INFORMATION AND CONTROL 11, 290–316 (1967)

On Some Properties of the Semigroup of a Machine Which Are Preserved Under State Minimization

J. C. BEATTY

IBM Watson Research Center, Yorktown Heights, New York 10598

Some results on special types of semigroups of transformations of a set (including permutation groups) are developed and combined with the fundamental results of Paull and Unger on state minimization of incompletely specified sequential machines to obtain some properties of the transformation semigroup of such a machine which are preserved in all minimum state machines (strong preservation), or in at least one (weak preservation) minimum state machine. The principal results are that for permutation machines (those whose states are permuted by every input) there is strong preservation and for simple machines (those whose semigroups have no proper ideals) there is weak preservation. A number of further properties of permutation machines in the satisfaction and minimum state relations are developed.

INTRODUCTION

The point of view taken in this paper is similar to that of Ginsburg (1960) and Elgot and Rutledge (1962) in that properties of incompletely-specified sequential machines are studied which are preserved either in at least one (weak sense) or in all (strong sense) minimum state machines. However the direction taken here is perhaps closer to Schützenberger (1962) in that the primary interest is in the properties of the semigroups of the machines. Whereas in Schützenberger (1962) a relation between the semigroups of arbitrary machines in the satisfaction relation was studied, the emphasis here is on showing that classes of machines having certain types of semigroups are closed under state minimization, either in the strong or the weak sense. Another difference between Schützenberger (1962) and the present study is that while there the abstract semigroup was the main point of interest, it seemed necessary when considering state minimization to study the semigroup of transformations connected with a machine. This is the motivation of Section 2, which develops the necessary properties of transformation semigroups. Section 1

gives a summary of standard definitions and properties of semigroups which will be needed in the sequel. In Section 3, the fundamental results of Paull and Unger (1959) for incompletely-specified sequential machines are developed (since their formulation differs somewhat from what was needed here) and are combined with the contents of Section 2 to obtain some new results on state minimization. Principally these results concern permutation machines (those whose states are permuted by every input) and simple machines (those whose semigroups are simple). For the former there is strong preservation (Corollary 3.18) and for the latter weak preservation (Corollary 3.14) under state minimization. In addition a result of Beatty and Miller (1963), involving a closure operation on sets of states of a machine, is generalized slightly in Theorem 4, whose proof is considerably simplified by the use of a new characterization of this operation. This is then applied to permutation machines. Finally, a variety of further properties of permutation machines is given.

Though the Moore model of a sequential machine is used (in which the output is a function of the state alone), it would appear that the application of these results of the Mealy model would be a straightforward matter.

1. SEMIGROUPS

It is assumed that the reader is familiar with the elementary properties of semigroups. For the basic definitions not given explicitly, reference can be made to Section 1.1 of Clifford and Preston (1961), whose notation is used here except where indicated.

Let S be a semigroup. A subset T of S is said to be a *left [right, two sided] ideal* of S if and only if $ST \subseteq T[TS \subseteq T, TS \cup ST \subseteq T]$. The semigroup S is said to be *simple* if and only if it has no proper two sided ideals and *0-simple* if its only such ideal is 0, where by 0 is meant an element of S (which must be unique if it exists) such that $s0 = 0s = 0$ for all $s \in S$. By S^1 is meant S itself in case S has an identity, and S with an identity adjoined otherwise. Two elements s and t of S are said to be $\mathfrak{L}$-[$\mathfrak{R}$-, $\mathfrak{J}$-] *equivalent* (written $s\mathfrak{L}t[s\mathfrak{R}t, s\mathfrak{J}t]$) if and only if $S^1s = S^1t[sS^1 = tS^1, S^1sS^1 = S^1tS^1]$, $\mathfrak{H}$-*equivalent* ($s\mathfrak{H}t$) if and only if $s\mathfrak{L}t$ and $s\mathfrak{R}t$, and $\mathfrak{D}$-*equivalent* ($s\mathfrak{D}t$) if and only if there exists $u \in S$ such that $s\mathfrak{L}u$ and $u\mathfrak{R}t$ (or equivalently such that $s\mathfrak{R}u$ and $u\mathfrak{L}t$). To see that $\mathfrak{D}$ is really an equivalence relation see Section 2.1 of Clifford and Preston, 1961. An element s of S is said to be *regular* if and only if there exists $s' \in S$ such

that $ss's = s$, and S is regular when each of its elements is. The following well known properties of semigroups will be used in the sequel:

PROPERTY 1.1. *In a semigroup S, if $s\mathfrak{D}t$ then $s\mathfrak{J}t$.*

PROPERTY 1.2. *A semigroup is simple if and only if all of its elements are $\mathfrak{J}$-equivalent. (For a discussion of these and related facts see Clifford and Preston, 1961, p. 48.)*

PROPERTY 1.3. *A finite simple semigroup is regular. (Theorem 2.51 of Clifford and Preston, 1961).*

PROPERTY 1.4. *In a finite semigroup, $\mathfrak{D} = \mathfrak{J}$. (Green, 1951, Theorem 3)*

By the free semigroup F, on a set X we mean the set of all finite sequences of elements of X, in which the product of two such sequences is simply their juxtaposition.

PROPERTY 1.5. *Let F be the free semigroup on X. Let S be any semigroup and let φ_0 be any mapping of X into S. Then φ_0 can be extended in one and only one way to a homomorphism of F into S. (Lemma 1.28 of Clifford and Preston, 1961).*

2. TRANSFORMATION SEMIGROUPS

Let A be a set. By a *transformation* of A we mean a mapping of A into A. If $a \in A$ and f is a mapping of A into any set, then af will denote the image of the element a under the mapping f, and if $B \subseteq A$ then Bf will denote the collection $\{af \mid a \in B\}$ of all images under f of elements of B. If s is a mapping of A into D and t a mapping of D into C, then by st, the composition of t with s, we mean the mapping of A into C obtained by applying first s then t. Thus if $a \in A$, then $a(st) = (as)t$, so the parentheses may be omitted without ambiguity. If s and t are transformations of A, then so is st, i.e. composition is a binary operation on the set $\mathfrak{I}_A$ of all transformations of A. In fact it is associative, so $\mathfrak{I}_A$ is a semigroup. By a [finite] *transformation semigroup* we mean an ordered pair $\langle A, S\rangle$, where A is a [finite] set and S is a subsemigroup of $\mathfrak{I}_A$. If s is a mapping of A into B and $B' \subseteq E$, then sB' will denote the collection $\{a \in A \mid as \in B'\}$ of all elements of A mapped into B' by s. A transformation semigroup $\langle A, S\rangle$ is called a *permutation group* if and only if S is a group and $As = A$ for every $s \in S$. It is an immediate consequence of this definition that the identity of the group S is the identity mapping of A and that all elements of S are one-to-one mappings.

If A is a set then by 2^A we mean the collection of all subsets of A. Let $\langle A, S\rangle$ be a transformation semigroup and let $\Sigma \subseteq 2^A$. We will say that Σ is *weakly closed under* S if and only if for every $B \in \Sigma$ and $s \in S$ there exists

$B' \in \Sigma$ with $Bs \subseteq B'$, and that Σ is *closed* under S if and only if $Bs \in \Sigma$ for each $B \in \Sigma$ and $s \in S$.

PROPOSITION 2.1. *If Σ is closed under S and $\varphi : S \to \mathfrak{I}_\Sigma$ is defined by letting $B(s\varphi)$ equal Bs for each $s \in S$ and $B \in \Sigma$, then φ is a homomorphism and will be called the homomorphism of S induced by Σ.*

Proof. For each $B \in \Sigma$ and $s, t \in S$, $B((st)\varphi) = B(st) = (Bs)t = B(s\varphi)(t\varphi)$, so $(st)\varphi = (s\varphi)(t\varphi)$, Q.E.D.

PROPOSITION 2.2. *If $\langle A, S\rangle$ is a permutation group, $\Sigma \subseteq 2^A$ is closed under S, and φ is the homomorphism of S induced by Σ, then $\langle \Sigma, S\varphi\rangle$ is a permutation group.*

Proof. That $S\varphi$ is a group follows from the fact that S is a group and φ is a homomorphism. Let $s \in S$ and $B \in \Sigma$. Since Σ is closed under S, $Bs^{-1} \in \Sigma$ and $B = (Bs^{-1})s$. Thus $\Sigma(s\varphi) = \Sigma$ and $\langle \Sigma, S\varphi\rangle$ is a permutation group, Q.E.D.

Let Σ be a collection of subsets of A such that each element of A is contained in at least one element of Σ. Then Σ is said to *cover* A, and the relation ρ on A defined by letting $x\rho y$ if and only if x and y are contained in exactly the same elements of Σ is readily seen to be an equivalence relation on A. The collection of all ρ-equivalence classes will be called the *coarsest partition of A refining Σ.*

In the transformation semigroup $\langle A, S\rangle$ we define $b \in A$ to be *accessible from $a \in A$* if and only if there exists $s \in S$ such that $as = b$. We will say of $\langle A, S\rangle$ that it is *accessible* if and only if every $b \in A$ is accessible from some $a \in A$. Clearly every permutation group is accessible. We will say that $\langle A, S\rangle$ is *connected* if and only if for every $a, b \in A$, either a is accessible from b or b is accessible from a, and that $\langle A, S\rangle$ is *strongly connected* if and only if each $a \in A$ is accessible from every $b \in A$.

The cardinality of a set A will be denoted by $|A|$.

PROPOSITION 2.3. *If $\langle A, S\rangle$ is a connected permutation group, then the subgroup $H = \{s \in S \mid as = a\}$ which fixes a single element a of A, is of* index $|A|$ *in S.*

Proof. See Corollary 2.5.1 of Hall (1959).

PROPOSITION 2.4. *If $\langle A, S\rangle$ is a finite connected permutation group, then $|A|$ divides $|S|$.*

Proof. By Proposition 2.3, S has a subgroup of index $|A|$, so $|A|$, divides $|S|$, Q.E.D.

PROPOSITION 2.5. *A connected permutation group is strongly connected.*

Proof. Let $\langle A, S\rangle$ be a connected permutation group and let $a, a' \in A$ and $s \in S$ be such that $as = a'$. Then $a's^{-1} = a$, Q.E.D.

What we have termed a connected permutation group is usually called a *transitive* permutation group. A permutation group $\langle A, S\rangle$ is called *simply transitive* if and only if for every $a, b \in A$ there is exactly one $s \in S$ such that $as = b$. Part of the following proposition is contained in Proposition 2.4 of Tully (1961).

PROPOSITION 2.6. *If $\langle A, S\rangle$ is a strongly connected transformation semigroup and S is commutative, then $\langle A, S\rangle$ is a simply transitive permutation group, and $|A| = |S|$.*

Proof. Suppose $as = a$ and $b \in A$. Let $t \in S$ be such that $at = b$. Then $bs = ats = ast = at = b$, so $s = 1$ (the identity transformation of A). Now suppose $as = b$ and let $t \in S$ be such that $bt = a$, so $ast = a$ and $st = 1$. Thus $\langle A, S\rangle$ is a permutation group. To show that $\langle A, S\rangle$ is simply transitive, suppose $as = as'$ for some $a \in A$ and $s, s' \in S$. Then $ass^{-1} = as's^{-1} = a$, so $s's^{-1} = 1$, and this implies that $s' = s$. Since $\langle A, S\rangle$ is simply transitive, then clearly $|A| = |S|$, Q.E.D.

PROPOSITION 2.7. *If $\langle A, S\rangle$ is a finite transformation semigroup and $As = A$ for each $s \in S$, then $\langle A, S\rangle$ is a permutation group.*

Proof. Since S is finite, then for each $s \in S$, some power of s is idempotent. But the only idempotent element of S is the identity transformation. Thus every $s \in S$ has an inverse, and S is a group, Q.E.D.

The following two lemmas parallel and generalize some of the material in Section 2.2 (See Clifford and Preston, 1961.) In the transformation semigroup $\langle A, S\rangle$ if $s \in S$, we denote by π_s the *partition* (or equivalence relation) of A *corresponding to* s, by which is meant that a and a' fall into the same block of $\pi_s(a\pi_s a')$ if and only if $as = a's$.

LEMMA 2.8. *Let $\langle A, S\rangle$ be a transformation semigroup and let $s, t \in S$. If $s\mathfrak{L}t$ then $As = At$. If s and t are regular and $As = At$ then $s\mathfrak{L}t$.*

Proof. By definition of $\mathfrak{L}$, $s\mathfrak{L}t$ if and only if there exist $s', t' \in S^1$ such that $s = s't$ and $t = t's$. Thus if $s\mathfrak{L}t$, then $As = As't \subseteq At$ and $At = At's \subseteq As$, so $As = At$. Now assume s and t are regular and $As = At$, so there exist $s', t' \in S$ such that $ss's = s$ and $tt't = t$. For any $a \in A$, since $As = At$, there exists $b \in A$ such that $as = bt$. Thus $ast't = btt't = bt = as$ for any $a \in A$. Consequently $(st')t = s$. Similarly $(ts')s = t$ and so $s\mathfrak{L}t$, Q.E.D

Lemma 2.9. *Let $\langle A, S\rangle$ be a transformation semigroup and let $s, t \in S$. If $s\mathfrak{R}t$, then $\pi_s = \pi_t$. If s and t are regular and $\pi_s = \pi_t$, then $s\mathfrak{R}t$.*

Proof. By definition of $\mathfrak{R}$, $s\mathfrak{R}t$ if and only if there exist $s', t' \in S^1$ such

that $s = ts'$ and $t = st'$. Thus if $s\mathcal{R}t$ and $at = bt$, then $as = ats' = bts' = bs$; similarly, if $as = bs$, then $at = bt$. Thus $\pi_s = \pi_t$. Now assume that s and t are regular and $\pi_s = \pi_t$, and let s' and t' be such that $ss's = s$ and $tt't = t$. For $a \in A$, since $att't = at$, then $(att')\pi_t a$, so $(att')\pi_s a$ and $att's = as$. Thus $t(t's) = s$, since a was arbitrarily chosen. Similarly $s(s't) = t$, so $s\mathcal{R}t$, Q.E.D.

A transformation semigroup $\langle A, S\rangle$ will be called simple if and only if S is simple. Suschkewitsch (1928) was apparently aware of the following characterizations of finite simple transformation semigroups, though he did not state them explicitly:

THEOREM 2.10. *The following conditions on a finite transformation semigroup $\langle A, S\rangle$ are equivalent:*

(a) *$\langle A, S\rangle$ is simple*

(b) *for every $s, t \in S$, $|As| = |At|$;*

(c) *for every $s, t \in S$, $Ast = At$;*

(d) *for every $s, t \in S$, the restriction of t to As is a one-to-one mapping of As onto At.*

Proof. $(a) \Rightarrow (b)$: Since S is finite, then $\mathcal{D} = \mathcal{J}$ by Property 1.4, so all elements of S are $\mathcal{D}$-equivalent by Property 1.2 and (a). Thus if $s, t \in S$, there exists $u \in S$ such that $s\mathcal{L}u$ and $u\mathcal{R}t$. By Lemma 2.8 and 2.9, then $As = Au$ and $\pi_u = \pi_t$. But clearly $|Au| = |\pi_u| = |\pi_t| = |At|$, so $|As| = |At|$.

$(b) \Rightarrow (c)$: Since $As \subseteq A$, then $Ast \subseteq At$. But $|Ast| = |At|$ by (b), and since the sets are finite, it follows that $Ast = At$.

$(c) \Rightarrow (d)$: By (c), t maps As onto At; and s maps At onto As. Since the sets are finite, then t must be one-to-one on As.

$(d) \Rightarrow (a)$: Let $a, b \in A$ and $s, t \in S$. If $as = bs$, then $ast = bst$; conversely if $ast = bst$, then $as = bs$ by (d), since t is one-to-one on As. Thus $\pi_{st} = \pi_s$. Since also $Ast = At$ by (d), it suffices to show that S is regular; for then it will follow from Lemmas 2.8 and 2.9 that $t\mathcal{L}(st)$ and $(st)\mathcal{R}s$ and hence that $s\mathcal{D}t$ and by Property 1.1 that $s\mathcal{J}t$; finally since s and t were chosen arbitrarily, then all elements of S are $\mathcal{J}$-equivalent and S is simple (Property 1.2). To show that S is regular, let $s \in S$ and let G be the set of restrictions to As of the elements of the set $\{s' \in S \mid As' = As\}$. Thus because of (d), G is a semigroup of permutations of the finite set As and hence, by Proposition 2.7, must be a group. Let $g \in G$ be the restriction of s to As and let $s' \in S$ be such that its restriction to As is g^{-1}. Thus for any $a \in A$, $ass's = (as)g^{-1}g = as$, so $ss's = s$ and s is regular, Q.E.D.

If $\langle A, S\rangle$ is a transformation semigroup and $\Sigma \subseteq 2^A$, then Σ will be called a *weakly closed cover of* $\langle A, S\rangle$ if and only if Σ is a cover of A and is weakly closed under S. A weakly closed cover Σ of $\langle A, S\rangle$ will be called *irredundant* if and only if for every $\Sigma' \subseteq \Sigma$ if Σ' is a weakly closed cover of $\langle A, S\rangle$ then $\Sigma' = \Sigma$. If A is a set, then $\Sigma \subseteq 2^A$ will be called *normal* if and only if for $B, B' \in \Sigma, B \subseteq B'$ implies $B = B'$. Clearly any irredundant weakly closed cover of $\langle A, S\rangle$ is normal.

LEMMA 2.11. *Let $\langle A, S\rangle$ be a permutation group and let $\Sigma \subseteq 2^A$ be normal and weakly closed under S. Then Σ is closed under S.*

Proof. Let $B \in \Sigma$ and $s \in S$. Let $B', B'' \in \Sigma$ be such that $Bs \subseteq B'$, and $B's^{-1} \subseteq B''$. Then $B = Bss^{-1} \subseteq B's^{-1} \subseteq B''$ and so, since Σ is normal, $B = B'' = B's^{-1}$. Thus $Bs = B's^{-1}s = B'$, and Σ is closed under S,

Q.E.D.

LEMMA 2.12. *Let $\langle A, S\rangle$ be a connected permutation group and Σ an irredundant weakly closed cover of $\langle A, S\rangle$. Then Σ is closed under S and if φ is the homomorphism of S induced by Σ, then $\langle \Sigma, S\varphi\rangle$ is connected.*

Proof. Since Σ is irredundant, it is normal, and hence, by Lemma 2.11, closed under S. Let $B \in \Sigma$ and let $\Sigma' = \{Bs \mid s \in S\}$. Then $\Sigma' \subseteq \Sigma$ and Σ' is closed under S. Let $b \in B$ and $a \in A$ and let $s \in S$ be such that $bs = a$. Then $a \in Bs \in \Sigma'$, so Σ' covers A. Thus $\Sigma' = \Sigma$, since otherwise Σ would not be irredundant. Since $B(s\varphi) = Bs$, this proves that $\langle \Sigma, S\varphi\rangle$ is connected, Q.E.D.

Let A be a set, $\Sigma \subseteq 2^A$, $C \in \Sigma$, and $B \subseteq A$. Then we will say that C *intersects* B *maximally* (with respect to Σ) and call $C \cap B$ a *maximal Σ-intersection with* B if and only if for all $C' \in \Sigma$, if $C \cap B \subseteq C' \cap B$ then $C \cap B = C' \cap B$. Let $\langle A, S\rangle$ be a transformation semigroup, $s \in S$, and $\Sigma \subseteq 2^A$. Then by Σ_s' we will denote the collection of all maximal Σ-intersections with the set As. Clearly Σ_s' is normal. If $f : \Sigma \to 2^A$ is the mapping defined for $B \in \Sigma$ by $Bf = Bs$, then we will say that s *induces* f.

LEMMA 2.13. *Let $\langle A, S\rangle$ be a finite simple transformation semigroup and suppose $\Sigma \subseteq 2^A$ is weakly closed under S. Then for any $s, t \in S$, t induces a one-to-one mapping of Σ_s' onto Σ_t'.*

Proof. For $s \in S$, let s^* be the restriction of s to As. By Theorem 2.10, the set $G_s = \{t^* \mid At = As\}$ is a group of permutations of As. If $C = B \cap As \in \Sigma_s'$, where $B \in \Sigma$, and $At = As$, then by the fact that Σ is weakly closed under S, there exists $B' \in \Sigma$ such that $Bt \subseteq B'$. Thus $Ct^* = Ct = (B \cap As)t \subseteq Bt \cap Ast = Bt \cap At = Bt \cap As \subseteq B' \cap As$. Thus there exists $C' \in \Sigma_s'$ such that $Ct^* \subseteq C'$, so Σ_s' is weakly closed under G_s and hence by Lemma 2.11, Σ_s' is closed under G_s. Now let $s, t \in S$ and

$C = B \cap As \in \Sigma_s'$, where $B \in \Sigma$. Since Σ is weakly closed under S, there exists $B' \in \Sigma$ such that $Bt \subseteq B'$. Since $C \subseteq B$, then $Ct \subseteq B'$. By Theorem 2.10, since $\langle A, S\rangle$ is simple, t maps As one-to-one onto At, and since $C \subseteq As$, then t maps C one-to-one onto $Ct \subseteq At$, so $Ct \subseteq B' \cap At$. Thus $Ct \subseteq D$ for some $D \in \Sigma_t'$. Similarly $Ds \subseteq C'$ for some $C' \in \Sigma_s'$. Since $Ats = As$, then $(ts)^* \in G_s$. Since $C(ts)^* = Cts \subseteq C' \in \Sigma_s'$ and Σ_s' is normal and closed under G_s, then $Cts = C'$, so $|C| = |C'|$. But $|C| = |Ct| \leq |D| = |Ds| \leq |C'|$, so equality holds in each case. Thus $Ct = D$, and t induces a mapping of Σ_s' into Σ_t'. If C, $C' \in \Sigma_s'$ and $Ct = C't$, then $(C \cup C')t = Ct$ and since t is one-to-one on As and $C \cup C' \subseteq As$, then $|C \cup C'| = |C| = |C'|$ so $C' = C$. Thus t induces a one-to-one mapping of Σ_s' into Σ_t'. Since s also induces a one-to-one mapping of Σ_t' into Σ_s' and both are finite, then both mappings are necessarily onto, Q.E.D.

LEMMA 2.14. *Let $\langle A, S\rangle$ be a finite simple accessible transformation semigroup and $\Sigma \subseteq 2^A$ an irredundant weakly closed cover of $\langle A, S\rangle$. Then for each $B \in \Sigma$ there exists $s \in S$ such that B intersects As maximally.*

Proof. Suppose by way of contradiction that $B \in \Sigma$ intersects no As maximally. It will be shown that $\Sigma - \{B\}$ is a weakly closed cover of $\langle A, S\rangle$, and hence that Σ is not irredundant, contrary to the hypothesis of the Lemma. Since $\langle A, S\rangle$ is accessible, then for each $a \in A$ there exists $s \in S$ such that $a \in As$. If $a \in B$ then, since B does not intersect As maximally, there exists $B' \in \Sigma - \{B\}$ such that $B \cap As \subseteq B' \cap As$, so $a \in B'$. This shows that $\Sigma - \{B\}$ is a cover of A. To show that $\Sigma - \{B\}$ is weakly closed under S, one need only note that, because Σ is weakly closed under S, for each $B' \in \Sigma$ and $s \in S$, $B's \subseteq As \cap B''$ for some $B'' \in \Sigma$ which intersects As maximally. Hence $B'' \in \Sigma - \{B\}$, Q.E.D.

Let $\langle A, S\rangle$ be a transformation semigroup, let $\Sigma \subseteq 2^A$, let $S' \subseteq S$, and let ρ be a mapping of S' into $\mathfrak{I}_\Sigma$. Then ρ will be called *Σ-consistent* if and only if for each $s \in S'$ and $B \in \Sigma$, $Bs \subseteq B(s\rho)$.

LEMMA 2.15. *Let $\langle A, S\rangle$ be a finite simple transformation semigroup, let $\Sigma \subseteq 2^A$ be a weakly closed cover of $\langle A, S\rangle$, and let $S' \subseteq S$ be any set of generators of S. Then there exists a Σ-consistent mapping ρ of S' into $\mathfrak{I}_\Sigma$ such that $S'\rho$ generates a simple subsemigroup T of $\mathfrak{I}_\Sigma$. If $\langle A, S\rangle$ is accessible and Σ is irredundant, then ρ can be extended to a homomorphism of S onto T and $\langle \Sigma, T\rangle$ is accessible.*

Proof. Let $\Sigma' = \bigcup_{s \in S} \Sigma_s'$, i.e., Σ' is the collection of all maximal Σ-intersections with the sets As for $s \in S$. Now let f be an arbitrary but fixed mapping of Σ' into Σ such that for each $C \in \Sigma'$, $C \subseteq Cf$. It is clear from

the definition of Σ' that such a mapping exists. For each $s \in S$ let $\Sigma_s = \Sigma_s' f$. Now if $C \in \Sigma_s'$, $C \subseteq B_1 \in \Sigma_s$, and $C \subseteq B_2 \in \Sigma_s$, then we must have $B_1 = C_1 f$ and $B_2 = C_2 f$ for C_1, $C_2 \in \Sigma_s'$, so $C_1 \cup C \subseteq B_1$ and $C_2 \cup C \subseteq B_2$. Thus since C, C_1, and C_2 are maximal Σ-intersections with As, then $C_1 = C = C_2$, so $B_1 = C_1 f = C_2 f = B_2$. This shows that no distinct elements of Σ_s can have the same element of Σ_s' as a subset, and hence that $|\Sigma_s| = |\Sigma_s'|$. Now we are ready to define the mapping ρ of S' into $\mathfrak{I}_\Sigma$. For each $B \in \Sigma$ and $s \in S'$ let $B(s\rho) = B'$, where B' is an arbitrary element of Σ_s such that $Bs \subseteq B'$. That at least one such element exists is evident from the fact that Σ is weakly closed under S; for $Bs \subseteq As$ and there exists $B'' \in \Sigma$ with $Bs \subseteq B''$, so $Bs \subseteq As \cup B''$. Thus $Bs \subseteq C$ for some $C \in \Sigma_s'$, and $C \subseteq B'$ for some $B' \in \Sigma_s$, so $Bs \subseteq B'$. Clearly ρ is Σ-consistent. Now we will prove that for each s, $t \in S'$. $\Sigma_s(t\rho) = \Sigma_t$. From the definition of ρ it is obvious that $\Sigma(t\rho) \subseteq \Sigma_t$. By Lemma 2.13, t induces a one-to-one mapping of Σ_s' onto Σ_t'. If $B \in \Sigma_t$, then $B = Cf$ for some $C \in \Sigma_t'$. Let $C' \in \Sigma_s'$ be such that $C't = C$, and let $B' = C'f \in \Sigma_s$. Then $C = C't \subseteq B't \subseteq B'(t\rho) \in \Sigma_t$. Thus $B'(t\rho) = B$, since both are elements of Σ_t and contain the element C of Σ_t' as a subset. This shows that $\Sigma(t\rho) = \Sigma_s(t\rho) = \Sigma_t$, and hence that the classes $\Sigma(t\rho)$ have the same cardinality for all $t \in S'$, since this is true of the Σ_t. Let T be the subsemigroup of $\mathfrak{I}_\Sigma$ generated by $S'\rho$. Clearly if $t \in T$ then there exist $s_1, \cdots, s_n \in S'$ such that $t = t_1 \cdots t_n$ and $t_j = s_j\rho$ for $1 \leq j \leq n$. Thus $\Sigma t = \Sigma(s_1\rho) \cdots (s_n\rho) = \Sigma(s_n\rho)$, and so the Σt have the same cardinality for all $t \in T$. Thus by Theorem 2.10, T is simple. It remains to show that if $\langle A, S\rangle$ is accessible and Σ is irredundant, then ρ can be extended to a homomorphism of S onto T and $\langle \Sigma, T\rangle$ is accessible. Let $s = s_1 \cdots s_n = r_1 \cdots r_m$ where s_j, $r_i \in S'$, $u_j = s_j\rho$, and $t_i = r_i\rho$ for $1 \leq j \leq n$ and $1 \leq i \leq m$; and let $t = t_1 \cdots t_m \in T$ and $u = u_1 \cdots u_n \in T$. We would like to show that $t = u$, i.e., for every $B \in \Sigma$ that $Bt = Bu$. Now by Theorem 2.10, $As_n = As = Ar_m$, so $\Sigma_{s_n} = \Sigma_{s_n}' f = \Sigma_s' f = \Sigma_s$ and $\Sigma_{r_m} = \Sigma_s$. Also by Theorem 2.10 (since T is simple) $\Sigma t = \Sigma t_m = \Sigma(r_m\rho) = \Sigma_{r_m}$ and $\Sigma u = \Sigma u_n = \Sigma(s_n\rho) = \Sigma_{s_n}$. Thus $\Sigma t = \Sigma u = \Sigma_s$. Now let $B \in \Sigma$. By m and n respective applications of the Σ-consistency of ρ we obtain $Bs \subseteq Bt$ and $Bs \subseteq Bu$. By Lemma 2.14, B intersects As' maximally for some $s' \in S$. Thus $C = B \cap As' \in \Sigma_{s'}'$, so $Cs \in \Sigma_s'$ by Lemma 2.13. Therefore $Cs \subseteq Bs \subseteq Bt \cap Bu$. But Bt and Bu are both elements of Σ_s, and they have a common subset $Cs \in \Sigma_s'$, so it follows that $Bt = Bu$. This completes the proof that $t = u$ and enables us to define a mapping φ of S onto T as follows: for any $s \in S$ let $s = s_1 \cdots s_n$ be any factorization of s

into a product of elements of S' and define $s\varphi = (s_1\rho) \cdots (s_n\rho)$. What we have just shown guarantees that φ is well defined, i.e., independent of the particular factorization chosen. Clearly for $s \in S'$, $s\varphi = s\rho$, i.e., φ is an extension of ρ, and $S\varphi = T$ since $S'\rho$ generates T. Now it is immediate that φ is a homomorphism, for if $r, s \in S$, let $r = r_1 \cdots r_m$, $s = s_1 \cdots s_n$ where $r_i, s_j \in S'$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. Then $(rs)\varphi = (r_1\rho) \cdots (r_m\rho)(s_1\rho) \cdots (s_n\rho) = (r\varphi)(s\varphi)$. Finally to prove that $\langle \Sigma, T\rangle$ is accessible, we notice that $\Sigma' f \subseteq \Sigma$ is a weakly closed cover of $\langle A, S\rangle$ and hence $\Sigma' f = \Sigma$. Thus for each $B \in \Sigma$, there exists $s \in S$ such that $B \in \Sigma_s = \Sigma(s\varphi)$ and hence there exists $B' \in \Sigma$ such that $B'(s\varphi) = B$, Q.E.D.

Let $\langle A, S\rangle$ be a transformation semigroup and $\Sigma \subseteq 2^A$. Then Σ will be said to be *inverse closed* (under S) if and only if for every $B \in \Sigma$ and $s \in S$, $sB(=\{a \in A \mid as \in B\}) \in \Sigma$. By the *inverse closure* of Σ we mean the class $\Sigma \cup \{sB \mid s \in S \text{ and } B \in \Sigma\}$.

Let A be an arbitrary set and $\Sigma \subseteq 2^A$ and define the function f on 2^A by letting $Bf = \bigcap \{B' \in \Sigma \mid B \subseteq B'\}$, where it is to be understood that $\bigcap \emptyset = A$ if $\emptyset$ denotes the empty class of subsets of A. It is clear that f is a closure operation on the complete lattice 2^A (in the sense of Birkhoff (1948), p. 49, that for all $B, C \in 2^A$, $B \subseteq Bf$, $Bff = Bf$, and if $B \subseteq C$ then $Bf \subseteq Cf$), and we will call f *the closure operation on* 2^A *determined by* Σ. A set $B \in 2^A$ will be said to be *closed with respect to* Σ if and only if $Bf = B$.

LEMMA 2.16. *Let $\langle A, S\rangle$ be a transformation semigroup, $\Sigma \subseteq 2^A$, $R \subseteq S$, and ρ a Σ-consistent mapping of R into $\mathfrak{I}_\Sigma$. Let $\Sigma' \subseteq 2^A$ be inverse closed under S. Let f be the closure operation on 2^A determined by Σ'. Let ρ' map R into $\mathfrak{I}_{\Sigma f}$ as follows: if $s \in R$ and $B \in \Sigma$ let $(Bf)(s\rho') = (B(s\rho))f$. Let T and T' be the subsemigroups of $\mathfrak{I}_\Sigma$ and $\mathfrak{I}_{\Sigma f}$ generated by $R\rho$ and $R\rho'$ respectively. Then ρ' is (Σf)-consistent.*

Proof. It is to be shown that $(Bf)s \subseteq (Bf)(s\rho')$ for every $B \in \Sigma$ and $s \in R$. By definition of ρ', this is equivalent to showing that $(Bf)s \subseteq (B(s\rho))f$. By definition of f, $(Bf)s = (\bigcap \{B' \in \Sigma' \mid B \subseteq B'\})s \subseteq \bigcap \{B's \mid B \subseteq B' \in \Sigma'\}$, and because ρ is Σ-consistent and f is a closure operation, $\bigcap \{B' \in \Sigma' \mid Bs \subseteq B'\} = (Bs)f \subseteq (B(s\rho))f$. Thus it would suffice to prove that $\bigcap \{B's \mid B \subseteq B' \in \Sigma'\} \subseteq \bigcap \{B' \in \Sigma' \mid Bs \subseteq B'\}$. Suppose $a \in \bigcap \{B's \mid B \subseteq B' \in \Sigma'\}$. If $a \notin \bigcap \{B' \in \Sigma' \mid Bs \subseteq B'\}$, then there exists $B' \in \Sigma'$ with $Bs \subseteq B'$ but $a \notin B'$. Since Σ' is inverse closed then $sB' \in \Sigma'$. Since $Bs \subseteq B'$ then $B \subseteq sB'$. But $(sB')s \subseteq B'$, so $a \notin \bigcap \{Cs \mid B \subseteq C \in \Sigma'\}$, contrary to assumption. Thus $a \in \bigcap \{B' \in \Sigma \mid Bs \subseteq B'\}$ and the proof is complete, Q.E.D.

COROLLARY 2.17. *If* $\langle A, S\rangle$ *is a transformation semigroup,* $\Sigma \subseteq 2^A$ *is weakly closed under* S, $\Sigma' \subseteq 2^A$ *is inverse closed under* S, *and* f *is the closure operation on* 2^A *determined by* Σ', *then* Σf *is weakly closed under* S.

Proof. Since Σ is weakly closed under S, it is possible to define a Σ-consistent mapping ρ of S into $\mathfrak{I}_\Sigma$. The lemma then yields a (Σf)-consistent mapping of S into $\mathfrak{I}_{\Sigma f}$, so Σf must be weakly closed under S, Q.E.D.

THEOREM 2.18. *Let* $\langle A, S\rangle$ *be a permutation group and let* $\Sigma \subseteq 2^A$ *be closed under* S *and cover* A *and let* Π *be the coarsest partition of* A *refining* Σ. *Then* Π *is closed under* S *and if we denote by* σ *and* π *the homomorphisms of* S *induced by* Σ *and* Π *respectively, then* $S\sigma \cong S\pi$.

Proof. Clearly the class $A' = \{\{a\} \mid a \in A\}$ is closed under S. Since the elements of S are one-to-one mappings, and each has its inverse in S, then Σ is inverse closed. Let f be the closure operation on 2^A determined by Σ. Then clearly $A'f = \Pi$ and by Corollary 2.17, $A'f$ is weakly closed under S. Since Π is a partition, it is normal and hence closed under S (Lemma 2.11). Suppose $s_1\sigma = s_2\sigma$ and $P \in \Pi$, $P = \{a\}f$. Thus $Bs_1 = Bs_2$ for all $B \in \Sigma$. Then since s_1 and s_2 are one-to-one mappings, $P(s_1\pi) = Ps_1 = (\bigcap \{B \in \Sigma \mid a \in B\})s_1 = \bigcap \{Bs_1 \mid a \in B \in \Sigma\} = \bigcap \{Bs_2 \mid a \in B \in \Sigma\} = (\bigcap \{B \in \Sigma \mid a \in B\})s_2 = Ps_2 = P(s_2\pi)$. Thus, $s_1\pi = s_2\pi$. This shows that by letting $t\varphi = s\pi$ for $t = s\sigma \in S\sigma$ we get a mapping φ of $S\sigma$ into $S\pi$. Since σ and π are homomorphisms, it is immediate that φ is a homomorphism of $S\sigma$ onto $S\pi$. Suppose $(s_1\sigma)\varphi = (s_2\sigma)\varphi$, so $s_1\pi = s_2\pi$. Since any $B \in \Sigma$ is a union of elements of Π, it follows that $s_1\sigma = s_2\sigma$. Thus φ is an isomorphism, Q.E.D.

3. MACHINES

An (incompletely-specified finite-state sequential deterministic) *machine* (with input alphabet X and output alphabet Y) is a quadruple $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ where A is a finite set called the set of states of $\mathfrak{A}$, S is a subsemigroup of $\mathfrak{I}_A$, σ is a homomorphism of the free semigroup F on X onto S, and α is a mapping of a subset of A into Y. This is equivalent to the usual definition of a Moore-type machine (without initial state) in terms of a completely specified transition function; for such a function simply maps each element of X to a transformation of the states of the machine and can thus be extended uniquely to a homomorphism of F into $\mathfrak{I}_A$ by Property 1.5. Machines with incompletely-specified transition functions can be reduced to the above model by introducing a "sink state". (See Narasimhan, 1961.) The machine $\mathfrak{A}$ defined above is said to be complete if α is defined on all of A. All machines in this paper will be

assumed to have input alphabet X and output alphabet Y. The free semigroup on X will be denoted throughout by F. Given the machine $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$, we will denote by $\bar{\sigma}$ the extension of σ to $F^1 = F \cup \{1\}$ obtained by letting $1\bar{\sigma}$ be the identity transformation of A. Here the identity 1 of F^1 may be thought of as the null string. It is clear that the mapping $\bar{\sigma}: F^1 \to \mathfrak{I}_A$ is a homomorphism. We will consistently identify an element x of X with the string consisting of x alone, i.e., $X \subseteq F$. The *behavior* β_a *of* $\mathfrak{A}$ *in state* $a (a \in A)$ is the mapping of a subset of F^1 to Y defined by letting $f\beta_a = (a(f\bar{\sigma}))\alpha$, if the latter is defined, and leaving $f\beta_a$ undefined otherwise. If $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ is a machine, $a \in A$ and $b \in B$, then we define $a \leq b$ to mean $\beta_a \subseteq \beta_b$, i.e., for all $f \in F^1$ if $f\beta_a$ is defined, then $f\beta_b$ is defined and they are equal. If for every $a \in A$ there exists $b \in B$ such that $a \leq b$, then we shall write $\mathfrak{A} \leq \mathfrak{B}$ and say that $\mathfrak{B}$ *satisfies* $\mathfrak{A}$. In case $\mathfrak{A} \leq \mathfrak{B}$ and no machine with fewer states than $\mathfrak{B}$ satisfies $\mathfrak{A}$, we write $\mathfrak{A} \leq_m \mathfrak{B}$ and say that $\mathfrak{B}$ is a *minimum state machine for* $\mathfrak{A}$. Two states a and b of $\mathfrak{A}$ are said to be *compatible* if and only if β_a and β_b agree on the intersection of their domains, i.e. for all $f \in F^1$ if $f\beta_a$ and $f\beta_b$ are both defined, then they are equal. A set C of states of $\mathfrak{A}$ is said to be compatible if and only if $C \neq \emptyset$ and all pairs of states in C are compatible. Given the machine $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$, we may refer to the semigroup S of $\mathfrak{A}$ or to the transformation semigroup $\langle A, S\rangle$ of $\mathfrak{A}$. In case $\langle A, S\rangle$ is a permutation group, we will say that $\mathfrak{A}$ is a *permutation machine*, and in case S is a simple [commutative] semigroup, we will say a *simple* [*commutative*] machine. If $\langle A, S\rangle$ is accessible [connected], then we say that $\mathfrak{A}$ is *accessible* [*connected*].

PROPOSITION 3.1. *Let* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *and* $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ *be machines such that* $\mathfrak{A} \leq \mathfrak{B}$. *If* $a \in A$ *and* $b \in B$ *are such that* $a \leq b$ *and* $f \in F^1$, *then* $a(f\sigma) \leq b(f\tau)$.

Proof. If $(a(f\sigma)(g\sigma))\alpha$ is defined and equals y then since $a(f\sigma)(g\sigma) = a((fg)\sigma)$, it follows that $(b((fg)\tau))\beta$ is defined and equals y. But $b((fg)\tau) = b(f\tau)(g\tau)$. Thus $a(f\sigma) \leq b(f\tau)$, Q.E.D.

Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$, and $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ be machines such that $\mathfrak{A} \leq \mathfrak{B}$. We define $A_b = \{a \in A \mid a \leq b\}$ for each $b \in B$ and let $\Sigma = \{A_b \mid b \in B \text{ and } A_b \neq \emptyset\}$. Then Σ will be called the *projection of* $\mathfrak{B}$ onto $\mathfrak{A}$. A class $\Sigma \subseteq 2^A$ will be called a *C-class for* $\mathfrak{A}$ if and only if it satisfies the following conditions: (1) Σ covers A, (2) each element of Σ is compatible, and (3) Σ is weakly closed under S. Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ be a machine and $\Sigma \subseteq 2^A$. Let $\mathfrak{B} = \langle \Sigma, T, \tau, \beta\rangle$ be a machine satisfying the following conditions: (1) the mapping which takes $x\sigma$ to $x\tau$ for all

$x \in X$ is a Σ-consistent mapping of $X\sigma$ into $\mathfrak{I}_\Sigma$, and (2) for all $B \in \Sigma$, if there exists $a \in B$ with $a\alpha$ defined, then $B\beta$ is defined and $B\beta = a\alpha$. Then we will say that $\mathfrak{B}$ is a *construct of* $\mathfrak{A}$ *with* Σ. It is an immediate consequence of this definition that for all $f \in F^1$ and $B \in \Sigma$ we have $B(f\bar{\sigma}) \subseteq B(f\tau)$. Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ and $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ be machines and let φ be a mapping of A onto B such that for all $a \in A$ and $x \in X$, $(a(s\sigma))\varphi = (a\varphi)(x\tau)$. Then φ will be called a *homomorphism* of $\mathfrak{A}$ onto $\mathfrak{B}$. If, in addition to being a homomorphism, φ has the property that whenever $a\alpha$ is defined then $(a\varphi)\beta$ is defined and $(a\varphi)\beta = a\alpha$, then we will say that φ is a *machine* homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$. If φ is a one-to-one homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$, then it will be called an *isomorphism* of $\mathfrak{A}$ onto $\mathfrak{B}$ and $\mathfrak{A}$ and $\mathfrak{B}$ will be said to be *isomorphic*; if φ is a one-to-one machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ such that φ^{-1} is a machine homomorphism of $\mathfrak{B}$ onto $\mathfrak{A}$, then φ will be called a *machine isomorphism* of $\mathfrak{A}$ onto $\mathfrak{B}$, and we say that $\mathfrak{A}$ and $\mathfrak{B}$ are *machine isomorphic*. If there is an isomorphism of $\mathfrak{B}$ onto $\mathfrak{A}$, which is also a machine homomorphism, then we will say that $\mathfrak{B}$ is a *restriction* of $\mathfrak{A}$. If Σ is a C-class for $\mathfrak{A}$ which is closed under S, then by the *natural construct* of $\mathfrak{A}$ with Σ, we mean the construct $\mathfrak{B} = \langle \Sigma, T, \tau, \beta\rangle$ of $\mathfrak{A}$ with Σ obtained by defining $B(x\tau) = B(x\sigma)$ for all $B \in \Sigma$ and $x \in X$ and by leaving $B\beta$ undefined unless there exists $a \in B$ with $a\alpha$ defined (in which case $B\beta$ must be defined equal to $a\alpha$).

PROPOSITION 3.2. *Let* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *and* $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ *be machines and let* φ *be a homomorphism of* $\mathfrak{A}$ *onto* $\mathfrak{B}$. *Then* T *is a homomorphic image of* S. *If* φ *is an isomorphism then* $S \cong T$.

Proof. For each $s \in S$ and $a \in A$ we define $(a\varphi)(s\psi) = (as)\varphi$ and claim that the mapping ψ so defined is a homomorphism of S onto T. Clearly ψ maps S into $\mathfrak{I}_B$, since each $b \in B$ is of the form $a\varphi$ for some $a \in A$, so that $b(s\psi) = (as)\varphi$ is well defined. To prove that ψ is a homomorphism let $s, s' \in S$. It must be shown that $(s's)\psi = (s'\psi)(s\psi)$ i.e. for every $a \in A$ that $(a\varphi)((s's)\psi) = (a\varphi)(s'\psi)(s\psi)$. But $(a\varphi)((s's)\psi) = (as's)\varphi = ((as')\varphi)(s\psi) = ((a\varphi)(s'\psi))(s\psi) = (a\varphi)((s'\psi)(s\psi))$. Since φ is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$, for any $a \in A$ and $x \in X$, $(a\varphi)(x\sigma\psi) = (a(x\sigma))\varphi = (a\varphi)(x\tau)$. Thus $x\sigma\psi = x\tau$ for all $x \in X$. By Property 1.5, since $\sigma\psi$ is a homomorphism of F into $\mathfrak{I}_B$, then $\sigma\psi = \tau$. Thus $S\psi = F\sigma\psi = F\tau = T$. If φ is an isomorphism, then clearly ψ is also, Q.E.D.

PROPOSITION 3.3. *If* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *is a machine,* Σ *is a* C*-class for* $\mathfrak{A}$ *which is closed under* S, $\beta = \langle \Sigma, T, \tau, \beta\rangle$ *is the natural construct of* $\mathfrak{A}$ *with* Σ, *and* φ *the homomorphism of* S *induced by* Σ, *then* $\tau = \sigma\varphi$ *and* $S\varphi = T$.

Proof. By definition of the natural construct, $B(x\tau) = B(x\sigma)$ for each $B \in \Sigma$ and $x \in X$. Thus $x\tau = (x\sigma)\varphi$ for $x \in X$. Since σ is a homomorphism of F onto S and φ a homomorphism of S into $\mathfrak{I}_\Sigma$, then $\sigma\varphi$ is a homomorphism of F into $\mathfrak{I}_\Sigma$ which agrees with τ on X. Thus $\sigma\varphi = \tau$ by Property 1.5, and $S\varphi = F\sigma\varphi = F\tau = T$, Q.E.D.

Propositions 3.4, 3.5, and 3.6 are essentially due to Paull and Unger (1959).

PROPOSITION 3.4. *If $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ is a machine and Σ is a C-class for $\mathfrak{A}$, then there exists at least one construct of $\mathfrak{A}$ with Σ. If $\mathfrak{B}$ is any such construct then $\mathfrak{A} \leq \mathfrak{B}$.*

Proof. Let τ be the unique homomorphic extension, (see Property 1.5), of the mapping $\tau' : X \to \mathfrak{I}_\Sigma$ defined by letting $B(x\tau') = B'$, where B' is such that $B(x\sigma) \subseteq B'$. (Such an element B' must exist for each $B \in \Sigma$ and $x \in X$ by the fact that Σ is weakly closed under S). Let $T = F\tau$ and let $\beta : \Sigma \to Y$ be such that $B\beta = a\alpha$ for each $a \in B$ for which $a\alpha$ is defined. Since B is compatible this is always possible. It is clear that $\langle \Sigma, T, \tau, \beta\rangle$ is a construct of $\mathfrak{A}$ with Σ. Now let $\mathfrak{B} = \langle \Sigma, T, \tau, \beta\rangle$ be any such construct. It will be shown that if $a \in B \in \Sigma$, then $a \leq B$. Since Σ covers A it will follow that $\mathfrak{A} \leq \mathfrak{B}$. Suppose then that $(a(f\bar{\sigma}))\alpha$ is defined and equals y. Then $a(f\bar{\sigma}) \in B(f\bar{\sigma}) \subseteq B(f\bar{\tau}) \in \Sigma$, so $(B(f\bar{\tau}))\beta$ is defined and equals y. Thus $\mathfrak{A} \leq \mathfrak{B}$, Q.E.D.

PROPOSITION 3.5. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ and $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ be machines such that $\mathfrak{A} \leq \beta$ and let $\Sigma = \{A_b \mid b \in B \text{ and } A_b \neq \emptyset\}$ be the projection of $\mathfrak{B}$ onto $\mathfrak{A}$ (where $A_b = \{a \in A \mid a \leq b\}$). Then Σ is a C-class for $\mathfrak{A}$, and in fact $A_b(f\bar{\sigma}) \subseteq A_{b(f\bar{\tau})}$ for all $f \in F^1$ and $b \in B$. Moreover there exists a construct $\mathfrak{B}'$ of $\mathfrak{A}$ such that $\mathfrak{A} \leq \mathfrak{B}' \leq \mathfrak{B}$ and such that if $\mathfrak{A} \leq_m \mathfrak{B}$, then $\mathfrak{B}'$ is machine isomorphic to $\mathfrak{B}$.*

Proof. That Σ covers A is evident from the definition of $\leq$. Suppose $a \leq b$ and $a' \leq b$, so $\beta_a \subseteq \beta_b$ and $\beta_{a'} \subseteq \beta_b$. Thus if $(a(f\bar{\sigma}))\alpha$ and $(a'(f\bar{\sigma}))\alpha$ are both defined, then they are both equal to $(b(f\bar{\tau}))\beta$ and hence equal to each other. Thus A_b is compatible. If $a \in A_b$, then $a \leq b$ so $a(f\bar{\sigma}) \leq b(f\bar{\tau})$ by Proposition 3.1, i.e. $a(f\bar{\sigma}) \in A_{b(f\bar{\tau})}$. Thus $A_b(f\bar{\sigma}) \subseteq A_{b(f\bar{\tau})}$ and Σ is weakly closed under S, and a C-class for $\mathfrak{A}$. Now let $A_b(x\tau_0') = A_{b(x\tau)}$ for $x \in X$ and $b \in B$ and let τ' be the unique extension of the mapping $\tau_0' : X \to \mathfrak{I}_\Sigma$ to a homomorphism of F (Property 1.5). Let $T' = F\tau'$; let $A_b\beta'$ be defined equal to y if $b'\beta = y$ for all $b' \in B$ such that $A_b = A_{b'}$, and leave $A_b\beta'$ undefined otherwise. Finally let $\mathfrak{B}' = \langle \Sigma, T', \tau', \beta'\rangle$. Clearly $\mathfrak{B}'$ is a construct of $\mathfrak{A}$ with Σ, so $\mathfrak{A} \leq \mathfrak{B}'$ by Proposition 3.4. Now we will show that $A_b \leq b$ for each $b \in B$. Thus suppose $(A_b(f\bar{\tau'}))\beta'$

is defined and equals y. Since $A_b(f\bar{\tau}') = A_{b(f\bar{\tau})}$ then $(b(f\bar{\tau}))\beta$ is defined and equals y. Thus $A_b \leq b$ and so $\mathfrak{B}' \leq \mathfrak{B}$. Now if $\mathfrak{A}^m \leq \mathfrak{B}$ then the mapping φ which takes $b \in B$ to $A_b \in \Sigma$ must be one-to-one, for otherwise $\mathfrak{B}$ would not be a minimum state machine for $\mathfrak{A}$. By definition of τ' and β', for all $b \in B$ and $x \in X$, $(b(x\tau))\varphi = (b\varphi)(x\tau')$, and $b\beta$ is defined and equal to y if and only if $(b\varphi)\beta'$ is defined and equal to y. Thus $\mathfrak{B}'$ is machine isomorphic to $\mathfrak{B}$, Q.E.D.

If $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ is a machine, then Σ will be called a *minimum C-class for* $\mathfrak{A}$ if and only if (1) Σ is a C-class for $\mathfrak{A}$ and (2) there exists no C-class for $\mathfrak{A}$ having cardinality less than that of Σ.

PROPOSITION 3.6. *The minimum state machines for a machine* $\mathfrak{A}$ *are, up to machine isomorphism, the constructs of* $\mathfrak{A}$ *with its minimum C-classes.*

Proof. From Proposition 3.5 it is evident that any minimum state machine for $\mathfrak{A}$ is isomorphic to a construct of $\mathfrak{A}$ with some C-class Σ for $\mathfrak{A}$. If Σ were not a minimum C-class for $\mathfrak{A}$ then $\mathfrak{B}$ would not be a minimum state machine for $\mathfrak{A}$, by Proposition 3.4. Given any minimum C-class Σ for $\mathfrak{A}$ and any construct $\mathfrak{B}$ of $\mathfrak{A}$ with Σ, then it is immediate from Propositions 3.5 and 3.4 that $\mathfrak{A} \leq_m \mathfrak{B}$, Q.E.D.

PROPOSITION 3.7. *Let* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *be a machine and let* Σ *be a C-class for* $\mathfrak{A}$ *which is a partition of* A. *Let* $\mathfrak{B} = \langle \Sigma, T, \tau, \beta\rangle$ *be any construct of* $\mathfrak{A}$ *with* Σ. *Then there is a machine homomorphism of* $\mathfrak{A}$ *onto* $\mathfrak{B}$.

Proof. Let $\varphi : A \to \Sigma$ be the natural mapping, i.e. $a\varphi = B$ if and only if $a \in B$. Let $a \in B \in \Sigma$ and $x \in X$, so $a\varphi = B$. Then $(a\varphi)(x\tau) = B(x\tau)$ and $a(x\sigma) \in B(x\sigma) \subseteq B(x\tau) \in \Sigma$, so $(a(x\sigma))\varphi = B(x\tau) = (a\varphi)(x\tau)$. Clearly $(a\varphi)\beta = a\alpha$ whenever the latter is defined. This shows that φ is a machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$, Q.E.D.

If $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ is a machine, then $C \subseteq A$ will be called a *maximal compatible of* $\mathfrak{A}$ if and only if C is compatible and not a proper subset of any compatible (set of states) of $\mathfrak{A}$. Let Φ be the collection of all maximal compatibles of $\mathfrak{A}$, Ω the inverse closure of Φ in the transformation semigroup $\langle A, S\rangle$, and φ the closure operation on 2^A determined by Ω. We will call φ *the closure operation of* $\mathfrak{A}$, and define $B \subseteq A$ to be a *closed* set of states of $\mathfrak{A}$ if and only if $B\varphi = B$.

Remarks. In case Φ happens to be a partition, then it is a minimum C-class for $\mathfrak{A}$ and all constructs of $\mathfrak{A}$ with Φ (and hence all minimum state machines for $\mathfrak{A}$) are isomorphic, and there is, by Proposition 3.7, a machine homomorphism of $\mathfrak{A}$ onto any minimum state machine for $\mathfrak{A}$. This is the case in particular when $\mathfrak{A}$ is complete, and then in addition all minimum state machines are machine isomorphic. (See Moore,

1956.) In general Φ is not a partition and, though it is always a C-class, is not a minimum C-class. The definition of a closed set of states of a machine given here is equivalent to that used in Beatty and Miller (1963) when allowance is made for the difference in the models used. This will be proved elsewhere. Given this equivalence, Theorem 3.8 and Corollary 3.9 are closely related to results presented in Beatty and Miller (1963).

THEOREM 3.8. *Let* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *be a machine, and* φ *the closure operation of* $\mathfrak{A}$. *Let* Σ *be a* C*-class for* $\mathfrak{A}$ *and let* $\Sigma' = \Sigma\varphi$. *Then* Σ' *is a* C*-class for* $\mathfrak{A}$, *and if* $\mathfrak{B} = \langle \Sigma, T, \tau, \beta\rangle$ *is a construct of* $\mathfrak{A}$ *with* Σ *then there is a construct* $\mathfrak{B}' = \langle \Sigma', T', \tau', \beta'\rangle$ *of* $\mathfrak{A}$ *with* Σ' *such that* φ *is a homomorphism of* $\mathfrak{B}$ *onto* $\mathfrak{B}'$.

Proof. Let Φ be the class of all maximal compatibles of $\mathfrak{A}$ and Ω the inverse closure of Φ. If $B \in \Sigma$ then B is compatible, so $B \subseteq C$ for some $C \in \Phi \subseteq \Omega$ so $B\varphi \subseteq C\varphi = C$, and $B\varphi$ is compatible. Since Σ is weakly closed under S then Σ' is also, by Corollary 2.17. Since Σ covers A, then so does Σ'. Thus Σ' is a C-class for $\mathfrak{A}$. The set $R = \{x\sigma \mid x \in X\}$ generates S and the mapping ρ which takes $x\sigma$ to $x\tau$ is Σ-consistent by the fact that $\mathfrak{B}$ is a construct of $\mathfrak{A}$ with Σ. We define the mapping $\rho' : R \to \mathfrak{I}_{\Sigma'}$ from ρ and φ as in Lemma 2.16, namely let $(B\varphi)(s\rho') = (B(s\rho))\varphi$ for $B \in \Sigma$ and $s \in R$. Define $x\tau_0' = (x\sigma)\rho'$ for $x \in X$, let τ' be the unique extension of τ_0' to a homomorphism of F (Property 1.5), and let $T' = F\tau'$. Clearly T and T' are the semigroups generated by $R\rho$ and $R\rho'$ respectively. To complete the definition of $\mathfrak{B}'$, we define β' for $B \in \Sigma'$ such that $B\beta' = a\alpha$ if $a \in B$ and $a\alpha$ is defined, and it is clear that $\mathfrak{B}'$ is a construct of $\mathfrak{A}$ with Σ'. From the definition of ρ and ρ' we conclude for $B \in \Sigma$ and $x \in X$ that $(B(x\tau))\varphi = (B(x\sigma\rho))\varphi = (B\varphi)((x\sigma)\rho') = (B\varphi)(x\tau')$ so that α is a homomorphism of $\mathfrak{B}$ onto $\mathfrak{B}'$, Q.E.D.

COROLLARY 3.9. *If* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *and* $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ *are machines such that* $\mathfrak{A} \leq_m \mathfrak{B}$, *then there exists a* C*-class* Σ' *for* $\mathfrak{A}$ *consisting entirely of closed sets of states of* $\mathfrak{A}$, *and a construct* $\mathfrak{B}'$ *of* $\mathfrak{A}$ *with* Σ' *which is isomorphic to* $\mathfrak{B}$.

Proof. By Proposition 3.6 $\mathfrak{B}$ is machine isomorphic to a construct of $\mathfrak{A}$ with Σ, where Σ is some minimum C-class for $\mathfrak{A}$. If we define φ, Σ', τ', T', β' and $\mathfrak{B}'$ as in Theorem 3.8, then Σ' consists entirely of closed sets, (since φ is a closure operation, $(B\varphi)\varphi = B\varphi$). Since $\Sigma' = \Sigma\varphi$ is a C-class for $\mathfrak{A}$, then the homomorphism φ must be one-to-one and hence an isomorphism of $\mathfrak{B}$ onto $\mathfrak{B}'$. Q.E.D.

LEMMA 3.10. *Let* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *be a machine and let* $a, b \in A$ *be compatible and* $s \in S$. *Then* as *and* bs *are compatible.*

Proof. Let $f \in F$ be such that $s = f\sigma$ and let $g \in F^1$ be arbitrary. Suppose $(as(g\bar{\sigma}))\alpha$ and $(bs(g\bar{\sigma}))\alpha$ are both defined. Since a and b are compatible and $s(g\bar{\sigma}) = (fg)\bar{\sigma}$ then $(as(g\bar{\sigma}))\alpha = (bs(g\bar{\sigma}))\alpha$, Q.E.D.

By the *intersection closure* of a class $\Sigma \subseteq 2^A$ is meant the class $\{\bigcap\Sigma' \mid \emptyset \neq \Sigma' \subseteq \Sigma\}$.

LEMMA 3.11. *Let* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *be a permutation machine. Then the class of closed compatible sets of states of* $\mathfrak{A}$ *is the intersection closure of the class* Φ *of all maximal compatibles of* $\mathfrak{A}$.

Proof. By Lemma 2.11, Φ is closed under S, for it is weakly closed under S by Lemma 3.10 and normal. Also if $B \in \Phi$ and $s \in S$ then $sB = Bs^{-1} \in \Sigma$, since elements of S are one-to-one mappings. Thus Φ is inverse closed hence equal to its inverse closure, so $B \subseteq A$ is closed if and only if $B = \bigcap\{B' \in \Phi \mid B \subseteq B'\}$ if and only if B is an element of the intersection closure of Φ. Q.E.D.

COROLLARY 3.12. *Any minimum state machine for a permutation machine* $\mathfrak{A}$ *is isomorphic to a construct of* $\mathfrak{A}$ *with a C-class* Σ *for* $\mathfrak{A}$ *consisting only of intersections of maximal compatibles of* $\mathfrak{A}$.

A C-class for a machine $\mathfrak{A}$ will be called irredundant if and only if it has no proper subclass which is a C-class for $\mathfrak{A}$.

THEOREM 3.13. *If* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *is a simple machine* (i.e. S *is a simple semigroup*) *and* Σ *is a C-class for* $\mathfrak{A}$, *then there exists a simple construct* $\mathfrak{B} = \langle \Sigma, T, \tau, \beta\rangle$ *of* $\mathfrak{A}$ *with* Σ. *Moreover, if* Σ *is an irredundant C-class and* $\mathfrak{A}$ *is accessible, then* T *is a homomorphic image of* S *and* $\mathfrak{B}$ *is accessible.*

Proof. Since Σ is a weakly closed cover of the transformation semigroup $\langle A, S\rangle$ and $R = X\sigma$ generates S, then by Lemma 2.15 there exists a Σ-consistent function ρ of R into $\mathfrak{I}_\Sigma$ such that $R\rho$ generates a simple subsemigroup of $\mathfrak{I}_\Sigma$. Let $x\tau' = (x\sigma)\rho$ for $x \in X$, let τ be the unique extension of τ' to a homomorphism of F into $\mathfrak{I}_\Sigma$, and let $T = F\tau$. Then $X\tau' = R\rho$ and $X\tau'$ generates T, so T is simple by Lemma 2.15. Defining β such that $B\beta = a\alpha$ whenever $a \in B$ and $a\alpha$ is defined, we see that $\mathfrak{B} = \langle \Sigma, T, \tau, \beta\rangle$ is a simple construct of $\mathfrak{A}$ with Σ. If Σ is an irredundant C-class for $\mathfrak{A}$ and $\mathfrak{A}$ is accessible, then Σ is an irredundant weakly closed cover of the accessible transformation semigroup $\langle A, S\rangle$. So by Lemma 2.15, ρ can be extended to a homomorphism of S onto T and $\langle \Sigma, T\rangle$ is accessible, Q.E.D.

COROLLARY 3.14. *Every simple machine has at least one simple minimum state machine.*

Proof. Let Σ be a minimum C-class for the simple machine $\mathfrak{A}$. By Theorem 3.13 there is a simple construct $\mathfrak{B}$ of $\mathfrak{A}$ with Σ. By Proposition 3.6, $\mathfrak{B}$ is a minimum state machine for $\mathfrak{A}$, Q.E.D.

COROLLARY 3.15. *If $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ is a simple accessible machine, then $\mathfrak{A}$ has at least one simple accessible minimum state machine $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ such that T is a homomorphic image of S.*

Proof. Let Σ be any minimum C-class for $\mathfrak{A}$. Then Σ must be irredundant, so the construct $\mathfrak{B}$ of $\mathfrak{A}$ with Σ defined in Theorem 3.13 has the desired properties, Q.E.D.

Remark. One might also ask whether the related property of 0-simplicity can always be preserved in at least one minimum state machine. Fig. 1 shows this to be false by exhibiting a machine with a 0-simple semigroup and all of its minimum state machines, none of whose semigroups even has a 0. Notice that in the figures a machine $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ is given in the conventional form of a directed graph with a node for each element of A and an edge directed from $a \in A$ to $b \in A$ and labeled by $x \in X$ if and only if $a(x\sigma) = b$. Moreover, the node a is labeled y if and only if $a\alpha = y$ and provided with a dash in case $a\alpha$ is undefined. That not *every* minimum state machine for a simple accessible machine need even be simple is illustrated by Fig. 2.

PROPOSITION 3.16. *If $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ is a connected permutation machine and there is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B} = \langle B, T, \sigma, \beta\rangle$ then $|B|$ divides $|A|$.*

Proof. It is clear that if φ is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ then the sets $P_b = \{a \in A \mid a\varphi = b\}$ are mapped onto each other by each $s \in S$. Since $\langle A, S\rangle$ is transitive, it follows that the P_b all have the same cardinality, so $|B|$ divides $|A|$, Q.E.D.

THEOREM 3.17. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ be a permutation machine, let $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ be a minimum state machine for $\mathfrak{A}$, and let Σ be the projection of $\mathfrak{B}$ onto $\mathfrak{A}$. Then Σ is closed under S and if $\mathfrak{B}' = \langle \Sigma, T', \tau', \beta'\rangle$ is the natural construct of $\mathfrak{A}$ with Σ, then $\mathfrak{A} \leq \mathfrak{B}' \leq \mathfrak{B}$ and $\mathfrak{B}'$ is a restriction of $\mathfrak{B}$.*

Proof. Since Σ is a minimum C-class for $\mathfrak{A}$, it is certainly an irredundant weakly closed cover of $\langle A, S\rangle$ and hence normal. Thus by Lemma 2.11, since $\langle A, S\rangle$ is a permutation group, then Σ is closed under S. By Proposition 3.5, $\mathfrak{B}$ is isomorphic to a construct of $\mathfrak{A}$ with Σ, so we

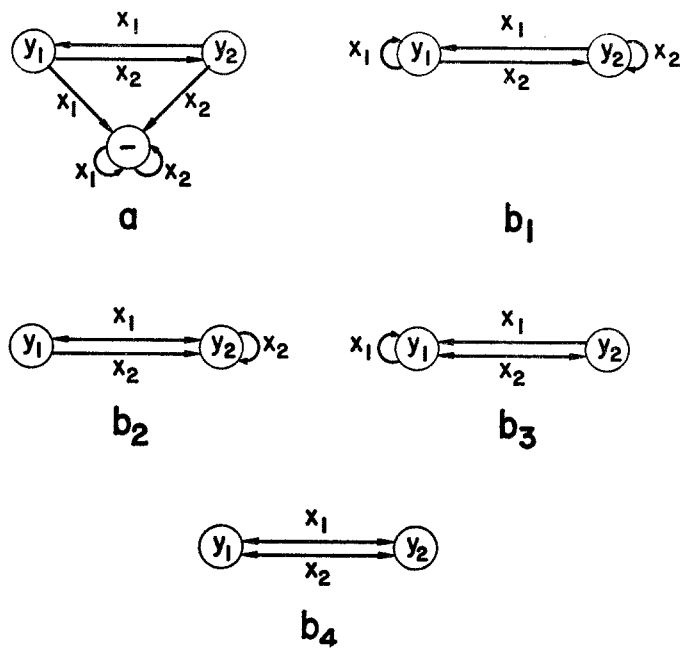

FIG. 1. A 0-simple machine (a) and all of its minimum state machines (b_1–b_4) (none of whose semigroups has a zero).

may write $\mathfrak{B} = \langle \Sigma, T, \tau, \beta \rangle$, and if $C \in \Sigma$ and $x \in X$, then $C(x\tau') = C(x\sigma) \subseteq C(x\tau)$. But Σ is normal, so $C(x\tau') = C(x\tau)$ and hence $\tau = \tau'$ by Property 1.5, showing that $\mathfrak{B}$ and $\mathfrak{B}'$ are isomorphic. If $C\beta' = y$ then there exists $a \in C$ such that $a\alpha = y$ and since $\mathfrak{B}$ is a construct of $\mathfrak{A}$ with Σ then $C\beta = y$. This proves that $\mathfrak{B}'$ is a restriction of $\mathfrak{B}$, Q.E.D.

COROLLARY 3.18. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha \rangle$ be a permutation machine and let $\mathfrak{B} = \langle B, T, \tau, \beta \rangle$ be a minimum state machine for $\mathfrak{A}$. Then $\mathfrak{B}$ is a permutation machine, and there is a homomorphism φ of S onto T such that $\tau = \sigma\varphi$ and such that if $a \in A$, $b \in B$, $s \in S$ and $a \leq b$, then $as \leq b(s\varphi)$. Moreover, if $\mathfrak{A}$ is connected then $\mathfrak{B}$ is also connected.*

Proof. Let Σ be the projection of $\mathfrak{B}$ onto $\mathfrak{A}$ and let $\mathfrak{B}'$ be the natural construct of $\mathfrak{A}$ with Σ (which is closed under S by Theorem 3.17). By Theorem 3.17 we may write $\mathfrak{B}' = \langle \Sigma, T, \tau, \beta' \rangle$ since $\mathfrak{B}'$ is a restriction of $\mathfrak{B}$. By Proposition 3.3 if φ is the homomorphism of S induced by Σ, then $\tau = \sigma\varphi$ and $S\varphi = T$. Now if $a \leq b$ and $s = f\sigma$, then $s\varphi = f\sigma\varphi = f\tau$, and by Proposition 3.1, $a(f\sigma) \leq b(f\tau)$. Thus $as \leq b(s\varphi)$. Since Σ is a

minimum C-class for $\mathfrak{A}$ then Σ is an irredundant weakly closed cover of the permutation group $\langle A, S\rangle$. Thus if $\langle A, S\rangle$ is connected, then $\langle \Sigma, S\varphi\rangle$ is connected, byLemma 2.12, Q.E.D.

Remark. Corollary 3.18 confirms the conjecture of C. C. Elgot referred to in Schützenberger (1962) that any minimum state machine for a permutation machine is a permutation machine.

COROLLARY 3.19. *If* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *is a connected permutation machine such that* $\mathfrak{A} \leq_m \mathfrak{B} = \langle B, T, \tau, \beta\rangle$, *then* $|B|$ *divides* $|S|$.

Proof. Since $\langle B, T\rangle$ is a connected permutation group by Corollary 3.18, then $|B|$ divides $|T|$ by Proposition 2.3. Since T is a homomorphic image of S, then $|T|$ divides $|S|$. Thus $|B|$ divides $|S|$, Q.E.D.

COROLLARY 3.20. *Let* $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ *be a connected permutation machine and* $\mathfrak{A} \leq_m \mathfrak{B} = \langle B, T, \tau, \beta\rangle$. *Let* $A_b = \{a \in A \mid a \leq b\}$ *for* $b \in B$ *and* $B_a = \{b \in B \mid a \leq b\}$ *for* $a \in A$. *Then the* A_b *all have the same cardinality* n, *and the* B_a *all have the same cardinality* m. *Moreover,* $|B|n = |A|m$.

Proof. By Theorem 3.17 and Corollary 3.18, $\mathfrak{B}$ is isomorphic to the natural construct of $\mathfrak{A}$ with $\Sigma = \{A_b \mid b \in B\}$ and $\mathfrak{B}$ is connected. Thus for any C, $C' \in \Sigma$ there exists $s \in S$ such that $Cs = C'$. Since s is a one-to-one mapping, then $|C| = |C'|$. Thus the A_b all have the same cardinality n. Now we wish to show that $\Sigma' = \{B_a \mid a \in A\}$ is closed under T, and hence that the B_a all have the same cardinality m. Let φ be the homomorphism of S onto T given by Corollary 3.18. We will show that $B_a(s\varphi) = B_{as}$ for $a \in A$ and $s \in S$. First suppose $b \in B_a$ so $a \leq b$. Thus $as \leq b(s\varphi)$ by Corollary 3.18, so $b(s\varphi) \in B_{as}$, and

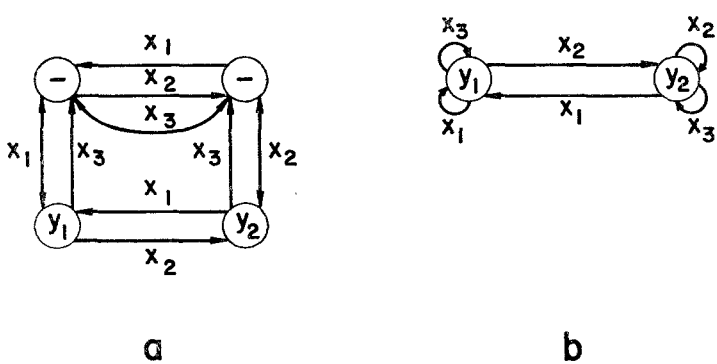

FIG. 2. A simple machine (a) with a non-simple minimum state machine (b)

$B_a(s\varphi) \subseteq B_{as}$. Now let $b \in B_{as}$ so $as \leq b$. Again by Corollary 3.18, $a \leq b(s^{-1}\varphi)$ so $b(s^{-1}\varphi) \in B_a$. Thus $b \in B_a(s\varphi)$, and $B_a(s\varphi) = B_{as}$. Now clearly the number of pairs (a, b) such that $a \in A$, $b \in B$ and $a \leq b$ is expressible either as $\Sigma_{a \in A} |B_a| = |A| m$, or as $\Sigma_{b \in B} |A_b| = |B| n$, Q.E.D.

We will say of a machine $\mathfrak{A} = \langle A, S, \sigma, \alpha \rangle$ that it is *trivial* if and only if A is compatible. Clearly $\mathfrak{A}$ is trivial if and only if it has a one state minimum state machine.

COROLLARY 3.21. *If $\mathfrak{A} = \langle A, S, \sigma, \alpha \rangle$ is a nontrivial connected permutation machine and $\mathfrak{A} \leq_m \mathfrak{B} = \langle B, T, \tau, \beta \rangle$, then $|A|$ and $|B|$ are not relatively prime.*

Proof. Let the sets A_b and B_a and the numbers $n = |A_b|$ and $m = |B_a|$ be as in Corollary 3.20, so $|B| n = |A| m$. Since $A_b \subseteq A$ then $n \leq |A|$. If $|A|$ and $|B|$ are relatively prime then $|A|$ divides n. Thus $|A| = n$, so $A_b = A$. Since the sets A_b are compatible (Proposition 3.5) then $\mathfrak{A}$ is trivial, Q.E.D.

COROLLARY 3.22. *A connected permutation machine $\mathfrak{A}$ with a prime number of states is either trivial or self-minimum* (i.e. $\mathfrak{A} \leq_m \mathfrak{A}$).

THEOREM 3.23. *If $\mathfrak{A} = \langle A, S, \sigma, \alpha \rangle$ and $\mathfrak{B} = \langle B, T, \tau, \beta \rangle$ are permutation machines such that $\mathfrak{A}' \leq \mathfrak{B}$, if $\Sigma = \{A_b \mid b \in B\}$ is the projection of $\mathfrak{B}$ onto $\mathfrak{A}$ (where $A_b = \{a \in A \mid a \leq b\}$) then Σ is closed under S, and if $\mathfrak{B}' = \langle \Sigma, T', \tau', \beta' \rangle$ is the natural construct of $\mathfrak{A}$ with Σ, and $\varphi : B \to \Sigma$ the mapping which takes b to A_b for each $b \in B$, then φ is a homomorphism of $\mathfrak{B}$ onto $\mathfrak{B}'$, $\mathfrak{B}'$ is a permutation machine, and $\mathfrak{A} \leq \mathfrak{B}' \leq \mathfrak{B}$. Moreover, if φ is an isomorphism then φ^{-1} is a machine homomorphism.*

Proof. Let $b \in B$ and $f \in F$. Then by Proposition 3.5, $A_b(f\sigma) \subseteq A_{b(f\tau)}$. Let $g \in F$ be such that $g\tau = (f\tau)^{-1}$. Then $A_b((fg)\sigma) = A_b(f\sigma)(g\sigma) \subseteq A_{b(f\tau)}(g\sigma) \subseteq A_{b(f\tau)(g\tau)} = A_b$. But $(fg)\sigma \in S$ is a one-to-one mapping since $\langle A, S \rangle$ is a permutation group. Thus since A is finite it follows that $A_b((fg)\sigma) = A_{b(f\tau)}(g\sigma) = A_b$. But $f\sigma$ and $g\sigma$ are also one-to-one mappings, so $|A_b(f\sigma)| = |A_b| = |A_{b(f\tau)}|$. Thus $A_b(f\sigma) = A_{b(f\tau)}$. This proves that Σ is closed under S, and that for $x \in X$ and $b \in B$, $(b(x\tau))\varphi = A_{b(x\tau)} = A_b(x\sigma) = (b\varphi)(x\sigma)$, i.e. that φ is the homomorphism claimed. Now let ψ be the homomorphism of S induced by Σ. By Proposition 3.3, $S\psi = T'$, so by Proposition 2.2, $\langle \Sigma, T' \rangle$ is a permutation group, i.e. $\mathfrak{B}'$ is a permutation machine. Since $\mathfrak{B}'$ is a construct of $\mathfrak{A}$ then $\mathfrak{A} \leq \mathfrak{B}'$. In order to show that $\mathfrak{B}' \leq \mathfrak{B}$ and that φ^{-1} is a machine homomorphism if φ is an isomorphism, we will show $A_b \leq b$ for $b \in B$. Suppose $(A_b(f\tau^{-1}))\beta'$

is defined and equals y so there exists $a \in A_b(f\bar{\tau}') = A_{b(f\bar{\tau})}$ such that $a\alpha = y$. Thus since $a \leq b(f\bar{\tau})$ then $(b(f\bar{\tau}))\beta = y$, Q.E.D.

A permutation machine $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ will be called *simply transitive* if and only if $\langle A, S\rangle$ is a simply transitive permutation group.

COROLLARY 3.24. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ and $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ be permutation machines such that $\mathfrak{A}$ is simply transitive, $\mathfrak{B}$ is connected, and $\mathfrak{A} \leq \mathfrak{B}$. Then there is a machine $\mathfrak{B}' = \langle B', T', \tau', \beta'\rangle$ such that $\mathfrak{A} \leq \mathfrak{B}' \leq \mathfrak{B}$ and there are a machine homomorphism ψ of $\mathfrak{A}$ onto $\mathfrak{B}'$ and a homomorphism ξ of $\mathfrak{B}$ onto $\mathfrak{B}'$ such that if ξ is an isomorphism then ξ^{-1} is a machine homomorphism. Thus $|B'|$ divides both $|A|$ and $|B|$.*

Proof. Let Σ be the projection of $\mathfrak{B}$ onto $\mathfrak{A}$ and $\mathfrak{B}' = \langle B', T', \tau', \beta'\rangle$ be the natural construct of $\mathfrak{A}$ with Σ, so $\mathfrak{A} \leq \mathfrak{B}' \leq \mathfrak{B}$ by Theorem 3.23. The homomorphism ξ is given by Theorem 3.23. Since $\mathfrak{B}$ is connected then $\mathfrak{B}'$ is connected. Let $a_0 \in A$ and $b_0 \in B'$ be such that $a_0 \leq b_0$. Let φ be the homomorphism of S induced by Σ. By Proposition 3.3 then $\sigma\varphi = \tau'$ and $S\varphi = T'$. For each $s \in S$ define $(a_0 s)\psi = b_0(s\varphi)$. Since for every $a \in A$ there is a unique $s \in S$ such that $a_0 s = a$ and since $\langle B', T'\rangle$ is transitive, it follows that ψ is a mapping of A onto B'. For every $x \in X$ and $a \in A$ if we let $s \in S$ be such that $a_0 s = a$, then $(a(x\sigma))\psi = (a_0 s(x\sigma))\psi = b_0((s(x\sigma))\varphi) = b_0(s\varphi)(x\sigma\varphi) = b_0(s\varphi)(x\tau') = ((a_0 s)\psi)(x\tau') = (a\psi)(x\tau')$, and ψ is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}'$. To show that ψ is a machine homomorphism it clearly suffices to show that $a \leq a\psi$ for all $a \in A$. But if $a = a_0 s$, then $a\psi = b_0(s\varphi)$, and since $a_0 \leq b_0$ by choice of b_0, then $a_0 s \leq b_0(s\varphi)$ by Corollary 3.18. That $|B'|$ divides $|A|$ and $|B|$ follows from Proposition 3.16, Q.E.D.

Remark. Elgot and Rutledge (1962) define a machine to be *input-free* if its input alphabet X consists of a single letter. The semigroup of such a machine is cyclic, hence commutative. If an input-free machine is strongly connected, it is a simply transitive permutation machine. Thus Corollary 3.24, though not a direct generalization of the "Interpolation Theorem" of Elgot and Ruthledge (1962) for input-free machines, clearly generalizes an essential portion of it.

COROLLARY 3.25. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ be a simply transitive permutation machine and $\mathfrak{A} \leq_m \mathfrak{B} = \langle B, T, \tau, \beta\rangle$. Then there is a machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ and $|B|$ divides $|A|$.*

Proof. By Corollary 3.24 there exists a machine $\mathfrak{B}'$ such that $\mathfrak{A} \leq \mathfrak{B}' \leq \mathfrak{B}$ and there is a machine homomorphism ψ of $\mathfrak{A}$ onto $\mathfrak{B}'$ and a homomorphism ξ of $\mathfrak{B}$ onto $\mathfrak{B}'$. Since $\mathfrak{A} \leq_m \mathfrak{B}$ then ξ must be an

isomorphism. Thus $\varphi = \psi\xi^{-1}$ is a machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$, by Corollary 3.24. That $|B|$ divides $|A|$ follows from Proposition 3.16, Q.E.D.

Remark. The divisibility property of Corollary 3.25. does not, in general, extend to connected permutation machines which are not simply transitive, as is evidenced by the machines in Fig. 3.

COROLLARY 3.26. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ be a strongly connected commutative machine and $\mathfrak{A} \leq_m \mathfrak{B} = \langle B, T, \tau, \beta\rangle$. Then there is a machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{B}$ and $|B|$ divides $|A|$.*

Proof. By Proposition 2.6, $\langle A, S\rangle$ is simply transitive, so the results follow from Corollary 3.25, Q.E.D.

Remark. Corollary 3.25 and Corollary 3.26 are related to the Corollary of Elgot and Rutledge (1962) on input-free machines. The uniqueness of the minimum state machine (proved there for input-free machines), however, does not hold even in the strongly connected commutative case for non-input-free machines. (See Fig. 4.)

THEOREM 3.27. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ and $\mathfrak{B} = \langle B, T, \tau, \beta\rangle$ be permutation machines such that $\mathfrak{A} \leq \mathfrak{B}$. Then there exist permutation machines $\mathfrak{A}' = \langle A', S', \sigma', \alpha'\rangle$ and $\mathfrak{B}' = \langle B', T', \tau', \beta'\rangle$ such that (1) $\mathfrak{A} \leq \mathfrak{A}' \leq \mathfrak{B}' \leq \mathfrak{B}$; (2) there is a machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{A}'$ and a homomorphism of $\mathfrak{B}$ onto $\mathfrak{B}'$; and (3) $S' \cong T'$.*

Proof. Let Σ be the projection of $\mathfrak{B}$ onto $\mathfrak{A}$, so Σ is closed by Theorem 3.23. Let $\mathfrak{B}'$ be the natural construct of $\mathfrak{A}$ with Σ, so again by Theorem 3.23 there is a homomorphism of $\mathfrak{B}$ onto $\mathfrak{B}'$, $\mathfrak{B}'$ is a permutation machine and $\mathfrak{A} \leq \mathfrak{B}' \leq \mathfrak{B}$. Now let Π be the coarsest partition of A refining Σ. By Theorem 2.18, Π is closed under S. Thus Π is a C-class

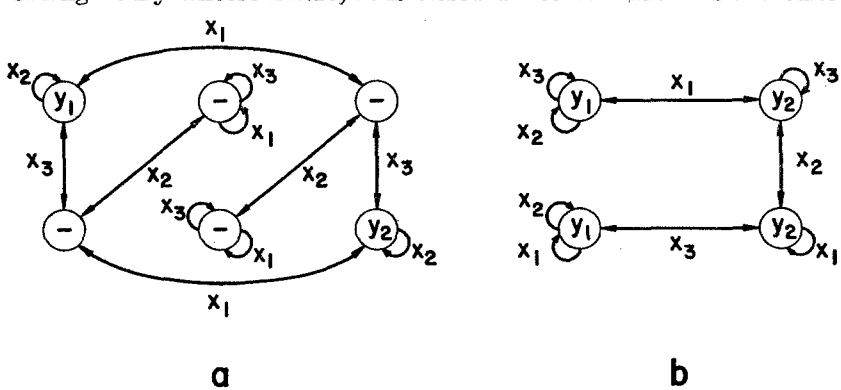

FIG. 3. A connected permutation machine (a) with a minimum state machine (b)

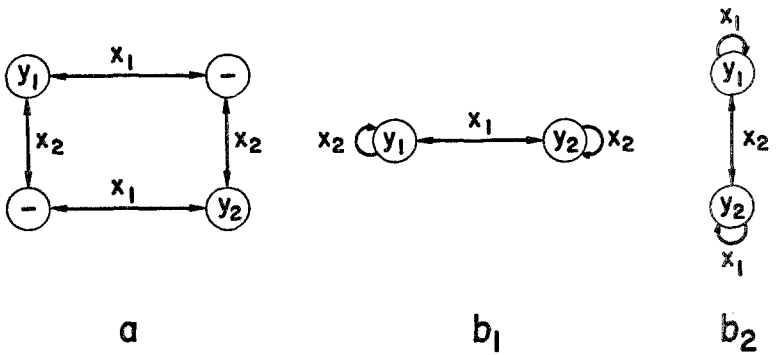

FIG. 4. A commutative connected permutation machine (a) with non-isomorphic *minimum state machines* (b_1) and (b_2).

for $\mathfrak{A}$. Let $\mathfrak{A}' = \langle \Pi, S', \sigma', \alpha' \rangle$ be the natural construct of $\mathfrak{A}$ with Π. Let φ and ψ be the homomorphisms of S induced by Σ and Π respectively. By Proposition 3.3 then $S' = S\psi$ and $T' = S\varphi$. By Theorem 2.18, $S\varphi \cong S\psi$ so $S' \cong T'$. Clearly $\mathfrak{A} \leq \mathfrak{A}'$. For every $C \in \Pi$ there exists $D \in \Sigma$ with $C \subseteq D$. We will now show that $C \subseteq D$ implies $C \leq D$ and conclude that $\mathfrak{A}' \leq \mathfrak{B}'$. Suppose $f \in F^1$ and $(C(f\bar{\sigma}'))\alpha'$ is defined. Then there exists $a \in C(f\bar{\sigma}')$ such that $a\alpha = (C(f\bar{\sigma}'))\alpha'$. By Proposition 3.3, $\bar{\sigma}' = \bar{\sigma}\psi$ and $\bar{\tau}' = \bar{\sigma}\varphi$. Thus $C(f\bar{\sigma}') = C(f\bar{\sigma}\psi) = C(f\bar{\sigma})$ and $D(f\bar{\tau}') = D(f\bar{\sigma}\varphi) = D(f\bar{\sigma})$. Since $C \subseteq D$ then $C(f\bar{\sigma}) \subseteq D(f\bar{\sigma})$. Thus $a \in C(f\bar{\sigma}') \subseteq D(f\bar{\tau}')$, so $(D(f\bar{\tau}'))\beta' = a\alpha = (C(f\bar{\sigma}'))\alpha'$. This concludes the proof that $C \leq D$, and hence that $\mathfrak{A}' \leq \mathfrak{B}'$. That there is a machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{A}'$ follows from Proposition 3.7, Q.E.D.

COROLLARY 3.28. *Let $\mathfrak{A} = \langle A, S, \sigma, \alpha \rangle$ be a permutation machine and $\mathfrak{B} = \langle B, T, \tau, \beta \rangle$ a minimum state machine for $\mathfrak{A}$. Then there exists a machine $\mathfrak{A}' = \langle A', S', \sigma', \alpha' \rangle$ such that $\mathfrak{A} \leq \mathfrak{A}' \leq \mathfrak{B}$, $S' \cong T$, and there is a machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{A}'$.*

Proof. By Corollary 3.18, $\mathfrak{B}$ is a permutation machine, so we may choose $\mathfrak{A}'$ and $\mathfrak{B}'$ as in Theorem 3.27. Then the homomorphism of $\mathfrak{B}$ onto $\mathfrak{B}'$ given by the theorem must be an isomorphism, since otherwise $\mathfrak{B}$ would not be a minimum state machine for $\mathfrak{A}$. Thus $S' \cong T' \cong T$ by Proposition 3.2 and Theorem 3.27. The latter also gives the machine homomorphism of $\mathfrak{A}$ onto $\mathfrak{A}'$, Q.E.D.

COROLLARY 3.29. *If $\mathfrak{A} = \langle A, S, \sigma, \alpha \rangle$ is a connected permutation machine whose minimum state machines have more than $|A|/2$ states, and if $\mathfrak{A} \leq_m \mathfrak{B} = \langle B, T, \tau, \beta \rangle$, then $S \cong T$.*

Proof. Let $\mathfrak{A}'$ be the machine given by Corollary 3.28, so $\mathfrak{A} \leq \mathfrak{A}' \leq \mathfrak{B}$,

$S' \cong T$ and there is a homomorphism φ of $\mathfrak{A}$ onto $\mathfrak{A}'$. By Proposition 3.16, since $\mathfrak{A}$ is connected, then $|A'|$ divides $|A|$. If $|A'| < |A|$, then $|A'| \leq |A|/2$, which is impossible since $\mathfrak{A} \leq \mathfrak{A}'$ implies $|A'| > |A|/2$. Thus $|A'| = |A|$, so φ is an isomorphism. By Proposition 3.2 then $S \cong S'$ so $S \cong T$, Q.E.D.

Remark. In the example of Fig. 4, it will be noticed that although the minimum state machines are not isomorphic, at least their semigroups are isomorphic. In order not to lead the reader into the mistaken conjecture that this is a general property of permutation machines, we close with the following:

THEOREM 3.30. *Let B be a finite set and let $\langle B, S_1\rangle, \cdots, \langle B, S_n\rangle$ be permutation groups. Then there exist sets X and Y and a permutation machine $\mathfrak{A} = \langle A, S, \sigma, \alpha\rangle$ with input alphabet X, output alphabet Y, and minimum state machines $\mathfrak{A}_1, \cdots, \mathfrak{A}_n$ such that for each $j(1 \leq j \leq n)$ the permutation group of $\mathfrak{A}_j$ is isomorphic to $\langle B, S_j\rangle$.*

Proof. Let $A = B^n$, i.e. the set of all n-tuples of elements of B, and let $Y = B$. Let $(b_1, \cdots, b_n)\alpha$ be defined and equal to b if and only

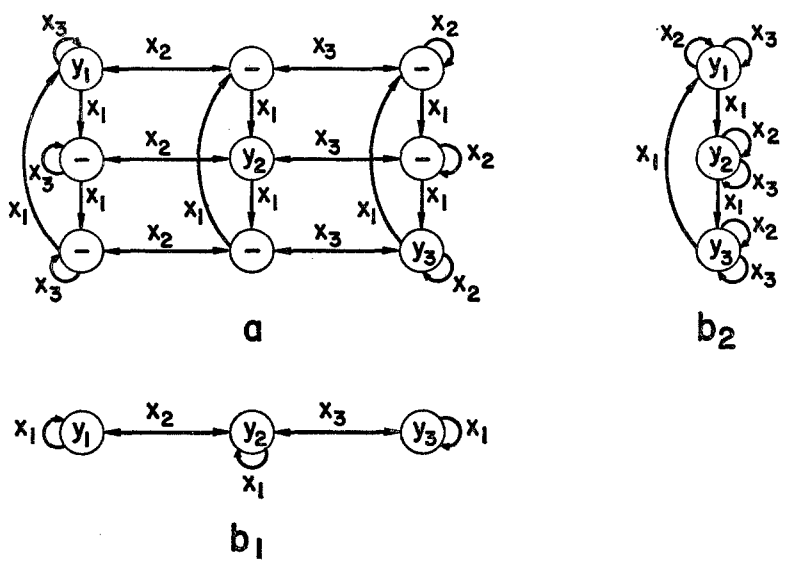

FIG. 5. A permutation machine (a) with minimum state machines (b_1) and (b_2) having non-isomorphic groups.

if $b_j = b$ for $1 \leq j \leq n$. Let R_j be a set of generators of S_j for $1 \leq j \leq n$. Let f_j be a one-to-one mapping of a set X_j onto R_j for $1 \leq j \leq n$, where the X_j are chosen to be mutually disjoint, and let $X = \bigcup_{j=1}^{n} X_j$. Define $\sigma' : X \to \mathfrak{I}_A$ as follows: if $x \in X_j$ then let $(b_1, \cdots, b_n)(x\sigma') = (b_1', \cdots, b_n')$, where $b_i' = b_i$ if $i \neq j$ and $b_j' = b_j(xf_j)$. Let σ be the unique extension of σ' to a homomorphism of F and $S = F\sigma$. It is readily seen that for each $j(1 \leq j \leq n)$, $\Sigma_j = \{\{(b_1, \cdots, b_n) \in A \mid b_j = b\} \mid b \in B\}$ is a minimum C-class for $\mathfrak{A}$, and if $\mathfrak{A}_j$ is the natural construct of $\mathfrak{A}$ with Σ_j, then $\langle B, S_j \rangle$ is isomorphic to the permutation group of $\mathfrak{A}_j$, Q.E.D.

An example of the construction of Theorem 3.30 for $n = 2$ is given in Fig. 5.

ACKNOWLEDGEMENT

The author would like to express his appreciation for the helpful suggestions and comments of J. Mezei.

RECEIVED: November 15, 1966

REFERENCES

BEATTY, J. C. AND MILLER, R. E. (1963), An approach to state minimization for incompletely specified sequential machines. IBM Research Report. **RC 1055**, Sept., 1963.

BIRKHOFF, G. (1948), "Lattice Theory." American Mathematical Society, Providence, Rhode Island.

CLIFFORD, A. H. AND PRESTON, G. B. (1961), "The Algebraic Theory of Semigroups," Vol. 1, American Mathematical Society, Providence, Rhode Island.

ELGOT, C. C. AND RUTLEDGE, J. D. (1962), Machine properties preserved under state minimization. *AIEE Proc. 3rd Ann. Symp. Switching Circuit Theory Logical Design*, Sept. 1962, pp. 61–70. Also IBM Research Report. **RC 717**, June 1962.

GINSBURG, S. (1960), Connective properties preserved in minimal-state machines. *J. Assoc. Comp. Mach.*, Oct. 1960, pp. 311–325.

GREEN, J. A. (1951), On the structure of semigroups. *Ann. Math.* **54**, pp. 163–172.

HALL, M. (1959), "The Theory of Groups," Macmillan, New York.

MOORE, E. F. (1956), Gedanken-experiments on sequential machines. Automata Studies, Study 34, pp. 129–153, Princeton University Press, Princeton, New Jersey.

NARASIMHAN, R. (1961), Miminizing incompletely specified sequential switching functions. *IRE Trans. Electron. Computers* **EC-10**, 531–532.

PAULL, M. C. AND UNGER, S. H. (1959), Miminizing the number of states in in-

completely specified sequential switching functions. *IRE Trans. Electron. Computers* **EC-8**, 356–367.

SCHÜTZENBERGER, M. P. (1962), On an abstract machine property preserved under the satisfaction relation. IBM Research Note. **NC-167**, Nov. 1962.

SUSCHKEWITSCH, A. (1928), Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit. *Math. Ann.* **99** (1928) pp. 30–50.

TULLY, E. J., JR. (1961), Representation of a semigroup by transformations acting transitively on a set. *Am. J. Math.* **83** (1961), pp. 533–541.