RESIDUATION THEORY AND BOOLEAN MATRICES

by T. S. BLYTH

(Received 26 September, 1963, and in revised form 17 January, 1964)

We begin this paper by considering a Boolean algebra as a lattice which is relatively pseudo-complemented (i.e., residuated with respect to intersection) and give, in this case, certain properties of the equivalences of types A, B and F (as introduced by Molinaro [**1**]). We then show how these results carry over to the case of Boolean matrices, which form a Boolean algebra residuated also with respect to matrix multiplication. Other properties of matrix residuals are established and we conclude with three algebraic characterisations of invertible Boolean matrices.

1. By an *ordered groupoid* we mean simply a set G of elements on which is defined (a) a closed binary multiplication, and (b) a partial ordering $\leqq$ with respect to which the multiplication is isotone (i.e., $x \leqq y \Rightarrow zx \leqq zy$ and $xz \leqq yz$, $\forall z \in G$).

The ordered groupoid G is said to be *residuated on the left* (*right*) if, given $a, b \in G$, the set of elements $x \in G$ satisfying $xa \leqq b$ ($ax \leqq b$) is not empty and has a maximum element, denoted by $b \cdot .a$ ($b . \cdot a$) and called the *left* (*right*) *residual of b by a*.

An ordered groupoid in which both left and right residuals exist for every pair of elements is said to be *residuated*.

We refer to [**1**, Chapter 1] for the general properties of residuals.

Now in the general theory of residuated groupoids, an important rôle is played by the equivalences of types A, B and F. These equivalences are introduced as follows [**1**, Chapter 1]. With each element x of the groupoid, we associate

(α) *equivalences of type A*, defined by

$$\begin{cases} a \equiv b(A_x) \Leftrightarrow x . \cdot a = x . \cdot b \\ a \equiv b({}_xA) \Leftrightarrow x \cdot .a = x \cdot .b, \end{cases}$$

(β) *equivalences of type B*, defined by

$$\begin{cases} a \equiv b(B_x) \Leftrightarrow a . \cdot x = b . \cdot x \\ a \equiv b({}_xB) \Leftrightarrow a \cdot .x = b \cdot .x, \end{cases}$$

(γ) *equivalences of type F*, defined by

$$\begin{cases} a \equiv b(F_x) \Leftrightarrow xa = xb \\ a \equiv b({}_xF) \Leftrightarrow ax = bx. \end{cases}$$

These equivalences possess many interesting properties, of which we mention only the following.

(α^*) [**1**, p. 332, Th. 2^a] Each class modulo A_x [resp. ${}_xA$] has a maximum element, the maximum element in the class of y being the element $x \cdot .(x . \cdot y)$ [resp. $x . \cdot (x \cdot .y)$].

(β^*) [**1**, p. 338, Th. 2^b] Each class modulo B_x [resp. ${}_xB$] has a minimum element, the minimum element in the class of y being the element $x(y . \cdot x)$ [resp. $(y \cdot .x)x$].

(γ^*) [**1**, p. 342, Th. 2^f] Each class modulo F_x [resp. ${}_xF$] has a maximum element, the maximum element in the class of y being the element $xy . \cdot x$ [resp. $yx \cdot .x$].

https://doi.org/10.1017/S2040618500034997 Published online by Cambridge University Press

Consider now a Boolean algebra B. It is well known that B is residuated with respect to the multiplication defined by $xy = x \cap y$ and that residuals (called relative pseudo-complements in this case) are given by

$$x : y = x \cup y', \tag{1}$$

where y' denotes the complement of y in B, and $x : y$ means $x.\,{}^{\cdot}y$ or $x^{\cdot}\,.y$, these residuals being equal since the multiplication is commutative.

In this case, we have the following two results:

THEOREM 1. $A_{x'} = F_x$.

Proof. By (1) and the de Morgan laws, we have

$$\begin{aligned} x' : (x' : y) &= x' \cup (x' : y)' = x' \cup (x' \cup y')' \\ &= x' \cup (x \cap y) = x' \cup y \\ &= x' \cup xy = xy : x. \end{aligned} \tag{2}$$

Using (α^*) and (γ^*), it is then easily seen from this equality that $y \equiv z(A_{x'}) \Leftrightarrow y \equiv z(F_x)$.

THEOREM 2. $y \equiv z(B_x) \Leftrightarrow y' \equiv z'(A_{x'})$.

Proof. From the equality (2) obtained above, we have

$$\begin{aligned} [x' : (x' : y')]' &= (x' \cup y')' = x \cap y = (x \cap y) \cup 0 \\ &= (x \cap y) \cup (x \cap x') = x \cap (y \cup x') = x \cap (y : x) = x(y : x). \end{aligned}$$

The result is then an immediate consequence of (α^*) and (β^*).

2. Consider now the set $M_n(B)$ of all $n \times n$ matrices $X = [x_{ij}]$, $i, j = 1, 2, \ldots, n$, whose elements x_{ij} lie in a given Boolean algebra B. It is well known that $M_n(B)$ is a Boolean algebra with respect to the partial ordering $\preccurlyeq$ defined by

$$X \preccurlyeq Y \quad \Leftrightarrow \quad x_{ij} \leqq y_{ij} \quad \text{for all } i, j,$$

and is residuated also with respect to the matrix multiplication defined by

$$XY = Z \quad \Leftrightarrow \quad \bigcup_j (x_{ij} \cap y_{jk}) = z_{ik}. \tag{3}$$

Note that in this case multiplication is not the same as intersection; the question arises, therefore, as to whether relationships similar to those of §1 exist between the equivalences of types A, B and F when residuals are taken with respect to the multiplication defined in (3). We shall show in fact that Theorems 1 and 2 above carry over with a slight modification. Firstly, we give a few preliminary results.

Though we cannot use the formula (1) for matrix residuals with respect to the multiplication defined in (3), we do have the following formulae (first given by Luce [2]):

$$\left.\begin{aligned} X.\,{}^{\cdot}Y &= (Y^T X')', \\ X^{\cdot}\,.Y &= (X' Y^T)', \end{aligned}\right\} \tag{4}$$

https://doi.org/10.1017/S2040618500034997 Published online by Cambridge University Press

where Y^T denotes the transpose of Y and X' the complement of X in $M_n(B)$, i.e. the matrix $[x'_{ij}]$ where x'_{ij} denotes the complement of x_{ij} in B.

THEOREM 3.

$$(a)\ [X.\,{}^{\cdot}Y]^T = Y'.\,{}^{\cdot}X' = X^{T\cdot}.Y^T,$$
$$(b)\ [X^{\cdot}.Y]^T = Y''.X' = X^T.\,{}^{\cdot}Y^T.$$

Proof. Using (4), we have

$$[X.\,{}^{\cdot}Y]^T = [(Y^TX')']^T = [(Y^TX')^T]' = [(X')^T(Y^T)^T]'$$
$$= \begin{cases} [(X^T)'(Y^T)^T]' = X^{T\cdot}.Y^T \\ [(X')^T(Y')']' = Y'.\,{}^{\cdot}X'. \end{cases}$$

The proof of (*b*) is similar.

THEOREM 4.

$$(a)\ Y \equiv Z(A_X) \Leftrightarrow Y^T \equiv Z^T({}_{X^T}A),$$
$$(b)\ Y \equiv Z(B_X) \Leftrightarrow Y^T \equiv Z^T({}_{X^T}B),$$
$$(c)\ Y \equiv Z(F_X) \Leftrightarrow Y^T \equiv Z^T({}_{X^T}F).$$

Proof. (*a*) and (*b*) are immediate consequences of Theorem 3. As for (*c*), we have

$$Y \equiv Z(F_X) \Leftrightarrow XY = XZ$$
$$\Leftrightarrow (XY)^T = (XZ)^T$$
$$\Leftrightarrow Y^TX^T = Z^TX^T$$
$$\Leftrightarrow Y^T \equiv Z^T({}_{X^T}F).$$

Let P, Q be equivalences defined on $M_n(B)$. We shall write

$$P \sim Q \quad \Leftrightarrow \quad (X \equiv Y(P) \quad \Leftrightarrow \quad X' \equiv Y'(Q)).$$

In this way, Theorem 2 may be written $B_x \sim A_{x'}$, and the following result is the matrix analogue of the results stated in Theorems 1 and 2:

THEOREM 5.

$$(a)\ F_{X^T} = A_{X'} \sim B_X,$$
$$(b)\ {}_{X^T}F = {}_{X'}A \sim {}_XB.$$

Proof. Using (4), we have

$$X''.(X'.\,{}^{\cdot}Y) = \{X(X'.\,{}^{\cdot}Y)^T\}' = \{X[(Y^TX)']^T\}'$$
$$= \{X[(Y^TX)^T]'\}' = \{X[X^TY]'\}'$$
$$= \begin{cases} \{X[X^T(Y')']'\}' = \{X(Y'.\,{}^{\cdot}X)\}' \\ \{(X^T)^T[X^TY]'\}' = X^TY.\,{}^{\cdot}X^T. \end{cases}$$

https://doi.org/10.1017/S2040618500034997 Published online by Cambridge University Press

(a) therefore follows from these equalities using (α^*), (β^*) and (γ^*); (b) may be proved similarly, or deduced from (a) using Theorem 4.

3. In this section, we give three algebraic characterisations of *invertible* Boolean matrices. It is known [3] that if a Boolean matrix X has a one-sided inverse, that inverse is a two-sided inverse, is unique and is none other than X^T. Moreover, X has an inverse if and only if it satisfies the following Wedderburn-Rutherford conditions:

$$x'_{ij} = \bigcup_{k \neq i} a_{kj} = \bigcup_{k \neq j} a_{ik}. \tag{5}$$

DEFINITION. A matrix $X \in M_n(B)$ which is such that

$$\forall\, A, B \in M_n(B), \qquad XA = XB \Rightarrow A = B \tag{6}$$

will be called *left-cancellable.*

Similarly we define *right-cancellable* matrices.

From condition (6), the left cancellation law, it is immediate that X is left-cancellable if and only if the equivalence F_X reduces to equality; similarly, X is right-cancellable if and only if ${}_XF$ reduces to equality.

THEOREM 6. *The following conditions are equivalent in $M_n(B)$ and are necessary and sufficient for $X \in M_n(B)$ to have an inverse:*

(a) *X is left-cancellable,*

(b) *X is right-cancellable.*

Proof. If X has an inverse, then it is left-cancellable, for from $XA = XB$ we have

$$A = IA = (X^TX)A = X^T(XA) = X^T(XB) = (X^TX)B = IB = B.$$

Conversely, if X is left-cancellable, then the equivalence F_X reduces to equality. By Theorem 5, so also does the equivalence B_{X^T}. Hence in particular the unit matrix I is minimum in its class modulo B_{X^T} so that there exists a matrix $Y[= I.\,{}^{\cdot}X^T]$ such that $X^TY = I$. Hence

$$Y^TX = (X^TY)^T = I^T = I,$$

and so X has an inverse.

A similar proof shows the equivalence of the condition (b).

THEOREM 7. *$X \in M_n(B)$ has an inverse if and only if*

$$I.\,{}^{\cdot}X = I^{\cdot}.X = X^T.$$

Proof. Consider the matrices $I.\,{}^{\cdot}X$ and $I^{\cdot}.X$; by (4), we have

$$I.\,{}^{\cdot}X = (X^TI')' \quad \text{and} \quad I^{\cdot}.X = (I'X^T)',$$

so that

$$[I.\,{}^{\cdot}X]_{ik} = \left\{ \bigcup_j (x_{ji} \cap \delta'_{jk}) \right\}' = \left(\bigcup_{j \neq k} x_{ji} \right)',$$

https://doi.org/10.1017/S2040618500034997 Published online by Cambridge University Press

and similarly

$$[I^{\cdot} .X]_{ik} = \left(\bigcup_{j \neq i} x_{kj} \right)'.$$

The result then follows from the Wedderburn-Rutherford conditions (5), on interchanging dummy suffices.

The final characterisation of invertible Boolean matrices which we give is in terms of the Artin equivalences on $M_n(B)$; these are simply the equivalences of type A associated with the unit matrix I.

THEOREM 8. *$X \in M_n(B)$ has an inverse if and only if the equivalences of type A associated with X are equal to the corresponding Artin equivalences.*

Proof. Suppose that X has an inverse; then X^T also has an inverse and by Theorem 7 we have

$$X = (X^T)^T = I^{\cdot} .X^T,$$

so that

$$X^{\cdot} .X = (I^{\cdot} .X^T)^{\cdot} .X.$$

But since matrix multiplication is associative, we have the formula [**1**, p. 327]

$$(P^{\cdot} .Q)^{\cdot} .R = P^{\cdot} .RQ, \quad \forall\, P, Q, R \in M_n(B);$$

hence

$$X^{\cdot} .X = I^{\cdot} .XX^T = I^{\cdot} .I = I.$$

Again by the associativity of matrix multiplication, we also have

$$\begin{aligned} X \equiv Y(A_P) &\Rightarrow P. \,{}^{\cdot}X = P. \,{}^{\cdot}Y \\ &\Rightarrow (P. \,{}^{\cdot}X)^{\cdot} .Q = (P. \,{}^{\cdot}Y)^{\cdot} .Q \\ &\Rightarrow (P^{\cdot} .Q). \,{}^{\cdot}X = (P^{\cdot} .Q). \,{}^{\cdot}Y \quad [\mathbf{1}, \text{p. } 328] \\ &\Rightarrow X \equiv Y(A_{P^{\cdot} .Q}), \end{aligned}$$

so that

$$A_P \subseteq A_{P^{\cdot} .Q}, \quad \forall\, P, Q \in M_n(B).$$

Hence on the one hand

$$A_I \subseteq A_{I^{\cdot} .X^T} = A_X,$$

and on the other

$$A_X \subseteq A_{X^{\cdot} .X} = A_I,$$

so that $A_X = A_I$. Similarly, by taking the left-right dual, we find that ${}_XA = {}_IA$.

Conversely, suppose that (i) $A_X = A_I$ and (ii) ${}_XA = {}_IA$. The greatest element in the class of I modulo A_X is, by (α^*), the element $X^{\cdot} .(X. \,{}^{\cdot}I) = X^{\cdot} .X$. But the greatest element in the class of I modulo A_I is $I^{\cdot} .(I. \,{}^{\cdot}I) = I^{\cdot} .I = I$; hence, by virtue of (i), we have

$$X^{\cdot} .X = I.$$

https://doi.org/10.1017/S2040618500034997 Published online by Cambridge University Press

Furthermore, from (ii) and Theorem 4(a), we have also $A_{X^T} = A_I$ and so, similarly to the above, $X^{T\cdot}.X^T = I$ which, by virtue of Theorem 3(a), may be written

$$X.\,{}^{\cdot}X = I.$$

Now the greatest element in the class of X modulo A_X is $X^{\cdot}.(X.\,{}^{\cdot}X) = X^{\cdot}.I = X$, and since, by hypothesis, $A_X = A_I$, it follows that X is the greatest element in its class modulo A_I and so we may write $X = I^{\cdot}.Y$ for some $Y \in M_n(B)$. We thus have

$$I^{\cdot}.XY = (I^{\cdot}.Y)^{\cdot}.X = X^{\cdot}.X = I.$$

Now let $Z = XY$ and let us show that $Z = I$. Since $I^{\cdot}.Z = I$, we have $(I'Z^T)' = I$, so that

$$\left\{ \bigcup_j (\delta'_{ij} \cap z_{kj}) \right\}' = \delta_{ik},$$

which gives

$$\bigcup_{j \neq i} z_{kj} = \delta'_{ik} = \begin{cases} 0 & \text{if } i = k, \\ 1 & \text{if } i \neq k. \end{cases}$$

The first of these conditions yields $\bigcup_{j \neq i} z_{ij} = 0$, so that $z_{ij} = 0$ for all i, j with $i \neq j$. This result, taken in conjunction with the second condition, gives $z_{kk} = 1$ for all k. Hence we may write $z_{ij} = \delta_{ij}$ for all i, j and so $Z = I$. Since $Z = XY$, it then follows that X has an inverse and the proof is thus complete.

Note that in the above proof we showed that $Z \equiv I({}_IA) \Rightarrow Z = I$. This implies that the element I is the only element in its class modulo ${}_IA$; but it is not true in general that the Artin equivalences in $M_n(B)$ reduce to equality. In fact, from Theorem 5, A_I is equality if and only if $F_{(I')^T} = F_{I'}$ is equality, which is equivalent to I' being cancellable, which is equivalent to I' being invertible. By considering the Wedderburn-Rutherford conditions (5), it is clear that this is the case only when $n = 2$.

REFERENCES

1. I. Molinaro, Demi-groupes résidutifs, *D. ès Sc. thesis*, Paris, 1956; also *J. Math. Pures Appl.* **39** (1960), 319–356 and **40** (1961), 43–110.

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

3. D. E. Rutherford, Inverses of Boolean matrices, *Proc. Glasgow Math. Assoc.* **6** (1963), 49–53.

ST SALVATOR'S COLLEGE
ST ANDREWS

https://doi.org/10.1017/S2040618500034997 Published online by Cambridge University Press