Semigroup Forum, Vol. 5 (1972), 95-119.

RESEARCH ARTICLES

IDEMPOTENTS AND PRODUCT REPRESENTATIONS WITH APPLICATIONS TO THE SEMIGROUP OF BINARY RELATIONS

George Markowsky

Communicated by A.H. Clifford

1. Introduction

In this paper we show (Corollary 2.6) that the number of idempotents in D_A, where A is an element of an arbitrary semigroup , is equal to the number of ways A can be written as a product XY with $X\varepsilon R_A$ and $Y\varepsilon L_A$, divided by $|H_A|$. (See [5] for general reference.) We use this to prove that if A is a regular element of rank r of the semigroup of binary relations on a finite set of cardinal n, then the number of idempotents in D_A is $1/|H_A|\sum_{i=0}^{r}(-1)^i\binom{r}{i}(M_A-i)^n$, where M_A is an integer(Theorem 5.3). Special cases of this result have been found by K.K.-H. Butler [4a]. Formulas for the number of idempotents in L_A and R_A are also derived. A method for calculating M_A directly from the Zaretsky lattice of A [8] is also given (Theorem 5.8).

2. General Results

We begin with a few lemmas whose proofs are obvious.

LEMMA 2.1 Let S be a semigroup , $A,B\varepsilon S$.

(i) $A\mathcal{L}B \leftrightarrow$ there exist $X,Y\varepsilon S'$ such that $XA = B$ and $YB= A$.

(ii) $A\mathcal{R}B \leftrightarrow$ there exist $X,Y \varepsilon S'$ such that $AX = B$ and

$BY = A$.

LEMMA 2.2 Let S be a semigroup, $A,B \in S$. The following are equivalent.

(i) There exist $a,b,c,d \in S'$ such that $caA = Abd = A$ and $aAb = B$.

(ii) There exist $a,b,c,d \in S'$ such that $acB = Bdb = B$ and $cBd = A$.

(iii) $A\mathcal{D}B$.

We will use the following theorem of Miller and Clifford [5;p.59] in the derivation of some of the following results.

THEOREM 2.3 Let S be a semigroup, $a,b \in S$. Then $ab \in R_a \cap L_b$ if and only if $R_b \cap L_a$ contains an idempotent. In this case $aH_b = H_a b = H_{ab} = R_a \cap L_b = H_a H_b$.

REMARK: It is important to note that in the case considered in Theorem 2.3 above, multiplication by a on the left induces a bijection between H_b and H_{ab}. Similarly, multiplication on the right by b induces a bijection between H_a and H_{ab}.

DEFINITION 2.4

(i) Let X be a set. By $|X|$ we shall mean the cardinality of X.

(ii) Let S be a semigroup and X be a subset of S. By $E(X)$ we shall mean the set of all idempotents contained in X.

(iii) Let S be a semigroup and let $A \in S$. By P_A we mean $\{(X,Y) \mid X \in R_A,\ Y \in L_A \text{ and } XY = A\}$.

REMARK: We note that $P_A \neq \phi$ if and only if A is regular, since if $P_A \neq \phi$ by Theorem 2.3 it follows that $E(D_A) \neq \phi$ and hence A is regular. Similarly, if A is

regular then there exists an idempotent $M \in L_A$ [5], but M is a right identity for L_A and hence $(A,M) \in P_A$. Thus in the proofs of the following theorems we are only concerned with the cases $P_A \neq \phi$ (i.e. A is regular) since in the other cases the theorems are trivial.

THEOREM 2.5 Let S be a semigroup, $A \in S$. Let $\theta: P_A \longrightarrow E(D_A)$ be given by: $\theta(X,Y)$ is the unique idempotent in $L_X \cap R_Y$ (an H-class can have at most one idempotent). Then θ is a surjection and if $B \in E(D_A)$, then $|\theta^{-1}(B)| = |H_A|$.

PROOF: As was noted in the remark above we need only consider the case where A is regular. By Theorem 2.3 θ is well-defined. θ is surjective since if $B \in E(D_A)$, then by Lemma 2.2 there exist $a,b,c,d \in S$ such that $aBb = A$, $caB = Bbd = B$. Let $X = aB$, $Y = Bb$. It is easy to verify that $(X,Y) \in P_A$ and $\theta(X,Y) = B$.

Now we proceed to the second part of the theorem. $\theta^{-1}(B) = \{(X,Y) \mid X \in R_A \cap L_B,\ Y \in L_A \cap R_B \text{ and } XY = A\}$. Pick $(X_0,Y_0) \in \theta^{-1}(B)$, and let $\pi: \theta^{-1}(B) \longrightarrow H_{X_0}$ be the projection map on the first factor. π is surjective since if $X \in H_{X_0}$, $XY_0 \in H_A$ by Theorem 2.3 and hence by Theorem 2.3 again we see that $XH_{Y_0} = H_A$. π is injective because if $(X,Y) \in \theta^{-1}(B)$ then multiplication by X on the left gives a bijection between H_Y and H_A. Hence $|\theta^{-1}(B)| = |H_A|$.

REMARK: If A should happen to be an idempotent, then $\theta(X,Y) = YX$, where θ is as in Theorem 2.5.

COROLLARY 2.6 Let S be a finite semigroup and $A \in S$. Then $|E(D_A)| = (1/|H_A|) \cdot |P_A|$.

THEOREM 2.7 Let S be a semigroup, $A \epsilon S$ and let π_i $(i = 1,2)$ be the projection map $(S \times S \longrightarrow S)$ on the i-th factor. Then:

(i) $\pi_2 : P_A \cap \pi_1^{-1}(A) \longrightarrow E(L_A)$ is a bijection.

(ii) $\pi_1 : P_A \cap \pi_2^{-1}(A) \longrightarrow E(R_A)$ is a bijection.

PROOF:

(i) If $Y \epsilon E(L_A)$ then Y is a right-identity for L_A and hence $(A,Y) \epsilon P_A \cap \pi_1^{-1}(A)$. Conversely, $(A,Y) \epsilon P_A$ implies that $AY = A$. $Y \epsilon L_A$ implies that $Y = XA$ for some $X \epsilon S'$ by Lemma 2.1 and thus $Y = XA = X(AY) = (XA)Y = Y^2$. Thus $Y \epsilon E(L_A)$.

(ii) Proved similarly to (i).

REMARKS: The mappings in Theorem 2.7 are induced by θ of Theorem 2.5 . The next theorem follows from Theorem 2.5 , but we will just give a short direct proof.

THEOREM 2.8 Let S be a semigroup , $A \epsilon S$. Let $B \epsilon D_A$, then there exists a bijection between P_A and P_B .

PROOF: If $B \epsilon D_A$ then by Lemma 2.2 there exist a,b, $c,d \epsilon S'$ such that $caA = Abd = A$ and $aAb = B$. If $X \epsilon R_A$ and $Y \epsilon L_A$ then there exist $t,u \epsilon S'$ such that $At = X$ and $uA = Y$. Let $f_{A,B}: P_A \longrightarrow P_B$ be given by $(X,Y) \longmapsto (aX,Yb)$ and similarly let $f_{B,A} : P_B \longrightarrow P_A$ be given by $(W,Z) \longmapsto (cW,Zd)$.

(i) $(aX)(Yb) = a(XY)b = aAb = B$.

(ii) $(aX)(Yb) = B$ and $Bdt = a(Abd)t = a(At) = aX$ and thus $aX \epsilon R_B$.

(iii) $(aX)(Yb) = B$ and $ucB = u(caA)b = Yb$ and thus $Yb \epsilon L_B$.

Thus $f_{A,B}$ and similarly $f_{B,A}$ are well-defined. It is easy to see that these two maps are inverses.

3. Some Combinatorial Results

The following results are important in the sequel.

LEMMA 3.1 The number of permutations of n objects with repetitions allowed which may be formed from p objects of which k have been singled out to appear in every one of these permutations is $\sum_{i=0}^{k} (-1)^i \binom{k}{i} (p-i)^n$, where $\binom{k}{i}$ is the binomial coefficient.

Proof: We will prove this lemma by the method of generating functions [7]. The generating function for the situation described above will be

$$(*) \quad \left(t + \frac{t^2}{2!} + \ldots\right)^k \left(1 + t + \frac{t^2}{2!} + \ldots\right)^{p-k} = (e^t - 1)^k (e^t)^{p-k}$$

$$= \left(\sum_{i=0}^{k} (-1)^i \binom{k}{i} e^{(k-i)t}\right) e^{(p-k)t} = \sum_{i=0}^{k} (-1)^i \binom{k}{i} e^{(p-i)t} .$$

But $e^{(p-i)t} = \sum_{i=0}^{\infty} (p-i)^n \frac{t^n}{n!}$. Thus (*) reduces to

$$\sum_{n=0}^{\infty} \left(\sum_{i=0}^{k} (-1)^i \binom{k}{i} (p-i)^n \right) \frac{t^n}{n!}$$

, which proves the lemma.

Another proof of this lemma can be found in [3].

COROLLARY 3.2 If $k=n$ $(p \geq k)$, then

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} (p-i)^n = n! .$$

Proof: This follows from Theorem 3.1 and the fact that the number of possible permutations described in

Lemma 3.1 is n! whenever n = k.

Remark: Corollary 3.2 actually holds for any p at all, since $\sum_{i=0}^{n} (-1)^i \binom{n}{i}(p-i)^n$ is a polynomial in p of degree less than or equal to n.

4. Some Basic Facts about the Semigroup of Binary Relations.

Let X be a set. Then the set of binary relations on X (denoted by B_X) forms a semigroup under the following operation : if $A,B \in B_X$ then by $A \cdot B$ we mean $\{(a,c) \in X \times X \mid$ there exists $b \in X$ such that $(a,b) \in A$ and $(b,c) \in B\}$. If X and Y are two sets with the same cardinality , B_X and B_Y are isomorphic semigroups.

On occasion we will want to state some of our results in a more general setting and hence we make the following definition . Let X and Y be sets. By $B_{X,Y}$ we mean $2^{X \times Y}$, i.e., the power set of X×Y. Thus B_X is just $B_{X,X}$ with a semigroup operation. Since $B_{X,Y}$ is not a semigroup in general , by stating some of our results within the context of $B_{X,Y}$ we point out their combinatorial nature.

If $A \in B_{X,Y}$ and $x \in X$, then by A_{x*} we mean the set $\{ y \in Y \mid (x,y) \in A \}$. Similarly, if $y \in Y$, then A_{*y} denotes the set $\{ x \in X \mid (x,y) \in A \}$. A_{x*} (A_{*y}) is called a row (column) of A. By R(A) (called the row space of A) we mean the set $\{ \bigcup_{x \in S} A_{x*} \mid S \subset X\}$, and by C(A) (called the column space of A) we mean the following set

$\{ \bigcup_{y \in T} A_{*y} \mid T \subset Y\}$. If $A \in B_{X,Y}$, R(A) and C(A) form complete lattices (see[1]) with respect to set inclusion and union (join) with the meet being the union of all elements which are less than or equal to each element in the set whose meet we want. For more details see [8].

DEFINITION: Let n be a natural number. By $\underline{n}$ we mean $\{ 1,\ldots,n\}$.

If n is a natural number , by B_n we mean $B_{\underline{n}}$ and by $B_{m,n}$ we mean $B_{\underline{m},\underline{n}}$. Naturally , B_n is isomorphic to B_X where X is any other set of n elements . We will simply write $\underline{n}$, $B_{X,Y}$, B_X, etc. , and omit the statements let n be a natural number , let X and Y be sets , etc.

The following are quite easy to prove ([4],[6],[8]).

PROPOSITION 4.1 : *If* $A,B \in B_X$, *then*

(a) $R(AB) \subset R(B)$

(b) $C(AB) \subset C(A)$.

PROPOSITION 4.2 : *Let* $A,B \in B_X$, *then*

(a) $A\mathcal{L}B$ *iff* R(A) = R(B)

(b) $A\mathcal{R}B$ *iff* C(A) = C(B) .

The proof of the following two Theorems can be found in [8].

THEOREM 4.3 *Let* $A,B \in B_X$. *Then* $A\mathcal{D}B$ *iff* R(A) *and* R(B) *are isomorphic as lattices*.

THEOREM 4.4 *Let* $A \in B_X$. *Then* A *is regular iff* R(A) *is a completely distributive lattice*.

The following is a slight generalization of a theorem found in [8]. We are including it in detail since we will need some of the details from it.

<u>THEOREM 4.5</u> <u>Let</u> $A\epsilon B_{X,Y}$ <u>and for each</u> $w\epsilon C(A)$ <u>let</u> $w' = X - w$. <u>Then the map</u> $f: C(A) \longrightarrow R(A)$ <u>given by</u> $f(w) = \bigcup_{x\epsilon w'} A_{x*}$ <u>is an anti-isomorphism of lattices.</u>

<u>PROOF</u>: Clearly f is well-defined .

<u>f is injective</u>: Let $v,w\epsilon C(A)$ be such that $v \neq w$ but $f(v) = f(w)$. We may assume that there exists $x_0 \epsilon w - v$. $w\epsilon C(A)$ implies that there exists $y_0 \epsilon Y$ such that $x_0 \epsilon A_{*y_0} \subset w$. Thus $y_0 \epsilon A_{x_0 *}$. But $x_0 \epsilon v'$ and thus $A_{x_0 *} \subseteq f(v) = f(w)$. Therefore , there exists $x_1 \epsilon w'$ such that $y_0 \epsilon A_{x_1 *}$,i.e. , $x_1 \epsilon A_{*y_0}$, which implies that $x_1 \epsilon w$, which contradicts the fact that $x_1 \epsilon w'$.

<u>f is surjective</u>: Let $S \subset X$ and consider $\bigcup_{x\epsilon S} A_{x*}$. Let T be the subset of X having the following properties: (i) $\bigcup_{x\epsilon T} A_{x*} = \bigcup_{x\epsilon S} A_{x*}$; (ii) for all $U \subset X$ such that $\bigcup_{x\epsilon U} A_{x*} = \bigcup_{x\epsilon S} A_{x*}$, we have that $U \subset T$. We now claim that $T' \epsilon C(A)$. If $T' \notin C(A)$, then there exists $x_0 \epsilon T'$ such that for all $U \subset T'$ where $x_0 \epsilon U$, we have that $U \notin C(A)$. If $y\epsilon Y$ is such that $(x_0,y)\epsilon A$. Then $A_{*y} \cap T \neq \phi$ (since $A_{*y} \not\subset T'$),i.e., there exists $x_1 \epsilon T$ such that $(x_1,y)\epsilon A$. Thus $A_{x_0 *} \cup (\bigcup_{x\epsilon T} A_{x*}) = \bigcup_{x\epsilon T} A_{x*}$, which by the definition of T implies that $x_0 \epsilon T$. This contradicts the fact that $x_0 \epsilon T'$. Now we proceed to show that f is order reversing.

<u>$v \subset w$ iff $f(v) \supset f(w)$</u> .

(i) if $v \subset w$ then $v' \supset w'$ and hence $f(v) \supset f(w)$.

(ii) the proof in the other direction follows from the fact that if $Z\epsilon C(A)$, and $\bar{Y} \subset X$ is such that $\bigcup_{x\epsilon \bar{Y}} A_{x*} = \bigcup_{x\epsilon Z'} A_{x*}$, then $\bar{Y} \subset Z'$. This last statement follows from what was proved earlier. But $\bigcup_{x\epsilon v'} A_{x*} \supset$

$$\supset \bigcup_{x\epsilon w'} A_{x*} \rightarrow \bigcup_{x\epsilon v'} A_{x*} = \bigcup_{x\epsilon w' \cup v'} A_{x*} \rightarrow v' \supset w' \cup v' \rightarrow$$

$v' \supset w'$ $\rightarrow$ $v \subset w$. It is easy to show that any bijection between two lattices which is order-reversing both ways is an anti-isomorphism (it takes meets to joins and vice-versa).

We need the following concepts and conventions for the rest of this paper. We will write + or Σ instead of $\cup$ and will use $\leq$ for $\subset$ and < for $\subsetneq$, as well as $\wedge$ for meet.

If $A\epsilon B_n$, then R(A) (C(A)) is finite , and we define the basis of R(A) (C(A)) to be the set of all join-irreducible elements of R(A) (C(A)) . Clearly any element of R(A) (C(A)) can be written as a join of elements of this basis, and any element in this basis cannot be written as a union of any of the remaining elements of R(A) . It is easy to see that the subset of the join--irreducible elements of a finite lattice L (actually we need only assume that the lattice is a lattice of finite length) is the only subset of L which join-generates all of L but also contains no redundant elements. Thus we may say for $A\epsilon B_n$, R(A) (C(A)) has a unique basis $B_r(A)$ $(B_c(A))$. A somewhat different approach may be found in [4] and [6]. Let $A \epsilon B_n$, by $\rho_r(A)$ $(\rho_c(A))$ we mean $|B_r(A)|$ $(|B_c(A)|)$. It follows from Theorems 4.4, 4.5 and the fact that a finite distributive lattice has as many join-irreducible elements as meet-irreducible elements [1], that if $A \epsilon B_n$ is regular then $\rho_r(A) = \rho_c(A)$. We assume that the reader is acquainted with the principle of duality as it applies to lattices and will recognize which theorems and proofs have duals.

5. Applications to B_n

To obtain our chief results we will use the following characterization of regularity.

THEOREM 5.1 *Let $A \epsilon B_X$. For each $x \epsilon X$, let $S_x = \{W \epsilon R(A) | x \epsilon W\}$ and $T_x = \bigwedge_{W \epsilon S_x} W$. Then A is regular iff for all $V \epsilon R(A)$, $V = \sum_{x \epsilon V} T_x$.*

PROOF: Since A is regular there exists an idempotent $C \epsilon L_A$ (i.e., $R(A) = R(C)$). We first observe that $T_x = \bigwedge_{u \epsilon y} C_{u*}$ where $y = \{u \epsilon X | x \epsilon C_{u*}\}$, since clearly $\bigwedge_{u \epsilon y} C_{u*} \geq T_x$ and since for each $W \epsilon S_x$ there exists a $u_w \epsilon y$ such that $C_{u_w *} \leq W$. Furthermore, the following are true:

(a) $x \epsilon C_{u*} \Rightarrow C_{x*} \leq C_{u*}$ since C is an idempotent and thus $T_x \geq C_{x*}$ for all x;

(b) $x \epsilon C_{u*} \Rightarrow T_x \leq C_{u*}$ and hence that $\sum_{x \epsilon C_{u*}} C_{x*} \leq \sum_{x \epsilon C_{u*}} T_x \leq C_{u*}$ for all $u \epsilon X$. But since C is an idempotent we have that $C_{u*} = \sum_{x \epsilon C_{u*}} C_{x*}$ for all $u \epsilon X$ and from (b) and the fact that all the elements of $R(C)$ are unions of the rows of C the necessity part of the theorem follows. We now proceed to prove the sufficiency part of the theorem.

Let $C \epsilon B_X$ be such that $C_{u*} = T_u$ for all $u \epsilon X$ (the empty meet is the universal upper bound of $R(A)$). Since $T_u \epsilon R(A)$ it follows that C is an idempotent and since $\{T_x\}_{x \epsilon X}$ spans $R(A)$, it follows that $C \epsilon L_A$ and that A is regular.

THEOREM 5.2 *Let $A \epsilon B_n$ be regular, then the following are true:*

(i) if $V \epsilon B_c(A)$, there exists $x_V \epsilon V$ such that for $W \epsilon C(A)$ where $x_V \epsilon W$, $V \leq W$.

(ii) $\{A_{x_V *} | V \epsilon B_c(A)$ and x_V is as in (i)$\} = B_r(A)$.

Obviously, the duals of (i) and (ii) are also true.

PROOF:

(i) By Theorem 5.1, $V = \sum_{x \epsilon V} T_x$. Since V is join-irreducible there exists $x_V \epsilon V$ such that $T_{x_V} = V$. Thus for all $W \epsilon C(A)$, where $x_V \epsilon W$, we have $V = T_{x_V} \leq W$.

(ii) $V \in B_c(A) \Rightarrow V = A_{*j}$ for some $j \in \underline{n} \Rightarrow (x_V, j) \in A$.

(*) If $z \in V$ then $A_{x_V *} \le A_{z*}$ since $t \in A_{x_V *} \Rightarrow x_V \in A_{*t} \Rightarrow A_{*j} \le A_{*t} \Rightarrow z \in A_{*t} \Rightarrow t \in A_{z*}$. Thus $A_{x_V *}$ is join--irreducible. Let $V, W \in B_c(A)$ be such that $V \neq W$, then $x_V \neq x_W$ and $A_{x_V *} \neq A_{x_W *}$. Thus $|B_c(A)| \le |B_r(A)|$ and dually $|B_r(A)| \le |B_c(A)|$, and we are done. Notice that we have shown at the same time that $\rho_r(A) = \rho_c(A)$.

Alternately, we may conclude the proof by observing that if $y \in A_{s*}$, $s \in \underline{n}$, then there exists $V \in B_c(A)$ such that $s \in V \le A_{*y}$. Hence, $x_V \in A_{*y} \Rightarrow y \in A_{x_V *}$, but by (*) above we know that $A_{x_V *} \le A_{s*}$.

NOTE: In Theorem 5.2 we prove rather directly that if $A \in B_n$ is regular, then $\rho_r(A) = \rho_c(A)$. It is possible to prove Theorem 4.4 rather directly using Theorem 5.1 as a starting point. The value of Theorems 5.1 and 5.2 is that they allow us to work directly with any regular element in B_n, without introducing any additional machinery.

THEOREM 5.3 *Let* $A \in B_n$ *be regular, and let* $r = \rho_r(A) = \rho_c(A)$. *Then* $|P_A| = \sum_{i=0}^{r} (-1)^i \binom{r}{i} (M_A - i)^n$ *where* M_A *is an integer determined as follows. Let* $v_1, \ldots, v_t$ *be the elements of* $C(A)$ *such that* $\{v_1, \ldots, v_r\} = B_c(A)$.

For each $i \in \underline{t}$, *let* $q_i = |\{ w \in R(A) \mid w \le \bigwedge_{x \in v_i} A_{x*}\}|$; *finally, let* $M_A = \sum_{i=1}^{t} q_i$. (*Note that* $q_i \ge 1$ *for all* $i \in \underline{t}$ *since* $\phi \in R(A)$).

PROOF: If $(X,Y) \in P_A$ then we must have that for $j \in \underline{n}$ $Y_{j*} \le \bigwedge_{y \in X_{*j}} A_{y*}$. Thus if $X_{*j} = v_i$, there exist at most q_i possibilities in $R(A)$ for Y_{j*}. Let $ST = \{(\theta, \Delta) \mid \Delta \in R(A),\ \theta \in C(A)$ and $\Delta \le \bigwedge_{x \in \theta} A_{x*}\}$. Clearly $M_A = |ST|$.

We now make a series of assertions.

(1) For each $(X,Y) \in P_A$ and $j \in \underline{n}$ it is clear that $(X_{*j}, Y_{j*}) \in ST$.

(2) Let $i \in \underline{r}$ (i.e., $v_i \in B_c(A)$), then $(v_i, A_{x_{v_i} *}) \in ST$ where x_{v_i} is as in Theorem 5.2. This follows from the proof of Theorem 5.2 (ii), since we showed that $A_{x_{v_i} *} \le A_{z*}$ whenever $z \in v_i$.

(3) It is obvious that if $X, Y \in B_n$ are such that for all $j \in \underline{n}$, $(X_{*j}, Y_{j*}) \in ST$, then $C(X) \subset C(A)$ and $R(Y) \subset R(A)$.

(4) Let X, Y be as in (3), then clearly for all $j \in \underline{n}$ $(XY)_{j*} \le A_{j*}$.

(5) If $(X,Y) \in P_A$, each v_i and each $A_{x_{v_i} *}$ $(i \in \underline{r})$ must appear at least once as a column of X and a row of Y respectively, since the bases of $C(A)$ and $R(A)$ are

unique and because of Theorem 5.2 .

(6) Let $X,Y\epsilon B_n$ be such that $(X_{*j},Y_{j*})\epsilon ST$ for all $j\epsilon\underline{n}$. Then $(X,Y)\epsilon P_A \leftrightarrow$ for each $i\epsilon\underline{r}$ there exists $k_i\epsilon\underline{n}$ such that $X_{*k_i} = v_i$ and $Y_{k_i*} = A_{x_{v_i}*}$.

PROOF:

$\leftarrow$: Clearly $X\epsilon R_A$ and $Y\epsilon L_A$. Let $j\epsilon\underline{n}$, then by (4) above , $(XY)_{j*} \leq A_{j*}$. By the last part of the proof of Theorem 5.2 , there exists $\Delta\subset\underline{r}$ such that $A_{j*} = \sum_{i\epsilon\Delta} A_{x_{v_i}*}$ and $j\epsilon v_i$ for all $i\epsilon\Delta$. Let $z\epsilon A_{j*}$. Then $z\epsilon A_{x_{v_i}*} = Y_{k_i*}$ for some $i\epsilon\Delta$. Since $j\epsilon v_i = X_{*k_i}$, we conclude that $z\epsilon(XY)_{j*}$. Hence $(XY)_{j*} = A_{j*}$ for all $j\epsilon\underline{n}$ and therefore $(X,Y)\epsilon P_A$.

$\rightarrow$: Let $t = x_{v_i}$. From $A = XY$ we have that $A_{t*} = \sum_j X_{tj}Y_{j*}$. Since A_{t*} is join-irreducible , there exists $j\epsilon\underline{n}$ such that $X_{tj} = 1$ and $Y_{j*} = A_{t*}$. Thus $x_{v_i} = t\epsilon X_{*j}$ and $Y_{j*} = A_{x_{v_i}*}$. We claim that $v_i = X_{*j}$. If $X_{*j} \neq v_i$, then by Theorem 5.2 $X_{*j} > v_i$ and there exists $u\epsilon X_{*j} - v_i \rightarrow A_{x_{v_i}*} \leq A_{u*}$ (since XY = A). There exists $z\epsilon\underline{n}$ such that $v_i = A_{*z} \rightarrow (x_{v_i},z)\epsilon A$, but since $u\notin v_i$ we have that $(u,z)\notin A \rightarrow A_{x_{v_i}*} \not\leq A_{u*}$ which is a contradiction. Hence $X_{*j} = v_i$.

From the preceding , and from (6) in particular it follows that by taking any element of ST and using the first component as the k-th column of X and using the second component as the k-th row of Y and seeing that each of the r elements $(v_i,A_{x_{v_i}*})$ $(i\epsilon\underline{r})$ is used at least once , we will get $(X,Y)\epsilon P_A$. Furthermore , it follows that all $(X,Y)\epsilon P_A$ can be constructed in this manner. Hence this theorem follows from what has just been said and Lemma 3.1 . A slight modification of the above arguments will be used to calculate the number of idempotents in L_A and R_A (Theorem 5.6) .

THEOREM 5.4 Let $A\epsilon B_n$ be regular , then
$$|E(D_A)| = (1/|H_A|)\sum_{i=0}^{r}(-1)^i\binom{r}{i}(M_A - i)^n,$$
where $r = \rho_r(A)$ and M_A is as in Theorem 5.3 .

PROOF: This follows immediately from Corollary 2.6 and Theorem 5.3 .

The following fairly well-known result follows from Theorem 5.4 and Corollary 3.2 .

COROLLARY 5.5 Let $A\epsilon B_n$ be regular . If $\rho_r(A) = n$ then $|E(D_A)| = (1/|H_A|)\ n!$.

THEOREM 5.6 Let $A\epsilon B_n$ be regular and $k = \rho_r(A)$. Let $\{v_1,\ldots,v_a\} = C(A)$ and $\{w_1,\ldots,w_a\} = R(A)$ be such that

$\{v_1,\dots,v_k\} = B_c(A)$ and $\{w_1,\dots,w_k\} = B_r(A)$. Let n_i be the number of times v_i appears as a column of A and n_i' the number of times w_i appears as a row of A. Then

$$(1)\quad |E(L_A)| = \prod_{i=1}^{k}((q_i)^{n_i} - (q_i - 1)^{n_i}) \prod_{i=k+1}^{a} (q_i)^{n_i}$$

$$(2)\quad |E(R_A)| = \prod_{i=1}^{k}((q_i')^{n_i'} - (q_i' - 1)^{n_i'}) \prod_{i=k+1}^{a} (q_i')^{n_i'} ,$$

where q_i is as in Theorem 5.3 and q_i' is defined similarly to q_i but with the role of row and column spaces switched.

PROOF: We will only prove (1) , since the proof of (2) is dual. By Theorem 2.7 we need only calculate the number of elements in $P_A \cap \pi_1^{-1}(A)$. Recall the proof of Theorem 5.3 and in particular step (6) . We replace the element X by A . The only condition we need place on Y is that for at least one appearance of each v_i $(i \epsilon \underline{k})$, $A_{x_{v_i}^*}$ must appear as the corresponding row of Y . For $i>k$, whenever v_i appears as a column of A we may have any of the q_i possibilities appearing as the corresponding row of Y , and thus the n_i appearances of v_i give us $(q_i)^{n_i}$ possible choices for the corresponding rows of Y . If $i \leq k$, we see that of the n_i appearances of v_i , $A_{x_{v_i}^*}$ must appear at least once as the corresponding row , whereas other than this restriction we are free to

permit q_i choices for the corresponding row of Y . Thus by Lemma 3.1 there are $(q_i)^{n_i} - (q_i - 1)^{n_i}$ different ways of picking the n_i rows of Y which correspond to the n_i appearances of v_i . Since all these various choices are independent the theorem follows.

REMARK: We will now turn our attention to the nature of the quantities M_A, q_i, q_i' used above , and relate them to the lattice R(A). We will show that q_i, q_i', and M_A depend only on R(A) , and that $M_A = M_A'$ where $M_A' = \sum_{i=1}^{a} q_i'$, as one would suspect on the basis of Theorems 5.3 and 5.6 . We will also say a few words about n_i and n_i' . We begin with a definition to help collect all the quantities involved in one place and to define them in a more general context.

DEFINITION 5.7 Let $A \epsilon B_{m,n}$ and let $\{v_1,\dots,v_b\} = C(A)$, $\{w_1,\dots,w_b\} = R(A)$ be such that $\{v_1,\dots,v_r\} = B_c(A)$ and $\{w_1,\dots,w_s\} = B_r(A)$. By Q_i we mean $\{w \epsilon R(A) \mid w \leq \bigwedge_{p \epsilon v_i} A_{p*}\}$ and Q_i' we mean $\{v \epsilon C(A) \mid v \leq \bigwedge_{p \epsilon w_i} A_{*p}\}$. Finally we let $q_i = |Q_i|$, $q_i' = |Q_i'|$, $M_A = \sum_{i=1}^{b} q_i$, $M_A' = \sum_{i=1}^{b} q_i'$. If $v \epsilon C(A)$ we will sometimes write q(v) , meaning q_i where $v_i = v$. Similarly for q'(w),Q(v),and

Q'(w).

Note that the definitions above agree with those we have used in the more special cases. The purpose of this generalization is to show that q_i, q'_i, M_A and M'_A are really combinatorial in nature and do not really depend on the semigroup operation in B_n.

THEOREM 5.8 Let $A \in B_{m,n}$. *We will use the same symbols as in Definition 5.7 above. Then:*

(1) *If we let* $T_i = \{j \in \underline{b} \mid v_j$ is meet-irreducible and $v_i \not\leq v_j\}$ *and if we let* $\theta_i = \{ v \in C(A) \mid v \geq \sum_{j \in T_i} v_j\}$ *then* $q_i = |\theta_i|$ *for all* $i \in \underline{b}$. *Of course a dual result holds for* q'_i ;

(2) $M_A = M'_A$.

PROOF:

(1): Let f: C(A) ⟶ R(A) be the bijection of Theorem 4.5 . For each $i \in \underline{b}$, let $U_i = \{j \in \underline{b} \mid v_j \leq v_i\}$. Thus $v_i = \sum_{j \in U_i} v_j$. We make the following observations:

(a) Clearly $q_i = |\{v \in C(A) \mid v \geq f^{-1}(\bigwedge_{p \in v_i} A_{p*})\}|$.

(b) Let $S_i = \{p \in v_i \mid A_{p*} \in B_r(A)\}$, then $\bigwedge_{p \in v_i} A_{p*} = \bigwedge_{p \in S_i} A_{p*}$.

Clearly $\bigwedge_{p \in v_i} A_{p*} \leq \bigwedge_{p \in S_i} A_{p*}$. Let $k \in v_i$, then there exists $j \in \underline{n}$ such that $A_{*j} \leq v_i$ and $(k,j) \in A$. Hence there exists $d_k \in \underline{m}$ such that $A_{d_k *} \in B_r(A)$, $A_{d_k *} \leq A_{k*}$, and $(d_k, j) \in A$. Thus $d_k \in S_i$ and $\bigwedge_{p \in S_i} A_{p*} \leq A_{k*}$. Since k was arbitrary , the result follows.

(c) $p \in S_i \leftrightarrow A_{p*} \in B_r(A)$ and $A_{p*} \not\leq f(v_i)$.

$\underline{\rightarrow}$: $p \in S_i \rightarrow p \in S_k$ for some $k \in U_i \cap \underline{r}$ $\rightarrow$ $(p,j) \in A$ for some j such that $A_{*j} = v_k$. But since $f(v_i) = \bigwedge_{p \in U_i} f(v_p)$ and $j \notin f(v_k)$, $A_{p*} \not\leq f(v_k)$ and thus $A_{p*} \not\leq f(v_i)$.

$\underline{\leftarrow}$: Assume $p \notin v_i$. Since $f(v_i) = \sum_{x \in v'_i} A_{x*}$, and $p \in v'_i$ we conclude that $f(v_i) \geq A_{p*}$. But this contradicts the fact that $A_{p*} \not\leq f(v_i)$. Hence we must have that $p \in v_i$.

(d) From (b) it follows that $f^{-1}(\bigwedge_{p \in v_i} A_{p*}) = f^{-1}(\bigwedge_{p \in S_i} A_{p*})$ $= \sum_{p \in S_i} f^{-1}(A_{p*})$. From (c) it follows that f induces a bijection between T_i and S_i and (1) follows from (a) and (d).

(2): Let f be as in (1) . We claim that $q'(f(a)) = |\{ i \in \underline{b} \mid a \in \theta_i\}|$ for all $a \in C(A)$. We prove this in the following steps:

(a) The following two sets are equal: $Q'(f(a))$ and the set $B_a = \{v \in C(A) \mid v \le \bigwedge_{c \in U_a} v_c\}$ where $U_a =$

$= \{c \in \underline{b} \mid v_c$ is join-irreducible and $a \not\ge v_c\}$. This follows from the fact that $Q'(f(a)) = \{v \in C(A) \mid v \le \bigwedge_{p \in f(a)} A_{*p}\}$ and the fact that (b) and (c) in the proof of (1) hold with appropriate changes since f^{-1} has the same properties as f.

(b) $v_i \in B_a$ iff $a \in \theta_i$.

$\Leftarrow$: $a \in \theta_i \rightarrow a \ge \sum_{p \in T_i} v_p$. If $v_i \notin B_a$ there exists $c \in U_a$ such that $v_i \not\le v_c$ and $v_c \not\le a$. Since C(A) is a lattice of finite length there exists $k \in \underline{b}$ such that v_k is meet-irreducible , $v_k \ge v_c$ but $v_k \not\ge v_i$. Since $a \in \theta_i$, $a \ge v_k$ and hence $a \ge v_c$ which is impossible.

$\Rightarrow$: This proof is dual to the proof above , i.e., $v_i \in B_a \rightarrow v_i \le v_c$ for all $c \in U_a$. If $a \notin \theta_i$ there must exist $p \in T_i$ such that $a \not\ge v_p$. Again since C(A) is a lattice of finite length there exists $k \in \underline{b}$ such that v_k is join-irreducible , $v_k \le v_p$, and $v_k \not\le a$. Hence $k \in U_a$ and thus $v_i \le v_k$, i.e. , $v_i \le v_p$ which is impossible since $p \in T_i$. Hence $a \in \theta_i$.

Thus $q'(f(a)) = |\{ i \in \underline{b} \mid a \in \theta_i \}|$ for all $a \in C(A)$.

Since f is a bijection we have that $M'_A = \sum_{w \in R(A)} q'(w) = \sum_{a \in C(A)} q'(f(a)) = \sum_{a \in C(A)} |\{i \in \underline{b} \mid a \in \theta_i\}| = \sum_{i \in \underline{b}} |\theta_i| = \sum_{i \in \underline{b}} q_i = M_A$.

<u>REMARK</u>: In view of Theorem 5.8 , there is no longer any need to use the term M'_A and we will use M_A as the sum of the q_i and as the sum of the q'_i . We will give some consequences of Theorem 5.8 and then make clear the lattice-theoretic properties of the various quantities involved.

<u>COROLLARY 5.9</u> <u>Let</u> $A, B \in B_{m,n}$, $A^T \in B_{n,m}$ (where $A^T = \{(y,x) \mid (x,y) \in A\}$) , <u>and</u> $E, F \in B_n$.

(1) <u>If</u> f <u>is</u> <u>an</u> <u>isomorphism</u> <u>between</u> C(A) <u>and</u> C(B) <u>then</u> $q(f(a)) = q(a)$ <u>for</u> <u>all</u> $a \in C(B)$ <u>and</u> <u>hence</u> $M_A = M_B$.

(2) $E \mathcal{D} F \rightarrow M_E = M_F$.

(3) $M_{A^T} = M_A$.

<u>PROOF</u>:

(1): follows from Theorem 5.8 (1) since f is an isomorphism and from the definition of M_A and M_B .

(2): follows from (1) above and from Theorems 4.3 and 4.5 .

(3): follows from Theorem 5.8(2) .

<u>PROPOSITION 5.10</u> <u>Let</u> $A, B \in B_n$ <u>be</u> <u>such</u> <u>that</u> $B \in L_A$. <u>Then</u> <u>there</u> <u>exists</u> <u>an</u> <u>isomorphism</u> $f: C(A) \longrightarrow C(B)$ <u>such</u> <u>that</u> $q(v) = q(f(v))$ <u>and</u> <u>the</u> <u>number</u> <u>of</u> <u>times</u> v

appears as a column of A is equal to the number of times $f(v)$ appears as a column of B. Furthermore, we have that $v \in B_c(A) \leftrightarrow f(v) \in B_c(B)$. Of course a similar theorem is true in the case where $B \in R_A$.

PROOF: Since $B \in L_A$, by Lemma 2.1 there exist $X, Y \in B_n$ such that $XA = B$ and $YB = A$. Let $f_x : C(A) \longrightarrow C(B)$ be given by $f_x(v) = \{j \in \underline{n} \mid$ there exists $k \in \underline{n}$ such that $(j,k) \in X$ and $k \in v\}$. Define f_y from $C(B)$ to $C(A)$ in a similar manner. If we were viewing elements of B_n as matrices, f_x would correspond to multiplying a column of A by X on the left. Since $YXA = A$, etc., it is not hard to show that f_x and f_y are inverses of one another and are lattice isomorphisms. Thus by Corollary 5.9 $q(f_x(v)) = q(v)$. Since $XA = B$, $f_x(v)$ appears as a column of B as many times as v appears as a column of A. Since f_x is an isomorphism, v is join-irreducible $\leftrightarrow$ $f_x(v)$ is join-irreducible.

One would suspect that Proposition 5.10 is true from Theorem 5.6 since clearly $|E(L_A)|$ depends only on L_A.

DEFINITION 5.11 Let L be a complete lattice and let $w \in L$. Let $T_w = \{\theta \in L \mid \theta$ is meet-irreducible and $\theta \not\geq w\}$. Define $q(w) = |\{v \in L \mid v \geq \sum_{\theta \in T_w} \theta\}|$.

REMARK: Because of Theorem 5.8 we see that the definitions of q and T agree with the ones given earlier

in the case where $L = C(A)$. To calculate M_A on the basis of the characterization given above is easy in case $C(A)$ is small or has a very regular structure.

EXAMPLE: Let $A \in B_n$ be such that $C(A)$ is isomorphic to the lattice L formed by the power set of some set of r elements. Clearly $M_A = \sum_{w \in L} q(w)$.

The meet-irreducible elements of L are obviously the r sets which contain $r - 1$ elements. $|T_w| \geq 2$ for all $w \in L$, except for ϕ and the r singletons. Hence, if $w \neq \phi$ and w is not a singleton, $q(w) = 1$. If w is a singleton, $|T_w| = 1$ since T_w just consists of the complement of w and hence $q(w) = 2$. Finally, if $w = \phi$, $T_w = \phi$ and $q(w) = 2^r$. Thus $M_A = 2^{r+1} + r - 1$.

DEFINITION 5.12 Let $A \in B_{m,n}$. Let $v \in C(A)$. Then define $U_v = \{\theta \in B_c(A) \mid \theta \not\leq v\}$ and $r(v) = |\{w \in C(A) \mid w \leq \bigwedge_{\theta \in U_v} \theta\}|$ and $N_A = \sum_{v \in C(A)} r(v)$.

THEOREM 5.13 Let $A \in B_{m,n}$, then $M_A = N_A$.

PROOF: Since $C(A)$ and $R(A)$ are anti-isomorphic with respect to f of Theorem 4.5, it follows that $U_v = f^{-1}(T_{f(v)})$ and that $q(f(v)) = r(v)$. Hence by Theorem 5.8 it follows that $M_A = N_A$, since $q(f(v))$ (where $f(v) \in R(A)$) is the same as $q'(f(v))$ which was defined earlier.

REMARK: The purpose of Definition 5.12 and Theorem 5.13 is to enable one to work with the join-irreducible elements as well as meet-irreducible elements. Note that in Theorem 5.4 it is necessary to know $|H_A|$. In [2] it is shown that $|H_A|$ is equal to $|Aut(C(A))|$, where $Aut(C(A))$ is the group of lattice automorphisms of $C(A)$. Thus if one constructs $C(A)$ one can figure out $|Aut(C(A))|$ and hence $|H_A|$. Since we are interested in the case where $A \epsilon B_n$ is regular, $C(A)$ is distributive. The following theorem shows that $|Aut(C(A))| = |Aut(B_c(A))|$ where $B_c(A)$ is the partially ordered set formed by the join-irreducible elements of $C(A)$.

THEOREM 5.14 Let L be a finite distrbutive lattice. Let $S \subset L$ be the set of all join-irreducible elements of L. S is a partially ordered set. There is a natural group isomorphism between $Aut(S)$ and $Aut(L)$.

PROOF: Let $S = \{v_1, \ldots, v_t\}$ and let $F: Aut(S) \longrightarrow Aut(L)$ be given by $F(f)(\sum_{i \epsilon \Delta} v_i) = \sum_{i \epsilon \Delta} f(v_i)$ where $\Delta \subset \underline{t}$ and $f \epsilon Aut(S)$. Recall that every element of L can be written as a join of the v_i. We first show that $\sum_{i \epsilon U} v_i \leq \sum_{i \epsilon T} v_i \leftrightarrow \sum_{i \epsilon U} f(v_i) \leq \sum_{i \epsilon T} f(v_i)$ where $U, T \subset \underline{t}$.

$\rightarrow$: Since L is distributive, for each $j \epsilon U$ there exists $p_j \epsilon T$ such that $v_j \leq v_{p_j}$ [1]. This implies that $f(v_j) \leq f(v_{j_p})$.

$\leftarrow$: Same proof as above since $f^{-1} \epsilon Aut(S)$. Hence $F(f)$ preserves order on L and has an inverse $F(f^{-1})$, and thus is a bijection. Thus it is easy to see that

$F(f) \epsilon Aut(L)$. F is clearly injective since $F(f) = F(g)$ implies that $f(v_i) = g(v_i)$ for all $i \epsilon \underline{t}$ which in turn implies that $f = g$. F is surjective since any element of $Aut(L)$ restricts to an element of $Aut(S)$. F is clearly a homomorphism.

REFERENCES

[1] BIRKHOFF, G., Lattice Theory. AMS Colloq. Publ. Vol. XXV, Providence, R.I., 1967.

[2] BRANDON, R.L., D.W. HARDY and G. MARKOWSKY, The Schützenberger Group of an H-Class in the Semigroup of Binary Relations. Semigroup Forum, to appear.

[3] BUTLER, K.K.-H., An Identity in Combinations. Kyungpook Mathematical Journal, Vol.11, No.2 (1971), 197-198.

[4] BUTLER, K.K.-H., Binary Relations, in Recent Trends in Graph Theory. Lecture Notes in Mathematics, No. 186 (Springer Verlag, Berlin, N.Y., 1971), 25-47.

[4a] BUTLER, K.K.-H., On (0,1)-Matrix Semigroups. Semigroup Forum 3 (1971), 74-79.

[5] CLIFFORD, A.H. and G.B. PRESTON, The Algebraic Theory of Semigroups. Vol. 1, AMS Math. Surveys No. 7, Providence, R.I., 1961.

[6] PLEMMONS, R.J., Idempotent Binary Relations. Tech. Report, Univ. of Tennessee, Knoxville, 1969.

[7] RIORDAN, J., An Introduction to Combinatorial Analysis. Wiley, New York, 1958.

[8] ZARETSKII, K.A., The Semigroup of Binary Relations. Mat. Sbornik, (Russian) 61 (1963), 291-305.

Department of Mathematics
St. Mary's College of Maryland
St. Mary's City, Maryland 20686

Received March 17, 1972