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 \( S \), is equal to the number of ways \( A \) can be written as a product \( XY \) with \( X \in R_A \) and \( Y \in L_A \), 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

\[
\frac{1}{|H_A|} \sum_{i=0}^{r} (-1)^i \binom{r}{i} (M_A - i)^n
\]

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 \( , A,B \in S \).
(i) \( AB \) there exist \( X,Y \in S \) such that \( AX = B \) and \( YB = A \).
(ii) \( BA \) there exist \( X,Y \in S \) such that \( AX = B \) and \( YB = A \)
By = A.

Lemma 2.2 Let S be a semigroup, A, B ∈ S. The following are equivalent.

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

(ii) There exist a, b, c, d ∈ S' such that acB = BdB = B and cBd = A.

(iii) ADB.

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 ∈ S. Then ab ∈ R_a ∩ L_b if and only if R_b ∩ L_a contains an idempotent. In this case aH_b = H_a b = H_ab = R_a ∩ 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_a and H_ab. Similarly, multiplication on the right by b induces a bijection between H_b 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 ∈ S. By P_A we mean \( \{(X,Y) | X \in R_A, Y \in L_A \text{ and } XY = A\} \).

Remark: We note that P_A ≠ ∅ if and only if A is regular, since if P_A ≠ ∅ by Theorem 2.3 it follows that E(D_A) ≠ ∅ and hence A is regular. Similarly, if A is regular then there exists an idempotent Me_l_A [5], but M is a right identity for L_A and hence (A, M) ∈ P_A. Thus in the proofs of the following theorems we are only concerned with the cases P_A ≠ ∅ (i.e., A is regular) since in the other cases the theorems are trivial.

Theorem 2.5 Let S be a semigroup, A ∈ S. Let θ: P_A \rightarrow E(D_A) be given by θ(X, Y) is the unique idempotent in L_X ∩ R_Y (an H-class can have at most one idempotent). Then θ is a surjection and if BeE(D_A), then |θ^{-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 BeE(D_A), then by Lemma 2.2 there exist a, b, c, d ∈ S such that abB = A, cBb = Bb = B. Let X = ab, Y = Bb. It is easy to verify that (X, Y) ∈ P_A and θ(X, Y) = B.

Now we proceed to the second part of the theorem. \( \theta^{-1}(B) = \{(X, Y) | X \in R_A, Y \in L_A \cap R_B \text{ and } XY = A\} \). Pick \((X_0, Y_0) \in \theta^{-1}(B)\), and let \( \pi: \theta^{-1}(B) \rightarrow H_{X_0} \) be the projection map on the first factor. \( \pi \) 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 \( XH_{Y_0} = H_A \). \( \pi \) 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 \( \theta(X, Y) = XY \), where θ is as in Theorem 2.5.

Corollary 2.6 Let S be a finite semigroup and A ∈ S. Then \( |E(D_A)| = (1/|H_A|) \cdot |P_A| \).
THEOREM 2.7 Let \( S \) be a semigroup, \( A \in S \) and let \( \pi_i \) (\( i = 1,2 \)) be the projection map \( (S \times S \rightarrow S) \) on the \( i \)-th factor. Then:

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

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

PROOF:

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

(ii) Proved similarly to (i).

REMARKS: The mappings in Theorem 2.7 are induced by \( \theta \) 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, \( A \in S \). Let \( B \in D_A \), then there exists a bijection between \( P_A \) and \( P_B \).

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

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

(ii) \( (aX)(Yb) = B \) and \( Bdt = a(AB)d = a(At) = aX \) and thus \( aX \in R_B \).

(iii) \( (aX)(Yb) = B \) and \( ucB = u(caA)b = Yb \) and thus \( Y \in L_A \). 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

\[
\left( 1 + \frac{t^2}{2!} + \ldots \right)^k \left( 1 + \frac{t^2}{2!} + \ldots \right)^{p-k} = \left( e^{t}-1 \right)^k \left( e^{t} \right)^{p-k} = \sum_{i=0}^{k} (-1)^i \binom{k}{i} t^{p-i} \cdot \frac{t^i}{i!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} \frac{t^i}{i!} \cdot \frac{t^i}{i!} \sum_{i=0}^{k} \frac{t^i}{i!}
\]

But \( e^{p-i} = \sum_{i=0}^{\infty} \frac{t^i}{i!} \cdot \frac{t^i}{i!} \sum_{i=0}^{\infty} \frac{t^i}{i!} \cdot \frac{t^i}{i!} \), which proves the lemma.

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 \( \{(a, c) | (a, c) \in A \times X \times Y \} \). 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 \( X \times Y \). 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 \( \{ y \in Y | (x, y) \in A \} \). Similarly, if \( y \in Y \), then \( A_y \) denotes the set \( \{ x \in X | (x, y) \in A \} \). \( A_x \) \( (A_y) \) is called a row (column) of \( A \). By \( R(A) \) (called the row space of \( A \)) we mean the set \( \{ \bigcup_{x \in S} A_x \} \), and by \( C(A) \) (called the column space of \( A \)) we mean the following set:

\[ \{ \bigcup_{y \in T} A_y \} \ . \]

If \( A, B \in B_X \), \( R(A) \) and \( C(A) \) form complete lattices (see [6]) 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 \( n \) we mean \( \{ 1, \ldots, n \} \).

If \( n \) is a natural number, by \( B_n \) we mean \( B_{n,n} \). Naturally, \( B_n \) is isomorphic to \( B_X \) where \( X \) is any other set of \( n \) elements. We will simply write \( n, B_X, B_Y, \) 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) \( R(AB) \subseteq R(B) \)

(b) \( C(AB) \subseteq C(A) \).

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

(a) \( AB \iff R(A) = R(B) \)

(b) \( ARB \iff C(A) = C(B) \).

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

**THEOREM 4.3** Let \( A, B \in B_X \). Then \( ADB \iff R(A) \) 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.
THEOREM 4.5 Let \( A \in B_n \) and for each \( w \in C(A) \) let 
\[ w' = X - w. \]
Then the map \( f: C(A) \rightarrow R(A) \) given by 
\[ f(w) = \bigcup_{x \in w'} A_{x^*} \]
is an anti-isomorphism of lattices.

**Proof:** Clearly \( f \) is well-defined.

\( f \) is injective: Let \( v, w \in C(A) \) be such that \( v \neq w \) but \( f(v) = f(w) \). We may assume that there exists \( x_0 \in w - v \). \( w \in C(A) \) implies that there exists \( y_0 \in Y \) such that \( x_0 \in A_{y_0} \subseteq w \). Thus \( y_0 \in A_{x_0} \). But \( x_0 \in w' \) and thus \[ A_{x_0} \subseteq f(v) = f(w). \]

Therefore, there exists \( x_1 \in w' \) such that \( y_0 \in A_{x_1} \), i.e., \( x_1 \in A_{y_0} \), which implies that \( x_1 \in w \), which contradicts the fact that \( x_0 \in w' \).

\( f \) is surjective: Let \( S \subseteq X \) and consider \( \bigcup_{x \in S} A_{x^*} \).

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

\[ v \subseteq w \iff f(v) \supseteq f(w) \]

(i) if \( v \subseteq w \) then \( v \supseteq w' \) and hence \( f(v) \supseteq f(w) \).

(ii) the proof in the other direction follows from the fact that if \( z \in C(A) \), and \( \forall \subseteq X \) is such that \( \bigcup_{x \in Y} A_{x^*} = \bigcup_{x \in X'} A_{x^*} \), then \( \forall \subseteq \bigcup_{x \in X'} A_{x^*} \). This last statement follows from what was proved earlier. But \( \bigcup_{x \in X'} A_{x^*} \supseteq \bigcup_{x \in w'} A_{x^*} \), \( \forall \subseteq \bigcup_{x \in w'} A_{x^*} \), \( \forall \subseteq \bigcup_{x \in w'} A_{x^*} \), \( \forall \subseteq \bigcup_{x \in w'} A_{x^*} \).

The fact that \( f \) is an anti-isomorphism follows from the above observations.

We need the following concepts and conventions for the rest of this paper. We will write \( \oplus \) or \( \star \) instead of \( \bigcup \) and will use \( \leq \) for \( C \) and \( \leq \) for \( \subseteq \), as well as \( \Lambda \) for \( \forall \).

If \( A \in B_n \), 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 \( A \in B_n \), \( R(A) \) (C(A)) has a unique
basis $B_\pi(A)$ ($B_\pi(A)$). A somewhat different approach may be found in [4] and [6]. Let $A \in B_n$, by $\rho_\pi(A)$ ($\rho_\pi(A)$) we mean $|B_\pi(A)|$ ($|B_\pi(A)|$). 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 $A \in B_n$ is regular then $\rho_\pi(A) = \rho_\pi(A)$. 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 $A \in B_n$. For each $x \in X$, let $S_x = \{w \in A | x \vee w\}$ and $T_x = \bigwedge_{w \in S_x} w$. Then $A$ is regular iff for all $w \in A$, $V = \bigwedge_{x \in X} T_x$.

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

(a) $x \in C_{u^*} \Rightarrow x \vee C_x = C_{u^*}$ since $C$ is an idempotent and thus $T_x \leq C_x$ for all $x$;

(b) $x \in C_{u^*} \Rightarrow T_x \leq C_{u^*}$ and hence that $\Sigma_{x \in C_{u^*}} x \vee C_{u^*} \leq C_{u^*}$ for all $u \in x$. But since $C$ is an idempotent we have that $C_{u^*} = \Sigma_{x \in C_{u^*}} x \vee C_{u^*}$ for all $u \in x$ and from $x \in C_{u^*}$.

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

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

(i) if $V \in C(A)$, there exists $x \in V$ such that for $W \in C(A)$ where $x \vee W$, $V \subseteq W$.

(ii) $A_{x^*} \in V \in C(A)$ and $x \in V$ is as in (i) = $B_\pi(A)$.

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

**PROOF:**

(i) By Theorem 5.1, $V = \bigwedge_{x \in X} T_x$. Since $V$ is join-irreducible there exists $x \in V$ such that $T_x = V$.

Thus for all $w \in C(A)$, where $x \in V$, we have $V = T_x \leq W$. 104
(ii) \( \forall c \in B_c(A) \Rightarrow V = A \ast j \) for some \( j \in \mathbb{N} \Rightarrow (x_v, j) \in A.

(*) If \( z \in V \) then \( A_{x_v}^* \leq A_z^* \), since \( \exists c \in A_{x_v} \Rightarrow x_v \in A_{x_v}^* \Rightarrow \).
\[ A_{x_v}^* \leq A_{x_v} \Rightarrow z \in A_{x_v} \Rightarrow t \in A_{x_v} \ast z \ast . \] Thus \( A_{x_v} \) is join-
irreducible. Let \( V, W \in \mathcal{B}_c(A) \) be such that \( V \neq W \), then \( x_v \neq x_w \) and \( A_{x_v}^* \neq A_{x_w}^* \). Thus \( |B_c(A)| \leq |B_r(A)| \) and
\[ dually |B_r(A)| \leq |B_c(A)| , \] 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 \( y \in A_s \ast , s \in \mathbb{N} \), then there exists \( V \in \mathcal{B}_c(A) \) such
\[ y \in V \leq A_s \ast . \] Hence, \( x_v \in A_{x_y} \ast \Rightarrow y \in A_{x_v} \ast \), but by (*)
above we know that \( A_{x_v} \ast \leq A_s \ast \).

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 addi-
tional machinery.

THEOREM 5.3 Let \( A \in B_n \) be regular and let \( \rho_r(A) = \rho_c(A) \).
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 \( v_1, \ldots, v_r \)
be the elements of \( C(A) \) such that \( \{v_1, \ldots, v_r\} = B_c(A) \).

For each \( i \in \mathbb{N} \), let \( q_i = \{w \in R(A) | w \leq \underbrace{A \ast \cdots \ast}_{\text{times} v_i} \} \).

Finally, let \( \mathcal{M}_A = \sum_{i=1}^t q_i \). (Note that \( q_i \geq 1 \) for all
\( i \in \mathbb{N} \).)

PROOF: If \( (X, Y) \in P_A \) then we must have that for \( j \in \mathbb{N} \),
\( Y_j \leq A_{x_j} \ast \). Thus if \( X_s = v_i \), there exist at most
\( q_i \) possibilities in \( R(A) \) for \( Y_j \ast \). Let \( ST = \{((\emptyset, \emptyset), \emptyset) \}
\) be the \( R(A) \)'s, \( \emptyset \in C(A) \) and \( \Delta \leq \underbrace{A \ast \cdots \ast}_{\text{times} x \in \emptyset} \). Clearly \( \mathcal{M}_A = |ST| \).

We now make a series of assertions:

1. For each \( (X, Y) \in P_A \) and \( j \in \mathbb{N} \) it is clear that
\( (X_s, Y_j) \in ST \).
2. Let \( i \in \mathbb{N} \) (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
\( A_{x_{v_i}} \ast \leq A_z \ast \) whenever \( z \in v_i \).

3. It is obvious that if \( X, Y \in B_n \) are such that for
all \( j \in \mathbb{N} \), \( (X_s, Y_j) \in ST \), then \( C(X) \subseteq C(A) \) and \( R(Y) \subseteq R(A) \).

4. Let \( X, Y \) be as in (3), then clearly for all \( j \in \mathbb{N} \),
\( (XY)_j \ast \leq A_j \ast \).

5. If \( (X, Y) \in P_A \), each \( v_i \) and each \( A_{x_{v_i}} \ast \) (i.e.) 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 \(X, Y \in \mathbb{E}_n\) be such that \((X_*, Y_*) \in ST\) for all \(j \in \mathbb{N}\). Then \((X, Y) \in P_A\) for each \(i \in \mathbb{N}\) there exists \(k_i \in \mathbb{N}\) such that \(X_{*, k_i} = v_i\) and \(Y_{k_i,*} = A_{v_i,*}\).

**PROOF:**

\[\pm: \text{ Clearly } X \in \mathbb{R}_A \text{ and } Y \in \mathbb{L}_A. \] Let \(j \in \mathbb{N}\), then by (4) above, \((XY)_j * \leq A_j *\). By the last part of the proof of Theorem 5.2, there exists \(\Delta \subseteq \mathbb{R}\) such that \(A_j * = \sum_{i \in \Delta} A_{v_i,*}\) and \(j \in \mathbb{N}\). Let \(z \in \mathbb{A}_j *\). Then \(z \in \mathbb{A}_{v_i,*} = Y_{k_i,*}\) for some \(i \in \Delta\). Since \(j \in \mathbb{N}\) and \(z \in \mathbb{A}_j *\), we conclude that \(z \in (XY)_j *\). Hence \((XY)_j * = A_j *\) for all \(j \in \mathbb{N}\) and therefore \((X, Y) \in P_A\).

\(\pm: \text{ Let } t = x_{v_i}. \) From \(A = XY\), we have that \(A_{t,*} = \sum_j X_{*, j} Y_{j,*}\). Since \(A_{t,*}\) is join-irreducible, there exists \(j \in \mathbb{N}\) such that \(X_{t,j} = 1\) and \(Y_{j,*} = A_{t,*}\). Thus \(x_{v_i} = t \in X_{*, j}\) 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 \(u \in X_{*, j} - v_i + A_{x_{v_i,*}} \leq A_{v_i,*}\) (since \(XY = A\)). There exists \(z \in \mathbb{N}\) such that \(v_i = A_{x_{v_i,*}} + (x_{v_i}, z) \in A\), but since \(u \notin v_i\) we have that \((u, z) \notin A_{x_{v_i,*}} \notin A_{v_i,*}\) 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 \((v_i, A_{x_{v_i,*}})\) \((i \in \mathbb{N})\) is used at least once, we will get \((X, Y) \in P_A\). Furthermore, it follows that all \((X, Y) \in P_A\) 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 \(A \in \mathbb{E}_n\) be regular, then
\[|E(D_A)| = \frac{1}{|H_A|} \sum_{i=0}^{r} (-1)^i {i \choose r} (M_A - i)^n,\]
where \(r = p_x(A)\) 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 \(A \in \mathbb{E}_n\) be regular. If \(p_x(A) = n\) then \(|E(D_A)| = \frac{1}{|H_A|} \cdot n!\).

**THEOREM 5.6** Let \(A \in \mathbb{E}_n\) be regular and \(k = p_x(A)\). Let \(\{v_1, \ldots, v_a\} = C(A)\) and \(\{w_1, \ldots, w_a\} = R(A)\) be such that
\{v_1, \ldots, v_k\} = B_c(A) \text{ and } \{w_1, \ldots, w_k\} = B_r(A). \text{ Let } n_i \text{ be the number of times } v_i \text{ appears as a column of } A \text{ and } n_i' \text{ the number of times } w_i \text{ appears as a row of } A. \text{ Then }

(1) |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) |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 \( P_A \cap \pi^{-1}_A(A) \). 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.e., \( A_{x_{v_i}} \) 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 \( A \in \mathbb{B}_{m,n} \) and let \( \{v_1, \ldots, v_b\} = C(A), \{w_1, \ldots, w_b\} = R(A) \) be such that \( \{v_1, \ldots, v_r\} = B_c(A) \) and \( \{w_1, \ldots, w_s\} = B_r(A) \). By \( Q_i \) we mean \( \{w \in R(A) | w \leq A_{v_i} \} \), and \( Q_i' \) we mean \( \{v \in C(A) | v \leq A_{x_{v_i}} \} \).

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 \( v \in C(A) \) 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 $T_i = \{ j \in b \mid v_j \text{ is meet-irreducible and } v_i \not< v_j \}$ and if we let $\Theta_i = \{ v \in C(A) \mid v \geq \bigwedge j \in T_i v_j \}$ then $q_i = |\Theta_i|$ for all $i \in b$. Of course a dual result holds for $q'_i$.

2. $M_A = M'_A$.

**PROOF:**

(1): Let $f : C(A) \rightarrow R(A)$ be the bijection of Theorem 4.5. For each $i \in b$, let $U_i = \{ j \in b \mid v_j \leq v_i \}$.

Thus $v_i = \bigwedge j \in U_i v_j$. We make the following observations:

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

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

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

(c) $p \in S_i$ if and only if $A_{p^*} \leq f(v_i)$.

$\Rightarrow$: Assume $p \leq v_i$. Since $f(v_i) = \bigwedge_{p \in S_i} A_{p^*}$, we conclude that $f(v_i) \geq A_{p^*}$. But this contradicts the fact that $A_{p^*} \leq f(v_i)$. Hence we must have that $p \leq v_i$.

(d) From (b) it follows that $f^{-1}(\bigwedge_{p \in S_i} A_{p^*}) = f^{-1}(\bigwedge_{p \in S_i} A_{p^*})$.

Thus, $\bigwedge_{p \in S_i} A_{p^*}$. 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 $q'(f(a)) = |\{ i \in b \mid a \in \Theta_i \}|$ for all $a \in C(A)$. We prove this in the following steps:

112

113
(a) The following two sets are equal: \( Q'(f(a)) \) and the set \( B_a = \{ v \in C(A) \mid v \leq A_a \} \) where \( U_a = \).

\[ B_a = \{ v \in C(A) \mid v \leq A_a \} \]

This follows from the fact that \( Q'(f(a)) = \{ v \in C(A) \mid v \leq A_a \} \) 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) \( v_i \in B_a \iff a \in \theta_i \).

\[ a \in \theta_i \iff a \geq \bigvee_{p \in T_i} v_p \]

If \( v_i \notin B_a \) there exists \( c \in U_a \) such that \( v_i \leq v_c \) and \( v_c \not\leq a \). Since \( C(A) \) is a lattice of finite length there exists \( k \in B \) such that \( v_k \) is meet-irreducible, \( v_k \geq v_c \) but \( v_k \not\leq v_i \). Since \( a \in \theta_i \), \( a \geq v_k \) and hence \( a \geq v_c \) which is impossible.

\[ v_i \leq v_c \text{ for all } c \in U_a \text{ if } a \notin \theta_i \]

If \( a \notin \theta_i \) there must exist \( p \in T_i \) such that \( a \not\leq p \). Again since \( C(A) \) is a lattice of finite length there exists \( k \in B \) such that \( v_k \) is join-irreducible, \( v_k \geq v_p \), and \( v_k \not\leq a \). Hence \( k \in U_a \) and thus \( v_i \leq v_k \), i.e., \( v_i \leq v_p \) which is impossible since \( p \in T_i \). Hence \( a \notin \theta_i \).

Thus \( Q'(f(a)) = \{ i \in \theta_i \mid a \in \theta_i \} \) for all \( a \in C(A) \).

Since \( f \) is a bijection we have that \( M_A' = \bigvee_{w \in R(A)} q'(w) = \bigvee_{a \in C(A)} \theta_i \mid i \in \theta_i \mid a \in \theta_i \).

\[ q_i = M_A' \]

REMARK: 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.

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

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

(2) \( EDF \rightarrow M_E = M_F \).

(3) \( M_A \cdot T = M_A \).

PROOF:

(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).

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

**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 \( f_X : C(A) \rightarrow C(B) \) be given by \( f_X(v) = \{ j \in n \mid \text{there exists } k \in X \text{ such that } (j, k) \in X \text{ and } k \in v \} \). Define \( f_Y \) from \( C(B) \) to \( C(A) \) in a similar manner. If we were viewing elements of \( B_n \) as matrices, \( f_X(v) \) would correspond to multiplying a column of \( B \) 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 \( T_w = \{ \theta \in L \mid \theta \text{ is meet-irreducible and } \theta \not< w \} \). 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 \( \emptyset \) and the \( r \) singletons. Hence, if \( w \neq \emptyset \) 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 \( w = \emptyset \), \( T_w = \emptyset \) 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 \( U_v = \{ \theta \in C(A) \mid \theta \not< v \} \) and \( r(v) = |\{ w \in C(A) \mid w \leq \sum_{\theta \in U_v} \theta \}| \). Then \( N_A = \sum_{v \in C(A)} r(v) \).

**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 \(|\text{Aut}(C(A))|\), where \(\text{Aut}(C(A))\) is the group of lattice automorphisms of \(C(A)\). Thus if one constructs \(C(A)\) one can figure out \(|\text{Aut}(C(A))|\) and hence \(|H_A|\). Since we are interested in the case where \(A \leq B\) is regular, \(C(A)\) is distributive. The following theorem shows that \(|\text{Aut}(C(A))| = |\text{Aut}(B_c(A))|\), 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 distributive lattice. Let \(S\) be the set of all join-irreducible elements of \(L\). \(S\) is a partially ordered set. There is a natural group isomorphism between \(\text{Aut}(S)\) and \(\text{Aut}(L)\).

**Proof**: Let \(S = \{v_1, \ldots, v_t\}\) and let

\[F: \text{Aut}(S) \rightarrow \text{Aut}(L)\]

be given by \(F(f)(\sum_{i \in \Delta} v_i) = \sum_{i \in \Delta} f(v_i)\)

where \(\Delta = t\) and \(f\in \text{Aut}(S)\). Recall that every element of \(L\) can be written as a join of the \(v_i\). We first show that \(\sum_{i \in U} v_i = \sum_{i \in U} f(v_i) = \sum_{i \in U} f(v_i)\) where \(U, T \in \Delta\) and \(T \subseteq U\).

\[\therefore: \text{Since } L \text{ is distributive, for each } j \in U \text{ there exists } p_j \in T \text{ such that } v_j \leq p_j\]

This implies that \(f(v_j) \leq f(p_j)\).

\[\therefore: \text{Same proof as above since } f^{-1} \in \text{Aut}(S). \text{ Hence } F(f) \text{ preserves order on } L \text{ and has an inverse } F(f^{-1}), \text{ and thus is a bijection.} \]

Thus it is easy to see that \(F(f) \in \text{Aut}(L)\). \(F\) is clearly injective since \(F(f) = F(g)\) implies that \(f(v_i) = g(v_i)\) for all \(i\in \Delta\) which in turn implies that \(f = g\). \(F\) is surjective since any element of \(\text{Aut}(L)\) restricts to an element of \(\text{Aut}(S)\). \(F\) is clearly a homomorphism.

**References**


