MATRICES WITH ELEMENTS IN A BOOLEAN RING

A. T. BUTSON

1. Introduction. Let $\mathfrak{B}$ be a Boolean ring of at least two elements containing a unit 1. Form the set $\mathfrak{M}$ of matrices $A, B, \ldots$ of order n having entries $a_{ij}, b_{ij}, \ldots$ $(i, j = 1, 2, \ldots, n)$, which are members of $\mathfrak{B}$. A matrix U of $\mathfrak{M}$ is called *unimodular* if there exists a matrix V of $\mathfrak{M}$ such that $VU = I$, the identity matrix. Two matrices A and B are said to be *left-associates* if there exists a unimodular matrix U satisfying $UA = B$. The main results in this paper are the constructions of two canonical forms for left-associated matrices of $\mathfrak{M}$. The first form may be described very simply; however, it lacks the desirable property of containing the maximum possible number of rows which consist entirely of 0's. Although the second has this property, its description is quite complicated. They are somewhat similar to the well-known Hermite form for matrices with elements in a principal ideal ring **(4)**; and, accordingly, use is made of them to establish analogues of several other familiar results concerning matrices with elements in a principal ideal ring. Although row equivalence (left-associativity) and a diagonal canonical form for equivalent matrices of $\mathfrak{M}$ are mentioned in **(2**, pp. 164–165**)**, the author has been unable to locate his results anywhere in the literature.

2. Properties of $\mathfrak{B}$. A Boolean ring may be defined as a ring whose elements are all idempotent. It is easily shown, see **(2**, pp. 154–155**)**, that it is a commutative ring of characteristic two, in the usual sense. Then for any x in $\mathfrak{B}$, the element $x' = 1 + x$, called the complement of x, satisfies $x + x' = 1$, $xx' = 0$, and $(x')' = x$. Bell **(1)** observed that $x \vee y = x + x'y$ is the g.c.d. of x and y. Following is a summary of the less obvious but easily established properties of $\mathfrak{B}$ which we shall use in the sequel:

(2.1) $xx = x$;

(2.2) $xy = yx$;

(2.3) $x + x = 0$;

(2.4) $x + x' = 1, xx' = 0, (x')' = x$;

(2.5) $\bigvee_{i=1}^{n} x_i = x_1 \vee x_2 \vee \ldots \vee x_n = x_1 + x_1'x_2 + x_1'x_2'x_3 + \ldots + x_1'x_2' \ldots x_{n-1}'x_n$ is the g.c.d. of $x_1, x_2, \ldots, x_n$;

(2.6) $\left(\sum_{j=1}^{t} x_j\right)\left(\bigvee_{i=1}^{n} x_i\right) = \sum_{j=1}^{t} x_j, \quad t = 1, 2, \ldots, n$;

Received March 4, 1956.

$$(2.7)\quad \left(\bigvee_{i=1}^{n} x_i\right)' = x_1'x_2'\ldots x_n', \quad (x_1x_2\ldots x_n)' = \bigvee_{i=1}^{n} x_i';$$

$$(2.8)\quad \bigvee_{i=1}^{n} x_i = 0 \text{ if and only if } x_1 = x_2 = \ldots = x_n = 0;$$

$$(2.9)\quad xy = 0 \text{ if and only if } xy' = x.$$

3. Canonical forms. In constructing the canonical forms only one type of *elementary operation* is needed, the addition to the elements of a row of x times the corresponding elements of another row, x being in $\mathfrak{B}$. Furthermore, this elementary operation can be accomplished by multiplying the given matrix on the left by an *elementary matrix*, namely the matrix obtained by performing the desired elementary operation upon the identity matrix I. If E is any elementary matrix, it follows from (2.3) that $EE = I$. Quite obviously then, any elementary matrix is unimodular, and a product of unimodular matrices is unimodular. To facilitate describing the constructions, we first establish a lemma.

LEMMA 3.1. *For $0 \leqslant j \leqslant n$, let $A(j) = [B(j)\ H(n-j)]$ be the following matrix of $\mathfrak{M}$:*

$$\begin{bmatrix}
b_{11} & b_{12} & \ldots & b_{1j} & 0 & 0 & \ldots & 0 \\
b_{21} & b_{22} & \ldots & b_{2j} & 0 & 0 & \ldots & 0 \\
\ldots & & \ldots & & \ldots & & \ldots & \\
b_{j1} & b_{j2} & \ldots & b_{jj} & 0 & 0 & \ldots & 0 \\
b_{j+1,1} & b_{j+1,2} & \ldots & b_{j+1,j} & h_{j+1,j+1} & 0 & \ldots & 0 \\
b_{j+2,1} & b_{j+2,2} & \ldots & b_{j+2,j} & h_{j+2,j+1} & h_{j+2,j+2} & \ldots & 0 \\
\ldots & & \ldots & & \ldots & & \ldots & \\
b_{n1} & b_{n2} & \ldots & b_{nj} & h_{n,j+1} & h_{n,j+2} & \ldots & h_{nn}
\end{bmatrix}$$

where $A = A(n) = [B(n)\ H(0)]$, $H = A(0) = [B(0)\ H(n)]$, and $h_{pq}h_{qq} = 0$, $h_{pq}h_{pp} = h_{pq}$ for $p = q+1,\ q+2, \ldots, n;\ q = j+1,\ j+2, \ldots, n$. Then there exists a unimodular matrix U_j (which is a product of elementary matrices) such that multiplying $A(j)$ on the left by U_j leaves the last $n-j$ columns of $A(j)$ invariant, and replaces the elements b_{kj} of the jth column of $A(j)$ by elements h_{kj}, where $h_{kj} = 0$ for $k = 1, 2, \ldots, j-1$; and $h_{kj}h_{jj} = 0$, $h_{kj}h_{kk} = h_{kj}$ for $k = j+1, j+2, \ldots, n$. (In terms of matrices we have

$$A(j-1) = U_jA(j) = U_j[B(j)\ H(n-j)] = [B(j-1)\ H(n-j+1)],$$

where it is to be understood that although $H(n-j)$ is a submatrix of $H(n-j+1)$, $B(j-1)$ is not necessarily a submatrix of $B(j)$).

Let E_{kj} denote the elementary matrix obtained from I by adding x_{kj} times the elements of the kth row to the corresponding elements of the jth row, where $x_{1j} = b'_{jj}$;

$$x_{kj} = b'_{jj}b'_{1j}b'_{2j}\ldots b'_{k-1,j}, \qquad k = 2, 3, \ldots, j-1;$$

$$x_{kj} = h'_{kk}b'_{1j}b'_{2j}\ldots b'_{k-1,j}, \qquad k = j+1,\ j+2, \ldots, n.$$

https://doi.org/10.4153/CJM-1957-007-3 Published online by Cambridge University Press

It is quite obvious that adding x_{kj} times the elements of the kth row to the corresponding elements of the jth row, for $k = 1, 2, \ldots, j-1$, does not affect the last $n-j$ columns of $A(j)$. For $q = j+1,\ j+2, \ldots, k$; $k = j+1, j+2, \ldots, n$;

$$\begin{aligned} x_{kj}h_{kq} &= h'_{kk}b'_{1j}b'_{2j}\ldots b'_{k-1,j}h_{kq} = h_{kq}h'_{kk}b'_{1j}b'_{2j}\ldots b'_{k-1,j} \\ &= h_{kq}h_{kk}h'_{kk}b'_{1j}b'_{2j}\ldots b'_{k-1,j} = 0. \end{aligned}$$

Hence adding x_{kj} times the elements of the kth row to the corresponding elements of the jth row, for $k = j+1, j+2, \ldots, n$, does not affect the last $n-j$ columns of $A(j)$ either. Then multiplying $A(j)$ on the left by the unimodular matrix

$$E_j = E_{nj}E_{n-1,j}\ldots E_{j+1,j}E_{j-1,j}\ldots E_{2j}E_{1j}$$

leaves the last $n-j$ columns unaltered, and replaces b_{jj} by

$$h_{jj} = b_{1j} \vee \ldots \vee b_{jj} \vee (b_{j+1,j}h'_{j+1,j+1}) \vee \ldots \vee (b_{nj}h'_{nn}).$$

Let F_{kj}, for $k = 1, 2, \ldots, j-1, j+1, \ldots, n$, denote the elementary matrix obtained from I by adding b_{kj} times the elements of the jth row to the corresponding elements of the kth row. Multiplication of $E_jA(j)$ on the left by F_{kj} obviously leaves the last $n-j$ columns invariant, and replaces b_{kj} by $h_{kj} = b_{kj} + b_{kj}h_{jj}$. By (2.6) and (2.3) $h_{kj} = b_{kj} + b_{kj} = 0$ for $k = 1, 2, \ldots, j-1$. For $k = j+1, j+2, \ldots, n$;

$$h_{kj}h_{jj} = (b_{kj} + b_{kj}h_{jj})h_{jj} = b_{kj}h_{jj} + b_{kj}h_{jj} = 0.$$

Using (2.7) we can write

$$\begin{aligned} h_{kj} &= (b_{kj} + b_{kj}h_{jj}) = b_{kj}h'_{jj} \\ &= b_{kj}(b_{kj}h'_{kk})'b'_{1j}b'_{2j}\ldots b'_{jj}(b_{j+1,j}h'_{j+1,j+1})'\ldots \\ &\qquad (b_{k-1,j}h'_{k-1,k-1})'(b_{k+1,j}h'_{k+1,k+1})'\ldots(b_{nj}h'_{nn})'; \end{aligned}$$

and since

$$\begin{aligned} b_{kj}(b_{kj}h'_{kk})' &= b_{kj}(1 + b_{kj}h'_{kk}) = b_{kj} + b_{kj}h'_{kk} \\ &= b_{kj}(1 + h'_{kk}) = b_{kj}h_{kk}, \end{aligned}$$

$$\begin{aligned} h_{kj} &= b_{kj}h_{kk}b'_{1j}b'_{2j}\ldots b'_{jj}(b_{j+1,j}h'_{j+1,j+1})'\ldots \\ &\qquad (b_{k-1,j}h'_{k-1,k-1})'(b_{k+1,j}h'_{k+1,k+1})'\ldots(b_{nj}h'_{nn})', \end{aligned}$$

and it is now obvious that $h_{kj}h_{kk} = h_{kj}$. Letting

$$F_j = F_{nj}F_{n-1,j}\ldots F_{j+1,j}F_{j-1,j}\ldots F_{2j}F_{1j},$$

it is apparent that F_jE_j is the desired unimodular matrix U_j.

We remark that if $h_{jj} = 0$, then by (2.8)

$$b_{1j} = b_{2j} = \ldots = b_{jj} = 0, \quad (b_{kj}h'_{kk}) = 0, \qquad k = j+1, j+2, \ldots, n,$$

whence by (2.9) $b_{kj}h_{kk} = b_{kj}$. So in this particular case we may choose $U_j = I$.

https://doi.org/10.4153/CJM-1957-007-3 Published online by Cambridge University Press

We also note that if $h_{pp} = 0$, then the requirement that $h_{pq}h_{pp} = h_{pq}$ implies that $h_{pq} = 0$ for $q = j + 1, j + 2, \ldots, p$.

THEOREM 3.1. *For any matrix A of $\mathfrak{M}$ there exists a unimodular matrix U of $\mathfrak{M}$ which is a product of elementary matrices and such that $UA = H$ has the following properties: $h_{pq} = 0$ for $q > p$, $h_{pq}h_{qq} = 0$, and $h_{pq}h_{pp} = h_{pq}$.* (Note that if a diagonal element is 0, then the entire row consists of 0's). *This form H is unique.*

Successive applications of Lemma 3.1 to $A = A(n)$ for $j = n, n - 1, \ldots, 1$ yields $A(0) = [B(0)\ H(n)] = H$ and $U_1U_2 \ldots U_n = U$ as the desired matrices.

To prove the uniqueness of H, let U and V be unimodular matrices such that $UA = H$ and $VA = G$ each have the form described above. (The result that a unimodular matrix has an inverse is implied by the succeeding corollary, which is established without assuming the uniqueness of H. To simplify matters, we use this now.) Then $U^{-1}H = A = V^{-1}G$, and $PH = G$, $QG = H$, where $P = VU^{-1}$ and $Q = UV^{-1}$. Thus, for fixed i, the following systems of equations must be satisfied:

$$\sum_{k=t}^{n} p_{ik}h_{kt} = g_{it}, \quad \sum_{k=t}^{n} q_{ik}g_{kt} = h_{it}, \qquad t = 1, 2, \ldots, n,$$

where $g_{it} = h_{it} = 0$ for $t > i$. Consider the first system. The last equation $p_{in}h_{nn} = 0$ and the condition $h_{nt}h_{nn} = h_{nt}$ imply $p_{in}h_{nt} = 0$ for $t = 1, 2, \ldots, n$. Thus the first system is equivalent to

$$\sum_{k=t}^{n-1} p_{ik}h_{kt} = g_{it}, \qquad t = 1, 2, \ldots, n - 1.$$

The last equation $p_{i,n-1}h_{n-1,n-1} = 0$ of this system and the condition $h_{n-1,t}$ $h_{n-1,n-1} = h_{n-1,t}$ imply $p_{i,n-1}h_{n-1,t} = 0$ for $t = 1, 2, \ldots, n - 1$. Thus this system may be reduced to

$$\sum_{k=t}^{n-2} p_{ik}h_{kt} = g_{it}, \qquad t = 1, 2, \ldots, n - 2.$$

Continuing this reduction for $t = n - 2, n - 3, \ldots, i + 1$ yields $p_{ik}h_{kt} = 0$ for $k > i$, $t = 1, 2, \ldots, n$, and replaces the first system by the equivalent system

$$\sum_{k=t}^{i} p_{ik}h_{kt} = g_{it}, \qquad t = 1, 2, \ldots, i.$$

Similarly, the second system is equivalent to

$$\sum_{k=t}^{i} q_{ik}g_{kt} = h_{it}, \qquad t = 1, 2, \ldots, i.$$

Now $p_{ii}h_{ii} = g_{ii}$ and $q_{ii}g_{ii} = h_{ii}$ imply

$$\begin{aligned} g_{ii} &= p_{ii}h_{ii} = p_{ii}q_{ii}g_{ii} = p_{ii}q_{ii}p_{ii}h_{ii} \\ &= q_{ii}p_{ii}h_{ii} = q_{ii}g_{ii} = h_{ii}. \end{aligned}$$

Thus $p_{ii}h_{ii} = h_{ii}$, and $p_{ii}h_{it} = h_{it}$, for $t = 1, 2, \ldots, i$, since $h_{ii}h_{it} = h_{it}$. Similarly, $q_{ii}g_{ii} = g_{ii}$ and $q_{ii}g_{it} = g_{it}$. Now consider

$$p_{i,i-1}h_{i-1,i-1} + p_{ii}h_{i,i-1} = g_{i,i-1},$$
$$q_{i,i-1}g_{i-1,i-1} + q_{ii}g_{i,i-1} = h_{i,i-1}.$$

Multiplying by $h_{i,i-1}$ and $g_{i,i-1}$, respectively, gives

$$h_{i,i-1} = h_{i,i-1}g_{i,i-1}, \quad g_{i,i-1} = h_{i,i-1}g_{i,i-1},$$

since $h_{i,i-1}h_{i-1,i-1} = g_{i,i-1}g_{i-1,i-1} = 0$, and $p_{ii}h_{i,i-1} = h_{i,i-1}$, $q_{ii}g_{i,i-1} = g_{i,i-1}$. Hence $g_{i,i-1} = h_{i,i-1}$, and also $p_{i,i-1}h_{i-1,i-1} = q_{i,i-1}g_{i-1,i-1} = 0$ which implies

$$p_{i,i-1}h_{i-1,t} = q_{i,i-1}g_{i-1,t} = 0, \qquad t = 1, 2, \ldots, i-1.$$

Next we consider

$$p_{i,i-2}h_{i-2,i-2} + p_{i,i-1}h_{i-1,i-2} + p_{ii}h_{i,i-2} = g_{i,i-2},$$
$$q_{i,i-2}g_{i-2,i-2} + q_{i,i-1}g_{i-1,i-2} + q_{ii}g_{i,i-2} = h_{i,i-2}$$

which are simply $p_{i,i-2}h_{i-2,i-2} + h_{i,i-2} = g_{i,i-2}$ and $q_{i,i-2}g_{i-2,i-2} + g_{i,i-2} = h_{i,i-2}$. Multiplying by $h_{i,i-2}$ and $g_{i,i-2}$, respectively, gives

$$h_{i,i-2} = g_{i,i-2}h_{i,i-2}, \quad g_{i,i-2} = h_{i,i-2}g_{i,i-2}.$$

Then $g_{i,i-2} = h_{i,i-2}$, and $p_{i,i-2}h_{i-2,i-2} = q_{i,t-2}g_{i-2,i-2} = 0$ which implies

$$p_{i,i-2}h_{i-2,t} = q_{i,i-2}g_{i-2,t} = 0, \qquad t = 1, 2, \ldots, i-2.$$

Continuing this procedure yields $g_{it} = h_{it}$ for $t = 1, 2, \ldots, i$. Now letting i range from 1 to n establishes the identity of G and H. Hence H is unique.

COROLLARY 3.1. *Every unimodular matrix of $\mathfrak{M}$ is a product of a finite number of elementary matrices.*

If the matrix A in the above theorem is unimodular, then $UA = H$, being a product of unimodular matrices, is also unimodular. Then there exists a matrix K such that $KH = I$. The properties of the elements of H are restrictive enough to require that $H = K = I$. Since U is a product of elementary matrices, say $E_tE_{t-1} \ldots E_1$, we have $E_tE_{t-1} \ldots E_1A = I$. Hence $A = E_1E_2 \ldots E_t$, the desired result. We remark that it is now obvious that $AU = I$ so that $U = A^{-1}$.

The canonical form H does not have, in general, the maximum possible number of rows whose elements are all 0's that could be obtained by elementary row operations on A. The succeeding lemma makes this apparent. Our procedure now will be to obtain a second canonical form for A by performing elementary operations on H that will replace a row wherever possible by a row of 0's and alter the form of H as little as possible.

LEMMA 3.2. *Let H be the matrix described in the preceding theorem and $h_{jj}, h_{j_1j_1}, \ldots, h_{j_tj_t}$, $j_1 < j_2 < \ldots < j_t$, be the diagonal elements in the last*

$n - j + 1$ columns of H that are different from 0. Then a necessary and sufficient condition that there exists a unimodular matrix V_j, such that multiplication of H on the left by V_j replaces h_{jj} by 0, *and leaves invariant the last $n - j$ columns of H and any row which consists entirely of* 0*'s, is that $h_{jj}h_{j_1 j_1}h_{j_2 j_2} \ldots h_{j_t j_t} = 0$.*

The most general sequence of elementary operations that could be performed on the rows of H and leave the necessary things invariant is: the addition of an arbitrary multiple, say x_{j_r}, of the elements of the jth row to the corresponding elements of j_rth row, for $r = 1, 2, \ldots, t$; then the addition of say $y_{jr}h'_{jrjr}$, where y_{jr} is arbitrary, times the elements of the j_rth row to the corresponding elements of the jth row, for $r = 1, 2, \ldots, t$. This replaces h_{jj} by

$$h_{jj} + \sum_{r=1}^{t} y_{j_r}h'_{j_r j_r}(h_{j_r j} + x_{j_r}h_{jj}),$$

which is simply

$$h_{jj} + h_{jj}\sum_{r=1}^{t} y_{j_r}x_{j_r}h'_{j_r j_r},$$

since

$$h'_{j_r j_r}h_{j_r j} = 0.$$

In order to be able to replace h_{jj} by 0, under the required conditions it is then necessary that there exist

$$x_{j_r} \text{ and } y_{j_r}, \qquad r = 1, 2, \ldots, t,$$

such that

$$h_{jj} + h_{jj}\sum_{r=1}^{t} y_{j_r}x_{j_r}h'_{j_r j_r} = 0.$$

By adding h_{jj} to both sides we obtain the equivalent condition

$$h_{jj}\sum_{r=1}^{t} y_{j_r}x_{j_r}h'_{j_r j_r} = h_{jj}.$$

Since

$$y_{j_r}x_{j_r}h'_{j_r j_r} \bigvee_{s=1}^{t} h'_{j_s j_s} = y_{j_r}x_{j_r}h'_{j_r j_r}$$

by (2.6), we have

$$\begin{aligned} h_{jj} \bigvee_{s=1}^{t} h'_{j_s j_s} &= \left(h_{jj}\sum_{r=1}^{t} y_{j_r}x_{j_r}h'_{j_r j_r}\right) \bigvee_{s=1}^{t} h'_{j_s j_s} \\ &= h_{jj}\sum_{r=1}^{t}\left(y_{j_r}x_{j_r}h'_{j_r j_r} \bigvee_{s=1}^{t} h'_{j_s j_s}\right) \\ &= h_{jj}\sum_{r=1}^{t} y_{j_r}x_{j_r}h'_{j_r j_r} \\ &= h_{jj}. \end{aligned}$$

https://doi.org/10.4153/CJM-1957-007-3 Published online by Cambridge University Press

But this last relation implies, by (2.9), (2.7), and (2.4), that

$$h_{jj}h_{j_1j_1}h_{j_2j_2}\ldots h_{j_tj_t} = 0.$$

Hence the condition is necessary.

Conversely, suppose

$$h_{jj}h_{j_1j_1}\ldots h_{j_tj_t} = 0.$$

Then

$$h_{jj}\bigvee_{s=1}^{t} h'_{j_sj_s} = h_{jj},$$

and the aforementioned sequence of operations with

$$x_{j_r} = 1, \qquad (r = 1, 2, \ldots, t),$$

$$y_{j_1} = 1,\ y_{j_r} = h_{j_1j_1}h_{j_2j_2}\ldots h_{j_{r-1}j_{r-1}} \qquad (r = 2, 3, \ldots, t),$$

replaces h_{jj} by

$$h_{jj} + h_{jj}\sum_{r=1}^{t} y_{j_r}x_{j_r}h'_{j_rj_r} = h_{jj} + h_{jj}\bigvee_{r=1}^{t} h'_{j_rj_r} = h_{jj} + h_{jj} = 0$$

and leaves the necessary things invariant. Thus the condition is sufficient and the lemma is proved.

Let us now determine precisely what happens to the elements in the first j columns of H when h_{jj} is replaced by 0 in the manner described in Lemma 3.2. Since

$$h'_{j_rj_r}h_{j_rq} = 0,$$

h_{jq} for $q = 1, 2, \ldots, j-1$, is replaced by

$$h_{jq} + h_{jq}\bigvee_{r=1}^{t} h'_{j_rj_r}.$$

It is necessary that

$$h_{jj}h_{j_1j_1}\ldots h_{j_tj_t} = 0,$$

so that

$$h_{jj}\bigvee_{r=1}^{t} h'_{j_rj_r} = h_{jj}.$$

Using this and the fact that $h_{jq} = h_{jq}h_{jj}$, we have

$$\begin{aligned} h_{jq} + h_{jq}\bigvee_{r=1}^{t} h'_{j_rj_r} &= h_{jq} + h_{jq}h_{jj}\bigvee_{r=1}^{t} h'_{j_rj_r} \\ &= h_{jq} + h_{jq}h_{jj} = h_{jq} + h_{jq} \\ &= 0. \end{aligned}$$

Thus replacing h_{jj} by 0 replaces h_{jq}, for $q = 1, 2, \ldots, j-1$, by 0 also. For $r = 1, 2, \ldots, t$ and $q = 1, 2, \ldots, j$, h_{j_rq} is replaced by

$$d_{j_rq} = h_{jq} + h_{j_rq}.$$

We observe that

$$d_{j_r q} h_{qq} = (h_{jq} + h_{j_r q}) h_{qq} = h_{jq} h_{qq} + h_{j_r q} h_{qq} = 0,$$

so that the property of H that the product of an element with the diagonal element above it be 0 is preserved. Although

$$d_{j_r q} h_{j_r j_r} \neq d_{j_r q}$$

in general, we note that

$$\begin{aligned} d_{j_r q}(h_{jj} \vee h_{j_r j_r}) &= (h_{jq} + h_{j_r q})(h_{jj} \vee h_{j_r j_r}) \\ &= h_{jq}(h_{jj} \vee h_{j_r j_r}) + h_{j_r q}(h_{jj} \vee h_{j_r j_r}) \\ &= h_{jq} h_{jj}(h_{jj} \vee h_{j_r j_r}) + h_{j_r q} h_{j_r j_r}(h_{jj} \vee h_{j_r j_r}) \\ &= h_{jq} h_{jj} + h_{j_r q} h_{j_r j_r} = h_{jq} + h_{j_r q} \\ &= d_{j_r q}. \end{aligned}$$

We also see that, for $q = 1, 2, \ldots, j$,

$$h_{jq} h_{j_1 j_1} \ldots h_{j_t j_t} = h_{jq} h_{jj} h_{j_1 j_1} \ldots h_{j_t j_t} = 0.$$

Hence $h_{j_r q}$ is replaced by an element

$$d_{j_r q} = h_{jq} + h_{j_r q}$$

such that

$$d_{j_r q} h_{qq} = 0, \quad h_{jq} h_{jj} = h_{jq}, \quad h_{jq} h_{j_1 j_1} \ldots h_{j_t j_t} = 0,$$

$$d_{j_r q}(h_{jj} \vee h_{j_r j_r}) = d_{j_r q}.$$

Now let H_1 denote the matrix resulting from replacing h_{jj} by 0 according to the procedure just described. We want to consider the problem of replacing a diagonal element, say h_{ii}, of H_1 by 0 using elementary operations that leave invariant the last $n - i$ columns and any row whose elements are all 0's. Let

$$h_{i_1 i_1}, \; h_{i_2 i_2}, \ldots, h_{i_v i_v}, \quad i < i_1 < i_2 < \ldots < i_v < j,$$

denote the diagonal elements of H_1 between

$$h_{ii} \text{ and } h_{j_1 j_1}$$

which are not 0. When we attempt to parallel the discussion of Lemma 3.2 we find that, although we can add

$$y_{i_r} h'_{i_r t_r}, \text{ where } y_{i_r} \text{ is arbitrary,}$$

times the elements of the i_rth row to the corresponding elements of the ith row, we can't add

$$y_{j_r} h'_{j_r j_r}, \text{ where } y_{j_r} \text{ is arbitrary,}$$

times the elements of the j_rth row to the corresponding elements of the ith row. In order to leave invariant the last $n - i$ columns of H_1 we must add instead

$$y_{j_r}h'_{jj}h_{j_r j_r}, \text{ where } y_{j_r} \text{ is arbitrary,}$$

times the elements of the j_rth row to the corresponding elements of the ith row. With only this change, however, we obtain the following result. A necessary and sufficient condition that h_{ii} can be replaced by 0, by means of elementary operations that leave invariant the last $n - i$ columns and any row consisting of 0's, is that

$$h_{ii}h_{i_1 i_1} \ldots h_{i_v i_v}(h_{j_1 j_1} \vee h_{jj})(h_{j_2 j_2} \vee h_{jj}) \ldots (h_{j_t j_t} \vee h_{jj}) = 0.$$

If this condition is satisfied, to replace h_{ii} by 0 we choose

$$x_{i_r} = x_{j_s} = 1, \qquad r = 1, 2, \ldots, v, s = 1, 2, \ldots, t.$$

That is, we first add the ith row to each succeeding row which does not consist entirely of 0's. Then a multiple of the elements of each of these rows is added to the corresponding elements of the ith row. Choosing the y's appropriately, this replaces $h_{iq}(q = 1, 2, \ldots, i)$, by

$$h_{iq} + h_{iq}\left\{\bigvee_{r=1}^{v} h'_{i_r i_r} \vee \bigvee_{s=1}^{t} (h'_{j_r j_r}h'_{jj})\right\} = h_{iq} + h_{iq} = 0.$$

We note that

$$h_{i_r q}, \qquad q = 1, 2, \ldots, i, r = 1, 2, \ldots, v,$$

is replaced by

$$h_{i_r q} + h_{iq};$$

and

$$d_{j_s q}, \qquad q = 1, 2, \ldots, i, s = 1, 2, \ldots, t,$$

is replaced by

$$d_{j_s q} + h_{iq} = h_{j_s q} + h_{jq} + h_{iq}.$$

Denote this matrix by H_2.

We are now able to describe the procedure for obtaining from the first canonical form H the second canonical form, which we shall call C. Consider successively the products

$$h_{j_t j_t}h_{j_{t-1} j_{t-1}}, \ldots, h_{j_t j_t} \ldots h_{jj}, h_{j_t j_t} \ldots h_{jj}h_{i_v i_v}, \ldots$$

of the diagonal elements of H which are different from 0. If none of these are 0, then $C = H$. Otherwise, there is a first one, say

$$h_{jj}h_{j_1 j_1} \ldots h_{j_t j_t},$$

which is 0. In this case replace h_{jj} by 0 according to the procedure described in Lemma 3.2. Let

$$Z_j = (h_{j_1 j_1} \vee h_{jj})(h_{j_2 j_2} \vee h_{jj}) \ldots (h_{j_t j_t} \vee h_{jj}),$$

and consider successively the products

$$Z_j h_{i_v i_v}, \ldots, Z_j h_{i_v i_v} \ldots h_{ii}, \ldots,$$

https://doi.org/10.4153/CJM-1957-007-3 Published online by Cambridge University Press

If all of these are 0, then $C = H_1$. Otherwise, there is a first one, say

$$h_{ii}h_{i_1i_1} \ldots h_{i_vi_v}Z_j,$$

which is 0. In this case, replace h_{ii} by 0 as before. Let

$$Z_{i,j} = (h_{i_1i_1} \vee h_{ii}) \ldots (h_{i_vi_v} \vee h_{ii})(h_{j_1j_1} \vee h_{jj} \vee h_{ii}) \ldots (h_{j_tj_t} \vee h_{jj} \vee h_{ii}),$$

and let

$$h_{k_1k_1}, \ldots, h_{k_wk_w}, \ k_1 < k_2 < \ldots < k_w,$$

denote the diagonal elements in the first $i - 1$ columns of H_2 which are not 0. Consider successively the products

$$Z_{i,j}h_{k_wk_w}, \ldots, Z_{i,j}h_{k_wk_w} \ldots h_{k_1k_1}.$$

If all of these are 0, then $C = H_2$. Otherwise, there is a first one, say

$$Z_{i,j}h_{k_wk_w} \ldots h_{k_fk_f},$$

which is different from 0. Replace $h_{k_fk_f}$ by 0 in, what should be by now, the obvious manner. Continuing this procedure yields the desired matrix C. Obviously each one of these steps can be accomplished by multiplying the particular H_t on the left by a unimodular matrix V_t. Hence there is a unimodular matrix V such that $VH = C$.

Note that replacing h_{tt} by 0 affects the element in the (p, q)-position of H_t only if $q \leqslant t < p$. Then, for $c_{pp} \neq 0$, if we let

$$c_{q_1q_1}, \ c_{q_2q_2}, \ldots, c_{q_{t_p}q_{t_p}}$$

denote the diagonal elements of C between $c_{q-1,q-1}$ and c_{pp} which are 0, we see that

$$c_{pq} = h_{pq} + h_{q_1q} + h_{q_2q} + \ldots + h_{q_{t_p}q}.$$

(Although the $c_{q_rq_r}$'s include any diagonal element that was originally 0 in H, say

$$h_{q_sq_s} = c_{q_sq_s},$$

this does not affect the representation of c_{pq} since the corresponding $h_{q_sq} = 0$.) We summarize all this in the following theorem.

THEOREM 3.2. *Let A be any matrix of $\mathfrak{M}$ and $UA = H$ its first canonical form. Then there exists a unimodular matrix V such that $WA = VUA = VH = C$, where $W = VU$, has the following form: $c_{pq} = 0$ for $q > p$; if $c_{pp} = 0$, then $c_{pq} = 0$ for $q = 1, 2, \ldots, n$; $c_{pq}c_{qq} = 0$; if $c_{pp} \neq 0$ and*

$$c_{q_1q_1}, \ c_{q_2q_2}, \ldots, c_{q_{t_p}q_{t_p}}$$

denote the diagonal elements of C between $c_{q-1,q-1}$ and c_{pp} which are 0, then

$$c_{pq} = h_{pq} + h_{q_1q} + h_{q_2q} + \ldots + h_{q_{t_p}q}.$$

Furthermore, it is impossible to replace a diagonal element of C by 0 using elementary operations that leave invariant the succeeding columns and any row which consists entirely of 0's. This form C is unique.

https://doi.org/10.4153/CJM-1957-007-3 Published online by Cambridge University Press

The proof that C is unique proceeds along the same lines as the proof of the uniqueness of H, and will be omitted. We wish to emphasize, however, that to ensure uniqueness it is absolutely necessary to add the elements of the kth row to the corresponding elements of each succeeding row whose elements are not all 0's, as the first step in replacing any diagonal element h_{kk} by 0.

THEOREM 3.3. *A necessary and sufficient condition that two matrices A and B of $\mathfrak{M}$ be left-associates is that they have the same canonical form H (or C).*

If $PB = A$, where P is unimodular, let U be a unimodular matrix such that $UA = H$ is the first canonical form of A. Then $H = UPB = VB$, where $V = UP$ is unimodular, so that H is the first canonical form of B also. Conversely, suppose that E and F are unimodular matrices such that $EA = FB = H$ is the first canonical form of A and of B. Then $QB = A$, where $Q = E^{-1}F$ is unimodular, and A and B are left-associates.

4. Mutual left-divisibility, g.c.r.d., and l.c.l.m. Two matrices A and B of $\mathfrak{M}$ are said to be *mutually left-divisible* if and only if there exist matrices R and T of $\mathfrak{M}$ such that $RA = B$ and $TB = A$. It is well known that the concepts of mutual left-divisibility and left-associativity are equivalent for matrices with elements in a principal ideal ring. Steinitz **(5)** has shown their equivalence for matrices with elements in an algebraic domain. Kaplansky **(3)** considered this problem and obtained some results based on the radical of a ring. We now show that the two concepts are equivalent for matrices of $\mathfrak{M}$. If A and B are left-associates so that $PA = B$, where P is unimodular, then $P^{-1}B = A$ and A and B are mutually left-divisible. Conversely, suppose $RA = B$ and $TB = A$. Let $UA = H$ and $VB = G$ be the first canonical forms of A and B, respectively. Then $A = U^{-1}H$ and $B = V^{-1}G$ imply $RU^{-1}H = V^{-1}G$ and $TV^{-1}G = U^{-1}H$. Whence, $PH = G$ and $QG = H$, where $P = VRU^{-1}$ and $Q = UTV^{-1}$; that is, H and G are mutually left-divisible. In proving the uniqueness of the first canonical form H, we showed that $PH = G$ and $QG = H$, where P and Q are unimodular, imply $H = G$. However, the unimodularity of P and Q was not used anywhere in this proof. Hence, we established at that point also that if H and G are mutually left-divisible, then $H = G$. This enables us to state the following result.

THEOREM 4.1. *A necessary and sufficient condition that two matrices A and B of $\mathfrak{M}$ be mutually left-divisible is that they be left-associates.*

Let us now consider the matrix

$$\begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix}$$

of order $2n$. Then there exists a unimodular matrix X of order $2n$, which we write in the form of $n \times n$ blocks, such that

$$\begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}\begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix} = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

is the first canonical form of the above matrix. Thus

$$X_{11}A + X_{12}B = D$$

so that every c.r.d. of A and B is a right divisor of D. Since X is unimodular there exists a matrix $Y = X^{-1}$ such that

$$\begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix}\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix};$$

whence $A = Y_{11}D$, $B = Y_{21}D$, so that D is a c.r.d. of A and B. Hence D is a g.c.r.d. of A and B.

The matrix $M = X_{21}A = X_{22}B$ is a c.l.m. of A and B. Using an argument due to Stewart **(6)**, we are able to show that M is the l.c.l.m. of A and B when $D = I$. To do this, let $M_1 = UA = VB$ be any other c.l.m. of A and B. We can then write the following equations:

$$\begin{bmatrix} X_{11} & X_{12} \\ U & V \end{bmatrix}\begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix} = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} X_{11} & X_{12} \\ U & V \end{bmatrix}\begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix}\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}.$$

Consider the most general solution of the equation

$$\begin{bmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{bmatrix}\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}.$$

Here Z_{12} and Z_{22} are arbitrary, but Z_{11} and Z_{21} must be chosen so that

$$Z_{11}D = D, \quad Z_{21}D = 0.$$

Subject to these conditions the following equations must hold:

$$\begin{bmatrix} X_{11} & X_{12} \\ U & V \end{bmatrix}\begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix} = \begin{bmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{bmatrix},$$

$$\begin{bmatrix} X_{11} & X_{12} \\ U & V \end{bmatrix} = \begin{bmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{bmatrix}\begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}.$$

In particular, it appears that U has the form

$$U = Z_{21}X_{11} + Z_{22}X_{21}.$$

But if $D = I$ the only solution of $Z_{21}D = 0$ is $Z_{21} = 0$. Hence it follows in this case that $U = Z_{22}X_{21}$; then from $M_1 = UA = Z_{22}X_{21}A = Z_{22}M$ it follows that $M = X_{21}A = X_{22}B$ is indeed a l.c.l.m. of A and B. These results are stated in the following theorem.

THEOREM 4.2. *In the matric equation*

$$\begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}\begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix} = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix},$$

written in the form of $n \times n$ blocks, where X is unimodular, the matrix D is in all cases a g.c.r.d. *of A and B; if $D = I$, then the matrix $M = X_{21}A = X_{22}B$ is a* l.c.l.m. *of A and B.*

THEOREM 4.3. *The* g.c.r.d. *D and the* l.c.l.m. *M of two matrices A and B are uniquely determined up to unimodular left factors.*

If D and D_1 are two g.c.r.d.'s of A and B, then each is a c.l.m. of the other, say $D = UD_1$ and $D_1 = VD$. Then by theorem 4.1, D and D_1 are left-associates.

If M and M_1 are two l.c.l.m.'s of A and B, then each is a common right divisor of the other, say $M_1 = UM$ and $M = VM_1$. Then by Theorem 4.1, M and M_1 are left-associates.

5. Conclusion. The analogy of our results to the corresponding ones for the classical case seems remarkable when one considers that a principal ideal ring contains no proper divisors of 0, whereas every element of a Boolean ring except 1 and 0 is a proper divisor of 0. Finally we mention that the restriction to square matrices was inessential.

REFERENCES

1. E. T. Bell, *Arithmetic of logic*, Trans. Amer. Math. Soc., *29* (1927), 597–611.
2. G. Birkhoff, *Lattice Theory*, Amer. Math. Soc. Colloq. Publ., *25* (rev. ed., New York, 1948).
3. I. Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc., *66* (1949), 464–491.
4. C. C. MacDuffee, *Matrices with elements in a principal ideal ring*, Bull. Amer. Math. Soc., *39* (1933), 564–584.
5. E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern*, Math. Ann., *71* (1911), 328–354, and *72* (1912), 297–345.
6. B. M. Stewart, *A note on least common left multiples*, Bull. Amer. Math. Soc., *55* (1949), 587–591.

University of Florida