

THE ALGEBRAIC STRUCTURE OF THE SEMIGROUP OF BINARY RELATIONS ON A FINITE SET

by KI HANG KIM and FRED WILLIAM ROUSH

(Received 9 May, 1977; revised 8 July, 1979)

0. Introduction. In this paper we study some questions proposed by B. Schein [8] regarding the semigroup of binary relations B_X for a finite set X : what is the ideal structure of B_X , what are the congruences on B_X , what are the endomorphisms of B_X ? For $|X|=n$ it is convenient to regard B_X as the semigroup B_n of $n \times n$ (0, 1)-matrices under Boolean matrix multiplication.

For all semigroup notation, terms, and facts used here without explanation, see [2].

1. Ideals.

DEFINITION. The *lattice* generated by a poset P is the idempotent abelian semigroup generated by P and an identity 0 subject to the relation $x + y = y$ whenever $x < y$ in P .

DEFINITION. A *basis* for a lattice L is a set B of non-zero elements of L such that every non-zero element of L is a finite union of elements of B , and no element $x \in B$ is a union of elements of $B \setminus \{x\}$.

Every finite lattice has a unique basis. Every finite distributive lattice is the lattice generated by its basis elements regarded as a poset. See Birkhoff [1] for the theory behind these definitions.

PROPOSITION 1. *The lattice of ideals in any finite semigroup is the lattice generated by the poset of principal ideals. (Here \emptyset must be included as a non-principal ideal in order to obtain the element 0).*

Proof. This lattice is distributive, and the principal ideals form a basis.

DEFINITION. A *maximal chain* of ideals in a semigroup S is a sequence of ideals $\emptyset = I_0 \subset I_1 \subset \dots \subset I_k = S$ which cannot be refined by inserting another ideal properly between two ideals of the sequence. The *length* of the chain is k .

PROPOSITION 2. *In any finite semigroup, the length of any maximal chain of ideals is equal to the number of \mathcal{D} -classes in the semigroup.*

Proof. It suffices to prove that in any finite distributive lattice, the length of any maximal chain is equal to the size of the generating poset, so the number of \mathcal{D} -classes equals the number of principal ideals.

Write each lattice element in the chain as a sum of poset elements in such a way that every poset element less than a summand is also a summand. Each element of the chain must have properly more summands than the preceding one. Unless each element has exactly one more summand than the preceding one, the chain could be further refined. This proves the proposition.

Glasgow Math. J. **22** (1981) 57–68.

2. Congruences. Some facts about Boolean matrices will be used frequently in the following proofs. The set V_n of all n -tuples (v_1, v_2, \dots, v_n) , $(v_i \in \{0, 1\})$ is a semigroup under

$$(v_1, v_2, \dots, v_n) + (w_1, w_2, \dots, w_n) = (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n)$$

where $+$ denotes Boolean sum, and V_n admits the operations

$$c(v_1, v_2, \dots, v_n) = (cv_1, cv_2, \dots, cv_n),$$

where the products are Boolean. It is referred to as the set of n -dimensional Boolean vectors. Occasionally we make use of the Boolean inner product $v \cdot w = \sum v_i w_i$, where the sum and product are Boolean.

A nonempty subset $W \subset V_n$ is called a *subspace* if it is closed under addition and multiplication by constants. All subspaces, being idempotent abelian semigroups, are lattices, though not usually sublattices of V_n . Elements of V_n are sometimes called *row vectors* to distinguish them from n -tuples

$$\begin{bmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ \cdot \\ v_n \end{bmatrix}$$

called *column vectors*. The *row (column) rank* of a Boolean matrix is the number of elements in a lattice basis for the subspace generated by its rows (columns). (See Kim [4].)

Let J denote the Boolean matrix consisting entirely of ones. (This should not be confused with the \mathcal{J} -ordering defined later.)

The i th row $(AB)_{i*}$ of a Boolean matrix product can be written as either $(A_{i*})B$ or as $\sum a_{ij}B_{j*}$. For this, as well as any other general result about rows of a Boolean matrix, there is a dual result about columns, obtained by symmetry under transpose.

An $n \times n$ Boolean matrix is said to be *nonsingular* if it has row and column rank n and is regular as a semigroup element (Plemmons [5], Kim [3]). If two Boolean matrices X, Y of row rank n are \mathcal{L} -equivalent, they have the same row space. But the rows of these matrices must constitute the unique basis for this space, and differ only by rearrangement. Thus there exists a permutation matrix P such that $PX = Y$.

Every idempotent matrix E can be written in block triangular form by conjugating E with a permutation matrix P . In this form all blocks above the main diagonal are zero, each block consists entirely of zeros or entirely of ones, and the main diagonal blocks if zero are 1×1 . (See Schwarz [9], Rosenblatt [6].) The rank of such a matrix equals the number of main diagonal blocks consisting of ones. In fact, choose a set of 1 entries, one from each nonzero main diagonal block. Then the rows (columns) of these diagonal 1 entries will form a row (column) basis.

A Boolean matrix has row rank 1 if and only if it has column rank 1, if and only if all non-zero rows are equal and some row is non-zero, if and only if it can be represented as

$x'y$ where x' is a Boolean column vector and y is a Boolean row vector. Products of rank 1 matrices are described by

$$(x'y)(v'w) = x'(yv')w = (yv')(x'w) = (y \cdot v)x'w$$

where $y \cdot v$ is the Boolean inner product. It readily follows that any rank 1 matrices are \mathcal{D} -equivalent (take one of y, v to be the vector all of whose entries are one).

By the *image space* of a Boolean matrix A we mean $\{vA\}$, where v ranges over all Boolean row vectors of the appropriate dimension. The image space of a Boolean vector equals its row space (consider vectors v with exactly one 1). Two Boolean matrices are $\mathcal{L}(\mathcal{R}, \mathcal{D})$ -equivalent if and only if they have the same row space (the same column space, isomorphic row space). The row spaces of regular elements will be isomorphic if and only if the row bases are isomorphic as partially ordered sets [11]. The following result was proved in [8].

LEMMA 3. *Every nontrivial congruence on B_n sends all matrices of rank 1 to zero.*

Proof. Let w be a Boolean vector such that the Boolean inner product of w with one of av', bv' is zero, but with the other is nonzero. Then multiplying $w'w$ with $av'v$ and $bv'v$ we find $w'v$ is sent to zero in the quotient semigroup. The set of all elements sent to zero is an ideal. Since rank 1 matrices form a single \mathcal{D} -class, every rank 1 matrix will be in the ideal if one is. This proves the lemma.

DEFINITION. The \mathcal{J} -ordering in a semigroup is the quasi-order $x \leq y$ iff the principal two-sided ideal generated by x is contained in the principal two-sided ideal generated by y .

THEOREM 4. *Every congruence on B_n which induces a nontrivial quotient of the symmetric group sends all regular \mathcal{D} -classes to zero, except the \mathcal{D} -class consisting of the symmetric group.*

Proof. Let G be the kernel of the homomorphism from the symmetric group to its image. Then G is the symmetric group, the alternating group for $n \geq 3$, or the Klein 4-group. It suffices to show all idempotents other than the identity are sent to zero. Let z be a \mathcal{J} -minimal idempotent other than the identity which is not sent to 0, if one exists. Since \mathcal{D} -equivalent elements are sent to \mathcal{D} -equivalent elements, any other idempotent in the same \mathcal{D} -class will also have this property.

Case 1. z is nonsingular. By replacing z by a conjugate we may assume it is in triangular form, with ones down the diagonal. Thus there will be vectors u, v with only one 1 such that $uz = u, vz > u$. Let g in G send u to v . If zgz is \mathcal{D} -equivalent to z , it will be \mathcal{H} -equivalent. If it is \mathcal{H} -equivalent, there will be an automorphism A of image z such that $zgzA = z$, since the \mathcal{H} -class of z will be a group. But since $uzgz = vz > u$, no such automorphism can exist. So zgz is less than z in the \mathcal{J} -ordering. But zgz is sent to the same element as $z^2 = z$. So no power of zgz will be sent to zero. So an idempotent power of zgz contradicts the minimality of z .

Case 2. z has rank less than n , but some element of a row basis for z is greater than some other element of a row basis for z . Then we can find an idempotent in the same \mathcal{D} -class which is the direct sum of a nonsingular idempotent z_1 from B_k for $k < n$ and 0. (Take a row basis for z , regard it as a poset on k elements, and take z_1 to be the matrix of this poset as a binary relation.) Then the argument above applies to give a contradiction.

Case 3. z has rank less than n , and no element of a row basis for z is larger than any other element of a row basis for z . Then the \mathcal{D} -class contains an idempotent partial permutation z_1 . By Lemma 3, the rank of this permutation is larger than 1. Let g be an element of G which does not preserve the image of this partial permutation. Then z_1gz_1 is less than z_1 in the \mathcal{J} -ordering. This contradiction completes the proof.

3. Endomorphisms

DEFINITION. An endomorphism of B_n is of *Type I* or *Type II* according as it does or does not induce a nontrivial quotient of the symmetric group.

Examples of Type II endomorphisms are automorphisms, maps sending all non-permutation matrices to J or to 0, and two special kinds of endomorphisms on 2×2 matrices. Let S_n denote the symmetric group.

LEMMA 5. In a Type II endomorphism h , $h(S_n) = S_n$ and either $h(0) = 0$ or $h(0) = J$.

Proof. The image of S_n will be contained in some \mathcal{H} -class containing an idempotent. Since the elements $h(1)h(x)$ are distinct, S_n will act effectively on the distributive lattice which is the image of $h(1)$. The only possible structure for its generating poset is that of n points with no strict inequalities among them. Thus $h(1)$ is a permutation matrix. Since it is idempotent $h(1) = I$. So S_n is sent to the \mathcal{H} -class of I , or S_n .

Then $h(0)$ must be an element y such that $PyQ = y$ for all permutation matrices P, Q . The only two such elements are 0, J .

LEMMA 6. For a Type II endomorphism h which is not an automorphism or a map sending all non-permutations to $h(0)$, let D_1 be a \mathcal{J} -minimal regular \mathcal{D} -class which is not sent to $h(0)$. If $h(0) = 0$, the image of D_1 consists of rank 1 matrices. If $h(0) = J$, the image of D_1 consists of rank 2 matrices in which every row and column vector is a basis vector, for each idempotent in $h(D_1)$.

Proof. Assume $h(0) = 0$ and let z be an idempotent in $h(D_1)$. Assume rank $z > 1$.

Case 1. Some row of z is properly greater than some row basis vector. Let u, v be vectors with only one 1 such that uz corresponds to a minimal row basis vector, located in z so that a 1 occurs on the diagonal, and $vz > u$. Let $ug = v$ for some $g \in S_n$. Then $uzgz$ is not a minimal row in z , so zgz is not \mathcal{H} -equivalent to z . So zgz is not \mathcal{D} -equivalent to z . So some power of zgz is J less than z , and is the image of an idempotent under h , and is nonzero, since $u(zgz)^n \geq u$.

Case 2. The hypothesis of Case I is false, but some row of z contains several 1's. Let such a row be uz , where u has only one 1. Let g send the 1's in uz to the locations of

distinct row basis vectors with 1's on the diagonal, at least one of which is equal to uz . Then zgz is not \mathcal{D} -equivalent to z , and no power of zgz is zero.

Case 3. Column analogues of Cases 1, 2.

Case 4. Other. Every nonzero row vector is a row basis vector (Case 1) and has only one 1. Likewise for column vectors. Thus z is a partial permutation. For rank $z > 1$, again a zgz can be found of smaller rank such that no power of zgz is zero.

Now assume $h(0) = J$. The image of h then will consist entirely of matrices having at least one 1 in each row and at least one 1 in each column, since $h(0)h(x) = h(x)h(0) = J$ for all x in B_n . Let z be an idempotent in $h(D_1)$ and suppose that either z has rank at least three or has rank two and has some row or column vector which is not a basis vector. In the proofs below, vectors u, v, u_i, w are to have exactly one 1.

Case 1. Suppose z has a row basis vector which is not minimal and is not equal to the vector $(1, 1, \dots, 1)$. Let v be a vector such that vz corresponds to such a row, located with diagonal 1. Let uz correspond to a minimal row basis vector less than v , with a diagonal 1. Let g be the transposition which interchanges u and v . Then $uzgz \geq vz$ so zgz is J less than z , and $vzgz = vzz = vz$, so $(zgz)^n$ is not J .

Case 2. Suppose Case 1 fails, but z has a properly dependent row vector. Let $vz = \sum u_i z$ where vz is a minimal properly dependent row, and the $u_i z$ are row basis vectors smaller than vz , with $u_i z \geq u_i$. Let g be the transposition which interchanges u_1 and v . Then zgz is not \mathcal{F} -equivalent to z , and since $u_2 zgz = u_2 z$, $(zgz)^n$ is not the matrix J .

Case 3. Suppose previous cases do not hold, there exist at least two row basis vectors other than $(1, 1, \dots, 1)$, and $(1, 1, \dots, 1)$ is a row basis vector. Let uz, vz be row basis vectors other than $(1, 1, \dots, 1)$ with $uz \geq u, vz \geq v$, and let $wz = (1, 1, \dots, 1)$. Let g be the transposition interchanging v, w . Then zgz is not \mathcal{D} -equivalent to z , and no power of zgz is the matrix J .

Case 4. Suppose some row basis vector contains more than one 1, z has rank at least three, and previous cases do not hold (so no row vector is greater than another row vector, and $(1, 1, \dots, 1)$ is not a row). Let u, v, w, x contain exactly one 1 and be distinct such that $uz \geq u + x$ and uz, vz, wz are distinct row basis vectors. If x is not $\leq vz$, let g be the transposition (xw) . Then $uzgz \geq uz + wz$ and $vzgz = vz$. If $x \leq vz$ let g be the transposition (ux) . Then $uzgz = uzz = uz, vzgz \geq vz + uz$.

Case 5. Column analogues of 1, 2, 3, 4.

Case 6. Other. Every row vector is a row basis vector and likewise for columns, so z has rank at least 3. And every row, column vector contains exactly one 1. Thus z is a permutation. But this contradicts the hypothesis of the lemma.

LEMMA 7. Let h, D_1 be as in Lemma 6. Let $h(0) = J$. Suppose $h(D_1)$ is contained in the \mathcal{D} -class corresponding to the four element lattice of rank 2. Then for some number $c, h(D_1)$ consists of all matrices of the form

$$P \begin{bmatrix} J_c & 0 \\ 0 & J_{n-c} \end{bmatrix} Q$$

where J_c is the $c \times c$ matrix with all entries equal to 1, where P, Q are permutation matrices, and $c = n/2$.

Proof. Every idempotent by Lemma 6 is conjugate to an element of this form. Thus for any element, its row basis vectors must be complements of each other, and also its column basis vectors. This implies that the other vector in the row space, $(1, 1, \dots, 1)$, cannot occur as a row or column vector of any element. Also the number c must be constant and equal to $n/2$, or some product would give elements which are not J but have some rows consisting entirely of 1's.

LEMMA 8. *Let h, D_1 be as in Lemma 6. Then if D_1 consists of matrices of rank less than n , D_1 must be the \mathcal{D} -class containing all rank k partial permutations, for some k .*

Proof. The trace semigroup of D_1 can be defined by a product, denoted by \circ , on $D_1 \cup 0$ given by $a \circ b = ab$ if $a, b, ab \in D_1$, and $a \circ b = 0$ otherwise. The endomorphism h induces a homomorphism from the trace semigroup $\text{Tr}(D_1)$ to $\text{Tr}(h(D_1))$. The trace semigroup of D_1 is 0-simple and can be regarded as a Rees matrix semigroup with sandwich matrix P indexed on the \mathcal{R} -, \mathcal{L} -classes of D_1 . Let P' denote the matrix obtained from P by replacing each nonzero entry by a 1.

Let T_2 be the subsemigroup of $\text{Tr}(D_1)$ consisting of all matrices with at least $n - k$ zero rows and $n - k$ zero columns in D_1 together with 0, where k is the rank of the matrices in D_1 . Let P'_2 be the restriction of P' to T_2 . By comparison with nonsingular matrices in B_k it can be observed that T_2 has exactly one idempotent in each \mathcal{R} -class and exactly one idempotent in each \mathcal{L} -class. Thus P'_2 is a permutation matrix. This means that no non-trivial partition of P'_2 is possible in which the blocks are all 1's or all 0's. Thus distinct \mathcal{R} -classes in T_2 map to distinct \mathcal{R} -classes in $h(D_1)$. In the image semigroup, by Lemmas 6, 7, each \mathcal{R} -class must be preserved by a group of the form $S(a) \times S(n - a)$. So this must be true also in T_2 . Thus some $S(a) \times S(n - a)$ preserves the image of each element in T_2 . For $k < n$, either $a = k$ or $n - a = k$. And the only \mathcal{D} -class in B_k of rank k for which $S(k)$ preserves the image of an element is the \mathcal{D} -class of partial permutations.

Let P_{k-1} denote the \mathcal{D} -class in B_k containing partial permutations of rank $k - 1$.

PROPOSITION 9. *Every matrix in P_{k-1} has the form*

$$P \begin{bmatrix} I_{k-1} & v_1 \\ v_2 & s \end{bmatrix} Q$$

where I_{k-1} is the $(k - 1) \times (k - 1)$ identity matrix and s is a 1×1 matrix equal to the inner product of v_1 and v_2 , and P, Q are permutation matrices.

Proof. By deleting a dependent row and a dependent column we obtain a matrix which must be a permutation.

PROPOSITION 10. *Every idempotent in P_{k-1} is (1) the sum of I_k with some 1 changed to a zero and a matrix which has 1's only in the row of that diagonal zero but not at the diagonal zero or (2) the sum of I_k with some 1 changed to a zero and a matrix which has 1's only in the column of that diagonal zero, off the diagonal, or (3) a conjugate of the direct sum $J_2 + I_{k-2}$.*

Proof. By conjugation write the idempotent in block triangular form. If some

diagonal block has size larger than 1×1 the third case must hold. Otherwise, by rank there will be exactly one diagonal zero. All off-diagonal 1's must lie either in the row or in the column of this diagonal zero. If there are off-diagonal 1's both in the row of this zero and in its column, there must be a product off-diagonal 1 in neither. So either the row of the off-diagonal 1 or its column must be vacant. By reversing the conjugation we obtain form (1) or (2). It can be observed that all the matrices described in the proposition are idempotent.

We can classify \mathcal{R} -, \mathcal{L} -classes in P_{k-1} into the following three types.

Type A: All basis vectors have exactly one 1.

Type B: Exactly one basis vector has two 1's, the others have one 1.

Type C: More than one basis vector has two 1's.

PROPOSITION 11. All \mathcal{R} - or \mathcal{L} -classes of type C have exactly one idempotent which is in an \mathcal{L} - or \mathcal{R} -class of type A. All \mathcal{R} - or \mathcal{L} -classes of type B have two idempotents for \mathcal{L} - or \mathcal{R} -classes of type A and one for \mathcal{L} - or \mathcal{R} -classes of type B. All \mathcal{R} - or \mathcal{L} -classes of type A have one idempotent for \mathcal{L} - or \mathcal{R} -classes of type A.

Proof. This follows from Proposition 10. Thus the matrix P' has the form

	A	B	C
A			
B			0
C		0	0

where $P'(A, A)$ and $P'(B, B)$ are permutation matrices, $P'(A, B)$ has exactly two 1's in each column, $P'(A, C)$ has exactly one 1 in each column, and the matrix P' is symmetric.

Similar results hold for the trace semigroup of the \mathcal{D} -class which contains rank k partial permutations in B_n . Let T_3 be the subsemigroup of this trace semigroup consisting of 0 and all matrices in the \mathcal{D} -class which have at least $(n - k - 1)$ zero rows and at least $(n - k - 1)$ zero columns. We can specialize further by assuming the row and column spaces are of types A, B only. Then the matrix P' , if partitioned into (A, A) , (A, B) , (B, A) and (B, B) blocks, will be symmetric, with the (A, A) and (B, B) blocks being permutation matrices. Also the (A, B) block will have exactly two 1's in each column. No non-trivial partition in which all blocks consist entirely of 1's or entirely of zeros is possible for this matrix. So we must have one-to-one mappings on \mathcal{R} - (\mathcal{L} -) classes.

LEMMA 12. D_1 consists entirely of nonsingular matrices.

Proof. Otherwise D_1 must be the \mathcal{D} -class of partial permutations of some rank k less than n . We have a mapping from the T_3 above to the trace semigroup of rank 1 matrices, or a trace semigroup of rank 2 matrices for which $(1, 1, \dots, 1)$ is both a row basis vector

and a column basis vector, or the matrices of Lemma 7. In the last case, symmetric group action implies the mapping on trace semigroups is epimorphic. But since the P' matrices are different, this is impossible.

Suppose the image consists of rank 1 matrices. Then since the (A, A) and (B, B) blocks of P' in the domain are permutation matrices, and are invariant under multiplication by permutation matrices, both must map to the set of rank 1 matrices with only one non-zero entry. But this is impossible. Suppose the image consists of rank 2 matrices in which $(1, 1, \dots, 1)$ is both a row basis vector and column basis vector. For both types A and B , since the P' matrix has permutation matrices for its (A, A) and (B, B) blocks, the number of 1's in a row with less than n 1's plus the number of 1's in a column with less than n 1's must equal n . Symbolically we may write:

$$\begin{aligned} A &\rightarrow (a_1, a_2), & a_1 + a_2 &= n, \\ B &\rightarrow (b_1, b_2), & b_1 + b_2 &= n, \end{aligned}$$

where the numbers denote the number of 1's in rows and columns which have less than n 1's. The condition on the (A, B) and (B, A) blocks implies $a_1 + b_2 = n - 1$ and $a_2 + b_1 = n - 1$. But these contradict the equations above.

From now on we will usually assume that $n \geq 3$ (the case $n = 2$ can be treated separately) and that $h(x) = x$ on the symmetric group (by composing h with an automorphism).

Let x denote the element $I_n + E(2, 1)$ (where $E(i, j)$ has a 1 in location (i, j) and zeros elsewhere).

LEMMA 13. *If h is of Type II and is not an automorphism and $h(0) = 0$, and $h(g) = g$ for $g \in S_n$ then $h(x) = 0$ or $h(x) = E(1, 1)$ or $h(x) = E(2, 2)$.*

Proof. If P is the transposition $(1, 2)$ we have the following relations on $h(x)$.

- (1) $h(x)$ is invariant under conjugation by elements of S_{n-2} .
- (2) $h(x)^2 = h(x)$.
- (3) $h(x)Ph(x) = 0$.

The first property implies that $h(x)$ can be partitioned in the form

$$\begin{bmatrix} a & b & C \\ d & e & F \\ G & H & K \end{bmatrix},$$

where a, e are 1×1 and K is $(n-2) \times (n-2)$. Also by (1) K must be I_{n-2} , J_{n-2} , 0 , or I_{n-2}' (the complement of I_{n-2}). Also, the matrices C, F, G, H will each contain either all 1's or all zeros.

Condition 3 implies K is zero, and at most one of a, b, d, e is nonzero. Condition 2 and $K = 0$ and Condition 3 imply either both C, F are zero or both G, H are zero. By symmetry under transposition assume C, F are zero. By (3), b and d are zero. By symmetry under conjugation by P assume $e = 0$. If $a = 0$ then (2) implies $h(x) = 0$. Assume $a = 1$. Then (2) implies $H = 0$. If $G = 0$ we have $h(x) = E(1, 1)$. So assume G

consists entirely of 1's. By transposition and conjugation by P we have 4 cases. However the resulting semigroup can always be described by

$$(\alpha, \beta)(\gamma, \delta) = \begin{cases} (\alpha, \delta) & \text{if } \beta \neq \gamma, \\ 0 & \text{otherwise.} \end{cases}$$

Here $\alpha, \beta, \gamma, \delta$ are numbers from 1 to n . The image of x will be $(1, 2)$ or $(2, 1)$. Let Q be the transposition $(2\ 3)$. Then $x(QxQ) = (QxQ)x$, but this relation will not be satisfied on $h(x)$. This contradiction rules out the case where G consists of 1's.

LEMMA 14. *If h is of Type II and is not an automorphism and if $h(x) = x$ for $x \in S_n$ and $h(0) = J$, then $h(x)$ is obtained from one of the following matrices by taking a possible transpose and a possible conjugation by $(1\ 2)$:*

$$J_n, \begin{bmatrix} 1 & 0 & 0 \\ \dots & \dots & \dots \\ 1 & 1 & \bar{1} \\ \dots & \dots & \dots \\ \bar{1} & 0 & I_{n-2} \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ \dots & \dots & \dots \\ 1 & 1 & \bar{1} \\ \dots & \dots & \dots \\ \bar{1} & 0 & J_{n-2} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \dots & \dots \\ \bar{1} & J_{n-1} \end{bmatrix}.$$

Here $\bar{1}$ represents a vector containing only 1 components.

Proof. We have

- (1) $h(x)$ is invariant under conjugation by S_{n-2} ,
- (2) $h(x)^2 = h(x)$,
- (3) $h(x)Ph(x) = J$.

Property (1) implies that $h(x)$ can be partitioned as

$$\begin{bmatrix} a & b & C \\ d & e & F \\ G & H & K \end{bmatrix},$$

where K is 0, I_{n-2} , J_{n-2} , or I_{n-2} , and the other blocks contain all 1's or all 0's. If we replace zero blocks by 0 and nonzero blocks by 1 we must have a 3×3 matrix which solves (2) and (3).

We may first find all 3×3 matrices M which satisfy $M^2 = M$, $MPM = J$ for some transposition P . Up to conjugation and transposition they are

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

(First show some row or column has three 1's, make it the first column, then if $M \neq J$, the first row has one or two 1's. If two, M has only two zeros and by transposition and conjugation they can be made the first two, etc.) It can next be observed that for

$P = (1\ 2)$, the solutions must be these up to transposition and conjugation by $(1\ 2)$. The first and last two forms yield those stated in the lemma. It can be observed that $h(x)^2 = h(x)$ implies that K has only the given forms. Now we will suppose $h(x)$ has the block form

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

The semigroup of such matrices together with 0 can be described by

$$(n, m)(r, s) = \begin{cases} (n, s) & \text{if } m \neq r, \\ J & \text{if } m = r. \end{cases}$$

If Q is $(2\ 3)$ we have $x(QxQ) = (QxQ)x$, yet $(1, 2)(1, 3)$ or $(2, 1)(3, 1)$ will not commute. This contradiction rules out the second form.

THEOREM 15. *All endomorphisms of B_n have one of the following forms, up to composition with an automorphism, for $n \geq 3$, where x denotes the matrix having 1's precisely on the main diagonal and in location $(2, 1)$.*

(1) *The identity.*

(2) *An endomorphism which induces a non-trivial quotient on the symmetric group and sends all regular elements to a single element of the image.*

(3) *An endomorphism which is the identity on the symmetric group and sends 0 to 0 and sends all regular singular elements to 0 and sends x to $E(1, 1)$ or $E(2, 2)$ or 0.*

(4) *An endomorphism which is the identity on the symmetric group and sends 0 to J and all singular regular matrices to J and sends x to J or to a matrix which is one of*

$$\begin{bmatrix} 1 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 1 & 1 & \bar{1} \\ \vdots & \vdots & \vdots \\ \bar{1} & 0 & I_{n-2} \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 1 & 1 & \bar{1} \\ \vdots & \vdots & \vdots \\ \bar{1} & 0 & J_{n-2} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \vdots & \vdots \\ \bar{1} & J_{n-1} \end{bmatrix},$$

up to transposition or conjugation by $(1\ 2)$.

This theorem is the sum of the preceding lemmas.

It can be observed that since x , a partial permutation, and $S(n)$ generate all regular elements, the images of these are prescribed. In some of the above cases regular elements may go to zero and some irregular elements may not go to zero. We think that all the cases listed are represented by actual endomorphisms, but will prove only one case below.

DEFINITION. An $n \times n$ Boolean matrix A is *fully indecomposable* if and only if there do not exist permutation matrices P, Q such that PAQ has the block form

$$\begin{bmatrix} * & 0 \\ * & * \end{bmatrix},$$

main diagonal blocks being square.

This definition is equivalent to the fact that if $a_{ij} = 0$ for $(i, j) \in R \times S$, and R, S are nonempty then $|R| + |S| < n$. (See Schwarz [10].)

PROPOSITION 16. *Let x be a Boolean matrix. Then x has permanent 1 as a matrix over \mathbb{Z} if and only if x is cogredient to a subtriangular matrix with 1's down its diagonal.*

Proof. We prove this by induction. If x is partly decomposable we can reduce the problem to that for smaller matrices. But it is known that all fully indecomposable $(0, 1)$ -matrices have permanent at least 2. In fact by the Hall-Koenig theorem a fully indecomposable matrix has a generalized diagonal passing through each 1 entry. (See Ryser [7].)

PROPOSITION 17. *Let x, y be Boolean matrices of permanent 1 as matrices over \mathbb{Z} . Suppose there is no integer i such that x has an off-diagonal 1 in column i and y has an off-diagonal 1 in row i . Suppose further that the identity is the unique permutation contained in x and the unique permutation contained in y . Then xy has permanent 1.*

Proof. Suppose there is a non-identity permutation π contained in xy . The hypothesis implies $xy = x + y$. Let z be a cycle of π which has size larger than 1. Then z consists of off-diagonal elements contained in x or y . If z were entirely from x or entirely from y , then x or y would have permanent larger than 1. If z contains elements from both, let i, j from x be followed by r, s from y in the cycle. The definition of a cycle implies $j = r$, and the hypothesis of the proposition is contradicted.

PROPOSITION 18. *Let h be the mapping $B_n \rightarrow B_n$ defined as follows: if x does not have permanent 1, $h(x) = J$; if x has permanent 1 and contains the identity matrix, $h(x)$ is the matrix M such that $M(i, j) = 1$ iff $i = j$ or x has an off-diagonal 1 in row i or x has an off-diagonal 1 in column j ; for other elements of permanent 1, define $h(Px) = Ph(x)$ for permutation matrices P . Then h is an endomorphism.*

Proof. We observe that h commutes with conjugation so that $h(PxQ) = Ph(x)Q$. Consider $h(xy)$. Suppose $h(xy) = J$. If x or y does not have permanent 1, $h(xy) = h(x)h(y)$. If x and y do have permanent 1, and xy does not, then Proposition 17 implies that $h(x)h(y)$ is J . If x and y have permanent 1 and xy has permanent 1, a computation shows that $h(x)h(y) = h(xy)$. If $h(xy)$ is not J but one of x, y does not have permanent 1, we have a product of two matrices, one of which does not have permanent 1, giving a matrix of permanent 1. Then one of the factors must have permanent zero. Therefore it will have an $r \times s$ block of zeros, where $r + s = n + 1$. The Schein rank of a matrix is the least number of rank 1 matrices whose sum is given matrix. A matrix with an $r \times s$ block of zeros will have Schein rank less than n . Therefore the Schein rank of the product will be less than n . Write the product in subtriangular form. Then two diagonal 1's will be in the same summand of a Schein decomposition. But this is impossible because no 1's occur above the diagonal in the product. So a permanent 1 matrix can be factored only by permanent 1 matrices. This proves the proposition.

REFERENCES

1. G. Birkhoff, *Lattice theory* (Amer. Math. Soc., 1967).
2. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. 1, Math. Surveys No. 7, Amer. Math. Soc. (Providence R. I., 1961).
3. K. H. Kim (Butler), A Moore-Penrose inverse for Boolean matrices, *Proceedings of Second Australian Conference on Combinatorial Mathematics*, Lecture Notes in Mathematics **403** (Springer-Verlag, 1974), 18–28.
4. K. H. Kim (Butler), Combinatorial properties of binary semigroups, *Period. Math. Hungar.* **5** (1974), 3–46.
5. R. J. Plemmons, Generalized inverses of Boolean relation matrices, *SIAM J. Appl. Math.* **20** (1971), 426–433.
6. D. Rosenblatt, On the graphs of finite idempotent Boolean relation matrices, *J. Res. Nat. Bur. Standards, Sect. B* **61B-4** (1963), 249–256.
7. H. J. Ryser, *Combinatorial mathematics* (Wiley, 1963).
8. B. M. Schein, Problems 1–3, *Proceedings of Conference on Algebraic Semigroup Theory*, Szeged, Hungary, August 1972, 64.
9. Š. Schwarz, On the semigroup of binary relations on a finite set, *Czechoslovak Math. J.* **20-95** (1970), 632–679.
10. Š. Schwarz, On semigroups in combinatorics, *Proceedings of Conference on Algebraic Semigroup Theory*, Szeged, Hungary, August 1972, 24–31.
11. K. A. Zaretskii, Regular elements in the semigroup of binary relations (Russian), *Uspehi Mat. Nauk.* **17** (1962), 105–108.

MATHEMATICS RESEARCH GROUP
ALABAMA STATE UNIVERSITY
MONTGOMERY
ALABAMA 36101, U.S.A.