JOURNAL OF COMPUTER AND SYSTEM SCIENCES 20, 32–49 (1980)

Languages of $\mathcal{R}$-Trivial Monoids*

J. A. BRZOZOWSKI

Department of Computer Science, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada

AND

FAITH E. FICH

Computer Science Division, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, California 94720

Received September 4, 1979

We consider the family of languages whose syntactic monoids are $\mathcal{R}$-trivial. Languages whose syntactic monoids are $\mathcal{J}$-trivial correspond to a congruence which tests the subwords of length n or less that appear in a given word, for some integer n. We show that in the $\mathcal{R}$-trivial case the required congruence also takes into account the order in which these subwords first appear, from left to right. Characterizations of the related finite automata and regular expressions are summarized. Dual results for $\mathcal{L}$-trivial monoids are also discussed.

1. INTRODUCTION

The well-known Green equivalence relations are fundamental in the theory of monoids [2, 6]. They are defined as follows. Let M be a monoid and $f, g \in M$; then

$$\begin{aligned} f\mathcal{J}g \quad & \text{iff} \quad MfM = MgM, \\ f\mathcal{L}g \quad & \text{iff} \quad Mf = Mg, \\ f\mathcal{R}g \quad & \text{iff} \quad fM = gM, \\ f\mathcal{H}g \quad & \text{iff} \quad f\mathcal{L}g \text{ and } f\mathcal{R}g. \end{aligned}$$

If ρ is an equivalence relation on M, we say that M is ρ-trivial iff $f\rho g$ implies $f = g$. In 1965 Schützenberger [8] showed that finite $\mathcal{H}$-trivial monoids correspond to star-free languages, i.e., languages that can be denoted by regular expressions using only Boolean operations and concatenation. In 1972 Simon [9, 10] characterized the languages corresponding to finite $\mathcal{J}$-trivial monoids. These languages play a key role in the dot–depth hierarchy [3, 9] of star-free languages. This hierarchy and $\mathcal{J}$-trivial and $\mathcal{H}$-trivial monoids are also treated in [4].

* This research was supported by the National Research Council of Canada under a postgraduate scholarship and under Grant A-1617.

0022-0000/80/010032-18$02.00/0

The languages corresponding to finite $\mathscr{R}$-trivial (and $\mathscr{L}$-trivial) monoids are studied here. Eilenberg showed [4] that $\mathscr{R}$-trivial monoids form a variety and characterized the corresponding variety of languages. Several new characterizations of these languages are given here.

2. Terminology and Notation

Let A be a finite nonempty alphabet and A^* the free monoid generated by A, with unit element 1 (the empty word). The length of $x \in A^*$ is denoted by $|x|$; note that $|1| = 0$. The product (concatenation) of two words x and y in A^* is denoted by xy. The "alphabet" of a word $x \in A^*$ is

$$\alpha(x) = \{a \in A \mid x = uav \text{ for some } u, v \in A^*\}.$$

The reverse x^ρ of a word x is defined by induction on $|x|$:

$$1^\rho = 1 \qquad \text{and} \qquad (xa)^\rho = ax^\rho.$$

Subsets of A^* are called languages. If $X, Y \subseteq A^*$ then $\bar{X} = A^* - X$, $X \cup Y$, and $X \cap Y$ denote the complement of X and the union and intersection of X and Y, respectively. The product of two languages is $XY = \{w \mid w = xy, x \in X, y \in Y\}$. Also $X^* = \bigcup_{n \geqslant 0} X^n$ (where $X^0 = \{1\}$) is the submonoid of A^* generated by X. The reverse of X is $X^\rho = \{x^\rho \mid x \in X\}$.

For any family $\mathscr{F}$ of languages $\mathscr{F}\mathbf{B}$ is the smallest family containing $\mathscr{F}$ and closed under complementation and finite unions. Similarly $\mathscr{F}\mathbf{M}$ is the smallest family containing $\mathscr{F} \cup \{\{1\}\}$ and closed under concatenation. Thus $\mathscr{F}\mathbf{B}$ and $\mathscr{F}\mathbf{M}$ are the Boolean algebra and monoid generated by $\mathscr{F}$, respectively.

The syntactic congruence $\equiv_X$ of $X \subseteq A^*$ is defined as follows. For all $x, y \in A^*$,

$$x \equiv_X y \text{ iff for all } u, v \in A^* \ (uxv \in X \text{ iff } uyv \in X).$$

The quotient monoid $M = A^*/{\equiv_X}$ is the syntactic monoid of X and the natural morphism φ: $A^* \to M$, mapping $x \in A^*$ onto the equivalence class of $\equiv_X$ containing x, is the syntactic morphism of X. For convenience we often denote $\varphi(x)$ by $\underset{\sim}{x}$.

If $\sim$ is any congruence on A^* we say that X is a $\sim$ language iff X is a union of congruence classes of $\sim$. Thus X is a $\sim$ language iff for all $x, y \in A^*$,

$$x \sim y \text{ implies } (x \in X \text{ iff } y \in X).$$

Since $\sim$ is a congruence, $x \sim y$ implies $uxv \sim uyv$ for all $u, v \in A^*$. Thus X is a $\sim$ language iff

$$x \sim y \text{ implies } x \equiv_X y, \text{ i.e., } \underset{\sim}{x} = \underset{\sim}{y}.$$

A finite semiautomaton is a triple $\mathbf{S} = \langle A, Q, \sigma \rangle$, where A is the input alphabet, Q is a finite set of states and σ: $Q \times A \to Q$ is the transition function. A finite automaton is a system $\mathbf{A} = \langle A, Q, q_0, F, \sigma\rangle$ where A, Q and σ are as above, $q_0 \in Q$ is the initial state, and $F \subseteq Q$ is the set of final states. In any finite semiautomaton define the relation $\to$ as follows. For $p, q \in Q$

$$p \to q \qquad \text{iff} \quad \sigma(p, x) = q$$

for some $x \in A^*$. $\mathbf{S}$ (or $\mathbf{A}$) is partially ordered iff the relation $\to$ on Q is a partial order. A semiautomaton is a chain reset iff $\to$ is a total order.

The direct product of two semiautomata $\mathbf{S} = \langle A, Q, \sigma\rangle$ and $\mathbf{T} = \langle A, P, \tau\rangle$ is the semiautomaton $\mathbf{S} \times \mathbf{T} = \langle A, Q \times P, \pi\rangle$, where

$$\pi((q, p), a) = (\sigma(q, a), \tau(p, a)).$$

The cascade product of $\mathbf{S} = \langle A, Q, \sigma\rangle$ and $\mathbf{T} = \langle B, P, \tau\rangle$ with connection $\omega: Q \times A \to B$ is the semiautomaton $\mathbf{S} \circ \mathbf{T} = \langle A, Q \times P, \pi\rangle$, where

$$\pi((q, p), a) = (\sigma(q, a), \tau(p, \omega(q, a)).$$

An initialized semiautomaton is a semiautomaton with an initial state, i.e., $\mathbf{S} = \langle A, Q, q_0, \sigma\rangle$. Let $\mathbf{S}$ and $\mathbf{T} = \langle B, P, p_0, \tau\rangle$ be two initialized semiautomata. $\mathbf{T}$ is a subsemiautomaton of $\mathbf{S}$ iff $B \subseteq A$, $P \subseteq Q$, $q_0 = p_0$, and τ is the restriction of σ to $P \times B$. A semiautomaton $\mathbf{S}$ is a homomorphic image of semiautomaton $\mathbf{T}$ iff $B = A$ and there exists a surjective mapping $\psi: P \to Q$ such that $\psi(p_0) = q_0$ and

$$\psi(\tau(p, a)) = \sigma(\psi(p), a).$$

$\mathbf{S}$ is covered by $\mathbf{T}$ iff $\mathbf{S}$ is a homomorphic image of a subsemiautomaton of $\mathbf{T}$.

The transformation monoid of a semiautomaton $\mathbf{S} = \langle A, Q, \sigma\rangle$ (or of a finite automaton $\langle A, Q, q_0, F, \sigma\rangle$) is the set of all transformations of Q onto itself of the form $(q_1, ..., q_n) \to (\sigma(q_1, x), ..., \sigma(q_n, x))$ for some $x \in A^*$. It is well known that if $\mathbf{A}$ is a reduced finite automaton recognizing the language $X \subseteq A^*$, then the transformation monoid of $\mathbf{A}$ is isomorphic to the syntactic monoid of X.

Let M be any monoid and $f \in M$. Then $P_f = \{g \in M \mid f \in MgM\}$ and $M_f = P_f^*$. Thus M_f is the submonoid of M generated by the elements g "with which f can be written" ($f \in MgM$).

3. Languages of $\mathcal{J}$-Trivial Monoids

Simon [9, 10] provides many characterizations for languages with $\mathcal{J}$-trivial syntactic monoids as is summarized in the following theorem. An additional property, M3, is taken from [1].

THEOREM 3.1. *Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $\mathbf{A} = \langle A, Q, q_0, F, \tau\rangle$ and $\mathbf{A}^\rho$ be the reduced finite automata accepting X and X^ρ, respectively. The following conditions are equivalent.*

M1. *M is $\mathscr{J}$-trivial.*

M2. *M is $\mathscr{R}$-trivial and $\mathscr{L}$-trivial.*

M3. *For all idempotents $e \in M$, $eM_e \cup M_e e = e$.*

M4. *There exists an $n > 0$ such that for all $f, g \in M$, $(fg)^n = (fg)^n f = g(fg)^n$.*

M5. *There exists an $n > 0$ such that for all $f, g \in M$, $f^n = f^{n+1}$ and $(fg)^n = (gf)^n$.*

X1. *X is a ${}_n\!\sim$ language for some $n \geqslant 0$.*

E1. $X \in \{A^*aA^* \mid a \in A\}$ **MB**.

A1. **A** *and* $\mathbf{A}^\rho$ *are both partially ordered.*

A2. **A** *is partially ordered and for all $q \in Q$, $x, y \in A^*$, $\tau(q, x) = \tau(q, xx) = \tau(q, xy)$ and $\tau(q, y) = \tau(q, yy) = \tau(q, yx)$ imply $\tau(q, x) = \tau(q, y)$.*

A3. **A** *can be covered by a direct product of chain resets.*

This paper provides analogous results for languages with $\mathscr{R}$-trivial syntactic monoids. We require the following concepts from [9].

The congruence ${}_n\!\sim$, mentioned above, is defined in terms of the subwords of length less than or equal to n that a given word contains. More precisely we have:

DEFINITION 3.2. Let $x, y \in A^*$ and $n \geqslant 0$. Then

(a) x is a *subword* of y, $x \leqslant y$, iff there exist $x_1, \ldots, x_n$, $u_0, \ldots, u_n \in A^*$ such that $x = x_1 \cdots x_n$ and $y = u_0 x_1 u_1 \cdots x_n u_n$,

(b) the *n-contents* of y, denoted by $\mu_n(y)$, is the set $\{x \mid x \leqslant y \text{ and } |x| \leqslant n\}$,

(c) $x \;{}_n\!\sim y$ iff $\mu_n(x) = \mu_n(y)$.

It is straightforward to show that ${}_n\!\sim$ is a congruence of finite index for any $n \geqslant 0$ [9]. Simon also proves the following three results which are needed for the next section.

PROPOSITION 3.3. *Let $x, y \in A^*$ and $n \geqslant 0$. Then*

(a) $x^n \;{}_n\!\sim x^{n+1}$,

(b) $(xy)^n \;{}_n\!\sim (xy)^n x$,

(c) $(xy)^n \;{}_n\!\sim y(xy)^n$.

PROPOSITION 3.4. *Let $x, y \in A^*$ and $n \geqslant 0$. Then $x \;{}_{n+1}\!\sim y$ implies $x \;{}_n\!\sim y$.*

LEMMA 3.5. *Let $u, v \in A^*$ and $n > 0$. Then $u \;{}_n\!\sim uv$ iff there exist $u_1, \ldots, u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) \supseteq \alpha(u_2) \supseteq \cdots \supseteq \alpha(u_n) \supseteq \alpha(v)$.*

One additional definition is required.

DEFINITION 3.6. Let $n \geqslant 0$ and $x \in A^*$. Then x is *n-full* iff $\mu_n(x) = \bigcup \{(\alpha(x))^i \mid i = 0,..., n\}$.

Clearly every word is both 0-full and 1-full. One verifies that, for $n \geqslant 1$, x is n-full iff there exist $x_1,..., x_n \in A^*$ such that $x = x_1 \cdots x_n$ and $\alpha(x_1) = \cdots = \alpha(x_n)$.

4. THE ${}_n{\sim}_{\mathscr{R}}$ CONGRUENCE

The congruence ${}_n{\sim}_{\mathscr{R}}$ is defined to be a refinement of ${}_n{\sim}$ in which the order of appearance (from the left) of the subwords in a word is also taken into account. More formally:

DEFINITION 4.1. Let $x, y \in A^*$ and $n \geqslant 0$. Then $x \;{}_n{\sim}_{\mathscr{R}}\; y$ iff

(a) for each prefix u of x there exists a prefix v of y such that $u \;{}_n{\sim}\; v$, and

(b) for each prefix v of y there exists a prefix u of x such that $u \;{}_n{\sim}\; v$.

Note that if $|x| < n$, $x \;{}_n{\sim}_{\mathscr{R}}\; y$ iff $x = y$.

The two equivalence relations ${}_n{\sim}$ and ${}_n{\sim}_{\mathscr{R}}$ are closely related and satisfy many similar properties.

PROPOSITION 4.2. *Let $x, y \in A^*$ and $n \geqslant 0$.*

(a) *If $x \;{}_n{\sim}_{\mathscr{R}}\; y$ then $x \;{}_n{\sim}\; y$.*

(b) *$x \;{}_n{\sim}\; xy$ iff $x \;{}_n{\sim}_{\mathscr{R}}\; xy$.*

(c) *If $x \;{}_n{\sim}_{\mathscr{R}}\; y$ then for each prefix x' of x and for each prefix y' of y, $x' \;{}_n{\sim}_{\mathscr{R}}\; y'$ iff $x' \;{}_n{\sim}\; y'$.*

Proof.

(a) Since x is a prefix of x there exists a prefix v of y such that $x \;{}_n{\sim}\; v$. Thus $\mu_n(x) = \mu_n(v) \subseteq \mu_n(y)$. Similarly $\mu_n(y) \subseteq \mu_n(x)$; so $\mu_n(x) = \mu_n(y)$. Therefore $x \;{}_n{\sim}\; y$.

(b) Any prefix of x is also a prefix of xy. Let v be any prefix of xy. Then either v is a prefix of x or x is a prefix of v. In the second case $\mu_n(x) \subseteq \mu_n(v) \subseteq \mu_n(xy) = \mu_n(x)$ so that $x \;{}_n{\sim}\; v$. Therefore $x \;{}_n{\sim}_{\mathscr{R}}\; xy$. The converse follows from (a).

(c) Suppose $x' \;{}_n{\sim}\; y'$. Let u be a prefix of x'. Since u is also a prefix of x there exists a prefix v of y such that $u \;{}_n{\sim}\; v$. Now either v is a prefix of y' or y' is a prefix of v. In the second case $\mu_n(y') \subseteq \mu_n(v) = \mu_n(u) \subseteq \mu_n(x') = \mu_n(y')$, so that $y' \;{}_n{\sim}\; v$ and hence $u \;{}_n{\sim}\; y'$. Similarly for each prefix v of y' there exists a prefix u of x' such that $u \;{}_n{\sim}\; v$. Therefore $x' \;{}_n{\sim}_{\mathscr{R}}\; y'$. The converse follows from (a).

PROPOSITION 4.3. *Let $x, y \in A^*$ and $n \geqslant 0$. Then*

(a) $x^n \;{}_n{\sim}_{\mathscr{R}}\; x^{n+1}$.

(b) $(xy)^n \;{}_n{\sim}_{\mathscr{R}}\; (xy)^n x$.

Proof. Immediate from Propositions 3.3(a,b), and 4.2(b).

PROPOSITION 4.4. *Let $x, y \in A^*$ and $n \geqslant 0$. Then $x \,_{n+1}{\sim}_{\mathscr{R}}\, y$ implies $x \,_{n}{\sim}_{\mathscr{R}}\, y$.*

Proof. Follows from Proposition 3.4.

LEMMA 4.5. *Let $u, v \in A^*$ and $n > 0$. Then $u \,_{n}{\sim}_{\mathscr{R}}\, uv$ iff there exist $u_1, \ldots, u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_n) \supseteq \alpha(v)$.*

Proof. Follows from Lemma 3.5 and Proposition 4.2(b).

PROPOSITION 4.6. *$_{n}{\sim}_{\mathscr{R}}$ is a congruence of finite index for all $n \geqslant 0$.*

Proof. Let $n \geqslant 0$ and let $x, y \in A^*$ be such that $x \,_{n}{\sim}_{\mathscr{R}}\, y$. Let $a \in A$.

Suppose u is a prefix of xa. Then either u is a prefix of x or $u = xa$. In the first case, because $x \,_{n}{\sim}_{\mathscr{R}}\, y$, there is a prefix v of y such that $u \,_{n}{\sim}\, v$. If $u = xa$ then from Proposition 4.2(a) $x \,_{n}{\sim}\, y$, and since $_{n}{\sim}$ is a congruence $u = xa \,_{n}{\sim}\, ya$. By symmetry, for each prefix v of ya there exists a prefix u of xa such that $u \,_{n}{\sim}\, v$. Therefore $_{n}{\sim}_{\mathscr{R}}$ is a right congruence.

Suppose u is a prefix of ax. Then either $u = 1$ or $u = au'$ for some prefix u' of x. If $u = 1$ then u is also a prefix of ay. Otherwise, since $x \,_{n}{\sim}_{\mathscr{R}}\, y$, there exists a prefix v' of y such that $u' \,_{n}{\sim}\, v'$. But $_{n}{\sim}$ is a congruence so $u = au' \,_{n}{\sim}\, av'$. Similarly for each prefix v of ay there exists a prefix u of ax such that $u \,_{n}{\sim}\, v$. Hence $_{n}{\sim}_{\mathscr{R}}$ is a left congruence.

The fact that $_{n}{\sim}_{\mathscr{R}}$ is of finite index follows directly from the fact that $_{n}{\sim}$ is of finite index.

One nice property of $_{n}{\sim}_{\mathscr{R}}$, which is not shared by $_{n}{\sim}$, is that each congruence class has a unique shortest element.

THEOREM 4.7. *Every congruence class of $_{n}{\sim}_{\mathscr{R}}$ contains a unique element of minimal length. Furthermore, if $a_1, \ldots, a_m \in A$ then $a_1 \cdots a_m$ is minimal iff $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \mu_n(a_1a_2) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m)$.*

Proof. By induction on k, the minimum length of elements in a given $_{n}{\sim}_{\mathscr{R}}$ class. Note that minimum length elements exist because length is a function from A^* to the nonnegative integers which form a well-ordered set.

For $k = 0$ the lemma is true since 1 is the only word of length 0. Let $k \geqslant 1$ and assume the lemma is true for all $_{n}{\sim}_{\mathscr{R}}$ classes containing elements of length less than k.

Suppose there exists a $_{n}{\sim}_{\mathscr{R}}$ class containing minimal elements x and y of length k. Since $k \geqslant 1$, $x = ua$ for some $u \in A^*$, $a \in A$. Now $\mu_n(u) \subseteq \mu_n(x)$, and $u \,_{n}{\sim}\, x$ implies $u \,_{n}{\sim}_{\mathscr{R}}\, x$ by Proposition 4.2(b), so $\mu_n(u) \neq \mu_n(x)$. Employing the induction hypothesis (since $|u| < k$) the $_{n}{\sim}_{\mathscr{R}}$ class containing u has a unique element of minimal length. Call this element w. If $w \neq u$ then $|w| < |u|$ and hence $|wa| < |x|$. But $w \,_{n}{\sim}_{\mathscr{R}}\, u$ and $_{n}{\sim}_{\mathscr{R}}$ is a congruence, so $wa \,_{n}{\sim}_{\mathscr{R}}\, ua = x$ contradicting the minimality of x. Therefore $u = w$. By the induction hypothesis $u = a_1 \cdots a_m$ where $\mu_n(a_1) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m)$ and thus $x = a_1 \cdots a_m a$ where $\mu_n(a_1) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m) \subsetneq \mu_n(a_1 \cdots a_m a)$.

Because $x \;{}_n\!\sim_{\mathscr{R}}\; y$ there exists a prefix v of y such that $u \;{}_n\!\sim\; v$. By Proposition 4.2(c), $u \;{}_n\!\sim_{\mathscr{R}}\; v$. Also, v is a proper prefix of y since $\mu_n(v) = \mu_n(u) \subsetneq \mu_n(x) = \mu_n(y)$. Thus $v = u$, for otherwise $k = |y| \geqslant 1 + |v| > 1 + |u| = |x| = k$ which is impossible. Therefore $y = ua'$ for some $a' \in A$. Now $\mu_n(u) \subsetneq \mu_n(ua)$; hence there exists a word $za \in \mu_n(ua) - \mu_n(u)$. But $\mu_n(ua) = \mu_n(ua')$, so $za \in \mu_n(ua') - \mu_n(u)$. That being the case $a = a'$ and thus $x = y$.

By induction on k every congruence class of ${}_n\!\sim_{\mathscr{R}}$ contains a unique element of minimal length, and if $a_1, \ldots, a_m \in A$ are such that $a_1 \cdots a_m$ is minimal then $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m)$.

Finally, suppose $x = a_1 \cdots a_m$ where $a_1, \ldots, a_m \in A$ and $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m)$. Let $u_0 = 1$, $u_1 = a_1, \ldots, u_m = a_1 \cdots a_m$ be the prefixes of x and let y be the unique minimal element of the ${}_n\!\sim_{\mathscr{R}}$ class containing x. Since $x \;{}_n\!\sim_{\mathscr{R}}\; y$ there exist prefixes $v_0, v_1, \ldots, v_m$ of y such that $u_i \;{}_n\!\sim\; v_i$ for $0 \leqslant i \leqslant m$. Because $\mu_n(v_i) = \mu_n(u_i) \neq \mu_n(u_j) = \mu_n(v_j)$ for all $i \neq j$, the v_i's must be distinct. Thus $|y| \geqslant m$. But $|x| = m$; therefore by the uniqueness of the minimal element $x = y$.

DEFINITION 4.8. For $n \geqslant 0$ define the function $\chi_n \colon A^* \to A^*$ by $\chi_n(x) =$ the unique minimal element ${}_n\!\sim_{\mathscr{R}}$ congruent to x.

The following is an algorithm for finding the minimal element of a congruence class of ${}_n\!\sim_{\mathscr{R}}$ given any word x in the class.

Algorithm 4.9. Compute $\chi_n(x)$.

Find the shortest prefix ua of x such that $u \in A^*$, $a \in A$, and $u \;{}_n\!\sim\; ua$. If none exists then $x = a_1 \cdots a_m$ where $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \mu_n(a_1 a_2) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m)$ and $\chi_n(x) = x$.

Otherwise $x = uav$ for some $v \in A^*$. Since $u \;{}_n\!\sim\; ua$ implies $u \;{}_n\!\sim_{\mathscr{R}}\; ua$ and ${}_n\!\sim_{\mathscr{R}}$ is a congruence, $uv \;{}_n\!\sim_{\mathscr{R}}\; uav = x$. Thus $\chi_n(x) = \chi_n(uv)$. Note that uv is shorter than x and so the algorithm always terminates.

EXAMPLE. Let $x = abccbcac$ and $n = 2$

Prefix u of x	$\mu_2(u)$
1	1
a	1, a
ab	1, a, b, ab
abc	1, a, b, ab, c, ac, bc
$abcc$	1, a, b, ab, c, ac, bc, cc
$abccb$	1, a, b, ab, c, ac, bc, cc, cb, bb
$abccbc$	1, a, b, ab, c, ac, bc, cc, cb, bb

Since $\mu_2(abccb) = \mu_2(abccbc)$, $abccb \;{}_2\!\sim_{\mathscr{R}}\; abccbc$ and hence $abccbac \;{}_2\!\sim_{\mathscr{R}}\; abccbcac = x$. Replace x by $abccbac$.

$abccba$	1, a, b, ab, c, ac, bc, cc, cb, bb, aa, ba, ca
$abccbac$	1, a, b, ab, c, ac, bc, cc, cb, bb, aa, ba, ca

Since $\mu_2(abccba) = \mu_2(abccbac)$, $abccba \;{}_2{\sim}_{\mathscr{R}}\; abccbac$. Now $\mu_2(1) \subsetneq \mu_2(a) \subsetneq \mu_2(ab) \subsetneq \mu_2(abc) \subsetneq \mu_2(abcc) \subsetneq \mu_2(abccb) \subsetneq \mu_2(abccba)$; therefore $\chi_2(x) = abccba$.

To construct $\mu_n(ua)$ from $\mu_n(u)$ it is only necessary to add those elements wa such that $w \in \mu_{n-1}(u)$ but $wa \notin \mu_n(u)$. The number of elements in $\mu_n(u)$ is bounded by $\sum_{i=0}^{n} m^i$, where m is the cardinality of the alphabet. Given x, $\chi_n(x)$ can be found in $O(|x|)$ steps. Thus in $O(|x| + |y|)$ steps one can determine whether $x \;{}_n{\sim}_{\mathscr{R}}\; y$.

5. $\mathscr{R}$-Trivial Monoids

The following theorem is from [9, 1].

Theorem 5.1. *Let M be a finite monoid. The following conditions are equivalent.*

1. *M is $\mathscr{R}$-trivial.*
2. *For all $f, g, h \in M$, $fgh = f$ implies $fg = f$.*
3. *For all idempotents $e \in M$, $eM_e = e$.*
4. *There exists $n > 0$ such that, for all $f, g \in M$, $(fg)^n f = (fg)^n$.*

Lemma 5.2. *Let M be a finite $\mathscr{R}$-trivial monoid and $\varphi\colon A^* \to M$ a surjective morphism. Let n be the cardinality of M and let $u, v \in A^*$. Then*

$$u \;{}_n{\sim}\; uv \text{ implies } \underline{u} = \underline{uv},$$

where $\underline{x}$ denotes $\varphi(x)$.

Proof. Suppose $u \;{}_n{\sim}\; uv$. By Lemma 3.5, there exist $u_1, \ldots, u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_n) \supseteq \alpha(v)$. Let $u_0 = 1$. By the choice of n, the elements $\underline{u_0}, \underline{u_0 u_1}, \ldots, \underline{u_0 u_1 \cdots u_n}$ cannot all be distinct. Hence there exist i and j, $0 \leqslant i < j \leqslant n$, such that

$$f = \underline{u_0 \cdots u_i} = \underline{u_i \cdots u_i \cdots u_j} = f\underline{u_{i+1} \cdots u_j} = f\underline{u_{i+1}(u_{i+2} \cdots u_j)}.$$

Since M is $\mathscr{R}$-trivial, $f = f\underline{u_{i+1}}$. If $\alpha(u_n) = \varnothing$ then $v = 1$ and there is nothing to prove. Thus suppose $\alpha(u_n) \neq \varnothing$. Since $\alpha(u_{i+1}) \supseteq \alpha(u_n) \neq \varnothing$, we have $u_{i+1} = az$ for some $a \in \alpha(u_{i+1})$, $z \in A^*$. Then $f = f\underline{az}$ and $f = f\underline{a}$. Consequently $f = f\underline{a}$ for all $a \in \alpha(u_{i+1})$. Because $u_{i+1} \cdots u_n v \in (\alpha(u_{i+1}))^*$ it follows that

$$\underline{u} = \underline{u_0 \cdots u_n} = f\underline{u_{i+1} \cdots u_n} = f\underline{u_{i+1} \cdots u_n v} = \underline{uv}.$$

Theorem 5.3. *Let M be the syntactic monoid of $X \subseteq A^*$. Then M is finite and $\mathscr{R}$-trivial iff X is a ${}_n{\sim}_{\mathscr{R}}$ language for some $n \geqslant 0$.*

Proof. Assume M is finite and $\mathscr{R}$-trivial. Let n be the cardinality of M and let $x, y \in A^*$. We have to prove $x \;{}_n{\sim}_{\mathscr{R}}\; y$ implies $\underline{x} = \underline{y}$.

Since $\chi_n(x) = \chi_n(y)$ it is sufficient to prove that $\underline{x} = \underline{\chi_n(x)}$. Let $x_0 = x, x_1, ..., x_p = \chi_n(x)$ be the words obtained after each reduction in Algorithm 4.9. (In the example of the text, one has $x_0 = abccbcac$, $x_1 = abccbac$, and $x_2 = abccba = \chi_2(x)$.) Then, for $i = 0, 1, ..., p-1$, the words x_i and x_{i+1} have the form $x_i = uav$ and $x_{i+1} = uv$ with $u \; {}_n\!\sim v$.

Using Lemma 5.2, we have $\underline{u} = \underline{ua}$ and therefore $\underline{x_i} = \underline{x_{i+1}}$. The result $\underline{x} = \underline{\chi_n(x)}$ follows.

By Proposition 4.3, for all $x, y \in A^*$,

$$(xy)^n \; {}_n\!\sim_{\mathscr{R}} (xy)^n x.$$

If X is a ${}_n\!\sim_{\mathscr{R}}$ language we must have

$$(\underline{xy})^n = (\underline{xy})^n \underline{x}.$$

Since M is the range of the surjective morphism $\varphi: A^* \to M$, it follows that for all $f, g \in M$,

$$(fg)^n = (fg)^n f.$$

Because ${}_n\!\sim_{\mathscr{R}}$ is of finite index M is finite, and it is $\mathscr{R}$-trivial by Theorem 5.1.

6. Partially Ordered Finite Automata

In this section the finite automata associated with ${}_n\!\sim_{\mathscr{R}}$ languages are considered. In the sequel we assume that all semiautomata and automata are finite.

Recall the definition of partially ordered automata and semiautomata given in the Introduction. The following equivalent characterization is from [9].

Proposition 6.1. $\mathbf{S} = \langle A, Q, \sigma \rangle$ *is partially ordered iff for all* $q \in Q$, $x, y \in A^*$, $\sigma(q, xy) = q$ *implies* $\sigma(q, x) = q$.

Proposition 6.2. *Let* $\mathbf{S} = \langle A, Q, \sigma \rangle$ *be a partially ordered semiautomaton. Then the transformation monoid,* M, *of* $\mathbf{S}$ *is* $\mathscr{R}$*-trivial.*

Proof. Suppose $f, g, h \in M$ are such that $fgh = f$. Since M is the transformation monoid of $\mathbf{S}$ there exist $x, y, z \in A^*$ such that $\underline{x} = f$, $\underline{y} = g$, and $\underline{z} = h$. Now $\underline{xyz} = fgh = f = \underline{x}$ and $\mathbf{S}$ is partially ordered. Thus $\sigma(q, x) = \sigma(q, xyz) = \sigma(\sigma(q, x), yz)$, and by Proposition 6.1, $\sigma(q, x) = \sigma(\sigma(q, x), y) = \sigma(q, xy)$ for all $q \in Q$. Therefore $f = \underline{x} = \underline{xy} = fg$.

We now present additional properties of partially ordered semiautomata mentioned in [7, 9, 11] The proofs of these results are straightforward and can be easily verified by the reader.

PROPOSITION 6.3. *If* $\mathbf{T}$ *is a semiautomaton which is covered by some partially ordered semiautomaton* $\mathbf{S}$ *then* $\mathbf{T}$ *is partially ordered.*

PROPOSITION 6.4. *The direct product of two partially ordered semiautomata is partially ordered.*

PROPOSITION 6.5. *The cascade product of two partially ordered semiautomata is partially ordered.*

Let $\mathbf{A} = \langle A, Q, q_0, F, \sigma\rangle$ *and* $\mathbf{B} = \langle A, P, p_0, G, \tau\rangle$ *be finite automata and let* $\langle A, Q \times P, \pi\rangle = \langle A, Q, \sigma\rangle \times \langle A, P, \tau\rangle$. *Then the union of* $\mathbf{A}$ *and* $\mathbf{B}$ *is*

$$\mathbf{A} \cup \mathbf{B} = \langle A, Q \times P, (q_0, p_0), F \times P \cup Q \times G, \pi\rangle,$$

the intersection of $\mathbf{A}$ *and* $\mathbf{B}$ *is*

$$\mathbf{A} \cap \mathbf{B} = \langle A, Q \times P, (q_0, p_0), F \times G, \pi\rangle,$$

and the complement of $\mathbf{A}$ *is*

$$\bar{\mathbf{A}} = \langle A, Q, q_0, Q - F, \sigma\rangle.$$

Because the definition of a partially ordered automaton does not depend on the set of final states it follows that if $\mathbf{A}$ and $\mathbf{B}$ are partially ordered then $\mathbf{A} \cup \mathbf{B}$, $\mathbf{A} \cap \mathbf{B}$, and $\bar{\mathbf{A}}$ are also. Hence the set of all partially ordered finite automata with alphabet A forms a Boolean algebra.

Another way partially ordered automata can be characterized is in terms of certain sequential networks.

DEFINITION 6.6. *For* $n \geqslant 0$, *an n-way fork* is an initialized semiautomaton $\langle A, \{q_0, q_1, \ldots, q_n\}, q_0, \sigma\rangle$ where $A = A_0 \cup A_1 \cup \cdots \cup A_n$, the A_i's are nonempty and pairwise disjoint, $\sigma(q_0, a) = q_i$ for all $a \in A_i$, and $\sigma(q_i, a) = q_i$ for all $a \in A$, $i = 1, \ldots, n$. (See Fig. 1.) A *half-reset* is a one-way fork.

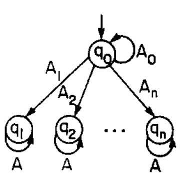

FIG. 1. An n-way fork.

PROPOSITION 6.7. *If a semiautomaton can be covered by a cascade product of half-resets then it is partially ordered.*

Proof. Immediate from Propositions 6.3 and 6.5 and the fact that a half-reset is partially ordered.

In [7, 11] it is proved that any partially ordered finite automaton can be covered by a cascade product of half-resets. Introducing n-way forks is a convenient intermediate step.

PROPOSITION 6.8. *Any n-way fork is isomorphic to the connected initialized subsemiautomaton of a cascade product of n half-resets.*

Proof. By induction on n. The case $n = 0$ is degenerate. For $n = 1$ the result follows from the definition of a half-reset. Assume the result is true for $n \geqslant 1$. Consider the $(n + 1)$-way fork $\mathbf{F}_{n+1}$ illustrated in Fig. 2a.

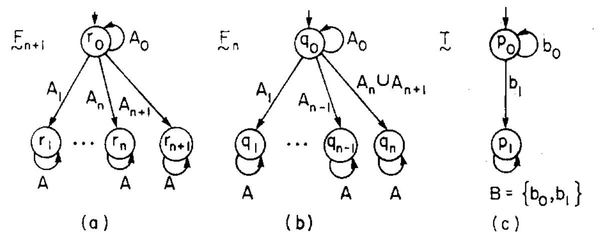

FIG. 2. The forks $\mathbf{F}_{n+1}$, $\mathbf{F}_n$, and $\mathbf{T}$.

Let $\mathbf{F}_n = \langle A, Q, q_0, \sigma\rangle$ be the n-way fork of Fig. 2b and let $\mathbf{T} = \langle\{b_0, b_1\}, P, p_0, \tau\rangle$ be the half-reset in Fig. 2c. Define the connection ω as follows:

$$\begin{aligned} \omega(q, a) &= b_1 \qquad \text{if } q = q_0 \text{ and } a \in A_{n+1} \\ &= b_0 \qquad \text{otherwise.} \end{aligned}$$

Let $\mathbf{R} = \langle A, R, (q_0, p_0), \eta\rangle$ be the connected initialized subsemiautomaton of $\mathbf{F}_n \circ \mathbf{T}$. Note that $R = \{(q_0, p_0), (q_1, p_0), \ldots, (q_n, p_0), (q_n, p_1)\}$ since these are the only states which are accessible from (q_0, p_0). Except for (q_0, p_0) each is a terminal state (i.e., $\eta(r, a) = r$ for all $a \in A$, $r \in R - \{(p_0, q_0)\}$). It is clear that $\mathbf{F}_{n+1}$ is isomorphic to $\mathbf{R}$.

By the induction hypothesis $\mathbf{F}_n$ is isomorphic to the connected initialized subsemiautomaton of a cascade product of n half-resets; therefore $\mathbf{F}_{n+1}$ is isomorphic to the connected initialized subsemiautomaton of a cascade product of $n + 1$ half-resets. Thus the result is true for all $n \geqslant 1$.

We call a graph G *tree-like* iff the graph G' obtained from G by removing all trivial loops is a tree. (A trivial loop is an edge from a vertex to itself.) The height of G is defined to be the height of the tree G'.

PROPOSITION 6.9. *Any initialized semiautomaton whose state graph is tree-like is isomorphic to the connected initialized subsemiautomaton of a cascade product of forks.*

Proof. By induction on the height of the graph.

If the graph of an initialized semiautomaton is tree-like of height less than or equal to 1 then the semiautomaton is a fork. Assume the result is true for all initialized semiautomata whose graphs are tree-like of height less than h, where $h > 1$.

Let $\mathbf{S} = \langle A, Q, q_0, \sigma\rangle$ be an initialized semiautomaton whose graph is tree-like of height h. Let $\{q_1, ..., q_n\} = \{q \in Q - \{q_0\} \mid \sigma(q_0, a) = q$ for some $a \in A\}$ be the set of sons of q_0. For $1 \leqslant i \leqslant n$ let $\mathbf{S}_i = \langle A, Q_i, q_i, \sigma_i\rangle$ be the subsemiautomaton of $\mathbf{S}$ initialized at q_i. Since $q_i \neq q_0$, the height of the graph is less than h; thus $\mathbf{S}_i$ is isomorphic to the connected initialized subsemiautomaton of $\mathbf{S}_i' = \langle A, Q_i', q_i, \sigma_i'\rangle$, a cascade product of forks.

Define $\mathbf{T}_i' = \langle B_i, Q_i', q_i, \tau_i'\rangle$ as follows. If there exists an $a_i \in A$ such that $\sigma_i'(q, a_i) = q$ for all $q \in Q_i'$ let $B_i = A$ and $\tau_i' = \sigma_i'$. Otherwise let $B_i = A \cup \{e\}$, where $e \notin A$, and let τ_i' be such that for $q \in Q_i'$, $b \in B_i$,

$$\begin{aligned} \tau_i'(q, b) &= \sigma_i'(q, b) && \text{if } b \in A \\ &= q && \text{if } b = e. \end{aligned}$$

Note that $\mathbf{T}_i'$ is still a cascade product of forks.

Let $\mathbf{T}_0 = \langle A, P, p_0, \tau_0\rangle$ be the n-way fork where $P = \{p_0, p_1, ..., p_n\}$ and

$$\begin{aligned} \tau_0(p, a) &= p_i && \text{if } p = p_0 \text{ and } \sigma(q_0, a) = q_i \\ &= p && \text{otherwise.} \end{aligned}$$

Inductively define $\mathbf{T}_i = \mathbf{T}_{i-1} \circ \mathbf{T}_i'$ for $i = 1, ..., n$ where the connection ω_i: $P \times Q_1' \times \cdots \times Q_{i-1}' \times A \to B_i$ is given by

$$\begin{aligned} \omega_i(r, a) &= a && \text{if } r = (p_i, q_1, ..., q_{i-1}) \\ &= b_i && \text{otherwise,} \end{aligned}$$

where $\tau_i'(q, b_i) = q$ for all $q \in Q_i'$.

It is a straightforward proof by induction to show that the set of states of $\mathbf{T}_i$ accessible from the initial state $(p_0, q_1, ..., q_i)$ is

$$R_i = \{(p_0, q_1, ..., q_i)\} \cup \{(p_k, q_1, ..., q_{k-1}, q, q_{k+1}, ..., q_i) \mid q \in Q_k', 1 \leqslant k \leqslant i\}$$

and that the following equations hold:

$$\begin{aligned} &\tau_i((p_0, q_1, ..., q_i), a) \\ &\quad = (p_k, q_1, ..., q_i) \qquad \text{for all } a \in A \text{ such that } \sigma(q_0, a) = q_k, \\ &\tau_i((p_k, q_1, ..., q_{k-1}, q, q_{k+1}, ..., q_i), a) \\ &\quad = (p_k, q_1, ..., q_{k-1}, \tau_k'(q, a), q_{k+1}, ..., q_i) \qquad \text{for} \quad q \in Q_k', \quad 1 \leqslant k \leqslant i, \end{aligned}$$

and

$$\tau_i((p_k, q_1, ..., q_i), a) = (p_k, q_1, ..., q_i) \qquad \text{for} \quad i < k \leqslant n.$$

Now consider the bijection $\psi: Q \to R_n$ defined by

$$\begin{aligned}\psi(q) &= (p_0, q_1, \ldots, q_n) && \text{if} \quad q = q_0\\ &= (p_i, q_1, \ldots, q_{i-1}, \psi_i(q), q_{i+1}, \ldots, q_n) && \text{if} \quad q \in Q_i,\end{aligned}$$

where $\psi_i: Q_i \to Q_i'$ is the isomorphism from $\mathbf{S}_i$ to the connected initialized subsemiautomaton of $\mathbf{S}_i'$. Let $a \in A$ and $q \in Q$. If $q \in Q_i$ then

$$\begin{aligned}\psi(\sigma(q, a)) &= \psi(\sigma_i(q, a))\\ &= (p_i, q_1, \ldots, q_{i-1}, \psi_i(\sigma_i(q, a)), q_{i+1}, \ldots, q_n)\\ &= (p_i, q_1, \ldots, q_{i-1}, \sigma_i'(\psi_i(q), a), q_{i+1}, \ldots, q_n)\\ &= (p_i, q_1, \ldots, q_{i-1}, \tau_i'(\psi_i(q), a), q_{i+1}, \ldots, q_n)\\ &= \tau_n((p_i, q_1, \ldots, q_{i-1}, \psi_i(q), q_{i+1}, q_n), a)\\ &= \tau_n(\psi(q), a),\end{aligned}$$

and if $q = q_0$ and $\sigma(q_0, a) = q_i$ then

$$\begin{aligned}\psi(\sigma(q, a)) &= \psi(q_i)\\ &= (p_i, q_1, \ldots, q_{i-1}, \psi_i(q_i), q_{i+1}, \ldots, q_n)\\ &= (p_i, q_1, \ldots, q_{i-1}, q_i, q_{i+1}, \ldots, q_n)\\ &= \tau_n((p_0, q_1, \ldots, q_n), a)\\ &= \tau_n(\psi(q_0), a).\end{aligned}$$

Thus ψ is an isomorphism between $\mathbf{S}$ and the connected initialized subsemiautomaton of $\mathbf{T}_n$; so the result is true for $\mathbf{S}$. It follows by induction that the proposition is true.

COROLLARY 6.10. *Any partially ordered initialized semiautomaton is the homomorphic image of the connected initialized subsemiautomaton of a cascade product of half-resets.*

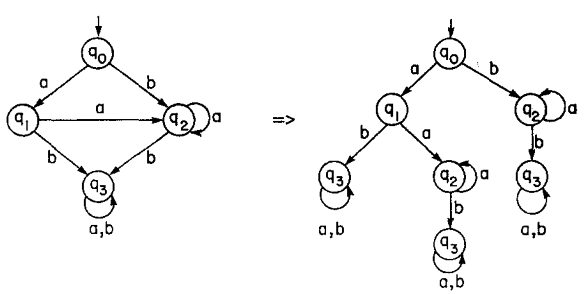

FIG. 3. Transformation to a tree-like graph.

Proof. Any partially ordered rooted graph can be transformed into a tree-like graph by splitting nodes (see Fig. 3). The desired homomorphism is the obvious one which maps a node in the tree-like graph to the node in the original graph from which it was produced. The result then follows by Proposition 6.9.

7. $\mathcal{R}$-EXPRESSIONS

DEFINITION 7.1. Let A be a finite alphabet. An ***$\mathcal{R}$-expression*** is a finite union of regular expressions of the form $A_0^* a_1 A_1^* \cdots a_m A_m^*$ where $m \geqslant 0$, $a_1, \ldots, a_m \in A$, $A_i \subseteq A$ for $0 \leqslant i \leqslant m$, and $a_i \notin A_{i-1}$ for $1 \leqslant i \leqslant m$.

The relationship between partially ordered semiautomata and $\mathcal{R}$-expressions is mentioned in [7]. For further details see [5].

PROPOSITION 7.2. *Let $X \subseteq A^*$ be the language denoted by some $\mathcal{R}$-expression. Then the reduced finite automaton recognizing X is partially ordered.*

With the aid of Theorem 4.7 one can verify the following result:

PROPOSITION 7.3. *Every ${}_n{\sim}_{\mathcal{R}}$ language can be denoted by an $\mathcal{R}$-expression.*

With this result, Theorem 5.3, Proposition 6.2, and Proposition 7.2 the languages defined by the congruences ${}_n{\sim}_{\mathcal{R}}$, $\mathcal{R}$-trivial monoids, partially ordered finite automata and $\mathcal{R}$-expressions are seen to be the same. An alternate proof of this can be constructed using Eilenberg's result [4] showing the equivalence of $\mathcal{R}$-expressions and $\mathcal{R}$-trivial monoids.

These characterizations are analogous to and generalizations of characterizations of the well-known family of Reverse Definite languages. This correspondence was first studied in [1]; further work appears in [5]. In particular, the expressional characterization

$$(\mathcal{W} \cup \mathcal{W}A^*)\mathbf{B} \qquad \text{where} \quad \mathcal{W} = \{\{x\} \mid x \in A^*\}$$

for Reverse Definite languages motivated the following theorem.

PROPOSITION 7.4. *Let A be an alphabet and let $\mathcal{D} = \{C^*a \mid C \subseteq A - \{a\}\}\mathbf{M}$. Then $(\mathcal{D} \cup \mathcal{D}A^*)\mathbf{B}$ is equal to the set of $\mathcal{R}$-expressions over the alphabet A.*

Proof. It is convenient to consider elements of $\mathcal{D}$ as "words" over the alphabet $\{C^*a \mid C \subseteq A - \{a\}\}$. This is reflected in the notation below.

($\subseteq$) Let $w \in \mathcal{D}$. If $w = 1$ then w and wA^* can be expressed by the $\mathcal{R}$-expressions ϕ^* and A^*, respectively. Otherwise $w = A_1^* a_1 \cdots A_m^* a_m$ where $m > 0$ and $a_i \notin A_i$ for $1 \leqslant i \leqslant m$. In this case $w = A_1^* a_1 \cdots A_m^* a_m \phi^*$ and $wA^* = A_1^* a_1 \cdots A_m^* a_m A^*$ which are both $\mathcal{R}$-expressions. The set of $\mathcal{R}$-expressions forms a Boolean algebra (since the set of partially ordered finite automata over A does) and thus it contains $(\mathcal{D} \cup \mathcal{D}A^*)\mathbf{B}$.

(E) Suppose $w = A_0^* a_1 \cdots a_m A_m^*$, where $m \geqslant 0$ and $A_{i-1} \subseteq A - \{a_i\}$ for $1 \leqslant i \leqslant m$. Clearly, if $A_m = \phi$ then $w \in \mathscr{D}$, and if $A_m = A$ then $w \in \mathscr{D}A^*$, so suppose $\phi \neq A_m \subsetneq A$. Let $w' = A_0^* a_1 \cdots A_{m-1}^* a_m \in \mathscr{D}$.

Claim:

$$w = w'A^* \cap \overline{\bigcup_{b \in A - A_m} wbA^*}.$$

Let $x \in w$. Clearly $x \in w'A^*$. Now $a_1 \cdots a_m b$ is a subword of all words in wbA^* but, if $b \notin A_m$, $a_1 \cdots a_m b$ is *not* a subword of x. Therefore $x \notin wbA^*$ for $b \in A - A_m$, that is, $x \in \overline{\bigcup_{b \in A - A_m} wbA^*}$. Thus $w \subseteq w'A^* \cap \overline{\bigcup_{b \in A - A_m} wbA^*}$.

Let $x \in w'A^* \cap \overline{\bigcup_{b \in A - A_m} wbA^*}$. Since $x \in w'A^*$, $x = yz$ where $y \in w'$ and $z \in A^*$. Now suppose $\alpha(z) \cap (A - A_m) \neq \phi$. Then $z = ubv$ where $u \in A_m^*$, $b \in \alpha(z) \cap (A - A_m)$, and $v \in A^*$. But this implies $x = yubz \in w'A_m^* bA^* = wbA^* \subseteq \bigcup_{b \in A_m - A} wbA^*$, which is a contradiction. Therefore $z \in A_m^*$, so $x \in w'A_m^* = w$. Thus $w'A^* \cap \overline{\bigcup_{b \in A - A_m} wbA^*} \subseteq w$, and hence the claim is true.

Now for $b \in A - A_m$, $wb \in \mathscr{D}$ and thus $w = w'A^* \cap \overline{\bigcup_{b \in A - A_m} wbA^*} \in (\mathscr{D} \cup \mathscr{D}A^*)\mathbf{B}$. Since $(\mathscr{D} \cup \mathscr{D}A^*)\mathbf{B}$ is a Boolean algebra it follows that every $\mathscr{R}$-expression is in $(\mathscr{D} \cup \mathscr{D}A^*)\mathbf{B}$.

THEOREM 7.5. *Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $\mathbf{A} = \langle A, Q, q_0, F, \sigma \rangle$ be the reduced automaton accepting X. The following conditions are equivalent.*

M1. *M is $\mathscr{R}$-trivial.*

M2. *For all $f, g, h \in M$, $fgh = f$ implies $fg = f$.*

M3. *For all idempotents $e \in M$, $eM_e = e$.*

M4. *There exists an $n > 0$ such that for all $f, g \in M$, $(fg)^n f = (fg)^n$.*

X1. *X is an ${}_n{\sim}_{\mathscr{R}}$ language for some $n \geqslant 0$.*

E1. *X can be denoted by an $\mathscr{R}$-expression.*

E2 *$X \in (\mathscr{D} \cup \mathscr{D}A^*)\mathbf{B}$ where $\mathscr{D} = \{C^*a \mid C \subseteq A - \{a\}\}\mathbf{M}$.*

A1. *$\mathbf{A}$ is partially ordered.*

A2. *For all $x, y \in A^*$ and for all $q \in Q$, $\sigma(q, xy) = q$ implies $\sigma(q, x) = q$.*

A3. *$\mathbf{A}$ is covered by a cascade product of half-resets.*

It is now possible to relate the family of languages corresponding to finite $\mathscr{R}$-trivial monoids to the dot-depth hierarchy. That hierarchy is defined by $\mathscr{B}_0 = \{\{a\} \mid a \in A\}\,\mathbf{MB}$ and $\mathscr{B}_{i+1} = B_i\mathbf{MB}$ for $i \geqslant 0$.

Since $\{\{a\} \mid a \in A\}\mathbf{M} = \{\phi^*a \mid a \in A\}\mathbf{M} \subseteq \{C^*a \mid C \subseteq A - \{a\}\}\mathbf{M} = \mathscr{D}$, $\mathscr{B}_0 = \{\{a\} \mid a \in A\}\,\mathbf{MB} \subseteq \mathscr{D}\mathbf{B} \subsetneq (\mathscr{D} \cup \mathscr{D}A^*)\mathbf{B}$. Thus all languages in $\mathscr{B}_0$ have finite $\mathscr{R}$-trivial monoids.

Any ${}_n{\sim}$ language (${}_n{\sim}_1$ in the notation of [9]) is also an ${}_n{\sim}_{\mathscr{R}}$ language. However, the family $\mathscr{B}_1$ is incomparable with our family. The language $A^*a \in \mathscr{B}_1$, where the cardinality of A is greater than 1, has a reduced finite automaton which is not partially ordered. In [9, p. 116], Simon shows that for the cardinality of A greater than 2 the language denoted by the $\mathscr{R}$-expression a^*bA^* is not in $\mathscr{B}_1$.

Finally, for any $A_i \subsetneq A$, $A_i^* = \bigcap\{\overline{A^*aA^*} \mid a \in A - A_i\} \in \mathscr{B}_1$, so that any $\mathscr{R}$-expression denotes a language in $\mathscr{B}_1\mathbf{MB} = \mathscr{B}_2$.

8. Languages of $\mathscr{L}$-Trivial Monoids

The $\mathscr{L}$-trivial property is dual to that of $\mathscr{R}$-trivialness. As a result, characterizations analogous to those in Theorem 7.5 hold.

Definitions for the corresponding congruences are formed by using suffixes in place of prefixes. More precisely, if $x, y \in A^*$ and $n \geqslant 0$ then $x \;{}_n{\sim}_{\mathscr{L}}\; y$ iff for each suffix u of x there exists a suffix v of y such that $u \;{}_n{\sim}\; v$ and vice versa.

If $\mathbf{A}$ is the finite automaton of a language with an $\mathscr{L}$-trivial syntactic monoid then $\mathbf{A}^\rho$ is partially ordered. However, it is possible to describe these automata more directly.

Lemma 8.1. *Let $\mathbf{S} = \langle A, Q, \sigma\rangle$ be a semiautomaton, let $x \in A^*$, and let $B \subseteq A$. If $\sigma(q, ax) = \sigma(q, x)$ for all $a \in B$ and all $q \in Q$ then $\sigma(q, wx) = \sigma(q, x)$ for all $w \in B^*$ and all $q \in Q$.*

Proof. By induction on $|w|$.

The result is clearly true for $|w| = 0$. Assume it is true for all words in B^n. Suppose $w \in B^{n+1}$. Then $w = aw'$, where $a \in B$ and $w' \in B^n$, so that $\sigma(q, wx) = \sigma(\sigma(q, a), w'x) = \sigma(\sigma(q, a), x) = \sigma(q, ax) = \sigma(q, x)$. By induction the result is true for all words in B^*.

Proposition 8.2. *Let $\mathbf{S} = \langle A, Q, \sigma\rangle$ be a semiautomaton and let M be its transformation monoid. The following are equivalent.*

1. *M is $\mathscr{L}$-trivial.*
2. *There exists an $n > 0$ such that for all connected subsemiautomata $\mathbf{T} = \langle C, P, p_0, \tau\rangle$ of $\mathbf{S}$ and all n-full words w with $\alpha(w) = C$, $\tau(p, w) = \tau(p', w)$ for all $p, p' \in P$.*
3. *If $x \in A^*$ then $\sigma(q, x) = \sigma(q, xx)$ for all $q \in Q$ implies $\sigma(q, x) = \sigma(q, ax)$ for all $q \in Q$, $a \in \alpha(x)$.*

Proof. ($1 \Rightarrow 2$) Suppose M is $\mathscr{L}$-trivial. By the dual of Lemma 5.2 there exists an $n > 0$ such that for all $x, y \in A^*$, $x \;{}_n{\sim}\; yx$ implies $\underline{x} = \underline{yx}$.

Let $\mathbf{T} = \langle C, P, p_0, \tau\rangle$ be a connected subsemiautomaton of $\mathbf{S}$, let $p, p' \in P$, and let w be an n-full word with $\alpha(w) = C$.

Since $\mathbf{T}$ is connected there exist $u, v \in C^*$ such that $\tau(p_0, u) = p$ and $\tau(p_0, v) = p'$. Now w is n-full and $u, v \in (\alpha(w))^*$ so $uw \;{}_n{\sim}\; w$ and $vw \;{}_n{\sim}\; w$. This implies that $\underline{uw} = \underline{w} = \underline{vw}$ and thus $\tau(p, w) = \tau(p_0, uw) = \sigma(p_0, uw) = \sigma(p_0, vw) = \tau(p_0, vw) = \tau(p', w)$.

($2 \Rightarrow 3$) Suppose $x \in A^*$ is such that $\sigma(q, x) = \sigma(q, xx)$ for all $q \in Q$. By induction it follows that $\sigma(q, x) = \sigma(q, x^n)$ for all $q \in Q$ and $n \geqslant 1$.

Let $q \in Q$ and let $a \in \alpha(x)$. Consider the connected subsemiautomaton $\mathbf{T} = \langle \alpha(x), P, q, \tau \rangle$ of $\mathbf{S}$. Since x^n is n-full $\sigma(q, x) = \sigma(q, x^n) = \tau(q, x^n) = \tau(\tau(q, a), x^n) = \sigma(\sigma(q, a), x^n) = \sigma(\sigma(q, a), x) = \sigma(q, ax)$.

$(3 \Rightarrow 1)$ Let $e \in M$ be idempotent and let $g \in P_e$. Let $f, h \in M$ be such that $e = fgh$ Since M is the transformation monoid of $\mathbf{S}$ there exist $x, y, z \in A^*$ such that $\underline{x} = f$, $\underline{y} = g$, and $\underline{z} = h$. Let $w = xyz$ so that $\underline{w} = \underline{xyz} = fgh = e$

Since e is idempotent $\underline{w} = e = e^2 = \underline{w}^2$ so $\sigma(q, w) = \sigma(q, ww)$ for all $q \in Q$. Therefore $\sigma(q, aw) = \sigma(q, w)$ for all $a \in \alpha(w)$, $q \in Q$. Because $\alpha(y) \subseteq \alpha(w)$ we have, by Lemma 8.1, that $\sigma(q, yw) = \sigma(q, w)$ for all $q \in Q$. Thus $ge = \underline{yw} = \underline{w} = e$ so $P_e e = e$. But $P_e e = e$ implies $M_e e = e$; hence M is $\mathscr{L}$-trivial.

The final theorem, analogous to Theorem 7.5, summarizes the characterizations of languages with $\mathscr{L}$-trivial monoids.

THEOREM 8.3. *Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $\mathbf{A} = \langle A, Q, q_0, F, \sigma \rangle$ be the reduced automaton accepting X. The following conditions are equivalent.*

M1. *M is $\mathscr{L}$-trivial.*

M2. *For all $f, g, h \in M$, $hgf = f$ implies $gf = f$.*

M3. *For all idempotents $e \in M$, $M_e e = e$.*

M4. *There exists an $n > 0$ such that for all $f, g \in M$, $g(fg)^n = (fg)^n$.*

X1. *X is an ${}_n\!\sim_{\mathscr{L}}$ language for some $n \geqslant 0$.*

E1. *X can be expressed as the finite union of regular expressions of the form $A_0^* a_1 A_1^* \cdots a_m A_m^*$ where $m \geqslant 0$, $a_1, \ldots, a_m \in A$, $A_i \subseteq A$ for $0 \leqslant i \leqslant m$, and $a_i \notin A_i$ for $1 \leqslant i \leqslant m$.*

E2. *$X \in (\mathscr{D} \cup A^*\mathscr{D})\mathbf{B}$ where $\mathscr{D} = \{aC^* \mid C \subseteq A - \{a\}\}\mathbf{M}$.*

A1. *$\mathbf{A}^\rho$ is partially ordered.*

A2. *If $x \in A^*$ then $\sigma(q, x) = \sigma(q, xx)$ for all $q \in Q$ implies $\sigma(q, x) = \sigma(q, ax)$ for all $q \in Q$, $a \in \alpha(x)$.*

A3. *There exists an $n > 0$ such that for all connected subsemiautomata $\mathbf{T} = \langle C, P, p_0, \tau \rangle$ of $\mathbf{A}$ and all n-full words w with $\alpha(w) = C$, $\tau(p, w) = \tau(p', w)$ for all $p, p' \in P$.*

A4. *$\mathbf{A}^\rho$ is covered by a cascade product of half-resets.*

REFERENCES

1. J. A. BRZOZOWSKI, A generalization of finiteness, *in* "Semigroup Forum 13 (1977)," pp. 239–251.
2. A. H. CLIFFORD AND G. B. PRESTON, "The Algebraic Theory of Semigroups," Vol. 1, Amer. Math. Soc., Providence, R.I., 1961.

3. R. S. COHEN AND J. A. BRZOZOWSKI, Dot depth of star-free events, *J. Comput. System Sci.* **5** (1971), 1–16.
4. S. EILENBERG, "Automata, Languages, and Machines," Vol. B, Academic Press, New York, 1976.
5. F. E. FICH, "Languages of $\mathscr{R}$-trivial and related monoids," M. Math. thesis, University of Waterloo, Canada, 1979.
6. J. A. GREEN, On the structure of semigroups, *Ann. of Math.* **54** (1951), 163–172.
7. A. R. MEYER AND C. THOMPSON, Remarks on algebraic decomposition of automata, *Math. Systems Theory* **3** (1969), 110–118.
8. M. P. SCHÜTZENBERGER, On finite monoids having only trivial subgroups, *Inform. Contr.* 8 (1965), 190–194.
9. I. SIMON, "Hierarchies of Events with Dot-Depth one," Ph.D. thesis, University of Waterloo, Canada, 1972.
10. I. SIMON, Piecewise testable events, *in* "Automata Theory and Formal Languages," 2nd GI Conference (H. Brakhage, Ed.), pp. 214–222, Lecture Notes in Computer Science No. 33, Springer-Verlag, Berlin, 1975.
11. P. E. STIFFLER, JR., Extensions of the fundamental theorem of finite semigroups, *Advances in Math.* **11** (1973), 159–209.
12. Y. ZALCSTEIN, Remarks on automata and semigroups, unpublished, 1971.