Printing Requisition/Graphic Services

Dept. No. 88954

Title or Description
CS 79-18

Date 4 July/80 **Date Required** ASAP **Account** 126-6240-41

Signature **Signing Authority**

Department Computer Science **Room** 5179 **Phone** 3143

Delivery □ Mail ☒ Pick-up □ Via Stores □ Other

1. Please complete unshaded areas on form as applicable. (4 part no carbon required).
2. Distribute copies as follows: White, Canary and Pink—Printing, Arts Library or applicable Copy Centre Goldenrod—**Retain.**
3. On completion of order, pink copy will be returned with printed material. Canary copy will be costed and returned to requisitioner, **Retain as a record of your charges.**
4. Please direct enquiries, quoting requisition number, to Printing/Graphic Services, Extension 3451.

Reproduction Requirements □ Offset □ Signs/Repro's □ Xerox

Number of Pages 105 **Number of Copies** 20

Type of Paper Stock □ Bond □ Book □ Cover □ Bristol □ Supplied

Paper Size □ 8½ x 11 □ 8½ x 14 □ 11 x 17

Paper Colour □ White □ Other **Ink** □ Black

Printing □ 1 Side □ 2 Sides **Numbering** to

Binding/Finishing Operations □ Collating □ Corner Stitching □ 3 Ring □ Tape □ Plastic Ring □ Perforating

Folding Finished Size **Cutting** Finished Size

Special Instructions
Unstaple them, and attach■ the tech. report listing to the end of the report, and then again put on new fronts and backs.

Film Qty Size **Plates** Qty Size & Type

Paper Qty Size **Plastic Rings** Qty Size

Outside Services

Cost: Time/Materials	Fun.	Prod.Un.	Prod. Cl.	Opr. No.	Mins.	Total
Signs/Repro's	1					
Camera	2					
Correcting & Masking Negatives	3					
Platemaking	4					
Printing	5					
Bindery	6		21 93	- 45 5		
Sub. Total Time						
Sub. Total Materials						
Prov. Tax						
Total						

224

PrintingRequisition/GraphicServices

Dept. No. 46072

1. Please complete unshaded areas on form as applicable. (4 part no carbon required).
2. Distribute copies as follows: White, Canary and Pink—Printing, Arts Library or applicable Copy Centre Goldenrod—**Retain.**
3. On completion of order, pink copy will be returned with printed material. Canary copy will be costed and returned to requisitioner, **Retain as a record of your charges.**
4. Please direct enquiries, quoting requisition number, to Printing/Graphic Services, Extension 3451.

Title or Description CS-79-18

Date May 9/79 **Date Required** **Account** 126-6240-41

Signature **Signing Authority**

Department Comp. Sci. **Room** 5100 **Phone** 3293

Delivery
□ Mail □ Via Stores
□ Pick-up □ Other

Reproduction Requirements
☑ Offset □ Signs/Repro's □ Xerox

Number of Pages 98 **Number of Copies** 50

Type of Paper Stock
☑ Bond □ Book □ Cover □ Bristol □ Supplied

Paper Size
☑ 8½ x 11 □ 8½ x 14 □ 11 x 17

Paper Colour
☑ White □ Other

Ink
☑ Black

Printing
☑ 1 Side □ 2 Sides

Numbering to

Binding/Finishing Operations
☑ Collating □ Corner Stitching □ 3 Ring □ Tape □ Plastic Ring □ Perforating

Folding
Finished Size

Cutting
Finished Size

Special Instructions
COVERS ATTACHED
ALL [illegible] 1 SIDE

Cost: Time/Materials	Fun.	Prod.Un.	Prod. Cl.	Opr. No.	Mins.	Total	
Signs/Repro's	1						
Camera	2						
Correcting & Masking Negatives	3						
Platemaking	4						
Printing	5	1	35		90		
			4-30				
Bindery	6						
J.B.							
Sub. Total Time							
Sub. Total Materials							
Prov. Tax							
Total							

Film Qty	Size	**Plates** Qty	Size & Type
Paper Qty	Size	**Plastic Rings** Qty	Size
Outside Services			

LANGUAGES OF R-TRIVIAL AND RELATED MONOIDS

by

Faith Ellen Fich

Computer Science Dept.
University of Waterloo
Waterloo, Ontario, Canada

Research Report CS-79-18

May 1979

Abstract

The family of languages, whose syntactic monoids are *R*-trivial, is considered. Languages whose syntactic monoids are *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*. It is shown that in the *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 automata and regular expressions are presented. Dual results for *L*-trivial monoids are also discussed.

The family of *G*-trivial monoids, a generalization which includes both *R*-trivial and *L*-trivial monoids, is investigated. Similar characterizations, in terms of congruences, automata and regular expressions are provided.

Finally, the relationship between the above families and some other well-known families of languages are considered.

Acknowledgements

I would like to thank my supervisor, John Brzozowski, who first introduced me to the beauty of star-free languages, guided me, and provided constant encouragement. I also appreciate the helpful comments of Karel Culik and Stanley Burris.

For the arduous task of transforming my handwritten rough draft into computer files ready for the phototypesetter, I had the willing aid of Randy Morrison, Ross Brown, and my husband, Michel. Kimberly King, who didn't want to be mentioned, was invaluable as a proofreader.

The National Science and Engineering Research Council of Canada supported this research through a Postgraduate Scholarship.

Table of Contents

CHAPTER 1 INTRODUCTION

1.1 Preliminaries

Let A be a finite non-empty alphabet, A^+ the free semigroup generated by A, and A^* the free monoid generated by A, with unit element 1 (the empty word). The cardinality of A is denoted by #A and 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 $\alpha(x) = \{a \in A \mid x = uav \text{ for some } u,v \in A^*\}$.

A word u is a prefix of $x \in A^*$ if and only if $x = uv$ for some $v \in A^*$. Similarly v is a suffix of x if and only if there exists $u \in A^*$ such that $x = uv$. The front of length n of x is defined to be

$$f_n(x) = \begin{cases} x & \text{if } |x| \leqslant n \\ u & \text{if } |x| > n \text{ and } u \text{ is the prefix of length } n \text{ of } x. \end{cases}$$

The tail of length n of x, $t_n(x)$, is defined analogously. The reverse x^ρ of a word x is defined by induction on $|x|$: $1^\rho = 1$ and $(xa)^\rho = ax^\rho$.

Subsets of A^* are called languages. If $X, Y \subseteq A^*$ then $\overline{X} = A^* - X$, $X \cup Y$, and $X \cap Y$ denote the complement of X, the union of X and Y, and the 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 F of languages $F\mathbf{B}$ is the smallest family containing F and closed under complementation and finite unions. Similarly $F\mathbf{M}$ is the smallest family containing $F \cup \{\{1\}\}$ and closed under concatenation. Thus $F\mathbf{B}$ and $F\mathbf{M}$ are the Boolean algebra and monoid generated by F, respectively.

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

$$x \equiv_X y \text{ if and only if } (uxv \in X \text{ if and only if } uyv \in X).$$

The quotient monoid $M = A^*/\equiv_X$ is the syntactic monoid of X, and the syntactic morphism of X is the natural morphism mapping $x \in A^*$ onto the equivalence class of $\equiv_X$ containing x. For convenience, $\underline{x}$ is used to represent the equivalence class of $\equiv_X$ containing x.

If $\sim$ is any congruence on A^* then X is defined to be a $\sim$ language if and only if X is a union of congruence classes of $\sim$. Thus X is a $\sim$ language if and only if for all $x, y \in A^*$

$$x \sim y \text{ implies } (x \in X \text{ if and only if } y \in X).$$

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

$$x \sim y \;\; \text{implies} \;\; x \equiv_X y, \;\; (\text{i.e. } \underline{x} = \underline{y}).$$

The congruence class of $\sim$ containing x is denoted by $[x]_\sim$.

A semiautomaton is a triple $S = <A, Q, \sigma>$, where A is the input alphabet, Q is a finite set of states, and $\sigma: Q \times A \rightarrow Q$ is the transition function. A (finite) automaton is a system $\mathbf{A} = <A, Q, q_0, F, \sigma>$ 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. The domain of σ is extended to $Q \times A^*$ in the natural way. That is, $\sigma(q, 1) = q$ and $\sigma(q,ax) = \sigma(\sigma(q,a),x)$ for all $q \in Q$, $x \in A^*$, and $a \in A$. The language accepted or recognized by an automaton is $\{x \in A^* \mid \sigma(q_0,x) \in F\}$. An automaton is reduced if and only if for all distinct $p,q \in Q$ there exists $x \in A^*$ such that $\sigma(p,x) \in F$ and $\sigma(q,x) \notin F$ or vice versa.

In any semiautomaton define the relation $\rightarrow$ as follows. For $p,q \in Q$

$$p \rightarrow q \;\; \text{if and only if} \;\; \sigma(p,x) = q \;\; \text{for some } x \in A^*.$$

S (or A) is partially ordered if and only if the relation $\rightarrow$ on Q is a partial order. A semiautomaton is a chain reset if and only if $\rightarrow$ is a total order.

The direct product of two semiautomata $S = <A, Q, \sigma>$ and $T = <A, P, \tau>$ is the semiautomaton $S \times T = <A, Q \times P, \eta>$, where $\eta((q,p),a) = (\sigma(q,a), \tau(p,a))$. The cascade product of $S = <A, Q, \sigma>$ and $T = <C, P, \tau>$ with connection $\omega : Q \times A \rightarrow C$ is the semiautomaton $S \circ T = <A, Q \times P, \eta>$ where $\eta((q,p),a) = (\sigma(q,a), \tau(p, \omega(q,a)))$. If $A = C$ and $\omega(q,a) = a$ for all $a \in A$ then $S \circ T$ reduces to $S \times T$.

An initialized semiautomaton is a semiautomaton with an initial state. Let $S = <A, Q, \sigma>$ and $T = <C, P, \tau>$ be two semiautomata. T is a subsemiautomaton of S if and only if $C \subseteq A$, $P \subseteq Q$, and τ is the restriction of σ to $P \times C$. If S and T are initialized semiautomata with initial states q_0 and p_0 respectively, then T is an initialized subsemiautomaton of S if it is a subsemiautomaton of S and $q_0 = p_0$. The initialized semiautomaton S is a homomorphic image of the initialized semiautomaton T if and only if $C = A$ and there exists a surjective mapping $\psi : P \rightarrow Q$ such that $\psi(p_0) = q_0$ and $\psi(\tau(p,a)) = \sigma(\psi(p),a)$. S is covered by T if and only if S is a homomorphic image of an initialized subsemiautomaton of T.

An initialized semiautomaton $S = <A, Q, q_0, \sigma>$ is connected if and only if for each $q \in Q$ there exists $x \in A^*$ such that $\sigma(q_0,x) = q$. The connected initialized subsemiautomaton of S is $<A, Q', q_0, \sigma'>$ where $Q' = \{q \in Q \mid \text{there exists } x \in A^* \text{ such that } \sigma(q_0,x) = q\}$ and σ' is the restriction of σ to $Q' \times A$.

The transformation monoid of a semiautomaton $S = <A, Q, \sigma>$ (or of an automaton $<A, Q, q_0, F, \sigma>$) is the set of all transformations of Q into itself of the form $(q_1, \ldots, q_n) \rightarrow (\sigma(q_1,x), \ldots, \sigma(q_n,x))$ for some $x \in A^*$. It is well-known that if A is a reduced automaton recognizing the language $X \subseteq A^*$, then the transformation monoid of A is isomorphic to the syntactic monoid of X.

Let M be any monoid. The cardinality of M is denoted by #M. An element $e \in M$ is said to be idempotent if $e = e^2$. M is idempotent if and only if e is idempotent for all $e \in M$. For $f \in M$ let $P_f = \{g \in M \mid f \in MgM\}$ and $M_f = P_f^*$. Then M_f is the submonoid of M generated by the elements g with which f can be written $(f \in MgM)$.

1.2 Background

The family of regular languages over an alphabet A is the set of all languages $X \subseteq A^*$ which can be built up from the languages $\{\{a\} \mid a \in A\}$ using Boolean operations, concatenation and the star operator. In 1956, Kleene [18] proved that the languages recognized by automata are regular and that any regular language is recognized by some automaton. A theorem due to Myhill [25] states that a language $X \subseteq A^*$ is regular if and only if it is a $\sim$ language for some congruence $\sim$ over A^* of finite index if and only if its syntactic monoid is finite.

The family of star-free languages over A is the set of all languages $X \subseteq A^*$ which can be built up from the languages $\{\{a\} \mid a \in A\}$ using only Boolean operations and concatenation. There are many different characterizations of star-free languages. A language X is star-free if and only if its syntactic monoid M is finite and group-free (i.e. every subgroup of M contains only one element), or, alternatively, if and only if M is finite and aperiodic (i.e. there exists $n \geqslant 1$ such that $f^n = f^{n+1}$ for all $f \in M$). It is necessary and sufficient for the reduced automaton $A = <A, Q, q_0, F, \sigma>$ accepting X to be permutation-free (i.e. for all $P \subseteq Q$, $x \in A^*$, $\{\sigma(p,x) \mid p \in P\} = P$ implies $\sigma(p,x) = p$ for all $p \in P$). A reset is an initialized semiautomaton $<C, \{p_0,p_1\}, p_0, \tau>$ such that for each $c \in C$ either $\tau(p_0,c) = \tau(p_1,c)$ or $\tau(p_0,c) = p_0$ and $\tau(p_1,c) = p_1$. X is star-free if and only if A can be covered by a cascade product of resets. The proofs of these and other characterizations can be found in [1], [11], [14], [19], [20], [21], [26], and [27].

Various subfamilies of the star-free languages have also proved interesting. Consider the families $B_0 \subseteq B_1 \subseteq B_2 \subseteq \cdots$ where $B_0 = \{\{a\} \mid a \in A\}\mathbf{MB}$ and $B_{i+1} = B_i\mathbf{MB}$ for all $i \geqslant 0$. Clearly $\bigcup_{i=0}^{\infty} B_i$ is equal to the family of all star-free languages over the alphabet A. This sequence of Boolean algebras is known as the dot-depth hierarchy and was introduced and first studied by Cohen and Brzozowski [11]. It is easily seen that B_0 is equal to the set of finite and cofinite languages over A. If #A = 1 then B_0 is also a monoid and thus is equal to the family of star-free languages over A. However, for #A > 1, the dot-depth hierarchy is infinite [7]. In [4], an excellent survey of this material can be found.

The well-known Green relations are fundamental in the theory of monoids [9,15]. They are defined as follows. Let M be a monoid and $f,g \in$ M; then

$$\begin{array}{rlc} fJg & \text{if and only if} & \mathrm{M}f\mathrm{M} = \mathrm{M}g\mathrm{M} \\ fLg & \text{if and only if} & \mathrm{M}f = \mathrm{M}g \\ fRg & \text{if and only if} & f\mathrm{M} = g\mathrm{M} \\ fHg & \text{if and only if} & fLg \text{ and } fRg \end{array}$$

Clearly J, L, R, and H are equivalence relations. If ρ is an equivalence relation on M, we say that M is ρ-trivial if and only if $f \rho g$ implies $f=g$. In 1965, Schützenberger [26] showed that a language is star-free if and only if its syntactic monoid is finite and H-trivial. In 1972, Simon [28,29] characterized the languages corresponding to finite J-trivial monoids. This latter family of languages plays a key role in the structure of B_1. J-trivial and H-trivial monoids and the dot-depth hierarchy are also treated in [12].

Here, the languages corresponding to finite R-trivial and L-trivial monoids are studied, as well as the set of languages of G-trivial monoids, which is a generalization of both of these. Characterizations are given in terms of congruences, monoids, automata, and regular expressions. The relationship of these families to the dot-depth hierarchy is also considered.

CHAPTER 2 LANGUAGES OF *R*-TRIVIAL MONOIDS

2.1 Languages of *J*-Trivial Monoids

Simon, in [28] and [29], provides many characterizations for languages with *J*-trivial syntactic monoids as is summarized in the following theorem. An additional property, M3, is taken from [5].

Theorem 1 Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $\mathbf{A} = <A, Q, q_0, F, \sigma>$ and $\mathbf{A}^\rho$ be the reduced finite automata accepting X and X^ρ, respectively. The following conditions are equivalent.

M1. M is *J*-trivial.

M2. M is *R*-trivial and *L*-trivial.

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

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

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

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

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

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

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

A3. $\mathbf{A}$ can be covered by a direct product of chain resets.

The congruence $\underset{n}{\sim}$, 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 2 Let $x,y \in A^*$ and $n \geqslant 0$. Then

(a) x is a *subword* of y if and only if 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 $\{x \mid x$ is a subword of y and $|x| \leqslant n\}$

(c) $x \underset{n}{\sim} y$ if and only if $\mu_n(x) = \mu_n(y)$.

It is straightforward to show that $\underset{n}{\sim}$ is a congruence of finite index for any $n \geqslant 0$. See [28, pages 67-68]. There Simon also proves three results which are needed for the next section.

Proposition 3 Let $x,y \in A^*$ and $n \geqslant 0$. Then

(a) $x^n \underset{n}{\sim} x^{n+1}$,

(b) $(xy)^n \underset{n}{\sim} (xy)^n x$, and

(c) $(xy)^n \underset{n}{\sim} y(xy)^n$.

Proposition 4 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n+1}{\sim} y$ implies $x \underset{n}{\sim} y$.

Lemma 5 Let $u,v \in A^*$ and $n > 0$. Then $u \underset{n}{\sim} uv$ if and only if 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 6 Let $x \in A^*$ and $n > 0$. Then x is *n-full* if and only if $\mu_n(x) = \bigcup_{i=0}^{n} (\alpha(x))^i$. That is, x contains as a subword every word over the alphabet $\alpha(x)$ of length at most n.

Clearly, x is n-full if and only if $x \underset{n}{\sim} xy$ for all $y \in (\alpha(x))^*$ which, by Lemma 5, is true if and only if there exist $x_1, \ldots, x_n \in A^*$ such that $x = x_1 \cdots x_n$ and $\alpha(x_1) = \cdots = \alpha(x_n) = \alpha(x)$. Every word is 1-full and any $(n+1)$-full word is also n-full.

2.2 The $\underset{n\,R}{\sim}$ Congruence

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

Definition 7 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n\,R}{\sim} y$ if and only if

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

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

Note that if $|x| < n$, $x \underset{n\,R}{\sim} y$ if and only if $x = y$.

The two equivalence relations $\underset{n}{\sim}$ and $\underset{n\,R}{\sim}$ are closely related and satisfy many similar properties.

Proposition 8 Let $x,y \in A^*$ and $n \geqslant 0$.

(a) If $x \underset{n\,R}{\sim} y$ then $x \underset{n}{\sim} y$.

(b) $x \underset{n}{\sim} xy$ if and only if $x \underset{n\,R}{\sim} xy$.

(c) If $xy \underset{n\,R}{\sim} x'y'$ and $x \underset{n}{\sim} x'$, then $x \underset{n\,R}{\sim} x'$.

Proof:

(a) Since x is a prefix of x there exists a prefix v of y such that $x \underset{n}{\sim} v$. 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 $x \underset{n}{\sim} y$.

(b) Assume $x \underset{n}{\sim} xy$. 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 $x \underset{n}{\sim} v$. Therefore $x \underset{n\,R}{\sim} xy$. The converse follows from (a).

(c) Let u be a prefix of x. Since u is also a prefix of xy there exists a prefix u' of $x'y'$ such that $u \underset{n}{\sim} u'$. Now either u' is a prefix of x' or x' is a prefix of u'. In the second case $\mu_n(x') \subseteq \mu_n(u') = \mu_n(u) \subseteq \mu_n(x) = \mu_n(x')$, so that $u \underset{n}{\sim} x'$. Similarly, for each prefix u'

of x', there exists a prefix u of x such that $u \underset{n}{\sim} u'$. Therefore $x \underset{n}{\sim}_R x'$.

Proposition 9 Let $x,y \in A^*$ and $n \geqslant 0$. Then

(a) $x^n \underset{n}{\sim}_R x^{n+1}$

(b) $(xy)^n \underset{n}{\sim}_R (xy)^n x$.

Proof: Immediate from Propositions 3(a) and (b) and 8(b).

Proposition 10 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n+1}{\sim}_R y$ implies $x \underset{n}{\sim}_R y$.

Proof: Follows from Proposition 4.

Lemma 11 Let $u,v \in A^*$ and $n > 0$. Then $u \underset{n}{\sim}_R uv$ if and only if there exist $u_1, u_2, \ldots, u_n \in A^*$ 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 5 and Proposition 8.

In the remaining part of this section some additional interesting properties of $\underset{n}{\sim}_R$ are presented.

Lemma 12 Let $n > 0$, $x,y,x',y' \in A^*$, and $a \in A$. If $xay \underset{n}{\sim}_R x'ay'$ and $a \notin \alpha(y) \cup \alpha(y')$ then $x \underset{n-1}{\sim}_R x'$.

Proof: Let $u \in \mu_{n-1}(x)$. Then $ua \in \mu_n(xa) \subseteq \mu_n(xay) = \mu_n(x'ay')$. Since $a \notin \alpha(y')$, $ua \in \mu_n(x'a)$. Now $u \in \mu_{n-1}(x')$; hence $\mu_{n-1}(x) \subseteq \mu_{n-1}(x')$. Similarly $\mu_{n-1}(x') \subseteq \mu_{n-1}(x)$. Therefore $x \underset{n-1}{\sim} x'$ and, by Proposition 8(c), $x \underset{n-1}{\sim}_R x'$.

Lemma 13 Let $n > 0$, $x \in A^*$, and $a \in A$. Then $x \underset{n}{\sim}_R xa$ if and only if there exists a prefix ua of x such that $u \underset{n-1}{\sim} x$.

Proof:

($\Rightarrow$) Suppose $x \underset{n}{\sim}_R xa$. Since $n > 0$, $\alpha(x) = \alpha(xa)$ and thus $a \in \alpha(x)$. Let $x = uav$ where

$a \notin \alpha(v)$. Then $uav = x \underset{n}{\sim}_R xa = (uav)a1$ so, by Lemma 12, $u \underset{n-1}{\sim}_R uav = x$. Hence $u \underset{n-1}{\sim} x$ by Proposition 8(a).

($\Leftarrow$) If $w \in \mu_n(xa)$ then either $w \in \mu_n(x)$ or $w = va$ where $v \in \mu_{n-1}(x) = \mu_{n-1}(u)$. Thus $w = va \in \mu_n(ua) \subseteq \mu_n(x)$. Hence $\mu_n(xa) \subseteq \mu_n(x)$. But $\mu_n(x) \subseteq \mu_n(xa)$; therefore $x \underset{n}{\sim} xa$. From Proposition 8(b) it follows that $x \underset{n}{\sim}_R xa$.

Lemma 14 Let $n \geqslant 0$, $x \in A^*$, and $a,b \in A$. If $x \underset{n}{\sim}_R xa$ and $xb \underset{n}{\sim}_R xbb$ then $xb \underset{n}{\sim}_R xba$.

Proof: If $n = 0$ then the result is trivially true since $y \underset{0}{\sim}_R z$ for all $y,z \in A^*$. Therefore assume $n > 0$. By Lemma 13 there exist $u,v \in A^*$ such that ua is a prefix of x, vb is a prefix of xb, $u \underset{n-1}{\sim} x$, and $v \underset{n-1}{\sim} xb$. But vb is a prefix of xb, so v is a prefix of x; hence $\mu_{n-1}(v) \subseteq \mu_{n-1}(x) \subseteq \mu_{n-1}(xb) = \mu_{n-1}(v)$. Thus $xb \underset{n-1}{\sim} x \underset{n-1}{\sim} u$ and, since ua is a prefix of xb, it follows by Lemma 13 that $xb \underset{n}{\sim}_R xba$.

Lemma 15 Let $u,v,v' \in A^*$ and $a,b \in A$. If $a \neq b$ and $uav \underset{n}{\sim}_R ubv'$ then either $u \underset{n}{\sim} ua$ or $u \underset{n}{\sim} ub$.

Proof: Suppose $a \neq b$ and $uav \underset{n}{\sim}_R ubv'$. Then there exists a prefix u' of ubv' such that $u' \underset{n}{\sim} ua$. If u' is a prefix of u then $\mu_n(u') \subseteq \mu_n(u) \subseteq \mu_n(ua) = \mu_n(u')$ so $u \underset{n}{\sim} ua$.

Otherwise ub is a prefix of u' so that $\mu_n(ub) \subseteq \mu_n(u') = \mu_n(ua)$. If $z \in \mu_n(ub)$ then either $z \in \mu_n(u)$ or $z = z'b$ where $z' \in \mu_{n-1}(u)$. But $z = z'b \in \mu_n(ua)$ and $a \neq b$ imply $z \in \mu_n(u)$. Thus $\mu_n(ub) \subseteq \mu_n(u)$ and, since $\mu_n(u) \subseteq \mu_n(ub)$, $u \underset{n}{\sim} ub$.

Lemma 16 Let $u,v \in A^*$, $a,b \in A$, and $n > i > 0$. If $\mu_{n-i}(u) \neq \mu_{n-i}(ua)$ and $\mu_i(v) \neq \mu_i(vb)$ then $\mu_n(uav) \neq \mu_n(uavb)$.

Proof: Suppose $\mu_{n-i}(u) \neq \mu_{n-i}(ua)$ and $\mu_i(v) \neq \mu_i(vb)$. Then there exist $u',v' \in A^*$ such that $u'a \in \mu_{n-i}(ua) - \mu_{n-i}(u)$ and $v'b \in \mu_i(vb) - \mu_i(v)$. Clearly $u'av'b \in \mu_n(uavb)$.

If $u'av'b \in \mu_n(uav)$ then there exist $r,s \in A^*$ such that $uav = rs$, $u'a$ is a subword of r, and $v'b$ is a subword of s. Since $u'a \in \mu_{n-i}(ua) - \mu_{n-i}(u)$, it follows that ua is a prefix of r. Hence s is a suffix of v. But if $v'b$ is a subword of s, then $v'b$ is a subword of v, contradicting the fact that $v'b \in \mu_i(vb) - \mu_i(v)$. Therefore $u'av'b \in \mu_n(uavb) - \mu_n(uav)$ and thus $\mu_n(uav) \neq \mu_n(uavb)$.

Proposition 17 $\underset{n\,R}{\sim}$ 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 $x \underset{n\,R}{\sim} y$. 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 $x \underset{n\,R}{\sim} y$, there is a prefix v of y such that $u \underset{n}{\sim} v$. If $u = xa$ then from Proposition 8(a) $x \underset{n}{\sim} y$, and since $\underset{n}{\sim}$ is a congruence $u = xa \underset{n}{\sim} ya$. By symmetry, for each prefix v of ya there exists a prefix u of xa such that $u \underset{n}{\sim} v$. Therefore $\underset{n\,R}{\sim}$ 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 $x \underset{n\,R}{\sim} y$, there exists a prefix v' of y such that $u' \underset{n}{\sim} v'$. But $\underset{n}{\sim}$ is a congruence so $u = au' \underset{n}{\sim} av'$. Similarily for each prefix v of ay there exists a prefix u of ax such that $u \underset{n}{\sim} v$. Hence $\underset{n\,R}{\sim}$ is a left congruence.

The fact that $\underset{n\,R}{\sim}$ is of finite index can be obtained from a counting argument using the fact that $\underset{n}{\sim}$ is of finite index.

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

Theorem 18 Every congruence class of $\underset{n\,R}{\sim}$ contains a unique element of minimal length. Furthermore, if $a_1, \ldots, a_m \in A$ then $a_1 \cdots a_m$ is minimal if and only if $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \mu_n(a_1a_2) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m)$.

Proof: By induction on k, the minimum length of elements in a given $\underset{n\,R}{\sim}$ 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 $\underset{n\,R}{\sim}$ classes containing elements of length less than k. Suppose there exists a $\underset{nR}{\sim}$ 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 $u \underset{n}{\sim} x$ implies $u \underset{nR}{\sim} x$ by Proposition 8(b); so $\mu_n(u) \neq \mu_n(x)$. Employing the induction hypothesis (since $|u| < k$) $[u]_{\underset{nR}{\sim}}$ has a unique element of minimal length. Call this element w. If $w \neq u$ then $|w| < |u|$ and hence $|wa| < |x|$. But $w \underset{nR}{\sim} u$ and $\underset{nR}{\sim}$ is a congruence, so $wa \underset{nR}{\sim} ua = x$ 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 $x \underset{nR}{\sim} y$ there exists a prefix v of y such that $u \underset{n}{\sim} v$. By Proposition 8(c) $u \underset{nR}{\sim} v$. Also, v is a proper prefix of y since $\mu_n(v) = \mu_n(u) \subsetneq \mu_n(x) = \mu_n(y)$. Then $v = u$, since otherwise $|y| \geqslant 1 + |v| > 1 + |u| = |x|$ contradicting the minimality of y. 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, every congruence class of $\underset{nR}{\sim}$ 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 $[x]_{\underset{nR}{\sim}}$. Since $x \underset{nR}{\sim} y$ there exist prefixes $v_0, v_1, \ldots, v_m$ of y such that $u_i \underset{n}{\sim} v_i$ 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 19 Let $n \geqslant 0$. Then

(a) the function $\chi_n : A^* \to A^*$ is defined by $\chi_n(x) =$ the unique minimal element of $[x]_{\underset{nR}{\sim}}$,

(b) the length of the longest minimal element is $\lambda_R(A, n) = \max\{|\chi_n(x)| \mid x \in A^*\}$, and

(c) the set of all longest words which are the minimal elements in their $\underset{nR}{\sim}$ classes is

$\Lambda_R(\mathrm{A}, n) = \{\chi_n(x) \mid x \in \mathrm{A}^* \text{ and } |\chi_n(x)| = \lambda_R(\mathrm{A}, n)\}.$

Proposition 20 Let $n \geqslant 0$. Then $\lambda_R(\mathrm{A}, n) = \binom{n+\#\mathrm{A}}{n} - 1$. Furthermore, for $\#\mathrm{A} > 1$ and $n > 0$, $x \in \Lambda_R(\mathrm{A}, n)$ if and only if $x = x_n a_n \cdots x_2 a_2 x_1 a_1$ where $a_i \in \mathrm{A}$ and $x_i \in \Lambda_R(\mathrm{A}-\{a_i\}, i)$ for $i = 1, \ldots, n$.

Proof: By induction on $\#\mathrm{A}$.

If $\#\mathrm{A} = 1$, say $\mathrm{A} = \{a\}$, then the result is clearly true since $\Lambda_R(\mathrm{A}, n) = \{a^n\}$ and $\lambda_R(\mathrm{A}, n) = n = \binom{n+1}{n} - 1$. Now assume the proposition is true for all alphabets with cardinality $\#\mathrm{A} - 1$, where $\#\mathrm{A} > 1$.

Because 1 is the only word of length 0 and $x \sim_{0R} y$ for all $x,y \in \mathrm{A}^*$, $\Lambda_R(\mathrm{A}, 0) = \{1\}$ and $\lambda_R(\mathrm{A}, 0) = 0 = \binom{0+\#\mathrm{A}}{0} - 1$. It remains to consider the case $n > 0$.

Let $x = x_n a_n \cdots x_1 a_1$ where $a_i \in \mathrm{A}$ and $x_i \in \Lambda_R(\mathrm{A}-\{a_i\}, i)$ for $i = 1, \ldots, n$. Clearly $a_n \cdots a_i \in \mu_{n-i+1}(x_n a_n \cdots x_i a_i)$ for $i = 1, \ldots, n$. However, since $x_n \in (\mathrm{A}-\{a_n\})^*$, $a_n \notin \mu_1(x_n)$. Assume $a_n \cdots a_{i+1} \notin \mu_{n-i}(x_n a_n \cdots x_{i+1})$ where $1 \leqslant i \leqslant n-1$. Then, because $x_i \in (\mathrm{A}-\{a_i\})^*$, $a_n \cdots a_{i+1} a_i \notin \mu_{n-i+1}(x_n a_n \cdots x_{i+1} a_{i+1} x_i)$. By induction it follows that $a_n \cdots a_i \in \mu_{n-i+1}(x_n a_n \cdots x_i a_i) - \mu_{n-i+1}(x_n a_n \cdots x_i)$ and hence $\mu_{n-i+1}(x_n a_n \cdots x_i) \neq \mu_{n-i+1}(x_n a_n \cdots x_i a_i)$.

Consider any prefix ua of x where $u \in \mathrm{A}^*$ and $a \in \mathrm{A}$. If $u = x_n a_n \cdots x_i$ and $a = a_i$ for some i, $1 \leqslant i \leqslant n$, then, from above and Proposition 4, $\mu_n(ua) \neq \mu_n(u)$. Otherwise $u = x_n a_n \cdots x_{i+1} a_{i+1} v$ where $v \in \mathrm{A}^*$, va is a prefix of x_i, and $1 \leqslant i \leqslant n$. Since $x_i \in \Lambda_R(\mathrm{A}-\{a_i\}, i)$, it is the minimal element of its $\sim_{iR}$ class; so $\mu_i(v) \subsetneq \mu_i(va)$ by Theorem 18. For $i < n$, it follows from the preceding paragraph and Lemma 16 that $\mu_n(u) \neq \mu_n(ua)$. And when $i = n$, $u = v$. Thus $\mu_n(u) \neq \mu_n(ua)$ for any prefix ua of x. Theorem 18 implies that x is the minimal element of its $\sim_{nR}$ class.

Now let $y \in \Lambda_R(\mathrm{A}, n)$. Then $y = \chi_n(y)$ is n-full and $\alpha(y) = \mathrm{A}$. Otherwise there exists $a \in \mathrm{A}$ such that $\mu_n(y) \neq \mu_n(ya)$. Since y is the minimal element of $[y]_{\sim_{nR}}$, it follows from

Theorem 18 that ya is the minimal element of $[ya]_{\sim_{nR}}$. This contradicts the fact that $y \in \Lambda_R(\mathrm{A},\, n)$.

Decompose y into $y_n a_n \cdots y_1 a_1 y_0$ where $y_0 \in \mathrm{A}^*$ and $\alpha(y_i) \neq \alpha(y_i a_i) = \mathrm{A}$ for $i = 1, \ldots, n$. Since $y_n a_n \cdots y_1 a_1$ is n-full, $y_n a_n \cdots y_1 a_1 \sim_{nR} y_n a_n \cdots y_1 a_1 y_0$ and therefore $y_0 = 1$.

Suppose for some i, $1 \leqslant i \leqslant n$, that $y_i \neq \chi_i(y_i)$. Then, by Theorem 18, there exist $a \in \mathrm{A} - \{a_i\}$ and $u, v \in \mathrm{A}^*$ such that $y_i = uav$ and $u \sim_{iR} ua$. Let $w \in \mu_n(y_n a_n \cdots y_{i+1} a_{i+1} ua)$. Now $w = w'w''$ where w' is a subword of $y_n a_n \cdots y_{i+1} a_{i+1}$ and w'' is a subword of ua. If $|w''| \leqslant i$ then $w'' \in \mu_i(ua) = \mu_i(u)$ so that $w \in \mu_n(y_n a_n \cdots y_{i+1} a_{i+1} u)$. Otherwise let $w_1, w_2 \in \mathrm{A}^*$ be such that $w_2 = t_i(w'')$ and $w = w_1 w_2$. Since $y_n a_n \cdots y_{i+1} a_{i+1}$ is $(n-i)$-full and $|w_1| = |w| - |w_2| \leqslant n-i$, w_1 is a subword of $y_n a_n \cdots y_{i+1} a_{i+1}$. But w_2 is a suffix of w'' so w_2 is a subword of ua. As above, $w_2 \in \mu_i(u)$, and thus $w = w_1 w_2 \in \mu_n(y_n a_n \cdots y_{i+1} a_{i+1} u)$. Therefore it follows that $\mu_n(y_n a_n \cdots y_{i+1} a_{i+1} u) = \mu_n(y_n a_n \cdots y_{i+1} a_{i+1} ua)$, which contradicts Theorem 18 since $y = \chi_n(y)$. Hence $x_i = \chi_i(x_i)$ for $i = 1, \ldots, n$.

If $|y_k| < \lambda_R(\mathrm{A} - \{a_k\},\, k)$ for some $1 \leqslant k \leqslant n$ then

$$|y| = \sum_{i=1}^{n} [\,|y_i| + 1\,] < \sum_{i=1}^{n} [\,\lambda_R(\mathrm{A} - \{a_i\},\, i) + 1\,] = \sum_{i=1}^{n} [\,|x_i| + 1\,] = |x|$$

contradicting the fact that $y \in \Lambda_R(\mathrm{A},\, n)$. Therefore $y_i \in \Lambda_R(\mathrm{A} - \{a_i\},\, i)$ for $i = 1, \ldots, n$. This also implies that $\lambda_R(\mathrm{A},\, n) = |x|$. Hence, by the induction hypothesis and [17, page 212],

$$\begin{aligned} \lambda_R(\mathrm{A},\, n) = |x| &= \sum_{i=1}^{n} \lambda_R(\mathrm{A} - \{a_i\},\, i) + 1 \\ &= \sum_{i=1}^{n} \binom{i + \#\mathrm{A} - 1}{i} \\ &= \binom{n + \#A}{n} - 1 \end{aligned}$$

The following is an algorithm for finding the minimal element of a congruence class of $\sim_{nR}$ given any word x in the class. A SNOBOL4 program which implements this algorithm can be found in the Appendix.

Algorithm 21 Determine $\chi_n(x)$ given x.

Find the shortest prefix ua of x such that $u \in A^*$, $a \in A$, and $u \underset{n}{\sim} ua$. 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 $u \underset{n}{\sim} ua$ implies $u \underset{nR}{\sim} ua$ and $\underset{nR}{\sim}$ is a congruence, $uv \underset{nR}{\sim} uav = x$. 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 $\mu_2(abccb) = \mu_2(abccbc)$, $abccb \underset{2R}{\sim} abccbc$ and hence $abccbac \underset{2R}{\sim} abccbcac = x$. 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 $\mu_2(abccba) = \mu_2(abccbac)$, $abccba \underset{2R}{\sim} abccbac$. 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. Thus for a fixed n and a fixed alphabet, $\chi_n(x)$ can be found in $O(|x|)$ steps. By employing the algorithm twice, $O(|x| + |y|)$ steps suffice to determine whether $x \underset{nR}{\sim} y$.

The algorithm motivates the following definition:

Definition 22 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{nR}{\dot{\approx}} y$ if and only if $x = rus$ and $y = ruvs$ for some $r,s,u,v \in A^*$ such that $u \underset{n}{\sim} uv$. Let $\underset{nR}{\approx}$ be the symmetric transitive closure of $\underset{nR}{\dot{\approx}}$.

One verifies that $x \underset{nR}{\dot{\approx}} x$ for all $x \in A^*$ since $1^n = 1 \underset{n}{\sim} 1 = 1^n 1$, $x = x(1^n)1$, and $x = x(1^n 1)1$. Hence $\underset{nR}{\approx}$ is an equivalence relation over A^* It is easy to see that $\underset{nR}{\approx}$ is the smallest congruence satisfying $u \underset{nR}{\approx} uv$ for all $u,v \in A^*$ such that $u \underset{n}{\sim} uv$.

Proposition 23 Let $n \geqslant 0$ and $x,y \in A^*$ Then $x \underset{nR}{\approx} y$ if and only if $x \underset{nR}{\sim} y$.

Proof: If $x \underset{nR}{\dot{\approx}} y$ then $x \underset{nR}{\sim} y$ by Proposition 8(b); thus $x \underset{nR}{\approx} y$ implies $x \underset{nR}{\sim} y$ since $\underset{nR}{\sim}$ is transitive. If $x \underset{nR}{\sim} y$ then by Theorem 18, $\chi_n(x) = \chi_n(y)$. From Algorithm 21 it follows that $x \underset{nR}{\approx} \chi_n(x)$ and $y \underset{nR}{\approx} \chi_n(y)$. Hence $x \underset{nR}{\approx} y$.

2.3 *R*-Trivial Monoids

Four equivalent characterizations of finite *R*-trivial monoids (from [28] and [5]) are presented. These monoids are then related to the congruences $\underset{n}{\sim}$, $\underset{nR}{\sim}$, and $\underset{nR}{\approxeq}$.

Theorem 24 Let M be a finite monoid. The following conditions are equivalent.

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

Proof:

(1⇒2) Let $f,g,h \in \mathrm{M}$ be such that $fgh = f$. Then $f\mathrm{M} \supseteq fg\mathrm{M} \supseteq fgh\mathrm{M} = f\mathrm{M}$. Since M is *R*-trivial, $f = fg$.

(2⇒3) Let $e \in \mathrm{M}$ be an idempotent and let $f \in \mathrm{P}_e$. Then $e \in \mathrm{M}f\mathrm{M}$ so there exist $g,h \in \mathrm{M}$ such that $e = gfh$. Since $e = e^2 = e(gfh) = eg(fh) = e(gf)h$, $e = eg$ and $e = e(gf) = (eg)f = ef$. Thus $e\mathrm{P}_e = e$ and hence $e\mathrm{M}_e = e(\mathrm{P}_e^*) = e$.

(3⇒4) Since M is finite there exists an $n > 0$ such f^n is idempotent for all $f \in \mathrm{M}$. Now let $f,g \in \mathrm{M}$. Because $e = (fg)^n \in \mathrm{M}f\mathrm{M}$ is idempotent, $f \in \mathrm{P}_e \subseteq \mathrm{M}_e$. Hence $(fg)^n f = (fg)^n$.

(4⇒1) Let $n > 0$ be such that $(hk)^n = (hk)^n h$ for all $h,k \in \mathrm{M}$. Suppose $f\mathrm{M} = g\mathrm{M}$. Then there exist $h,k \in \mathrm{M}$ such that $f = gk$ and $g = fh$. Thus $f = gk = fhk = f(hk)^m$ for all $m \geqslant 0$ and hence $f = f(hk)^n = f(hk)^n h = fh = g$.

Lemma 25 Suppose M is a finite *R*-trivial monoid and $\phi : \mathrm{A}^* \to \mathrm{M}$ is a surjective morphism. Let $n = \#\mathrm{M}$ and let $u,v \in \mathrm{A}^*$. Then $u \underset{n}{\sim} uv$ implies $\phi(u) = \phi(uv)$.

Proof: Suppose $u \underset{n}{\sim} uv$. By Lemma 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 $\phi(u_0)$, $\phi(u_0u_1)$ $, \ldots,$ $\phi(u_0u_1, \ldots, u_n)$ cannot all be distinct. Hence there exist i and j, $0 \leqslant i < j \leqslant n$, such that $f = \phi(u_0 \cdots u_i) = \phi(u_0 \cdots u_i \cdots u_j) = f\phi(u_{i+1} \cdots u_j) = f\phi(u_{i+1})\phi(u_{i+2} \cdots u_j)$. Since M is R-trivial, $f = f\phi(u_{i+1})$. If $\alpha(u_n) = \varnothing$ then $v = 1$ and there is nothing to prove. Thus suppose $\alpha(u_n) \neq \varnothing$. Since $\alpha(u_{i+1}) \supseteq \alpha(u_n) \neq \varnothing$, $u_{i+1} = az$ for some $a \in \alpha(u_{i+1})$, $z \in A^*$. Then $f = f\phi(az) = f\phi(a)\phi(z)$ and $f = f\phi(a)$. Consequently $f = f\phi(a)$ for all $a \in \alpha(u_{i+1})$. Because $u_{i+1} \cdots u_n v \in (\alpha(u_{i+1}))^*$ it follows that $\phi(u) = \phi(u_0 \cdots u_n) = f\phi(u_{i+1} \cdots u_n) = f\phi(u_{i+1} \cdots u_n v) = \phi(uv)$.

Theorem 26 Let M be the syntactic monoid of $X \subseteq A^*$. Then M is finite and R-trivial if and only if X is a $\underset{nR}{\sim}$ language for some $n \geqslant 0$.

Proof: Assume M is finite and R-trivial. Let $n = \#M$ and let $x,y \in A^*$. Suppose $x \underset{nR}{\dot{\approxeq}} y$. Then $x = rus$ and $y = ruvs$ for some $r,s,u,v \in A^*$ such that $u \underset{n}{\sim} uv$. By Lemma 25, $\underline{u} = \underline{uv}$ and $\underline{x} = \underline{rus} = \underline{ruvs} = \underline{y}$. Since $\underset{nR}{\approxeq}$ is the symmetric transitive closure of $\underset{nR}{\dot{\approxeq}}$, it follows that $x \underset{nR}{\approxeq} y$ implies $\underline{x} = \underline{y}$. By Proposition 23 $x \underset{nR}{\sim} y$ if and only if $x \underset{nR}{\approxeq} y$. Thus $x \underset{nR}{\sim} y$ implies $\underline{x} = \underline{y}$; i.e. X is a $\underset{nR}{\sim}$ language.

By Proposition 9, for all $x,y \in A^*$, $(xy)^n \underset{nR}{\sim} (xy)^n x$. If X is a $\underset{nR}{\sim}$ language then $(\underline{xy})^n = (\underline{xy})^n \underline{x}$. Since the syntactic morphism is a surjective function from A^* onto M, it follows that for all $f,g \in M$, $(fg)^n = (fg)^n f$. Because $\underset{nR}{\sim}$ is of finite index, M is finite and it is R-trivial by Theorem 24.

2.4 Partially Ordered Automata

In this section the automata associated with R-trivial monoids and $\sim_{nR}$ languages are considered.

Lemma 27 Let S = <A, Q, σ> be a semiautomaton, let $x \in A^*$ and let $C \subseteq A$. Then $\sigma(q,xa) = \sigma(q,x)$ for all $a \in C$, $q \in Q$ if and only if $\sigma(q,xy) = \sigma(q,x)$ for all $y \in C^*$, $q \in Q$.

Proof: Obvious.

Proposition 28 Let S = <A,Q,σ> be a semiautomaton and let M be its transformation monoid. The following are equivalent.

1. M is R-trivial.
2. There exists $n > 0$ such that for all $x,y \in A^*$, x n-full and $\alpha(x) \supseteq \alpha(y)$ imply $\sigma(q,x) = \sigma(q,xy)$ for all $q \in Q$.
3. For any $x \in A^*$, $\sigma(q,x) = \sigma(q,xx)$ for all $q \in Q$ implies $\sigma(q,x) = \sigma(q,xa)$ for all $q \in Q$, $a \in \alpha(x)$.

Proof:

(1$\Rightarrow$2) This follows from Lemma 25, the comment following Definition 6, and the fact that the syntactic morphism is surjective.

(2$\Rightarrow$3) Let $n > 0$ be such that for all $x,y \in A^*$, x n-full and $\alpha(x) \supseteq \alpha(y)$ imply $\sigma(q,x) = \sigma(q,xy)$ for all $q \in Q$. Suppose $x \in A^*$ satisfies $\sigma(q,x) = \sigma(q,xx)$ for all $q \in Q$. By induction it follows that $\sigma(q,x) = \sigma(q,x^n)$ for all $q \in Q$ and $n > 0$. Let $q \in Q$ and $a \in \alpha(x)$. Since x^n is n-full and $\alpha(a) \subseteq \alpha(x) = \alpha(x^n)$, $\sigma(q,x) = \sigma(q,x^n) = \sigma(q,x^na) = \sigma(\sigma(q,x^n),a) = \sigma(\sigma(q,x),a) = \sigma(q,xa)$.

(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 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 $\sigma(q,wa) = \sigma(q,w)$ for all $a \in \alpha(w)$, $q \in Q$. Because $\alpha(y) \subseteq \alpha(w)$ it follows by Lemma 27 that $\sigma(q,wy) = \sigma(q,w)$ for all $q \in Q$. Thus $eg = \underline{wy} = \underline{w} = e$ so $eP_e = e$. But $eP_e = e$ implies $eM_e = e$; hence M is R-trivial.

Definition 29 Let $S = < A, Q, \sigma >$ be a semiautomaton. Then $\Pi(S)$ is defined to be the semiautomaton $<A, Q_1, \sigma_1>$, where

$$Q_1 = \{q \in Q \mid \text{there exists } x \in A^* \text{ and } q' \in Q-\{q\} \text{ such that } \sigma(q',x) = q\}$$

and σ_1 is the restriction of σ to $Q_1 \times A$. Note that Q_1 is the set of all states that have nontrivial predecessors. $\Pi^n(S)$ can be defined inductively by:

$$\Pi^0(S) = S$$

$$\text{and } \Pi^n(S) = \Pi(\Pi^{n-1}(S)) \text{ for } n > 0.$$

The semiautomaton $<A, Q_n, \sigma_n>$ will be used to represent $\Pi^n(S)$. Clearly, for every S there exists a smallest integer n such that $Q = Q_0 \supseteq Q_1 \supseteq \cdots \supseteq Q_n = Q_{n+1}$.

Recall the definition of partially ordered semiautomata given in Section 1.1. For any semiautomaton $S = < A, Q, \sigma >$, $\rightarrow$ is clearly a preorder on Q since $\sigma(q,1) = q$ for all $q \in Q$ and $\sigma(p,x) = q$ and $\sigma(q,y) = r$ imply $\sigma(p,xy) = r$ for all $p,q,r \in Q$ and $x,y \in A^*$. Thus to prove that a semiautomaton is partially ordered it is sufficient to show that $\rightarrow$ is an antisymmetric relation on the state set.

Property 2 in the following proposition is from [28].

Proposition 30 Let $S= < A, Q, \sigma >$ be a semiautomaton. The following conditions are equivalent.

1. S is partially ordered.
2. For all $q \in Q$, $x,y \in A^*$, $\sigma(q,xy) = q$ implies $\sigma(q,x)=q$.
3. There exists an integer $n \geqslant 0$ such that $\Pi^n(S)$ has an empty state set.

Proof:

(1⇒2) Suppose $x,y \in A^*$ and $q \in Q$ are such that $\sigma(q,xy) = q$. Let $p = \sigma(q,x)$. Then $q \rightarrow p$. Now $q = \sigma(q,xy) = \sigma(p,y)$, therefore $p \rightarrow q$. Since $\rightarrow$ is a partial order, $p = q$ and thus $\sigma(q,x) = q$.

(2⇒3) Suppose that $\sigma(q,xy) = q$ implies $\sigma(q,x) = q$ for all $q \in Q$, $x,y \in A^*$, but that $\Pi^n(S)$ does not have an empty state set for any $n \geqslant 0$. Let n be such that $Q_n = Q_{n+1}$ and let $m = \# Q_n$. Because $Q_n \neq \varnothing$ there exists $q_1 \in Q_n$. Since $q_1 \in Q_{n+1}$ there exists $q_2 \in Q - \{q_1\}$ and $x_1 \in A^*$ such that $\sigma(q_2,x_1) = q_1$. Repeating this argument a total of m times, one has $q_1, \ldots, q_{m+1} \in Q$, $x_1, \ldots, x_m \in A^*$ where $\sigma(q_{i+1},x_i) = q_i \neq q_{i+1}$ for $i = 1, \ldots, n$. But $m+1 > \# Q_n$; therefore there exist i and j such that $0 \leqslant i < j \leqslant n$ and $q_i = q_{j+1}$. Then $\sigma(q_{j+1},x_j(x_{j-1} \cdots x_i)) = q_i = q_{j+1}$ so that $\sigma(q_{j+1},x_j) = q_{j+1}$. This contradicts the fact that $q_j \neq q_{j+1}$.

(3⇒1) Suppose S is not partially ordered. Then there exist $p,q \in Q$ such that $p \rightarrow q$, $q \rightarrow p$, and $p \neq q$. Let $x,y \in A^*$ be such that $\sigma(p,x) = q$ and $\sigma(q,y) = p$. From the definition of Π, if $p,q \in Q_i$ then $p,q \in Q_{i+1}$. Since $p,q \in Q = Q_0$ it follows by induction that $p,q \in Q_n$ for all $n \geqslant 0$. Thus there does not exist an integer $n \geqslant 0$ such that $\Pi^n(S)$ has an empty state set.

The two families of automata described in Propositions 28 and 30 are actually the same.

Proposition 31 If there exists $n > 0$ such that for all $x,y \in A^*$, x n-full and $\alpha(x) \supseteq \alpha(y)$ imply $\sigma(q,x) = \sigma(q,xy)$ for all $q \in Q$ then $\sigma(q,xy) = q$ implies $\sigma(q,x) = q$ for all $q \in Q$, $x,y \in A^*$.

Proof: Suppose $\sigma(q,xy) = q$. Then $\sigma(q, (xy)^n) = q$. Now $(xy)^n$ is n-full and $\alpha((xy)^n) \supseteq \alpha(x)$, so $q = \sigma(q, (xy)^n) = \sigma(q, (xy)^n x) = \sigma(\sigma(q, (xy)^n),x) = \sigma(q,x)$.

Proposition 32 Let $S = <A, Q, \sigma>$ be a partially ordered semiautomaton. Then the transformation monoid, M, of S is R-trivial.

Proof: Suppose $f,g,h \in \mathrm{M}$ are such that $fgh = f$. Since M is the transformation monoid of S there exist $x,y,z \in \mathrm{A}^*$ such that $\underline{x} = f$, $\underline{y} = g$, and $\underline{z} = h$. Now $\underline{xyz} = fgh = f = \underline{x}$ and S is partially ordered. Thus $\sigma(q,x) = \sigma(q,xyz) = \sigma(\sigma(q,x),yz)$ and, by Proposition 30, $\sigma(q,x) = \sigma(\sigma(q,x),y) = \sigma(q,xy)$ for all $q \in \mathrm{Q}$. Therefore $f = \underline{x} = \underline{xy} = fg$.

Three additional properties of partially ordered semiautomata, mentioned in [21], [28], and [31], are now presented.

Proposition 33 If **T** is a semiautomaton which is covered by some partially ordered semiautomaton S then **T** is partially ordered.

Proof: Assume S is partially ordered. Since any subsemiautomaton of a partially ordered semiautomaton is clearly partially ordered it is sufficient to prove the result when **T** is a homomorphic image of S.

Suppose $\mathrm{T} = <\mathrm{A},\mathrm{P},\tau>$ is a homomorphic image of $\mathrm{S} = <\mathrm{A},\mathrm{Q},\sigma>$. Then there exists a surjective map $\psi:\mathrm{Q}\rightarrow\mathrm{P}$ such that $\tau(\psi(q),x) = \psi(\sigma(q,x))$ for all $x \in \mathrm{A}^*$

Now suppose $\tau(p,xy) = p$ where $p \in \mathrm{P}$ and $x,y \in \mathrm{A}^*$. Let $\mathrm{Q}' = \{q \in \mathrm{Q} \mid \psi(q) = p\}$. Note $\mathrm{Q}' \neq \emptyset$ because ψ is surjective. Consider the map $\gamma:\mathrm{Q}'\rightarrow\mathrm{Q}'$ defined by $\gamma(q) = \sigma(q,xy)$. Because $\psi(\sigma(q,xy)) = \tau(\psi(q),xy) = \tau(p,xy) = p$, $\gamma(q)$ is indeed an element of Q' for each $q \in \mathrm{Q}'$.

Let $q' \in \mathrm{Q}'$, and let $n = \#\mathrm{Q}'$. Since $\{\gamma^0(q') = q', \gamma^1(q'), \gamma^2(q'), \ldots, \gamma^n(q')\} \subseteq \mathrm{Q}'$, there exist $0 \leqslant i < j \leqslant n$ such that $\gamma^i(q') = \gamma^j(q')$. From the definition of γ, $\gamma^j(q') = \sigma(q',(xy)^j)$ $= \sigma(\gamma^i(q'),(xy)^{j-i})$. Since S is partially ordered, $\sigma(\gamma^i(q'),x) = \gamma^i(q')$. Thus $\tau(p,x) = \tau(\psi(\gamma^i(q')),x) = \psi(\sigma(\gamma^i(q'),x)) = \psi(\gamma^i(q')) = p$ and hence **T** is partially ordered.

Proposition 34 The cascade product of two partially ordered semiautomata is partially ordered.

Proof: Suppose $\mathrm{S} = <\mathrm{A}, \mathrm{Q}, \sigma>$ and $\mathrm{T} = <\mathrm{C}, \mathrm{P}, \tau>$ are partially ordered and $\omega:\mathrm{Q}\times\mathrm{A}\rightarrow\mathrm{C}$ is a connection function. Let $(q,p) \in \mathrm{Q}\times\mathrm{P}$ and $x,y \in \mathrm{A}^*$ be such that $\eta((q,p),xy) = (q,p)$. Say

$x = x_1 \cdots x_n$ and $y = y_1 \cdots y_m$ where $n,m \geqslant 0$ and $x_i, y_i \in$ A.

Then $(q,p) = \eta((q,p),xy) = (\sigma(q,xy), \tau(p, \omega(q_1,x_1) \cdots \omega(q_n,x_n)\omega(q_{n+1},y_1) \cdots \omega(q_{n+m},y_m)))$ where $q_1 = q$, $q_{i+1} = \sigma(q_i,x_i)$ for $i = 1, \ldots, n-1$, and $q_{n+i+1} = \sigma(q_{n+i},y_i)$ for $i = 0, \ldots, m-1$. Thus $q = \sigma(q,xy)$ and $p = \tau(p, \omega(q_1,x_1) \cdots \omega(q_n,x_n)\omega(q_{n+1},y_1) \cdots \omega(q_{n+m},y_m))$.

But S and T are partially ordered; thus $\sigma(q,x) = q$ and $\tau(p, \omega(q_1,x_1) \cdots \omega(q_n,x_n)) = p$. Hence $\eta((q,p),x) = (\sigma(q,x), \tau(p, \omega(q_1,x_1) \cdots \omega(q_n,x_n))) = (q,p)$ so that $\mathbf{S} \circ \mathbf{T} = <\mathrm{A}, \mathrm{Q}\times\mathrm{P}, \eta>$ is partially ordered.

Corollary 35 The direct product of two partially ordered semiautomata is partially ordered.

Let $\mathbf{A} = <\mathrm{A}, \mathrm{Q}, q_0, \mathrm{F}, \sigma>$ and $\mathbf{C} = <\mathrm{A}, \mathrm{P}, p_0, \mathrm{G}, \tau>$ be automata and let $<\mathrm{A},\mathrm{Q}\times\mathrm{P},\eta> = <\mathrm{A}, \mathrm{Q}, \sigma> \times <\mathrm{A}, \mathrm{P}, \tau>$. Then the union of **A** and **C** is

$$\mathbf{A} \cup \mathbf{C} = <\mathrm{A}, \mathrm{Q}\times\mathrm{P}, (q_0, p_0), \mathrm{F}\times\mathrm{P} \cup \mathrm{Q}\times\mathrm{G}, \eta>,$$

the intersection of **A** and **C** is

$$\mathbf{A} \cap \mathbf{C} = <\mathrm{A}, \mathrm{Q}\times\mathrm{P}, (q_0, p_0), \mathrm{F}\times\mathrm{G}, \eta>,$$

and the complement of **A** is

$$\overline{\mathbf{A}} = <\mathrm{A}, \mathrm{Q}, q_0, \mathrm{Q}\text{-}\mathrm{F}, \sigma>.$$

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

Definition 36 A graph G is *tree-like* if and only if 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′.

Clearly any initialized semiautomaton whose state graph is tree-like is partially ordered.

Proposition 37 Let $n \geqslant 0$. The state graph of the initialized semiautomaton

$\sigma>$ is tree-like.

Proof: $[1]_{\underset{n}{\sim}R}$ is clearly the root since $\sigma([1]_{\underset{n}{\sim}R}, x) = [x]_{\underset{n}{\sim}R}$ for all $x \in A^*$. For any node $[x]_{\underset{n}{\sim}R} \in A^*/_{\underset{n}{\sim}R}$, the fact that there is a unique path from $[1]_{\underset{n}{\sim}R}$ to $[x]_{\underset{n}{\sim}R}$ which contains no trivial loops follows directly from Theorem 18. Thus the state graph is tree-like.

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

Definition 38 For $n \geqslant 0$, an *n-way fork* is an initialized semiautomaton $<A, \{q_0, q_1, \ldots, q_n\}, q_0, \sigma>$ where $A = A_0 \cup A_1 \cup \cdots \cup A_n$, the A_i's are pairwise disjoint and, for $i > 0$, are non-empty, $\sigma(q_0, a) = q_i$ for all $a \in A_i$, and $\sigma(q_i, a) = q_i$ for all $a \in A$, $i = 1, \ldots, n$. See Figure 1. A *half-reset* is a one-way fork.

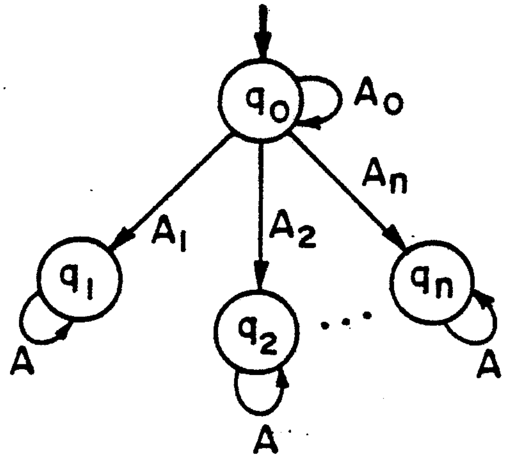

Figure 1 An *n*-way fork

Proposition 39 If a semiautomaton can be covered by a cascade product of half-resets then it is partially ordered.

Proof: Immediate from Propositions 33 and 34 and the fact that a half-reset is partially ordered.

In [21] and [31] 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 40 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 Figure 2(a).

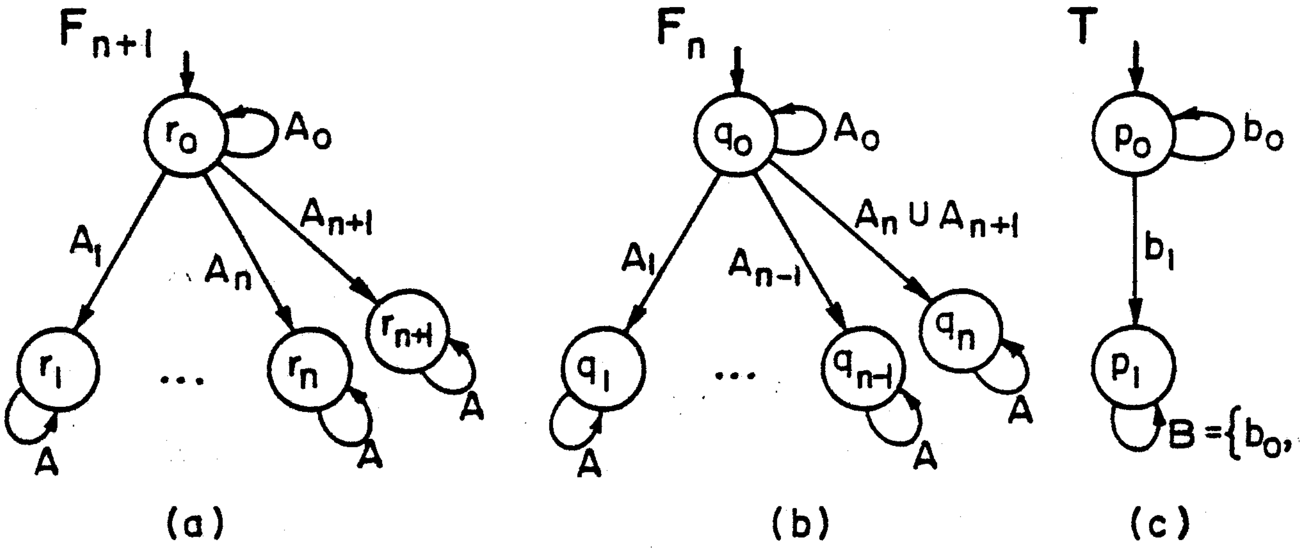

Figure 2

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

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

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 $n \geqslant 1$.

Proposition 41 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 0 or 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 $\mathrm{S} = <\mathrm{A}, \mathrm{Q}, q_0, \sigma>$ be an initialized semiautomaton whose graph is tree-like of height h. Let $\{q_1, \ldots, q_n\} = \{q \in \mathrm{Q} - \{q_0\} \mid \sigma(q_0,a) = q$ for some $a \in \mathrm{A}\}$ be the set of children of q_0. For $1 \leqslant i \leqslant n$, let $\mathrm{S}_i = <\mathrm{A}, \mathrm{Q}_i, q_i, \sigma_i>$ be the subsemiautomaton of S initialized at q_i. Since $q_i \neq q_0$, the height of the graph is less than h; thus S_i is isomorphic to the connected initialized subsemiautomaton of $\mathrm{S}_i' = <\mathrm{A}, \mathrm{Q}_i', q_i, \sigma_i'>$, a cascade product of forks.

Define $\mathrm{T}_i' = <\mathrm{C}_i, \mathrm{Q}_i', q_i, \tau_i'>$ as follows. If there exists an $a \in \mathrm{A}$ such that $\sigma_i'(q,a) = q$ for all $q \in \mathrm{Q}_i'$ let $\mathrm{C}_i = \mathrm{A}$ and $\tau_i' = \sigma_i'$. Otherwise let $\mathrm{C}_i = \mathrm{A} \cup \{e\}$, where $e \notin \mathrm{A}$, and let τ_i' be such that for $q \in \mathrm{Q}_i'$, $c \in \mathrm{C}_i$,

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

Note that if T_i is an n-way fork, then T_i' is an n-way fork too. Also, applying the transformation to the cascade product of two semiautomata gives the same result as applying it to the two semiautomata separately and then taking the cascade product. Hence T_i' is still a cascade product of forks.

Let $\mathrm{T}_0 = <\mathrm{A}, \mathrm{P}, p_0, \tau_0>$ be the n-way fork where $\mathrm{P} = \{p_0, p_1, \ldots, p_n\}$ and

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

Inductively define $\mathrm{T}_i = \mathrm{T}_{i-1} \circ \mathrm{T}_i'$ for $i = 1, \ldots, n$ where the connection

$\omega_i : \mathrm{P} \times \mathrm{Q}_1' \times \cdots \times \mathrm{Q}_{i-1}' \times \mathrm{A} \to \mathrm{C}_i$ is given by

$$\omega_i(r,a) = \begin{cases} a & \text{if } r = (p_i,\ q_1, \ldots, q_{i-1}) \\ c_i & \text{otherwise} \end{cases}$$

where $\tau_i'(q,c_i) = q$ for all $q \in \mathrm{Q}_i'$.

It is a straightforward proof by induction to show that the set of states of T_i accessible from the initial state $(p_0,q_1, \ldots, q_i)$ is

$$\mathrm{R}_i = \{(p_0,q_1, \ldots, q_i)\} \cup \{(p_k,q_1, \ldots, q_{k-1},q,q_{k+1}, \ldots, q_i) \mid q \in \mathrm{Q}_k',\ 1 \leqslant k \leqslant i\}$$

and that the following equations hold:

$\tau_i((p_0,\ q_1, \ldots,\ q_i),\ a) = (p_k,\ q_1, \ldots,\ q_i)$ for all $a \in \mathrm{A}$ such that $\sigma(q_0,a) = q_k$, $1 \leqslant k \leqslant i$,

$\tau_i((p_k,\ q_1, \ldots,\ q_{k-1},\ q,\ q_{k+1}, \ldots,\ q_i),\ a) = (p_k,\ q_1, \ldots,\ q_{k-1},\ \tau_k'(q,a),\ q_{k+1}, \ldots,\ q_i)$

for $q \in \mathrm{Q}_k'$, $1 \leqslant k \leqslant i$, and

$\tau_i((p_k,\ q_1, \ldots,\ q_i),\ a) = (p_k,\ q_1, \ldots,\ q_i)$ for $i < k \leqslant n$.

Now consider the bijection $\psi : \mathrm{Q} \to \mathrm{R}_n$ defined by

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

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

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

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

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

$$= \tau_n(\psi(q_0),\ a)\ .$$

Thus ψ is an isomorphism between S and the connected initialized subsemiautomaton of T_n; so the result is true for S . It follows by induction that the proposition is true.

Corollary 42 Any partially ordered initialized semiautomaton is the homomorphic image of the connected initialized subsemiautomaton of a cascade product of half-resets.

Proof: Any partially ordered rooted graph can be transformed into a tree-like graph by splitting nodes (see Figure 3). The desired homomorphism is the obvious one which maps a node in the tree-like graph to thè node in the original graph from which it was produced. The result then follows by Proposition 41.

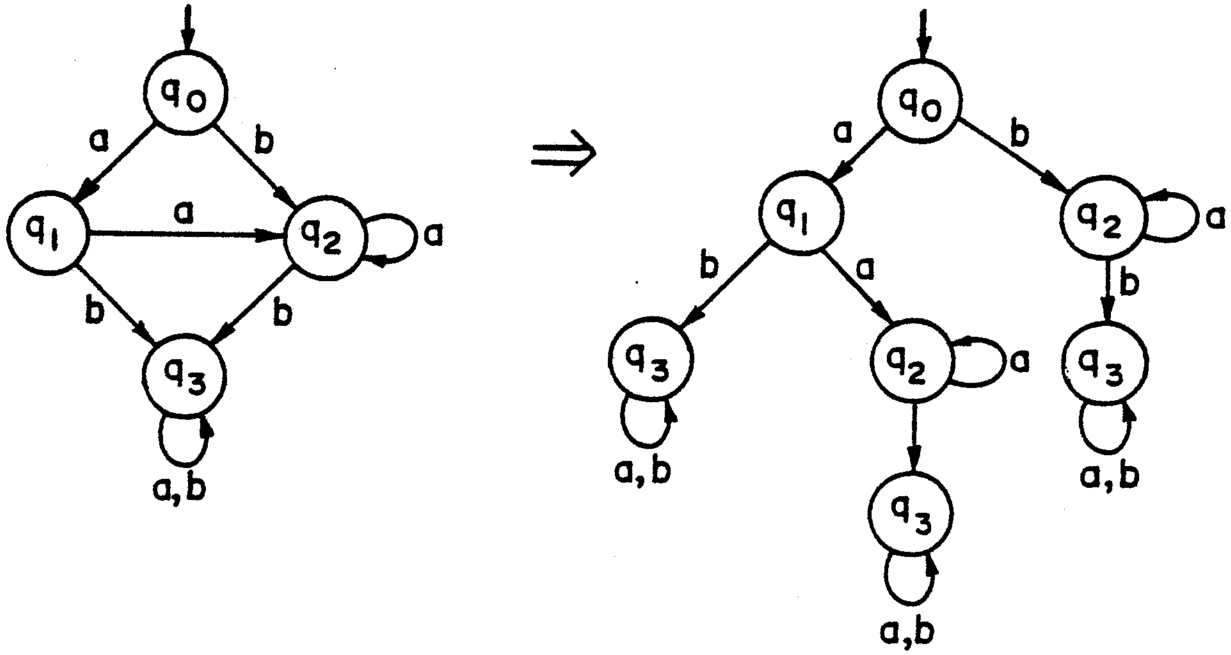

Figure 3

2.5 *R*-Expressions

Definition 43 Let A be a finite alphabet. An *R*-expression is a finite union of regular expressions of the form $A_0^*a_1A_1^* \cdots a_mA_m^*$ where $m \geqslant 0$, $a_1, \ldots, a_m \in A$, and $A_{i-1} \subseteq A-\{a_i\}$ for $1 \leqslant i \leqslant m$.

The relationship between partially ordered semiautomata and *R*-expressions is mentioned in [21].

Proposition 44 Let $X \subseteq A^*$ be the language denoted by some *R*-expression. Then the reduced automaton recognizing X is partially ordered.

Proof: Because of the remarks following Corollary 35 we may assume the expression is of the form $A_0^*a_1A_1^* \cdots a_mA_m^*$, where $m \geqslant 0$ and $A_{i-1} \subseteq A-\{a_i\}$ for $1 \leqslant i \leqslant m$, without any loss of generality.

Consider the automaton $\mathbf{A} = <A, Q, q_0, \{q_m\}, \sigma>$ where $Q = \{q_0, \ldots, q_m, q_d\}$ and σ is defined as follows:

$$\sigma(q_i,a) = \begin{cases} q_i & \text{if } a \in A_i \\ q_{i+1} & \text{if } a = a_{i+1} \\ q_d & \text{if } a \in A-(A_i \cup \{a_{i+1}\}) \end{cases}$$

$$\sigma(q_d,a) = q_d \qquad \text{for all } a \in A$$

It is straightforward to show that $\mathbf{A}$ is partially ordered and recognizes X.

Since the reduced automaton recognizing X is a homomorphic image of $\mathbf{A}$, it follows from Proposition 33 that it, too, is partially ordered.

Proposition 45 Every $\sim_{nR}$ language can be denoted by an *R*-expression.

Proof: It is sufficient to show the result for every congruence class of $\sim_{nR}$. The only $\sim_{0R}$ class is the language denoted by A^*. Therefore assume $n > 0$. Let x be the minimal element of its congruence class. If $|x| = 0$ then, since $n > 0$, $\underline{x} = \underline{1} = \{1\}$ which can be denoted by $\varnothing^*$. Otherwise $x = a_1 \cdots a_m$ for some $a_1, \ldots, a_m \in \mathrm{A}$. Let $\mathrm{A}_0 = \varnothing$ and let $\mathrm{A}_i = \{a \in \mathrm{A} \mid a_1 \cdots a_i a \underset{n}{\sim} a_1 \cdots a_i\}$ for $1 \leqslant i \leqslant m$. Since x is minimal, $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_{i-1}) \subsetneq \mu_n(a_1 \cdots a_{i-1}a_i) \subsetneq \cdots \subsetneq \mu_n(a_1 \cdots a_m)$ by Theorem 18. Hence $a_i \notin \mathrm{A}_{i-1}$ for $1 \leqslant i \leqslant m$ and thus $\mathrm{A}_0^* a_1 \mathrm{A}_1^* \cdots a_m \mathrm{A}_m^*$ is an R-expression. From Proposition 23 it easily follows that if $y \in \mathrm{A}_0^* a_1 \mathrm{A}_1^* \cdots a_m \mathrm{A}_m^*$ then $y \in \underline{x}$. Now let $y \in \underline{x}$ and, for $i = 1, \ldots, m$, let y_i be the shortest prefix of y such that $\mu_n(y_i) = \mu_n(a_1 \cdots a_i)$. Let $y_0 = 1$. Each y_i is a proper prefix of y_{i+1} and $a_1 \cdots a_{i+1} \in \mu_n(a_1 \cdots a_{i+1}) - \mu_n(a_1 \cdots a_i)$. Thus there exist $v_0, v_1, \ldots, v_m \in \mathrm{A}^*$ such that $y_{i+1} = y_i v_i a_{i+1}$ for $i = 0, \ldots, m-1$ and $y = y_m v_m = v_0 c_1 v_1 \cdots v_{m-1} c_m v_m$. Note that, from the definition of y_1, $v_0 = 1$ and, since $a_1 \cdots a_i v_i \underset{n}{\sim} y_i v_i \underset{n}{\sim} y_i \underset{n}{\sim} a_1 \cdots a_i$, $v_i \in \mathrm{A}_i^*$ for $i = 1, \ldots, m$. Also,

$$
\begin{aligned}
& a_1 \cdots a_{i+1} \in \mu_n(a_1 \cdots a_{i+1}) - \mu_n(a_1 \cdots a_i) \\
& = \mu_n(y_i v_i c_{i+1}) - \mu_n(y_i) \\
& = \mu_n(y_i c_{i+1}) - \mu_n(y_i)
\end{aligned}
$$

so that $c_{i+1} = a_{i+1}$ for $i = 0, \ldots, m-1$. Hence $y \in \mathrm{A}_0^* a_1 \mathrm{A}_1^* \cdots a_m \mathrm{A}_m^*$.

With this result, Theorem 26, Proposition 32, and Proposition 44, the languages defined by the congruences $\underset{n}{\sim}_R$, R-trivial monoids, partially ordered automata, and R-expressions are seen to be the same. Since the set of partially ordered automata over a given alphabet forms a Boolean algebra, the set of R-expressions (over the same alphabet) also does. This result is used in the following theorem.

Proposition 46 Let A be an alphabet and let $D = \{\mathrm{C}^* a \mid \mathrm{C} \subsetneq \mathrm{A} - \{a\}\}\mathbf{M}$. Then $(D \cup D\mathrm{A}^*)\mathbf{B}$ is equal to the set of R-expressions over the alphabet A.

Proof: Note: It is convenient to consider elements of D as 'words' over the alphabet $\{\mathrm{C}^* a \mid \mathrm{C} \subsetneq \mathrm{A} - \{a\}\}$. This is reflected in the notation below.

$(\subsetneq)$ Let $w \in D$. If $w = 1$ then w and $w\mathrm{A}^*$ can be expressed by the R-expressions $\varnothing^*$ 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 $w = A_1^*a_1 \cdots A_m^*a_m\varnothing^*$ and $wA^* = A_1^*a_1 \cdots A_m^*a_mA^*$ which are both R-expressions. Since the set of R-expressions forms a Boolean algebra it contains $(D \cup DA^*)\mathbf{B}$.

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

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

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

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

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

It is now possible to relate the family of languages corresponding to finite R-trivial monoids to the dot-depth hierarchy. This hierarchy is defined as follows:

$$B_0 = \{\{a\} \mid a \in A\}\mathbf{MB}$$

$$\text{and } B_{i+1} = B_i\mathbf{MB} \text{ for } i \geqslant 0.$$

Since the family of languages $\{\{a\} \mid a \in A\}\mathbf{M} = \{\varnothing^*a \mid a \in A\}\mathbf{M} \subseteq \{C^*a \mid C \subseteq A-\{a\}\}\mathbf{M} = D$, $B_0 = \{\{a\} \mid a \in A\}\mathbf{MB} \subseteq D\mathbf{B} \subseteq (D \cup DA^*)\mathbf{B}$. Thus all languages in B_0 have finite R-trivial monoids.

Any $\underset{n}{\sim}$ language is also an $\underset{n\,R}{\sim}$ language. However, the family B_1 is incomparable with the family of languages with R-trivial monoids. The language $\mathrm{A}^*a \in B_1$, where $\#\mathrm{A} > 1$, has a reduced automaton which is not partially ordered. See Figure 4. In [28, page 116], Simon shows that for $\#\mathrm{A} > 2$ the language denoted by the R-expression $a^*b\mathrm{A}^*$ is not in B_1.

Finally, for any $\mathrm{A}_i \subsetneq \mathrm{A}$, $\mathrm{A}_i^* = \bigcup_{a \in \mathrm{A}-\mathrm{A}_i} \overline{\mathrm{A}^*a\mathrm{A}^*} \in B_1$, so that any R-expression denotes a language in $B_1\mathbf{MB} = B_2$.

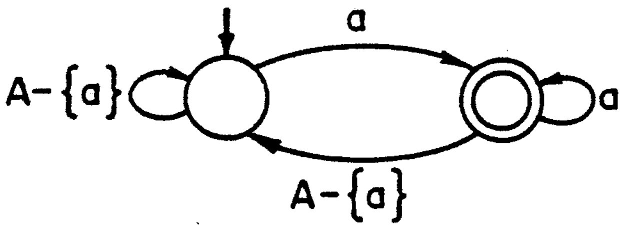

Figure 4

2.6 Other Congruences

Besides $\underset{nR}{\sim}$ and $\underset{nR}{\approx}$ other congruences can be used to characterize the languages corresponding to finite R-trivial monoids.

Definition 47 Let $x,y \in A^*$. Then $x \underset{0}{\leftarrow} y$ and $x \underset{n+1}{\leftarrow} y$ if and only if for each decomposition $x = x'ax''$ with $a \in A$, there exists a decomposition $y = y'ay''$ such that $x' \underset{n}{\sim} y'$ and vice versa.

Definition 48 Let $x,y \in A^*$. Then $x \underset{0}{\Leftarrow} y$, and $x \underset{n+1}{\Leftarrow} y$ if and only if for each decomposition $x = x'ax''$, with $a \in A$, there exists a decomposition $y = y'ay''$ such that $x' \underset{n}{\Leftarrow} y'$ and vice versa.

Definition 49 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{nR}{\dot{\equiv}} y$ if and only if there exist $u,v,z_1,z_2 \in A^*$ such that $x = z_1uz_2$, $y = z_1uvz_2$, u is n-full, and $\alpha(u) \supseteq \alpha(v)$. $\underset{nR}{\equiv}$ is the symmetric transitive closure of $\underset{nR}{\dot{\equiv}}$.

Note that $\underset{nR}{\equiv}$ is the smallest congruence satisfying $u \underset{nR}{\equiv} uv$ for all $u,v \in A^*$ such that u is n-full and $\alpha(u) \supseteq \alpha(v)$.

Definition 50 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{nR}{\doteq} y$ if and only if there exist $u,v,z_1,z_2 \in A^*$ such that $x = z_1uz_2$, $y = z_1uvz_2$, u is n-full, and $\alpha(u) = \alpha(v)$. $\underset{nR}{=}$ is the symmetric transitive closure of $\underset{nR}{\doteq}$.

Similarly $\underset{nR}{=}$ is the smallest congruence satisfying $u \underset{nR}{=} uv$ for all $u,v \in A^*$ such that u is n-full and $\alpha(u) = \alpha(v)$.

Proposition 51 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n+1}{\leftarrow} y$ implies $x \underset{nR}{\sim} y$. However $x \underset{n+1}{\leftarrow} y$ does not imply $x \underset{n+1R}{\sim} y$.

Proof: Suppose $x \underset{n+1}{\leftarrow} y$. Let u be a prefix of x. If $u = 1$ then u is a prefix of y. Otherwise $u = x'a$ for some $x' \in A^*$. Since $x \underset{n+1}{\leftarrow} y$ there exists a prefix $y'a$ of y such that $x' \underset{n}{\sim} y'$. But $\underset{n}{\sim}$

is a congruence so $u = x'a \underset{n}{\sim} y'a$. Similarly for every prefix v of y there exists a prefix u of x such that $u \underset{n}{\sim} v$. Therefore $x \underset{nR}{\sim} y$.

Let $x = (ab)^n ab$ and $y = (ab)^n ba$. Then $x \underset{n+1}{\leftarrow} y$ since $(ab)^n \underset{n}{\sim} (ab)^n b$ and $(ab)^n a \underset{n}{\sim} (ab)^n$. However $x \underset{n+1\,R}{\not\sim} y$.

Proposition 52 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{nR}{\cong} y$ implies $x \underset{n}{\leftarrow} y$. However $x \underset{nR}{\cong} y$ does not imply $x \underset{n+1}{\leftarrow} y$.

Proof: It is sufficient to show that if $x = uv$, $y = uav$, and $u \underset{n}{\sim} ua$, where $u,v \in A^*$ and $a \in A$, then $x \underset{n}{\leftarrow} y$.

Let $x = x'bx''$ be a decomposition of x. If $x'b$ is a prefix of u, let $y' = x'$. Otherwise $x'b = uzb$ for some $z \in A^*$. Let $y' = uaz$. Note that $ua \underset{n}{\sim} u$ so $y' = uaz \underset{n}{\sim} uz = x'$. In both cases $y'b$ is a prefix of y such that $y' \underset{n}{\sim} x'$. By Proposition 4, $y' \underset{n-1}{\sim} x'$.

Now let $y = y'by''$ be any decomposition of y. If $y'b$ is a prefix of u let $x' = y'$. If $y'b = uazb$ for some $z \in A^*$, let $x' = uz$. Since $ua \underset{n}{\sim} u$, $y' = uaz \underset{n}{\sim} uz = x'$. Otherwise $y'b = ua$. Since $u \underset{n}{\sim} ua$, there exist $u_1, \ldots, u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_n) \supseteq \alpha(a) = \{a\}$. Thus $a \in \alpha(u_n)$, so $u_n = u'_n a u''_n$ for some $u'_n, u''_n \in A^*$. Let $x' = u_1 \cdots u_{n-1} u'_n$. Now, from Proposition 5, $u_1 \cdots u_{n-1} \underset{n-1}{\sim} u_1 \cdots u_{n-1} u_n = u = y'$ and $u_1 \cdots u_{n-1} \underset{n-1}{\sim} u_1 \cdots u_{n-1} u'_n = x'$ hence $x' \underset{n-1}{\sim} y'$. In all three cases $x'b$ is a prefix of x such that $y' \underset{n-1}{\sim} x'$.

Therefore $x \underset{n}{\leftarrow} y$.

For $n = 0$ note that $a \underset{0R}{\cong} b$ but $a \underset{1}{\not\leftarrow} b$. Now consider $n > 0$. Let $x = (ab)^{n-1}a$ and $y = (ab)^{n-1}aa$. Clearly $x \underset{nR}{\cong} y$. Let $y' = (ab)^{n-1}a$. The only prefix of x $\underset{n}{\sim}$ congruent to y' is x itself, so there does not exist an x' such that $x = x'ax''$ and $x' \underset{n}{\sim} y'$. Therefore $x \underset{n+1}{\not\leftarrow} y$.

Proposition 53 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n}{\Leftarrow} y$ implies $x \underset{n}{\sim} y$.

Proof: By induction on n.

For $n = 0$ the result is trivial since $x \underset{0}{\sim} y$ for all $x,y \in A^*$. Let $n \geqslant 0$ and assume the result is true for n. Suppose $x \Lleftarrow_{n+1} y$.

Let $u \in \mu_{n+1}(x)$. Either $u = 1 \in \mu_{n+1}(y)$ or $u = u'a$ for some $u' \in A^*$, $a \in A$. In this second case there exists a prefix $x'a$ of x such that $u' \in \mu_n(x')$. Since $x \Lleftarrow_{n+1} y$, there exists a prefix $y'a$ of y such that $x' \Lleftarrow_n y'$. By the induction hypothesis $x' \ {}_{n}\!\sim y'$. Therefore $u' \in \mu_n(x') = \mu_n(y')$. Then $u = u'a \in \mu_{n+1}(y'a) \subseteq \mu_{n+1}(y)$. Hence $\mu_{n+1}(x) \subseteq \mu_{n+1}(y)$.

By symmetry $\mu_{n+1}(y) \subseteq \mu_{n+1}(x)$. Therefore $x \ {}_{n+1}\!\sim y$.

Proposition 54 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \Lleftarrow_n y$ if and only if $x \leftarrow_n y$.

Proof: For $n > 0$, $x \Lleftarrow_n y$ implies $x \leftarrow_n y$ is an immediate corollary of Proposition 53. From the definitions it is clear that $x \Lleftarrow_0 y$ if and only if $x \leftarrow_0 y$.

Let $n > 0$ and assume $x \leftarrow_{n-1} y$ implies $x \Lleftarrow_{n-1} y$ for all $x,y \in A^*$. Suppose $x \leftarrow_n y$. Let $x = x'ax''$ be any decomposition of x. Then there exists a decomposition $y = y'ay''$ of y such that $x' \ {}_{n-1}\!\sim y'$.

From Proposition 51, $x \leftarrow_n y$ implies $x \ {}_{n-1}\!\sim_R y$. Since x' is a prefix of x, y' is a prefix of y, and $x' \ {}_{n-1}\!\sim y'$, it follows by Proposition 8(c) that $x' \ {}_{n-1}\!\sim_R y'$. But $x' \ {}_{n-1}\!\sim_R y'$ implies $x' \ {}_{n-1}\!\cong_R y'$, which implies $x' \leftarrow_{n-1} y'$ by Proposition 52, which implies $x' \Lleftarrow_{n-1} y'$ by assumption.

Similarly, for every decomposition $y = y'ay''$ there exists a decomposition $x = x'ax''$ such that $x' \Lleftarrow_{n-1} y'$. Hence $x \Lleftarrow_n y$. By induction it follows that $x \leftarrow_n y$ implies $x \Lleftarrow_n y$ for all $n \geqslant 0$.

Proposition 55 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \ {}_{n}\!\cong_R y$ if and only if $x \ {}_{n}\!\equiv_R y$.

Proof:

($\Rightarrow$) Obvious.

($\Leftarrow$) Suppose $u,v \in A^*$ are such that u is n-full and $\alpha(u) \supseteq \alpha(v)$. Then there exist $u_1,\ldots,u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) = \cdots = \alpha(u_n)$. Since $\alpha(u_n) = \alpha(u) \supseteq \alpha(v)$, $\alpha(u_n v) = \alpha(u_n) = \alpha(vu_n)$. Therefore $u = u_1 \cdots u_n \ {}_{n}\!\doteq_R \ u_1 \cdots u_n(vu_n)$ and $uv = u_1 \cdots u_{n-1}(u_n v) \ {}_{n}\!\doteq_R \ u_1 \cdots u_{n-1}(u_n v)u_n$ so that $u \ {}_{n}\!\cong_R uv$. But ${}_{n}\!\equiv_R$ is the smallest congruence satisfying $u \ {}_{n}\!\equiv_R uv$ for all $u,v \in A^*$ such that u is n-full and $\alpha(u) \supseteq \alpha(v)$. Hence

$x \underset{n\,R}{\equiv} y$ implies $x \underset{n\,R}{\overline{=}} y$ for all $x,y \in A^*$.

Proposition 56 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{n\,R}{\equiv} y$ implies $x \underset{n\,R}{\cong} y$. However $x \underset{n\,R}{\equiv} y$ does not imply $x \underset{n+1\,R}{\cong} y$.

Proof: The proof of $x \underset{n\,R}{\equiv} y$ implies $x \underset{n\,R}{\cong} y$ follows immediately from the fact that if u is n-full and $\alpha(u) \supseteq \alpha(v)$ then $u \underset{n}{\sim} uv$. Now let $x = a^n$ and $y = a^{n+1}$ where $a \in A$. Then $a^n \underset{n\,R}{\equiv} a^{n+1}$ but $a^n \underset{n+1\,R}{\not\cong} a^{n+1}$ since $a^{n+1} \in \mu_{n+1}(a^{n+1}) - \mu_{n+1}(a^n)$.

Proposition 57 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{n\,R}{\equiv} y$ implies $x \leftarrow_{n} y$. However $x \underset{n\,R}{\equiv} y$ does not imply $x \leftarrow_{n+1} y$.

Proof: Since $x \underset{n\,R}{\equiv} y$ implies $x \underset{n\,R}{\cong} y$ from Proposition 56, and $x \underset{n\,R}{\cong} y$ implies $x \leftarrow_{n} y$ by Proposition 52, it follows that $x \underset{n\,R}{\equiv} y$ implies $x \leftarrow_{n} y$.

Let $x = a^n$ and $y = a^{n+1}$. Clearly $x \underset{n\,R}{\equiv} y$. Consider the decomposition $y = y'ay''$ of y where $y' = a^n$ and $y'' = 1$. Since the only prefix of x whose n-contents equal $\mu_n(y')$ is x itself, there does not exist a decomposition $x = x'ax''$ such that $x' \underset{n}{\sim} y'$. Hence $x \not\leftarrow_{n+1} y$.

Lemma 58 Let $n,l \geqslant 1$ and suppose $u_1, \ldots, u_l, v \in A^*$ are such that $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_l) \supseteq \alpha(v)$ and $l > (n-1)(\#\alpha(u_1) - \#\alpha(v)+1)$. Then $u_1 \cdots u_l \underset{n\,R}{\equiv} u_1 \cdots u_l z$ for all $z \in (\alpha(v))^*$.

Proof: Let $m_i = \#\alpha(u_i)$ for $i = 1, \ldots, l$. Then $\#\alpha(u_1) = m_1 \geqslant \cdots \geqslant m_l \geqslant \#\alpha(v)$. If for each integer m, $\#\alpha(v) \leqslant m \leqslant \#\alpha(u_1)$, there are at most $n-1$ elements of the sequence $m_1, \ldots, m_l$ with value m, then $l \leqslant (n-1)(\#\alpha(u_1) - \#\alpha(v)+1)$. Thus there exists k, $0 \leqslant k \leqslant l-n$ such that $m_{k+1} = \cdots = m_{k+n}$. This implies $\alpha(u_{k+1}) = \cdots = \alpha(u_{k+n})$.

Let $x_0 = u_1 \cdots u_k$ ($x_0 = 1$ if $k = 0$), let $x_i = u_{k+i}$ for $i = 1, \ldots, n-1$, and let $x_n = u_{k+n} \cdots u_l$. Also let $z \in (\alpha(v))^*$. Since $\alpha(u_{k+n}) \supseteq \alpha(u_{k+n+1}) \supseteq \cdots \supseteq \alpha(u_l) \supseteq \alpha(v) \supseteq \alpha(z)$ it follows that $\alpha(u_{k+n}) = \alpha(u_{k+n} \cdots u_l) \supseteq \alpha(z)$. Thus $\alpha(x_1) = \cdots = \alpha(x_n) \supseteq \alpha(z)$ and hence $u = x_0 x_1 \cdots x_n \underset{n\,R}{\equiv} x_0 x_1 \cdots x_n z = uz$.

Proposition 59 Let $x,y \in A^*$, $m = \# A$, and $n \geqslant 1$. Then $x \underset{(n-1)m+1\,R}{\cong} y$ implies $x \underset{n\,R}{\equiv} y$.

Proof: Let $l = (n-1)m+1$. It is sufficient to show that $x \underset{l\,R}{\doteq} y$ implies $x \underset{n\,R}{\equiv} y$.

Suppose $x \underset{l\,R}{\doteq} y$. Then there exist $u,v,z_1,z_2 \in A^*$ such that $x = z_1uz_2$, $y = z_1uvz_2$ and $u \underset{l}{\sim} uv$. Without loss of generality we may assume $v \neq 1$ since otherwise $x = y$.

By Lemma 5 there exist $u_1, \ldots, u_l \in A^*$ such that $u = u_1 \cdots u_l$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_l) \supseteq \alpha(v)$. Now $\# \alpha(u_1) \leqslant m$ and $\# \alpha(v) \geqslant 1$, so that $l = (n-1)m+1 > (n-1)(\# \alpha(u_1) - \# \alpha(v) + 1)$ and hence, by Lemma 58, $u \underset{n\,R}{\equiv} uv$. But $\underset{n\,R}{\equiv}$ is a congruence, thus $x = z_1uz_2 \underset{n\,R}{\equiv} z_1uvz_2 = y$.

Proposition 60 For $m = \# A$ and $n \geqslant 1$, $x \underset{(n-1)m\,R}{\sim} y$ does not imply $x \underset{n\,R}{\equiv} y$.

Proof: Suppose $A = \{a_1, \ldots, a_m\}$. Now $a_1 \underset{0\,R}{\sim} 1$ but $a_1 \underset{1\,R}{\not\equiv} 1$; thus the result is true for $n = 1$. Assume $n \geqslant 2$. For $i = 1, \ldots, m$ define $x_i = (a_1 \cdots a_i)^{n-1}$. Let $x = x_m x_{m-1} \cdots x_1$ and $y = xa_1$. Since each x_i is $n-1$-full and $\alpha(x_m) \supseteq \cdots \supseteq \alpha(x_1) = \{a_1\}$, it follows by Lemma 11 that $x \underset{(n-1)m\,R}{\sim} y$.

If $x \underset{n\,R}{\equiv} y$ then there exist $z_1,z_2,u \in A^*$ such that $x = z_1uz_2$, u is n-full, and $\alpha(u) \neq \varnothing$. Since a_m only occurs $n-1$ times in x, it is clear that $a_m \notin \alpha(u)$. Assume $a_m, \ldots, a_{i+1} \notin \alpha(u)$ for some i, $1 \leqslant i \leqslant m-1$.

If $x_m \cdots x_{i+1} = v_1u'v_2$ for some $v_1, v_2, u' \in A^*$ such that $\alpha(u') \subseteq \alpha(u)$ then $u' = a_j a_{j+1} \cdots a_{k-1} a_k$ for some j, k where $1 \leqslant j \leqslant k \leqslant i$. Note that none of these words are n-full. Since $t_1(x_m \cdots x_{i+1}) = a_{i+1} \notin \alpha(u)$, it follows that $x_i \cdots x_1 = z'_1uz_2$ for some suffix z'_1 of z_1. But $x_i \cdots x_1$ contains only $n-1$ occurrences of a_i; therefore $a_i \notin \alpha(u)$. By induction, $a_i \notin \alpha(u)$ for $i = m, m-1, \ldots, 1$.

Because $u \in A^*$, $\alpha(u) = \varnothing$, which is a contradiction. Therefore $[x]_{\underset{n\,R}{\equiv}} = \{x\}$ so that $x \underset{n\,R}{\not\equiv} y$.

Lemma 61 Let $u,v,v' \in A^*$ and $n \geqslant 1$. If $\alpha(v) = \alpha(v')$ and $u \underset{n-1}{\sim} ua$ for all $a \in \alpha(v)$ then $uv \underset{n}{\leftarrow} uv'$.

Proof: Suppose xay is a decomposition of uv.

If xa is a prefix of u, say $u = xaz$, let $x' = x$ and $y' = zv'$. Then $x \underset{n-1}{\sim} x'$ and $x'ay' = xazv' = uv'$.

Otherwise u is a prefix of x, so $x = uz$ and $v = zay$ for some $z \in A^*$. Since $a \in \alpha(v) = \alpha(v')$, $v' = z'ay'$ for some $z',y' \in A^*$. Let $x' = uz'$ so that $x'ay' = uz'ay' = uv'$ and $x = uz \underset{n-1}{\sim} u \underset{n-1}{\sim} uz' = x'$.

Therefore for every decomposition xay of uv there exists a decomposition $x'ay'$ of uv' such that $x \underset{n-1}{\sim} x'$.

By symmetry it follows that $uv \xleftarrow[n]{} uv'$.

This lemma is not true if $\xleftarrow[n]{}$ is replaced by $\underset{n\,R}{\sim}$. For example, let $u = ab$, $v = ab$, and $v' = ba$. Then $\alpha(v) = \alpha(v')$, $u = ab \underset{1}{\sim} aba = ua$, and $u = ab \underset{1}{\sim} abb = ub$. However $uv = abab \underset{2\,R}{\not\sim} abba = uv'$.

Definition 62 Let $x,y \in A^*$. The longest common prefix of x and y, $\operatorname{lcp}(x,y)$, is the longest $u \in A^*$ such that $x = ux'$ and $y = uy'$ for some $x',y' \in A^*$.

Proposition 63 Let $x,y \in A^*$, $m = \# A$, and $n \geqslant 2$. Then $x \xleftarrow[(n-1)m+1]{} y$ implies $x \underset{n\,R}{\equiv} y$.

Proof: By induction on $|x| + |y| - 2\,|\operatorname{lcp}(x,y)|$.

Let $l = (n-1)m+1$. Suppose that $x \xleftarrow[l]{} y$ and if x', $y' \in A^*$ are such that $|x'| + |y'| - 2\,|\operatorname{lcp}(x',y')| < |x| + |y| - 2\,|\operatorname{lcp}(x,y)|$, then $x' \xleftarrow[l]{} y'$ implies $x' \underset{n\,R}{\equiv} y'$. There are four separate cases to consider.

1. $|x| + |y| - 2\,|\operatorname{lcp}(x,y)| = 0$ if and only if $x = y$. In this case the result is trivially true since $\underset{n\,R}{\equiv}$ is reflexive.

2. Suppose x is a proper prefix of y, that is, $y = xz$ for some $z \in A^+$.

   (a) If $\#\alpha(z) = 1$ then $z = a^r$ for some $a \in A$, $r \geqslant 1$. Since $y = xz = xaa^{r-1}$ there exist $u,v \in A^*$ such that $x = uav$ and $u \underset{l-1}{\sim} x$. Lemma 5 implies that there exist $u_1, \ldots, u_{l-1} \in A^*$ such that $u = u_1 \cdots u_{l-1}$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_{l-1}) \supseteq \alpha(av)$. Let

$u_l = av$. Now $\alpha(u_l) \supseteq \alpha(z)$ and $l = (n-1)m+1 > (n-1)(\#\alpha(u_1)-\#\alpha(z)+1)$ so, by Lemma 58, $x \underset{n\,R}{\equiv} xz = y$, as required.

(b) Otherwise $\#\alpha(z) \geqslant 2$. From Proposition 51 $x \underset{l-1\,R}{\sim} y = xz$ so, employing Lemma 11, there exist $u_1, \ldots, u_{l-1} \in A^*$ such that $x = u_1 \cdots u_{l-1}$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_{l-1}) \supseteq \alpha(z)$. Since $n \geqslant 2$, $\#\alpha(u_1) \leqslant m$, and $\#\alpha(z) \geqslant 2$, $l-1 = (n-1)m > (n-1)(\#\alpha(u_1)-\#\alpha(z)+1)$ so $x \underset{n\,R}{\equiv} xz = y$ by Lemma 58.

3. If y is a proper prefix of x the result follows from 2 and the fact that $\underset{l}{\leftarrow}$ and $\underset{n\,R}{\equiv}$ are symmetric.

4. Otherwise let $u = \mathrm{lcp}(x,y)$. Then $x = uav$ and $y = ubw$ where $v,w \in A^*$, $a,b \in A$, and $a \neq b$. Since $x \underset{l}{\leftarrow} y$ there exist $x_1,x_2,y_1,y_2 \in A^*$ such that $y = y_1ay_2$, $x = x_1bx_2$, $y_1 \underset{l-1}{\sim} u$, and $x_1 \underset{l-1}{\sim} u$.

(a) If y_1a is a prefix of u then by Lemma 13 $u \underset{l\,R}{\sim} ua$, so from Propositions 23, 52 and 59 $u \underset{l}{\leftarrow} ua$ and $u \underset{n\,R}{\equiv} ua$. Since $\underset{l}{\leftarrow}$ and $\underset{n\,R}{\equiv}$ are congruences, $uv \underset{l}{\leftarrow} uav = x \underset{l}{\leftarrow} y$ and $uv \underset{n\,R}{\equiv} uav = x$. Now $|uv| + |y| - 2\,|\mathrm{lcp}\,(uv,y)| < |x| + |y| - 2\,|\mathrm{lcp}\,(x,y)|$ so by the induction hypothesis $uv \underset{n\,R}{\equiv} y$, and hence $x \underset{n\,R}{\equiv} y$.

(b) If x_1b is a prefix of u, then using the same arguments as above, $x \underset{n\,R}{\equiv} y$.

(c) Otherwise ub is a prefix of y_1 and ua is a prefix of x_1, say $y_1 = uby_3$ and $x_1 = uax_3$. Since $u \underset{l-1}{\sim} y_1 = uby_3$ and $u \underset{l-1}{\sim} x_1 = uax_3$, $u \underset{l-1}{\sim} uax_3by_3$. By Lemma 5, there exist $u_1, \ldots, u_{l-1} \in A^*$ such that $u = u_1 \cdots u_{l-1}$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_{l-1}) \supseteq \alpha(ax_3by_3)$. Now $\#\alpha(ax_3by_3) \geqslant 2$, and $n \geqslant 2$, and $\#\alpha(u_1) \leqslant m$, so $l-1 = (n-1)m > (n-1)(\#\alpha(u_1)-\#\alpha(ax_3by_3)+1)$. Hence, by Lemma 58, $u \underset{n\,R}{\equiv} uz$ for all $z \in (\alpha(ax_3by_3))^*$.

Let $x' = ubx_3ax_2$. Since $bx_3a, ax_3b \in (\alpha(ax_3by_3))^*$, $ubx_3a \underset{n\,R}{\equiv} u \underset{n\,R}{\equiv} uax_3b$, so that $x = uax_3bx_2 \underset{n\,R}{\equiv} ubx_3ax_2 = x'$. Now $\alpha(ax_3b) = \alpha(bx_3a)$ and $uc \underset{l-1}{\sim} u$ for all $c \in \alpha(ax_3b)$ since $u \underset{l-1}{\sim} uax_3by_3$, so by Lemma 61 $uax_3b \underset{l}{\leftarrow} ubx_3a$. Therefore $x = uax_3bx_2 \underset{l}{\leftarrow} ubx_3ax_2 = x'$.

But $x \underset{l}{\leftarrow} y$, so $x' \underset{l}{\leftarrow} y$. Since $|\mathrm{lcp}(x',y)| > |\mathrm{lcp}(x,y)|$ it follows that

$|x'| + |y| - 2\,|\mathrm{lcp}(x',y)| \; < \; |x| + |y| - 2\,|\mathrm{lcp}(x,y)|$. Hence by the induction hypothesis $x' \equiv_{nR} y$ and thus $x \equiv_{nR} y$.

Note that the above result is not true for $n = 1$. For example, $ab \leftarrow_{1} ba$ but $ab \not\equiv_{1R} ba$. Also, $x \leftarrow_{(n-1)m} y$ does not imply $x \equiv_{nR} y$. Otherwise from Propositions 23, 52, and 55, it follows that $x_{\;(n-1)\widetilde{m}\,R}\; y$ implies x *nm*1*mtwildr* y implies $x \leftarrow_{(n-1)m} y$ implies $x \equiv_{nR} y$ implies $x =_{nR} y$, contradicting Proposition 60.

The relationships between the various congruences can be conveniently summarized in the following diagram:

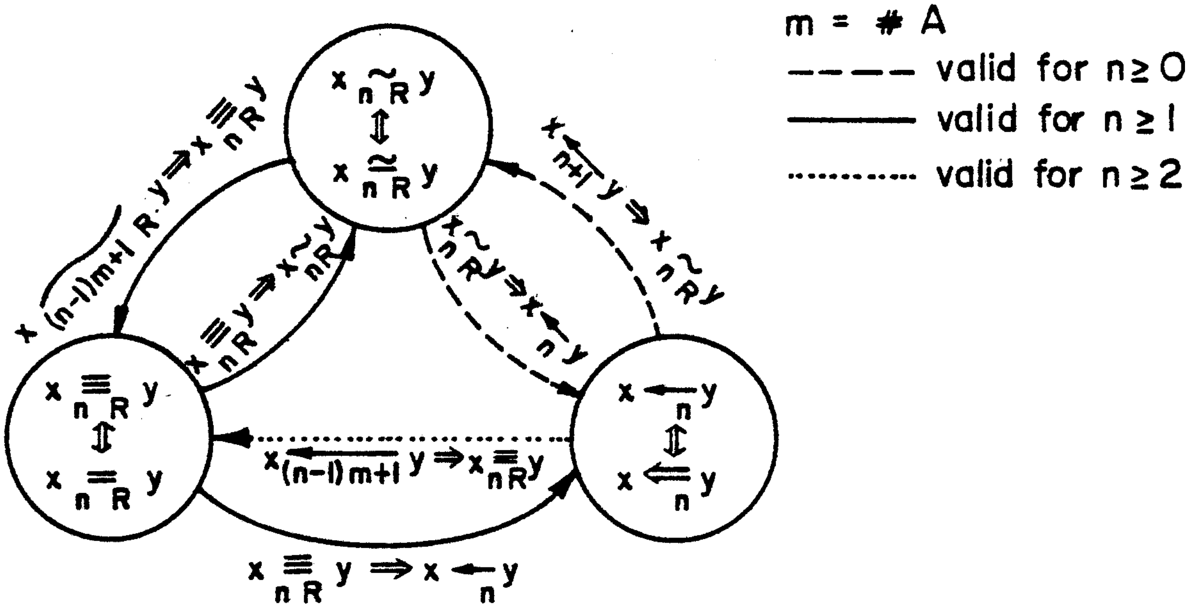

Figure 5

There is one further congruence which should be mentioned. In [5] Brzozowski describes a congruence $\oplus_{\bar{n}}$ which he proves characterizes the family of languages of R-trivial monoids over a two-letter alphabet. It is routine to verify that, in this case, $x \equiv_{nR} y$ implies $x \oplus_{\bar{n}} y$, and that $x \oplus_{\overline{2n}} y$ implies $x \equiv_{nR} y$ for all $x,y \in A^*$. However, for an alphabet of three or more letters, $\oplus_{\bar{n}}$ no longer 'works'.

Proposition 64 Let $\# \mathrm{A} \geqslant 3$. There does not exist $n \geqslant 1$ such that $x \oplus_{\overline{n}} y$ implies $x \sim_{1R} y$ for all $x,y \in \mathrm{A}^*$

Proof: Consider $x = (ab)^n$ and $y = (ab)^n c$. From the definition of $\oplus_{\overline{n}}$ it follows easily that $x \oplus_{\overline{n}} y$. However it is clear that $x \not\sim_{1R} y$ since $\alpha(x) \neq \alpha(y)$.

2.7 Summary

Theorem 65 Let $\mathrm{X} \subseteq \mathrm{A}^*$ be a regular language, let M be its syntactic monoid, and let $\mathbf{A} = <\mathrm{A},\mathrm{Q},q_0,\mathrm{F},\sigma>$ be the reduced automaton accepting X. The following conditions are equivalent.

M1. M is R-trivial.

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

M3. For all idempotents $e \in \mathrm{M}$, $e\mathrm{M}_e = e$.

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

X1. X is an $\underset{n\ R}{\sim}$ language for some $n \geqslant 0$.

X2. X is an $\underset{n\ R}{\simeq}$ language for some $n \geqslant 0$.

X3. X is an $\underset{n}{\leftharpoondown}$ language for some $n \geqslant 0$.

X4. X is an $\underset{n}{\Leftarrow}$ language for some $n \geqslant 0$.

X5. X is an $\underset{n\ R}{\equiv}$ language for some $n \geqslant 1$.

X6. X is an $\underset{n\ R}{=}$ language for some $n \geqslant 1$.

E1. X can be denoted by an R-expression.

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

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

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

A3. $\Pi^n(\mathbf{A})$ has an empty state set for some $n \geqslant 0$.

A4. There exists an $n > 0$ such that for all $x,y \in \mathrm{A}^*$, x n-full and $\alpha(x) \supseteq \alpha(y)$ imply $\sigma(q,x) = \sigma(q,xy)$ for all $q \in \mathrm{Q}$.

A5. For all $x \in \mathrm{A}^*$, $\sigma(q,x) = \sigma(q,xx)$ for all $q \in \mathrm{Q}$ implies $\sigma(q,x) = \sigma(q,xa)$ for all $q \in \mathrm{Q}$, $a \in \alpha(x)$.

A6. $\mathbf{A}$ is covered by a cascade product of half-resets.

CHAPTER 3 LANGUAGES OF L-TRIVIAL MONOIDS

The L-trivial property is dual to that of R-trivialness. As a result, characterizations analogous to those in Theorem 2.65 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 $x \underset{nL}{\sim} y$ if and only if for each suffix u of x there exists a suffix v of y such that $u \underset{n}{\sim} v$ and vice versa. The five other congruences ($\underset{nL}{\simeq}$, $\underset{n}{\rightarrow}$, $\underset{n}{\Rightarrow}$, $\underset{nL}{\equiv}$, and $\underset{nL}{=}$) have similarly modified definitions.

If A is the automaton of a language X with an L-trivial syntactic monoid then A^ρ, the automaton recognizing X^ρ, is partially ordered. However it is possible to describe these automata more directly.

Proposition 1 Let $S = <A, Q, \sigma>$ be a semiautomaton and let M be its transformation monoid. The following are equivalent.

1. M is L-trivial.
2. There exists an $n > 0$ such that, for all subsemiautomata $T = <C, P, p_{0,} \tau>$ of S which are connected and all n-full words w with $\alpha(w) = C$, $\tau(p,w) = \tau(p',w)$ for all $p,p' \in P$.
3. There exists an $n > 0$ such that for all $x,y \in A^*$, x n-full and $\alpha(x) \supseteq \alpha(y)$ imply $\sigma(q,yx) = \sigma(q,x)$ for all $q \in Q$.
4. 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⇒2) Suppose M is L-trivial. By the dual of Lemma 2.25 there exists an $n > 0$ such that for all $x,y \in A^*$, $x \underset{n}{\sim} yx$ implies $\underline{x} = \underline{yx}$. Let $T = <C, P, p_0, \tau>$ be a subsemiautomaton of S which is connected, let $p,p' \in P$, and let w be an n-full word with $\alpha(w) = C$.

Since 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 $uw \underset{n}{\sim} w$ and $vw \underset{n}{\sim} w$. This implies that $\underline{uw} = \underline{w} = \underline{vw}$ and thus $\tau(p,w) = \tau(p_0,uw) = \sigma(p_0,uw) = \sigma(p_0,vw) = \tau(p_0,vw) = \tau(p',w)$.

($2 \Rightarrow 3$) Let $n > 0$ be such that, for all subsemiautomata $T = \langle C, P, p_0, \tau \rangle$ of S which are connected and all n-full words w with $\alpha(w) = C$, $\tau(p,w) = \tau(p',w)$ for all $p,p' \in P$. Suppose x is n-full and $\alpha(x) \supseteq \alpha(y)$. Let $q \in Q$. Consider the subsemiautomaton $T = \langle C,P, q, \tau \rangle$ of S where P is chosen so that T is connected. Since $\alpha(x) \supseteq \alpha(y)$, $\tau(q,y) \in P$. And, because x is n-full, it follows that $\sigma(q,yx) = \tau(q,yx) = \tau(\tau(q,y), x) = \tau(q,x) = \sigma(q,x)$.

The proofs of ($3 \Rightarrow 4$) and ($4 \Rightarrow 1$) are the dual of those in Proposition 2.28.

Proposition 2 Let $S = \langle A, Q, \sigma \rangle$ be a semiautomaton and let M be its transformation monoid. If M is L-trivial then for all $x,y \in A^*$, $q \in Q$, $\sigma(q,x) = \sigma(q,xx) = \sigma(q,xy)$ and $\sigma(q,y) = \sigma(q,yy) = \sigma(q,yx)$ imply $\sigma(q,x) = \sigma(q,y)$.

Proof: Suppose M is L-trivial. Let $x,y \in A^*$, $q \in Q$, be such that $\sigma(q,x) = \sigma(q,xx) = \sigma(q,xy)$ and $\sigma(q,y) = \sigma(q,yy) = \sigma(q,yx)$. Then $\sigma(q, (xy)^n) = \sigma(q,x)$ and $\sigma(q, (yx)^n) = \sigma(q,y)$ for all $n > 0$.

Since M is L-trivial, it follows from Proposition 1 that there exists an $n > 0$ such that for all $x,y \in A^*$, x n-full and $\alpha(x) \supseteq \alpha(y)$ imply $\sigma(q,yx) = \sigma(q,x)$ for all $q \in Q$. Now $(xy)^n$ is n-full and $\alpha((xy)^n) \supseteq \alpha(y)$ so $\sigma(q,x) = \sigma(q, (xy)^n) = \sigma(q,y(xy)^n) = \sigma(q, (yx)^n y) = \sigma(\sigma(q, (yx)^n), y) = \sigma(\sigma(q,y), y) = \sigma(q,yy) = \sigma(q,y)$.

Note that these automata do not satisfy the property that for all $x,y \in A^*$ and all $q \in Q$, $\sigma(q,yx) = q$ implies $\sigma(q,x) = q$. For example, consider the semiautomaton $\langle \{a,b\}, \{q_0,q_1,q_2\}, \sigma \rangle$ illustrated in Figure 1.

It is easily verified that this automaton satisfies $\sigma(q,yx) = \sigma(q,x)$ for all $q \in Q$ and all $x,y \in A^*$ such that x is 2-full and $\alpha(x) \supseteq \alpha(y)$. However $\sigma(q_0,aba) = q_0 \neq q_2 = \sigma(q_0,a)$.

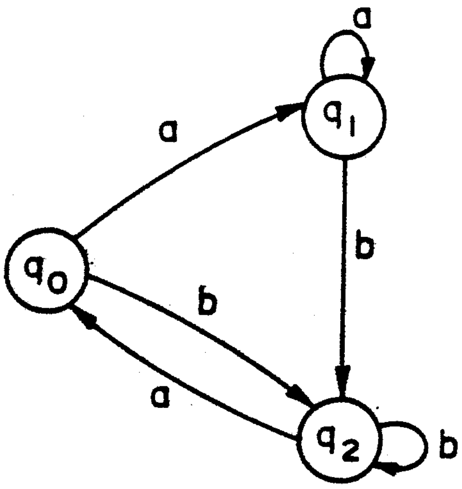

Figure 1

The final theorem, analogous to Theorem 2.65, summarizes the characterizations of languages with L-trivial monoids.

Theorem 3 Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $\mathrm{A} = <A, Q, q_0, F, \sigma>$ and A^ρ be the reduced automata accepting X and X^ρ respectively. The following conditions are equivalent.

M1. M is 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 $\underset{n\,L}{\sim}$ language for some $n \geqslant 0$.

X2. X is an $\underset{n\,L}{\approxeq}$ language for some $n \geqslant 0$.

X3. X is an $\rightarrow_n$ language for some $n \geqslant 0$.

X4. X is an $\Rightarrow_n$ language for some $n \geqslant 0$.

X5. X is an $\underset{n\,L}{\equiv}$ language for some $n \geqslant 1$.

X6. X is an $\underset{n\,L}{=}$ language for some $n \geqslant 1$.

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 $m \geqslant 0$, $a_1, \ldots, a_m \in \mathrm{A}$ and $\mathrm{A}_i \subseteq \mathrm{A} - \{a_i\}$ for $1 \leqslant i \leqslant m$.

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

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

A2. There exists an $n > 0$ such that for all subsemiautomata $\mathrm{T} = <\mathrm{C}, \mathrm{P}, p_0, \tau>$ of A which are connected and all n-full words w with $\alpha(w) = \mathrm{C}$, $\tau(p,w) = \tau(p',w)$ for all $p,\ p' \in \mathrm{P}$.

A3. There exists an $n > 0$ such that for all $x,y \in \mathrm{A}^*$, x n-full and $\alpha(x) \supseteq \alpha(y)$ imply $\sigma(q,yx) = \sigma(q,x)$ for all $q \in \mathrm{Q}$.

A4. If $x \in \mathrm{A}^*$ then $\sigma(q,x) = \sigma(q,xx)$ for all $q \in \mathrm{Q}$ implies $\sigma(q,x) = \sigma(q,ax)$ for all $q \in \mathrm{Q}$, $a \in \alpha(x)$.

A5. $\mathbf{A}^\rho$ is covered by a cascade product of half-resets.

CHAPTER 4 LANGUAGES OF *G*-TRIVIAL MONOIDS

4.1 Basic Congruences

In order to produce a congruence which is a generalization of the congruences in the previous two chapters, it is necessary to make both prefixes and suffixes significant in its definition.

Definition 1 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \overset{\cdot}{\equiv}_{nG} y$ if and only if there exist $z_1,z_2,u,v,w \in A^*$ such that $x = z_1uwz_2$, $y = z_1uvwz_2$, u and w are n-full, and $\alpha(u) = \alpha(w) \supseteq \alpha(v)$. $\overset{*}{\equiv}_{nG}$ is the transitive closure of $\overset{\cdot}{\equiv}_{nG}$, and $\equiv_{nG}$ is the symmetric transitive closure of $\overset{\cdot}{\equiv}_{nG}$.

Note that $\equiv_{nG}$ is the smallest congruence satisfying $uw \equiv_{nG} uvw$ for all $u,v,w \in A^*$ such that u and w are n-full and $\alpha(u) = \alpha(w) \supseteq \alpha(v)$.

Definition 2 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \doteq_{nG} y$ if and only if there exist $z_1,z_2,u,v,w \in A^*$ such that $x = z_1uwz_2$, $y = z_1uvwz_2$, u and w are n-full, and $\alpha(u) = \alpha(w) = \alpha(v)$. $=_{nG}$ is the symmetric transitive closure of $\doteq_{nG}$.

Similarly $=_{nG}$ is the smallest congruence satisfying $uw =_{nG} uvw$ for all $u,v,w \in A^*$ such that u and w are n-full and $\alpha(u) = \alpha(w) = \alpha(v)$.

Definition 3 Let $n \geqslant 1$. Then $\approx_{nG}$ is the smallest congruence satisfying $u \approx_{nG} uvu$ for all $u,v \in A^*$ such that u is n-full and $\alpha(u) \supseteq \alpha(v)$.

If u is $(n+1)$-full then it is also n-full. Hence $x \equiv_{n+1G} y$ implies $x \equiv_{nG} y$, $x =_{n+1G} y$ implies $x =_{nG} y$, and $x \approx_{n+1G} y$ implies $x \approx_{nG} y$ for all $x,y \in A^*$ and all $n \geqslant 1$.

Proposition 4 Let $n \geqslant 1$ and $u,v \in A^*$ be such that $\alpha(u) \supseteq \alpha(v)$. Then

(a) $u^{2n} =_{nG} u^{2n+1}$,

(b) $u^{2n} \underset{nG}{\equiv} u^{2n}vu^{2n}$,

(c) $u^n \underset{nG}{\approxeq} u^{n+1}$, and

(d) $u^n \underset{nG}{\approxeq} u^nvu^n$.

Proof: (a) and (d) follow immediately from the fact that u^n is n-full. Since $u^{2n} = u^nu^n \underset{nG}{\equiv} u^nu^{2n}u^n = u^nu^nu^nu^n \underset{nG}{\equiv} u^nu^nvu^nu^n = u^{2n}vu^{2n}$ and $u^n \underset{nG}{\approxeq} u^nu^n \underset{nG}{\approxeq} u^nu^2u^n = u^{n+1}u^{n+1} \underset{nG}{\approxeq} u^{n+1}$, (b) and (c) hold.

These three congruences are closely related. In fact, the families of languages $\{X \mid X$ is a $\underset{nG}{\equiv}$ language for some $n \geqslant 1\}$, $\{X \mid X$ is a $\underset{nG}{=}$ language for some $n \geqslant 1\}$, and $\{X \mid X$ is a $\underset{nG}{\approxeq}$ language for some $n \geqslant 1\}$ are the same.

Proposition 5 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{nG}{\equiv} y$ if and only if $x \underset{nG}{=} y$.

Proof: Clearly $x \underset{nG}{=} y$ implies $x \underset{nG}{\equiv} y$, so suppose $x \underset{nG}{\doteqdot} y$. Then there exist $z_1,z_2,u,v,w \in A^*$ such that $x = z_1uwz_2$, $y = z_1uvwz_2$, u and w are n-full, and $\alpha(u) = \alpha(w) \supseteq \alpha(v)$. Now $\alpha(u) = \alpha(w) = \alpha(uv) = \alpha(vw)$ and vw is n-full, so $x = z_1uwz_2 \underset{nG}{\doteq} z_1u(uv)wz_2$ and $y = z_1u(vw)z_2 \underset{nG}{\doteq} z_1uu(vw)z_2$. Therefore $x \underset{nG}{=} y$. Since $\underset{nG}{\equiv}$ is the symmetric transitive closure of $\underset{nG}{\doteqdot}$, it follows that $x \underset{nG}{\equiv} y$ implies $x \underset{nG}{=} y$.

Proposition 6 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{2nG}{\approxeq} y$ implies $x \underset{nG}{=} y$.

Proof: Suppose $u,v \in A^*$ are such that u is $2n$-full and $\alpha(u) \supseteq \alpha(v)$. From the remark following Definition 2.6 there exist $u_1, \ldots, u_{2n} \in A^*$ such that $u = u_1 \cdots u_{2n}$ and $\alpha(u_1) = \cdots = \alpha(u_{2n})$. Let $u' = u_1 \cdots u_n$ and $u'' = u_{n+1} \cdots u_{2n}$. Then u' and u'' are n-full, $u = u'u''$, and $\alpha(u') = \alpha(u'') = \alpha(u''vu')$. Thus $u = u'u'' \underset{nG}{=} u'(u''vu')u'' = uvu$. Since $\underset{2nG}{\approxeq}$ is the smallest congruence satisfying $u \underset{2nG}{\approxeq} uvu$ for all $u,v \in A^*$ such that u is $2n$-full and $\alpha(u) \supseteq \alpha(v)$, it follows that $x \underset{2nG}{\approxeq} y$ implies $x \underset{nG}{=} y$ for all $x,y \in A^*$.

Proposition 7 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{nG}{\equiv} y$ implies $x \underset{nG}{\approxeq} y$.

Proof: Let $u,v,w \in A^*$ be such that u and w are n-full and $\alpha(u) = \alpha(w) \supseteq \alpha(v)$. Since $\alpha(u) \supseteq \alpha(wuvw)$, $u \underset{nG}{\overset{\sim}{\approx}} uwuvwu$. But $u \underset{nG}{\overset{\sim}{\approx}} uwu$, $w \underset{nG}{\overset{\sim}{\approx}} wuw$, and $\underset{nG}{\overset{\sim}{\approx}}$ is a congruence; thus $uw \underset{nG}{\overset{\sim}{\approx}} uwuvwuw \underset{nG}{\overset{\sim}{\approx}} uvw$. Since $\underset{nG}{\equiv}$ is the smallest congruence satisfying $uw \underset{nG}{\equiv} uvw$ for all $u,v,w \in A^*$ such that u and w are n-full and $\alpha(u) = \alpha(w) \supseteq \alpha(v)$ it follows that $x \underset{nG}{\equiv} y$ implies $x \underset{nG}{\overset{\sim}{\approx}} y$ for all $x,y \in A^*$.

Like $\underset{nR}{\sim}$ and $\underset{nL}{\sim}$, every congruence class of $\underset{nG}{\equiv}$ has a unique element of minimal length. This is now shown.

Lemma 8 If $n \geqslant 1$ and $x,x',x'' \in A^*$ are such that $x \underset{nG}{\dot{\equiv}} x''$ and $x' \underset{nG}{\dot{\equiv}} x''$, then there exists $x_0 \in A^*$ such that $x_0 \underset{nG}{\dot{\equiv}} x$ and $x_0 \underset{nG}{\dot{\equiv}} x'$.

Proof: Suppose $x,x',x'' \in A^*$ are such that $x \underset{nG}{\dot{\equiv}} x''$ and $x' \underset{nG}{\dot{\equiv}} x''$. Then there exist $u,u',v,v',w,w',z_1,z'_1,z_2,z'_2 \in A^*$ such that $x = z_1uwz_2$, $x' = z'_1u'w'z'_2$, $z_1uvwz_2 = x'' = z'_1u'v'w'z'_2$, $\alpha(u) = \alpha(w) \supseteq \alpha(v)$, $\alpha(u') = \alpha(w') \supseteq \alpha(v')$, and u, u', w, and w' are n-full.

The proof proceeds by considering various cases.

1. z'_1u' is a prefix of z_1u.

1.1 z_1uv is a prefix of $z'_1u'v'$.

Here $z_1u = z'_1u'r$ and $wz_2 = sw'z'_2$ for some $r;s \in A^*$. Then $z'_1u'v'w'z'_2 = z_1uvwz_2 = z'_1u'rvsw'z'_2$ so that $v' = rvs$. Let $x_0 = x'$. Since $\alpha(u') = \alpha(w') \supseteq \alpha(v') \supseteq \alpha(rs)$, $x_0 = z'_1u'w'z'_2 \underset{nG}{\dot{\equiv}} z'_1u'rsw'z'_2 = z_1uwz_2 = x$. And, since $\underset{nG}{\dot{\equiv}}$ is reflexive, $x_0 \underset{nG}{\dot{\equiv}} x'$.

1.2 $z'_1u'v'$ is a prefix of z_1uv.

1.2.1 $z'_1u'v'$ is a prefix of z_1u.

Since u is n-full, there exist $u_1, \ldots, u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) = \cdots = \alpha(u_n)$. If $z'_1 = z_1q$ for some $q \in A^*$, then $z_1qu'v' = z'_1u'v'$ is a prefix of z_1u in which case $\alpha(u') \subseteq \alpha(u)$. Otherwise $z_1 = z'_1q$ for some $q \in A^*$. Hence, if $z_1u_1 = z'_1qu_1$ is a prefix of $z'_1u'v'w'$, then $\alpha(u) = \alpha(u_1) \subseteq \alpha(u'v'w') = \alpha(u')$. Thus $\alpha(u) \not\subseteq \alpha(u')$ and $\alpha(u') \not\subseteq \alpha(u)$ imply that $z'_1u'v'w'$ is a prefix of z_1u_1.

1.2.1.1 $z'_1u'v'w'$ is a prefix of z_1u_1.

There exists $r' \in A^*$ such that $z'_1u'v'w'r' = z_1u_1$ and $z'_2 = r'u_2 \cdots u_nvwz_2$.

1.2.1.1.1 $z'_1u'v'$ is a prefix of z_1.

Let $s' \in A^*$ be such that $z_1 = z'_1u'v's'$ and $s'u_1 = w'r'$, let $r_1 = z'_1u's'$, and let $r_2 = u_1$. Then $z'_1u'w'r' = z'_1u's'u_1 = r_1r_2$ and $\alpha(r_2) = \alpha(u_1)$.

1.2.1.1.2 z_1 is a prefix of z'_1u'.

Let $s' \in A^*$ be such that $z'_1u' = z_1s'$ and $s'v'w'r' = u_1$, let $r_1 = z_1$, and let $r_2 = s'w'r'$. Then $z'_1u'w'r' = z_1s'w'r' = r_1r_2$ and, since $\alpha(v') \subseteq \alpha(w')$, $\alpha(r_2) = \alpha(s'w'r') = \alpha(s'v'w'r') = \alpha(u_1)$.

1.2.1.1.3 z_1 is a prefix of $z'_1u'v'$ and z'_1u' is a prefix of z_1.

Let $s,s' \in A^*$ be such that $z_1 = z'_1u's$, $u_1 = s'w'r'$ and $v' = ss'$, let $r_1 = z'_1u'$, and let $r_2 = w'r'$. Then $z'_1u'w'r' = r_1r_2$ and, since $\alpha(s') \subseteq \alpha(v') \subseteq \alpha(w')$, $\alpha(r_2) = \alpha(w'r') = \alpha(s'w'r') = \alpha(u_1)$.

In all three cases there exist $r_1,r_2 \in A^*$ such that $z'_1u'w'r' = r_1r_2$ and $\alpha(r_2) = \alpha(u_1)$. Note that $r_2u_2 \cdots u_n$ is n-full and $\alpha(r_2u_2 \cdots u_n) = \alpha(u_1 \cdots u_n) = \alpha(u) = \alpha(w)$. Let $x_0 = z'_1u'w'r'u_2 \cdots u_nwz_2$. Then $x_0 = z'_1u'w'r'u_2 \cdots u_nwz_2 \underset{nG}{\equiv} z'_1u'v'w'r'u_2 \cdots u_nwz_2 = z_1uwz_2 = x$ and $x_0 = z'_1u'w'r'u_2 \cdots u_nwz_2 = r_1r_2u_2 \cdots u_nwz_2 \underset{nG}{\equiv} r_1r_2u_2 \cdots u_nvwz_2 = z'_1u'w'r'u_2 \cdots u_nvwz_2 = z'_1u'w'z'_2 = x'$.

1.2.1.2 $\alpha(u) = \alpha(u')$.

1.2.1.2.1 $z'_1u'v'w'$ is a prefix of z_1.

This is a special case of 1.2.1.1.

1.2.1.2.2 z_1u is a prefix of $z'_1u'v'w'$.

Since $z'_1u'v'$ is a prefix of z_1u, there exists $p \in A^*$ such that $z'_1u'v'p = z_1u$ and $w'z'_2 = pvwz_2$. But z_1u is a prefix of $z'_1u'v'w'$; thus p is a prefix of w'. Let $x_0 = z'_1u'wz_2$. Now $\alpha(p) \subseteq \alpha(w') = \alpha(u') =$

$\alpha(w)$, so that $\alpha(v'p), \alpha(pv) \subseteq \alpha(u')$. Hence $x_0 = z'_1u'wz_2 \;\dot{\equiv}_{nG}\; z'_1u'v'pwz_2 = z_1uwz_2 = x$ and $x_0 = z'_1u'wz_2 \;\dot{\equiv}_{nG}\; z'_1u'pvwz_2 = z'_1u'w'z'_2 = x'$.

1.2.1.2.3 z_1 is a prefix of $z'_1u'v'w'$ which is a prefix of z_1u.

In this case there exist $r,s \in A^*$ such that $z_1r = z'_1u'v'w'$, $z'_1u'v'w's = z_1u$, and $z'_2 = svwz_2$. Therefore $z_1rs = z_1u$ so that $\alpha(s) \subseteq \alpha(u) = \alpha(w) = \alpha(u')$. Let $x_0 = z'_1u'wz_2$. Then $x_0 = z'_1u'wz_2 \;\dot{\equiv}_{nG}\; z'_1u'(v'w's)wz_2 = z_1uwz_2 = x$ and $x_0 = z'_1u'wz_2 \;\dot{\equiv}_{nG}\; z'_1u'(w'sv)wz_2 = z'_1u'w'z'_2 = x'$.

1.2.1.3 $\alpha(u') \subsetneq \alpha(u)$.

This implies that $u'v'w'$ does not contain any u_i as a contiguous subword. The four subcases below consider the possible relationships between $u'v'w'$ and the u_i's.

1.2.1.3.1 $z'_1u'v'w'$ is a prefix of z_1u_1.

This is just case 1.2.1.1.

1.2.1.3.2 There exists i, $1 \leqslant i \leqslant n$, such that $z'_1 = z_1u_1 \cdots u_{i-1}r$, $z'_2 = su_{i+1} \cdots u_nvwz_2$, and $u_i = ru'v'w's$ for some $r,s \in A^*$.

Let $x_0 = z_1u_1 \cdots u_{i-1}ru'w'su_{i+1} \cdots u_nwz_2$. Since $\alpha(u') = \alpha(w') \supseteq \alpha(v')$ it follows that $\alpha(ru'w's) = \alpha(ru'v'w's) = \alpha(u_i)$. Therefore $u_1 \cdots u_{i-1}ru'w'su_{i+1} \cdots u_n$ is n-full and $\alpha(u_1 \cdots u_{i-1}ru'w'su_{i+1} \cdots u_n) = \alpha(u)$. Now this implies that $x_0 = z_1u_1 \cdots u_{i-1}ru'w'su_{i+1} \cdots u_nwz_2 \;\dot{\equiv}_{nG}\; z_1u_1 \cdots u_{i-1}ru'v'w'su_{i+1} \cdots u_nwz_2 = z_1u_1 \cdots u_{i-1}u_iu_{i+1} \cdots u_nwz_2 = z_1uwz_2 = x$ and $x_0 = z_1u_1 \cdots u_{i-1}ru'w'su_{i+1} \cdots u_nwz_2 \;\dot{\equiv}_{nG}\; z_1u_1 \cdots u_{i-1}ru'w'su_{i+1} \cdots u_nvwz_2 = z'_1u'w'z'_2 = x'$.

1.2.1.3.3 There exists i, $1 \leqslant i \leqslant n-1$, such that $u_iu_{i+1} = ru'v'w's$, $z'_1 = z_1u_1 \cdots u_{i-1}r$, and $z'_2 = su_{i+2} \cdots u_nvwz_2$ for some $r,s \in A^*$

Let $x_0 = z_1 u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n w z_2$.

1.2.1.3.3.1 $u_i = u'v'w'_1$ and $u_{i+1} = w'_2 s$ where $w' = w'_1 w'_2$.

Since $\alpha(v') \subseteq \alpha(u')$, $\alpha(ru'w'_1) = \alpha(ru'v'w'_1) = \alpha(u_i)$. In addition, $\alpha(w'_2) = \alpha(u_{i+1})$. Hence $u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n$ is n-full.

1.2.1.3.3.2 $u_i = ru'_1$, $u_{i+1} = u'_2 v' w' s$, and $u' = u'_1 u'_2$.

The proof is analogous to that of case 1.2.1.3.3.1.

1.2.1.3.3.3 $u_i = ru'v'_1$, $u_{i+1} = v'_2$, and $v' = v'_1 v'_2$.

Since $\alpha(u') \supseteq \alpha(v') \supseteq \alpha(v'_1)$, $\alpha(ru') = \alpha(ru'v'_1) = \alpha(u_i)$. Similarly, $\alpha(w's) = \alpha(u_{i+1})$. Thus $u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n$ is n-full.

In all three cases, $u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n$ is n-full. Clearly $\alpha(u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n) = \alpha(u) = \alpha(w)$. Therefore

$$
\begin{aligned}
x_0 &= z_1 u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n w z_2 \\
&\underset{nG}{\dot{\equiv}} z_1 u_1 \cdots u_{i-1} r u' v' w' s u_{i+2} \cdots u_n w z_2 \\
&= z_1 u_1 \cdots u_{i-1} u_i u_{i+1} u_{i+2} \cdots u_n w z_2 = z_1 u w z_2 = x
\end{aligned}
$$

and $x_0 = z_1 u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n w z_2$

$$\underset{nG}{\dot{\equiv}} z_1 u_1 \cdots u_{i-1} r u' w' s u_{i+2} \cdots u_n v w z_2 = z'_1 u' w' z'_2 = x'.$$

1.2.1.3.4 $u'v's$ is a suffix of u_n, for some prefix s of w', and $w'z'_2 = svwz_2$.

Since $u'v's$ is a suffix of u_n there exists $r \in A^*$ such that $u_n = ru'v's$ and $z'_1 = z_1 u_1 \cdots u_{n-1} r$. Since $\alpha(s), \alpha(v') \subseteq \alpha(w') = \alpha(u')$, $\alpha(ru') = \alpha(ru'v's) = \alpha(u_n)$. Hence $u_1 \cdots u_{n-1} r u'$ is n-full and $\alpha(u_1 \cdots u_{n-1} r u') = \alpha(w)$. Let $x_0 = z_1 u_1 \cdots u_{n-1} r u' w z_2$. Then $x_0 = z_1 u_1 \cdots u_{n-1} r u' w z_2 \underset{nG}{\dot{\equiv}} z_1 u_1 \cdots u_{n-1} r u' (sv) w z_2 = z'_1 u' w' z'_2 = x'$, since $\alpha(sv) \subseteq \alpha(w') \cup \alpha(v) \subseteq \alpha(w)$. Also $x_0 = z_1 u_1 \cdots u_{n-1} r u' w z_2 \underset{nG}{\dot{\equiv}} z_1 u_1 \cdots u_{n-1} r u' (v's) w z_2 = z_1 u_1 \cdots u_{n-1} u_n w z_2 = z_1 u w z_2 = x$, since $\alpha(v's) \subseteq \alpha(w') \subseteq \alpha(w)$.

1.2.1.4 $\alpha(u) \subsetneq \alpha(u')$.

Since $z'_1u'v'$ is a prefix of z_1u, vwz_2 is a suffix of $w'z'_2$. The result then follows by symmetry from case 1.2.1.3.

1.2.2 z_1u is a prefix of $z'_1u'v'$.

Here there exist $r,r' \in A^*$ such that r' is a prefix of v', r is a suffix of v, $z_1u = z'_1u'r'$, $r'vwz_2 = v'w'z'_2$, $z_1uv = z'_1u'v'r$, and $rwz_2 = w'z'_2$. Let $y'' = z_1urwz_2 = z'_1u'r'w'z_2$. Now $x \dot{\equiv}_{nG} y''$, $x' \dot{\equiv}_{nG} y''$, and $z'_1u'r'$ is a prefix of z_1u, so that the result follows from case 1.2.1.

2. z_1u is a prefix of z'_1u'.

This case is completely symmetric to case 1.

Proposition 9 Suppose $n \geqslant 1$ and $x \equiv_{nG} y$. If x is an element of its $\equiv_{nG}$ class with minimal length, then $x \overset{*}{\equiv}_{nG} y$.

Proof: If $x \equiv_{nG} y$, then there exist $m \geqslant 1$ and $z_0, z_1, \ldots, z_m \in A^*$ such that $x = z_0$, $y = z_m$ and, for $i = 1, \ldots, m$, either $z_{i-1} \dot{\equiv}_{nG} z_i$ or $z_i \dot{\equiv}_{nG} z_{i-1}$.

The proof proceeds by induction on m. If $m = 1$ then either $x \dot{\equiv}_{nG} y$ or $y \dot{\equiv}_{nG} x$. In the latter case, since x is minimal, $x = y$. Hence $x \dot{\equiv}_{nG} y$. Assume the result is true for $m-1$.

If $z_{i-1} \dot{\equiv}_{nG} z_i$ for $i = 1, \ldots, m$, then $x \overset{*}{\equiv}_{nG} y$ by definition. Otherwise there exists k, $0 \leqslant k \leqslant m-1$, such that $x \overset{*}{\equiv}_{nG} z_k$ but $z_k \not\dot{\equiv}_{nG} z_{k+1}$. Note that from the proof for $m = 1$, $x \dot{\equiv}_{nG} z_1$ so $k \geqslant 1$.

Since $z_{k+1} \dot{\equiv}_{nG} z_k$ and $z_{k-1} \dot{\equiv}_{nG} z_k$, it follows from Lemma 8 that there exists $z'_{k-1} \in A^*$ such that $z'_{k-1} \dot{\equiv}_{nG} z_{k+1}$ and $z'_{k-1} \dot{\equiv}_{nG} z_{k-1}$. Continuing inductively for $i = k-2, \ldots, 0$, since $z'_{i+1} \dot{\equiv}_{nG} z_{i+1}$ and $z_i \dot{\equiv}_{nG} z_{i+1}$, there exists $z'_i \in A^*$ such that $z'_i \dot{\equiv}_{nG} z'_{i+1}$ and $z'_i \dot{\equiv}_{nG} z_i$.

Let $z'_i = z_{i+1}$ for $i = k, \ldots, m-1$. Now $z'_0 \dot{\equiv}_{nG} z_0 = x$ and x is minimal, so $z'_0 = x$. Thus $z'_0, z'_1, \ldots, z'_{m-1}$ are such that $z'_0 = x$, $z'_{m-1} = z_m = y$, and, for $i = 1, \ldots, m-1$, either $z'_{i-1} \dot{\equiv}_{nG} z'_i$ or $z'_i \dot{\equiv}_{nG} z'_{i-1}$. By the induction hypothesis, $x \overset{*}{\equiv}_{nG} y$.

Corollary 10 Every congruence class of $\underset{nG}{\equiv}$, $n \geqslant 1$, contains a unique element of minimal length.

Proof: Suppose $n \geqslant 1$ and $x,y \in A^*$ are such that $x \underset{nG}{\equiv} y$ and x and y are both elements of minimal length. Hence $|x| = |y|$ and by Proposition 9 $x \underset{nG}{\overset{*}{\equiv}} y$. From Definition 1, if $z,z' \in A^*$ then $z \underset{nG}{\dot{\equiv}} z'$ implies $|z| \leqslant |z'|$, with equality if and only if $z = z'$. Since $\underset{nG}{\overset{*}{\equiv}}$ is the transitive closure of $\underset{nG}{\dot{\equiv}}$, it follows that $x = y$.

The following is an algorithm which, given x, transforms it into the unique minimal element of $[x]_{\underset{nG}{\equiv}}$.

Algorithm 11 Find the unique minimal element of $[x]_{\underset{nG}{\equiv}}$.

```
for each $C \subseteq \alpha(x)$ such that $C \neq \varnothing$ do
    for each decomposition $x = z_1 y z_2$ such that $y$ is $2n$-full, $\alpha(y) = C$, $t_1(z_1) \notin C$, and $f_1(z_2) \notin C$
    (note that $1 \notin C$) do
        let $u$ be the shortest prefix of $y$ such that $u$ is $n$-full and $\alpha(u) = \alpha(y)$.
        let $w$ be the shortest suffix of $y$ such that $w$ is $n$-full and $\alpha(w) = \alpha(y)$.
        let $v \in A^*$ be such that $y = uvw$.
        Replace $x$ by $z_1 u w z_2$. Note that since $uw \underset{nG}{\dot{\equiv}} uvw = y$, $z_1 u w z_2 \underset{nG}{\dot{\equiv}} x$.
```

By Lemma 8, the order in which 'pieces' are removed from a word is irrelevant. Also, it is clear that if $x = z_1 y z_2 = z'_1 y' z'_2$ where $\alpha(y) = \alpha(y')$ and $t_1(z_1)$, $f_1(z_2)$, $t_1(z'_1)$, $f_1(z'_2) \notin \alpha(y)$, then either $z'_1 y'$ is a proper prefix of z_1, $y' z'_2$ is a proper suffix of z_2, or $z_1 = z'_1$, $y = y'$, and $z_2 = z'_2$.

To prove the correctness of the algorithm it remains to be shown that if $x = z_1 uvwz_2$ cannot be written in the form $z'_1 u' v' w' z'_2$, where u' and v' are n-full and $\alpha(u) \neq \alpha(u') = \alpha(w') \supseteq \alpha(v') \neq \varnothing$, then neither can $z_1 uwz_2$.

Suppose x cannot be written in the above form but $z_1 uwz_2$ can. That is, $z_1 uwz_2 =$

$z'_1u'v'w'z'_2$ where u' and w' are n-full and $\alpha(u) \neq \alpha(u') = \alpha(w') \supseteq \alpha(v') \neq \varnothing$.

If $z'_1u'v'w'$ is a prefix of z_1u, say $z_1u = z'_1u'v'w'r$, then $x = z'_1u'v'w'vwz_2$ contrary to the assumption. Similarly $u'v'w'z'_2$ is not a suffix of wz_2. Therefore z_1u is a proper prefix of $z'_1u'v'w'$ and wz_2 is a proper suffix of $u'v'w'z'_2$ so that there exist $r,s \in \mathrm{A}^+$ such that $z'_1u'v'w' = z_1us$, $sz'_2 = wz_2$, $u'v'w'z'_2 = rwz_2$, and $z'_1r = z_1u$. Now $z'_1u'v'w' = z_1us = z'_1rs$ so that $u'v'w' = rs$.

If $\alpha(w) = \alpha(u) \not\subseteq \alpha(u') = \alpha(u'v'w') = \alpha(rs)$ then u is not a suffix of r and w is not a prefix of s. But this implies that r is a suffix of u and s is a prefix of w so that $\alpha(u) = \alpha(uw) \supseteq \alpha(rs) = \alpha(u'v'w')$.

Since u is the shortest n-full prefix of uvw which contains every letter in $\alpha(uvw)$ it follows that $u = u_1a_1 \cdots u_na_n$ where $u_1, \ldots, u_n \in \mathrm{A}^*$, $a_1, \ldots, a_n \in \mathrm{A}$ and $\alpha(u_i) \subsetneq \alpha(u_ia_i) = \alpha(u)$ for $i = 1, \ldots, n$. Similarly $w = b_1w_1 \cdots b_nw_n$ where $w_1, \ldots, w_n \in \mathrm{A}^*$, $b_1, \ldots, b_n \in \mathrm{A}$ and $\alpha(w_i) \subsetneq \alpha(b_iw_i) = \alpha(w) = \alpha(u)$ for $i = 1, \ldots, n$. However $\varnothing \neq \alpha(rs) \subsetneq \alpha(u) = \alpha(w)$; therefore r is a proper suffix of u_na_n and s is a proper prefix of b_1w_1.

Say $r = u'_na_n$ and $s = b_1w'_1$ where u'_n is a suffix of u_n and w'_1 is a prefix of w_1. Then $u'v'w' = rs = u'_na_nb_1w'_1$. Since $a_n \in \alpha(u'v'w') = \alpha(u') = \alpha(w') \supseteq \alpha(v')$ and $a_n \notin \alpha(u'_n)$, u'_na_n is a prefix of u'. Similarly $b_1w'_1$ is a suffix of w'. Therefore $u' = u'_na_n$, $w'' = b_1w'_1$, and $v' = 1$, contrary to the assumption that $\alpha(v') \neq \varnothing$. Hence $\alpha(u') \supseteq \alpha(u) \supseteq \alpha(v)$.

There are three cases to consider.

1. If $r = u'_1$ and $s = u'_2v'w'$, where $u' = u'_1u'_2$, let $u'' = u'_1vu'_2$, $v'' = v'$, and $w'' = w'$. Since $\alpha(v) \subseteq \alpha(u')$ it follows that $\alpha(u'') = \alpha(u') = \alpha(w'')$ and u'' is n-full. Then $x = z_1uvwz_2 = z'_1rvsz'_2 = z'_1u'_1vu'_2v'w'z'_2 = z'_1u''v''w''z'_2$ which contradicts the assumption that x cannot be written in this form.

2. If $r = u'v'_1$ and $s = v'_2w'$, where $v' = v'_1v'_2$, let $u'' = u'$, $v'' = v'_1vv'_2$ and $w'' = w'$. Since $\varnothing \neq \alpha(v') \subseteq \alpha(u')$ and $\alpha(v) \subseteq \alpha(u')$, $\varnothing \neq \alpha(v'') \subseteq \alpha(u'')$. Then $x = z_1uvwz_2 = z'_1rvsz'_2 = z'_1u'v'_1vv'_2w'z'_2 = z'_1u''v''w''z'_2$ which contradicts the assumption that x cannot be written in this form.

3. For $r = u'v'w'_1$ and $s = w'_2$ where $w' = w'_1w'_2$ the argument is similar to case 1.

Therefore if x cannot be written in the form $z'_1u'v'w'z'_2$, where u' and v' are n-full and $\alpha(u) = \alpha(u') = \alpha(w') \supseteq \alpha(v') \neq \emptyset$, then neither can z_1uwz_2.

Example Let $x = abaaacbccaab$ and $n = 1$.

Consider the non-empty subsets of $\alpha(x) = \{a,b,c\}$ in the following order: $\{a,b,c\}$, $\{a,b\}$, $\{b,c\}$, $\{a,c\}$, $\{a\}$, $\{b\}$, $\{c\}$. Let z_1uvwz_2 be any decomposition of x such that uw is 2-full and $\alpha(v) \subseteq \alpha(u) = \alpha(w)$. These decompositions are illustrated in the following table.

subset			decomposition of x			replace x by
	z_1	u	v	w	z_2	
$\{a,b,c\}$	1	*abaaac*	*bc*	*caab*	1	*abaaaccaab*
$\{a,b\}$						
$\{b,c\}$						
$\{a,c\}$	*ab*	*aaac*	1	*caa*	*b*	
$\{a\}$	*ab*	*a*	*a*	*a*	*ccaab*	*abaaccaab*
	abaacc	*a*	1	*a*	*b*	
$\{b\}$						
$\{c\}$	*abaa*	*c*	1	*c*	*aab*	

Therefore the unique minimal element $\underset{1G}{\equiv}$ congruent to *abaaacbccaab* is *abaaccaab*.

Proposition 12 Let $n \geqslant 1$ and let $\lambda_G(A,n) = \max\{|x| \mid x \in A^*$ and x is the unique minimal element of its $\underset{nG}{\equiv}$ class$\}$. Then $\underset{nG}{\equiv}$ is of finite index for any given alphabet A and, furthermore, $\lambda_G(A,n) = 2n\left(\dfrac{(2n)^{\#A}-1}{2n-1}\right)$.

Proof: By induction on #A.

If #A = 1, say A = $\{a\}$, then the $\underset{nG}{\equiv}$ classes are $\{1\}$, $\{a\}$, ... , $\{a^{2n-1}\}$ and $\{a^i \mid i \geqslant 2n\}$. Thus $\underset{nG}{\equiv}$ is of finite index on A and $\lambda(A,n) = 2n\left(\dfrac{(2n)^1-1}{2n-1}\right)$.

Assume the result is true for alphabets with cardinality #A − 1. For $a \in A$, let $y \in (A-\{a\})^*$ be such that y is the unique minimal element of $[y]_{\underset{nG}{\equiv}}$ and $|y| = \lambda_G(A-\{a\},n)$.

Suppose $x \in A^*$ is the unique minimal element of $[x]_{\underset{nG}{\equiv}}$. If x is not $2n$-full then there exist

$x_1, \ldots, x_{m+1} \in A^*$ and $a_1, \ldots, a_m \in A$ where $0 \leqslant m < 2n$, $x = x_1a_1 \cdots x_ma_mx_{m+1}$, $\alpha(x_ia_i) = \alpha(x)$ for all $i = 1, \ldots, m$, and $\alpha(x_i) \subsetneq \alpha(x)$ for $i = 1, \ldots, m+1$. Let $a_{m+1} \in \alpha(x) - \alpha(x_{m+1})$. Consider x_i where $1 \leqslant i \leqslant m+1$. If $|x_i| > |y|$ then there exists $x'_i \in (A - \{a_i\})^*$ such that $x'_i \equiv_{nG} x_i$ and $|x'_i| < |x_i|$. But $\equiv_{nG}$ is a congruence so $x_1a_1 \cdots a_{i-1}x'_ia_i \cdots x_{m+1} \equiv_{nG} x_1a_1 \cdots a_{i-1}x_ia_i \cdots x_{m+1} = x$. Since $|x_1a_1 \cdots a_{i-1}x'_ia_i \cdots x_{m+1}| < |x|$ this contradicts the fact that x is the minimal element of $[x]_{\equiv_{nG}}$. Therefore $|x_i| \leqslant |y|$ which implies $|x| \leqslant m + \sum_{i=1}^{m+1} |y| = m(1+|y|) < 2n(1+|y|)$.

Now consider the case when x is $2n$-full. Then there exist $x_1, \ldots, x_n, x'_1, \ldots, x'_n, z \in A^*$, and $a_1, \ldots, a_n, a'_1, \ldots, a'_n \in A$, such that $x = x_1a_1 \cdots x_na_nza'_nx'_n \cdots a'_1x'_1$ and $\alpha(x_i) \neq \alpha(x_ia_i) = \alpha(x) = \alpha(a'_ix'_i) \neq \alpha(x'_i)$ for $i = 1, \ldots, n$. As above, it follows that $|x_i|$, $|x'_i| \leqslant |y|$ for $i = 1, \ldots, n$. Since $x_1a_1 \cdots x_na_n$ and $a'_nx'_n \cdots a'_1x'_1$ are n-full and $\alpha(x_1a_1 \cdots x_na_n) = \alpha(a'_nx'_n \cdots a'_1x'_1) = \alpha(x) \supseteq \alpha(z)$, if $z \neq 1$ then $(x_1a_1 \cdots x_na_n)(a'_nx'_n \cdots a'_1x'_1) \equiv_{nG} x$. This contradicts the minimality of x. Thus $z = 1$, $|x| = \sum_{i=1}^{n} |x_ia_i| + |a'_ix'_i| \leqslant 2n(1+|y|)$, and, since x was an arbitrary minimal element, $\lambda_G(A,n) \leqslant 2n(1+|y|)$.

Let $x = (ya)^n(ay)^n$. If x is not the minimal element of $[x]_{\equiv_{nG}}$ then there exist $u, v, w, z_1, z_2 \in A^*$ such that $x = z_1uvwz_2$, u and w are n-full, and $\alpha(u) = \alpha(w) \supseteq \alpha(v) \neq \varnothing$. Now $(ya)^n$ is the shortest n-full prefix of x and $(ay)^n$ is the shortest n-full suffix of x containing all the letters in $\alpha(x)$; therefore $\alpha(uvw) \subsetneq \alpha(x)$. If $a \in \alpha(uvw)$ then $a \in \alpha(u)$ and $a \in \alpha(w)$ and, since $\alpha(v) \neq \varnothing$, it follows that $uvw = z_3ayaz_4$ for some $z_3, z_4 \in A^*$. But then $\alpha(uvw) \supseteq \alpha(ay) = \alpha(x)$, which is a contradiction. Therefore $\alpha(uvw) \subseteq \alpha(x) - \{a\}$, so that $y = z_5uvwz_6$ for some z_5, $z_6 \in A^*$. However this implies that $z_5uwz_6 \equiv_{nG} y$ which contradicts the fact that y is the minimal element of $[y]_{\equiv_{nG}}$.

Therefore x is the minimal element of $[x]_{\equiv_{nG}}$ and $\lambda_G(A,n) \geqslant |x| = 2n(1+|y|)$. Thus

$$\begin{aligned}\lambda_G(\mathrm{A},n) \geqslant 2n(1+|y|) &= 2n(\lambda_G(\mathrm{A}-\{a\},n)+1)\\ &= 2n\left(2n\left[\frac{(2n)^{\#\mathrm{A}-1}-1}{2n-1}\right]+1\right)\\ &= 2n\left(\frac{(2n)^{\#\mathrm{A}}-1}{2n-1}\right).\end{aligned}$$

Since there are only a finite number of words of length less than or equal to $\lambda_G(\mathrm{A},n)$ it follows that $\underset{nG}{\equiv}$ partitions A^* into a finite number of distinct congruence classes.

4.2 *G*-Trivial Monoids

Finite *J*-trivial, *R*-trivial, and *L*-trivial monoids are characterized by the properties $e\mathrm{M}_e \cup \mathrm{M}_e e = e$, $e\mathrm{M}_e = e$, and $\mathrm{M}_e e = e$, respectively, for all idempotents $e \in \mathrm{M}$. A natural generalization is the the following.

Definition 13 Let M be a finite monoid. Then M is *G-trivial* if and only if $e\mathrm{M}_e \cap \mathrm{M}_e e = e$ for all idempotents $e \in \mathrm{M}$.

As with the three other families of monoids there are various alternative characterizations for the family of *G*-trivial monoids.

Theorem 14 Let M be a finite monoid. The following conditions are equivalent.

1. M is *G*-trivial.
2. $e\mathrm{M}_e e = e$ for all idempotents $e \in \mathrm{M}$.
3. There exists an $n > 0$ such that for all $f_1, \ldots, f_m \in \mathrm{M}$ and all $g \in \{f_1, \ldots, f_m\}^*$, $(f_1 \cdots f_m)^n g (f_1 \cdots f_m)^n = (f_1 \cdots f_m)^n$.
4. For all $f,g,h,k \in \mathrm{M}$, $fghkf = f$ implies $fgkf = f$.

Proof:

(1⇒2) Suppose $e \in \mathrm{M}$ is idempotent and$f \in e\mathrm{M}_e e$. Then $f = ege$ for some $g \in \mathrm{M}_e$. But $e \in \mathrm{M}_e$ so eg, $ge \in \mathrm{M}_e$. Therefore $f = e(ge) \in e\mathrm{M}_e$ and $f = (eg)e \in \mathrm{M}_e e$ so that $f \in e\mathrm{M}_e \cap \mathrm{M}_e e$. Since M is *G*-trivial, $f = e$.

(2⇒1) Suppose $e \in \mathrm{M}$ is idempotent and $f \in e\mathrm{M}_e \cap \mathrm{M}_e e$. Then $f = eg = he$ for some $g,h \in \mathrm{M}_e$. Since e is idempotent, $f = eg = eeg = ehe \in e\mathrm{M}_e e$. Therefore $f = e$.

(2⇒3) Let $f_1, \ldots, f_m \in \mathrm{M}$ and let $g \in \{f_1, \ldots, f_m\}^*$. Since M is finite, there exists an $n > 0$ such that $e = (f_1 \cdots f_m)^n$ is idempotent. Now $f_1, \ldots, f_m \in \mathrm{P}_e$ so $g \in \mathrm{M}_e$. Thus $(f_1 \cdots f_m)^n g (f_1 \cdots f_m)^n = ege = e = (f_1 \cdots f_m)^n$.

(3⇒4) Let $f,g,h,k \in \mathrm{M}$ be such that $fghkf = f$. Then $f = (fghk)^n f$, so $fgkf =$

$[(fghk)^n]fgk[(fghk)^nf] = [(fghk)^n(fgk)(fghk)^n]f = (fghk)^nf = f.$

(4⇒2) Suppose $e \in M$ is idempotent and let $g \in M_e$. If $g = 1$ then $ege = ee = e$. Otherwise $g = g_1 \cdots g_m$ where $m \geqslant 1$ and $g_i \in P_e$ for $1 \leqslant i \leqslant m$. Since $g_i \in P_e$ there exist $f_i, h_i \in M$ such that $e = f_i g_i h_i$.

Now $e = eee = e(f_1 g_1 h_1)e = e1f_1(g_1h_1)e = eg_1h_1e$, so suppose $e = eg_1 \cdots g_i h_i e$ where $1 \leqslant i \leqslant m-1$. Then $e = ee = eg_1 \cdots g_i h_i ee = e(g_1 \cdots g_i)(h_i f_{i+1})(g_{i+1}h_{i+1})e = e(g_1 \cdots g_i)(g_{i+1}h_{i+1})e$. By induction, $e = eg_1 \cdots g_m h_m e$. Thus $e = e(g_1 \cdots g_m)h_m 1e = e(g_1 \cdots g_m)1e = ege$.

Definition 15 Let M be a monoid. Then $\equiv$ is the smallest congruence such that $f \equiv f^2$ and $fg \equiv gf$ for all $f,g \in M$.

Theorem 16 Let M be a finite monoid. M is *G*-trivial if and only if M is aperiodic and for all idempotents $e,f \in M$, $e \equiv f$ implies $MeM = MfM$.

Proof:

(⇒) Since M is finite there exists $n > 0$ such that f^n is idempotent for all $f \in M$. Let $f \in M$ and let $e = f^n$. Clearly $f \in M_e$ so $ef \in eM_e$ and $fe \in M_e e$. Since $ef = f^{n+1} = fe$, $f^{n+1} \in eM_e \cap M_e e = e$. Therefore $f^{n+1} = f^n$, i.e. M is aperiodic.

To prove that $e \equiv f$ implies $MeM = MfM$ for all idempotents $e,f \in M$ it is sufficient to show that for $g,h,k,l \in M$

1. if $e = ghk$ and $f = gh^2k$ are idempotent then $MeM = MfM$
2. if $e = ghkl$ and $f = gkhl$ are idempotent then $MeM = MfM$.

1. Since e is idempotent $e = ee^2e = e(ghk)(ghk)e = e(gh)(kg)(hk)e$. But M is *G*-trivial so $e = e(gh)(hk)e = efe$. Therefore $MeM = MefeM \subseteq MfM$. Similarly, $f = fff = f(gh)hkf$ so $f = f(gh)kf = fef$ and $MfM \subseteq MeM$. Thus $MeM = MfM$.

2. Since e is idempotent, $e = ee^2e = e(ghkl)(ghkl)e$. Because M is *G*-trivial it follows

that $e = egklghkle$, $e = egkhkle$, and finally $e = egkhle = efe$. Therefore $MeM \subseteq MfM$. By symmetry $MfM \subseteq MeM$; thus $MeM = MfM$.

$(\Leftarrow)$ Let $e \in M$ be idempotent and $f \in eM_e \cap M_e e$. Then $f = eg = he$ for some $g,h \in M_e$. If $g = 1$ then $f = e \equiv e$. Otherwise $g = g_1 \cdots g_m$ where $g_i \in P_e$ for $i = 1, \ldots, m$. For each i, $1 \leqslant i \leqslant m$, there exist $k_i, l_i \in M$ such that $e = k_i g_i l_i$. Then $f = eg = e^m g = e^m g_1 \cdots g_m \equiv (eg_1) \cdots (eg_m) = (k_1 g_1 l_1 g_1) \cdots (k_m g_m l_m g_m) \equiv (k_1 g_1 g_1 l_1) \cdots (k_m g_m g_m l_m) \equiv (k_1 g_1 l_1) \cdots (k_m g_m l_m) = e^m = e$. By assumption $MeM = MfM$.

M is finite; therefore there exists $n > 0$ such that k^n is idempotent for all $k \in M$. Since $e \in MeM = MfM = MegM$, there exist $k,l \in M$ such that $e = kegl = k^n e (gl)^n$. Then $e = k^n e (gl)^n = k^n e (gl)^n (gl)^n = e (gl)^n = egl (gl)^{n-1} \in egM = fM$. This implies $eM = fM$ because $f \in eM_e \subseteq eM$. Similarly $Me = Mf$.

Because M is finite and aperiodic, it is H-trivial; hence $f = e$. Therefore $eM_e \cap M_e e = e$.

An alternate proof of this theorem can be found in [5].

It is now possible to relate G-trivial monoids to the families of languages defined by the congruences in the previous section.

Proposition 17 If X is a $\sim$ language and there exists $n > 0$ such that for all $u, v \in A^*$, $\alpha(u) \supseteq \alpha(v)$ implies $u^n \sim u^n v u^n$ then the syntactic monoid, M, of X is G-trivial.

Proof: Let $f_1, \ldots, f_m \in M$ and let $g \in \{f_1, \ldots, f_m\}^*$. Then $g = f_{i_1} f_{i_2} \cdots f_{i_r}$ where $r \geqslant 0$ and $1 \leqslant i_j \leqslant m$ for $j = 1, \ldots, r$. Since the syntactic morphism is surjective, there exist $u_1, \ldots, u_m \in A^*$ such that $\underline{u_i} = f_i$ for $i = 1, \ldots, m$. Let $u = u_1 \cdots u_m$ and let $v = u_{i_1} \cdots u_{i_r}$.

Now $\alpha(u) \supseteq \alpha(v)$ so $u^n \sim u^n v u^n$. Since M is the syntactic monoid of X, $(f_1 \cdots f_m)^n g (f_1 \cdots f_m)^n = \underline{u^n v u^n} = \underline{u^n} = (f_1 \cdots f_m)^n$. By Theorem 14, M is G-trivial.

Lemma 18 Let M be a monoid and let $\phi : A^* \to M$ be a surjective morphism. Then $\alpha(x) \supseteq \alpha(y)$ implies $\phi(y) \in M_{\phi(x)}$ for all $x,y \in A^*$

Proof: If $y = 1$ then clearly $\phi(y) = 1 \in M_{\phi(x)}$. Otherwise $y = a_1 \cdots a_n$ for some $n > 0$ where $a_i \in A$. For $i = 1, \ldots, n$, $a_i \in \alpha(y) \subseteq \alpha(x)$ so $x = u_i a_i v_i$ for some $u_i, v_i \in A^*$ Since $\phi(x) = \phi(u_i)\phi(a_i)\phi(v_i)$, $\phi(a_i) \in P_{\phi(x)}$. Thus $\phi(y) = \phi(a_1) \cdots \phi(a_n) \in M_{\phi(x)}$.

Lemma 19 Let M be a finite *G*-trivial monoid and $\phi : A^* \to M$ be a surjective morphism. Let n be the cardinality of M and let $u, v \in A^*$ Then $u \underset{n}{\sim} uvu$ implies $\phi(u) = \phi(uvu)$.

Proof: Suppose $u \underset{n}{\sim} uvu$. By Lemma 2.5 there exist $u_1, \ldots, u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) = \cdots = \alpha(u_n) = \alpha(vu)$. Let $u_0 = 1$. By the choice of n, the elements $\phi(u_0)$, $\phi(u_0 u_1)$, . . . , $\phi(u_0 u_1 \cdots u_n)$ cannot all be distinct. Hence there exist i and j, $0 \leqslant i < j \leqslant n$, such that $\phi(u_0 u_1 \cdots u_i) = \phi(u_0 u_1 \cdots u_i u_{i+1} \cdots u_j)$.

Let $f = \phi(u_0 u_1 \cdots u_i)$, $g = \phi(u_{i+1} \cdots u_j)$, and $h = \phi(u_{j+1} \cdots u_n)$. Then $f = fg$ so $f = fg^m$ for all $m \geqslant 0$. Choose m such that g^m is idempotent. Now $\alpha(u_{j+1} \cdots u_n v u_0 \cdots u_i) \supseteq \alpha((u_{i+1} \cdots u_j)^m)$ so $h\phi(v)f = \phi(u_{j+1} \cdots u_n v u_0 \cdots u_i) \in M_{\phi((u_{i+1} \cdots u_j)^m)} = M_{g^m}$ by Lemma 18. Thus

$$\begin{aligned}\phi(uvu) &= fgh\phi(v)fgh = fg^m h\phi(v)fg^m h \\ &= fg^m h \quad \text{since } g^m M_{g^m} g^m = g^m \\ &= fgh \\ &= \phi(u).\end{aligned}$$

Theorem 20 Let M be the syntactic monoid of $X \subseteq A^*$ M is finite and *G*-trivial if and only if X is a $\underset{n\,G}{\approx}$ language for some $n \geqslant 1$.

Proof:

($\Rightarrow$) Suppose M is finite and *G*-trivial. Let n be the cardinality of M. Since $\underset{n\,G}{\approx}$ is the smallest congruence such that $u \underset{n\,G}{\approx} uvu$ for all $u, v \in A^*$ such that u is n-full and $\alpha(u) \supseteq \alpha(v)$, it is sufficient to show $u \underset{n\,G}{\approx} uvu$ implies $\underline{u} = \underline{uvu}$. But this follows from Lemma 19 since $u \underset{n\,G}{\approx} uvu$ implies $u \underset{n}{\sim} uvu$. Thus X is a $\underset{n\,G}{\approx}$ language.

($\Leftarrow$) Immediate from Propositions 4(d) and 17.

Some additional properties of these monoids and other related results are presented here for completeness.

Proposition 21 For all $f,g \in \mathrm{M}$, $\mathrm{P}_f = \mathrm{P}_g$ if and only if $\mathrm{M}f\mathrm{M} = \mathrm{M}g\mathrm{M}$.

Proof:

($\Rightarrow$) Since $f \in \mathrm{P}_f = \mathrm{P}_g$, $g \in \mathrm{M}f\mathrm{M}$ so $\mathrm{M}g\mathrm{M} \subseteq \mathrm{M}(\mathrm{M}f\mathrm{M})\mathrm{M} = \mathrm{M}f\mathrm{M}$. Similarly $\mathrm{M}f\mathrm{M} \subseteq \mathrm{M}g\mathrm{M}$; hence $\mathrm{M}f\mathrm{M} = \mathrm{M}g\mathrm{M}$.

($\Leftarrow$) Let $h \in P_f$. Then $f \in \mathrm{M}h\mathrm{M}$ so there exist $h,h' \in \mathrm{M}$ such that $f = h'hh''$. Now $g \in \mathrm{M}g\mathrm{M} = \mathrm{M}f\mathrm{M}$ so there exist $f',f'' \in \mathrm{M}$ such that $g = f'ff''$. Hence $g = f'ff'' = f'h'hh''f'' \in \mathrm{M}h\mathrm{M}$ so that $h \in \mathrm{P}_g$. Thus $\mathrm{P}_f \subseteq \mathrm{P}_g$ and by symmetry it follows that $\mathrm{P}_g \subseteq \mathrm{P}_f$.

Lemma 22 If $e\mathrm{M}_e e = e$ then $\mathrm{M}_e = \mathrm{P}_e$.

Proof: Clearly $\mathrm{P}_e \subseteq \mathrm{M}_e$. Suppose $f \in \mathrm{M}_e$. Then $efe = e$ and since $efe \in \mathrm{M}f\mathrm{M}$, it follows that $f \in \mathrm{P}_e = \{g \mid e \in \mathrm{M}g\mathrm{M}\}$. Hence $\mathrm{M}_e \subseteq \mathrm{P}_e$.

Proposition 23 Let M be a *G*-trivial monoid and let $\phi{:}\mathrm{A}^*\rightarrow\mathrm{M}$ be a homomorphism. For all $x,y \in \mathrm{A}^*$, if $\alpha(x) = \alpha(y)$ and $e = \phi(x)$ and $f = \phi(y)$ are idempotent then $\mathrm{P}_e = \mathrm{P}_f$ and $e\mathrm{M}_e f = ef$.

Proof: Suppose $x,y \in \mathrm{A}^*$ are such that $\alpha(x) = \alpha(y)$ and $e = \phi(x)$ and $f = \phi(y)$ are idempotent. Clearly $e \equiv f$ so, by Theorem 16, $\mathrm{M}e\mathrm{M} = \mathrm{M}f\mathrm{M}$. Proposition 21 implies that $\mathrm{P}_e = \mathrm{P}_f$. Since $f \in \mathrm{P}_f = \mathrm{P}_e \subseteq \mathrm{M}_e$, it follows from Theorem 14 that $efe \in e\mathrm{M}_e e = e$. Thus $e\mathrm{M}_e f = efe\mathrm{M}_e f \subseteq ef\mathrm{M}_e f = ef\mathrm{M}_f f = ef$.

Proposition 24 Let M be a *G*-trivial monoid. Then $\{\underline{x} \mid x \text{ is } \#\mathrm{M}\text{-full}\} = \{e \in \mathrm{M} \mid e$ is idempo-

Proposition 24 Let M be a G-trivial monoid. Then $\{\underline{x} \mid x$ is #M-full$\}$ $=$ $\{e \in \mathrm{M} \mid e$ is idempotent$\}$.

Proof: Let $n = \#\mathrm{M}$. Suppose x is n-full. Since $\alpha(1) \subseteq \alpha(x)$, $x \underset{n}{\sim} x1x = x^2$, so by Lemma 19 $\underline{x} = \underline{x^2} = \underline{x}^2$. Therefore $\underline{x}$ is idempotent.

Conversely if $e \in \mathrm{M}$ is idempotent then, since the syntactic morphism is surjective, there exists $x \in A^*$ such that $\underline{x} = e$. But e is idempotent, so $e = e^n = \underline{x}^n = \underline{x^n}$ and x^n is clearly n-full.

Corollary 25 If M is G-trivial and $n = \#\mathrm{M}$ then $\mathrm{M}^n = \{e \in \mathrm{M} \mid e$ is idempotent$\}$.

Theorem 26 Let M be a finite monoid. Then $e\mathrm{P}_e e = e$ for all idempotents $e \in \mathrm{M}$ if and only if there exists an $n > 0$ such that $(fgh)^n g (fgh)^n = (fgh)^n$ for all $f,g,h \in \mathrm{M}$.

Proof:

($\Rightarrow$) Since M is finite there exists $n > 0$ such that $e = (fgh)^n$ is idempotent. Now $e = fg[h(fgh)^{n-1}] \in \mathrm{M}g\mathrm{M}$ so that $g \in \mathrm{P}_e$. Therefore $(fgh)^n g (fgh)^n = ege = e = (fgh)^n$ since $e\mathrm{P}_e e = e$.

($\Leftarrow$) Let $g \in \mathrm{P}_e$. Then $e \in \mathrm{M}g\mathrm{M}$ so that $e = fgh$ for some $f,h \in \mathrm{M}$. Since e is idempotent, $ege = e^n g e^n = (fgh)^n g (fgh)^n = (fgh)^n = e^n = e$. Therefore $e\mathrm{P}_e e = e$.

4.3 Automata and Expressions

The automata and regular expressions corresponding to the family of languages discussed in the previous two sections have also been investigated.

Proposition 27 Let $S = < A, Q, \sigma >$ be a semiautomaton, and let M be its transformation monoid. Then M is G-trivial if and only if there exists $n > 0$ such that for all $q \in Q$, all n-full words x, and all $z \in (\alpha(x))^*$, $\sigma(q,x) = \sigma(q,xzx)$.

Proof:

($\Rightarrow$) The proof follows directly from Lemma 19.

($\Leftarrow$) Suppose $e \in M$ is idempotent. Let $f \in M_e$. If $f = 1$ then $efe = e^2 = e$. Otherwise $f = f_1 \cdots f_m$ where $m \geqslant 1$ and $f_i \in P_e$. Then there exist $g_i, h_i \in M$ such that $e = g_i f_i h_i$. Since the syntactic morphism is surjective, there exist $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, $z_1, \ldots, z_m \in A^*$ such that $\underline{x_i} = g_i$, $\underline{y_i} = f_i$, and $\underline{z_i} = h_i$ for $i = 1, \ldots, m$.

Thus $e = e^m = g_1 f_1 h_1 \cdots g_m f_m h_m = \underline{x_1 y_1 z_1 \cdots x_m y_m z_m}$ and $f = f_1 \cdots f_m = \underline{y_1 \cdots y_m}$. Let $u = x_1 y_1 z_1 \cdots x_m y_m z_m$ and let $v = y_1 \cdots y_m$. Clearly $\alpha(u^n) \supseteq \alpha(v)$ and u is n-full. Therefore $\sigma(q, u^n v u^n) = \sigma(q, u^n)$ for all $q \in Q$ so that $e = e^n = \underline{u^n} = \underline{u^n v u^n} = e^n f e^n = efe$.

Hence $e M_e e = e$ for all idempotents $e \in M$.

Consider the following algorithm, a modification of Algorithm 11, which transforms the unique minimal element x of a $\underset{nG}{\equiv}$ class into a regular expression which denotes $[x]_{\underset{nG}{\equiv}}$.

Algorithm 28

```
for $m = \#\alpha(x), \ldots, 1$ do
  for $C \subseteq \alpha(x)$ such that $\#C = m$ do
    for each decomposition $x = z_1 y z_2$ such that $y$ is $2n$-full, $\alpha(y) = C$, and $t_1(z_1), f_1(z_2) \notin C$
```

```
do
    let $u$ be the shortest prefix of $y$ such that $u$ is $n$-full and $\alpha(u) = \alpha(y)$.
    let $w$ be the shortest suffix of $y$ such that $w$ is $n$-full and $\alpha(w) = \alpha(y)$.
    Replace $x$ by $z_1 u \mathrm{C}^* w z_2$. Note that since $x$ is minimal, $y = uw$.
```

Since the subsets C are considered in order of decreasing cardinality the largest possible subset is always inserted. For example, the factorization $x = ab(aac)(caa)b$ does not have to be considered because any new words this would introduce would have already been introduced when $\mathrm{C} = \{a,b,c\}$. It follows from the correctness of Algorithm 11 that this algorithm is also correct.

Example Let $x = abaaccaab$. This is the unique minimal element of $[abaaacbccaab]_{\underset{1G}{\equiv}}$ which was determined in the example following Algorithm 11.

subset	decomposition of x such that uw is 2-full				replace x by
	z_1	u	w	z_2	
$\{a,b,c\}$	1	$abaac$	$caab$	1	$abaac\{a,b,c\}^*caab$
$\{a,b\}$					
$\{b,c\}$					
$\{a,c\}$					
$\{a\}$	ab	a	a	$c\{a,b,c\}^*caab$	$abaa^*ac\{a,b,c\}^*caab$
	$abaa^*ac\{a,b,c\}^*c$	a	a	b	$abaa^*ac\{a,b,c\}^*caa^*ab$
$\{b\}$					
$\{c\}$					

Therefore the regular expression which denotes $[x]_{\underset{1G}{\equiv}}$ is $abaa^*ac\{a,b,c\}^*caa^*ab$.

Now in the algorithm $\mathrm{C} \subseteq \mathrm{A}$ so $\mathrm{C}^* = \bigcap_{a \in \mathrm{A}-\mathrm{C}} \overline{\mathrm{A}^* a \mathrm{A}^*} \in B_1$. Thus $[x]_{\underset{nG}{\equiv}} \in (\{\mathrm{C}^* \mid \varnothing \neq \mathrm{C} \subseteq \mathrm{A}\} \cup \mathrm{A})^*$ is a language in $B_1\mathbf{M}$ and hence any $\underset{nG}{\equiv}$ language is an element of $B_1\mathbf{MB} = B_2$.

However, the family of languages with G-trivial syntactic monoids is incomparable with B_1. Consider the language in B_1 denoted by the expression $(ab)^*$. The graph of its automaton is illustrated in Figure 1.

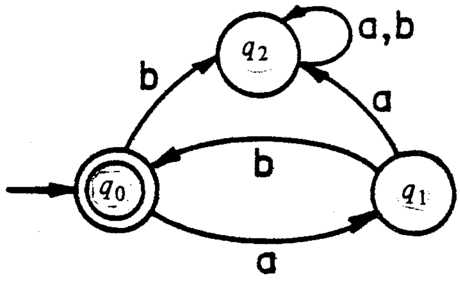

Figure 1

Let $f = \underline{ab}$, $g = \underline{a}$, $h = \underline{b}$ and $k = \underline{1}$. Then $fghkf = \underline{ababab} = \underline{ab} = f$ since $\sigma(q_0, (ab)^3) = q_0 = \sigma(q_0,ab)$, $\sigma(q_1, (ab)^3) = q_2 = \sigma(q_1,ab)$, and $\sigma(q_2, (ab)^3) = q_2 = \sigma(q_2,ab)$. But $fgkf = \underline{abaab} \neq \underline{ab} = f$ since $\sigma(q_0,abaab) = q_2 \neq q_0 = \sigma(q_0,ab)$.. From Theorem 14 it follows that the syntactic monoid of this language is not G-trivial.

Since $eM_e = e$ implies $eM_e \cap M_e e = e$, every finite R-trivial monoid is also G-trivial. But the family of languages with R-trivial syntactic monoids contains languages which are not in B_1, hence the family of languages with G-trivial syntactic monoids also does.

4.4 Noncounting Languages

The family of noncounting languages is also important in the study of star-free languages. In [10], [20], [22], and [26] it is proved that every star-free language is noncounting and, moreover, that a regular language is noncounting only if it is star-free.

Definition 29 For $n \geqslant 0$ define $\underset{n}{\sim}$ to be the smallest congruence such that $u^n \underset{n}{\sim} u^{n+1}$ for all $u \in A^*$. A language is *noncounting* if and only if it is a $\underset{n}{\sim}$ language for some $n \geqslant 0$.

Given some alphabet, A, let N_n denote the set of all $\underset{n}{\sim}$ languages over this alphabet. That is, $N_n = \{X \subseteq A^* | X \text{ is a } \underset{n}{\sim} \text{ language}\}$. The set of all noncounting languages is represented by $N = \bigcup_{n \geqslant 0} N_n$. Clearly N_n and N are Boolean algebras. It is immediate from the definition that $x \underset{n+1}{\sim} y$ implies $x \underset{n}{\sim} y$ for all $x,y \in A^*$ and $n \geqslant 0$. Thus $N_0 \subseteq N_1 \subseteq \cdots$. Each containment is proper; consider, for example, the languages $\{a^n\} \in N_{n+1} - N_n$ for $n \geqslant 0$.

Green and Rees [16] proved that $\underset{1}{\sim}$ is a congruence of finite index for any alphabet. Thus every language in N_1 is regular and hence star-free. However in [6], Brzozowski, Culik, and Gabrielian showed that for an alphabet of cardinality greater than 1, N_2 contains languages which are not even recursively enumerable.

Here attention will be focused on the relationship between N_1 and the languages of *G*-trivial monoids.

Proposition 30 Let $u,v \in A^*$. If $\alpha(u) \supseteq \alpha(v)$ then $u \underset{1}{\sim} uvu$.

Proof: By induction on $|v|$.

Assume the result is true for all $v' \in A^*$ such that $|v'| < |v|$. If $|v| = 0$ then $v = 1$ so $u \underset{1}{\sim} u^2 = uvu$. Otherwise $v = v'a$ for some $a \in A$, $v' \in A^*$. Now $a \in \alpha(v) \subseteq \alpha(u)$ so $u = ras$ for some $r,s \in A^*$. Since $\alpha(v') \subseteq \alpha(v) \subseteq \alpha(u) = \alpha(aras)$ and $|v'| < |v|$, it follows by the induction hypothesis that $aras \underset{1}{\sim} (aras)v'(aras)$. Thus $u = ras \underset{1}{\sim} raras \underset{1}{\sim} rarasv'aras \underset{1}{\sim}$

$rasv'aras = uvu$.

Definition 31 Let $x \in A^+$ and suppose $a \in A$ and $u, v \in A^*$ are such that $x = uav$ and $\alpha(u) \subsetneq \alpha(ua) = \alpha(x)$. Then the *initial mark* of x is $a_{\mathrm{L}}(x) = a$ and the *initial segment* of x is $f(x) = u$. Symmetrically, if $x = uav$ and $\alpha(v) \subsetneq \alpha(av) = \alpha(x)$ then the *terminal mark* of x is $a_{\mathrm{R}}(x) = a$ and the *terminal segment* of x is $t(x) = v$.

The initial segment of a word is just its longest prefix which does not contain every letter occurring in the word. The initial mark is the letter in the word whose first appearance occurs furthest to the right. Analogous remarks can be made concerning terminal segments and terminal marks.

The following characterization of $\underset{\mathrm{I}}{-}$ from [6] provides a useful working definition.

Lemma 32 Let $x,y \in A^*$. Then $x \underset{\mathrm{I}}{-} y$ if and only if $a_{\mathrm{L}}(x) = a_{\mathrm{L}}(y)$, $a_{\mathrm{R}}(x) = a_{\mathrm{R}}(y)$, $f(x) \underset{\mathrm{I}}{-} f(y)$, and $t(x) \underset{\mathrm{I}}{-} t(y)$.

Clearly $[1]_{\underset{\mathrm{I}}{-}} = 1$. From this lemma it follows that for $x \in A^+$, $[x]_{\underset{\mathrm{I}}{-}} = [f(x)]_{\underset{\mathrm{I}}{-}} a_{\mathrm{L}}(x)(\alpha(x))^* \cap (\alpha(x))^* a_{\mathrm{R}}(x)[t(x)]_{\underset{\mathrm{I}}{-}}$.

Lemma 33 Supppose $n \geqslant 0$, $a_1, \ldots, a_n \in \mathrm{A}$ and $a_i \neq a_j$ for $1 \leqslant i < j \leqslant n$. Then $a_1 \cdots a_n$ is the unique element of minimal length in $[a_1 \cdots a_n]_{\underset{\mathrm{I}}{-}}$.

Proof: By induction on n.

For $n = 0$ the result is immediate from the fact that $[1]_{\underset{\mathrm{I}}{-}} = 1$. Assume the result is true for n and suppose $a_1, \ldots, a_n, a_{n+1} \in \mathrm{A}$ are such that $a_i \neq a_j$ for $1 \leqslant i < j \leqslant n+1$.

Now $[a_1 \cdots a_{n+1}]_{\underset{\mathrm{I}}{-}} = [a_1 \cdots a_n]_{\underset{\mathrm{I}}{-}} a_{n+1}\{a_1, \ldots, a_{n+1}\}^* \cap \{a_1, \ldots, a_{n+1}\}^* a_1 [a_2 \cdots a_{n+1}]_{\underset{\mathrm{I}}{-}}$. By the induction hypothesis the unique minimal element of $[a_1 \cdots a_n]_{\underset{\mathrm{I}}{-}}$ is $a_1 \cdots a_n$. Since 1 is the unique minimal element of $\{a_1 \cdots a_{n+1}\}^*$, $a_1 \cdots a_n a_{n+1}$ is the unique minimal element of $[a_1 \cdots a_n]_{\underset{\mathrm{I}}{-}} a_{n+1}\{a_1 \cdots a_{n+1}\}^*$. Similarly,

$a_1 \cdots a_{n+1}$ is the unique minimal element of $\{a_1 \cdots a_{n+1}\}^* a_1 [a_2 \cdots a_{n+1}]_{\overline{1}}$ and hence is the unique minimal element of $[a_1 \cdots a_{n+1}]_{\overline{1}}$. By induction the result is true for all $n \geqslant 0$.

Proposition 34 Let $a \in \mathrm{A}$, $\mathrm{X} \subseteq \mathrm{A}^*$, and $\mathrm{Y},\mathrm{Z} \subseteq (\mathrm{A}-\{a\})^*$. Then

$$\text{(a)} \quad \mathrm{X}a(\mathrm{Y} \cap \mathrm{Z}) = (\mathrm{X}a\mathrm{Y}) \cap (\mathrm{X}a\mathrm{Z}), \text{ and}$$

$$\text{(b)} \quad (\mathrm{Y} \cap \mathrm{Z})a\mathrm{X} = (\mathrm{Y}a\mathrm{X}) \cap (\mathrm{Z}a\mathrm{X}).$$

Proof:

(a) It is easily verified that $\mathrm{X}a(\mathrm{Y} \cap \mathrm{Z}) \subseteq (\mathrm{X}a\mathrm{Y}) \cap (\mathrm{X}a\mathrm{Z})$. Now $w \in (\mathrm{X}a\mathrm{Y}) \cap (\mathrm{X}a\mathrm{Z})$ implies $w = x_1ay$ and $w = x_2az$, where $x_1,x_2 \in \mathrm{X}$, $y \in \mathrm{Y}$, and $z \in \mathrm{Z}$. If $|y| > |z|$ then $a \in \alpha(y)$; this contradicts the fact that $\mathrm{Y} \subseteq (\mathrm{A}-\{a\})^*$. Therefore $|y| \leqslant |z|$. Similarly, $|z| \leqslant |y|$. Consequently $|y| = |z|$ and $y = z$. Thus $w = x_1ay \in \mathrm{X}a(\mathrm{Y} \cap \mathrm{Z})$ and $(\mathrm{X}a\mathrm{Y}) \cap (\mathrm{X}a\mathrm{Z}) \subseteq \mathrm{X}a(\mathrm{Y} \cap \mathrm{Z})$.

(b) This follows by left-right duality.

Proposition 35 Let $x \in \mathrm{A}^*$. The language corresponding to the congruence class $[x]_{\overline{1}}$ can be expressed as a finite intersection of languages X_j for j in some index set J, such that $\alpha(\mathrm{X}_j) = \alpha(x)$ and $\mathrm{X}_j \in B_1\mathbf{M}$ for all $j \in \mathrm{J}$. That is, $[x]_{\overline{1}} = \bigcap_{j \in \mathrm{J}} \mathrm{X}_j$.

Proof: By induction on $|x|$.

If $|x| = 0$ then $x = 1$ and $[x]_{\overline{1}} = \{1\} \in B_1$. Assume that the claim holds for all $w \in \mathrm{A}^*$ with $|w| \leqslant n$. Consider $x \in \mathrm{A}^{n+1}$. Let $\mathrm{A}_x = \alpha(x)$ to simplify notation.

By the remark following Lemma 32,

$$[x]_{\overline{1}} = [f(x)]_{\overline{1}} a_{\mathrm{L}}(x)\mathrm{A}_x^* \cap \mathrm{A}_x a_{\mathrm{R}}(x)[t(x)]_{\overline{1}}.$$

Since $|f(x)|, |t(x)| < |x|$ it follows from the induction hypothesis that

$$[f(x)]_{\overline{1}} = \bigcap_{j \in \mathrm{J}} \mathrm{U}_j \text{ and } [t(x)]_{\overline{1}} = \bigcap_{k \in \mathrm{K}} \mathrm{V}_k$$

where $\alpha(\mathrm{U}_j) = \alpha(f(x))$, $\alpha(\mathrm{V}_k) = \alpha(t(x))$, and $\mathrm{U}_j, \mathrm{V}_k \in B_1\mathbf{M}$ for all $j \in \mathrm{J}$, $k \in \mathrm{K}$.

Using Proposition 34,

$$[x]_{\underset{1}{-}} = \left(\bigcap_{j \in J} (U_j a_L(x) A_x^*)\right) \cap \left(\bigcap_{k \in K} (A_x^* a_R(x) V_k)\right).$$

Clearly $\alpha(U_j a_L(x) A_x^*) = \alpha(x) = \alpha(A_x^* a_R(x) V_k)$ for all $j \in J$, $k \in K$. Also,

$$A_x^* = \begin{cases} \displaystyle\bigcap_{c \in A - \alpha(x)} \overline{\overline{\varnothing} c \overline{\varnothing}} \in B_0\mathbf{MB} \subseteq B_1\mathbf{M} \text{ if } \alpha(x) \subsetneq A \\ \overline{\varnothing} \quad \in B_0 \subseteq B_1\mathbf{M} \text{ if } \alpha(x) = A. \end{cases}$$

Hence $U_j a_L(x) A_x^*$, $A_x^* a_R(x) V_k \in B_1\mathbf{M}$ for all $j \in J$, $k \in K$. The result is therefore true for $n+1$.

Corollary 36 $N_1 \subseteq B_1\mathbf{MB} = B_2$.

Definition 37 Let $n \geqslant 0$, $m \geqslant 1$ and $x,y \in A^*$. Then $x \underset{n}{\overset{(m)}{-}} y$ if and only if for every decomposition $x = x_1 \cdots x_m$ there exists a decomposition $y = y_1 \cdots y_m$ such that $x_i \underset{n}{-} y_i$ for $i = 1, \ldots, m$ and vice versa. N_n^m denotes the set $\{X \subseteq A^* \mid X \text{ is a } \underset{n}{\overset{(m)}{-}} \text{ language}\}$.

In [7] it is shown that $(N_n)^m\mathbf{B} = \{ X \subseteq A^* \mid X \text{ is a } \underset{n}{\overset{(m)}{-}} \text{ language}\}$. This justifies the notation N_n^m. Since $\underset{1}{-}$ is of finite index, $\underset{1}{\overset{(m)}{-}}$ is also of finite index for $m \geqslant 1$. Hence every $\underset{1}{\overset{(m)}{-}}$ language is star-free.

Proposition 38 For $n \geqslant 1$, $N_1^n\mathbf{B} \subseteq N_{2n-1}$.

Proof: Let $x \in A^*$. If $x = 1$ then $x^{2n-1} = x^{2n}$, so assume $|x| \geqslant 1$.

Consider any decomposition of x^{2n} into n pieces $x_1, \ldots, x_n$. Since $|x_1| + \cdots + |x_n| = |x_1 \cdots x_n| = |x^{2n}| = 2n|x|$ there exists i, $1 \leqslant i \leqslant n$, such that $|x_i| \geqslant 2|x|$. Let $y = f_{2|x|}(x_i)$. Then $x_i = yz$ for some $z \in A^*$. Now $x^{2n} = (x_1 \cdots x_{i-1}) y (z x_{i+1} \cdots x_n)$; thus there exist $u,v \in A^*$ such that $y = uxv$ and $x = vu$. Let $x_i' = uvz$ and $x_j' = x_j$ for $j = 1, \ldots, i-1, i+1, \ldots, n$. Then $x_1' \cdots x_n' = (x_1 \cdots x_{i-1}) uvz (x_{i+1} \cdots x_n) = x^{2n-1}$ and, since $x_i = uxvz = uvuvz \underset{1}{-} uvz = x_i'$, $x_j \underset{1}{-} x_j'$ for $j = 1, \ldots, n$.

Conversely, consider any decomposition $x^{2n-1} = x_1' \cdots x_n'$. Since $|x_1'| + \cdots + |x_n'| = |x_1' \cdots x_n'| = |x^{2n-1}| = (2n-1)|x| \geqslant n|x|$ there exists i, $1 \leqslant i \leqslant n$, such that $|x_i'| \geqslant |x|$. As above, let $y = f_{|x|}(x_i')$, let $x_i' = yz$ where $z \in A^*$, and let $u,v \in A^*$ be such that $y = uv$ and $x = vu$.

Now, if $x_i = uxvy$ and $x_j = x_j'$ for $j = 1, \ldots, i-1, i+1, \ldots, n$, then $x_1 \cdots x_n = x^{2n}$ and $x_j' \mathrel{\underset{1}{-}} x_j$ for $j = 1, \ldots, n$.

Thus $x^{2n} \mathrel{\overset{(n)}{\underset{1}{-}}} x^{2n-1}$ for all $x \in A^*$. But $\underset{2n-1}{-}$ is, by definition, the smallest congruence satisfying this property. Hence $x \mathrel{\underset{2n-1}{-}} y$ implies $x \mathrel{\overset{(n)}{\underset{1}{-}}} y$ for all $x,y \in A^*$ and thus $N_1^n \subseteq N_{2n-1}$. Since N_{2n-1} is a Boolean algebra $N_1^n\mathbf{B} \subseteq N_{2n-1}$.

Proposition 39 For $n \geqslant 1$, $N_1^n \not\subseteq N_{2n-2}$.

Proof: Let $A = \{a_1, \ldots, a_n\}$, let $x = (a_1 \cdots a_n)^{2n-2}$, and let $y = (a_1 \cdots a_n)^{2n-1}$. Clearly $x \mathrel{\underset{2n-2}{-}} y$. Consider the decomposition $y = y_1 \cdots y_n$ where $y_1 = a_1 \cdots a_{n-1}a_na_1 \cdots a_{n-1}$, $y_n = a_2 \cdots a_na_1a_2 \cdots a_n$, and $y_i = a_{n+2-i} \cdots a_na_1 \cdots a_{n-i}a_{n+1-i}a_{n+2-i} \cdots a_na_1 \cdots a_{n-i}$ for $i = 2, \ldots, n-1$. From the remark following Lemma 32 it is clear that y_i is the unique minimal element of $[y_i]_{\underset{1}{-}}$. Since $|x| < |y|$ there do not exist $x_1, \ldots, x_n \in A^*$ such that $x = x_1 \cdots x_n$ and $x_i \mathrel{\underset{1}{-}} y_i$ for $i = 1, \ldots, n$. Therefore $x \mathrel{\overset{(n)}{\underset{1}{\not-}}} y$ and $N_1^n \not\subseteq N_{2n-2}$.

It is possible to relate noncounting languages with the languages of *G*-trivial monoids.

Proposition 40 A monoid M is idempotent if and only if $fM_ff = f$ for all $f \in M$.

Proof: Clearly, if $fM_ff = f$ for all $f \in M$ then M is idempotent since for any $f \in M$, $1 \in M_f$ and thus $f^2 = f1f = f$.

Now suppose M is idempotent, $f \in M$, and $g \in M_f$. Then $g \in P_f^n$ for some $n \geqslant 0$. The proof proceeds by induction on n. The case $n = 0$ is trivial since $f = f^2 = f1f$ in an idempotent monoid.

Let $g \in P_f$. Then $f = hgk$ for some $h,k \in M$ so that

$$\begin{aligned} f &= hgk = h(gk) \\ &= h(gk)(gk) = (hgk)gk \\ &= (f)gk = (fg)k \qquad \text{(note that } f = fgk\text{)} \\ &= (fg)(fg)k = (fg)(fgk) \end{aligned}$$

$$= fg(f) = fgf.$$

Assume now that $f = fgf$ and $f = fhf$. Then

$$\begin{aligned} f = fgf &= (f)gf \\ &= (fhf)gf = f(hfg)f \\ &= f(hfg)(hfg)f = (fhf)gh(fgf) \\ &= (f)gh(f) = fghf. \end{aligned}$$

It now follows that $f = fgf$ for all $g \in \mathrm{M}_f$.

Clearly a language is in N_1 if and only if its syntactic monoid is idempotent. From the above proposition and Theorem 14 it follows that every idempotent monoid is G-trivial. Thus every $\overline{}_1$ language has a G-trivial syntactic monoid.

Note that idempotent monoids are not necessarily R-trivial or L-trivial. Consider M, the free idempotent monoid on the two generators $\{a,b\}$. It is the transformation monoid of the automaton depicted in Figure 2.

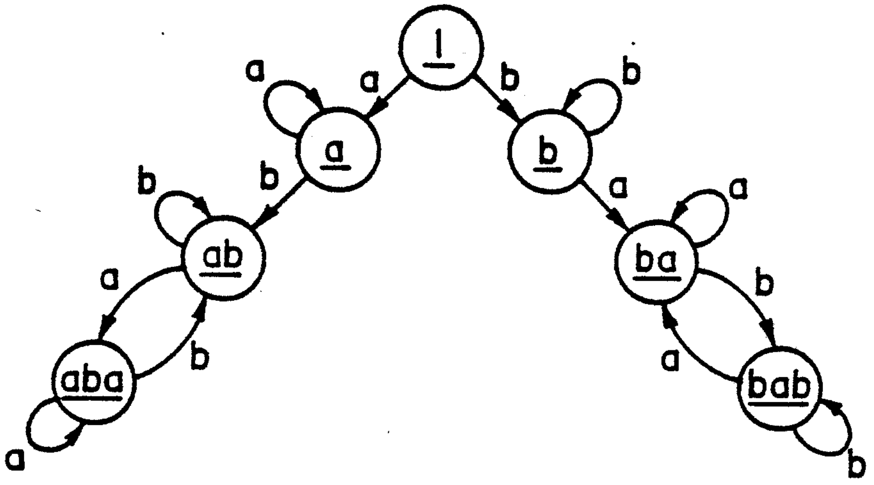

Figure 2

Here $\underline{ab}\mathrm{M} = \{\underline{ab}, \underline{aba}\} = \underline{aba}\mathrm{M}$ and $\mathrm{M}\underline{ab} = \{\underline{ab}, \underline{bab}\} = \mathrm{M}\underline{bab}$, but $\underline{aba} \neq \underline{ab} \neq \underline{bab}$. Thus M is neither R-trivial nor L-trivial.

By Lemma 4(c) $u^n \underset{nG}{\approx} u^{n+1}$ for all $u \in A^*$. But $\underset{n}{\sim}$ is the smallest congruence such that $u^n \underset{n}{\sim} u^{n+1}$ for all $u \in A^*$; thus $x \underset{n}{\sim} y$ implies $x \underset{nG}{\approx} y$ for all $x,y \in A^*$.

In the special case when $n = 1$ the following interesting relationship holds. It is a direct consequence of the above results and Proposition 30.

Proposition 41 Let $x,y \in A^*$. Then $x \underset{1}{\sim} y$ if and only if $x \underset{1G}{\approx} y$.

The congruences $\overset{(n)}{\underset{1}{\sim}}$, for $n \geqslant 2$, do not fare as well.

Proposition 42 There does not exist an $n \geqslant 1$ such that $x \underset{nG}{\equiv} y$ implies $x \overset{(2)}{\underset{1}{\sim}} y$ for all $x,y \in A^*$.

Proof: Let $x = (ab)^n b (ab)^n$ and let $y = (ab)^{2n}$. Since $\alpha((ab)^n) \supseteq \alpha(b)$ and $(ab)^n$ is n-full, it follows that $x \underset{nG}{\equiv} y$.

Now consider the decomposition $x = x_1 x_2$ where $x_1 = (ab)^n$ and $x_2 = b(ab)^n$. Suppose $y = y_1 y_2$ where $x_1 \underset{1}{\sim} y_1$. Then $y_1 = (ab)^i$ for some i, $1 \leqslant i \leqslant 2n$. However this implies $y_2 = (ab)^{2n-i} \underset{1}{\not\sim} x_2$. Therefore there does not exist a decomposition $y = y_1 y_2$ such that $x_1 \underset{1}{\sim} y_1$ and $x_2 \underset{1}{\sim} y_2$. Thus $x \overset{(2)}{\underset{1}{\not\sim}} y$.

Corollary 43 For $n \geqslant 2$, N_1^n contains languages whose syntactic monoids are not G-trivial.

4.5 Some Negative Results

A number of other congruences, also generalizations of the congruences used to characterize the languages of R-trivial and L-trivial monoids, were initially conjectured to be characterizations of the family of G-trivial monoids.

In this section properties of these congruences and the relationships between them and the congruences of Section 4.1 are investigated.

Definition 44 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n\,G}{\simeq} y$ if and only if $x \underset{n\,R}{\simeq} y$ and $x \underset{n\,L}{\simeq} y$.

Definition 45 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \overset{(2)}{\underset{n}{\sim}} y$ if and only if for every decomposition $x = x'x''$ there exists a decomposition $y = y'y''$ such that $x' \underset{n}{\sim} y'$ and $x'' \underset{n}{\sim} y''$ and vice versa.

Definition 46 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n\,G}{\dot{\simeq}} y$ if and only if there exist $u,v,w \in A^*$ such that $x = uw$, $y = uvw$, $u \underset{n\,R}{\simeq} uv$, and $w \underset{n\,L}{\simeq} vw$. $\underset{n\,G}{\approxeq}$ is the symmetric transitive closure of $\underset{n\,G}{\dot{\simeq}}$.

Definition 47 Let $x,y \in A^*$. Then $x \underset{0}{\leftrightarrows} y$ and $x \underset{n+1}{\leftrightarrows} y$ if and only if for each decomposition $x = x'ax''$ with $a \in A$ there exists a decomposition $y = y'ay''$ such that $x' \underset{n}{\sim} y'$ and $x'' \underset{n}{\sim} y''$ and vice versa.

Definition 48 Let $x,y \in A^*$. Then $x \underset{0}{\Leftrightarrow} y$ and $x \underset{n+1}{\Leftrightarrow} y$ if and only if for each decomposition $x = x'ax''$ with $a \in A$ there exists a decomposition $y = y'ay''$ such that $x' \underset{n}{\Leftrightarrow} y'$ and $x'' \underset{n}{\Leftrightarrow} y''$ and vice versa.

This congruence and the congruence $\underset{n}{\leftleftarrows}$ defined by Definition 2.48 are both special cases of a more general congruence which is discussed in [32].

Proposition 49 Let $u \in A^*$ and let $n \geqslant 0$. Then

(a) $u^n \underset{n\,G}{\simeq} u^{n+1}$,

(b) $u^{2n} \overset{(2)}{\underset{n}{\sim}} u^{2n+1}$,

(c) $u^{2n} \underset{n\,G}{\approxeq} u^{2n+1}$,

(d) $u^{2n-1} \underset{n}{\leftrightarrow} u^{2n}$, and

(e) $u^{2^n-1} \Longleftrightarrow_n u^{2^n}$.

Proof:

(a), (b), and (c) follow immediately from Proposition 2.8(a) and its dual.

(d) If $n = 0$ the result is trivial so assume $n > 0$. Suppose $x'ax''$ is a decomposition of u^{2n-1}. Since $a \in \alpha(u^{2n-1}) = \alpha(u)$, $|u| \geqslant 1$. Therefore either u^{n-1} is a prefix of x' or u^{n-1} is a suffix of x''. Since these two cases are symmetrical, assume, without loss of generality, that the former is true.

Let $y' = ux'$ and $y'' = x''$ so that $y'ay'' = ux'ax'' = uu^{2n-1} = u^{2n}$. Since u^{n-1} is a prefix of x' and $u^{2n-1} \mathrel{{}_{n-1}\sim} u^n$ it follows that $x' \mathrel{{}_{n-1}\sim} ux' = y'$.

Conversely, for any decomposition $u^{2n} = y'ay''$ there exists a decomposition $u^{2n-1} = x'ax''$ such that $x' \mathrel{{}_{n-1}\sim} y'$ and $x'' \mathrel{{}_{n-1}\sim} y''$. Thus $u^{2n-1} \underset{n}{\leftrightarrow} u^{2n}$.

(e) If $u = 1$ then $u^{2^n-1} = 1 \Longleftrightarrow_n 1 = u^{2^n}$. Therefore suppose $|u| \geqslant 1$. For $n = 0$, the result is clearly true, so assume it is true for $n-1$.

Let $x'ax''$ be a decomposition of u^{2^n-1}. Then either $u^{2^{n-1}-1}$ is a prefix of x' or $u^{2^{n-1}-1}$ is a suffix of x''. In the first case let $y' = ux'$, $y'' = x''$, and $x' = u^{2^{n-1}-1}z$ where $z \in A^*$. Then $y'ay'' = ux'ax'' = uu^{2^n-1} = u^{2^n}$. Clearly $x'' \Longleftrightarrow_{n-1} y''$ and, by the induction hypothesis, $x' = u^{2^{n-1}-1}z \Longleftrightarrow_{n-1} u^{2^{n-1}}z = ux' = y'$. The second case follows by symmetry.

Let $y'ay''$ be a decomposition of u^{2^n}. If $u^{2^{n-1}}$ is not a prefix of y' then $y'a$ is a prefix of $u^{2^{n-1}}$; hence $u^{2^{n-1}}$ is a suffix of y''. These two cases are symmetric, thus it suffices to consider the first. Let $y' = u^{2^{n-1}}z$ for some $z \in A^*$, let $x' = u^{2^{n-1}-1}z$, and let $x'' = y''$. As above, $x'ax'' = u^{2^n-1}$, $x' \Longleftrightarrow_{n-1} y'$, and $x'' \Longleftrightarrow_{n-1} y''$.

Hence $u^{2^n-1} \Longleftrightarrow_n u^{2^n}$.

In all five cases no stronger result can be achieved. To see this consider the example where $u \in A$.

Lemma 50 Let $u,v \in A^*$ and $n > 0$. Then $u \underset{n}{\sim}_G uvu$ if and only if u is n-full and $\alpha(u) \supseteq \alpha(v)$.

Proof: Suppose $u \underset{n}{\sim}_G uvu$. Then $u \underset{n}{\sim}_R u(vu)$ so by Lemma 2.11 there exist $u_1, \ldots, u_n \in A^*$ such that $u = u_1 \cdots u_n$ and $\alpha(u_1) \supseteq \cdots \supseteq \alpha(u_n) \supseteq \alpha(vu)$. But $\alpha(u) \supseteq \alpha(u_1)$ and $\alpha(vu) \supseteq \alpha(u)$. Therefore $\alpha(u) = \alpha(u_1) = \cdots = \alpha(u_n) = \alpha(uv)$, which implies that u is n-full. Also $\alpha(u) = \alpha(uv)$ so that $\alpha(u) \supseteq \alpha(v)$.

Conversely, if u is n-full and $\alpha(u) \supseteq \alpha(v)$ then, since $\alpha(vu)$, $\alpha(uv) \subseteq \alpha(u)$, $u(vu) \underset{n}{\sim}_R u \underset{n}{\sim}_L (uv)u$; that is $u \underset{n}{\sim}_G uvu$.

Corollary 51 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n}{\approx}_G y$ implies $x \underset{n}{\sim}_G y$.

Proof: Since $x \underset{0}{\sim}_G y$ for all $x,y \in A^*$ the result is true for $n = 0$. For $n > 0$ the result follows from Lemma 50, since $\underset{n}{\approx}_G$ is the smallest congruence satisfying $u \underset{n}{\approx}_G uvu$ for all $u,v \in A^*$ such that u is n-full and $\alpha(u) \supseteq \alpha(v)$.

Lemma 52 Let $u,v,u',v' \in A^*$ and let $n \geqslant 0$. If $uvu \underset{n}{\sim}_G u'v'u'$ and $u \underset{n}{\sim} u'$ then $u \underset{n}{\sim}_G u'$.

Proof: If $uvu \underset{n}{\sim}_G u'v'u'$ then $u(vu) \underset{n}{\sim}_R u'(v'u')$. Since $u \underset{n}{\sim} u'$ it follows from Proposition 2.8(c) that $u \underset{n}{\sim}_R u'$. Similarly $u \underset{n}{\sim}_L u'$. Thus $u \underset{n}{\sim}_G u'$.

Proposition 53 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n}{\sim}^{(2)} y$ implies $x \underset{n}{\sim}_G y$.

Proof: Suppose $x \underset{n}{\sim}^{(2)} y$. Let u be a prefix of x; say $x = uv$. Then there exists $u',v' \in A^*$ such that $y' = u'v'$, $u \underset{n}{\sim} u'$ and $v \underset{n}{\sim} v'$. Therefore $x \underset{n}{\sim}_R y$. Similarly $x \underset{n}{\sim}_L y$, hence $x \underset{n}{\sim}_G y$.

Proposition 54 Let $x,y \in A^*$ and $n \geqslant 0$. If x is $2n$-full then $x \underset{2n}{\sim}_G y$ implies $x \underset{n}{\sim}^{(2)} y$.

Proof: If x is $2n$-full then, since $x \underset{2n}{\sim}_G y$ implies $x \underset{n}{\sim} y$, it follows that y is $2n$-full. Since x is $2n$-full, there exist $x_1, \ldots, x_{2n} \in A^*$ such that $x = x_1 \cdots x_{2n}$ and $\alpha(x_i) = \alpha(x)$. Similarly there exist $y_1, \ldots, y_{2n} \in A^*$ such that $y = y_1 \cdots y_{2n}$ and $\alpha(y_i) = \alpha(y)$.

Let $x = u_1u_2$ be a decomposition of x. Then either

$$1.\ u_1 = x_1 \cdots x_n z \text{ where } u_2 z = x_{n+1} \cdots x_{2n}$$

$$\text{or } 2.\ u_2 = z x_{n+1} \cdots x_{2n} \text{ where } u_1 z = x_1 \cdots x_n.$$

1. Since $x \underset{2n\,G}{\sim} y$, $x \underset{2n\,L}{\sim} y$ and hence $x \underset{n\,L}{\sim} y$. Since $zu_2 = x_{n+1} \cdots x_{2n} \underset{n\,L}{\sim} (x_1 \cdots x_n)(x_{n+1} \cdots x_{2n}) = x$ and $y_{n+1} \cdots y_{2n} \underset{n\,L}{\sim} (y_1 \cdots y_n)(y_{n+1} \cdots y_n) = y$, $zu_2 \underset{n\,L}{\sim} y_{n+1} \cdots y_{2n}$. Therefore there exists a suffix v_2 of $y_{n+1} \cdots y_{2n}$ such that $v_2 \underset{n}{\sim} u_2$. Let v_1 be such that $y = v_1 v_2$. Since $x_1 \cdots x_n$ is a prefix of u_1, $y_1 \cdots y_n$ is a prefix of v_1, $x_1 \cdots x_n$ and $y_1 \cdots y_n$ are n-full, and $\alpha(x_1 \cdots x_n) = \alpha(x) = \alpha(y) = \alpha(y_1 \cdots y_n)$, it follows that $u_1 \underset{n}{\sim} x \underset{n}{\sim} y \underset{n}{\sim} v_1$.

2. is symmetrical.

Similarly for any decomposition $y = v_1 v_2$ there exists a decomposition $x = u_1 u_2$ such that $u_1 \underset{n}{\sim} v_1$ and $u_2 \underset{n}{\sim} v_2$. Thus $x \underset{n}{\overset{(2)}{\sim}} y$.

Proposition 55 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n}{\overset{(2)}{\sim}} y$ if and only if for every decomposition $x = x'x''$ there exists a decomposition $y = y'y''$ such that $x' \underset{n\,R}{\sim} y'$ and $x'' \underset{n\,L}{\sim} y''$ and vice versa.

Proof:

($\Rightarrow$) Suppose $x \underset{n}{\overset{(2)}{\sim}} y$. From Proposition 53 $x \underset{n\,G}{\sim} y$, therefore $x \underset{n\,R}{\sim} y$ and $x \underset{n\,L}{\sim} y$. Let $x = x'x''$ be any decomposition of x. Then there exist $y',y'' \in A^*$ such that $y = y'y''$, $x' \underset{n}{\sim} y'$, and $x'' \underset{n}{\sim} y''$. But by Proposition 2.8(c) and the corresponding result for $\underset{n\,L}{\sim}$ it follows that $x' \underset{n\,R}{\sim} y'$ and $x'' \underset{n\,L}{\sim} y''$. Similarly, for any decomposition $y = y'y''$ there exist $x',x'' \in A^*$ such that $x = x'x''$, $x' \underset{n\,R}{\sim} y'$, and $x'' \underset{n\,R}{\sim} y''$.

($\Leftarrow$) The result follows directly from Proposition 2.8(a) and its dual.

Proposition 56 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n\,G}{\approx} y$ implies $x \underset{n}{\overset{(2)}{\sim}} y$.

Proof: It is sufficient to show that $x \underset{n\,G}{\overset{.}{\approx}} y$ implies $x \underset{n}{\overset{(2)}{\sim}} y$. Assume $x \underset{n\,G}{\overset{.}{\approx}} y$. Then there exist $u,v,w \in A^*$ such that $x = uw$, $y = uvw$, $u \underset{n\,R}{\sim} uv$, and $w \underset{n\,L}{\sim} vw$.

Let $x = x'x''$ be a decomposition of x. Then either x' is a prefix of u or u is a prefix of x'. In the first case $u = x'z$ and $x'' = zw$ for some $z \in A^*$. Let $y' = x'$ and $y'' = zvw$. Then

$x' \underset{nR}{\sim} y'$ and, since $w \underset{nL}{\sim} vw$, $x'' = zw \underset{nL}{\sim} zvw = y''$. If u is a prefix of x' then x'' is a suffix of w and the result follows from symmetry with the first case.

Let $y = y'y''$ be a decomposition of y. There are three cases to consider. If y' is a prefix of u (say $u = y'z$ where $z \in A^*$) then choosing $x' = y'$ and $x'' = zw$ gives the result as above. Likewise, if y'' is a suffix of w. The only other case is when $y' = uv_1$ and $y'' = v_2w$ where $v = v_1v_2$. Let $x' = u$ and $x'' = w$. Since $u \underset{nR}{\sim} uv$ and v_1 is a prefix of v, $\mu_n(u) \subseteq \mu_n(uv_1) \subseteq \mu_n(uv) = \mu_n(u)$ so $u \underset{n}{\sim} uv_1$, and thus by Proposition 2.8(c), $x' = u \underset{nR}{\sim} uv_1 = y'$. Similarly, $x'' = w \underset{nL}{\sim} v_2w = y''$.

Therefore $x \underset{n}{\overset{(2)}{\sim}} y$.

Proposition 57 Let $x,y \in A^*$ and $n \geqslant 1$. Then $x \underset{nG}{\equiv} y$ implies $x \underset{nG}{\cong} y$.

Proof: It is sufficient to show that $x \underset{nG}{\dot{\equiv}} y$ implies $x \underset{nG}{\dot{\cong}} y$. Suppose $x \underset{nG}{\dot{\equiv}} y$. Then there exist $r,s,u,v,w \in A^*$ such that $x = ruws$, $y = ruvws$, u and w are n-full, and $\alpha(u) = \alpha(w) \supseteq \alpha(v)$. Since u is n-full and $\alpha(u) \supseteq \alpha(v)$, $u \underset{n}{\sim} uv$ so, by Proposition 2.8(b), $u \underset{nR}{\sim} uv$. But $\underset{nR}{\sim}$ is a congruence, so $ru \underset{nR}{\sim} ruv$. Likewise $ws \underset{nL}{\sim} vws$. Hence $x = (ru)(ws) \underset{nG}{\dot{\cong}} (ru)v(ws) = y$.

Proposition 58 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n+1G}{\equiv} y$ implies $x \underset{n}{\leftrightarrow} y$.

Proof: Suppose $u,v,w \in A^*$ are such that u and w are $(n+1)$-full and $\alpha(u) = \alpha(w) \supseteq \alpha(v)$. By the remark following Definition 2.6, there exist $u_1, \dots, u_{n+1} \in A^*$ such that $u = u_1 \cdots u_{n+1}$ and $\alpha(u_1) = \cdots = \alpha(u_{n+1})$.

Let $x'ax''$ be a decomposition of uw. If $x'a$ is a prefix of u then $u = x'az$ and $x'' = zw$ for some $z \in A^*$. Let $y' = x'$ and $y'' = zvw$. Then $y'ay'' = x'azvw = uvw$, and since $\alpha(v) \cup \alpha(z) \subseteq \alpha(u) = \alpha(w)$ and w is n-full, $x'' = zw \underset{n}{\sim} w \underset{n}{\sim} zvw = y''$. Similarly, if ax'' is a suffix of w then there exist $y', y'' \in A^*$ such that $y'ay'' = uvw$, $x' \underset{n}{\sim} y'$, and $x'' \underset{n}{\sim} y''$.

Now let $y'ay''$ be a decomposition of uvw. If $y'a$ is a prefix of u then $u = y'az$ and $y'' = zvw$ for some $z \in A^*$. Let $x' = y'$ and $x'' = zw$. As above $x'ax'' = uw$, $x' \underset{n}{\sim} y'$, and $x'' \underset{n}{\sim} y''$. If ay'' is a suffix of w then by symmetry it follows that there exist $x',x'' \in A^*$ such that

$x'ax'' = uw$, $x' \underset{n}{\sim} y'$, and $x'' \underset{n}{\sim} y''$.

The remaining case is when u is a prefix of y' and w is a suffix of y''. Then there exist $v_1, v_2 \in A^*$ such that $v = v_1 a v_2$, $y' = uv_1$, and $y'' = v_2 w$. Since $a \in \alpha(v) \subseteq \alpha(u_{n+1})$, $u_{n+1} = ras$ for some $r,s \in A^*$. Let $x' = u_1 \cdots u_n r$ and $x'' = sw$ so that $x'ax'' = u_1 \cdots u_n rasw = u_1 \cdots u_n u_{n+1} w = uw$. Now $u_1 \cdots u_n$ is n-full and $\alpha(u_n) \supseteq \alpha(u_{n+1} v_1) \supseteq \alpha(r)$ so that $x' = u_1 \cdots u_n r \underset{n}{\sim} u_1 \cdots u_n \underset{n}{\sim} u_1 \cdots u_n u_{n+1} v_1 = uv_1 = y'$. Also, w is n-full and $\alpha(w) \supseteq \alpha(s) \cup \alpha(v_2)$; hence $x'' = sw \underset{n}{\sim} w \underset{n}{\sim} v_2 w = y'$.

Therefore $uw \underset{n}{\leftrightarrows} uvw$. But $\underset{n+1G}{\equiv}$ is the smallest congruence satisfying $uw \underset{n+1G}{\equiv} uvw$ for all $u,\ v,\ w \in A^*$ such that u and w are $(n+1)$-full and $\alpha(u) = \alpha(w) \supseteq \alpha(y)$. Hence $x \underset{n+1G}{\equiv} y$ implies $x \underset{n}{\leftrightarrows} y$ for all $x,y \in A^*$

Proposition 59 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \underset{n+1}{\leftrightarrows} y$ implies $x \overset{(2)}{\underset{n}{\sim}} y$.

Proof: By induction on n.

Since $x \overset{(2)}{\underset{0}{\sim}} y$ for all $x,y \in A^*$ the result is true for $n = 0$. Suppose $n \geqslant 0$ and $x \underset{n+1}{\leftrightarrows} y$. If $x = 1$ then $y = 1$ so there is nothing to prove. Therefore assume $x \neq 1$.

Let $x = x_1 x_2$ be a decomposition of x. Since $x \neq 1$ either $x_1 \neq 1$ or $x_2 \neq 1$. Without loss of generality, assume $x_1 \neq 1$. Then $x_1 = x_0 a$ for some $a \in A$, $x_0 \in A^*$. But $x \underset{n+1}{\leftrightarrows} y$; therefore there exists a decomposition $y = y_0 a y_2$ such that $y_0 \underset{n}{\sim} x_0$ and $y_2 \underset{n}{\sim} x_2$. Let $y_1 = y_0 a$. Since $\underset{n}{\sim}$ is a congruence $y_1 = y_0 a \underset{n}{\sim} x_0 a = x_1$, so that $y = y_1 y_2$ is the required decomposition of y.

Similarly, for any decomposition $y = y_1 y_2$ of y there exists a decomposition $x = x_1 x_2$ of x such that $x_1 \underset{n}{\sim} y_1$ and $x_2 \underset{n}{\sim} y_2$. Hence $x \overset{(2)}{\underset{n}{\sim}} y$.

Proposition 60 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \Leftrightarrow_n y$ implies $x \underset{n}{\sim} y$.

Proof: By induction on n.

The result is clearly true for $n = 0$ since $x \underset{0}{\sim} y$ for all $x,y \in A^*$. Assume the result holds for n, and suppose $x \Leftrightarrow_{n+1} y$.

Let $u \in \mu_{n+1}(x)$. If $u = 1$ then $u \in \mu_{n+1}(y)$. Otherwise $u = av$ for some $a \in A$, $v \in A^*$. Since $u \in \mu_{n+1}(x)$, $x = x'ax''$ for some $x',x'' \in A^*$ such that $v \in (\mu_n(x''))^*$. But $x \Leftrightarrow_{n+1} y$ so there exist $y',y'' \in A^*$ such that $y = y'ay''$, $x' \Leftrightarrow_{n} y'$, and $x'' \Leftrightarrow_{n} y''$. By the induction hypothesis $x'' \underset{n}{\sim} y''$; therefore $v \in (\mu_n(y''))^*$. Thus $u = av \in \mu_n(y'ay'') = \mu_{n+1}(y)$. Hence $\mu_{n+1}(x) \subseteq \mu_{n+1}(y)$. Similarly, $\mu_{n+1}(y) \subseteq \mu_{n+1}(x)$, so that $x \underset{n+1}{\sim} y$.

Corollary 61 Let $x,y \in A^*$ and $n \geqslant 0$. Then $x \Leftrightarrow_{n} y$ implies $x \underset{n}{\leftrightarrow} y$.

Clearly $x \Leftrightarrow_{1} y$ if and only if $x \underset{1}{\leftrightarrow} y$ if and only if $x \underset{1}{\sim} y$. From Definitions 47 and 48 it then follows that $x \Leftrightarrow_{2} y$ if and only if $x \underset{2}{\leftrightarrow} y$.

Proposition 62 There does not exist an $n \geqslant 1$ such that $x \underset{n\,G}{\approx} y$ implies $x \Leftrightarrow_{3} y$ for all $x,y \in A^*$.

Proof: Let $x = (ab)^n$ and $y = (ab)^n a (ab)^n$. By Proposition 4(d), $x \underset{n\,G}{\approx} y$.

Now consider the decomposition $y = y'ay''$ of y where $y' = y'' = (ab)^n$. The decompositions of x of the form $x = x'ax'$ are

$$x' = (ab)^{n-1-i} \text{ and } x'' = b(ab)^i$$

where $0 \leqslant i \leqslant n-1$. But $x'' = b(ab)^i \not\Leftrightarrow_{2} (ab)^n = y''$ for any i, since there does not exist a decomposition $v'bv''$ of y'' such that $1 \Leftrightarrow_{1} v'$. Therefore $x \not\Leftrightarrow_{3} y$.

Proposition 63 There does not exist an $n \geqslant 0$ such that $x \underset{n}{\leftrightarrow} y$ implies $x \underset{2G}{\equiv} y$ for all $x,y \in A^*$.

Proof: Without loss of generality, assume $n \geqslant 4$, since $x \underset{i}{\leftrightarrow} y$ implies $x \underset{j}{\leftrightarrow} y$ for all i and j such that $i \geqslant j \geqslant 0$. Let $x = (ca)^n(ab)^n$ and $y = (ca)^n a (ab)^n$. The decompositions of x and y of the form udv where $d \in A$ are summarized in the following table. The value of i ranges from 0 to $n-1$.

decompositions of x			decompositions of y		
u	d	v	u	d	v
$(ca)^i$	c	$a(ca)^{n-1-i}(ab)^n$	$(ca)^i$	c	$a(ca)^{n-1-i}a(ab)^n$
$(ca)^i c$	a	$(ca)^{n-1-i}(ab)^n$	$(ca)^i c$	a	$(ca)^{n-1-i}a(ab)^n$
$(ca)^n(ab)^i$	a	$b(ab)^{n-1-i}$	$(ca)^n$	a	$(ab)^n$
$(ca)^n(ab)^i$	b	$(ab)^{n-1-i}$	$(ca)^n a(ab)^{n-1-i}$	a	$b(ab)^{n-1-i}$
			$(ca)^n a(ab)^{n-1-i}a$	b	$(ab)^{n-1-i}$

Since $(ca)^n$ and $(ab)^n$ are n-full it follows that $(ca)^n \underset{n}{\sim} (ca)^n a$ and $(ab)^n \underset{n}{\sim} a(ab)^n$. Hence for every decomposition $x = x'dx''$ there exists a decomposition $y = y'dy''$ such that $x' \underset{n}{\sim} y'$ and $x'' \underset{n}{\sim} y''$ and vice versa. Thus $x \underset{n+1}{\leftrightarrow} y$ and so $x \underset{n}{\leftrightarrow} y$.

Now $(ca)^4 a(ab)^4$ is the unique minimal element of its $\underset{2G}{\equiv}$ class and hence $(ca)^4 a(ab)^4 \underset{2G}{\not\equiv} (ca)^4(ba)^4$. But $(ca)^4(ab)^4 = (ca)^2(ca)^2(ab)^4 \underset{2G}{\equiv} (ca)^2(ca)^{n-4}(ca)^2(ab)^4 = (ca)^n(ab)^2(ab)^2 \underset{2G}{\equiv} (ca)^n(ab)^n$, and likewise $(ca)^4 a(ab)^4 \underset{2G}{\equiv} (ca)^n a(ab)^n$. Therefore $x = (ca)^n(ab)^n \underset{2G}{\not\equiv} (ca)^n a(ab)^n = y$.

Proposition 64 There does not exist an $n \geqslant 0$ such that $x \underset{n\,G}{\approxeq} y$ implies $x \underset{2}{\leftrightarrow} y$ for all $x,y \in A^*$.

Proof: Let $x = (ac)^n(ba)^n$ and $y = (ac)^n a(ba)^n$. Since $(ac)^n \underset{n\,R}{\sim} (ac)^n a$ and $(ba)^n \underset{n\,L}{\sim} a(ba)^n$, $x \underset{n\,G}{\approxeq} y$.

Consider the decomposition $y = y_1 a y_2$ of y where $y_1 = (ac)^n$ and $y_2 = (ba)^n$. The decompositions of x of the form $x = x_1 a x_2$ are:

$$x_1 = (ac)^i \text{ and } x_2 = c(ac)^{n-1-i}(ba)^n$$

$$\text{and } x_1 = (ac)^n(ba)^{n-1-i}b \text{ and } x_2 = (ba)^i$$

where $0 \leqslant i \leqslant n-1$.

In the first case $\alpha(x_2) = \{a,b,c\} \neq \{a,b\} = \alpha(y_2)$ so that $x_2 \underset{1}{\not\sim} y_2$, and in the second case $\alpha(x_1) = \{a,b,c\} \neq \{a,c\} = \alpha(y_1)$ so that $x_1 \underset{1}{\not\sim} y_1$.

Hence there does not exist a decomposition $x = x_1 a x_2$ such that $x_1 \underset{1}{\sim} y_1$ and $x_2 \underset{1}{\sim} y_2$. Thus $x \underset{2}{\not\leftrightarrow} y$.

The relationships proved in this section between the various congruences can be conveniently represented in the following diagram. A solid line from one congruence symbol to another indicates that the family of languages generated by the first set of congruences contains the family of languages characterized by the second set of congruences. A line with an × through it indicates that such a containment was shown not to hold. By transitivity, other relationships not explicitly drawn can be deduced.

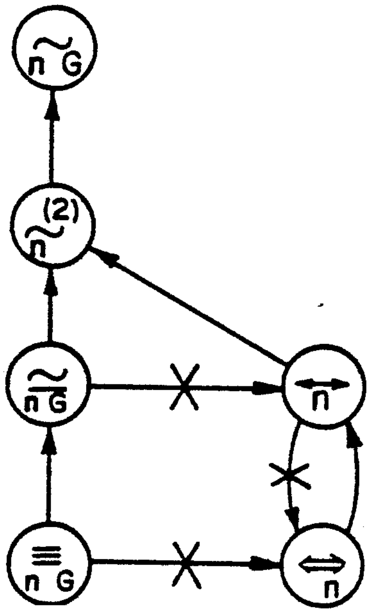

Figure 3

CHAPTER 5 DEFINITE AND RELATED LANGUAGES

The families of finite $\mathcal{J}$-trivial, $\mathcal{R}$-trivial, $\mathcal{L}$-trivial, and $\mathcal{G}$-trivial monoids can all be characterized by a condition involving the monoid and its idempotents. Specifically, M is

$\mathcal{J}$-trivial	if and only if	$eM_e \cup M_e e = e$	for all idempotents	$e \in M$
$\mathcal{R}$-trivial	if and only if	$eM_e = e$	for all idempotents	$e \in M$
$\mathcal{L}$-trivial	if and only if	$M_e e = e$	for all idempotents	$e \in M$
$\mathcal{G}$-trivial	if and only if	$eM_e \cap M_e e = e$	for all idempotents	$e \in M$

By replacing M_e by S, four other well known families are obtained. The first, finite semigroups in which $eS \cup Se = e$, characterize the set of finite and cofinite languages. Finite semigroups which satisfy $Se = e$, $eS = e$, and $eS \cap Se = e$ for all idempotents $e \in S$ are respectively definite [18], reverse definite [2], and generalized definite [13].

The following four theorems summarize some of their properties. Proofs of these results can be found in [8], [12], [23], [24], [30], and [34]. In all cases $X \subseteq A^*$ is a regular language, S is its syntactic semigroup, and $\mathbf{A} = <A,Q,q_0,F,\sigma>$ is the reduced automaton recognizing X. $\mathcal{W} = \{\{x\} \mid x \in A^*\}$ is the family of languages containing exactly one word. $\mathcal{F}$ and $\mathcal{C}$ represent the families of finite and cofinite languages respectively.

Theorem 1 (Finite/Cofinite Languages) The following are equivalent:

X1. X is a $\underset{n}{\mp}$ language for some $n \geqslant 0$, where $x \underset{n}{\mp} y$ if and only if $|x|, |y| \geqslant n$ or $x = y$ and $|x| < n$.

E1. $X \in (\mathcal{W} \cup A^*)\mathbf{B}$

E2. $X \in \mathcal{F} \cup \mathcal{C}$

S1. For all idempotents $e \in S, eS \cup Se = e$. (Every idempotent is a zero.)

A1. There exists an $n > 0$ such that for all $x \in A^n$, $y \in A^*$, and $q \in Q$, $\sigma(q,yx) = \sigma(q,x) = \sigma(q,xy)$.

Theorem 2 (Reverse Definite Languages) The following are equivalent:

X1. X is a $\overset{\cdot}{\underset{n}{\leftarrow}}$ language for some $n \geqslant 0$ where $x \overset{\cdot}{\underset{n}{\leftarrow}} y$ if and only if $f_n(x) = f_n(y)$.

E1. $X \in (W \cup WA^{\bullet})\mathbf{B}$

E2. $X \in (F^2 \cup FC \cup C^2)\mathbf{B}$

S1. For all idempotents $e \in S$, $eS = e$. (Every idempotent is a left zero.)

A1. There exists $n > 0$ such that for all $x \in A^n$, $y \in A^{\bullet}$, and $q \in Q$, $\sigma(q,xy) = \sigma(q,x)$.

Theorem 3 (Definite Languages) The following are equivalent:

X1. X is a $\overset{\cdot}{\underset{n}{\rightarrow}}$ language for some $n \geqslant 0$ where $x \overset{\cdot}{\underset{n}{\rightarrow}} y$ if and only if $t_n(x) = t_n(y)$.

E1. $X \in (W \cup A^{\bullet}W)\mathbf{B}$.

E2. $X \in (F^2 \cup CF \cup C^2)\mathbf{B}$.

S1. For all idempotents $e \in S$, $Se = e$ (Every idempotent is a right zero.)

A1. There exists $n > 0$ such that for all $x \in A^n$, $y \in A^{\bullet}$, and $q \in Q$, $\sigma(q,x) = \sigma(q,yx)$.

A2. There exists $n > 0$ such that for all $x \in A^n$, $p,q \in Q$, $\sigma(q,x) = \sigma(p,x)$.

Theorem 4 (Generalized Definite Languages) The following are equivalent:

X1. X is a $\overset{\cdot}{\underset{n}{\leftrightarrow}}$ language for some $n \geqslant 0$ where $x \overset{\cdot}{\underset{n}{\leftrightarrow}} y$ if and only if $f_n(x) = f_n(y)$ and $t_n(x) = t_n(y)$.

E1. $X \in (W \cup A^{\bullet})^2\mathbf{B} = (W \cup WA^{\bullet} \cup A^{\bullet}W)\mathbf{B}$.

E2. $X \in (F \cup C)^2\mathbf{B}$.

S1. For all idempotents $e \in S$, $eS \cap Se = eSe = e$. (Every idempotent is a middle zero).

A1. There exists $n \geqslant 0$ such that for all $x \in A^n$, $y \in A^{\bullet}$, and $q \in Q$, $\sigma(q,xyx) = \sigma(q,x)$.

In *J*-trivial monoids every idempotent is a local zero over its alphabet. *R*-trivial, *L*-trivial, and *G*-trivial monoids are such that every idempotent is a local left, local right, and local middle zero respectively. The congruences have this local nature too. Only letters from the alphabet of a word can be added to the word without changing its contents and hence its congruence class.

If, in addition, the concept of 'length n' is replaced by 'n-full' the definitions of $\underset{n}{\dot{-}}$, $\underset{n}{\dot{\leftarrow}}$, $\underset{n}{\dot{\rightarrow}}$, and $\underset{n}{\dot{\leftrightarrow}}$ parallel those of $\underset{n}{\sim}$, $\underset{n}{\equiv}_R$, $\underset{n}{\equiv}_L$, and $\underset{n}{\equiv}_G$.

A similar analogy between the automata of reverse definite and R-trivial, definite and L-trivial, and generalized definite and G-trivial monoids is also apparent. Look in particular at Theorem 2.65 property A4, Theorem 3.3 properties A3 and A4, and Proposition 4.27. In light of the above, Property A1 of Theorem 1 corresponds to Property A1 of Theorem 2.1.

Languages denoted by expressions in $(D \cup D\mathrm{A}^*)\mathbf{B}$, where $D = \{\mathrm{C}^*a \mid a \in \mathrm{A}, \mathrm{C} \subseteq \mathrm{A}-\{a\}\}\mathbf{M}$, are clearly generalizations of those in $(W \cup W\mathrm{A}^*)\mathbf{B}$ since $W = \{\{a\} \mid a \in A\}\mathbf{M} = \{\varnothing^*a \mid a \in \mathrm{A}\}\mathbf{M}$. The dual result for L-expressions also holds. If $D' = \{\mathrm{A}^*a\mathrm{A}^* \mid a \in \mathrm{A}\}\mathbf{M}$ then $(D' \cup \mathrm{A}^*)\mathbf{B}$ is the family of all languages with J-trivial monoids. The correspondence between G-trivial expressions and generalized definite expressions is not presently clear. When $\#\mathrm{A} \leqslant 2$, expressions more similar to those for finite/cofinite reverse definite, definite, and generalized definite have been found for languages with J-trivial, R-trivial, L-trivial, and G-trivial syntactic monoids, respectively. (See [3] and [5].) However, those results do not generalize to larger alphabets.

The families of finite/cofinite, definite, reverse definite, and generalized definite languages are just the beginning of an infinite hierarchy ([4] and [28]) whose next element is the family of locally testable languages and whose union is B_1. Can the J-trivial, L-trivial, R-trivial, G-trivial hierarchy be extended in a similar manner to yield B_2? If so, do there exist comparable hierarchies for each B_i, $i \geqslant 3$?

It is also unknown whether the families of languages defined in Section 4.5 are an important part of this hierarchy, nor is the relationship between them well understood. Providing alternate characterizations would certainly aid in the solution of these problems.

Bibliography

[1] Arbib, M.A.,(ed.), **Algebraic Theory of Machines, Languages, and Semigroups,** Academic Press, New York, 1968.

[2] Brzozowski, J.A., **Canonical Regular Expressions and Minimal State Graphs for Definite Events,** Mathematical Theory of Automata, New York, 1962, 529-561.

[3] Brzozowski, J.A., **Run Languages,** Discrete Mathematics 16 (1976), 299-307.

[4] Brzozowski, J.A., **Hierarchies of Aperiodic Languages,** R.A.I.R.O. Information Théorique 10 (1976), 35-49.

[5] Brzozowski, J.A., **A Generalization of Finiteness,** Semigroup Forum 13 (1977), 239-251.

[6] Brzozowski, J.A., Culik, K., and Gabrielian, A., **Classification of Noncounting Events,** J. Comput. System Sci. 5 (1971), 41-53.

[7] Brzozowski, J.A., and Knast, R., **The Dot-Depth Hierarchy of Star-Free Languages is Infinite,** J. Comput. System Sci. 16 (1978), 37-55.

[8] Brzozowski, J.A., and Simon, I., **Characterizations of Locally Testable Events,** Discrete Mathematics 4 (1973), 243-271.

[9] Clifford, A.H., and Preston, G.B., **The Algebraic Theory of Semigroups,** Volume 1, Math Surveys 7, Amer. Math. Soc., Providence, R.I., 1961.

[10] Cohen, R.S., and Brzozowski, J.A., **On Star-Free Events,** Proceedings of the Hawaii International Conference on System Sciences, University of Hawaii Press, Honolulu, Hawaii, 1968, 1-4.

[11] Cohen, R.S., and Brzozowski, J.A., **Dot Depth of Star-Free Events,** J. Comput. System Sci. 5 (1971), 1-16.

[12] Eilenberg, S., **Automata, Languages, and Machines,** Volume B, Academic Press, New York, 1976.

[13] Ginzburg, A., **About Some Properties of Definite, Reverse-Definite, and Related Automata,** IEEE Trans. Electronic Computers EC-15 (1966), 806-810.

[14] Ginzburg, A., **Algebraic Theory of Automata,** Academic Press, New York, 1968.

[15] Green, J.A., **On the Structure of Semigroups,** Annals of Math. 54 (1951), 163-172.

[16] Green, J.A., and Rees, D., **On Semigroups in which** $x^r = x$, Proc. Cambridge Philos. Soc. 48 (1952), 35-40.

[17] Jolley, L.B.W., **Summation of Series,** Second Revised Edition, Dover Publications Inc., New York, 1961.

[18] Kleene, S.C., **Representation of Events in Nerve Nets and Finite Automata,** in Automata Studies, Annals of Mathematics Studies 34, C.E.Shannon and J.McCarthy (eds.), Princeton University Press, Princeton, N.J., 1954, 3-41.

[19] McNaughton, R., and Papert, S., **Counter-Free Automata,** The M.I.T. Press, Cambridge, Mass., 1971.

[20] Meyer, A.R., **A Note on Star-Free Events,** J. ACM 16 (1969), 220-225.

[21] Meyer, A.R., and Thompson, C., **Remarks on Algebraic Decomposition of Automata,** Math. Systems Theory 3 (1969), 110-118.

[22] Papert, S. and McNaughton, R., **On Topological Events,** Theory of Automata, University

of Michigan Engineering Summer Conference, Ann Arbor, Mich., 1966.

[23] Perles, M., Rabin, M.O., and Shamir, E., **The Theory of Definite Automata,** IEEE Trans. on Electronic Computers EC-12 (1963), 233-243.

[24] Perrin, D., **Sur Certains Semigroupes Syntaxiques,** Séminaires de l'I.R.I.A. Logiques et Automates, 1971, 169-177.

[25] Rabin, M.O., and Scott, D., **Finite Automata and Their Decision Problems,** IBM J. Res. Dev. 3 (1959), 114-125.

[26] Schützenberger, M.P., **On Finite Monoids Having Only Trivial Subgroups,** Inform. and Control 8 (1965), 190-194.

[27] Schützenberger, M.P., **On a Family of Sets Related to McNaughton's L-Languages,** Automata Theory, E.R.Caianiello (ed.), Academic Press, New York, 1966, 320-324.

[28] Simon, I., **Hierarchies of Events with Dot-Depth One,** Ph.D. thesis, Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 1972.

[29] Simon, I., **Piecewise Testable Events,** in Automata Theory and Formal Languages, 2nd GI Conference, H. Brakhage (ed.), Lecture Notes in Computer Science 33, Springer-Verlag, Berlin, 1975, 214-222.

[30] Steinby, M., **On Definite Automata and Related Systems,** Ann. Acad. Sci. Fenn. Ser. AI 444, 1969.

[31] Stiffler, P.E., Jr., **Extensions of the Fundamental Theorem of Finite Semigroups,** Advances in Mathematics 11 (1973), 159-201.

[32] Therien, D., **Language Characterization of Finite Nilpotent and Solvable Groups,** University of Waterloo Computer Science Department Technical Report CS-78-44, 1978.

[33] Zalcstein, Y., **Remarks on Automata and Semigroups,** unpublished, 1971.

[34] Zalcstein, Y., **Locally Testable Languages,** J. Comput. System Sci. 6 (1972), 151-167.

Appendix

The SNOBOL4 program on the following page finds the unique minimal word (*minimal*) congruent to the input word (*word*). Some sample output from this program can be found on pages 99 and 100.

The primary data structure is an *m*-ary trie representing all subwords of length less than or equal to *n* found so far. Interior nodes are arrays of *m* pointers; leaves are integers in the range 0 to *n*. Label each edge in this structure by the index of the array cell in which the pointer that represents it is stored. In this way each path in the trie can be associated with a subword. A leaf with value *i* indicates that all subwords of length *i* have been found which have the same prefix as the labelled path to this leaf. This compression makes the searching faster as portions of the trie which are full (consisting of an array of *n*'s) do not have to be examined.

```
*This function succeeds, returning the null string, if concatenating letter to
*the end of minimal increases the n-contents of minimal. It fails otherwise.
*
update update = 'false'
       i = 1
do     update = ident(datatype(root[i]),'array')  update(root[i])          :f(for)
       root[i] = full(root[i]) n
for    i = lt(i,m) i + 1                                                    :s(do)
       (ident(datatype(root[letter]),'integer') lt(root[letter],n))       :f(done)
       root[letter] = eq(root[letter], n - 1) n                            :s(true)
       root[letter] = array(m,root[letter] + 1)
true   update =
done   ident(update)                                          :s(return)f(freturn)
*
*This function succeeds, returning the null string, if the trie with 'root' a
*is full.
*
full   j = 1
test   j = le(j,m) ident(a[j],n) j + 1                                     :s(test)
       gt(j,m)                                                :s(return)f(freturn)
*
*Initialization for the main program.
*
main   &anchor = 1
       &trim = 1
       define('update(root)i')
       define('full(a)j')
       m = input
       output = le(m,0) 'invalid alphabet size'                             :s(end)
       output = 'alphabet size is ' m
       n = input
       output = lt(n,0) 'invalid index'                                     :s(end)
       output = 'index of the congruence is ' n
*
*Read the next word and perform the necessary initialization.
*
read   word = input                                                         :f(end)
       output =
       output = word
       contents = gt(n,0) array(m,0)                                      :f(write)
       minimal =
*
*Process the word one letter at a time.
*
while  word break('123456789') span('0123456789') . letter =              :f(write)
       minimal = update(contents) minimal ' ' letter                      :f(while)
       full(contents)                                                     :f(while)
write  output = 'minimal congruent word is ' minimal                        :(read)
end    main
```

```
alphabet size is 3
index of the congruence is 2

1 2 3 3 2 3 1 3
minimal congruent word is  1 2 3 3 2 1

2 2 1 1 2
minimal congruent word is  2 2 1 1 2

1
minimal congruent word is  1


minimal congruent word is

2 2 1 2 2 2 3
minimal congruent word is  2 2 1 2 3

2 2 1 1
minimal congruent word is  2 2 1 1



alphabet size is 1
index of the congruence is 5

1 1 1 1 1 1 1
minimal congruent word is  1 1 1 1 1

1 1 1 1 1
minimal congruent word is  1 1 1 1 1

1 1
minimal congruent word is  1 1
```

```
alphabet size is 3
index of the congruence is 1

1 2 3
minimal congruent word is  1 2 3


minimal congruent word is

3 3 1 1 3 3 1 2
minimal congruent word is  3 1 2




alphabet size is 3
index of the congruence is 0


minimal congruent word is

3 1 2 1
minimal congruent word is




alphabet size is 12
index of the congruence is 6

10 3 10 10 10 10 10 10 3
minimal congruent word is  10 3 10 10 10 10 10 3
```

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF WATERLOO
TECHNICAL REPORTS 1979

Report No.	Author	Title
CS-79-01*	E.A. Ashcroft W.W. Wadge	Generality Considered Harmful - A Critique of Descriptive Semantics
CS-79-02*	T.S.E. Maibaum	Abstract Data Types and a Semantics for the ANSI/SPARC Architecture
CS-79-03*	D.R. McIntyre	A Maximum Column Partition for Sparse Positive Definite Linear Systems Ordered by the Minimum Degree Ordering Algorithm
CS-79-04*	K. Culik II A. Salomaa	Test Sets and Checking Words for Homomorphism Equivalence
CS-79-05*	T.S.E. Maibaum	The Semantics of Sharing in Parallel Processing
CS-79-06*	C.J. Colbourn K.S. Booth	Linear Time Automorphism Algorithms for Trees, Interval Graphs, and Planar Graphs
CS-79-07*	K. Culik, II N.D. Diamond	A Homomorphic Characterization of Time and Space Complexity Classes of Languages
CS-79-08*	M.R. Levy T.S.E. Maibaum	Continuous Data Types
CS-79-09	K.O. Geddes	Non-Truncated Power Series Solution of Linear ODE's in ALTRAN
CS-79-10*	D.J. Taylor J.P. Black D.E. Morgan	Robust Implementations of Compound Data Structures
CS-79-11*	G.H. Gonnet	Open Addressing Hashing with Unequal-Probability Keys
CS-79-12	M.O. Afolabi	The Design and Implementation of a Package for Symbolic Series Solution of Ordinary Differential Equations
CS-79-13*	W.M. Chan J.A. George	A Linear Time Implementation of the Reverse Cuthill-McKee Algorithm
CS-79-14	D.E. Morgan	Analysis of Closed Queueing Networks with Periodic Servers
CS-79-15*	M.H. van Emden G.J. de Lucena	Predicate Logic as a Language for Parallel Programming
CS-79-16*	J. Karhumäki I. Simon	A Note on Elementary Homorphisms and the Regularity of Equality Sets
CS-79-17*	K. Culik II J. Karhumäki	On the Equality Sets for Homomorphisms on Free Monoids with two Generators
CS-79-18*	F.E. Fich	Languages of R-Trivial and Related Monoids

* Out of print - contact author

CS-79-19*	D.R. Cheriton	Multi-Process Structuring and the Thoth Operating System
CS-79-20*	E.A. Ashcroft W.W. Wadge	A Logical Programming Language
CS-79-21*	E.A. Ashcroft W.W. Wadge	Structured LUCID
CS-79-22	G.B. Bonkowski W.M. Gentleman M.A. Malcolm	Porting the Zed Compiler
CS-79-23*	K.L. Clark M.H. van Emden	Consequence Verification of Flowcharts
CS-79-24*	D. Dobkin J.I. Munro	Optimal Time Minimal Space Selection Algorithms
CS-79-25*	P.R.F. Cunha C.J. Lucena T.S.E. Maibaum	On the Design and Specification of Message Oriented Programs
CS-79-26*	T.S.E. Maibaum	Non-Termination, Implicit Definitions and Abstract Data Types
CS-79-27*	D. Dobkin J.I. Munro	Determining the Mode
CS-79-28	T.A. Cargill	A View of Source Text for Diversely Configurable Software
CS-79-29*	R.J. Ramirez F.W. Tompa J.I. Munro	Optimum Reorganization Points for Arbitrary Database Costs
CS-79-30	A. Pereda R.L. Carvalho C.J. Lucena T.S.E. Maibaum	Data Specification Methods
CS-79-31*	J.I. Munro H. Suwanda	Implicit Data Structures for Fast Search and Update
CS-79-32*	D. Rotem J. Urrutia	Circular Permutation Graphs
CS-79-33*	M.S. Brader	PHOTON/532/Set - A Text Formatter
CS-79-34*	D.J. Taylor D.E. Morgan J.P. Black	Redundancy in Data Structures: Improving Software Fault Tolerance
CS-79-35	D.J. Taylor D.E. Morgan J.P. Black	Redundancy in Data Structures: Some Theoretical Results
CS-79-36	J.C. Beatty	On the Relationship between the LL(1) and LR(1) Grammars
CS-79-37	E.A. Ashcroft W.W. Wadge	R_x for Semantics

* Out of print - contact author

CS-79-38	E.A. Ashcroft W.W. Wadge	Some Common Misconceptions about LUCID
CS-79-39	J. Albert K. Culik II	Test Sets for Homomorphism Equivalence on Context Free Languages
CS-79-40	F.W. Tompa R.J. Ramirez	Selection of Efficient Storage Structures
CS-79-41*	P.T. Cox T. Pietrzykowski	Deduction Plans: A Basis for Intelligent Backtracking
CS-79-42	R.C. Read D. Rotem J. Urrutia	Orientations of Circle Graphs

* Out of print - contact author

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF WATERLOO

RESEARCH REPORTS 1980

Report No.	Author	Title
CS-80-01	P.T. Cox T. Pietrzykowski	On Reverse Skolemization
CS-80-02	K. Culik II	Homomorphisms: Decidability, Equality and Test Sets
CS-80-03	J. Brzozowski	Open Problems About Regular Languages
CS-80-04	H. Suwanda	Implicit Data Structures for the Dictionary Problem
CS-80-05	M.H. van Emden	Chess-Endgame Advice: A Case Study in Computer Utilization of Knowledge
CS-80-06	Y. Kobuchi K. Culik II	Simulation Relation of Dynamical Systems
CS-80-07	G.H. Gonnet J.I. Munro H. Suwanda	Exegesis of Self-Organizing Linear Search
CS-80-08	J.P. Black D.J. Taylor D.E. Morgan	An Introduction to Robust Data Structures
CS-80-09	J.Ll. Morris	The Extrapolation of First Order Methods for Parabolic Partial Differential Equations II
CS-80-10*	N. Santoro H. Suwanda	Entropy of the Self-Organizing Linear Lists
CS-80-11	T.S.E. Maibaum C.S. dos Santos A.L. Furtado	A Uniform Logical Treatment of Queries and Updates
CS-80-12	K.R. Apt M.H. van Emden	Contributions to the Theory of Logic Programming
CS-80-13	J.A. George M.T. Heath	Solution of Sparse Linear Least Squares Problems Using Givens Rotations
CS-80-14	T.S.E. Maibaum	Data Base Instances, Abstract Data Types and Data Base Specification
CS-80-15	J.P. Black D.J. Taylor D.E. Morgan	A Robust B-Tree Implementation
CS-80-16	K.O. Geddes	Block Structure in the Chebyshev-Padé Table
CS-80-17	P. Calamai A.R. Conn	A Stable Algorithm for Solving the Multi-facility Location Problem Involving Euclidean Distances

* In preparation

CS-80-18	R.J. Ramirez	Efficient Algorithms for Selecting Efficient Data Storage Structures
CS-80-19	D. Therien	Classification of Regular Languages by Congruences
CS-80-20	J. Buccino	A Reliable Typesetting System for Waterloo
CS-80-21	N. Santoro	Efficient Abstract Implementations for Relational Data Structures
CS-80-22	R.L. de Carvalho T.S.E. Maibaum T.H.C. Pequeno A.A. Pereda P.A.S. Veloso	A Model Theoretic Approach to the Theory of Abstract Data Types and Data Structures
CS-80-23	G.H. Gonnet	A Handbook on Algorithms and Data Structures
CS-80-24	J.P. Black D.J. Taylor D.E. Morgan	A Case Study in Fault Tolerant Software
CS-80-25	N. Santoro	Four 0(n**2) Multiplication Methods for Sparse and Dense Boolean Matrices
CS-80-26	J.A. Brzozowski	Development in the Theory of Regular Languages
CS-80-27	J. Bradford T. Pietrzykowski	The Eta Interface
CS-80-28	P. Cunha T.S.E. Maibaum	Resource = Abstract Data Type Data + Synchronization ...
CS-80-29	K. Culik II Arto Salomaa	On Infinite Words Obtained by Interating Morphisms
CS-80-30	T.F. Coleman A.R. Conn	Nonlinear Programming via an Exact Penalty Function: Asymptotic Analysis
CS-80-31	T.F. Coleman A.R. Conn	Nonlinear Programming via an Exact Penalty Function: Global Analysis
CS-80-32	P.R.F. Cunha C.J. Lucena T.S.E. Maibaum	Message Oriented Programming - A Resource Based Methodology
CS-80-33	Karel Culik II Tero Harju	Dominoes Over A Free Monoid