times N$-matrix $\tilde{G}=(\tilde{g}_{ij})$ as follows: $\tilde{g}_{ij}=1$ if $G_{ij}=E_{n_i n_j}$ and $\tilde{g}_{ij}=0$ otherwise. Then $\tilde{G}$ has the form (4) of lemma 3. Let $\mathfrak{J}$ be the set of pairs of indices, defined for this $\tilde{G}$ in the sense of lemma 3, and construct an $n\times n$-matrix $\hat{A}$ so that $\hat{A}$ may have the same partition as that of $P\cdot G\cdot P^{\top}$:

$$\begin{pmatrix} \hat{A}_{11}, & \cdots, & \hat{A}_{1N} \\ \vdots & & \vdots \\ \hat{A}_{N1}, & \cdots, & \hat{A}_{NN} \end{pmatrix}$$

where only one element of $\hat{A}_{ij}$ is 1 for each $(i,j)\in\mathfrak{J}(i\neq j)$, and each $\hat{A}_{ii}$ is, e.g., of the form

$$\begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 1 & & & & 1 \end{pmatrix}$$

which is an irreducible matrix. Then from lemma 3 and 1, $\hat{A}<\hat{A}^2<\hat{A}^3<\cdots<\hat{A}^m=\hat{A}^{m+1}=P\cdot G\cdot P^{\top}$ for some sufficiently large m and any 1 in this $\hat{A}$ cannot be removed. Thus the matrix $A=P^{\top}\cdot\hat{A}\cdot P$ $(=P^{\top}\hat{A}P)$ is one of the desired matrices. Q.E.D.

References

[1] R. S. Varga: Matrix Iterative Analysis. Prentice Hall (1962).
[2] G. Birkhoff: Lattice Theory. A.M.S. Colloq. Publ. (1948).