REMARKS ON ALGEBRAIC DECOMPOSITION OF AUTOMATA

by

A. R. Meyer and C. Thompson

Carnegie-Mellon University
Pittsburgh, Pennsylvania
August, 1968

This work was supported by the Advanced Research Projects Agency of the Office of the Secretary of Defense (F 44620-67-C-0058) and is monitored by the Air Force Office of Scientific Research.

REMARKS ON ALGEBRAIC DECOMPOSITION OF AUTOMATA

by

A. R. Meyer and C. Thompson

ABSTRACT

A version of the Krohn-Rhodes decomposition theorem for finite automata is proved in which capabilities as well as semigroups are preserved. Another elementary proof of the usual Krohn-Rhodes theorem is also presented.

1. INTRODUCTION

The constructive half of Krohn and Rhodes' decomposition theorem for finite automata states that any finite automaton can be simulated by a cascade of reset and permutation automata. Moreover, the groups of the permutation automata in the cascade need only be simple groups which divide the semigroup of the original automaton. Assorted proofs of this theorem appear in [1, 2, 3, 4, 5, 7] and we include our own elementary proof in Section 5.

Our object in this paper is to supply the few extra steps necessary to prove a corrected version of a slightly stronger decomposition theorem stated by Hartmanis and Stearns [4]. This theorem appears in Section 3. In Section 4 we exhibit a counter-example to the theorem as originally stated by Hartmanis and Stearns, and briefly consider cascades of "half-reset" automata.

2. PRELIMINARIES

Our notation follows Ginzburg [3]. In particular, function arguments appear on the left (so that xf is the value of function f at argument x). Composition of functions is designated by concatenation, with the leftmost function understood to apply first (so that xfg = (xf)g). For a function f and set S, the restriction of f to S is $f\restriction S$. The cardinality of S is $|S|$. We use "$\subset$" to mean improper inclusion. For a set S and family $\mathfrak{F}$ of functions with domains including S, $S\mathfrak{F}$ is $\{sf \mid s \in S, f \in \mathfrak{F}\}$. As usual, "$s\mathfrak{F}$" means $\{s\}\mathfrak{F}$, and "Sf" means $S\{f\}$.

A semiautomaton (or state machine) A consists of a finite set Q^A (of states), a finite set Σ^A (of inputs), and a set of (transition) functions from Q^A into Q^A indexed by Σ^A. The function from Q^A into Q^A indexed by $\sigma \in \Sigma^A$ is σ^A. When the context is unambiguous, we shall frequently omit superscripts and identify σ with σ^A.

Let A and B be semiautomata. B is a subautomaton of A iff $\Sigma^B \subset \Sigma^A$, $Q^B \subset Q^A$ and $\sigma^B = \sigma^A\restriction Q^B$ for each $\sigma \in \Sigma^B$. A subautomaton B of A is nontrivial if $\Sigma^B = \Sigma^A$ and $|Q^A| > |Q^B| > 1$. B is an image of A if there are functions $\eta\colon Q^A \to Q^B$ and $\xi\colon \Sigma^B \to \Sigma^A$ such that η is onto and $\eta\sigma^B = (\sigma\xi)^A\eta$ for each $\sigma \in \Sigma^B$. The function η is then called a homomorphism from A (on)to B. A covers B, in symbols "$A \geq B$", iff B is an image of a subautomaton of A. Covering is transitive. A and B are equivalent iff $A \geq B$ and $B \geq A$.

A partition π of Q^A is an admissible partition of A iff for every $X \in \pi$ and $\sigma \in \Sigma^A$, there is a $Y \in \pi$ such that $X\sigma \subset Y$. The quotient semiautomaton A/π (defined for admissible π) has state set π, inputs Σ^A, and transitions given by: $X\sigma^{A/\pi} = Y$ where Y is the (necessarily unique) element of π such that $X\sigma \subset Y$. The semiautomaton A/π is an image of A.

Given a (connecting) function ω: $Q^A \times \Sigma^A \to \Sigma^B$, the cascade product $(A \circ B)_\omega$ is the semiautomaton with state set $Q^A \times Q^B$, inputs Σ^A, and transitions given by: $(p,q)\sigma = (p\sigma, q((p,\sigma)\omega))$ for $(p,q) \in Q^A \times Q^B$ and $\sigma \in \Sigma^A$. We usually suppress mention of the connecting function and simply write "$A \circ B$". Cascade product is associative in the sense that given $(A \circ B) \circ C$, there is an equivalent semiautomaton $A \circ (B \circ C)$. A cascade product of a sequence of three or more semiautomata is any parenthesization of the sequence into a cascade product of pairs of semiautomata.

If $B \geq D$, then for every connecting function ω there is a connecting function ω' such that $(A \circ B)_{\omega'} \geq (A \circ D)_\omega$. Similarly, if $A \geq C$, there is an A' equivalent to A such that $A' \circ B \geq C \circ B$.

A is a permutation semiautomaton iff every $\sigma \in \Sigma^A$ is a permutation of Q^A. A is a reset iff every $\sigma \in \Sigma^A$ is a constant or identity function on Q^A; constant functions are also called resets. A is an identity semiautomaton iff every $\sigma \in \Sigma^A$ is the identity on Q^A.

We assume the reader is familiar with the elementary facts about groups and semigroups. Let S and T be semigroups. S is a subgroup of T iff S is a subsemigroup of T, and S is (abstractly isomorphic to) a group. S divides T, in symbols "$S \mid T$", iff S is a homomorphic image of a subsemigroup of T. Division is transitive. "$T \to S$" means S is a homomorphic image of T, and "$S = T$" means S and T are isomorphic. Most of the semigroups in this paper are transformation semigroups, but we use "$\to$" and "$=$" to mean homomorphism and isomorphism of abstract semigroups (though it will usually be clear when an abstract homomorphism is actually a transformation homomorphism). When T is a group, "$S \triangleleft T$" means S is a normal subgroup.

The semigroup of a semiautomaton A is the transformation semigroup generated by $\{\sigma^A | \sigma \in \Sigma^A\}$ under composition. The monoid G^A is the semigroup of A with Λ^A, the identity on Q^A, added if it is not already in the semigroup. If $A \geq B$, then $G^B | G^A$. The converse is not true. A is an identity semiautomaton iff $|G^A| = 1$. A is a permutation semiautomaton iff G^A is a group. Corresponding statements with the semigroup of A in place of G^A are not true.

3. THE DECOMPOSITION THEOREM

The following version of Krohn and Rhodes decomposition theorem is proved in [2, 3, 4, 7].

Theorem 1. For any semiautomaton A, there is a cascade product of semiautomata $A_1, A_2, \ldots, A_n$ which covers A such that for all i ($1 \leq i \leq n$) either

(1) G^{A_i} is a simple group*, and $G^{A_i} | G^A$,

or (2) A_i is a two-state reset.

Moreover, if G^A is a group, those A_i which are resets will actually be identity semiautomata.

The components A_i of the cascade covering A are no more complicated than A, insofar as semigroups reflect the complexity of semiautomata. On the other hand, Theorem 1 does not prohibit the A_i from being larger than A, and in fact the usual decomposition techniques applied to a five state machine whose semigroup consists of resets and the alternating group of degree five yields an A_i with sixty states. The following theorem eliminates this flaw.

*We remind the reader that A_i is a permutation semiautomaton iff G^{A_i} is a group.

Definition. Let A be a semiautomaton. The completion of A is the semiautomaton $\bar{A}$ such that $Q^{\bar{A}} = Q^A$, $\Sigma^{\bar{A}} = G^A$, and for $g \in G^A$, $g^{\bar{A}} \overset{df.}{=} g$.

Theorem 2. Theorem 1 is true when (1) is replaced by

(1') G^{A_i} is a simple group , and $\bar{A} \geq A_i$.

Clearly $G^{\bar{A}} = G^A$, and since $A \geq B$ implies $G^B | G^A$, we observe that Theorem 2 implies Theorem 1.

We take Theorem 1 as our starting point, and prove Theorem 2 from the following lemmas.

Lemma 1. Let C be a semiautomaton such that G^C is a group and $N \triangleleft G^C$. Let $\pi = \{qN | q \in Q^C\}$. π is an admissible partition and $G^C/N \rightarrow G^{C/\pi}$.

Proof: The elements of π are the orbits of Q^C under the group of transformations N, and so π is clearly a partition of Q^C. Moreover, π is admissible: $Ng = gN$ for all $g \in G^C$ since N is normal, and so for all $qN \in \pi$ it follows that $(qN)g = q(Ng) = q(gN) = (qg)N \in \pi$. Observe that the elements of $G^{C/\pi}$ are simply the elements of G^C acting on π. Hence, $G^C \rightarrow G^{C/\pi}$ and N is trivially included in the kernel of the homomorphism; therefore, $G^C/N \rightarrow G^{C/\pi}$. Q.E.D.

Lemma 2. Let A be a semiautomaton such that H is a simple group and $H | G^A$. there is a semiautomaton B such that $\bar{A} \geq B$ and $G^B = H$.

Proof: It is easy to show (cf. Ginzburg [3], section 1.16) that if a group divides a semigroup, then the group is actually a homomorphic image of a subgroup of the semigroup. Let K be a subgroup of G^A of minimum size such that $K \rightarrow H$, and let $N \triangleleft K$ be the kernel of the homomorphism. Let

C be the subautomaton of $\bar{A}$ such that $Q^C = Q^A K$ and $\Sigma^C = K$. Then $G^C = K$ (as the reader may verify)* and by Lemma 1, $\pi = \{qN | q \in Q^C\}$ is an admissible partition of C. Finally, let $B = C/\pi$.

Clearly, $\bar{A} \geq B$.

Lemma 1 also implies that $G^C/N \rightarrow G^B$. But $G^C/N = K/N = H$, and H is simple, so that if $|G^B| \neq 1$, it must be that $G^B = H$ as required.

On the other hand, suppose $|G^B| = 1$. Then every element of $K = G^C$ acts as an identity on π, viz., $(qN)k = qN$ for every $k \in K$ and $qN \in \pi$. For $q \in Q^C$, let $K_q = \{k \in K | qk=q\}$. Since $q \in qN = qNk$ for $q \in Q^C$ it follows that K_q intersects every coset of N in K, and so the restriction to K_q of the canonical homomorphism from K onto K/N is also onto. Therefore, $K_q \rightarrow K/N = H$ (obviously K_q is a group), and since K is of minimum size, $K = K_q$ for all $q \in Q^C$. But this implies $K = \{\Lambda^C\}$, which is absurd, since H is a non-trivial image of K. Q.E.D.

Lemma 3. If A and B are semiautomata such that $G^A = G^B$, then there is cascade product of copies of $\bar{B}$ and an identity semiautomaton which covers A.

Proof: For convenience assume $Q^B = \{1,2,\ldots,n\}$. The cascade covering A will consist of an identity machine with state set Q^A and n copies of $\bar{B}$, all acting in parallel. For $q_0 \in Q^A$, $q_i \in Q^B$, $1 \leq i \leq n$, and $g \in G^B$, the transitions in the cascade are defined by $(q_0,q_1,\ldots,q_n)g \stackrel{df.}{=} (q_0,q_1g,\ldots,q_ng)$.

The states $q_i \in Q^B$ uniquely determine a function $f: Q^B \rightarrow Q^B$ by the condition $f(i) = q_i$, $1 \leq i \leq n$. If it happens that $f \in G^B$, the state $q_0f \in Q^A$ is also uniquely determined by the isomorphism between G^B and G^A.

The states of the cascade which determine functions $f \in G^B$ obviously form a subautomaton of the cascade, and the mapping of $\langle q_0,q_1,\ldots,q_n\rangle$ to

*This is not quite immediate, since one must argue that the identity of K restricted to Q^C is actually Λ^C.

$q_0 f$ defines a homomorphism from this subautomaton onto $\bar{A}$ (and hence onto A), as is easily verified. Q.E.D.

Lemma 3 emphasizes the difficulty in interpreting the Krohn-Rhodes theorem as a "prime" decomposition theorem <u>for machines</u> (as opposed to semigroups). We might tentatively define A to be prime if (1) G^A is simple, and (2) $\bar{A} \geq B$ implies either $\bar{B} \geq A$ or $G^B \neq G^A$. There will then be prime machines for the same simple group which are incomparable under covering. Lemma 3 then leads to the unsatisfactory situation that one prime divides (is covered by) a power (cascade product of copies) of another prime.

The proof of Theorem 2 is now straightforward. Each A_i such that G^{A_i} is a simple group can be covered according to Lemma 3 by a cascade of copies of $\bar{B}$ and an identity semiautomaton, for any B such that $G^B = G^{A_i}$. Since $G^{A_i} | G^A$, Lemma 2 implies that such an automaton B can be found for which $\bar{A} \geq B$ (and hence $\bar{A} \geq \bar{B}$). The identity semiautomata which are introduced can trivially be replaced by cascades of two-state identity semiautomata, and the proof is complete.

Hartmanis and Stearns' notion "A has the capability of B" is equivalent to "$\bar{A} \geq B$". Theorem 2 above is thus a restatement of Theorem 7.10 of Hartmanis and Stearns [4], except that their Theorem 7.10 makes the additional assertion that $\bar{A} \geq A_i$ even when A_i is a reset. This is false, as we show in the next section.

4. HALF-RESETS

Let R_0 be the semiautomaton whose state set and input set equals $\{0,1\}$, and whose transitions are given by ordinary multiplication. Any semiautomaton covered by R_0 will be called a half-reset. Except for permutation semiautomata, every semiautomaton has the capability of R_0.

Definition. Let A be a semiautomaton, $p,q \in Q^A$. Then q is accessible from p iff $q = pg$ for some $g \in G^A$. A is partially ordered (p.o.) iff accessibility is a partial order on Q^A.

R_0 is trivially p.o., and it is easy to show that if A is p.o. and $A \geq B$, then B is p.o. Likewise, if A and B are p.o., so is $A \circ B$. Conversely, if A is p.o. (and not already a half-reset), then A has a nontrivial subautomaton which is a half-reset. We let the reader convince himself that A can then be covered by a p.o. semiautomaton with one fewer state followed by a half-reset (cf., Method I of Section 5). In short, we have

Theorem 4. A semiautomaton is covered by a cascade of half-resets if and only if it is partially ordered.

The regular events associated with p.o. semiautomata are obviously finite unions of events of the form "$F_1^*\sigma_1 F_2^*\sigma_2 \ldots F_n^*$" such that F_i is a finite set of input symbols and $\sigma_i \notin F_i$ $(1 \leq i \leq n)$. These events form a Boolean algebra, and can also be characterized by an inductive definition resembling that of the star-free events [6]. One can also define partially ordered semigroups in the obvious way, and conclude that A is p.o. iff G^A is p.o.

Consider a semiautomaton A with state set $\{1,2,3\}$ and inputs x and y such that $1x=2$, $2y=1$ and the remaining transitions lead to 3. No non-trivial groups divide G^A, so in the decomposition of A satisfying Theorem 2, only two-state resets appear. By Theorem 4, not all of these two-state resets can be half-resets (because states 1 and 2 are mutually accessible, viz., A is not p.o.). But the only two-state resets covered by $\bar{A}$ are half-resets (as can be verified by exhaustion), and so A cannot have the capability of all the components in its decomposition.

5. PROOF OF THEOREM 1

There are at least three elementary proofs of Theorem 1 in the literature: Ginzburg's [3] corrected version of Zeiger's proof using set systems or covers, Arbib's [2] version of Krohn-Rhodes' proof, and the elegant proof of Zeiger [7]. Nevertheless, none of these proofs are very simple,* and so we feel another proof may still be of interest. Readers familiar with the other proofs will note that our method I is essentially dual to that of Zeiger [7], and our Method III is almost the same as that of Arbib [2].

The following lemma appears in [2, 3, 4] and we shall not repeat the proof.

---

*The proof of Zeiger [7] is given in only two and a half pages, and separates non-permutation semiautomata into only two cases. Unfortunately, Zeiger's remark that his method applies to permutation-reset semiautomata is false, as can be seen by applying it to any permutation-reset semiautomaton. Moreover, a semiautomaton with state set $\{1,2,3\}$, reset inputs to each state, and an additional input leaving states 1 and 2 fixed and sending state 2 to state 3 is a counter-example to Zeiger's assertion that his second method reduces the number of non-permutation, non-reset elements. This counter-example invalidates the proof that his method terminates. When these errors are corrected, Zeiger's proof turns out to be no simpler than ours.

Lemma 4. Let A be a permutation semiautomaton. A can be covered by a cascade of two-state identity semiautomata and permutation semiautomata whose monoids are the factor groups in a composition series for G^A (and hence are simple groups dividing G^A).

We refer to permutation semiautomata and two state resets as basic. Theorem 1 follows immediately from Lemma 4 and

Theorem 5. For any semiautomaton A, there is a cascade product of basic semiautomata $A_1, A_2, \ldots, A_n$ which covers A such that for all i ($1 \leq i \leq n$), if G^{A_i} is a group, then $G^{A_i} | G^A$.

A natural way to prove Theorem 5 is to show that any semiautomaton can be covered by a product of two "smaller" semiautomata, and then use induction. (A disadvantage of the proof using set systems [3,4] is that it does not conform to this description.) The proper interpretation of "smaller" is necessarily a little devious.

Definition. For any transformation monoid S, N(S) is the submonoid generated by the nonconstant* (i.e., non-reset) elements of S. For any semiautomaton A, the measure of A is the triple of positive integers $\mu(A) \stackrel{df.}{=} (|N(G^A)|, |Q^A|, |G^A|)$.

Measures will be well-ordered lexicographically in the usual manner:

Definition. If $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ are triples of integers, then $x > y$ iff $x_1 > y_1$, or, $x_1 = y_1$ and $x_2 > y_2$, or, $x_1 = y_1$ and $x_2 = y_2$ and $x_3 > y_3$.

---

* By convention, N(S) = the identity when S acts on a singleton.

Lemma 5. For any semiautomaton A, which is not basic, there are semiautomata B and C such that

(1) $B \circ C \geq A$,

(2) $N(G^B) | G^A$, and either $\mu(B) < \mu(A)$ or B is basic,

(3) $N(G^C) | G^A$ and $\mu(C) < \mu(A)$.

Proof of Theorem 5: Let A be a semiautomaton. If A is basic (and in particular if $\mu(A) = (1,1,1)$ is minimum), then Theorem 5 is true trivially. Proceeding by (transfinite) induction, suppose Theorem 5 is true for all semiautomata with measures smaller than $\mu(A)$. Theorem 5 is then true by hypothesis for the semiautomata B and C produced by Lemma 5. Let B_i, $1 \leq i \leq n$, be the basic semiautomata in the cascade covering of B, and likewise for C_i, $1 \leq i \leq m$. Since $B \circ C \geq A$, a cascade of the B_i (or semiautomata equivalent to the B_i) followed by the C_i covers A. Suppose G^{B_i} is a group; then $G^{B_i} | G^B$. But if a group G divides a transformation monoid S, then it must be that $G | N(S)$. Hence, $G^{B_i} | N(G^B)$, by Lemma 5 $N(G^B) | G^A$, and by transitivity $G^{B_i} | G^A$. The same reasoning applies to the C_i, and it follows that Theorem 5 is true for A. Q.E.D.

Proof of Lemma 5: We describe three decomposition methods, one of which will yield appropriate B and C for any semiautomaton A which is not basic.

Definition. For any semiautomaton A, let N(A) be the subautomaton of A obtained by eliminating all reset inputs from Σ^A.

Method I. N(A) has a non-trivial subautomaton.

Let Q^C equal the states of the non-trivial subautomaton of N(A), and let $Q^B = (Q^A - Q^C) \cup \{d\}$ for $d \notin Q^A$. Transitions in $B \circ C$ are given by:

$$(b,c)\sigma = \begin{cases} (b\sigma,c) & \text{if } b\neq d \text{ and } b\sigma \notin Q^C, \\ (d,b\sigma) & \text{if } b\neq d \text{ and } b\sigma \in Q^C, \\ (r,c) & \text{if } \sigma \text{ is a reset to } r \in Q^A - Q^C. \\ (b,c\sigma) & \text{otherwise} \end{cases}$$

Since Q^C is the state set of a subautomaton of $N(A)$, it is closed under non-reset inputs. Hence the fourth clause only applies when $b=d$ and $c\sigma \in Q^C$, so the transitions of $B \circ C$ are well defined.

When $b\neq d$ map (b,c) to b, and when $b=d$ map (b,c) to c. This mapping defines a homomorphism from $B \circ C$ onto A (as is immediately verified by checking the four types of transitions in $B \circ C$), so part (1) of the lemma is satisfied.

Note that the singletons in $Q^A - Q^C$ together with Q^C form an admissible partition π of A, and that A/π is isomorphic to B. We conclude that $G^A \to G^B$ and that $N(G^B) | G^A$. Moreover, $|Q^B| = |Q^A - Q^C| + 1 < |Q^A|$ since the subautomaton on Q^C is non-trivial. This guarantees that part (2) is satisfied.

The only non-identity, non-reset transitions in G^C arise from the fourth clause in the definition of transitions of $B \circ C$. It follows that $N(G^C) = \{g \restriction Q^C \mid g \in N(G^A)\}$. Hence $N(G^A) \to N(G^C)$, and since $|Q^C| < |Q^A|$, part (3) is satisfied.

Method II. G^A contains a non-identity permutation.

Let P be the subgroup of G^A generated by the permutations, and T the subsemigroup generated by $G^A - P$. Note that $T \neq \emptyset$ (otherwise G^A is a group and A is basic), and that T is trivially a (two-sided) ideal. Let $Q^B = P$, and $Q^C = Q^A$. Transitions in $B \circ C$ are given by:

$$(p,q)\sigma = \begin{cases} (p\sigma, q) & \text{if } \sigma \in P \\ (p, qp\sigma p^{-1}) & \text{if } \sigma \in T \end{cases}$$

Since G^A is the disjoint union of P and T, the transitions of B∘C are well defined. Mapping (p,q) to qp defines a homomorphism from B∘C onto A.

Clearly $G^B = P$, so $N(G^B) | G^A$ and B is basic. Likewise $G^C = T \cup \{\Lambda^C\}$, so $N(G^C) | G^A$ and $N(G^C)$ does not contain the non-identity permutation in $N(G^A)$. Therefore, $\mu(C) < \mu(A)$.

Method III. $G^A = V \cup T$ where V is a subsemigroup such that $|N(V)| < |N(G^A)|$, and T is a proper left ideal of $G^A - \{\Lambda\}$.

Let $Q^B = V$ and $Q^C = Q^A$. Transitions in B∘C are given by:

$$(v,q)\sigma = \begin{cases} (v\sigma, q) & \text{if } \sigma \in V\text{-}T, \\ (\Lambda, qv\sigma) & \text{if } \sigma \in T. \end{cases}$$

Note that $\Lambda \notin T$ (and hence $\Lambda \in V$) since T is proper, and so the transitions in B∘C are well defined. Mapping (v,q) to qv defines a homomorphism from B∘C onto A.

Clearly $G^C = T \cup \{\Lambda\}$, so $G^C | G^A$. Moreover, $Q^C = Q^A$ and $|G^C| < |G^A|$ since T is proper. Hence, $\mu(C) < \mu(A)$.

Note that $N(G^B)$ is a submonoid (generated by V-T) of V acting on itself by right multiplication, and so $N(G^B) | V$. Moreover, any $r \in V$ which is a reset (on Q^A) is certainly a reset when V acts on itself. Therefore, $N(G^B)$ is isomorphic to a submonoid of N(V), and we actually have $N(G^B) | N(V)$. In particualr, $|N(G^B)| \leq |N(V)|$. By hypothesis, $|N(V)| < |N(G^A)|$, so $\mu(B) < \mu(A)$.

Let A be a semiautomaton such that neither method I nor method II applies to A and A is not basic. We claim that method III applies to A, which completes the proof of Lemma 5.

To verify the claim, let $S = G^A - \{\Lambda\}$. S is a subsemigroup because G^A contains no non-identity permutations. There is a non-reset element $s \in S$ (otherwise A is a reset and method I applies). If $G^A s \cup \{\text{resets}\} = S$, then N(A) has a non-trivial subautomaton on the states in the range of s, and method I applies. Therefore $G^A s \cup \{\text{resets}\} \neq S$, and in particular S has proper left ideals (e.g., $G^A s$).

Let T be a maximal left ideal of S, and let $V = G^A x \cup \{\Lambda\}$ for any $x \in S\text{-}T$. Then $(V - \{\Lambda\}) \cup T$ is a left ideal of S properly containing T, which implies $(V - \{\Lambda\}) \cup T = S$ and $V \cup T = G^A$. If x=s, we have observed that $V \cup \{\text{resets}\} \neq G^A$, and so $|N(V)| < |N(G^A)|$. Alternatively, if T contains every non-reset $s \in S$, then x is a reset, hence $G^A x$ contains only resets and $|N(V)| = 1 < |N(G^A)|$. Q.E.D.

There are usually many ways to decompose a semiautomaton into two semiautomata with smaller measures, and it is far from clear which choices ultimately yield the most satisfactory decomposition into basic semiautomata. It may even be desirable at times to cover a semiautomaton with semiautomata which have larger measures (but which presumably are "smaller" in some more general sense).

References

1. Arbib, M., Algebraic Theory of Machines, (1968), to appear.

2. Arbib, M., Theories of Abstract Automata, Prentice-Hall (1968), to appear.

3. Ginzburg, A., Algebraic Theory of Automata, ACM Monograph Series, to appear.

4. Hartmanis, J. and Stearns, R. E., Algebraic Structure Theory of Sequential Machines, Prentice-Hall, Englewood Cliffs, N. J. (1966).

5. Krohn, K. and Rhodes, J., "Algebraic Theory of Machines, I," Trans. Amer. Math. Soc., Vol. 116 (1965), 450-464.

6. Meyer, A. R., "A Note on Star-free Events," JACM (1968), to appear.

7. Zeiger, P., "Yet Another Proof of the Cascade Decomposition Theorem for Finite Automata", Mathematical Systems Theory, Vol. 1, No. 3 (1966), 225-288.

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) Carnegie-Mellon University Department of Computer Science Pittsburgh, Pennsylvania 15213	2a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED 2b. GROUP

3. REPORT TITLE

REMARKS ON ALGEBRAIC DECOMPOSITION OF AUTOMATA

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

Scientific Interim

5. AUTHOR(S) (First name, middle initial, last name)

A. R. Meyer and C. Thompson

6. REPORT DATE August 1968	7a. TOTAL NO. OF PAGES 16	7b. NO. OF REFS 7
8a. CONTRACT OR GRANT NO. F44620-67-C-0058 b. PROJECT NO. 9718 c. 6154501R d. 681304	9a. ORIGINATOR'S REPORT NUMBER(S)	
	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)	

10. DISTRIBUTION STATEMENT

1. This document has been approved for public release and sale; its distribution is unlimited.

11. SUPPLEMENTARY NOTES TECH, OTHER	12. SPONSORING MILITARY ACTIVITY Air Force Office of Scientific Research (SRMA) 1400 Wilson Boulevard Arlington, Virginia 22209

13. ABSTRACT

A version of the Krohn-Rhodes decomposition theorem for finite automata is proved in which capabilities as well as semigroups are preserved. Another elementary proof of the usual Krohn-Rhodes theorem is also presented.

DD FORM 1 NOV 65 1473

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT