INFORMATION AND CONTROL 7, 477–484 (1964)

Lattice Matrices

YEHOSHAFAT GIVE'ON

Logic of Computers Group, The University of Michigan, Ann Arbor, Michigan

I. INTRODUCTION

This paper is a revised version of part of a previous report (Give'on, 1962) which was prepared for the U. S. Office of Naval Rsearch, Information Systems Branch, under contract No. 62558-2214, at the Applied Logic Branch of the Hebrew University in Jerusalem, Israel (February 1962).

This revision was done for the U. S. Office of Naval Research, Information Systems Branch, under contract No. Nonr-1224(21), NR 049-114.

We discuss in this paper the particular properties of the algebra of square matrices over an arbitrary distributive lattice with 0 and 1 (*$\mathfrak{L}_n$-matrices*). Due to these properties, $\mathfrak{L}_n$-matrices in various special cases become useful tools in various domains like the theory of switching nets, automata theory, and the theory of finite graphs.

In addition to this, we develop the theory of invertible $\mathfrak{L}_n$-matrices, thus generalizing R. D. Luce's (1952) discussion on invertible Boolean matrices.

II. THE ALGEBRA OF LATTICE MATRICES

A. DEFINITIONS AND IMMEDIATE PROPERTIES

Let $\mathfrak{L}$ be a distributive lattice with 0 and 1 (Birkhoff, 1961). The l.u.b. and g.l.b. of $a, b \in \mathfrak{L}$ will be denoted by $a + b$ and $a \cdot b$ (or ab), respectively (here, for convenience, we diverge from the usual notations $a \cup b$ and $a \cap b$).

Let $\mathfrak{L}_n$ (for $n > 0$) be the set of $n \times n$ matrices over $\mathfrak{L}$ ($\mathfrak{L}_n$-matrices). We shall use early Roman capitals as variables over $\mathfrak{L}_n$, and denote by A_{ij} or by $(A)_{ij}$ the element of $\mathfrak{L}$ which stands in the (i, j)th entry of A. We define:

$$A + B = C \quad \text{iff} \quad C_{ij} = A_{ij} + B_{ij},$$

$$A \leqq B \quad \text{iff} \quad A + B = B, \text{ i.e., iff } A_{ij} \leqq B_{ij},$$

$$A \cap B = C \quad \text{iff} \quad C_{ij} = A_{ij} \cdot B_{ij},$$

$$A \cdot B = AB = C \quad \text{iff} \quad C_{ij} = \sum_{v=1}^{n} A_{iv} \cdot B_{vj},$$

$$A^{\tau} = C \quad \text{iff} \quad C_{ij} = A_{ji}$$

$$\text{for } a \in \mathfrak{L},\ aA = a \cdot A = C \quad \text{iff} \quad C_{ij} = a \cdot A_{ij},$$

$$(I)_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j, \end{cases}$$

$$A^0 = I, \quad A^{k+1} = A^k \cdot A,$$

$$(0)_{ij} = 0 \qquad (E)_{ij} = 1.$$

The following special properties, most of which will be useful in the sequel, are derived immediately from these definitions:

a. The multiplication in $\mathfrak{L}_n$:

(1) $A(BC) = (AB)C$,
(2) $AI = IA = A$,
(3) $A0 = 0A = 0$,
(4) $A^p \cdot A^q = A^{p+q}$,
(5) $(A^p)^q = A^{p \cdot q}$.

b. The multiplication and addition in $\mathfrak{L}_n$:

(6) $A(B + C) = AB + AC$,
(7) $(A + B)C = AC + BC$,
(8) if $A \leqq B$ and $C \leqq D$ then $AC \leqq BD$,
(9) $A + A = A$ and therefore if $p \leqq q$ then

$$\sum_{v=p}^{q} A^v = A^p(I + A)^{q-p}.$$

c. The transposition in $\mathfrak{L}_n$:

(10) $(A + B)^{\tau} = A^{\tau} + B^{\tau}$,
(11) if $A \leqq B$ then $A^{\tau} \leqq B^{\tau}$,
(12) $(A \cap B)^{\tau} = A^{\tau} \cap B^{\tau}$,
(13) $(A \cdot B)^{\tau} = B^{\tau} \cdot A^{\tau}$,
(14) $(A^{\tau})^{\tau} = \mathrm{A}$.

d. $\mathfrak{L}_n$ as an algebra:

(15) $\mathfrak{L}_n$ is a distributive lattice with zero (0) and one (E) with respect to the operations of $\cap$ and $+$,

(16) $\mathfrak{L}_n$ is a semigroup with the identity element I (hence, $\mathfrak{L}_n$ is a monoid) and with zero (0) with respect to the multiplication.

B. Some Basic Properties of the Powers of $\mathfrak{L}_n$-Matrices

One of the most important properties of the algebra of $\mathfrak{L}_n$-matrices is given by the following theorem:

Theorem 1. *If S is any nonempty finite set of $\mathfrak{L}_n$-matrices and $\mathfrak{L}_n(S)$ is the minimal set of $\mathfrak{L}_n$-matrices which includes S and is closed under multiplication and addition, then $\mathfrak{L}_n(S)$ is finite.*

($\mathfrak{L}_n(S)$ is in fact the subalgebra of $\mathfrak{L}_n$ generated by S.)

Proof: Let $T = \{a_1, \cdots, a_m\}$ be the set of all the elements of $\mathfrak{L}$ which occur in the matrices of S, and let $\mathfrak{L}(T)$ be the set of all the elements of $\mathfrak{L}$ which are obtained by a finite number of multiplications and additions of elements of T (clearly, $\mathfrak{L}(T)$ is the sublattice of $\mathfrak{L}$ which is generated by T). Since $\mathfrak{L}$ is distributive, each element of $\mathfrak{L}(T)$ can be represented as a polynomial, i.e., as a finite sum of monomials, each monomial being a finite product of elements of T. The multiplication and addition in $\mathfrak{L}$ are commutative and idempotent; thus, every monomial in $\mathfrak{L}(T)$ is equal to a monomial of the form $a_1^{\epsilon_1} \cdot a_2^{\epsilon_2} \cdot \cdots \cdot a_m^{\epsilon_m}$ where ϵ_i (for any $1 \leqq i \leqq m$) is zero or one. Therefore, there are no more that 2^m unequal monomials and no more than $2^{(2^m)}$ elements in $\mathfrak{L}(T)$ (i.e., the sublattice generated by a finite set of elements of a distributive lattice is finite; or, in other words, any distributive lattice is locally finite). Now, each element of $\mathfrak{L}$ which occurs in an $\mathfrak{L}_n$-matrix which is in $\mathfrak{L}_n(S)$ is an element of $\mathfrak{L}(T)$; hence, at most $(2^{(2^m)})^{n^2}$ different $\mathfrak{L}_n$-matrices can be elements of $\mathfrak{L}_n(S)$. Anyhow, $\mathfrak{L}_n(S)$ is finite.

Corollary 1.1. *For any $\mathfrak{L}_n$-matrix A, the sequence: $I, A, A^2, \cdots$; is ultimately periodic.*

Definition 1. Let $a \in \mathfrak{L}$. *We shall use the notation*

$$a \ni (A^k)_{ij}$$

whenever $a = A_{i_0 i_1} \cdot A_{i_1 i_2} \cdot \cdots \cdot A_{i_{k-1} i_k}$, $i_0 = i$ and $i_k = j$; for some $i_1, \cdots, i_{k-1}$.

Remark. Clearly

$$(A^k)_{ij} = \sum_{a \ni (A^k)_{ij}} a.$$

LEMMA 1. *If* $a \dashv (A^k)_{ij}$ *where* $k \geqq n$, then there are integers m_1, m_2, m_3 *and* ν *(all of them dependent on* a*) such that*

$$0 < m_2 \leqq n, \qquad m_1 + m_2 + m_3 = k, \quad 1 \leqq \nu \leqq n,$$

and such that for each m:

$$a \leqq (A^{m_1})_{i\nu} \cdot (A^{m \cdot m_2})_{\nu\nu} \cdot (A^{m_3})_{\nu j} .$$

PROOF: Let $a = A_{i_0 i_1} \cdot A_{i_1 i_2} \cdot \cdots \cdot A_{i_{k-1} i_k}$. Since $k + 1 > n$, two indices among the $k + 1$ indices $i_0, i_1, \cdots, i_k$; must be equal, say $i_r = i_s$ where $r < s$. Moreover, we can find such r and s so that $i_r = i_s$, $r < s$ and $s - r \leqq n$. So let $m_1 = r$, $m_2 = s - r$, $m_3 = k - s$ and $\nu = i_r = i_s$, and clearly the lemma follows.

COROLLARY. *If* $a \dashv (A^k)_{ij}$ *where* $k \geqq n$, *then there are natural numbers* m_1, m_2, m_3 *and* ν *(all of them dependent on* a*) such that*

$$m_1 + m_3 \leqq n, \qquad 0 < m_2 \leqq n, \qquad 1 \leqq \nu \leqq n,$$

and such that for each m:

$$a \leqq (A^{m_1})_{i\nu} \cdot (A^{m \cdot m_2})_{\nu\nu} \cdot (A^{m_3})_{\nu j} .$$

PROOF: Immediate.

THEOREM 2: *If* $k \geqq n$ *then* $A^k \leqq A^r$ *holds for an infinite set of values of* r. *In particular, for each* p:

$$A^k \leqq A^{k + p(n!)} .$$

PROOF: Suppose that $a \dashv (A^k)_{ij}$. By Lemma 1, there are natural numbers m_1, m_2, m_3 and ν (all of them dependent on a) such that $0 < m_2 \leqq n$, $m_1 + m_2 + m_3 = k$, $1 \leqq \nu \leqq n$ and such that for each m:

$$a \leqq (A^{m_1})_{i\nu} \cdot (A^{m \cdot m_2})_{\nu\nu} \cdot (A^{m_3})_{\nu j} .$$

Hence

$$a \leqq (A^{m_1 + m \cdot m_2 + m_3})_{ij} = (A^{k + (m-1) \cdot m_2})_{ij} .$$

Now, since m is arbitrary, we can replace $m - 1$ by $p \cdot (n!/m_2)$ where p is an arbitrary natural number, and obtain the theorem.

THEOREM 3. *If* $k \geqq r$ *then* $A^k \leqq A^r (I + A)^{n-1}$.

PROOF: Suppose that $a \dashv (A^k)_{ij}$. If $k \leqq r + n - 1$ then clearly $a \leqq (A^r (I + A)^{n-1})_{ij}$. If not, then $k \geqq n$ holds. In this case, by Lemma 1, there are natural numbers m_1, m_2, m_3 and ν such that $0 < m_2 \leqq n$, $m_1 + m_2 + m_3 = k$, $1 \leqq \nu \leqq n$ and $a \leqq (A^{m_1})_{i\nu} (A^{m_3})_{\nu j} \leqq (A^{m_1 + m_3})_{ij} =$

$(A^{k-m_2})_{ij}$. If $k - m_2 \leqq r + n - 1$ then the theorem is proved since $0 < m_2 \leqq n$. If not, then we apply Lemma 1 successively until we get $a \leqq (A^s)_{ij}$ for some $r \leqq s \leqq r + n - 1$ and the theorem follows.

REMARK AND DEFINITION 2. For $r = 0$ we get that $A^k \leqq (I + A)^{n-1}$ holds for any k; hence we can define $\sum_{k=0}^{\infty} A^k$ to be $(I + A)^{n-1}$ and to denote it by A^*. Note that the existence of this infinite sum is implied independently by Corollary 1.1.

COROLLARY 3.1. *If $k \geqq r$ then $A^k \leqq A^k \cdot A^* \leqq A^r \cdot A^*$.*

PROOF: Immediate.

THEOREM 4 (Lunts, 1950; Hohn and Schissler, 1955; Yoeli, 1959). *If $I \leqq A$ then $A^k \leqq A^{k+1}$ holds for any k; in particular, $A^k = A^{n-1}$ holds for $k \geqq n$, hence $A^* = A^{n-1}$.*

PROOF: If $I \leqq A$ then $I + A = A$ and therefore, for each k: $(I + A)^{k+1} = A^{k+1}$ and thus, $A^k \leqq A^{k+1}$. Moreover, $I \leqq A$ implies $A^* = A^{n-1}$, and so $A^k \leqq A^{n-1}$ holds for $k \geqq n$. Since $k \geqq n$ implies, in our case, $A^k \geqq A^{n-1}$, we get $A^k = A^{n-1}$ for any $k \geqq n$.

THEOREM 5. *$A^k \cdot A^n \cdot A^* = A^n \cdot A^*$ holds for any k.*

PROOF: For each i, $1 \leqq i \leqq n$, there is, by Theorem 2, a q_i such that $k + n + i < q_i$ and $A^{n+i-1} \leqq A^{q_i}$. Hence

$$A^n \cdot A^* = \sum_{i=1}^{n} A^{n+i-1} \leqq \sum_{i=1}^{n} A^{q_i} = A^k \cdot A^n \sum_{i=1}^{n} A^{q_i-n-k}.$$

But Theorem 3 implies that for each i: $A^{q_i-n-k} \leqq A^*$ and therefore,

$$A^k \cdot A^n \sum_{i=1}^{n} A^{q_i-n-k} \leqq A^k \cdot A^n \cdot A^*.$$

Hence $A^n \cdot A^* \leqq A^k \cdot A^n \cdot A^*$ and by Theorem 3 this theorem follows.

COROLLARY 5.1. *$(A^k)_{ij} \neq 0$ holds for an infinite set of values of k, iff $(A^n \cdot A^*)_{ij} \neq 0$.*

PROOF: Immediate.

COROLLARY 5.2. *There is a k such that $A^k = 0$, iff $A^n = 0$; i.e., A is nilpotent iff $A^n = 0$.*

PROOF: A is nilpotent iff $A^k = 0$ for any $k \geqq k_0$ and for some k_0. Hence A is nilpotent iff $A^n \cdot A^* = 0$. But $A^n \leqq A^n \cdot A^*$ and therefore, A is nilpotent iff $A^n = 0$.

C. INVERTIBLE AND ORTHOGONAL $\mathfrak{L}_n$-MATRICES

In this section, a generalization and development of R. D. Luce's discussion on invertible Boolean matrices is given.

DEFINITION 3. An $\mathfrak{L}_n$-matrix A is called a *unit* iff there is an $\mathfrak{L}_n$-matrix B such that $AB = BA = I$. A is called *orthogonal* iff $AA^\tau = A^\tau A = I$.

LEMMA 2. (i) *If* $CB = E$ *then* $EB = E$;
(ii) *If* $EAB = E$ *then* $EB = E$;
(iii) $EA = E$ iff $I \leqq A^\tau A$.

PROOF: (i) It is always true that $EB \leqq E$ and $C \leqq E$. Therefore (by property 8 in section 2) $CB \leqq EB$, i.e., $CB = E$ implies $E \leqq EB$. Thus, $CB = E$ implies $EB = E$.

(ii) This is a special case of (i).

(iii) $EA = E$ holds iff for each i and j

$$1 = (EA)_{ij} = \sum_{\nu=1}^{n} E_{i\nu}A_{\nu j} = \sum_{\nu=1}^{n} A_{\nu j}$$

$$= \sum_{\nu=1}^{n} A_{\nu j} \cdot A^\tau{}_j = \sum_{\nu=1}^{n} (A^\tau)_{j\nu}A_{\nu j} = (A^\tau A)_{ij} ;$$

hence $Ea = E$ holds iff $I \leqq A^\tau A$ holds.

REMARK. Note that by Lemma 2(i), $I \leqq A^\tau A$ implies $EA = E$: since $I \leqq A^\tau A$ implies $EI \leqq EA^\tau A$, that is, $I \leqq A^\tau A$ implies $EA^\tau A = E$.

THEOREM 6. *If* A *is a unit then* A *is orthogonal.*

PROOF: If A is a unit then there is a B such that $AB = BA = I$ and therefore $B^\tau A^\tau = A^\tau B^\tau = I$ too. Hence, $E = EAB = EBA = EB^\tau A^\tau = EA^\tau B^\tau$, and therefore, by Lemma 2, we have $I \leqq A^\tau A$, $I \leqq AA^\tau$, $I \leqq B^\tau B$ and $I \leqq BB^\tau$.

Thus, in order to prove that A i orthogonal, it is sufficient to show that $A^\tau A \leqq I$ and $AA^\tau \leqq I$ hold, i.e., to show that $A^\tau A \leqq BA$ and $AA^\tau \leqq AB$ hold. For this, it is suficient to show that $A^\tau \leqq B$ holds and to apply property 8 in Section II, A.

Now, since $I \leqq B^\tau B$ holds, by property 8 in section 2, we have $A^\tau \leqq A^\tau B^\tau B$, but $A^\tau B^\tau = I$ and therefore $A^\tau \leqq B$ holds and the theorem follows.

THEOREM 7. *If* $AB = I$ *then* A *and* B *are roots of* I.

PROOF: By Corollary 1.1 there are natural number k_1, k_2, l_1, and l_2 such that $k_1 > k_1$, $l_2 > l_1$, $A^{k_1} = A^{k_2}$ and $B^{l_1} = B^{l_2}$. If $I = AB$ then clearly

$$I = A^{k_1}B^{k_1} = A^{k_2}B^{k_2} = A^{l_1}B^{l_1} = A^{l_2}B^{l_2}.$$

Thus

$$I = A^{l_2}B^{l_2} = A^{l_2}B^{l_1} = A^{l_2-l_1}(A^{l_1}B^{l_1}) = A^{l_2-l_1}.$$

$$I = A^{k_2}B^{k_2} = A^{k_1}B^{k_2} = (A^{k_1}B^{k_1})B^{k_2-k_1} = B^{k_2-k_1}.$$

Hence A and B are roots of I.

The proofs of the following corollaries are immediate.

COROLLARY 7.1. *If A has some inverse then A is a unit.*

COROLLARY 7.2. *A is orthogonal* iff *A is a root of I.*

COROLLARY 7.3. *A is orthogonal* iff *one of the following holds:*

(i) *for each B there is an X such that $XA = B$;*

(ii) *for each B there is an X such that $AX = B$.*

From Lemma 2 we can derive a structural characterization of the orthogonal $\mathfrak{L}_n$-matrices; and furthermore, we can establish a connection between these and the $n \times n$ permutation matrices which are the orthogonal $\mathfrak{L}_n$-matrices whose elements are 0 and 1.

DEFINITION 4. a. A set $\{a_1, a_2, \cdots, a_m\}$ of elements of $\mathfrak{L}$ is a *decomposition of* 1 *in* $\mathfrak{L}$ iff $\sum_{\nu=1}^{m} a_\nu = 1$.

b. A set $\{a_1, a_2, \cdots, a_m\}$ of elements of $\mathfrak{L}$ is orthogonal iff $a_\mu a_\nu = 0$ holds for any μ and ν provided that $\mu \neq \nu$.

c. A set of elements of $\mathfrak{L}$ is an *orthogonal decomposition of* 1 *in* $\mathfrak{L}$ iff it is orthogonal and a decomposition of 1 in $\mathfrak{L}$.

d. An $\mathfrak{L}_n$-matrix is a $\mathfrak{B}_n$-*matrix* iff all its elements are 0 or 1.

e. An $\mathfrak{L}_n$-matrix A is an *orthogonal combination of* $\mathfrak{B}_n$-*matrices* iff there is an orthogonal decomposition of 1 in $\mathfrak{L}$, $\{a_i, a_2, \cdots, a_m\}$, and a set of $\mathfrak{B}_n$-matrices, $\{A_1, A_2, \cdots, A_m\}$, such that $A = \sum_{\nu=1}^{m} a_\nu A_\nu$.

From Lemma 2 we can immediately infer that an $\mathfrak{L}_n$-matrix A is orthogonal iff $EA = EA^\tau = E$, $AA^\tau \leqq I$ and $A^\tau A \leqq I$. Applying the terminology introduced in Definition 4 we get:

LEMMA 3. *A $\mathfrak{L}_n$-matrix is orthogonal* iff *each row and each column of it is an orthogonal decomposition of* 1 *in* $\mathfrak{L}$.

This leads us to the following theorem:

THEOREM 8. *An $\mathfrak{L}_n$-matrix is orthogonal* iff *it is an orthogonal combination of orthogonal $\mathfrak{B}_n$-matrices.*

PROOF: If A is such a combination, say $A = \sum_{\nu=1}^{m} a_\nu A_\nu$, then

$$AA^\tau = \left(\sum_{\mu=1}^{m} a_\mu A_\mu\right) \cdot \left(\sum_{\nu=1}^{m} a_\mu A_\nu\right)^\tau$$

$$= \sum_{\mu=1}^{m} \sum_{\nu=1}^{m} a_\mu a_\nu A_\mu A_\nu{}^\tau$$

$$= \sum_{\nu=1}^{m} a_\nu a_\nu A_\nu A_\nu'$$

$$= \sum_{\nu=1}^{m} a_\nu I = (\sum_{\nu=1}^{m} a_\nu) I = I,$$

hence A is orthogonal.

If A is orthogonal then, by Lemma 3, each row and each column of A is an orthogonal decomposition of 1 in $\mathfrak{L}$. Therefore, the set of all the products of any n elements which occur in different n entries of A, is also an orthogonal decomposition of 1 in $\mathfrak{L}$ (which is, in fact, a "refinement" of the rows and the columns of A). Let us denote the elements of this set by $a_1, a_2, \cdots, a_m$. It is clear that for each a_ν and for each entry of A, $a_\nu A_{ij}$ is equal either to 0 or to a_ν. Therefore, there is a unique $\mathfrak{B}_n$-matrix A_ν such that $a_\nu A = a_\nu A_\nu$ holds. Moreover, applying Lemma 3 on A and on A_ν, one can prove that A_ν is orthogonal. Clearly,

$$\sum_{\nu=1}^{m} a_\nu A_\nu = \sum_{\nu=1}^{m} a_\nu A = (\sum_{\nu=1}^{m} a_\nu) A = A.$$

RECEIVED: November 14, 1963

REFERENCES

BIRKHOFF, G. (1961), "Lattice Theory," Am. Math. Soc. Colloq. Publ., Vol. XXV.

GIVE'ON Y. (J. GIVEON) (1962), Lattice matrices and finite automata. Tech. Rept. No. 8, Applied Logic Branch, The Hebrew University of Jerusalem, Israel.

HOHN, R. E. AND SCHISSLER, R. L. (1955), Boolean matrices and the design of combinatorial relay switching circuits. *Bell System Tech. J.* **34**, 177–202.

LUCE, R. D. (1952), A note on Boolean matrix theory. *Proc. Am. Math. Soc.* **3**, 382–388.

LUNTS, A. G. (1950), The application of Boolean matrix algebra to the analysis and synthesis of relay contact network (in Russian). *Dokl. Akad. Nauk. SSSR*, **70**, 421–423.

YOELI, M. (1959), Mathematical theory of switching nets. Unpublished thesis, Technion-Israel, Institute of Technology, Haifa, Israel.