A NOTE ON BOOLEAN MATRIX THEORY[1]

R. DUNCAN LUCE

1. Introduction. Let U be a Boolean algebra of at least two elements. If a, $b \in U$, intersection, union, complementation, and inclusion are denoted by $a \cap b$, $a \cup b$, a', and $a \subset b$ respectively. Form the set V of matrices A, B, $\cdots$ of order n having entries A_{ij}, B_{ij}, $\cdots$, $i, j = 1, 2, \cdots, n$, which are members of U. The restriction to square matrices is inessential to some of the theorems; in particular, Theorems 5.1 and 5.2 are true for rectangular matrices which are subject to the usual restrictions on the range of the indices to make the indicated multiplication and equality meaningful.

In the set V define intersection, union, complementation, and inclusion by:

$$(A \cap B)_{ij} = A_{ij} \cap B_{ij}, \quad (A \cup B)_{ij} = A_{ij} \cup B_{ij}, \quad (A')_{ij} = A'_{ij},$$

$A \subset B$ if and only if for every i, j, $A_{ij} \subset B_{ij}$.

Under these definitions V forms a Boolean algebra, which is known as the algebra of Boolean matrices.[2]

A multiplication may be defined in V as follows:

$$(AB)_{ij} = \bigcup_{k=1}^{n} (A_{ik} \cap B_{kj}).$$

If o and e are the null and universal elements of U, then the zero (null), identity, and universal matrices O, I, and E are defined as:

$$(O)_{ij} = o, \quad (I)_{ij} = o \text{ if } i \neq j \text{ and } e \text{ if } i = j, \quad (E)_{ij} = e.$$

Under these definitions and the given multiplication, V forms a lattice-ordered semigroup with zero.[3]

As in ordinary matrix theory the transpose of A, A^T, is defined by $(A^T)_{ij} = A_{ji}$ and the elements of the transpose will be denoted by A_{ij}^T.

The following properties follow either immediately from the definitions or by virtue of V being a lattice-ordered semigroup:

$A(B \cup C) = AB \cup AC, \qquad (B \cup C)A = BA \cup CA,$

$A(B \cap C) \subset AB \cap AC, \qquad (B \cap C)A \subset BA \cap CA,$

$A(BC) = (AB)C, \ A \subset B$ implies $AC \subset BC$ and $CA \subset CB$ for all $C,$

$O \cap A = OA = AO = O$ and $IA = AI = A$ for all $A,$

$(A \cup B)^T = A^T \cup B^T, \qquad (A \cap B)^T = A^T \cap B^T,$

$\qquad (AB)^T = B^T A^T, \qquad (A^T)^T = A,$

$EE = E, \ O \subset A \subset E$ and $A \subset AE \subset E, \ A \subset EA \subset E$ for all $A.$

2. Symmetry and skew-symmetry. In analogy to ordinary matrix theory we wish to define concepts of symmetry and skew-symmetry; it is clear that the formal definition of symmetry may be carried over without change, but this is not true for skew-symmetry. Our choice for the latter (Definition 2) has in its favor a form parallel to one definition of symmetry and that it allows Theorem 2.1 to be proved.

DEFINITION 1. A Boolean matrix A is said to be symmetric if $A^T \cap A' = O.$

DEFINITION 2. A Boolean matrix A is said to be skew-symmetric if $A^T \cap A = O.$

Evidently the property $A = A^T$ implies A is symmetric, and conversely it is implied by symmetry for $A^T \cap A' = O$ implies $A^T \subset A.$ Taking the transpose, $A \subset A^T,$ whence $A = A^T.$ It is equally easy to show that A is skew-symmetric if and only if $A = A \cap A^{T'}.$ Moreover, A is skew-symmetric if for some $B, A = B \cap B^{T'}.$ For if there exists such a $B,$ then $A' = B' \cup B^T$ and so $A^T = B^T \cap B' \subset B^T \cup B' = A',$ whence $A^T = A^T \cap A',$ or what is the same, $A = A \cap A^{T'}.$

By the properties of the transpose mentioned in §1 one easily proves that symmetry is a property invariant under union, intersection, and complementation. Skew-symmetry is invariant under intersection, for if $A \cap A^T = O$ and $B \cap B^T = O,$ then $(A \cap A^T) \cap (B \cap B^T) = O = (A \cap B) \cap (A \cap B)^T.$ It is not, however, invariant under complementation as

$$A = \begin{bmatrix} o & e \\ o & o \end{bmatrix}$$

shows, nor under union as A and

$$B = \begin{bmatrix} o & o \\ e & o \end{bmatrix}$$

show.

THEOREM 2.1. *Any Boolean matrix can be uniquely decomposed into*

the disjoint union of a symmetric and a skew-symmetric matrix.

PROOF. If A is so decomposed, the decomposition is unique. For if $A = S \cup Q$ where $S \cap Q = O$, $S = S^T$, and $Q^T \cap Q = O$, then

$$A \cap A^T = (S \cup Q) \cap (S \cup Q^T)$$
$$= (S \cap S) \cup (S \cap Q^T) \cup (Q \cap S) \cup (Q \cap Q^T)$$
$$= S \cup (S^T \cap Q^T) \cup O \cup O = S \cup (S \cap Q)^T = S;$$
$$A \cap A^{T\prime} = (S \cup Q) \cap (S' \cap Q^{T\prime}) = (S \cap S' \cap Q^{T\prime}) \cup (Q \cap S' \cap Q^{T\prime})$$
$$= O \cup (S' \cap Q) = Q$$

since $Q \subset Q^{T\prime}$ and $Q \subset S'$.

Selecting $S = A \cap A^T$ and $Q = A \cap A^{T\prime}$ proves that the decomposition exists.

3. Consistent matrices.

DEFINITION 3. A Boolean matrix A is said to be row (column) consistent if $AE = E$ ($EA = E$).

LEMMA 3.1. *A is row (column) consistent if and only if $I \subset AA^T$ ($I \subset A^T A$).*

PROOF. By definition $I \subset AA^T$ if and only if $e = \cup_j (A_{ij} \cap A_{ji}^T)$ $= \cup_j A_{ij} = \cup_j (A_{ij} \cap E_{jk})$ for every i, k. This, by definition, is equivalent to $E = AE$.

LEMMA 3.2. (1) *If A and B are row (column) consistent, then AB is row (column) consistent.* (2) *If AB is row (column) consistent, then A is row consistent (B is column consistent).* (3) *Neither converse is true.*

PROOF. (1) By hypothesis $AE = E$ and $BE = E$; so $(AB)E = A(BE)$ $= AE = E$. (2) By hypothesis $(AB)E = E$ and it is always true that $AE \subset E$ and $BE \subset E$; so $E = (AB)E = A(BE) \subset AE$, whence $AE = E$.

$$(3) \quad \begin{bmatrix} e & o \\ e & o \end{bmatrix} \begin{bmatrix} e & o \\ o & o \end{bmatrix} = \begin{bmatrix} e & o \\ e & o \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} o & e \\ o & e \end{bmatrix} \begin{bmatrix} e & e \\ o & o \end{bmatrix} = \begin{bmatrix} o & o \\ o & o \end{bmatrix}.$$

This lemma states, in the terminology introduced by Dubreil for semigroup theory,[4] that under multiplication the set of row (column) consistent matrices forms a left (right) consistent subsemigroup of V.

The introduction of the concept of a consistent matrix suggests that at the other extreme of the relation $A \subset AE \subset E$ we might consider matrices A such that $AE = A$. Such a definition would be a slight

---

[4] P. Dubreil, *Contribution à la théorie de demi-groups*, Mémoires de l'Académie des Sciences de l'Institut de France (2) vol. 63 (1941).

generalization of the concept of a right ideal element in a relation algebra;[5] however, these matrices do not seem to be as important as consistent matrices. It may be mentioned, nonetheless, that the class of all ideal matrices (i.e., both left and right ideal) is a Boolean subalgebra isomorphic to the given algebra U.

4. **Inverses.** We shall denote the *inverse* of a matrix A, if it exists, by A^{-1}. Following the terminology of ordinary matrix theory a matrix A is called *orthogonal* if it has an inverse which is A^T. For example,

$$\begin{bmatrix} o & e \\ e & o \end{bmatrix}$$

is orthogonal. It is immediate that the product of two orthogonal matrices is orthogonal.

LEMMA 4.1. *A Boolean matrix A is orthogonal if and only if A is both row and column consistent and for every i, j, k, $i \neq j$, $A_{ik} \cap A_{jk} = o = A_{ki} \cap A_{kj}$.*

PROOF. If A is orthogonal, Lemma 3.1 implies that A is row and column consistent. For every i, j, $i \neq j$, $AA^T = I$ implies

$$o = \bigcup_k (A_{ik} \cap A_{kj}^T) = \bigcup_k (A_{ik} \cap A_{jk}),$$

whence for every k, $A_{ik} \cap A_{jk} = o$. Similarly, $A_{ki} \cap A_{kj} = o$ for every i, j, k, $i \neq j$, follows from $A^T A = I$.

Conversely, if $A_{ik} \cap A_{jk} = o$ for every i, j, k, $i \neq j$, then $\bigcup_k (A_{ik} \cap A_{jk}) = \bigcup_k (A_{ik} \cap A_{kj}^T) = o$, whence $AA^T \subset I$. Since A is row consistent, Lemma 3.1 implies $I \subset AA^T$, and so $AA^T = I$. Similarly $A^T A = I$.

THEOREM 4.2. *A Boolean matrix has an inverse if and only if it is orthogonal.*[6]

PROOF. The sufficiency is true by definition.

By Lemma 3.2, if A has an inverse, both A and A^{-1} are row and column consistent. Thus, using Lemma 4.1, it is sufficient to show $A_{ik} \cap A_{jk} = o = A_{ki} \cap A_{kj}$ for every i, j, k, $i \neq j$. We shall carry this out only for the first case as the other is essentially the same. $AA^{-1} = I$ implies that for every i, j, $i \neq j$, $\bigcup_k (A_{ik} \cap A_{kj}^{-1}) = o$, whence, for every

[5] Birkhoff, op. cit., p. 212.

[6] This result is stated by J. H. M. Wedderburn, Ann. of Math. vol. 35 (1934) pp. 185–194.

k, $A_{ik} \cap A_{kj}^{-1} = o$; summing over j, $j \neq i$, and holding k fixed, we have $\bigcup_{j \neq i} (A_{ik} \cap A_{kj}^{-1}) = o$. Thus,

$$A_{ik} \cap A_{ki}^{-1} = \bigcup_{j \neq i} (A_{ik} \cap A_{kj}^{-1}) \cup (A_{ik} \cap A_{ki}^{-1}) = \bigcup_{j} (A_{ik} \cap A_{kj}^{-1})$$

$$= A_{ik} \cap \bigcup_{j} A_{kj}^{-1} = A_{ik}$$

since $\bigcup_j A_{kj}^{-1} = e$ because A^{-1} is row consistent. Now, for every i, j, k, $i \neq j$,

$$A_{ik} \cap A_{jk} = (A_{ik} \cap A_{ki}^{-1}) \cap (A_{jk} \cap A_{kj}^{-1})$$

$$= (A_{ik} \cap A_{kj}^{-1}) \cap (A_{jk} \cap A_{ki}^{-1}) = o.$$

Hence A is orthogonal.

COROLLARY. *A is involutory $(A^2 = I)$ if and only if A is both symmetric and orthogonal.*

PROOF. Immediate.

5. **Linear matrix equations.** In this section we shall consider the problem of finding the class of matrices X such that $XA = B$ $(AX = B)$ when A and B are given Boolean matrices.[7] This is clearly equivalent to finding the intersection of the two classes of matrices X satisfying $XA \subset B$ and $XA \supset B$. The former case is relatively simple and is completely solved; however, the latter is much more difficult. We have been able only to give a sufficiency condition on X, which is not necessary, for X to be a solution of $XA \supset B$. We also present a necessary and sufficient condition on A and B that there be solutions to $XA = B$.

Utilizing the solutions to $XA \subset O$ (hence in this special case the complete set of solutions to $XA = O$), we completely characterize the divisors of zero occuring in the algebra of Boolean matrices.

It is clear from the previous section that if A is orthogonal, $X = BA^T$ is the unique solution of $XA = B$, but in general a solution will not be unique.

Toward our ends we prove the following lemma.

LEMMA 5.1. *Let A, B, and C be Boolean matrices. $ABC \subset I'$ if and only if $A' \supset (BC)^T$.*

PROOF. By definition $ABC \subset I'$ if and only if, for every i, $\bigcup_j \bigcup_k (A_{ij} \cap B_{jk} \cap C_{ki}) = o$ or, what is the same, $A_{ij} \cap B_{jk} \cap C_{ki} = o$ for

[7] The results of this section are generalizations of work by D. O. Ellis and J. W. Gaddum as stated in Bull. Amer. Math. Soc. Abstract 56-5-448.

every i, j, k. Rewriting, we have $A'_{ij} \supset B_{jk} \cap C_{ki} = C_{ik}^T \cap B_{kj}^T$. Since the left side is independent of the index k, this is equivalent to $A'_{ij} \supset U_k(C_{ik}^T \cap B_{kj}^T)$, that is, $A' \supset C^T B^T = (BC)^T$.

Birkhoff defines for any multiplicative lattice[8] the *right (left)* *residual* $B:A$ $(B::A)$ of B by A as the largest X (if it exists) satisfying $XA \subset B$ $(AX \subset B)$. A multiplicative lattice in which such residuals always exist is called a *residuated lattice*.[9]

THEOREM 5.2. *In the algebra of Boolean matrices* $XA \subset B$ *if and only if* $X \subset (B'A^T)'$, *and* $AX \subset B$ *if and only if* $X \subset (A^T B')'$; *hence the algebra is residuated and* $B:A = (B'A^T)'$ *and* $B::A = (A^T B')'$.

PROOF. $XA \subset B$ means by definition that $U_j(X_{ij} \cap A_{jk}) \subset B_{ik}$ for every i, k, and this is equivalent to $X_{ij} \cap A_{jk} \subset B_{ik}$, $i, j, k = 1, 2, \cdots$, n. This in turn is true if and only if $X_{ij} \cap A_{jk} \cap B'_{ik} = X_{ij} \cap A_{jk} \cap B'^T_{ki} = o$. Summing on j and k, $U_j U_k(X_{ij} \cap A_{jk} \cap B'_{ki}) = o$, which means, by definition, that $XAB'^T = XAB^{T'} \subset I'$. According to Lemma 5.1, this is true if and only if $X' \supset (AB'^T)^T$, that is, if and only if $X \subset (B'A^T)'$. A similar proof holds for $AX \subset B$.

COROLLARY 1. *The following are equivalent*: $XA = O$, $X \subset (AE)^{T'}$, $EX \subset (AE)^{T'}$. *A similar statement holds for* $AX = O$.

PROOF. Since it is always true that $O \subset XA$, it is sufficient to consider $XA \subset O$, which by the theorem is equivalent to $X \subset (O'A^T)' = (EA^T)' = (AE)^{T'}$. This is equivalent to $X' \supset (AE)^T$ and hence to $X'_{ij} \supset U_k(E_{ik} \cap A_{kj}^T) = U_k A_{kj}^T$ for every i, j. Since the right side of this expression is independent of i, it is the same as $U_k A_{kj}^T \subset \cap_i X'_{kj} = \cap_k(O_{ik} \cup X'_{kj}) = [U_k(E_{ik} \cap X_{kj})]'$. Rewriting, we have $EA^T \subset (EX)'$ and so $EX \subset (AE)^{T'}$.

As was mentioned in the introduction, this theorem and its corollaries are not restricted to square matrices; however the usual restrictions on the ranges of the indices are required. With this in mind, we may restrict X and B to be vectors; then Corollary 1 becomes, essentially, the first principal result of Ellis and Gaddum.[7] Their second result is included in the following corollary.

COROLLARY 2. $XA = B$ *has a solution if and only if* $B \subset (B'A^T)'A$.

PROOF. If there is a solution X, the theorem implies $X \subset (B'A^T)'$; however, $XA = B$ also implies $B \subset XA \subset (B'A^T)'A$.

Conversely, if $B \subset (B'A^T)'A$, then $X = (B'A^T)'$ is a solution for the hypothesis implies $XA \supset B$ and the theorem $XA \subset B$.

---

[8] Birkhoff, op. cit., p. 200.

[9] Ibid., p. 201.

In the first part of their third result Ellis and Gaddum note that if X solves $XA \subset B$, then, since $X \subset (B'A^T)'$, X may be written in parametric form $X = R \cap (B'A^T)'$ with R an arbitrary matrix. If, however, X is to solve $XA = B$, R may no longer be arbitrary. The second part of their third result is a statement of conditions on R necessary and sufficient for X to be a solution. These are trivial, for they may easily be shown equivalent (in the case X and B are vectors) to the following trivial result:

COROLLARY 3. $XA = B$ has the solution $X = R \cap (B'A^T)'$ if and only if $B \subset [R \cap (B'A^T)']A$.

THEOREM 5.3. Let A and B be Boolean matrices of the same order. If there exists a matrix C such that $C \subset A$ and $B \subset EC$, then all matrices X such that $X \supset BC^T$ are solutions of $XA \supset B$.

PROOF. If such a C exists, it is sufficient to show $BC^TA \supset B$ since $XA \supset BC^TA$. For every i, l,

$$\bigcup_j \bigcup_k (B_{ij} \cap C_{jk}^T \cap A_{kl}) \supset B_{il} \cap \bigcup_k (C_{ik}^T \cap A_{kl}) \supset B_{il} \cap \bigcup_k C_{kl}$$

since $C \subset A$. From the assumption $B \subset EC$ we obtain $B_{il} \subset \bigcup_k C_{kl}$, so the result follows by definition.

The condition of this theorem is by no means necessary for if $A = B = E$, then $X = I$ is a solution. Now suppose the C of the theorem satisfies $I \supset BC^T = EC^T$. Then for every $i, j, i \neq j$, $o = \bigcup_k (E_{ik} \cap C_{kj}^T) = \bigcup_k C_{jk}$, and so for every j and k, $C_{jk} = o$. $C = O$ contradicts the condition $B = E \subset EC$.

In the theory of semigroups with a zero element, an element A is a *right divisor of zero* if $A \neq O$ and there exists an element $B \neq O$ such that $BA = O$.

THEOREM 5.4. A Boolean matrix A is a right (left) divisor of zero if and only if A is not row (column) consistent.

PROOF. Suppose $BA = O$ and A is row consistent, then, by Corollary 1 of Theorem 5.2, $B \subset (AE)^{T'} = E^{T'} = O$, so A is not a right divisor of zero.

Conversely, if A is not row consistent, there exists some integer p such that $\bigcup_q A_{pq} \neq e$. Define: $B_{pp} = (\bigcup_q A_{pq})'$ and $B_{ij} = o$ otherwise, whence $B \neq O$. Consider BA: if $i \neq p$, $\bigcup_k (B_{ik} \cap A_{kj}) = o$ since $B_{ik} = o$. If $i = p$, $\bigcup_k (B_{pk} \cap A_{kj}) = B_{pp} \cap A_{pj} = (\bigcup_q A_{pq})' \cap A_{pj} \subset A_{pj}' \cap A_{pj} = o$. Thus $BA = O$ and $A, B \neq O$, so A is a right divisor of zero.

UNIVERSITY OF MICHIGAN