WITH

DOT-DEPTH ONE

by

Imre Simon

Faculty of Mathematics

University of Waterloo

Waterloo, Ontario

Canada

Department of Applied Analysis

&

Computer Science

HIERARCHIES OF EVENTS

WITH

DOT-DEPTH ONE

by

Imre Simon

A Thesis

Submitted in Partial Fulfillment

of the Requirements for

the degree of

DOCTOR OF PHILOSOPHY

at the

University of Waterloo

Waterloo, Ontario, Canada

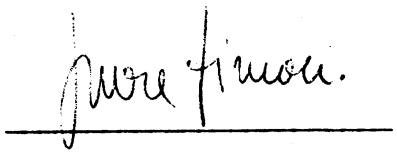
Department of Applied Analysis

and Computer Science

August, 1972

I hereby declare that I am the sole author of this thesis.

I authorize the University of Waterloo to lend it to other institutions or individuals for the purpose of scholarly research.

Signature 

To my wife Gabriella

and to my children, Claudio and Liliana.

Acknowledgements

I wish to express my sincere appreciation to Professor J.A. Brzozowski for introducing me to the subject of this thesis and for the many pleasant hours we spent in discussing it.

I extend my gratitude to Mrs. Jacqueline Macpherson for her patience and skill in typing this manuscript.

The financial assistance of the Fundacão de Amparo à Pesquisa do Estado de São Paulo, Brasil under grant 69-72/400 and that of the National Research Council of Canada under grant A-1617 is gratefully acknowledged. I also wish to thank the Instituto de Matemática e Estatística da Universidade de São Paulo, Brasil for granting the leave which made this work possible.

I also wish to thank the members of the examining committee: E.A. Ashcroft, K. Culik, R. McNaughton and H.S. Shank for their useful comments and suggestions.

Abstract

The family B_2 of regular star-free events of dot-depth not greater than one is subdivided in families $\alpha_{m,k}$ for integers $m \geq 0$ and $k > 0$. Roughly speaking, $\alpha_{m,k}$ is the family of those events E, for which membership of x in E can be determined by testing the first and last k-1 letters of x, as well as the set of m-tuples of subwords of length k which occur in x. Each $\alpha_{m,k}$ is a Boolean algebra and contains all $\alpha_{n,\ell}$, where $n \leq m$ and $\ell \leq k$. Denoting by δ_m and γ_k the union of all $\alpha_{m,\ell}$ $(\ell = 1,2,\ldots)$ and $\alpha_{n,k}$ $(n = 0,1,\ldots)$ respectively, one obtains the δ-hierarchy $(\delta_0 \subseteq \delta_1 \subseteq \ldots)$ and the γ-hierarchy $(\gamma_1 \subseteq \gamma_2 \subseteq \ldots)$ of Boolean algebras. It is shown that the union of each hierarchy is precisely the family B_2 and that both hierarchies are infinite. An alternate formulation of the δ-hierarchy is obtained by relating it to the B_2-hierarchy $(\beta_1 \subseteq \beta_2 \subseteq \ldots)$ where β_n is the smallest Boolean algebra containing concatenations of n events, each of which is either finite or cofinite. It follows that the B_2-hierarchy is also infinite. A structural characterization is obtained for each of the above mentioned families, thus showing that the definitions are natural.

The families δ_0 and δ_1 turn out to be the well known families of generalized definite and locally testable events. Locally testable events and the family γ_1 are characterized, in the sense that algorithms are given for deciding whether an event is in these

families. The first of these results solves a long standing open problem. Let E be an event and let S be its syntactic semigroup. We show that E is locally testable iff for each idempotent e in S, eSe is an idempotent and commutative monoid. We also prove that E is in γ_1 iff S is $\mathcal{J}$-trivial, i.e. each $\mathcal{J}$-class of S consists of a single element. Finally, we show that if E is in B_2, then for each idempotent e in S, eSe is a $\mathcal{J}$-trivial monoid. We conjecture that this necessary condition is sufficient as well.

Contents

List of Propositions

		Chapter				
		1	2	3	4	5
Corollary	1	-	19	62	71	118
	2	-	36	-	72	-
	3	-	-	-	77	-
	4	-	-	-	83	-
	5	-	-	-	91	-
Lemma	1	5	20	57	84	-
	2	5	30	57	86	-
	3	-	32	59	88	-
	4	-	48	-	-	-
Proposition	1	6	17	52	67	115
	2	11	18	63	67	-
	3	12	20	66	68	-
	4	-	22	-	68	-
	5	-	23	-	71	-
	6	-	23	-	72	-
	7	-	39	-	72	-
	8	-	-	-	74	-
	9	-	-	-	75	-
	10	-	-	-	78	-

		Chapter				
		1	2	3	4	5
Proposition	11	-	-	-	81	-
	12	-	-	-	83	-
	13	-	-	-	83	-
	14	-	-	-	100	-
	15	-	-	-	111	-
	16	-	-	-	112	-
Theorem	1	7	29	61	76	-
	2	-	42	64	77	-
	3	-	43	64	89	-
	4	-	46	65	91	-
	5	-	48	-	93	-
	6	-	-	-	95	-
	7	-	-	-	100	-

Index of Symbols

Index of Definitions

Note

Definitions, lemmas, propositions, theorems and corollaries are numbered sequentially within each chapter. Thus a reference to theorem 2 means theorem 2 of the chapter in which the reference appears. A reference to proposition 3.2 means proposition 2 of chapter 3.

The symbol $\square$ is used to mark the end of a proof.

The symbol iff means if and only if.

CHAPTER 1

Introduction

We begin with establishing our notation in section 1. In section 2 we describe previous work upon which this thesis is based. Finally, in section 3 we give a summary of the development in subsequent chapters.

1. Preliminaries.

The main purpose of this section is to indicate our notation. To do this, we give a number of standard definitions from automata and semigroup theory. At the end of the section, we prove some results which will be used throughout the thesis.

Our notation is based on that of Ginzburg [G1] and we use the standard notation for semigroups; see for instance Clifford and Preston [CP].

Let S be a nonempty set and let $\circ$ denote a binary operation in S, usually called multiplication. The system $\langle S,\circ\rangle$ is a semigroup if $\circ$ is an associative operation, i.e. for all $a,b,c \in S$ $(a\circ b)\circ c = a\circ(b\circ c)$. A monoid is a semigroup $\langle S,\circ\rangle$ with an identity element $\Lambda \in S$, such that $a\circ\Lambda = \Lambda\circ a = a$ for all $a \in S$. As usual, we denote $a\circ b$ by ab and $\langle S,\circ\rangle$ by S. Let $e \in S$, then e is idempotent if $e = ee$. A semigroup S is group-free if every subgroup of S is trivial, i.e. contains one element only.

Let S be a semigroup, then S^1 is a monoid obtained as follows: if S is a monoid, then $S^1 = S$; otherwise $S^1 = S \cup \{\Lambda\}$,

where Λ is an identity for S^1 and multiplication in S is unchanged.

Let S be a semigroup and let ρ be an equivalence relation on S; ρ is a <u>congruence</u> on S if for all $c \in S$, $a \rho b$ implies $ac \rho bc$ and $ca \rho cb$. S/ρ denotes the factor semigroup of S modulo ρ.

Let Σ be a nonempty finite set, called <u>alphabet</u> and let Σ^* denote the free monoid generated by Σ. The elements of Σ^* are called <u>words</u> and the binary operation for Σ^* is called <u>concatenation</u>. The <u>empty word</u> in Σ^* is denoted by λ and it is the identity in Σ^*. Let $x \in \Sigma^*$. The <u>length</u> of x is denoted by $|x|$; it is defined by $|\lambda| = 0$ and $|y\sigma| = |y| + 1$ for $y \in \Sigma^*$ and $\sigma \in \Sigma$. The <u>reverse</u> of x is denoted by x^T; it is defined by $\lambda^T = \lambda$ and $(y\sigma)^T = \sigma y^T$ for $y \in \Sigma^*$ and $\sigma \in \Sigma$. Let $x,y,z \in \Sigma^*$ be such that $x = yz$, then y (z) is a <u>prefix</u> (<u>suffix</u>) of x. The free semigroup generated by Σ is denoted by Σ^+; we have $\Sigma^+ = \Sigma^* - \{\lambda\}$. A <u>language</u> over Σ is a subset L of Σ^*.

Let $L \subseteq \Sigma^*$ be a language and let $\equiv \pmod{L}$ be the relation over Σ^+, defined by

$$x \equiv y \pmod{L} \text{ iff for all } u,v \in \Sigma^*,\ uxv \in L \text{ iff } uyv \in L.$$

The factor semigroup $\Sigma^+/\equiv \pmod{L}$ is called the <u>syntactic semigroup</u> of L.

Let f be a function, $f:A \to B$, and let $x \in A$; we denote the image of x by $f(x)$ or xf. If $X \subseteq A$, $Xf = \{xf \mid x \in X\}$. If $g:B \to C$ then the <u>composition</u> of f with g, fg, is $fg:A \to C$, where $x(fg) = (xf)g$. We also use xfg or $g(f(x))$ to denote $x(fg)$.

An initialized semiautomaton (semiautomaton for short) is a quadruple $A = (Q,\Sigma,M,q_0)$ where Q and Σ are nonempty finite sets (of states and inputs respectively), $q_0 \in Q$ is the initial state and M is a set of functions $\sigma^A:Q \to Q$, one for each $\sigma \in \Sigma$. For $q \in Q$, $q\sigma^A \in Q$ is the next-state of q under input $\sigma \in \Sigma$. For $x \in \Sigma^*$ the function $x^A:Q \to Q$ is defined inductively: λ^A is the identity function on Q, and if $x = y\sigma$, $\sigma \in \Sigma$, then $x^A = y^A\sigma^A$. Clearly, for all $x,y \in \Sigma^*$, $(xy)^A = x^Ay^A$. For $x \in \Sigma^*$ $x^0 = \lambda$, $(x^A)^0 = \lambda^A$, and for any integer $k \geq 0$, $x^{k+1} = x^kx$ and $(x^A)^{k+1} = (x^A)^kx^A$. Clearly $(x^k)^A = (x^A)^k$. A semiautomaton A is connected if for every $q \in Q$ there exists an $x \in \Sigma^*$ such that $q_0x^A = q$. A is permutation-free if for any $R \subseteq Q$, any $x \in \Sigma^*$, $Rx^A = R$ implies $rx^A = r$ for all $r \in R$.

Let A be a semiautomaton. The set of functions

$$\{x^A \mid x \in \Sigma^+\}$$

is a finite semigroup under composition of functions. It is denoted by S_A and is called the semigroup of A. Note that S_A is not necessarily a monoid; it is a monoid iff there exist a nonempty word $x \in \Sigma^+$, such that for all $q \in Q$, $qx^A = q$. The monoid of A, denoted by G_A, is the set of functions

$$\{x^A \mid x \in \Sigma^*\};$$

multiplication in G_A is the composition of functions. Note that G_A is isomorphic to S_A^1. As will be seen later, the distinction between G_A and S_A is essential in this thesis. We warn the reader that in general this distinction is not made clear in standard textbooks.

An automaton is a quintuple $\hat{A} = (Q,\Sigma,M,q_0,F)$ where $A = (Q,\Sigma,M,q_0)$ is a semiautomaton, called the semiautomaton of $\hat{A}$, and F is a subset of Q, called the set of final states. The language accepted by $\hat{A}$ is

$$E = \{x \mid x \in \Sigma^* \text{ and } q_0x^A \in F\}.$$

$\hat{A}$ is reduced if A is connected and for every two distinct states $p,q \in Q$, there exists an $x \in \Sigma^*$, such that $px^A \in F$ iff $qx^A \notin F$.

It is well known that a language is regular iff there exists an automaton $\hat{B}$ accepting E iff there exists a reduced automaton $\hat{A}$ accepting E. This reduced automaton $\hat{A}$ is unique (up to isomorphism) and S_A is isomorphic to the syntactic semigroup of E. A regular language is called an event.

Let $A = (Q,\Sigma,M,q_0)$ and $B = (R,\Sigma,N,r_0)$ be semiautomata. The direct product of A and B is the semiautomaton $A \times B = (Q\times R,\Sigma,P,(q_0,r_0))$ where for all $\sigma \in \Sigma$, $(q,r)\sigma^{A\times B} = (q\sigma^A,r\sigma^B)$. A is covered by B, $A \leq B$, if there exist $R_1 \subseteq R$ and an onto function $\eta:R_1 \to Q$, such that $r_0 \in R_1$, $r_0\eta = q_0$ and for all $r \in R_1$ and $\sigma \in \Sigma$, $r\sigma^B \in R_1$ and $r\sigma^B\eta = r\eta\sigma^A$. Let π be a function $\pi:R \to 2^Q$; then B is a π-factor of A, $B = A/\pi$, if the following hold:

(i) $\bigcup_{r\in R} r\pi = Q$,

(ii) for every $r \in R$ and $\sigma \in \Sigma$ $r\pi\sigma^A \subseteq r\sigma^B\pi$,

(iii) $q_0 \in r_0\pi$.

Let $A = (Q,\Sigma,M,q_0)$ and $B = (R,Q\times\Sigma,N,r_0)$ be semiautomata. The cascade product of A and B is the semiautomaton $A\circ B = (Q\times R,\Sigma,P,(q_0,r_0))$ where $(q,r)\sigma^{A\circ B} = (q\sigma^A,r(q,\sigma)^B)$.

For a finite set A, $\#A$ denotes the cardinality of A.

Now we have the following general results which will be used later on.

Lemma 1. Let $A = (Q,\Sigma,M,q_0)$ be a permutation-free semiautomaton and let $n = \#Q$. Then, for every $x \in \Sigma^*$, $(x^n)^A = (x^{n+1})^A$.

Proof. It is clear that

$$Q \supseteq Qx^A \supseteq Q(x^2)^A \supseteq \ldots \supseteq Q(x^n)^A \supseteq Q(x^{n+1})^A.$$

Furthermore, for all $p \geq 0$, $Q(x^{p+1})^A \supsetneq Q(x^{p+2})^A$ implies $Q(x^p)^A \supsetneq Q(x^{p+1})^A$. Thus, $Q(x^n)^A \supsetneq Q(x^{n+1})^A$ implies that all $n + 1$ inclusions in the chain are proper; this is a contradiction since $n = \#Q$. Therefore $Q(x^n)^A = Q(x^{n+1})^A$. Since A is permutation-free, it follows that for all $q \in Q$, $q(x^n)^A = q(x^{n+1})^A$. Hence $(x^n)^A = (x^{n+1})^A$. □

Lemma 2. Let $A = (Q,\Sigma,M,q_0)$ and $B = (R,\Sigma,N,r_0)$ be semiautomata, and assume that A is connected. Then $A \leq B$ iff for all $x,y \in \Sigma^*$, $r_0x^B = r_0y^B$ implies $q_0x^A = q_0y^A$.

Proof. If $A \leq B$, there exists an onto function $\eta:R_1 \to Q$; where $r_0 \in R_1 \subseteq R$, such that $r_0\eta = q_0$ and for all $r \in R_1$ and $\sigma \in \Sigma$ $r\sigma^B \in R_1$ and $r\sigma^B\eta = r\eta\sigma^A$. This implies that for all $x \in \Sigma^*$, $rx^B \in R_1$ and $rx^B\eta = r\eta x^A$. Thus, if $r_0x^B = r_0y^B$, then $r_0x^B\eta = r_0y^B\eta$ and also $r_0x^B\eta = r_0\eta x^A = q_0x^A$ and $r_0y^B\eta = r_0\eta y^A = q_0y^A$. Hence $q_0x^A = q_0y^A$. Conversely, if for all $x,y \in \Sigma^*$, $r_0x^B = r_0y^B$ implies $q_0x^A = q_0y^A$, then we can define a function η by $r_0x^B\eta = q_0x^A$.

Since A is connected, η is onto Q and clearly η satisfies the conditions in the definition of $A \leq B$. □

Proposition 1. Let ρ be a congruence relation over Σ^*, and let $\hat{A} = (Q,\Sigma,M,q_0,F)$ be the reduced automaton accepting the event E. E is a union of congruence classes of ρ iff for all $x,y \in \Sigma^*$, $x \rho y$ implies $x^A = y^A$.

Proof. Let E be a union of congruence classes of ρ, and suppose that for some $x,y \in \Sigma^*$ $x \rho y$ and $x^A \neq y^A$. Then there exists $q \in Q$, such that $qx^A \neq qy^A$. Since $\hat{A}$ is reduced, there exist $u,v \in \Sigma^*$, such that $q_0u^A = q$, and $q(xv)^A \in F$ iff $q(yv)^A \notin F$. Thus $uxv \in E$ iff $uyv \notin E$. On the other hand, since ρ is a congruence, and $x \rho y$, it follows that $uxv \rho uyv$. Since E is a union of congruence classes of ρ, $uxv \in E$ iff $uyv \in E$, a contradiction. Conversely, let $x \rho y$. Then $x^A = y^A$ by assumption, and hence $x \in E$ iff $y \in E$. Thus, E is a union of congruence classes of ρ. □

2. Generation of star-free events.

This section is based on previous work by several authors. It contains the general setting for our investigation in the remainder of this thesis. We begin with a short review of the theory of star-free events; an extensive treatment of this subject can be found in McNaughton and Papert's monograph [MP].

An event is star-free iff it can be denoted by a regular expression using only Boolean operations and concatenations. Note that Σ^* is star-free, since $\Sigma^* = \overline{\phi}$. In regular expressions we will denote Σ^* by I, when Σ is understood. Now, let $\Sigma = \{0,1\}$; the events $E_1 = 0^*$, $E_2 = (01)^*$ and $E_3 = (01 \cup 10)^*$ are star-free events, since we have:

$$E_1 = 0^* = \overline{I1I},$$

$$E_2 = (01)^* = \lambda \cup (0I \cap I1 \cap \overline{I00I} \cap \overline{I11I}),$$

and $$E_3 = (01 \cup 10)^* = \overline{\overline{I0}\ A\ \overline{0I} \cup \overline{I1}\ B\ \overline{1I}},$$

where $$A = 1(01)^* = 1I \cap I1 \cap \overline{I00I} \cap \overline{I11I},$$

and $$B = 0(10)^* = 0I \cap I0 \cap \overline{I00I} \cap \overline{I11I}.$$

The validity of the above equalities can be verified by well known techniques. We note here that in general, it requires some ingenuity to obtain these star-free expressions and to our knowledge no "reasonable" algorithm exists to obtain them. The family of star-free events has a number of different characterizations; we summarize some of these in the following theorem.

Theorem 1. Let $\hat{A}$ be the reduced automaton accepting the event E. The following are equivalent:

(a) E is star-free.

(b) A is permutation-free.

(c) S_A is group-free.

(d) There exists an integer n, such that for all $a \in S_A$, $a^n = a^{n+1}$.

(e) There exists an integer ℓ and 2-state identity resets [see G1] $B_1, B_2, \ldots, B_\ell$, such that $A \leq ((B_1 \circ B_2) \circ \ldots \circ B_\ell)$.

The equivalence of (a) and (c) was first proved by Schützenberger [S1, S2]. The equivalence of (b), (c) and (d) are proved by McNaughton and Papert [MP] who also prove the equivalence of these and (a), as well as a number of other characterizations of star-free events. The implication (c) implies (e) is a corollary of the Krohn-Rhodes decomposition theorem for finite semigroups. There are several proofs of this theorem, see for instance [KR, KRT, Z3, Z4, G1, MT]. The implication (e) implies (a) has been proved by Meyer [M2, G1] and Cohen and Brzozowski [CB].

In [CB], Cohen and Brzozowski define the dot-depth of a star-free event and subdivide the family of star-free events into Boolean algebras, according to their dot-depth. Now we summarize their work. Let $\Sigma = \{\sigma_0, \sigma_1, \ldots, \sigma_n\}$. One can generate the family of star-free events over Σ^*, by starting with the family $E_0 = \{\{\sigma_0\}, \ldots, \{\sigma_n\}, \{\lambda\}, \phi\}$ of <u>basic</u> events (requiring no operations) and form a sequence of families by taking the closure of the previous family under Boolean operations and concatenation alternately. Thus, depending whether Boolean operations or concatenation is applied first, one obtains two sequences of families. More formally, let K be a family of events.

Denote by $B(K)$ and $M(K)$ the smallest family of events containing K and closed under Boolean operations and concatenation respectively. Let $B_1 = B(E_0)$, $M_n = M(B_n)$ for $n \geq 1$ and let $B_n = B(M_{n-1})$ for $n > 1$. Thus, starting with closure under Boolean operations, we have the sequence of families

$$E_0 \subseteq B_1 \subseteq M_1 \subseteq B_2 \subseteq M_2 \subseteq \cdots \quad . \tag{1}$$

Considering only the Boolean algebras in (1), we have the dot-depth hierarchy

$$B_1 \subseteq B_2 \subseteq \cdots \quad .$$

Clearly the union of all B_i's is the family of star-free events. The dot-depth of a star-free event E is the smallest integer n, such that $E \in B_{n+1}$. Now, let $\hat{M}_1 = M(E_0)$, $\hat{B}_n = B(\hat{M}_n)$ for $n \geq 1$ and $\hat{M}_n = M(\hat{B}_{n-1})$ for $n > 1$. Starting with closure under concatenation, we have the following sequence of families

$$E_0 \subseteq \hat{M}_1 \subseteq \hat{B}_1 \subseteq \hat{M}_2 \subseteq \hat{B}_2 \subseteq \cdots \quad , \tag{2}$$

whose union is again the family of star-free events. It has been shown [CB] that $B_2 = \hat{B}_2$ and thus, apart from an initial portion, the sequences (1) and (2) are identical. We represent the situation in figure 1.

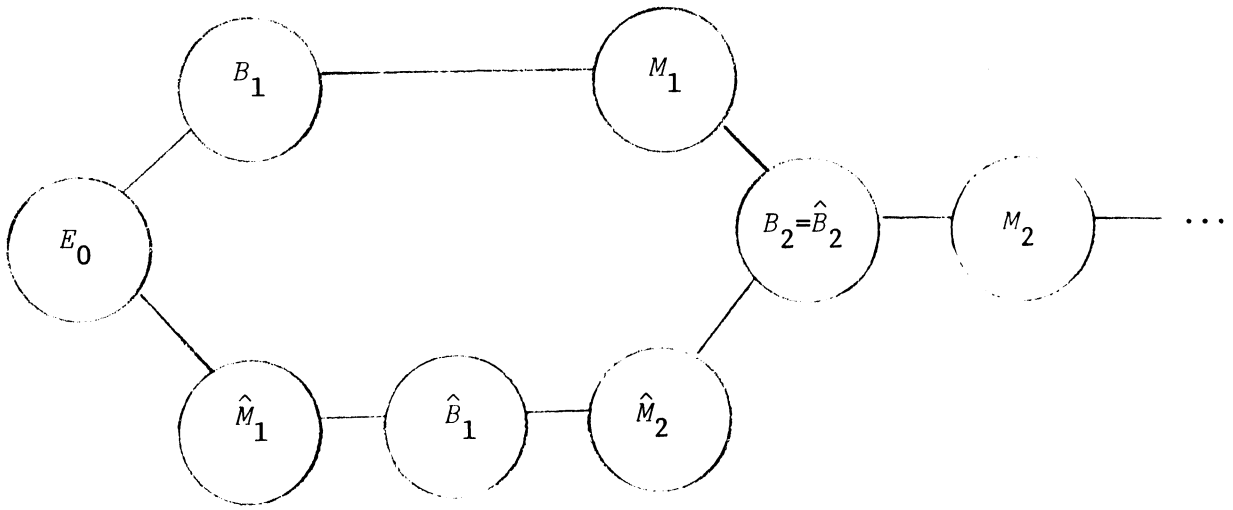


Figure 1 Generation of star-free events.

3. Synopsis.

In this section we give a brief description of the development in subsequent chapters.

First we note that very little is known about the dot-depth hierarchy. It is not known whether the hierarchy is finite or infinite, in fact it is not known whether B_3 is properly contained in the family of star-free events; i.e. whether there exist star-free events of dot-depth 3. Another open problem concerns the family B_2 of star-free events with dot-depth at most one. There is no known algorithm to test whether an event is in B_2. This is the first interesting family in the dot-depth hierarchy, since B_1 is easily seen to be a finite Boolean algebra. Of course, no characterization, in fact not even a necessary condition for membership, is known for the families B_n, $n > 2$.

Our thesis is motivated by an effective characterization of B_2. As will be seen, we could not obtain this result, we only have an effective necessary condition for membership in B_2, and we conjecture that this condition is sufficient as well. However, by studying the family B_2 we found results and subfamilies of B_2 which are interesting in their own right. At the same time we were able to prove our conjecture in two particular cases.

First we define a hierarchy of Boolean algebras whose union is B_2. An event is cofinite iff its complement is finite. Let F and C denote the families of finite and cofinite events respectively. It is easy to see that $F \cup C$ is a Boolean algebra and that $\hat{B}_1 = F \cup C$.

Let $\beta_m = B((F \cup C)^m)$ for $m \geq 1$, where $(F \cup C)^m$ denotes the family of events expressible as concatenations of m events, each of which is either finite or cofinite. Since $F \cup C$ is a Boolean algebra, we have $\beta_1 = F \cup C = \hat{B}_1$. Clearly $\beta_m \subseteq \beta_{m+1}$ for all $m \geq 1$. We have:

Definition 1. The B_2-hierarchy is the sequence of Boolean algebras

$$\beta_1 \subseteq \beta_2 \subseteq \beta_3 \subseteq \beta_4 \subseteq \cdots \quad .$$

Clearly $\bigcup_{m \geq 1} \beta_m = B_2$.

Proposition 2. For all $m \geq 1$, $\beta_{2m+1} = \beta_{2m+2}$.

Proof. Note that β_m can be defined equivalently as the smallest Boolean algebra containing all events in the family $[w,I]^m$, which we define as the set of all concatenations of m factors, each of which is either a word w in Σ^* or is I. This follows from the fact that each finite event is a finite union of words, and each cofinite event is expressible as a finite union of words and of events of the form wI, for $w \in \Sigma^*$. Thus $\beta_m = B((F \cup C)^m) = B([w,I]^m)$. Now, the only events in $[w,I]^{2m+2} - [w,I]^{2m+1}$ are those of the form $E_1 = wIw_1Iw_2 \ldots Iw_mI$ or $E_2 = Iw_1Iw_2 \ldots Iw_mIw$. However, $E_1 = wI \cap \Sigma^{|w|} Iw_1Iw_2 \ldots Iw_mI = wI \cap I\Sigma^{|w|} w_1Iw_2 \ldots Iw_mI$. Thus E_1 can be expressed as a Boolean function of products in $[w,I]^{2m+1}$, and the same is true for E_2. Hence, for $m \geq 1$, $[w,I]^{2m+2} \subseteq B([w,I]^{2m+1}) = \beta_{2m+1}$. Therefore $\beta_{2m+2} \subseteq \beta_{2m+1}$. Since also $\beta_{2m+1} \subseteq \beta_{2m+2}$, the claim follows. □

Now we show that the family β_2 contains several well known families of events.

Definition 2. An event E is definite [K, PRS, B], reverse definite [B, G2], generalized definite [G2], iff it can be expressed in the form (3), (4), (5) respectively:

$$\text{(definite)} \quad E = F \cup IG, \tag{3}$$

$$\text{(reverse definite)} \quad E = F \cup GI, \tag{4}$$

$$\text{(generalized definite)} \quad E = F \cup \Big(\bigcup_{i=1,j} H_i I G_i \Big) \quad \text{for some } j, \tag{5}$$

where F, G and H_i, G_i for $i = 1,2,\ldots,j$ are finite events. Let D, RD and GD denote the families of definite, reverse definite and generalized definite events respectively.

Proposition 3. Let $\beta_{2L} = \mathbf{B}(F^2 \cup CF \cup C^2)$ and $\beta_{2R} = \mathrm{B}(F^2 \cup FC \cup C^2)$. Then

(a) $D = \beta_{2L}$,

(b) $RD = \beta_{2R}$,

(c) $GD = \beta_2$.

Proof. (a) From (3), it follows that if E is definite then $E \in \beta_{2L}$; hence $D \subseteq \beta_{2L}$. Conversely, one verifies that any event in $(F^2 \cup FC \cup C^2)$ is definite, since if E and E' are finite (cofinite) then EE' is finite (cofinite). Since D is a Boolean algebra [PRS], we have $D \supseteq \beta_{2L}$. Thus $D = \beta_{2L}$.

(b) The proof is similar to that of (a).

(c) From (5) and the fact that for any $u,v \in \Sigma^*$ $uIv = uI\Sigma^{|v|} \cap \Sigma^{|u|}Iv = u\Sigma^{|v|}I \cap I\Sigma^{|u|}v$, it follows that $GD \subseteq \beta_2$. Next, one verifies that any event in $(F \cup C)^2$ is in GD. From the definition, GD is closed under union and from [G2] it is closed under complementation; hence GD

is a Boolean algebra. Thus $GD \supseteq B((F \cup C)^2) = \beta_2$, and the claim follows. □

Now we describe briefly our work. As will be seen in chapter 2, the family $\beta_3 = \beta_4$ is precisely the family of locally testable events, defined by McNaughton and Papert [MP]. We will characterize this family and prove that an event E is locally testable iff for every idempotent e in the syntactic semigroup S of E, the subsemigroup eSe is an idempotent and commutative monoid. It follows that one can effectively decide whether an event is locally testable. This solves a long standing open problem, proposed by McNaughton and Papert [MP]. We also give in chapter 2, other characterizations of locally testable events, as well as an algebraic characterization of generalized definite events.

The underlying problem for chapter 3 is to show that the B_2-hierarchy is infinite. In order to prove this, we subdivide the family B_2 in Boolean algebras $\alpha_{m,k}$ for integers $m \geq 0$ and $k > 0$. This subdivision will be based on a natural generalization of the k-testability concept for locally testable events. It will be shown that each $\alpha_{m,k}$ contains all $\alpha_{n,\ell}$, where $n \leq m$ and $\ell \leq k$. This fact allows us to define two hierarchies of Boolean algebras. Let δ_m and γ_k denote the union of all $\alpha_{m,\ell}$ ($\ell = 1,2,\ldots$) and $\alpha_{n,k}$ ($n = 0,1,\ldots$) respectively. The γ-hierarchy is the sequence of Boolean algebras

$$\gamma_1 \subseteq \gamma_2 \subseteq \cdots \quad ;$$

the δ-hierarchy is the sequence of Boolean algebras

$$\delta_0 \subseteq \delta_1 \subseteq \cdots \quad .$$

It will be shown that $\delta_0 = \beta_2$ and that for all $m \geq 1$, $\delta_m = \beta_{2m+1} = \beta_{2m+2}$, and that all three hierarchies are infinite.

In chapter 4 we address ourselves to the problem of characterizing the family γ_1 of events. It will follow from the definitions that an event E is in γ_1 iff there exists an integer m, such that membership of x in E can be determined by testing the set of m-tuples of letters in x. Among other characterizations, we will prove that an event E is in γ_1 iff the syntactic semigroup S of E is J-trivial, i.e. each J-class of S consists of a single element. It follows that one can effectively decide whether an event is in γ_1.

In chapter 5, we derive an effective necessary condition for membership in B_2. We prove that if E is in B_2, then for each idempotent e in the syntactic semigroup S of E, the subsemigroup eSe is a J-trivial monoid. It follows from this and the results in chapter 4, that if the syntactic semigroup of E is a monoid, then E is in B_2 iff E is in γ_1. We conjecture that the necessary condition above is sufficient as well. The results of chapters 2 and 4 give some evidence for this conjecture, since they both contain proofs of particular cases. Finally, we give structural characterizations of all families defined in chapter 3, i.e. $\alpha_{m,k}$, δ_m and γ_k, as well as that of B_2.

Chapter 6 contains a few open problems which present themselves during the development in chapters 2 to 5.

CHAPTER 2

Characterizations of Locally Testable Events

1. Introduction.

Locally testable events were defined by R. McNaughton and S. Papert in drafts of their monograph [MP] dating back to 1965. However, the problem of deciding whether a given regular event is locally testable remained open until early spring of 1971. In this chapter we solve this problem, and also relate the family of locally testable events to the B_2-hierarchy, defined in section 1.3. We will prove, among other characterizations of locally testable events, that an event E, accepted by a reduced automaton $\hat{A}$, is locally testable iff for each idempotent e in the semigroup S_A of A, eS_Ae is an idempotent and commutative monoid. Note that S_A is the semigroup of A, and cannot be replaced by the monoid G_A of A. The distinction is essential. Indeed, if one replaces S_A by G_A, the condition above becomes equivalent to saying that G_A is idempotent and commutative, since the identity in G_A is an idempotent. As will be seen in section 2, this latter class corresponds precisely to the family of 1-testable events. As a corollary of this characterization, we can decide whether an event is locally testable by computing the semigroup S_A and checking for the given conditions. This can be done, since S_A is finite.

This chapter is based on a paper [BS] written jointly with Professor J. A. Brzozowski in 1971. At about the same time, the problem

has also been independently solved by R. McNaughton and Y. Zalcstein. See [MZ], [M1] and [Z1].

Let us now define k-testable and locally testable events. For $x \in \Sigma^*$ and an integer $k \geq 0$, $f_k(x)$ $[t_k(x)]$ is x if $|x| \leq k$, and it is the prefix [suffix] of x of length k, otherwise. Let

$$m_k(x) = \{v \mid x = uvw \text{ and } |v| = k\}.$$

In other words, $m_k(x)$ is the set of subwords of length k of x.

Definition 1. For $x,y \in \Sigma^*$ and for an integer $k > 0$, define $x \sim_k y$ iff $f_{k-1}(x) = f_{k-1}(y)$, $t_{k-1}(x) = t_{k-1}(y)$ and $m_k(x) = m_k(y)$.

It is easily verified that $\sim_k$ is a congruence relation of finite index over Σ^*, and that $x \sim_{k+1} y$ implies $x \sim_k y$. Let $\lceil x \rceil_k$ denote the congruence class containing x.

Definition 2. An event $E \subseteq \Sigma^*$ is k-testable iff it is a union of congruence classes of $\sim_k$. E is locally testable iff it is k-testable for some k. Let LT denote the family of locally testable events.

The reader will note that our definitions are different from those in [MP]. The reason for this is that with our definitions we are able to give a structural characterization of the family of k-testable events. The differences between the two definitions are:

(1) McNaughton and Papert test the prefixes and suffixes of length k, instead of our shorter test of length $k-1$; and (2) they test only the interior subwords of length k, while we do this for all subwords of length k. It is straightforward to verify that, even though the families of k-testable events are not the same, the family of locally testable events is unchanged.

One verifies that, if $|x| < k$ then $[x]_k = \{x\}$. Let $|x| \geq k$ and let $u = f_{k-1}(x)$, $v = t_{k-1}(x)$ and $m_k(x) = \{w_1, w_2, \ldots, w_p\}$, then it follows from the definition that,

$$[x]_k = uI \cap Iv \cap (Iw_1I \cap Iw_2I \cap \ldots \cap Iw_pI) \cap \overline{I(\Sigma^k - m_k(x))I} \; . \tag{1}$$

Now we relate the family of locally testable events to the B_2-hierarchy.

Proposition 1. $LT = \beta_3$.

Proof. It follows from (1) that each congruence class $[x]_k$ is in β_3. Hence, any finite union of such congruence classes, i.e. any locally testable event, is in β_3. Hence $LT \subseteq \beta_3$. To see the reverse inclusion, note that β_3 can be defined alternately as $B([w,I]^3)$. One easily checks that each product in $[w,I]^3$ is locally testable. Since LT is a Boolean algebra, we have that $\beta_3 \subseteq LT$. □

2. Idempotent and commutative semiautomata.

In this section we study idempotent and commutative semiautomata. As will be seen, these play an important role in the study of locally testable events. Indeed, we will prove that an event E is 1-testable, iff the reduced automaton accepting E is idempotent and commutative. On the other hand, idempotent and commutative semiautomata will be used as tail machines in the structural characterization of automata accepting locally testable events.

Definition 3. A semiautomaton $A = (Q,\Sigma,M,q_0)$ is idempotent if, for all $x \in \Sigma^*$, $x^A = (x^2)^A$; it is commutative if, for all $x,y \in \Sigma^*$, $(xy)^A = (yx)^A$.

It is clear that A is idempotent and commutative iff the monoid G_A of A is idempotent and commutative. Thus, it is effectively decidable whether A is idempotent and commutative. The next result establishes that it is sufficient to verify the idempotent and commutative properties for $\{\sigma^A \mid \sigma \in \Sigma\}$.

Proposition 2. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton. The following are equivalent:

(a) A is idempotent and commutative.

(b) For all $x,y \in \Sigma^*$, $m_1(x) = m_1(y)$ implies $x^A = y^A$.

(c) For all $\sigma_1,\sigma_2 \in \Sigma$, ${\sigma_1}^A = ({\sigma_1}^2)^A$ and $(\sigma_1\sigma_2)^A = (\sigma_2\sigma_1)^A$.

Proof. (a) implies (b). Let $x \in \Sigma^*$ and $\sigma \in m_1(x)$. Then $x = u\sigma v$ for some $u,v \in \Sigma^*$, and $x^A = (u\sigma v)^A = (u\sigma\sigma v)^A = (u\sigma v\sigma)^A = (x\sigma)^A$, since A is idempotent and commutative. This clearly implies that, if $y \in \Sigma^*$ and $m_1(y) \subseteq m_1(x)$, then $x^A = (xy)^A$. Since by hypothesis $m_1(x) = m_1(y)$,

we also have $y^A = (yx)^A$. Since A is commutative, $(xy)^A = (yx)^A$ and so $x^A = y^A$.

(b) implies (c). $m_1(\sigma_1) = m_1(\sigma_1^2) = \{\sigma_1\}$, and $m_1(\sigma_1\sigma_2) = m_1(\sigma_2\sigma_1) =$ $= \{\sigma_1,\sigma_2\}$. Hence (c) follows from (a).

(c) implies (a). One verifies first, by induction on $|u|$, that for all $u \in \Sigma^*$ and $\sigma \in \Sigma$, $(u\sigma)^A = (\sigma u)^A$. Then it follows, by induction on $|x|$, that for all $x,y \in \Sigma^*$, $x^A = (x^2)^A$ and $(xy)^A = (yx)^A$. These proofs are straightforward and we leave them to the reader. □

Corollary 1. Let $\hat{A} = (Q,\Sigma,M,q_0,F)$ be the reduced automaton accepting the event E. E is 1-testable iff A is idempotent and commutative.

Proof. This follows from the equivalence of (a) and (b), and by proposition 1.1. □

Now we proceed to give a structural characterization of idempotent and commutative semiautomata.

Definition 4. A half-reset is a semiautomaton $D = (\{q_0,q_1\},\Sigma,M,q_0)$, where for every $\sigma \in \Sigma$, σ^D is either an identity or is a reset to q_1, (σ^D is a reset to q_1 iff $q_0\sigma^D = q_1\sigma^D = q_1$).

Note that a half-reset is one of the units in the Krohn-Rhodes decomposition theory [G1].

Definition 5. Let $\Delta = (Q,\Sigma,M,q_0)$ be a semiautomaton, where $Q = 2^\Sigma$, $q_0 = \phi$ and for $\theta \subseteq \Sigma$ and $\sigma \in \Sigma$ $\theta\sigma^\Delta = \theta \cup \{\sigma\}$. One verifies that Λ is idempotent and commutative; it will be called the free idempotent and commutative semiautomaton over Σ.

The following result will be used in the proof of proposition 3.

Lemma 1. Let $A = (Q,\Sigma,M,q_0)$ and $B = (R,\Sigma,N,r_0)$ be semiautomata, such that $A \leq B$. If B is idempotent and commutative, then so is A.

Proof. Let η be the function relating B to A as in the definition of $A \leq B$; $\eta:R_1 \to Q$, where $r_0 \in R_1 \subseteq R$. Let $q \in Q$; then, since η is onto, there exists $r \in R_1$, such that $r\eta = q$. Thus $q\sigma^A = r\eta\sigma^A = r\sigma^B\eta = r\sigma^B\sigma^B\eta = (r\sigma^B)\eta\sigma^A = r\eta\sigma^A\sigma^A = q(\sigma^2)^A$, where the third equality above follows from the fact that B is idempotent. By similar reasoning, using the fact that B is commutative, one verifies that for $\sigma_1 \in \Sigma$, $q(\sigma\sigma_1)^A = q(\sigma_1\sigma)^A$, and (by proposition 1) A is idempotent and commutative. □

Proposition 3. Let $A = (Q,\Sigma,M,q_0)$ be a connected semiautomaton and let Δ be the free idempotent and commutative semiautomaton over Σ. The following are equivalent:

(a) A is idempotent and commutative.

(b) $A \leq \Delta$.

(c) There exists an integer $\ell \geq 1$ and ℓ half-resets $D_1,D_2,\ldots,D_\ell$, such that $A \leq D_1 \times D_2 \times \ldots \times D_\ell$.

Proof. (a) implies (b). In view of lemma 1.2, it is sufficient to prove that for $x,y \in \Sigma^*$, $\phi x^\Delta = \phi y^\Delta$ implies $q_0x^A = q_0y^A$. From the definition of Δ we have $\phi x^\Delta = \{\sigma \mid \sigma \in \Sigma$ and $x = u\sigma v$ for some $u,v \in \Sigma^*\} = m_1(x)$. Thus $\phi x^\Delta = \phi y^\Delta$ implies $m_1(x) = m_1(y)$. Since A is idempotent and commutative, it follows from proposition 2 that $x^A = y^A$. In particular $q_0x^A = q_0y^A$, and $A \leq \Delta$.

(b) implies (c). We first show that, if $\ell = \#\Sigma$, there exist ℓ

half-resets $D_1, D_2, \ldots, D_\ell$ such that $\Delta \leq D_1 \times D_2 \times \ldots \times D_\ell$. Let $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_\ell\}$ and let $D_i = (\{q_{i,0}, q_{i,1}\}, \Sigma, M_i, q_{i,0})$ for $1 \leq i \leq \ell$, where $\sigma_j^{D_i}$ is a reset to $q_{i,1}$ if $i = j$ and is an identity otherwise. Let $B = D_1 \times D_2 \times \ldots \times D_\ell$, and $x \in \Sigma^*$; then $(q_{1,0}, q_{2,0}, \ldots, q_{\ell,0})\, x^B = (q_{1,0}x^{D_1}, q_{2,0}x^{D_2}, \ldots, q_{\ell,0}x^{D_\ell})$. Now $q_{i,0}x^{D_i}$ is $q_{i,1}$ if $\sigma_i \in m_1(x)$ and it is $q_{i,0}$ otherwise. Thus $(q_{1,0}, q_{2,0}, \ldots, q_{\ell,0})x^B = (q_{1,0}, q_{2,0}, \ldots, q_{\ell,0})y^B$ implies $m_1(x) = m_1(y)$, and therefore $\phi x^\Delta = \phi y^\Delta$. Since Δ is connected, lemma 1.2 applies, and $\Delta \leq B$. Since covering of semiautomata is a transitive relation [G1], $A \leq \Delta$ and $\Delta \leq B$ implies $A \leq B$. (In fact one can verify that also $B \leq \Delta$ and thus Δ is isomorphic to B.)

(c) implies (a). One can verify that a half-reset is idempotent and commutative. Also, if C and D are idempotent and commutative semiautomata, then so is $C \times D$. It follows that $B = D_1 \times D_2 \times \ldots \times D_\ell$ is idempotent and commutative. Since $A \leq B$, A is idempotent and commutative by lemma 1. □

3. Characterization of k-testable events.

31. A necessary condition and a sufficient one.

First we prove some properties of the congruence $\sim_k$, which will motivate the next definition and will finally lead to the characterization of k-testable events.

Proposition 4. For $x,y,z \in \Sigma^*$, and $k = |x| + 1$,

(a) If $xy = zx$ then $xy \sim_k xy^2$,

(b) $xyxzx \sim_k xzxyx$.

Proof. (a) One verifies that for $u,v,w \in \Sigma^*$ and $|v| = k - 1$, the relation $m_k(uvw) = m_k(uv) \cup m_k(vw)$ holds. Now, $xy = zx$ implies that $xy^2 = z^2x$. Thus the length $k - 1$ prefixes and suffixes of both xy and xy^2 are equal to x. Furthermore

$$m_k(xy^2) = m_k(zxy) = m_k(zx) \cup m_k(xy) = m_k(xy).$$

(b) The length $k - 1$ prefixes and suffixes of $xyxzx$ and $xzxyx$ are equal to x, and

$$m_k(xyxzx) = m_k(xyx) \cup m_k(xzx) = m_k(xzxyx). \quad \square$$

Definition 6. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton and let $k \geq 1$ be an integer. Then A is k-testable, iff for all $x,y,z \in \Sigma^*$, such that $|x| = k - 1$,

$$xy = zx \text{ implies } (xy)^A = (xy^2)^A, \tag{2}$$

and

$$(xyxzx)^A = (xzxyx)^A. \tag{3}$$

Notice that the condition $xy = zx$ is required only in (2).

Note that, given a semiautomaton A and an integer $k > 0$, it is effectively decidable whether A is k-testable. Indeed, note that S_A is finite, and let

$$T = \{x^A \mid |x| = k - 1\} \subseteq S_A.$$

Now, (3) holds iff for all $a,b \in S_A$ and for all $c \in T$, $cacbc = cbcac$ and $cacc = ccac$ (the latter corresponds to the case where either y or z is λ; this has to be verified separately, since in general $\lambda^A \notin S_A$). To test for (2), one proceeds in two steps. Consider first all $x,y,z \in \Sigma^*$, such that $|x| = k - 1$, $xy = zx$ and $|xy| \leq 2(k-1)$. Since there exist a finite number of such triples (x,y,z), (2) can be verified for these. Now, if $|xy| > 2(k-1)$, then $xy = zx$ implies that, for some $w \in \Sigma^+$, $xy = xwx$. On the other hand, $xy^2 = xwxwx$ in this case; hence it is sufficient to verify whether for all $a \in S_A$ and for all $c \in T$, $cac = cacac$.

Now we have the following necessary condition for k-testability.

Proposition 5. Let $\hat{A} = (Q,\Sigma,M,q_0,F)$ be the reduced automaton accepting the k-testable event E. Then A is k-testable.

Proof. This clearly follows from proposition 4 and proposition 1.1. □

Now we derive a sufficient condition for k-testability. First, we need the following:

Definition 7. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton and let $k \geq 0$ be an integer. We say that A is k-definite if for all $x \in \Sigma^*$ such that $|x| = k$, $\#(Qx^A) = 1$. A is definite if it is k-definite for some k.

Notation. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton and let $q \in Q$. We denote by E_q^A the event accepted by the automaton $(Q,\Sigma,M,q_0,\{q\})$.

Proposition 6. Let $k \geq 1$ be an integer and let $A = (Q,\Sigma,M,q_0)$, $B = (R,\Sigma,N,r_0)$ and $C = (S,R\times\Sigma,P,s_0)$ be semiautomata such that B

is (k-1)-definite, C is idempotent and commutative and $A \leq B \circ C$. Then for all $q \in Q$, E^A_q is a k-testable event.

Proof. Without loss of generality we assume that all semiautomata are connected. It is clear that if $A_i = (Q_i, \Sigma, M_i, q_{0,i})(i = 1,2)$ are semiautomata such that $A_1 \leq A_2$ then for all $q_1 \in Q_1$, $E^{A_1}_{q_1} = \bigcup_{Q_3} E^{A_2}_{q_2}$ where $Q_3 = \{q_2 \in Q_2 \mid q_2\eta = q_1\}$. On the other hand, by proposition 3, there is an integer $\ell \geq 1$ and half-resets $D_1, D_2, \ldots, D_\ell$ such that $C \leq D$, where $D = D_1 \times D_2 \times \ldots \times D_\ell$. By a theorem of [G1, p.115], $B \circ C \leq B \circ D$ and hence $A \leq B \circ D$, since $\leq$ is transitive. Thus, in view of the earlier remark and the fact that k-testable events form a Boolean algebra, it is sufficient to prove that, if C is the direct product of half-resets, then each $E^{B\circ C}_{(r,s)}$ is a k-testable event. Furthermore, if $C = C_1 \times C_2$, then clearly $E^{B\circ C}_{(r,s)} = E^{B\circ C_1}_{(r,q_1)} \cap E^{B\circ C_2}_{(r,q_2)}$, where $s = (q_1, q_2)$, and q_1 and q_2 are states of C_1 and C_2 respectively. Since k-testable events are closed under intersection, it is sufficient to prove that, if C is a half-reset, then $E^{B\circ C}_{(r,s)}$ is k-testable. Thus, let $C = (\{s_0, s_1\}, R \times \Sigma, P, s_0)$ and let $\theta = \{(p,\sigma) \mid p \in R, \sigma \in \Sigma,$ and $(p,\sigma)^C$ is a reset$\}$. Then,

$$E^{B\circ C}_{(r,s_1)} = E^B_r \cap \left(\bigcup_{(p,\sigma)\in\theta} E^B_p \sigma I\right),$$

where $I = \Sigma^*$. Now, since B is (k-1)-definite it follows that for all $p \in R$ there are finite sets F_p and G_p such that $E^B_p = F_p \cup IG_p$ and F_p and G_p contain words of length less than k-1, and k-1,

respectively [PRS]. Thus,

$$E^{B\circ C}_{(r,s_1)} = E^{B}_{r} \cap \left(\bigcup_{(p,\sigma)\in\theta} F_p\sigma I \cup IG_p\sigma I\right).$$

Clearly E^{B}_{r}, $F_p\sigma I$ and $IG_p\sigma I$ are k-testable events; hence so is $E^{B\circ C}_{(r,s_1)}$. Finally, we have

$$E^{B\circ C}_{(r,s_0)} = E^{B}_{r} \cap \overline{E^{B\circ C}_{(r,s_1)}}.$$

Hence $E^{B\circ C}_{(r,s_0)}$ is also k-testable. □

At this point, one can verify, without too much effort, that if $\hat{A}$ is the reduced automaton accepting the event E, then E is k-testable iff there exist a (k-1)-definite B and an idempotent and commutative C, such that $A \leq B\circ C$. Indeed, the if part follows from proposition 6. To show the only if part, it is clearly sufficient to verify, in view of (1), that the result holds for events of the form w, uI, Iv and IxI, where $|w| < k$, $|u| = |v| = k - 1$ and $|x| = k$. Also note that the result is contained in theorem 2. Now, this in turn implies that the following holds: If $\hat{A}$ is the reduced automaton accepting the event E, then E is locally testable iff there exist semiautomata B and C, B definite and C idempotent and commutative, such that $A \leq B\circ C$. Note however, that it is not clear how to decide whether a semiautomaton A can be covered by a cascade $B\circ C$ with the above properties. Thus, we need to find other characterizations of locally testable events. To achieve this we will prove first that the necessary condition in proposition 5 implies the sufficient one in proposition 6. In other words, given a k-testable semiautomaton A,

we will find a (k-1)-definite B and an idempotent and commutative C, such that $A \leq B \circ C$. This is done in the next two subsections.

32. A covering theorem.

In this subsection we characterize semiautomata A and B, for which there exists some idempotent and commutative C, such that $A \leq B \circ C$. The results in this section are general, in the sense that we do not require A to be k-testable, or B to be (k-1)-definite. The condition is defined as follows:

Definition 8. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton and let $B = (R,\Sigma,N,r_0)$ be a π-factor of A. We say that B is an idempotent π-factor of A if, for all $r \in R$, for all $q \in r\pi$ and for all $x \in \Sigma^*$, $rx^B = r$ implies $qx^A = q(x^2)^A$. B is a commutative π-factor of A if, for all $r \in R$, for all $q \in r\pi$ and for all $x,y \in \Sigma^*$, $rx^B = ry^B = r$ implies $q(xy)^A = q(yx)^A$.

Note that, given a π-factor $B = A/\pi$, one can verify whether it is an idempotent and commutative π-factor. In fact, for $r \in R$ and for $x \in \Sigma^*$ such that $rx^B = r$, the restriction of x^A to $r\pi$ is a function from $r\pi$ into $r\pi$, since B is a π-factor of A. The set of all such functions, say S_r, is a finite monoid under composition of functions. Now, B is an idempotent and commutative π-factor of A, iff for all $r \in R$, S_r is an idempotent commutative monoid. Finally, we indicate how to obtain the monoids S_r for given A and B. Let $A \cup B$ be the semiautomaton $A \cup B = (Q \cup R,\Sigma,P,q_0)$, where the restrictions of $\sigma^{A\cup B} \in P$ to Q and R are σ^A and σ^B respectively. Compute the monoid $G_{A\cup B}$ of $A \cup B$. Now, S_r is the set of all

$x^{A\cup B}|_{r\pi}$ (restriction of $x^{A\cup B}$ to $r\pi$) such that $rx^{A\cup B} = r$.

Definition 9. Let $A = (Q,\Sigma,M,q_0)$ be a connected semiautomaton and let $B = (R,\Sigma,N,r_0)$ be a π-factor of A. We say that B (with the function π) is a minimal π-factor of A if, for all $r \in R$ and for all $q \in r\pi$, there exists an $x \in \Sigma^*$, such that $r_0x^B = r$ and $q_0x^A = q$.

Notice that, according to definition 9, B is a minimal π-factor of A iff the function π relating A to B is minimal, in the sense that for all $r \in R$, $r\pi$ is minimal. Given semiautomata A and B, this minimal function π is unique and can be found by constructing the semiautomaton $A \times B$. We have

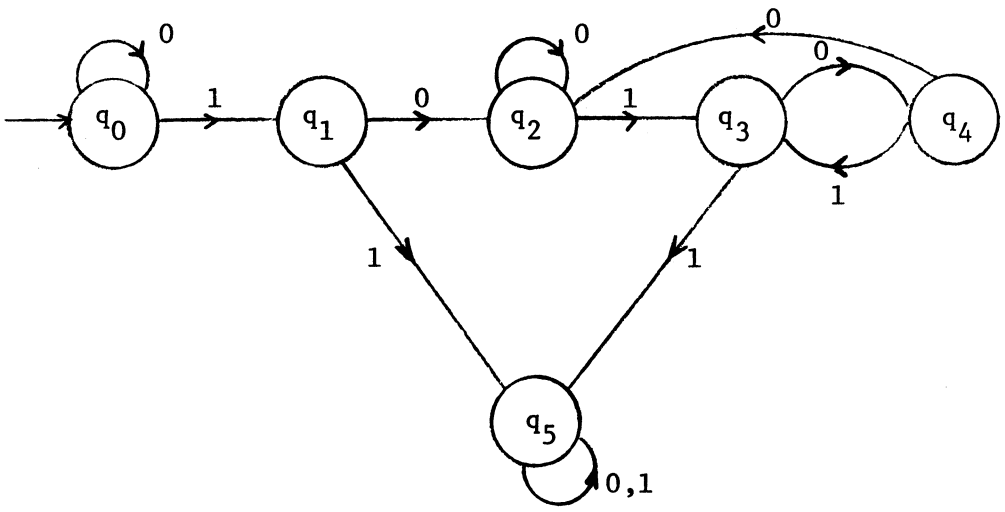
$$r\pi = \{q \mid (q_0,r_0)x^{A\times B} = (q,r) \text{ for some } x \in \Sigma^*\}.$$

In other words, $q \in r\pi$ iff (q,r) is in the connected part of $A \times B$ (from (q_0,r_0)).

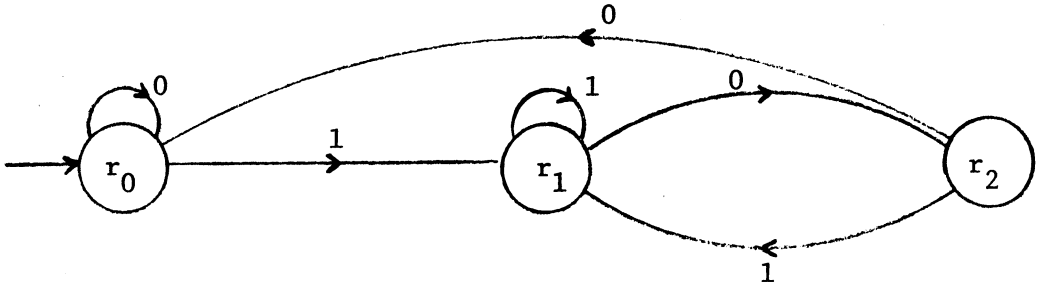
Before proceeding we give an example. Let $\Sigma = \{0,1\}$ and let A and B be semiautomata as represented (with the usual conventions) in figures 1a and 1b. Note that B is a 2-definite semiautomaton. B with the function π given in figure 1c is a (minimal) π-factor of A. The monoids S_r are given in figure 1d, where we only represent the indices i of q_i. We illustrate the convention used in figure 1d: the second row 225 in S_{r_0} represents the function

$$\begin{pmatrix} q_0 & q_2 & q_5 \\ q_2 & q_2 & q_5 \end{pmatrix}$$

which corresponds to the restriction of $(100)^{A\cup B}$,



a. semiautomaton A.



b. semiautomaton B.

r	r_0	r_1	r_2
$r\pi$	$q_0q_2q_5$	$q_1q_3q_5$	$q_2q_4q_5$

c. the function $\pi : R \to 2^Q$.

x	S_{r_0}
λ	0 2 5
100	2 2 5
1100	5 5 5

x	S_{r_1}
λ	1 3 5
01	3 3 5
1	5 5 5

x	S_{r_2}
λ	2 4 5
10	4 4 5
110	5 5 5

d. the monoids S_r.

Figure 1 An example.

$$(100)^{A\cup B} = \begin{pmatrix} q_0 & q_1 & q_2 & q_3 & q_4 & q_5 & r_0 & r_1 & r_2 \\ q_2 & q_5 & q_2 & q_5 & q_2 & q_5 & r_0 & r_0 & r_0 \end{pmatrix},$$

(note that $r_0(100)^{A\cup B} = r_0$) to $r_0\pi = \{q_0,q_2,q_5\}$. One verifies that each S_r is an idempotent and commutative monoid; hence B is an idempotent and commutative π-factor of A.

Theorem 1. Let $A = (Q,\Sigma,M,q_0)$ be a connected semiautomaton, let $B = (R,\Sigma,N,r_0)$ be an idempotent and commutative π-factor of A and let Δ be the free idempotent and commutative semiautomaton over $R \times \Sigma$. Then $A \leq B\circ\Delta$. Conversely, if B is a minimal π-factor of A, then $A \leq B\circ\Delta$ implies that B is an idempotent and commutative π-factor of A.

Proof. First we prove the last statement. Thus, let $r \in R$ and $x,y \in \Sigma^*$ be such that, $rx^B = ry^B = r$, and let $q \in r\pi$. Since B is a minimal π-factor of A, there exists $z \in \Sigma^*$ such that $q_0z^A = q$ and $r_0z^B = r$. Now, for some $\theta \subseteq R\times\Sigma$, $(r_0,\phi)z^{B\circ\Delta} = (r,\theta)$ and, if η is the function relating $B\circ\Delta$ to A $(A \leq B\circ\Delta)$, then $(r,\theta)\eta = (r_0,\phi)z^{B\circ\Delta}\eta = (r_0,\phi)\eta z^A = q_0z^A = q$, i.e. $(r,\theta)\eta = q$. Since $rx^B = r$ and Δ is idempotent and commutative, it follows that $(r,\theta)x^{B\circ\Delta} = (r,\theta)(x^2)^{B\circ\Delta}$. Hence $(r,\theta)x^{B\circ\Delta}\eta = (r,\theta)(x^2)^{B\circ\Delta}\eta$ and $qx^A = q(x^2)^A$. Similarly $q(xy)^A = q(yx)^A$ and therefore B is an idempotent and commutative π-factor of A.

Now we proceed to prove the first part. We will refer, without explicitly stating it, to semiautomata A, B and Δ as in the statement of the theorem and we assume that B is an idempotent and commutative π-factor of A. We begin with two definitions.

For $x \in \Sigma^*$ and $r \in R$ we define the function θ as:

$$\theta(r,x) = \{(s,\sigma) \mid s \in R,\ \sigma \in \Sigma, \text{ and } x = y\sigma z \text{ for some } y,z \in \Sigma^* \text{ such that } ry^B = s\}.$$

Intuitively "$\theta(r,x)$ is the subset of the set $R \times \Sigma$ of transitions of B traveled when spelling x in B, starting from r".

For $x,y \in \Sigma^*$ and $r \in R$ we define the relation $\leftrightarrow_r$ over Σ^* as:

$$x \leftrightarrow_r y \text{ iff } rx^B = ry^B \text{ and, for all } q \in r\pi,\ qx^A = qy^A.$$

We state, without proof, the following properties of the relation $\leftrightarrow_r$:

$\leftrightarrow_r$ is an equivalence relation on Σ^*.

If $x \leftrightarrow_r y$ then, for all $z \in \Sigma^*$, $xz \leftrightarrow_r yz$. (4)

If $z \in \Sigma^*$ and $s \in R$ are such that $sz^B = r$, and if $x \leftrightarrow_r y$, then $zx \leftrightarrow_s zy$. (5)

It follows from (4) and (5) that, if

$$x \leftrightarrow_r y \text{ and } su^B = r, \text{ then } uxv \leftrightarrow_s uyv. \quad (6)$$

Since B is an idempotent and commutative π-factor of A, it follows that for $x,y \in \Sigma^*$ and $r \in R$ such that $rx^B = ry^B = r$,

$$x \leftrightarrow_r x^2 \quad (7)$$

and

$$xy \leftrightarrow_r yx. \quad (8)$$

Now we relate these two definitions by the following lemmas:

Lemma 2. Let $x,y \in \Sigma^*$ and $r \in R$ be such that $\theta(r,x) = \theta(r,xy)$ and $rx^B = r(xy)^B$. Then $x \leftrightarrow_r xy$.

Proof. Let $s = rx^B$. It is clear that $\theta(r,xy) = \theta(r,x) \cup \theta(s,y)$. Since $\theta(r,x) = \theta(r,xy)$ it follows that

$$\theta(s,y) \subseteq \theta(r,x). \tag{9}$$

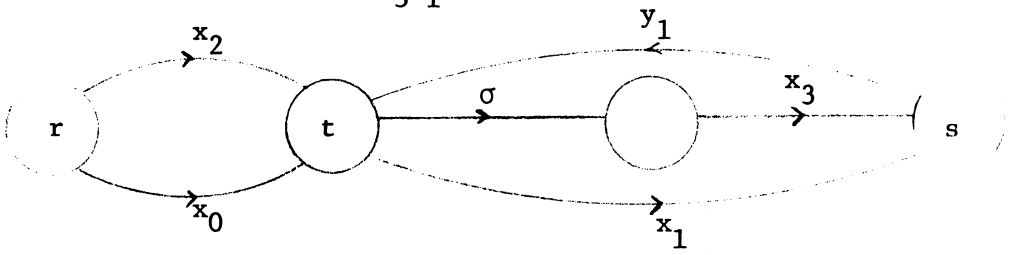
Now we prove that for any prefix y_1 of y there exist $x_0,x_1 \in \Sigma^*$, such that

$$x = x_0x_1,\ rx_0^B = sy_1^B \text{ and } x \leftrightarrow_r xy_1x_1. \tag{10}$$

We proceed by induction on $|y_1|$. For $|y_1| = 0$, i.e. $y_1 = \lambda$ we take $x_0 = x$ and $x_1 = \lambda$ which clearly satisfy (10). Assume that the assertion holds for y_1, i.e. there exist $x_0,x_1 \in \Sigma^*$ such that $x = x_0x_1$, $rx_0^B = sy_1^B$ and

$$x \leftrightarrow_r xy_1x_1. \tag{11}$$

If $y = y_1$, we are finished. Otherwise for some $\sigma \in \Sigma$ and $y_2 \in \Sigma^*$, $y = y_1\sigma y_2$. Let $t = sy_1^B$; then it follows that $tx_1^B = s$. Thus $(t,\sigma) \in \theta(s,y)$ and, by (9), $(t,\sigma) \in \theta(r,x)$. Hence, there exist $x_2,x_3 \in \Sigma^*$ such that $x = x_2\sigma x_3$ and $rx_2^B = t$. Clearly $t(\sigma x_3)^B = s$ (see Fig. 2). Thus, $t(\sigma x_3y_1)^B = t$ and it follows from (7) that



$$x = x_0x_1 = x_2\sigma x_3$$

Figure 2.

$\sigma x_3 y_1 \leftrightarrow_t \sigma x_3 y_1 \sigma x_3 y_1$. Thus letting $u = x_2$ and $v = x_1$, since $rx_2^B = t$, we have from (6) that $x_2\sigma x_3 y_1 x_1 \leftrightarrow_r x_2\sigma x_3 y_1 \sigma x_3 y_1 x_1$. Since $x_2\sigma x_3 = x$, we have

$$xy_1x_1 \leftrightarrow_r xy_1\sigma x_3 y_1 x_1. \tag{12}$$

On the other hand, since $s(y_1\sigma x_3)^B = s(y_1x_1)^B = s$, it follows from (8) that $y_1\sigma x_3 y_1 x_1 \leftrightarrow_s y_1 x_1 y_1 \sigma x_3$. Thus letting $z = x$, since $rx^B = s$, we have from (5) that

$$xy_1\sigma x_3 y_1 x_1 \leftrightarrow_r xy_1 x_1 y_1 \sigma x_3. \tag{13}$$

Now, from (11) and letting $z = y_1\sigma x_3$, we have from (4) that

$$xy_1\sigma x_3 \leftrightarrow_r xy_1 x_1 y_1 \sigma x_3. \tag{14}$$

Finally, by transitivity, from (11), (12), (13) and (14) it follows that $x \leftrightarrow_r xy_1\sigma x_3$ which proves the induction step, since $x = x_2\sigma x_3$ and $r(x_2\sigma)^B = s(y_1\sigma)^B = t\sigma^B$.

Now, since y itself is a prefix of y, it follows from (11) that there are $x_0, x_1 \in \Sigma^*$ such that $x = x_0x_1$, $rx_0^B = sy^B$ and

$$x \leftrightarrow_r xyx_1. \tag{15}$$

Since $sy^B = s$ it follows that $rx_0^B = s$ and $sx_1^B = s$. Thus we have from (7) and (8) that $x_1 y \leftrightarrow_s x_1 y x_1$ and letting $z = x_0$, since $rx_0^B = s$, it follows from (5) that $x_0x_1y \leftrightarrow_r x_0x_1yx_1$, i.e. $xy \leftrightarrow_r xyx_1$, since $x_0x_1 = x$. Now from (15) by transitivity $x \leftrightarrow_r xy$. ||

Lemma 3. Let $x,y \in \Sigma^*$ and $r \in R$ be such that $\theta(r,x) = \theta(r,y)$ and $rx^B = ry^B$. Then $x \leftrightarrow_r y$.

Proof. We proceed by induction on $\#\theta(r,x)$. If $\#\theta(r,x) = 0$ then $x = \lambda$ and, since $\theta(r,x) = \theta(r,y)$, also $y = \lambda$. Hence $x \leftrightarrow_r y$. Assume now that $\#\theta(r,x) > 0$ and that for all $r' \in R$ and for all $x',y' \in \Sigma^*$ such that $r'(x')^B = r'(y')^B$, $\theta(r',x') = \theta(r',y')$ and $\#\theta(r',x') < \#\theta(r,x)$ we have $x' \leftrightarrow_{r'} y'$. Let $s = rx^B = ry^B$ and let $P = \{sz^B \mid z \in \Sigma^*$ and $\theta(s,z) \subseteq \theta(r,x)\}$.

Intuitively "P is the subset of Q, reachable from s, using only transitions in $\theta(r,x)$. In other words, if we delete from the state graph of B the transitions not in $\theta(r,x)$, P will be the set of states in the strongly connected component which contains s". We have:

Case 1. If $r \in P$ then there exists $z \in \Sigma^*$ such that $sz^B = r$ and $\theta(s,z) \subseteq \theta(r,x)$. Clearly $r(xz)^B = r(yz)^B = r$; therefore by (4) and (8) $xzyzx \leftrightarrow_r yzxzx$. On the other hand $\theta(r,x) = \theta(r,y) = \theta(r,xzyzx) = \theta(r,yzxzx)$. Hence, by lemma 2 $x \leftrightarrow_r xzyzx$ and $y \leftrightarrow_r yzxzx$. Thus by transitivity $x \leftrightarrow_r y$.

Case 2. If $r \notin P$, then $x = x_1\sigma x_2$ for some $x_1,x_2 \in \Sigma^*$ and $\sigma \in \Sigma$, such that $p = rx_1^B \notin P$ and $q = r(x_1\sigma)^B \in P$. This is so, since $rx^B = s \in P$ and $r \notin P$. Now, since $\theta(r,x) = \theta(r,y)$ and $(p,\sigma) \in \theta(r,x)$ it follows that $(p,\sigma) \in \theta(r,y)$, i.e. there are $y_1,y_2 \in \Sigma^*$, such that $y = y_1\sigma y_2$ and $ry_1^B = p$. Clearly, $qy_2^B = qx_2^B = s$. (See Fig. 3.)

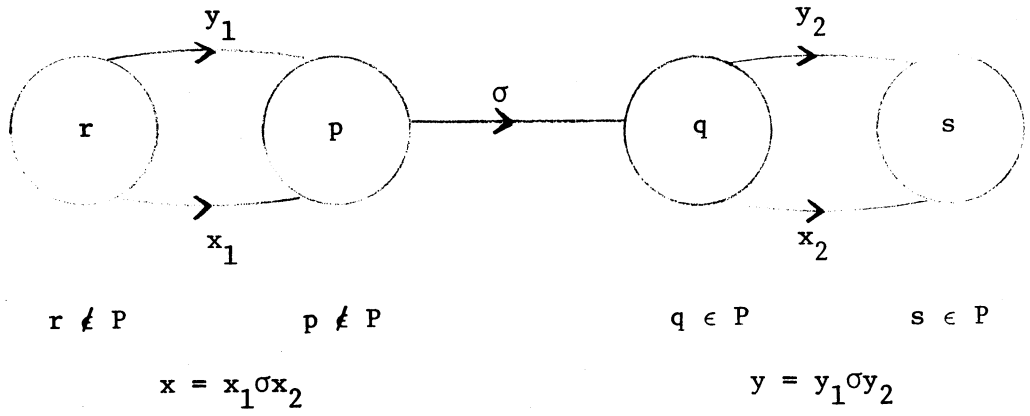


Figure 3.

Now we claim that

$$(p,\sigma) \notin \theta(r,x_1) \cup \theta(q,x_2). \tag{16}$$

To see this, suppose $(p,\sigma) \in \theta(r,x_1)$, i.e. $x_1 = x_3\sigma x_4$ for some $x_3,x_4 \in \Sigma^*$ such that $rx_3^B = p$. It follows that $qx_4^B = rx_1^B = p$. Since $q \in P$ and clearly $\theta(q,x_4) \subseteq \theta(r,x)$, we also have $p \in P$; this is a contradiction. If we suppose that $(p,\sigma) \in \theta(q,x_2)$ then $x_2 = x_3\sigma x_4$ where $qx_3^B = p$, which is again a contradiction of $p \notin P$.

A similar argument shows that

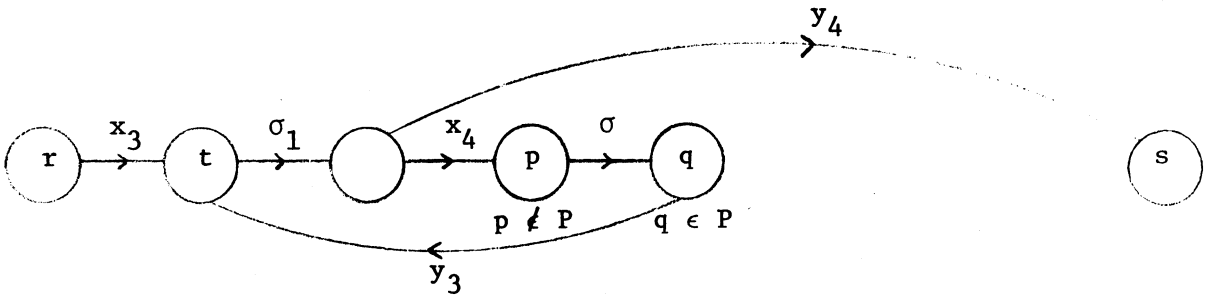
$$(p,\sigma) \notin \theta(r,y_1) \cup \theta(q,y_2). \tag{17}$$

Next we claim that

$$\theta(r,x_1) \cap \theta(q,y_2) = \phi. \tag{18}$$

In fact, suppose that there are $t \in R$ and $\sigma_1 \in \Sigma$, such that $(t,\sigma_1) \in \theta(r,x_1) \cap \theta(q,y_2)$. Then, (see Fig. 4) $x_1 = x_3\sigma_1 x_4$ and $y_2 = y_3\sigma_1 y_4$ for some $x_3,x_4,y_3,y_4 \in \Sigma^*$, such that $rx_3^B = qy_3^B = t$.

It follows that $q(y_3\sigma_1 x_4)^B = p$ and thus since $\theta(q,y_3\sigma_1 x_4) \subseteq \theta(r,x)$, $p \in P$; this is a contradiction. On the other hand,



$x_1 = x_3\sigma_1 x_4$ $\qquad\qquad$ $y_2 = y_3\sigma_1 y_4$

Figure 4.

$$\theta(r,x_1) \cup \{(p,\sigma)\} \cup \theta(q,x_2) = \theta(r,x) = \theta(r,y) = \theta(r,y_1) \cup$$
$$\cup \{(p,\sigma)\} \cup \theta(q,y_2). \qquad (19)$$

It follows from (16), (18) and (19) that $\theta(r,x_1) \subseteq \theta(r,y_1)$ and from (17), (18) and (19) that $\theta(q,y_2) \subseteq \theta(q,x_2)$. Similarly $\theta(r,y_1) \cap \theta(q,x_2) = \phi$ and then from (16), (17) and (19), $\theta(r,y_1) \subseteq \theta(r,x_1)$ and $\theta(q,x_2) \subseteq \theta(q,y_2)$. Altogether, $\theta(r,x_1) = \theta(r,y_1) \subsetneq \theta(r,x)$ and $\theta(q,x_2) = \theta(q,y_2) \subsetneq \theta(r,x)$. Since $rx_1^B = ry_1^B = p$ and $qx_2^B = qy_2^B = s$, it follows from the induction hypothesis that $x_1 \leftrightarrow_r y_1$ and $x_2 \leftrightarrow_q y_2$. Finally, we have from (6) that $x = x_1\sigma x_2 \leftrightarrow_r y_1\sigma x_2$ and $y_1\sigma x_2 \leftrightarrow_r y_1\sigma y_2 = y$. Thus $x \leftrightarrow_r y$. □

Now, it is easy to prove that $A \leq B\circ\Delta$. In fact, in view of lemma 1.2, it is sufficient to prove that, if $x,y \in \Sigma^*$ are such that

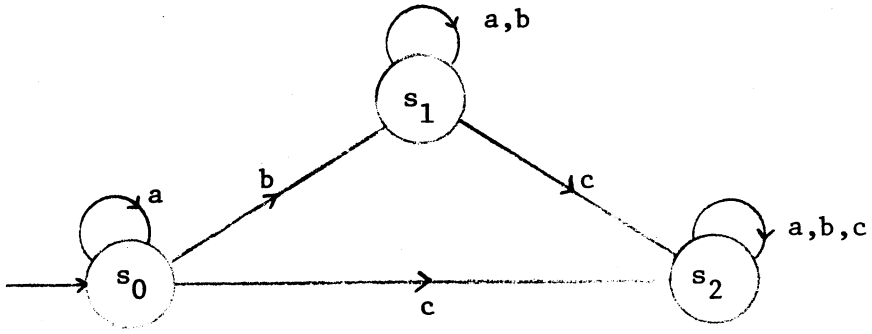
$(r_0,\phi)x^{B\circ\Delta} = (r_0,\phi)y^{B\circ\Delta}$, then $q_0x^A = q_0y^A$. But $(r_0,\phi)x^{B\circ\Delta} = (r_0,\phi)y^{B\circ\Delta}$ implies that $r_0x^B = r_0y^B$ and $\theta(r_0,x) = \theta(r_0,y)$. Hence, by lemma 3, $x \leftrightarrow_{r_0} y$ and since $q_0 \in r_0\pi$ it follows that $q_0x^A = q_0y^A$. □

Note that the minimality of B in the second statement of theorem 1 is necessary. In fact, if B is isomorphic to A and $r\pi = Q$ for all $r \in R$, then clearly $A \leq B\circ\Delta$. However, in general, B is not an idempotent and commutative π-factor of A. We also note that the equivalence of (a) and (b) of proposition 3 also follows from theorem 1, if we take $B = (\{r_0\},\Sigma,N,r_0)$ and $r_0\pi = Q$. We also have:

Corollary 2. Let $A = (Q,\Sigma,M,q_0)$ be a connected semiautomaton and $B = (R,\Sigma,N,r_0)$ be a minimal π-factor of A. Then there is an idempotent and commutative semiautomaton C such that $A \leq B\circ C$ iff B is an idempotent and commutative π-factor of A.

Proof. For the if part, take $C = \Delta$. For the only if, $A \leq B\circ C$ and A connected imply that $A \leq B\circ\Delta$. □

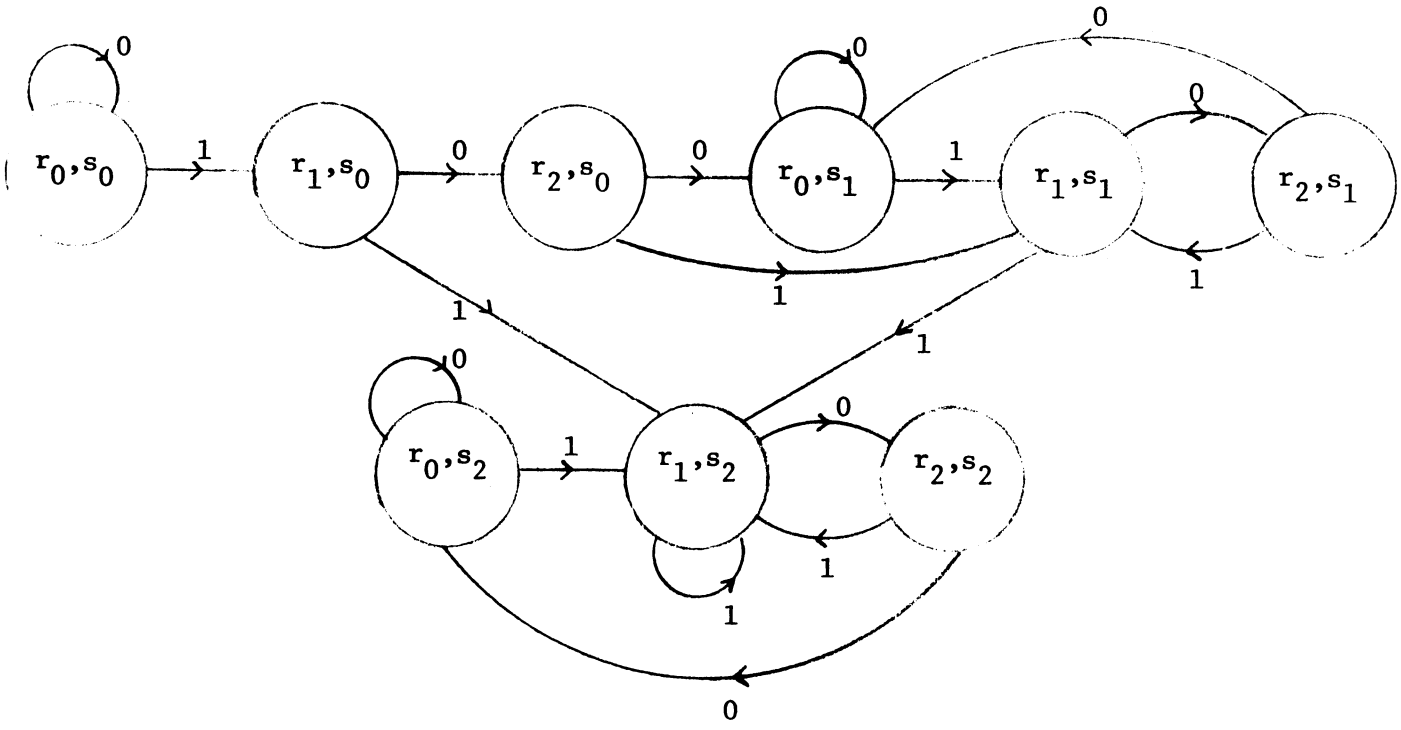
Returning to the previous example, (figure 1), since B is an idempotent and commutative π-factor of A, it follows from theorem 1 that A is covered by $B\circ\Delta$, where Δ is the free idempotent and commutative semiautomaton over $\{r_0,r_1,r_2\} \times \{0,1\}$. Since Δ has $2^6 = 64$ states, we exhibit a smaller semiautomaton C, over input alphabet Γ, in figure 5a, which is idempotent and commutative. In figure 5c we have the semiautomaton $B\circ C$, where the correspondence



a. semiautomaton C over $\Gamma = \{a,b,c\}$.

$R\times\Sigma$	$r_0,0$	$r_0,1$	$r_1,0$	$r_1,1$	$r_2,0$	$r_2,1$
Γ	a	a	a	c	b	b

b. correspondence between $R\times\Sigma$ and Γ.



c. semiautomaton B∘C.

Figure 5. More about the example.

between $R\times\Sigma$ and the inputs Γ of C is given in figure 5b. The reader can easily verify that $A \leq B\circ C$. Note that C was obtained by "ad hoc" methods. Indeed, we do not know how to obtain these smaller semiautomata. At any rate, it follows from proposition 6 that the events accepted by A are 3-testable (since B is 2-definite).

33. Definite π-factors.

According to theorem 1, in order to complete our goal, given at the end of section 31., we only have to show that, given a k-testable semiautomaton A, it has a (k-1)-definite π-factor B, which is an idempotent and commutative π-factor. This will be done in what follows.

Definition 10. For $k \geq 0$ the semiautomaton $B = (R,\Sigma,N,r_0)$ where $R = \{\langle x\rangle \mid x \in \Sigma^* \text{ and } |x| \leq k\}$, $r_0 = \langle\lambda\rangle$,

$$\langle x\rangle\sigma^B = \begin{cases} \langle x\sigma\rangle, & \text{if } |x| < k \\ \langle y\rangle, & \text{if } |x| = k, \text{ where } x\sigma = \sigma' y \text{ for some } \sigma' \in \Sigma,\ y \in \Sigma^*, \end{cases}$$

is called the free k-definite semiautomaton over Σ [PRS].

Definition 11. Let $A = (Q,\Sigma,M,q_0)$ be a connected semiautomaton and let $B = (R,\Sigma,N,r_0)$ be the free k-definite semiautomaton over Σ. Let $\pi: R \to 2^Q$ be the function defined by

$$\langle x\rangle\pi = \begin{cases} \{q_0 x^A\}, & \text{if } |x| < k \\ Qx^A, & \text{if } |x| = k. \end{cases}$$

One can verify that B is a π-factor of A and we call B the free k-definite π-factor of A.

Proposition 7. Let $k \geq 1$ and let $A = (Q,\Sigma,M,q_0)$ be a connected k-testable semiautomaton. Then the free (k-1)-definite π-factor of A is an idempotent and commutative π-factor.

Proof. Let $B = (R,\Sigma,N,r_0)$ be the free (k-1)-definite π-factor of A.

For $x \in \Sigma^*$ such that $|x| < k-1, \langle x\rangle\pi = \{q_0 x^A\}$. Hence $\#(\langle x\rangle\pi) = 1$ and the conditions of definition 8 are trivially satisfied. Thus, let $x,y,z \in \Sigma^*$ be such that $|x| = k-1$ and $\langle x\rangle y^B = \langle x\rangle z^B = \langle x\rangle$. We have to prove that for all $q \in \langle x\rangle\pi$, $qy^A = q(y^2)^A$ and $q(yz)^A = q(zy)^A$. Since $\langle x\rangle\pi = Qx^A$ this holds iff for all $q \in Q$, $q(xy)^A = q(xy^2)^A$ and $q(xyz)^A = q(xzy)^A$, i.e.

$$(xy)^A = (xyy)^A, \text{ and} \tag{20}$$

$$(xyz)^A = (xzy)^A. \tag{21}$$

If $y = \lambda$ or $z = \lambda$ this is trivial, so let us assume $y,z \in \Sigma^+$. Let $y_1, x' \in \Sigma^*$ be such that $|x'| = k-1$ and $xy = y_1 x'$. Since B is the free (k-1)-definite semiautomaton over Σ, and $|x| = |x'| = k-1$, it is easily seen that $Rx^B = \{\langle x\rangle\}$ and $R(y_1x')^B = \{\langle x'\rangle\}$. Thus $\{\langle x'\rangle\} = R(y_1x')^B = R(xy)^B = \{\langle x\rangle\}y^B$. Since $\langle x\rangle y^B = \langle x\rangle$, it follows that $x = x'$ and hence $xy = y_1x$. Since A is k-testable, (20) holds. Similarly $(xz)^A = (xzz)^A$. Therefore $(xyz)^A = (y_1xz)^A = (y_1xz^k)^A =$ $= (xyz^k)^A = (xy^kz^k)^A$, i.e.

$$(xyz)^A = (xy^kz^k)^A. \tag{22}$$

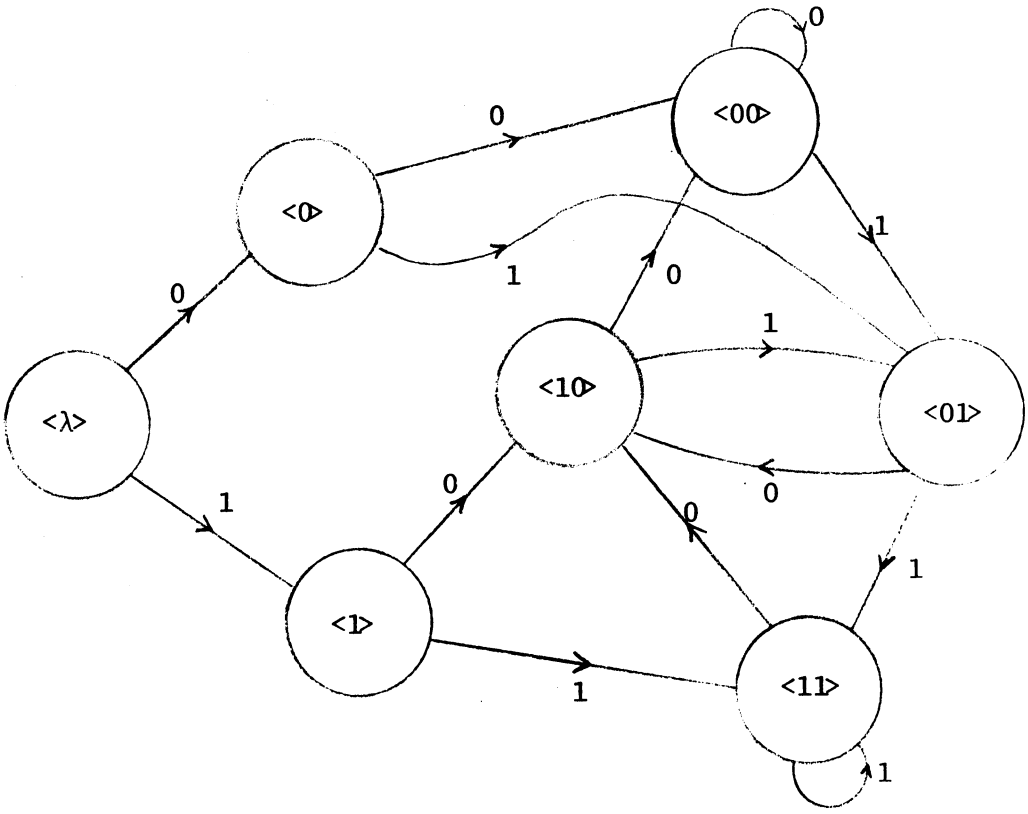
Similarly

$$(xzy)^A = (xz^ky^k)^A. \tag{23}$$

Now, $xy = y_1x$ implies that $xy^k = y_1^kx$ and since $y \in \Sigma^+$, $|y^k| > k-1$. Hence $y^k = y_2x$ for some $y_2 \in \Sigma^*$. Similarly, $z^k = z_2x$ for some $z_2 \in \Sigma^*$. Thus $(xy^kz^k)^A = (xy_2xz_2x)^A$. Since A is k-testable, $(xy_2xz_2x)^A = (xz_2xy_2x)^A$ and it follows that $(xy^kz^k)^A = (xz^ky^k)^A$. By

(22) and (23) $(xyz)^A = (xzy)^A$. Hence (21) also holds. Thus B is an idempotent and commutative π-factor of A. □

By way of an example, we represent in figure 6 the free 2-definite π-factor B_1 of semiautomaton A, given in figure 1. One



a. semiautomaton B_1.

r	<λ>	<0>	<1>	<00>	<01>	<10>	<11>
rπ	q_0	q_0	q_1	$q_0q_2q_5$	$q_1q_3q_5$	$q_2q_4q_5$	q_5

b. the function π.

Figure 6. The free 2-definite π-factor of A.

can verify that B_1 is an idempotent and commutative π-factor of A. Notice that we found in figure 1 a smaller 2-definite semiautomaton B which is an idempotent and commutative π-factor of A. Again, as in the case of the idempotent and commutative tails, we do not know how to obtain these smaller semiautomata.

34. Characterization.

Now we combine the previous subsections to get the main result of this section.

Theorem 2. Let $\hat{A}$ be the reduced automaton accepting the event E, and let $k > 0$. The following are equivalent:

(a) E is k-testable.

(b) A is k-testable.

(c) There exists an idempotent and commutative π-factor B of A which is a (k-1)-definite semiautomaton.

(d) There exist semiautomata B and C, B (k-1)-definite and C idempotent and commutative, such that $A \leq B \circ C$.

Proof. (a) implies (b) by proposition 5.

(b) implies (c) by proposition 7.

(c) implies (d) by theorem 1.

(d) implies (a) by proposition 6. □

4. Characterization of locally testable events.

In this section we study semiautomata which satisfy the conditions of theorem 2 for some k. Thus we will achieve the desired characterization of locally testable events.

Definition 12. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton, and let $n = \#Q$. A is locally testable iff for all $x \in \Sigma^+$ and for all $y,z \in \Sigma^*$

$$(x^n y x^n)^A = (x^n y x^n y x^n)^A, \tag{24}$$

and

$$(x^n y x^n z x^n)^A = (x^n z x^n y x^n)^A. \tag{25}$$

Definition 13. A finite semigroup S is locally testable iff for every idempotent e in S, the subsemigroup eSe of S is an idempotent and commutative monoid.

Now we have the following:

Theorem 3. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton. The following are equivalent:

(a) S_A is locally testable.

(b) A is locally testable.

(c) There exist an integer k such that A is k-testable.

Proof. (a) implies (b). We first claim that S_A is a group-free semigroup. In fact, let G be a subgroup of S_A; then $G = eGe$, where e is the identity of G. Hence G is a subgroup of eS_Ae. Since e is idempotent and S_A is locally testable, every element of G is idempotent. This implies that G consists solely of the element e; hence the claim holds. It follows then from theorem 1.1 that A is a permutation-free semiautomaton. Thus, by lemma 1.1, for any $x \in \Sigma^+$, $(x^n)^A = (x^{n+1})^A$, where $n = \#Q$. Thus $(x^n)^A$ is idempotent. Since

S_A is locally testable, $(x^n)^A S_A (x^n)^A$ is an idempotent and commutative monoid. Thus for all $y \in \Sigma^+$, $(x^n y x^n)^A = (x^n y x^n)^A (x^n y x^n)^A = (x^n y x^n y x^n)^A$. This is also true for $y = \lambda$, and (24) follows. By a similar argument, (25) follows and A is locally testable.

(b) implies (c). Let $k = \#S_A + 2$. We will prove that A is k-testable. Let $x \in \Sigma^*$ be such that $|x| = k - 1$. It follows from the choice of k that there exist $x_1, x_3 \in \Sigma^*$ and $x_2 \in \Sigma^+$, such that

$$x = x_1 x_2 x_3, \quad \text{and} \tag{26}$$

$$x_1^A = (x_1 x_2)^A. \tag{27}$$

Now, (27) implies that for all $m \geq 0$

$$x_1^A = (x_1 x_2^m)^A. \tag{28}$$

To see that (2) holds, let $y, z \in \Sigma^*$ be such that $xy = zx$. If $y = \lambda$ we have nothing to prove, so assume that $y \in \Sigma^+$. From (26) it follows that there is a shortest $v \in \Sigma^*$, such that for some $u \in \Sigma^*$

$$x = u x_1 x_2 v. \tag{29}$$

We claim that $|v| < |y|$. In fact, from $xy = zx$ and (29) we have

$$u x_1 x_2 v y = z u x_1 x_2 v. \tag{30}$$

Now, if $|v| \geq |y|$ then $v = v'y$ for some $v' \in \Sigma^*$ and $u x_1 x_2 v = z u x_1 x_2 v'$. By (29), $x = z u x_1 x_2 v'$. Since $|y| > 0$ it follows that $|v'| < |v|$, i.e. there is a $v' \in \Sigma^*$ shorter than v which satisfies (29). This is a contradiction; hence $|v| < |y|$. Thus, from (30) we have that, for some $y_1 \in \Sigma^*$, $y = y_1 v$ and

$$ux_1x_2vy_1 = zux_1x_2. \tag{31}$$

Now, from (29), (28) and (31) it follows that for all $m \geq 0$, $(xy_1)^A = (xy_1x_2^m)^A$. Thus, if $n = \#Q$, then $(xy)^A = (xy_1v)^A = (xy_1x_2^nv)^A$. From (29) and (28) we also have that $(xy_1x_2^nv)^A = (ux_1x_2^nvy_1x_2^nv)^A$. Hence,

$$(xy)^A = (ux_1x_2^nvy_1x_2^nv)^A. \tag{32}$$

On the other hand, $(xyy)^A = (zxy)^A$ and from (32) and (28), $(xyy)^A = (zux_1x_2^{n+1}vy_1x_2^nv)^A$. Using (31) and (28), $(xyy)^A =$ $= (ux_1x_2^nvy_1x_2^nvy_1x_2^nv)^A$. Since A is locally testable (24) holds, and from (32) and the last equality, $(xy)^A = (xyy)^A$, i.e. (2) also holds. To see that (3) holds, we have from (26) and (28), for any $y,z \in \Sigma^*$, $(xyxzx)^A = (x_1x_2^nx_3yx_1x_2^nx_3zx_1x_2^nx_3)^A$ and $(xzxyx)^A =$ $= (x_1x_2^nx_3zx_1x_2^nx_3yx_1x_2^nx_3)^A$. From (25) it follows that $(xyxzx)^A =$ $= (xzxyx)^A$. Hence A is k-testable.

(c) implies (a). Let A be k-testable, and let e be an idempotent of S_A. We claim that the subsemigroup eS_Ae of S_A is idempotent and commutative. Let $a \in S_A$, and let $x,y \in \Sigma^+$ be such that $e = x^A$ and $a = y^A$. Since $|x| > 0$, there exist $u,v \in \Sigma^*$, such that $x^k = uv$ and $|v| = k - 1$. Let $w = yx^k = yuv$. Since A is k-testable, it follows from (2) that $(vyuv)^A = (vyuvyuv)^A$. Thus, since x^A is idempotent, $eae = (xyx)^A = (x^kyx^k)^A = (uvyuv)^A = (uvyuvyuv)^A = (x^kyx^kyx^k)^A =$ $= eaeae = eaeeae$. Hence eS_Ae is idempotent. By a similar argument, using (3), one can show that eS_Ae is commutative. Thus, S_A is

locally testable. □

Combining now, theorems 2 and 3 and proposition 1, we have the main result of chapter 2:

Theorem 4. Let $\hat{A}$ be the reduced automaton accepting the event E. The following are equivalent:

(a) E is locally testable.

(b) A is locally testable.

(c) S_A is locally testable.

(d) There exist semiautomata B and C, B definite and C idempotent and commutative, such that $A \leq B \circ C$.

(e) $E \in \beta_3$.

Finally, we mention the following open problems regarding locally testable events. Theorem 3 implies that the event E, accepted by the reduced automaton $\hat{A}$, is locally testable iff A is k-testable, where $k = \#S_A + 2$. Can this bound on k be improved? A related problem is to find "efficiently" the smallest k such that a given locally testable semiautomaton is k-testable. With the present methods, one would test if it is k-testable for $k = 1,\ldots,\#S_A + 2$. Finally, find a step by step method to decompose a locally testable semiautomaton, e.g. like that of Zeiger [G1]. Our approach uses the free k-definite and the free idempotent and commutative semiautomata to do this, and it succeeds since these are finite for a fixed alphabet. However, in general, there are smaller semiautomata, the cascade product of which covers A. See for instance, the example given in section 32. This

problem could be of interest since in general the free automata are infinite and their use would be impossible.

5. Generalized definite events.

For the sake of completeness we include a characterization of generalized definite events which is obtained by methods similar to those used for locally testable events. We leave it to the reader to verify the following.

Lemma 4. An event E is generalized definite iff there exists an integer $k \geq 0$ such that for all $u,v \in \Sigma^*$, if $f_k(u) = f_k(v)$ and $t_k(u) = t_k(v)$ then $u \in E$ iff $v \in E$.

Now we have:

Theorem 5. Let $\hat{A} = (Q,\Sigma,M,q_0,F)$ be the reduced automaton accepting the event E. Then E is generalized definite iff for every idempotent $e \in S_A$ the monoid eS_Ae consists solely of the element e.

Proof. Let us suppose E is generalized definite. Then, by lemma 4, there is a $k \geq 0$ such that for all $u,v \in \Sigma^*$, if $f_k(u) = f_k(v)$ and $t_k(u) = t_k(v)$ then $u \in E$ iff $v \in E$. Let e be an idempotent of S_A and let $a \in S_A$. Then there exist $x,y \in \Sigma^+$, such that $e = x^A$ and $a = y^A$. Let us assume that $(xyx)^A \neq x^A$. Since $x^A = (x^2)^A$, it follows that $(x^{k+1}yx^{k+1})^A \neq (x^{k+1})^A$. Since $\hat{A}$ is reduced, there are $z_1,z_2 \in \Sigma^*$ such that $w_1 = z_1x^{k+1}yx^{k+1}z_2 \in E$ iff $w_2 = z_1x^{k+1}z_2 \notin E$. Now, $x \in \Sigma^+$ implies that $f_k(w_1) = f_k(w_2) = f_k(z_1x^k)$ and $t_k(w_1) = t_k(w_2) = t_k(x^kz_2)$. Thus, $w_1 \in E$ iff $w_2 \in E$ which is a contradiction. Hence $(xyx)^A = x^A$ and therefore eS_Ae consists of e only.

Conversely, let us assume that for every idempotent $e \in S_A$,

eS_Ae consists of e only. Let $\ell = \#S_A + 1$ and let $k = 2\ell$. Furthermore, let $u,v \in \Sigma^*$ be such that $f_k(u) = f_k(v)$ and $t_k(u) = t_k(v)$. We will prove that $u^A = v^A$. In fact, if $|u| < k$ then $f_k(u) = f_k(v)$ implies that $u = v$, and hence $u^A = v^A$. If $|u| \geq k$ then also $|v| \geq k$. Since $f_k(u) = f_k(v)$ and $k = 2\ell$ also $f_\ell(u) = f_\ell(v)$. Similarly $t_\ell(u) = t_\ell(v)$. Let $x = f_\ell(u)$ and $y = t_\ell(u)$. Since $k = 2\ell$, it follows that there exist $u_1,v_1 \in \Sigma^*$ such that $u = xu_1y$ and $v = xv_1y$. Now, since $\ell = \#S_A + 1$ there exist $x_1,x_3,y_1,y_3 \in \Sigma^*$ and $x_2,y_2 \in \Sigma^+$ such that $x = x_1x_2x_3$, $y = y_1y_2y_3$, $x_1^A = (x_1x_2)^A$ and $y_1^A = (y_1y_2)^A$. On the other hand, clearly S_A is group-free; hence A is permutation-free and thus, by lemma 1.1, if $n = \#Q$ then $(x_2^n)^A$ and $(y_2^n)^A$ are idempotents of S_A. Now, clearly

$$u^A = (x_1x_2^nx_3u_1y_1y_2^ny_3)^A.$$

On the other hand, since $(y_2^n)^A$ is an idempotent, $(y_2^n)^A = (y_2^nx_2^ny_2^n)^A$. Thus,

$$u^A = (x_1x_2^nx_3u_1y_1y_2^nx_2^ny_2^ny_3)^A.$$

Since $(x_2^n)^A$ is also idempotent

$$(x_2^nx_3u_1y_1y_2^nx_2^n)^A = (x_2^n)^A.$$

Hence $u^A = (x_1x_2^ny_2^ny_3)^A$. Similarly, $v^A = (x_1x_2^ny_2^ny_3)^A$ and therefore $u^A = v^A$. Thus $u \in E$ iff $v \in E$ and, by lemma 4, E is generalized definite. □

CHAPTER 3

Infinite Hierarchies of Dot-Depth One Events

1. Introduction.

We begin this chapter by defining a congruence relation ${}_m\sim_k$ over Σ^*, which is a generalization of the congruence $\sim_k$, studied in Chapter 2. We introduce a multiplicity parameter m, in the sense that instead of considering subwords of x of length k, we consider m-tuples of subwords of x of length k. This is motivated by events of the form $Iw_1Iw_2\ldots Iw_mI$ in the basis of β_{2m+1}, instead of IwI in the basis of β_3. The first idea which comes to mind is to say that an m-tuple $(w_1,w_2,\ldots,w_m)$ occurs in x iff there exist $u_1,u_2,\ldots,u_{m+1} \in \Sigma^*$, such that $x = u_1w_1u_2w_2\ldots u_mw_mu_{m+1}$. One can verify however that, if one substitutes this instead of (1-tuples of) subwords in the definition of $\sim_k$, the resulting relation is not a congruence. For example, let $m = k = 2$ and let $x = 101000$ and $y = 10100$. Both words begin with 1, end with 0, and contain the 2-tuples (10,10), (10,00) and (01,00). However, $x0 = 1010000$ contains (00,00), while $y0 = 101000$ does not. One way of overcoming this difficulty is to allow a partial overlapping of consecutive subwords in the m-tuple. This will be done in what follows.

First, we need some notation.

Notation. We will denote the cartesian product $A \times A \times \ldots \times A$ (m-times) by $(A)^m$. Note that A^m denotes the concatenation AA...A (m-times). For $w_1,w_2,\ldots,w_m \in A$, the m-tuple $\underline{w} = (w_1,w_2,\ldots,w_m)$ denotes an element of $(A)^m$. By convention $(A)^0 = \{()\}$, i.e. $(A)^0$ contains only

one element with no components. For $m = 1$, we sometimes write w_1 instead of $\underline{w}$, where $\underline{w} = (w_1)$. If $\underline{w}_i = (w_{i,1},\ldots,w_{i,j_i}) \in (A)^{j_i}$, for $1 \leq i \leq n$, then $(\underline{w}_1,\underline{w}_2,\ldots,\underline{w}_n)$ denotes $(w_{1,1},\ldots,w_{1,j_1},\ldots,w_{n,1},\ldots,w_{n,j_n}) \in (A)^{j_1+\ldots+j_n}$.

Definition 1. Let k,m be integers, $k,m > 0$; let $x \in \Sigma^*$ and let $\underline{w} \in (\Sigma^k)^m$. We say that $\underline{w}$ occurs in x if there exist $\underline{u},\underline{v} \in (\Sigma^*)^m$ such that for $i = 1,2,\ldots,m$, $x = u_i w_i v_i$ and $|u_1| < |u_2| < \ldots < |u_m|$. We write $x = \underline{u}\underline{w}\underline{v}$, and say that $\underline{u}$ ($\underline{v}$) is a front (tail) of $\underline{w}$ in x, or that $\underline{w}$ occurs in x with front $\underline{u}$ and tail $\underline{v}$. Let

$$\mu_{m,k}(x) = \{\underline{w} \mid \underline{w} \in (\Sigma^k)^m, \underline{w} \text{ occurs in } x\}.$$

By convention, $\mu_{0,k}(x) = \phi$.

Note that, in general, $x = \underline{u}\underline{w}\underline{v} = \underline{u}'\underline{w}\underline{v}'$ does not imply $\underline{u} = \underline{u}'$, nor $\underline{v} = \underline{v}'$; i.e. $\underline{w}$ might occur in x with different fronts and tails. We also note that, for $k,m > 0$, $\mu_{m,k}(x) = \phi$ iff $|x| < m + k - 1$.

By way of an example, let $m = k = 2$, and let $x = 010110$, $y = 1010110$ and $z = 01010110$. We have:

$$\mu_{2,2}(x) = \mu_{2,2}(y) = \mu_{2,2}(z) =$$
$$= \{(01,10), (01,01), (01,11),$$
$$(10,01), (10,11), (10,10),$$
$$(11,10)\}.$$

Now we define the relation $\underset{m}{\sim}_k$.

Definition 2. For $x,y \in \Sigma^*$ and for integers $k > 0$ and $m \geq 0$, define

$$x \; {}_{m}\!\sim_{k} \; y \text{ iff } x = y \text{ if } |x| < m + k - 1, \text{ or}$$

$$f_{k-1}(x) = f_{k-1}(y),\ t_{k-1}(x) = t_{k-1}(y)$$

$$\text{and } \mu_{m,k}(x) = \mu_{m,k}(y) \text{ otherwise.}$$

It is easily verified that, for all m,k, ${}_{m}\!\sim_{k}$ is an equivalence relation over Σ^*. We denote by ${}_{m}[x]_{k}$ the equivalence class containing x.

Let m,k,x,y and z be as in the last example. Then $x \; {}_{2}\!\sim_{2} \; z$, but $x \; {}_{2}\!\not\sim_{2} \; y$, since the length 1 prefixes of x and y are different.

Note that, for $m = 0$, $x \; {}_{0}\!\sim_{k} \; y$ iff $f_{k-1}(x) = f_{k-1}(y)$ and $t_{k-1}(x) = t_{k-1}(y)$, since $\mu_{0,k} = \phi$ and if $|x| < k - 1$, then $f_{k-1}(x) = f_{k-1}(y)$ implies $x = y$. Thus, (cf. lemma 4 in chapter 2), an event E is generalized definite iff there exists a k such that E is a union of congruence classes of ${}_{0}\!\sim_{k}$. On the other hand, $\mu_{1,k}(x) = m_k(x)$ and hence ${}_{1}\!\sim_{k}$ is the same relation as $\sim_k$ in chapter 2. Thus, an event E is k-testable iff E is a union of congruence classes of ${}_{1}\!\sim_{k}$.

In order to further illustrate the above definitions we prove the following proposition:

Proposition 1. Let m,m_1,k,k_1 be integers such that $0 \leq m \leq m_1$ and $0 < k \leq k_1$, and let $x,y \in \Sigma^*$. Then,

(a) $x \; {}_{m_1}\!\sim_{k} \; y$ implies $x \; {}_{m}\!\sim_{k} \; y$,

(b) $x \; {}_{m}\!\sim_{k_1} \; y$ implies $x \; {}_{m}\!\sim_{k} \; y$,

(c) $x \; {}_{m_1}\!\sim_{k_1} \; y$ implies $x \; {}_{m}\!\sim_{k} \; y$,

(d) $\underset{m}{\sim}_k$ is a congruence relation of finite index over Σ^*.

Proof. (a) It is sufficient to prove (a) for $m_1 = m + 1$. If $|x| < m_1 + k - 1 = m + k$, then $x = y$, hence $x \underset{m}{\sim}_k y$. Let us then consider $|x| \geq m + k$. Since $f_{k-1}(x) = f_{k-1}(y)$ and $t_{k-1}(x) = t_{k-1}(y)$ by hypothesis, it is sufficient to prove that $\mu_{m,k}(x) = \mu_{m,k}(y)$. If $m = 0$ we have nothing to prove; otherwise $\mu_{m,k}(x) \neq \phi$. Let $\underline{w} \in \mu_{m,k}(x)$ and let $\underline{u} \in (\Sigma^*)^m$ be a front of $\underline{w}$ in x. Since x has at least $m + 1$ prefixes (including λ) not longer than $|x| - k$, there exist an integer j, $0 \leq j \leq m$, and $u' \in \Sigma^*$, $w' \in \Sigma^k$, $\underline{z}_1, \underline{z}_3 \in (\Sigma^*)^j$ and $\underline{z}_2, \underline{z}_4 \in (\Sigma^*)^{m-j}$, such that $\underline{w} = (\underline{z}_1, \underline{z}_2)$, $\underline{u} = (\underline{z}_3, \underline{z}_4)$ and $(\underline{z}_1, w', \underline{z}_2)$ occurs in x with front $(\underline{z}_3, u', \underline{z}_4)$. Since $x \underset{m+1}{\sim}_k y$, it follows that $(\underline{z}_1, w', \underline{z}_2)$ occurs in y, say with front $(\underline{z}_5, u'', \underline{z}_6)$, where $\underline{z}_5 \in (\Sigma^*)^j$ and $\underline{z}_6 \in (\Sigma^*)^{m-j}$. Then $\underline{w} = (\underline{z}_1, \underline{z}_2)$ occurs in y with front $(\underline{z}_5, \underline{z}_6)$. Hence $\underline{w} \in \mu_{m,k}(y)$ and $\mu_{m,k}(x) \subseteq \mu_{m,k}(y)$. Similarly $\mu_{m,k}(y) \subseteq \mu_{m,k}(x)$ and (a) follows.

(b) It is sufficient to consider the case $k_1 = k + 1$. If $|x| < m + k_1 - 1 = m + k$, then $x = y$; hence $x \underset{m}{\sim}_k y$. Otherwise $f_{k_1-1}(x) = f_{k_1-1}(y)$ implies $f_{k-1}(x) = f_{k-1}(y)$. Similarly $t_{k-1}(x) = t_{k-1}(y)$. Thus, it suffices to prove that $\mu_{m,k}(x) = \mu_{m,k}(y)$. If $m = 0$ this holds, so let us consider $m > 0$. Let $\underline{w} \in \mu_{m,k}(x)$ and let $\underline{u}, \underline{v} \in (\Sigma^*)^m$ be such that $x = \underline{uwv}$. We claim that there exist an integer j, $0 \leq j \leq m$, such that $\underline{z} \in \mu_{m,k+1}(x)$ occurs in x with front $\underline{t}$, where $z_i = w_i\sigma_i$, $t_i = u_i$ and $\sigma_i = f_1(v_i)$ if $i \leq j$, and $z_i = \sigma_i w_i$ and t_i and $\sigma_i \in \Sigma$ are such that $u_i = t_i\sigma_i$ if $i > j$.

If $u_1 \neq \lambda$, take $j = 0$; if $v_m \neq \lambda$, take $j = m$. If $u_1 = v_m = \lambda$ then take j, $0 < j < m$, such that $|u_j| + 1 < |u_{j+1}|$. Such j exists, since $|x| \geq m + k$. Now, since $x \underset{m}{\sim}_{k+1} y$, $\underline{z}$ occurs in y, and this implies that $\underline{w}$ also occurs in y. Hence $\mu_{m,k}(x) \subseteq \mu_{m,k}(y)$. Similarly $\mu_{m,k}(y) \subseteq \mu_{m,k}(x)$ and (b) follows.

(c) This follows directly from (a) and (b).

(d) First we prove that if $x \underset{m}{\sim}_k y$ and $\sigma \in \Sigma$, then

$$x\sigma \underset{m}{\sim}_k y\sigma. \tag{1}$$

If $|x| < m + k - 1$ then $x = y$ and (1) holds. Hence, consider $|x| \geq m + k - 1$. Clearly $f_{k-1}(x\sigma) = f_{k-1}(y\sigma)$ and $t_{k-1}(x\sigma) = t_{k-1}(y\sigma)$. Thus, it suffices to prove that $\mu_{m,k}(x\sigma) = \mu_{m,k}(y\sigma)$. Since this holds for $m = 0$, assume that $m > 0$. Let $\underline{w} \in \mu_{m,k}(x\sigma)$ occur in $x\sigma$ with tail $\underline{v}$. If $|v_m| > 0$, then $\underline{w} \in \mu_{m,k}(x) = \mu_{m,k}(y) \subseteq \mu_{m,k}(y\sigma)$. If $|v_m| = 0$ then $w_m = t_{k-1}(x)\sigma$. By (a), $x \underset{m-1}{\sim}_k y$; hence, $(w_1,\ldots,w_{m-1}) \in \mu_{m-1,k}(y)$, and $\underline{w} \in \mu_{m,k}(y\sigma)$ since $w_m = t_{k-1}(x)\sigma = t_{k-1}(y)\sigma$. Thus $\mu_{m,k}(x\sigma) \subseteq \mu_{m,k}(y\sigma)$. Similarly $\mu_{m,k}(y\sigma) \subseteq \mu_{m,k}(x\sigma)$ and (1) follows. By induction on $|z|$, it follows that if $x \underset{m}{\sim}_k y$, then $xz \underset{m}{\sim}_k yz$; thus $\underset{m}{\sim}_k$ is a right congruence. By a similar argument $\underset{m}{\sim}_k$ is also a left congruence; hence $\underset{m}{\sim}_k$ is a congruence relation. It is clear that there are only finitely many congruence classes. □

Definition 3. Let $m \geq 0$ and $k > 0$. An event $E \subseteq \Sigma^*$ is (m,k)-testable iff E is a union of congruence classes of $\underset{m}{\sim}_k$. E is (-,k)-testable ((m,-)-testable) if it is (m,k)-testable for some m (for some k). We denote by $\alpha_{m,k}$, γ_k and δ_m the families of (m,k)-testable, (-,k)-testable and (m,-)-testable events, respectively.

It is seen from the definitions and proposition 1 that for a given Σ, $\alpha_{m,k}$ is a finite Boolean algebra of regular events and, for $0 \leq m < m_1$ and $0 < k < k_1$, $\alpha_{m,k} \subseteq \alpha_{m_1,k_1}$. It follows that δ_m and γ_k are Boolean algebras of regular events, such that $\delta_m \subseteq \delta_{m+1}$ and $\gamma_k \subseteq \gamma_{k+1}$.

Definition 4. The δ-hierarchy is the sequence of Boolean algebras

$$\delta_0 \subseteq \delta_1 \subseteq \delta_2 \subseteq \cdots .$$

The γ-hierarchy is the sequence of Boolean algebras

$$\gamma_1 \subseteq \gamma_2 \subseteq \gamma_3 \subseteq \cdots .$$

Clearly $\bigcup_{m\geq 0} \delta_m = \bigcup_{k>0} \gamma_k$.

We illustrate the families of events just defined in Figure 1. The entry (m,k) corresponds to the family $\alpha_{m,k}$. The last entry in a row or column represents the union of all families in that row or column, respectively. Hence these are δ_m and γ_k respectively. We have seen that δ_0 and δ_1 coincide with the families of generalized definite and locally testable events. We will soon establish that the union of all δ_m's is precisely B_2. This is represented by the lower right corner in the figure. We also have $\alpha_{0,1} = \{\phi, I\}$ and $\alpha_{1,1} = IC$

i.e. the family of events accepted by idempotent and commutative automata.

m \ k	1	2	3	. . k . .	-
0	ϕ, I				$\delta_0 = GD$
1	IC				$\delta_1 = LT$
2					δ_2
. . m . .				. . $\alpha_{m,k}$.	δ_m
-	γ_1	γ_2	γ_3	γ_k	B_2

Figure 1 The families $\alpha_{m,k}$, δ_m and γ_k.

2. Relating the δ- and B_2-hierarchies.

Our next objective is to relate the δ- and B_2-hierarchies. The latter has been defined in chapter 1. We will prove that $\delta_0 = \beta_2$ and that for all $m \geq 1$, $\delta_m = \beta_{2m+1}$. This is done in theorem 1. Lemmas 1 and 2 are used to establish $\beta_{2m+1} \subseteq \delta_m$; while lemma 3 is used in the proof of the reverse inclusion.

Lemma 1. Let $m > 1$, $w_1,\ldots,w_m \in \Sigma^*$ and let $E = Iw_1Iw_2\ldots Iw_mI$. Then $E = A \cup B$, where $A \in \beta_{2m}$ and B is a finite union of events of the form $Iz_1Iz_2\ldots Iz_mI$, such that $|z_1| = |z_2| = \ldots = |z_m|$.

Proof. Given an expression $E = Iw_1Iw_2\ldots Iw_mI$, let $g(E) = \sum_{i=1,m} (M - |w_i|)$, where $M = \max\{|w_i|\}$. We proceed by induction on $g(E)$. If $g(E) = 0$, then $|w_1| = |w_2| = \ldots = |w_m|$ and we take $A = \phi$ and $B = E$. Suppose now that $g(E) > 0$ and that the assertion holds for expressions E' such that $g(E') < g(E)$. Since $g(E) > 0$, there is an i, $1 \leq i \leq m$, such that $|w_i| < M$. We have $E = Iw_1Iw_2\ldots Iw_i(\lambda \cup \Sigma I)w_{i+1}\ldots Iw_mI =$

$$= Iw_1Iw_2\ldots Iw_iw_{i+1}\ldots Iw_mI \cup \left[\bigcup_{\sigma\in\Sigma} Iw_1Iw_2\ldots Iw_i\sigma Iw_{i+1}\ldots Iw_mI\right].$$

The first term in the last expression is in β_{2m} and, for each $\sigma \in \Sigma$, $g(Iw_1Iw_2\ldots Iw_i\sigma Iw_{i+1}\ldots Iw_mI) = g(E) - 1$. Since β_{2m} is closed under union, the claim follows by applying the induction hypothesis. []

Lemma 2. Let $m,k > 0$, let $w_1,w_2,\ldots,w_m \in \Sigma^k$, and let $E = Iw_1Iw_2\ldots Iw_mI$. Then $E \in \delta_m$.

Proof. Let $k_1 = m(k - 1) + 1$. We claim that $E \in \alpha_{m,k_1}$. To see this, it is sufficient to prove that if $x \tilde{m} {}_{k_1} y$ then $x \in E$ iff $y \in E$.

Let us suppose then that $x \tilde{m} y$ and $x \in E$, i.e. there exist $u_1,u_2,\ldots,u_{m+1} \in \Sigma^*$ such that $x = u_1w_1u_2w_2\ldots u_mw_mu_{m+1}$. We will construct a $\underline{z} \in (\Sigma^{k_1})^m$, which occurs in x with front $\underline{a}$ and tail $\underline{b}$. The occurrence of $\underline{z}$ in y, will force y to be in E. Let $x_i,t_i,a_i,b_i \in \Sigma^*$ $(i = 1,2,\ldots,m)$ be such that $|s_i| = (i-1)(k-1)$, $|t_i| = (m-i)(k-1)$ and

$$u_1w_1u_2\ldots w_{i-1}u_i = a_is_i$$

$$u_{i+1}w_{i+1}u_{i+2}\ldots w_mu_{m+1} = t_ib_i.$$

Since $a_is_iw_iu_{i+1} = a_{i+1}s_{i+1}$ and $|s_{i+1}| = |s_i| + k - 1$, it follows that $|a_i| < |a_{i+1}|$, for $i = 1,2,\ldots,m-1$. Also $x = a_is_iw_it_ib_i$ and $|s_iw_it_i| = k_1$, hence $\underline{z} \in \mu_{m,k_1}(x)$ occurs in x with front $\underline{a}$ where $z_i = s_iw_it_i$. From $x \tilde{m} y$ it follows that $\underline{z}$ occurs in y, say with front $\underline{c}$ and tail $\underline{d}$. Now we claim that, for $i = 1,2,\ldots,m-1$, $|c_is_iw_i| \leq |c_{i+1}s_{i+1}|$. In fact, $|c_i| < |c_{i+1}|$, since $\underline{c}$ is a front of $\underline{z}$ in y; hence $|c_is_iw_i| = |c_i| + (i-1)(k-1) + k = |c_i| + 1 + i(k-1) \leq |c_{i+1}| + i(k-1) = |c_{i+1}s_{i+1}|$. Thus, there exist $v_1,v_2,\ldots,v_{m-1} \in \Sigma^*$ such that $c_is_iw_iv_i = c_{i+1}s_{i+1}$. Then, one verifies that

$$y = c_1w_1v_1w_2v_2\ldots w_{m-1}v_{m-1}w_md_m.$$

Hence $y \in E$. A similar argument shows that if $y \in E$ then $x \in E$; thus the claim follows and $E \in \delta_m$. □

Note that in the last proof we found a k_1 such that $E \in \alpha_{m,k_1}$. Now we point out that this k_1 is the best possible, in the sense that there exist events $E = Iw_1Iw_2\ldots Iw_mI$, with $w_i \in \Sigma^k$, such that

$E \notin \alpha_{m,k_1-1}$. To see this, consider $w_1 = w_2 = \ldots = w_m = 0^k$; and let $x = 0^{mk-1}$ and $y = 0^{mk}$. Let $\ell = k_1 - 1 = m(k-1)$. Now we claim that $x \underset{m}{\sim}_{\ell} y$. In fact, since $m + \ell - 1 = mk - 1$, neither of $\mu_{m,\ell}(x)$ or $\mu_{m,\ell}(y)$ is empty, and the only $\underline{w} \in (\Sigma^{\ell})^m$ which occurs in x or y is $(0^{\ell},\ldots,0^{\ell})$. The claim follows. Note however that $y \in E$, but $x \notin E$; hence $E \notin \alpha_{m,\ell}$.

Before proving the next result, we introduce the following notation. For $\underline{w} \in (\Sigma^k)^m$, define

$$L(\underline{w}) = \{x \mid \underline{w} \text{ occurs in } x\}.$$

Lemma 3. Let $m,k > 0$, and let $\underline{w} \in (\Sigma^k)^m$. Then $L(\underline{w})$ is a finite union of events of the form $Iz_1Iz_2\ldots Iz_pI$, where $1 \le p \le m$, and $z_1,z_2,\ldots,z_p \in \Sigma^*$.

Proof. We proceed by induction on m. For $m = 1$, $L(w) = \{x \mid x = uwv$ for some $u,v \in \Sigma^*\} = IwI$. Suppose now, that, for $m \ge 1$, the assertion holds for all n, $0 < n \le m$. Let $\underline{w} \in (\Sigma^k)^{m+1}$. We claim that

$$L(\underline{w}) = \left[\bigcup_{i=1,m} L((w_1,\ldots,w_i))L((w_{i+1},\ldots,w_{m+1}))\right] \cup IFI, \tag{2}$$

where

$$F = \{y \mid y \in L(\underline{w}) \text{ and } m + k \le |y| \le m(k-1) + k\}.$$

Note that F is a finite set. For $k = 1$, $F = \phi$, since in this case $m + k > m(k-1) + k$. Denote the expression in brackets by A. If $x \in A$, then there exist $u,v \in \Sigma^*$ and an i, $1 \le i \le m$, such that $x = uv$ and $u \in L((w_1,\ldots,w_i)) = L(\underline{a})$, $v \in L((w_{i+1},\ldots,w_{m+1})) = L(\underline{b})$.

Since $\underline{a}$ occurs in u and $\underline{b}$ occurs in v, it follows that $(\underline{a},\underline{b}) = \underline{w}$ occurs in $uv = x$. Thus $x \in L(\underline{w})$. If $x \in IFI$, then $x = uyv$, where $y \in F$. Since $F \subseteq L(\underline{w})$, we have $y \in L(\underline{w})$. Clearly $x \in L(\underline{w})$. Hence $L(\underline{w}) \supseteq A \cup IFI$. To show the reverse inclusion, let $x \in L(\underline{w})$; then $\underline{w}$ occurs in x, say with front $\underline{u}$ and tail $\underline{v}$. (In what follows, we distinguish two cases. In the first case, there are two consecutive words in $\underline{w}$ which do not overlap in x. In the second one, each pair of consecutive words in $\underline{w}$ do have some overlap.) If there is an i, $1 \leq i \leq m$, such that $|u_i w_i| \leq |u_{i+1}|$, then $(w_1,\ldots,w_i)$ occurs in $u_i w_i$ and $(w_{i+1},\ldots,w_{m+1})$ occurs in v_i. Since $x = u_i w_i v_i$, it follows that $x \in A$. Suppose now that there is no such i, i.e.

$$\text{for all } i,\ 1 \leq i \leq m,\ |u_i w_i| > |u_{i+1}|. \tag{3}$$

Let $y \in \Sigma^*$ be such that $x = u_1 y v_{m+1}$. Now, $\underline{w}$ occurs in y with front $\underline{s}$ and tail $\underline{t}$, where $u_1 s_i = u_i$ and $t_i v_{m+1} = v_i$ $(i = 1,2,\ldots,m+1)$. Hence $y \in L(\underline{w})$. Now, $s_1 = t_{m+1} = \lambda$, hence

$$0 = |s_1| < |s_2| < \ldots < |s_{m+1}| = |y| - k \tag{4}$$

and from (3),

$$\text{for all } i,\ 1 \leq i \leq m,\ |s_i w_i| > |s_{i+1}|. \tag{5}$$

We leave it to the reader to verify that (4) and (5) imply that $m \leq |s_{m+1}| \leq m(k-1)$. Since $y = s_{m+1} w_{m+1}$ and $|w_{m+1}| = k$, it follows that $m + k \leq |y| \leq m(k-1) + k$. Altogether $y \in F$. Thus $x \in IFI$ and $L(\underline{w}) \subseteq A \cup IFI$. Hence (2) holds. Now, replace the $L(\underline{a})$'s in A by the expressions obtained by the induction hypothesis. Using distributivity of concatenation over union, the identity $II = I$ and substituting IFI by $\bigcup_{z \in F} IzI$, one verifies the induction step. □

Note that, even though F is defined in terms of $L(\underline{w})$ itself, it can be obtained directly from $\underline{w}$, since the words in F are not longer than $m(k-1) + k$.

We have now the main result of this section.

Theorem 1. $\delta_0 = \beta_2$. For $m \geq 1$, $\delta_m = \beta_{2m+1} = \beta_{2m+2}$.

Proof. $\delta_0 = \beta_2$ (= family of generalized definite events) and $\delta_1 = \beta_3$ (= family of locally testable events) by propositions 1.3 and 2.1, and by the observation following definition 1. It has been shown in chapter 1 that for $m \geq 1$, $\beta_{2m+1} = \beta_{2m+2}$. We proceed by induction on m to prove that $\delta_m = \beta_{2m+1}$. Suppose that $m > 1$ and that $\delta_{m-1} = \beta_{2m-1} = \beta_{2m}$. We now prove $\beta_{2m+1} \subseteq \delta_m$. It has been noted in chapter 1 (p. 11) that $\beta_{2m+1} = B([w,I]^{2m+1})$, where $[w,I]^n$ denotes the set of concatenations of n factors, each of which is either a word w, or is I. Since δ_m is a Boolean algebra, it is sufficient to prove that $\lceil w,I \rceil^{2m+1} \subseteq \delta_m$. Since $\lceil w,I \rceil^{2m} \subseteq \delta_{m-1}$ by the induction hypothesis, and since $\delta_{m-1} \subseteq \delta_m$, it suffices to prove that $\lceil w,I \rceil^{2m+1} - \lceil w,I \rceil^{2m} \subseteq \delta_m$. If $E \in \lceil w,I \rceil^{2m+1} - [w,I]^{2m}$ then E has one of the following forms: $E_1 = w_1 I w_2 \ldots I w_{m+1}$ or $E_2 = I w_1 I w_2 \ldots I w_m I$. In the first case $E_1 = I\Sigma^{|w_1|} w_2 \ldots I w_m \cap w_1 I$, hence $E_1 \in \beta_{2m} = \delta_{m-1} \subseteq \delta_m$. In the second case, combining lemmas 1 and 2, it follows that $E_2 \in \delta_m$; hence $\beta_{2m+1} \subseteq \delta_m$. Now we claim that $\delta_m \subseteq \beta_{2m+1}$. Since β_{2m+1} is a Boolean algebra, it is sufficient to prove that each congruence class ${}_m\lceil x \rceil_k$ is in β_{2m+1}. Since ${}_m\lceil x \rceil_k = \{x\}$ if $|x| < m + k - 1$, assume

$|x| \geq m + k - 1$. Let $u = f_{k-1}(x)$, $v = t_{k-1}(x)$, $A = \mu_{m,k}(x)$ and $B = (\Sigma^k)^m - A$. One verifies that

$$ {}_m[x]_k = uI \cap Iv \cap \left[\bigcap_{\underline{w} \in A} L(\underline{w}) \right] \cap \left[\bigcap_{\underline{w} \in B} \overline{L(\underline{w})} \right]. $$

By lemma 3, each $L(\underline{w})$ is in β_{2m+1}, and so are uI and Iv. Thus ${}_m[x]_k \in \beta_{2m+1}$ and the theorem holds. □

Corollary 1. $\bigcup_{m \geq 0} \delta_m = \bigcup_{k>0} \gamma_k = \bigcup_{n \geq 1} \beta_n = B_2$.

Note that this shows that the family in the lower right corner of figure 1 is, in fact, B_2.

3. The hierarchies are infinite.

Now we will prove that all three of the B_2, γ and δ-hierarchies are infinite. The following proposition plays a key role in this proof.

Proposition 2. Let $m \geq 0$, $k > 0$, $x \in \Sigma^{k-1}$, $y,z \in \Sigma^*$. Then

(a) $x(yx)^m \underset{m}{\sim}_k x(yx)^{m+1}$,

(b) $x(yxzx)^m \underset{m}{\sim}_k x(yxzx)^m yx$.

Proof. (a) We proceed by induction on m. For $m = 0$ $x \underset{0}{\sim}_k xyx$, since $|x| = k - 1$. For $m = 1$, the result holds by proposition 2.4(a) in chapter 2. Assume that $m > 1$, and that

$$z_1 = x(yx)^{m-1} \underset{m-1}{\sim}_k x(yx)^m = z_2. \tag{6}$$

We claim that

$$z_2 = x(yx)^m \underset{m}{\sim}_k x(yx)^{m+1} = z_3. \tag{7}$$

If $x = y = \lambda$ we have nothing to prove. Otherwise $m + k - 1 \leq |z_2| < |z_3|$; hence $\mu_{m,k}(z_3) \neq \phi$. Now, $f_{k-1}(z_2) = f_{k-1}(z_3) = t_{k-1}(z_2) = t_{k-1}(z_3) = x$. Also $\mu_{m,k}(z_2) \subseteq \mu_{m,k}(z_3)$, since z_2 is a prefix of z_3. Let us prove the reverse inclusion. Let $(\underline{w},s) \in \mu_{m,k}(z_3)$. Clearly $\underline{w} \in \mu_{m-1,k}(z_3)$ and $s \in \mu_{1,k}(z_3)$. Now, $xyx \underset{1}{\sim}_k x(yx)^2$ by the induction hypothesis. It follows that $xyx \underset{1}{\sim}_k x(yx)^{m+1} = z_3$, thus $\mu_{1,k}(z_3) = \mu_{1,k}(xyx)$. Hence, there exist $u,v \in \Sigma^*$, such that $xyx = usv$. On the other hand, from (6) $z_1 = x(yx)^{m-1} \underset{m-1}{\sim}_k x(yx)^{m+1} = z_3$. Thus $\underline{w}$ occurs in z_1, say with front $\underline{a}$. Since $|w_{m-1}| = k$ and $|x| = k - 1$, it follows that $|a_{m-1}| < |(xy)^{m-1}|$. Hence $(\underline{w},s)$ occurs in $x(yx)^m = z_2$ with front $(\underline{a},(xy)^{m-1}u)$. Thus, $\mu_{m,k}(z_3) \subseteq \mu_{m,k}(z_2)$, and (7) holds.

(b) Replacing y in (a) by yxz we have:

$$w_1 = x(yxzx)^m \underset{m}{\sim}_k x(yxzx)^{m+1} = w_3. \qquad (8)$$

Let $w_2 = x(yxzx)^m yx$. We claim that $w_1 \underset{m}{\sim}_k w_2$. If $yx = \lambda$, then $w_1 = w_2$; otherwise $m + k - 1 \leq |w_1| < |w_2|$. We have: $f_{k-1}(w_1) = f_{k-1}(w_2) = t_{k-1}(w_1) = t_{k-1}(w_2) = x$. Since $w_2 = w_1 yx$ and $w_3 = w_2 zx$, it follows that $\mu_{m,k}(w_1) \subseteq \mu_{m,k}(w_2) \subseteq \mu_{m,k}(w_3)$. From (8), $\mu_{m,k}(w_1) = \mu_{m,k}(w_3)$; hence $\mu_{m,k}(w_1) = \mu_{m,k}(w_2)$. □

Now we have the main results of this section.

Theorem 2. For all $m \geq 0$, $\delta_m \subsetneq \delta_{m+1}$. $\beta_1 \subsetneq \beta_2 \subsetneq \beta_3$ and, for all $m \geq 1$, $\beta_{2m+1} \subsetneq \beta_{2m+3}$. Hence the B_2 and δ-hierarchies are infinite.

Proof. Let $\Sigma = \{0,1\}$ and let $E = (I0)^{m+1}I$. Suppose $E \in \delta_m$, i.e. for some $k > 0$, $E \in \alpha_{m,k}$. Let $\ell = k - 1$, $x = 1^\ell$, $y = 0$, $z = \lambda$. By proposition 2(b) $z_1 = 1^\ell(01^\ell 1^\ell)^m \underset{m}{\sim}_k 1^\ell(01^\ell 1^\ell)^m 01^\ell = z_2$. Hence $z_1 \in E$ iff $z_2 \in E$. However, $z_1 \notin E$ and $z_2 \in E$, a contradiction. Thus $E \notin \delta_m$. Since, by lemma 2 $E \in \delta_{m+1}$, it follows that $\delta_m \subsetneq \delta_{m+1}$. It is easy to see from the results of chapter 2, that $\beta_1 \subsetneq \beta_2 \subsetneq \beta_3$. From theorem 1, for $m \geq 1$, $\beta_{2m+1} = \delta_m \subsetneq \delta_{m+1} = \beta_{2m+3}$. □

Theorem 3. For all $k > 0$, $\gamma_k \subsetneq \gamma_{k+1}$; hence the γ-hierarchy is infinite.

Proof. Let $\Sigma = \{0,1\}$ and let $E = I0^k$. Suppose $E \in \gamma_k$, i.e. for some $m \geq 0$, $E \in \alpha_{m,k}$. Let $x = 0^{k-1}$, $y = 0$ and $z = 1$. By proposition 2(b)

$z_1 = 0^{k-1}(00^{k-1}10^{k-1})^m \underset{m}{\sim}_k 0^{k-1}(00^{k-1}10^{k-1})^m 00^{k-1} = z_2$. Hence, $z_1 \in E$ iff $z_2 \in E$. However $z_1 \notin E$ and $z_2 \in E$, a contradiction. Thus $E \notin \gamma_k$. Clearly $E \in \alpha_{0,k+1} \subseteq \gamma_{k+1}$; hence $\gamma_k \subsetneq \gamma_{k+1}$. □

Theorem 4. The γ and δ-hierarchies are incomparable, in the sense that for all $m \geq 0$ and $k > 0$, $\delta_m \not\subseteq \gamma_k$ and $\gamma_k \not\subseteq \delta_m$.

Proof. Let $\Sigma = \{0,1\}$, $I0^k \in \alpha_{0,k+1}$; thus $I0^k \in \delta_0 \subseteq \delta_m$. By the proof of theorem 3, $I0^k \notin \gamma_k$; hence $\delta_m \not\subseteq \gamma_k$. $(I0)^{m+1}I \in \alpha_{m+1,1}$; thus $(I0)^{m+1}I \in \gamma_1 \subseteq \gamma_k$. By the proof of theorem 2 $(I0)^{m+1}I \notin \delta_m$; hence $\gamma_k \not\subseteq \delta_m$. □

4. Duality.

In this section we introduce a left-right duality, which will be extensively used throughout the next two chapters.

The dual of a concept or proposition is obtained by replacing in its statement every concatenation uv by vu, every concatenation of m-tuples $(\underline{t}_1,\underline{t}_2,\ldots,\underline{t}_n)$ by $(\underline{t}_n,\ldots,\underline{t}_2,\underline{t}_1)$, and every concept by its dual. Thus, prefix and suffix are dual concepts, while subword is self-dual. Similarly, $f_k(x)$ and $t_k(x)$ are duals but $\mu_{m,k}(x)$ is self-dual. It follows that $\underset{m}{\sim}_k$ is self-dual and this is why duality will be useful.

For example, the dual of proposition 2 is: Let $m \geq 0$, $k > 0$, $x \in \Sigma^{k-1}$, $y,z \in \Sigma^*$. Then

(a) $(xy)^m x \underset{m}{\sim}_k (xy)^{m+1} x$;

(b) $(xzxy)^m x \underset{m}{\sim}_k xy(xzxy)^m x$.

Note that 2(a) is self-dual, but 2(b) is not.

The proof of the dual of a proposition is obtained by making the necessary changes throughout the original proof. We will use the duals of certain propositions, subject to the agreement that their proofs, obtained as above, are valid. If desired, this can be checked in each case; in fact we assume that this has been done.

In many cases, the dual of a proposition can also be proved by using the following:

Proposition 3. $x \underset{m}{\sim}_k y$ iff $x^T \underset{m}{\sim}_k y^T$.

Proof. We leave the proof to the reader. □

CHAPTER 4

Characterizations of Events in γ_1.

1. Introduction.

In this chapter we study the particular case of the congruence $\tilde{m}_k$, where $k = 1$. We will denote $\tilde{m}_1$ by $\tilde{m}$, and $\mu_{m,1}(x)$ by $\mu_m(x)$. The next two propositions illustrate how the concepts "$\underline{w}$ occurs in x" and "$x \tilde{m} y$" become simpler in this case.

Proposition 1. Let $m > 0$, $\underline{\sigma} \in (\Sigma)^m$ and $x \in \Sigma^*$. Then $\underline{\sigma}$ occurs in x iff there exists $\underline{u} \in (\Sigma^*)^{m+1}$, such that $x = u_1\sigma_1u_2\sigma_2\ldots u_m\sigma_m u_{m+1}$.

Proof. The proof is left to the reader. □

Definition 1. Let $m > 0$, $\underline{\sigma} \in (\Sigma)^m$ and $x \in \Sigma^*$. $\underline{\sigma}$ is an m-tuple in x iff $\underline{\sigma}$ occurs in x. A ($\leq m$)-tuple in x is an n-tuple in x for some n, $0 < n \leq m$. Let $U_m(x)$ denote the set of ($\leq m$)-tuples in x. Clearly $U_m(x) = \bigcup_{i=1}^{m} \mu_i(x)$. By convention, $U_0(x) = \phi$. With this terminology we have:

Proposition 2. Let $m \geq 0$, and $x,y \in \Sigma^*$. $x \tilde{m} y$ iff $U_m(x) = U_m(y)$.

Proof. Suppose that $x \tilde{m} y$. If $|x| < m$ then $x = y$, hence $U_m(x) = U_m(y)$. If $|x| \geq m$, then $\mu_m(x) = \mu_m(y)$. By proposition 3.1(a), for all i, $0 \leq i \leq m$, $x \tilde{i} y$. Thus $\mu_i(x) = \mu_i(y)$ and it follows that $U_m(x) = U_m(y)$. Conversely, let $x,y \in \Sigma^*$ be such that $U_m(x) = U_m(y)$. This implies that for all i, $0 \leq i \leq m$, $\mu_i(x) = \mu_i(y)$. If $|x| \geq m$ then $\mu_m(x) = \mu_m(y)$ implies that $x \tilde{m} y$. Suppose now,

that $|x| < m$, then $\mu_m(x) = \phi$. If $U_m(x) = \phi$ then $x = y = \lambda$. If $U_m(x) \neq \phi$ then let n be the greatest integer such that $\mu_n(x) \neq \phi$ and let $\underline{\sigma} \in \mu_n(x)$. Clearly, by the choice of n, $x = y = \sigma_1\sigma_2\ldots\sigma_n$. In any case $x \underset{m}{\sim} y$. □

In what follows, proposition 2 will replace, without reference, the definition of $\underset{m}{\sim}$.

For the sake of completeness and easy reference, we restate some of the results of the previous chapter.

Proposition 3. Let $m \geq 0$ and $x,y \in \Sigma^*$.

(a) If $0 \leq m \leq n$ then $x \underset{n}{\sim} y$ implies $x \underset{m}{\sim} y$.

(b) $\underset{m}{\sim}$ is a congruence relation of finite index over Σ^*.

(c) $x^m \underset{m}{\sim} x^{m+1}$.

(d) $(xy)^m \underset{m}{\sim} (xy)^m x$.

We now have a result, which will be used in the next section.

Proposition 4. Let $u,x,y \in \Sigma^*$ and let $m \geq 0$. If $u \underset{m}{\sim} uxy$ then $u \underset{m}{\sim} ux \underset{m}{\sim} uy \underset{m}{\sim} uxy \underset{m}{\sim} uyx$.

Proof. We first prove that $u \underset{m}{\sim} ux$. In fact, for any $u,x,y \in \Sigma^*$, $U_m(u) \subseteq U_m(ux) \subseteq U_m(uxy)$. Since $U_m(u) = U_m(uxy)$ by hypothesis, it follows that $U_m(u) = U_m(ux)$. Hence $u \underset{m}{\sim} ux$. The remaining equivalences follow easily, since $\underset{m}{\sim}$ is a congruence relation. □

The main result of this chapter is:

Theorem 7. Let $\hat{A} = (Q,\Sigma,M,q_0)$ and $\hat{B} = (R,\Sigma,N,r_0)$ be reduced automata accepting the events E and E^T respectively. The following are

equivalent:

(a) E is $(-,1)$-testable, i.e. $E \in \gamma_1$.

(b) A and B are partially ordered semiautomata.

(c) A is a partially ordered semiautomaton, such that, for all $q \in Q$, and for all $x,y \in \Sigma^*$, $qx^A = q(xx)^A = q(xy)^A$ and $qy^A = q(yy)^A = q(yx)^A$ imply $qx^A = qy^A$.

(d) S_A is J-trivial.

The definitions of J-trivial semigroup and partially ordered semiautomata are given in sections 3 and 4 respectively.

A corollary of this theorem is that one can decide whether an event E is $(m,1)$-testable for some m, i.e. whether an event is in γ_1.

In the proof of the theorem, (a) implies (b), (b) implies (c) and (c) implies (d) are not difficult to prove, and these three implications are proved in section 4. The situation is quite different when proving (d) implies (a), which is basically done in sections 2 and 3. Our strategy will be to find, in section 2, an equivalent formulation of $x \underset{m}{\sim} y$ (cf. theorem 4). From this, after studying J-trivial semigroups in section 3, we will be able to complete the proof of the main result. Following theorem 7 in section 4, we give a review of the proof of (d) implies (a). The reader may wish to consult this review, while reading through sections 2 and 3. Finally, we remark that the results of section 2 can also be used for "efficiently" testing whether two words are m-equivalent. This clearly can be done ("inefficiently") by using proposition 2.

2. Characterization of $\underset{m}{\sim}$.

21. Reduced words.

In this subsection we define m-reduced words and characterize them. In doing so we reduce the problem of deciding whether $x \underset{m}{\sim} y$, to the particular case when x and y are m-reduced. Intuitively, x is m-reduced if no letter can be deleted from x, without loosing some m-tuple; i.e. for any u,σ,v such that $x = u\sigma v$ some ($\leq m$)-tuple in $u\sigma v$ does not occur in uv. More formally, we have:

Definition 2. Let $m > 0$. A word $x \in \Sigma^+$ is m-reduced if for all $u,v \in \Sigma^*$, and for all $\sigma \in \Sigma$, $x = u\sigma v$ implies $u\sigma v \underset{m}{\not\sim} uv$.

Thus, 012 is an example of a 1-reduced word. In fact, $012 \underset{1}{\not\sim} 12$, $012 \underset{1}{\not\sim} 02$ and $012 \underset{1}{\not\sim} 01$. On the other hand, 0102 is not 1-reduced, since $0102 \underset{1}{\sim} 012$. The reader can verify that 0102 is 2-reduced. Also note, that it follows from proposition 3(a) that, if x is m-reduced, then it is also (m+1)-reduced.

Now we define the function $r(u,x)$ and show how to compute it.

Definition 3. Let $u \in \Sigma^*$ and $x \in \Sigma^+$. Then $r(u,x)$ is the greatest integer m, such that $u \underset{m}{\sim} ux$.

Since for all u and x, $u \underset{0}{\sim} ux$, and since $x \in \Sigma^+$ implies that for all $n \geq |ux|$ $u \underset{n}{\not\sim} ux$, the function $r(u,x)$ is well defined. In view of proposition 3(a) one easily verifies that $u \underset{m}{\sim} ux$ iff $m \leq r(u,x)$. This will be used without reference. Also note that, for $\sigma \in \Sigma$, $r(u,\sigma) = 0$ iff σ does not occur in u.

Proposition 5. Let $u \in \Sigma^*$ and $x,y \in \Sigma^+$. Then

$$r(u,xy) = \min[r(u,x),r(ux,y)] = \min[r(u,x),r(u,y)].$$

Proof. Let $q_1 = r(u,xy)$, $p_1 = r(u,x)$, $p_2 = r(ux,y)$, $p_3 = r(u,y)$, $q_2 = \min[p_1,p_2]$ and $q_3 = \min[p_1,p_3]$. We have to prove that $q_1 = q_2 = q_3$. Since $q_1 = r(u,xy)$, $u \underset{q_1}{\sim} xy$. By proposition 4, $u \underset{q_1}{\sim} ux \underset{q_1}{\sim} xy$, hence $q_1 \leq p_1 = r(u,x)$ and $q_1 \leq p_2 = r(ux,y)$. Thus,

$$q_1 \leq \min[p_1,p_2] = q_2. \tag{1}$$

Since $q_2 = \min[r(u,x), r(ux,y)]$, it follows that $u \underset{q_2}{\sim} ux$ and $ux \underset{q_2}{\sim} xy$. Hence, $u \underset{q_2}{\sim} xy$. By proposition 4 $u \underset{q_2}{\sim} uy$, hence $q_2 \leq p_3 = r(u,y)$. Since $q_2 \leq p_1$ by assumption, we have

$$q_2 \leq \min[p_1,p_3] = q_3. \tag{2}$$

Finally, since $q_3 = \min[r(u,x), r(u,y)]$, it follows that $u \underset{q_3}{\sim} ux$ and $u \underset{q_3}{\sim} uy$. Hence $uy \underset{q_3}{\sim} xy$ and $u \underset{q_3}{\sim} xy$. Thus,

$$q_3 \leq q_1 = r(u,xy). \tag{3}$$

The claim follows from (1), (2) and (3). □

Corollary 1. Let $u \in \Sigma^*$ and $x \in \Sigma^+$. Then

$$r(u,x) = \min_{\substack{a,b \in \Sigma^*,\ \sigma \in \Sigma \\ a\sigma b = x}} [r(ua,\sigma)] \tag{a}$$

$$= \min_{\sigma \in \mu_1(x)} [r(u,\sigma)].$$

Proof. This follows by induction on $|x|$. □

Corollary 2. Let $x,y \in \Sigma^+$ be such that $x \ {}_1\!\sim\ y$. Then for all $u \in \Sigma^*$, $r(u,x) = r(u,y)$.

Proof. Since $\mu_1(x) = \mu_1(y)$, this follows from corollary 1. □

Proposition 6. Let $u,v \in \Sigma^*$, $\sigma \in \Sigma$ and let $m \geq 0$.

(a) If $u \ {}_m\!\sim\ u\sigma v$ then $u\sigma v \ {}_{m+1}\!\sim\ u\sigma v\sigma$.

(b) If $\sigma \notin \mu_1(v)$ and $u\sigma v \ {}_{m+1}\!\sim\ u\sigma v\sigma$ then $u \ {}_m\!\sim\ u\sigma v$.

Proof. (a) Clearly $U_{m+1}(u\sigma v) \subseteq U_{m+1}(u\sigma v\sigma)$. To see the reverse inclusion, it is sufficient to consider a ($\leq$ m+1)-tuple $\underline{t}_1$ in $u\sigma v\sigma$, such that $\underline{t}_1 = (\underline{t}_2,\sigma)$ for some ($\leq$ m)-tuple $\underline{t}_2$ in $u\sigma v$, and show that $\underline{t}_1$ occurs in $u\sigma v$. In fact, since $u \ {}_m\!\sim\ u\sigma v$, it follows that $\underline{t}_2$ occurs in u; hence $\underline{t}_1 = (\underline{t}_2,\sigma)$ occurs in $u\sigma$ and also in $u\sigma v$. Thus, $u\sigma v \ {}_{m+1}\!\sim\ u\sigma v\sigma$.

(b) Clearly $U_m(u) \subseteq U_m(u\sigma v)$. Conversely, let $\underline{t}$ be a ($\leq$ m)-tuple in $u\sigma v$. Then $(\underline{t},\sigma)$ is a ($\leq$ m+1)-tuple in $u\sigma v\sigma$. Since $u\sigma v \ {}_{m+1}\!\sim\ u\sigma v\sigma$ it follows that $(\underline{t},\sigma)$ occurs in $u\sigma v$. Since, by assumption σ does not occur in v, it follows that $\underline{t}$ occurs in u. Thus $U_m(u\sigma v) \subseteq U_m(u)$ and the claim follows. □

Note that (b) is a partial converse to (a). That the converse of (a) does not hold can be seen by the following example. Let $m \geq 1$, $u = \lambda$, $v = 0^m$ and $\sigma = 0$. By proposition 3(c) $u\sigma v = 0^{m+1} \ {}_{m+1}\!\sim\ 0^{m+2} = u\sigma v\sigma$. However, it is clear that $u = \lambda \ {}_m\!\not\sim\ 0^{m+1} = u\sigma v$.

Proposition 7. Let $u,v \in \Sigma^*$ and $\sigma \in \Sigma$ be such that $\sigma \notin \mu_1(v)$. Then $r(u\sigma v,\sigma) = 1 + r(u,\sigma v)$.

Proof. Let $p = r(u\sigma v,\sigma)$ and $q = r(u,\sigma v)$. Since $u\sigma v \overset{}{}_{1}\sim u\sigma v\sigma$ it follows that $p \geq 1$. Thus, since $u\sigma v \overset{}{}_{p}\sim u\sigma v\sigma$ and $\sigma \notin \mu_1(v)$, $u \overset{}{}_{p-1}\sim u\sigma v$ by proposition 6(b). Hence $q \geq p - 1$. On the other hand, since $u \overset{}{}_{q}\sim u\sigma v$, $u\sigma v \overset{}{}_{q+1}\sim u\sigma v\sigma$ by proposition 6(a). Hence $p \geq q + 1$. Thus, $p = q + 1$. □

As noted earlier, $r(u,\sigma) = 0$ iff $\sigma \notin \mu_1(u)$. Using this fact, corollary 1(a) and proposition 7, one can compute $r(u,x)$ for any u and x. We illustrate this by an example. First we have:

Definition 4. Let $x = \sigma_1\sigma_2\ldots\sigma_n$ be in Σ^+, where each $\sigma_i \in \Sigma$. The r-vector of x is $(p_1,p_2,\ldots,p_n)$, where $p_i = r(\sigma_1\sigma_2\ldots\sigma_{i-1},\sigma_i)$ if $i > 1$, and $p_1 = r(\lambda,\sigma_1)$.

We will represent the r-vector of x by writing p_i below σ_i. For $x = 01020110$ we have:

i	1	2	3	4	5	6	7	8
σ_i	0	1	0	2	0	1	1	0
p_i	0	0	1	0	1	1	2	2

(4)

We summarize the computation as follows:

$p_1 = r(\lambda,0) = 0,$

$p_2 = r(0,1) = 0,$

$p_3 = r(01,0) = 1 + r(\lambda,01) = 1 + \min[p_1,p_2] = 1,$

$p_4 = r(010,2) = 0,$

$p_5 = r(0102,0) = 1 + \min[p_3,p_4] = 1,$

$p_6 = r(01020,1) = 1 + \min[p_2,p_3,p_4,p_5] = 1,$

$p_7 = r(010201,1) = 1 + \min[p_6] = 2,$

$p_8 = r(0102011,0) = 1 + \min[p_5,p_6,p_7] = 2.$

Now, to compute $r(u,x)$ it is sufficient to compute the r-vector of ux and apply corollary 1(a). E.g. $r(0102,0110) = \min[p_5,p_6,p_7,p_8] = 1$. Since the computation of p_i depends only on p_j's, where $j < i$, the example also gives us $r(01,020) = \min[p_3,p_4,p_5] = 0$.

Proposition 8. Let $u \in \Sigma^*$, $\sigma \in \Sigma$ and $p = r(u,\sigma)$. Then there exists a p-tuple $\underline{t}$ in u, such that $(\underline{t},\sigma)$ does not occur in u.

Proof. Since $u \tilde{p} u\sigma$, it is easily seen that if no such $\underline{t}$ exists, then $u \overset{\sim}{p+1} u\sigma$, which is a contradiction. However, due to the importance of such $\underline{t}$ in what follows, we give a constructive proof by induction on p. If $p = r(u,\sigma) = 0$ then $u \not\overset{\sim}{1} u\sigma$, hence σ does not occur in u. Let $r(u,\sigma) = p > 0$. It follows that $u \overset{\sim}{1} u\sigma$, hence σ occurs in u. Let $v_1,v_2 \in \Sigma^*$ be such that $u = v_1\sigma v_2$ and σ does not occur in v_2. By proposition 7 $p = r(v_1\sigma v_2,\sigma) = 1 + r(v_1,\sigma v_2)$, i.e. $r(v_1,\sigma v_2) = p - 1$. By corollary 1(a) there exist $a,b \in \Sigma^*$ and $\xi \in \Sigma$ such that $\sigma v_2 = a\xi b$ and $r(v_1a,\xi) = r(v_1,\sigma v_2) = p - 1$. By the induction hypothesis there exists a (p-1)-tuple $\underline{s}$ in v_1a, such that $\underline{t} = (\underline{s},\xi)$ does not occur in v_1a. We claim that $(\underline{t},\sigma)$ does not occur in $u = v_1\sigma v_2$. Suppose it does. Then, since σ does not occur in v_2, $\underline{t}$ occurs in v_1. Hence $\underline{t}$ also occurs in v_1a, a contradiction. □

We have seen that $r(0102011,0) = 2$. Applying the above construction we can get $\underline{t} = (\sigma_4,\sigma_6) = (2,1)$, where $(\underline{t},0) = (2,1,0)$ does not occur in 0102011. Note that this $\underline{t}$ is not unique; in fact any of (σ_4,σ_6), (σ_2,σ_6) and (σ_4,σ_5) can be obtained by the construction.

Now we introduce the dual concept of $r(u,x)$ and that of r-vector.

Definition 5. Let $u \in \Sigma^*$ and $x \in \Sigma^+$. Then $\ell(x,u)$ is the greatest integer m, such that $u \underset{m}{\sim} xu$. Let $x = \sigma_1\sigma_2\ldots\sigma_n$ be in Σ^+, where each $\sigma_i \in \Sigma$. The ℓ-vector of x is $(q_1,q_2,\ldots,q_n)$, where $q_i = \ell(\sigma_i,\sigma_{i+1}\sigma_{i+2}\ldots\sigma_n)$ if $i < n$, and $q_n = \ell(\sigma_n,\lambda)$.

We assume now that the duals of propositions 5, 6, 7 and 8, and those of corollaries 1 and 2 have been proved. Using these we can compute the ℓ-vector of a word, and thus, $\ell(x,u)$ for any x and u. Completing the previous example (4) we have:

i	1	2	3	4	5	6	7	8
σ_i	0	1	0	2	0	1	1	0
p_i	0	0	1	0	1	1	2	2
q_i	2	1	1	0	1	1	0	0

(5)

Thus $\ell(0,1020110) = 2$ and the dual construction of proposition 8 gives $\underline{t} = (\sigma_2,\sigma_4)$, which is unique this time. In fact, $(0,\underline{t}) = (0,1,2)$ does not occur in 1020110.

Now we have the following:

Proposition 9. Let $u,v \in \Sigma^*$ and $\sigma \in \Sigma$. Then $u\sigma v \underset{m}{\sim} uv$ iff $m \leq r(u,\sigma) + \ell(\sigma,v)$.

Proof. Let $p = r(u,\sigma)$ and $q = \ell(\sigma,v)$. Let us suppose that $m \leq p + q$, and prove that $u\sigma v \underset{m}{\sim} uv$. Clearly $U_m(uv) \subseteq U_m(u\sigma v)$. To prove the reverse inclusion, it is sufficient to consider ($< m$)-tuples $\underline{t}$ in $u\sigma v$ of the form $\underline{t} = (\underline{t}_1,\sigma,\underline{t}_2)$, where $\underline{t}_1$ is an m_1-tuple in u, $\underline{t}_2$ is an m_2-tuple in v, and

$$m_1 + m_2 < m. \tag{6}$$

If $m_1 < p$, then $(\underline{t}_1,\sigma)$ occurs in u, since $u \underset{p}{\sim} u\sigma$. Similarly, if $m_2 < q$, then $(\sigma,\underline{t}_2)$ occurs in v. In any case, $\underline{t}$ occurs in uv. If $m_1 \geq p$ and $m_2 \geq q$, then $m_1 + m_2 \geq p + q$; hence, from (6) $m > p + q$, a contradiction. Thus, $\underline{t}$ occurs in uv and $u\sigma v \underset{m}{\sim} uv$. Conversely, suppose that $u\sigma v \underset{m}{\sim} uv$. By proposition 8 there exists a p-tuple $\underline{t}_1$ in u, such that $(\underline{t}_1,\sigma)$ does not occur in u. Dually, there exists a q-tuple $\underline{t}_2$ in v, such that $(\sigma,\underline{t}_2)$ does not occur in v. Thus, $(\underline{t}_1,\sigma,\underline{t}_2)$ is a (p+q+1)-tuple which occurs in $u\sigma v$, but not in uv. Hence $u\sigma v \underset{p+q+1}{\not\sim} uv$. It follows by proposition 3(a) that $m < p + q + 1$, i.e. $m \leq p + q$. □

As an immediate corollary of proposition 9 we have:

Theorem 1. A word x is m-reduced iff for all $u,v \in \Sigma^*$ and $\sigma \in \Sigma$, $x = u\sigma v$ implies $r(u,\sigma) + \ell(\sigma,v) < m$.

Thus, in example (5), $x = 01020110$ is 3-reduced since the maximum of $p_i + q_i$ is 2. For the same reason x is not 2-reduced. However, by using proposition 9, we can obtain a 2-reduced word y such that $x \underset{2}{\sim} y$. In fact, we can delete from x any of σ_1, σ_3, σ_5, σ_6, σ_7 or σ_8 and obtain $y_1 \underset{2}{\sim} x$. Let us delete σ_1, then $y_1 = 1020110$. Note that we have to compute the r and ℓ-vectors of y_1. We have:

i	1	2	3	4	5	6	7
σ_i	1	0	2	0	1	1	0
p_i	0	0	0	1	1	2	2
q_i	1	1	0	1	1	0	0

(7)

Let us delete σ_4, we obtain $y_2 = 102110$ and

i	1	2	3	4	5	6
σ_i	1	0	2	1	1	0
p_i	0	0	0	1	2	1
q_i	1	1	0	1	0	0

(8)

Deleting σ_4 we obtain $y = 10210$, which is 2-reduced (see below) and $x \underset{2}{\sim} y$.

i	1	2	3	4	5
σ_i	1	0	2	1	0
p_i	0	0	0	1	1
q_i	1	1	0	0	0

(9)

Now we formalize this reduction procedure.

Definition 5. Let $x,y \in \Sigma^+$ and $m > 0$. Define $x R_m y$ iff there exist $u,v \in \Sigma^*$ and $\sigma \in \Sigma$, such that $r(u,\sigma) + \ell(\sigma,v) \geq m$, $x = u\sigma v$ and $y = uv$. Let R_m^* be the reflexive and transitive closure of R_m.

We have the following corollary of proposition 9.

Corollary 3. If $x R_m^* y$ then $x \underset{m}{\sim} y$.

We also have:

Theorem 2. Let $m > 0$. For every x in Σ^+ there is an m-reduced y, such that $x R_m^* y$ and $x \underset{m}{\sim} y$.

Proof. If x is m-reduced, we have nothing to prove. Suppose that x is not m-reduced. Then there exist $u,v \in \Sigma^*$ and $\sigma \in \Sigma$, such that $x = u\sigma v$ and $u\sigma v \underset{m}{\sim} uv$. By proposition 9 $r(u,\sigma) + \ell(\sigma,v) \geq m$, hence $u\sigma v R_m uv$. The theorem follows by induction. □

Note that theorem 2 reduces the problem of deciding whether

$x \underset{m}{\sim} y$ to the particular case when x and y are m-reduced. This will be studied in the next section.

Clearly R_m^* is not a symmetric relation, in fact it is a partial order over Σ^*. Thus we make the following:

Definition 6. Let $x,y \in \Sigma^+$ and $m > 0$. Define $x \, E_m \, y$ iff $x \, R_m \, y$ or $y \, R_m \, x$. Let E_m^* be the reflexive and transitive closure of E_m.

It follows from corollary 3 that, if $x \, E_m^* \, y$, then $x \underset{m}{\sim} y$. We will eventually prove the converse of this in section 23.

Finally we prove the following proposition, which will be used in section 3.

Proposition 10. Let $u,v \in \Sigma^+$ and $m > 0$. Then $u \underset{m}{\sim} uv$ iff there exist $u_1,u_2,\ldots,u_m \in \Sigma^+$, such that $u = u_1u_2\ldots u_m$ and

$$\mu_1(u_1) \supseteq \mu_1(u_2) \supseteq \ldots \supseteq \mu_1(u_m) \supseteq \mu_1(v).$$

Proof. We prove the only if part first, by induction on m. For $m = 1$ take $u_1 = u$. Since $u \underset{1}{\sim} uv$; it follows that $\mu_1(u) \supseteq \mu_1(v)$. Suppose the proposition holds for $m \geq 1$ and let u,v be such that $u \underset{m+1}{\sim} uv$. Let $u_{m+1} \in \Sigma^+$ be the longest suffix of u, such that $r(u_0,u_{m+1}) \geq m$, where $u = u_0u_{m+1}$; or λ if no such suffix exists. We claim that $\mu_1(u_{m+1}) \supseteq \mu_1(v)$. Let $\sigma \in \mu_1(v)$, then there exist $v_1,v_2 \in \Sigma^*$, such that $v = v_1\sigma v_2$ and σ does not occur in v_1. By corollary 1(a) $r(uv_1,\sigma) \geq r(u,v)$. Since $u \underset{m+1}{\sim} uv$, $r(u,v) \geq m+1$; hence

$$r(uv_1,\sigma) \geq m + 1. \tag{10}$$

Since $m + 1 > 1$, it follows that σ occurs in u; let $w_1, w_2 \in \Sigma^*$ be such that $u = w_1 \sigma w_2$ and σ does not occur in w_2. By propositions 7 and 5 $r(uv_1,\sigma) = r(w_1\sigma w_2 v_1,\sigma) = 1 + r(w_1,\sigma w_2 v_1) =$

$= 1 + \min[r(w_1,\sigma w_2), r(w_1\sigma w_2,v_1)]$. From (10) $\min[r(w_1,\sigma w_2), r(w_1\sigma w_2,v_1)] \geq m$, hence $r(w_1,\sigma w_2) \geq m$. This implies that u_{m+1} is not λ, and in fact, by the choice of u_{m+1}, $u_{m+1} = w_3\sigma w_2$, for some $w_3 \in \Sigma^*$. Thus $\sigma \in \mu_1(u_{m+1})$, and it follows that $\mu_1(u_{m+1}) \supseteq \mu_1(v)$. Since $r(u_0,u_{m+1}) \geq m$, it follows that $u_0 \underset{m}{\sim} u_0u_{m+1}$ and the proposition follows by applying the induction hypothesis. To see the if part, we proceed, once again, by induction on m. For $m = 1$, $\mu_1(u) \supseteq \mu_1(v)$ implies that $u \underset{1}{\sim} uv$. Suppose the proposition holds for $m \geq 1$, and let $u_1,u_2,\ldots,u_{m+1},v \in \Sigma^+$ be such that $\mu_1(u_1) \supseteq \mu_1(u_2) \supseteq \ldots \supseteq \mu_1(u_m) \supseteq \mu_1(u_{m+1}) \supseteq \mu_1(v)$. Let $u_0 = u_1u_2\ldots u_m$, and let $v_1,v_2 \in \Sigma^*$ and $\sigma \in \Sigma$ be such that $v = v_1\sigma v_2$. Since $\mu_1(u_{m+1}) \supseteq \mu_1(v)$, there exist $w_1,w_2 \in \Sigma^*$ such that $u_{m+1} = w_1\sigma w_2$. Clearly $\mu_1(u_{m+1}) = \mu_1(u_{m+1}v_1)$, hence, by the induction hypothesis $u_0 \underset{m}{\sim} u_0u_{m+1}v_1 = u_0w_1\sigma w_2v_1$. From proposition 4, $u_0 \underset{m}{\sim} u_0w_1$, hence $u_0w_1 \underset{m}{\sim} u_0w_1\sigma w_2v_1$. From proposition 6(a) $u_0u_{m+1}v_1 =$

$= u_0w_1\sigma w_2v_1 \underset{m+1}{\sim} u_0w_1\sigma w_2v_1\sigma = u_0u_{m+1}v_1\sigma$. Hence $r(u_0u_{m+1}v_1,\sigma) \geq m + 1$. Since this holds for any choice of v_1,σ and v_2, it follows by corollary 1(a) that $r(u_0u_{m+1},v) \geq m + 1$; hence $u_0u_{m+1} \underset{m+1}{\sim} u_0u_{m+1}v$. □

22. Equivalence of reduced words.

In this subsection we characterize m-equivalence of m-reduced words. The "conjecture" that if x and y are m-reduced, then $x \overset{\sim}{}_m y$ iff $x = y$ is quickly disproved. In fact, we have seen, in (9), that $z_1 = 10210$ is 2-reduced, and that $w \, R_2^* \, z_1$, where $w = 01020110$. Deleting σ_6 instead of σ_1 in w (see before (7)) we get $x = 0102010$, and $w \, R_2 \, x$. Figure 1 shows the different ways in which x can be reduced. Figure 1 is a portion of the partial

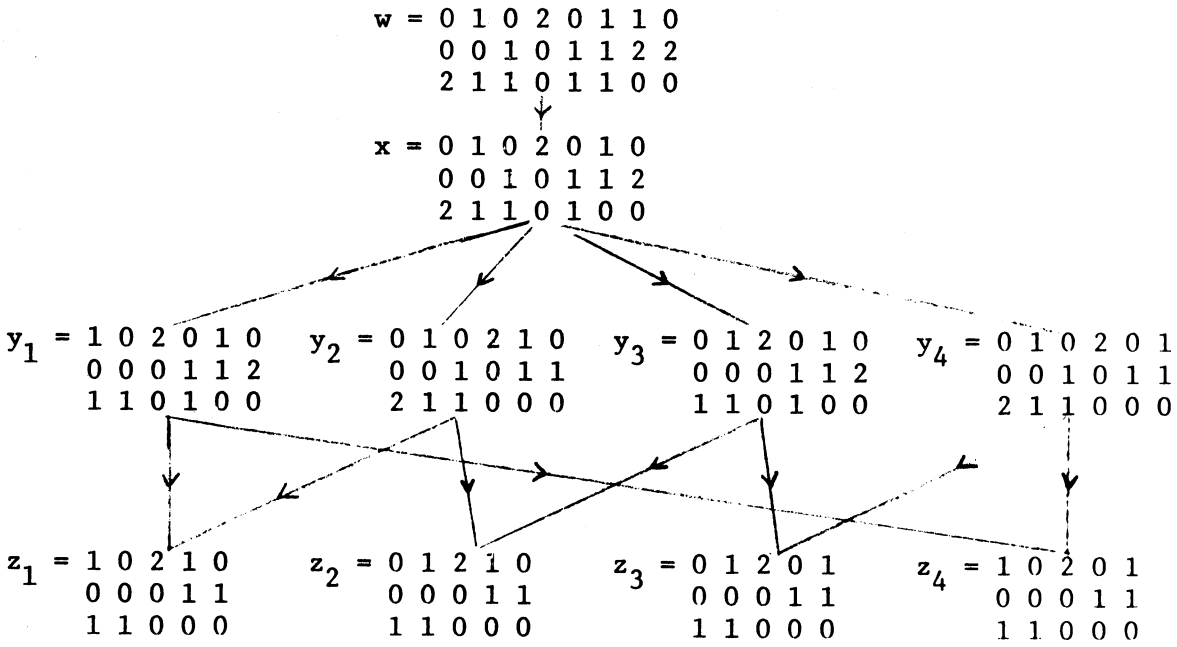


Figure 1 A portion of R_2^*.

order R_2^*. Each word that appears has its r-vector and ℓ-vector in the second and third rows, respectively. An arrow has been drawn from u to v iff $u \, R_2 \, v$. Note that z_1, z_2, z_3 and z_4, are all

2-reduced and by corollary 3 they are pairwise 2-equivalent. Also note that they have the same r-vector and ℓ-vector, and that they can be obtained from each other by commuting (one or more times) two symbols σ_i and σ_{i+1}, whenever $p_i = p_{i+1}$, $q_i = q_{i+1}$ and $p_i + q_i = m - 1 = 1$. In what follows, we will define this restricted commutativity by a relation C_m. Our objective will be to prove that if x and y are m-reduced, then $x \underset{m}{\sim} y$ iff $x\ C_m^*\ y$.

We begin with the following:

Proposition 11. Let $u \in \Sigma^*$, and $\sigma,\xi \in \Sigma$ be such that $r(u,\sigma) = r(u\sigma,\xi)$. Then $\sigma \neq \xi$ and for all $w \in \Sigma^*$, $u\sigma\xi w$ and $u\xi\sigma w$ have the same r-vector.

Proof. Let $p = r(u,\sigma) = r(u\sigma,\xi)$. It follows from proposition 7 that $\sigma \neq \xi$. Now we proceed by induction on $|w|$. If $w = \lambda$, then we only have to prove that $r(u,\xi) = r(u\xi,\sigma) = p$. If $p = 0$ then neither ξ, nor σ occur in u, hence the claim follows. If $p > 0$ then both σ and ξ occur in u. Let $u_1,u_2,u_3,u_4 \in \Sigma^*$ be such that $u = u_1\xi u_2 = u_3\sigma u_4$, ξ does not occur in u_2, and σ does not occur in u_4. Since $\sigma \neq \xi$, we have, from propositions 7 and 5

$$r(u,\xi) = 1 + r(u_1,\xi u_2), \tag{11}$$

$$r(u\sigma,\xi) = 1 + r(u_1,\xi u_2\sigma) =$$

$$= 1 + \min[r(u_1,\xi u_2),\ r(u,\sigma)], \tag{12}$$

$$r(u,\sigma) = 1 + r(u_3,\sigma u_4), \text{ and} \tag{13}$$

$$r(u\xi,\sigma) = 1 + r(u_3,\sigma u_4\xi) =$$

$$= 1 + \min[r(u_3,\sigma u_4),\ r(u,\xi)]. \tag{14}$$

Since $r(u\sigma,\xi) = r(u,\sigma) = p$, it follows from (12) that

$p = 1 + \min[r(u_1,\xi u_2), p]$. Thus $r(u_1,\xi u_2) = p - 1$, and from (11),

$$r(u,\xi) = p. \tag{15}$$

Since $r(u,\sigma) = p$, it follows from (13) that $r(u_3,\sigma u_4) = p - 1$. Substituting this and (15) into (14), it follows that $r(u\xi,\sigma) = p$. This completes the proof for $w = \lambda$. Suppose now, that the proposition holds for $w \in \Sigma^*$, and let $\eta \in \Sigma$. The proof is complete if we show that $r(u\sigma\xi w,\eta) = r(u\xi\sigma w,\eta)$. If η occurs in w, or if η does not occur in $\sigma\xi w$, then the claim clearly follows from the induction hypothesis, proposition 7 and corollary 1(a). The remaining case is when $\eta = \sigma$ or $\eta = \xi$, but η does not occur in w. Suppose that $\eta = \sigma$. By propositions 7 and 5

$$r(u\sigma\xi w,\sigma) = 1 + r(u,\sigma\xi w) = 1 + \min[r(u,\sigma), r(u\sigma,\xi w)] \tag{16}$$

and

$$r(u\xi\sigma w,\sigma) = 1 + r(u\xi,\sigma w). \tag{17}$$

By corollary 1(a), $r(u\sigma,\xi w) \leq r(u\sigma,\xi)$. Since $r(u\sigma,\xi) = r(u,\sigma)$, we have that $r(u\sigma,\xi w) \leq r(u,\sigma)$. Thus, $\min[r(u,\sigma), r(u\sigma,\xi w)] = r(u\sigma,\xi w)$. Then, from (16),

$$r(u\sigma\xi w,\sigma) = 1 + r(u\sigma,\xi w). \tag{18}$$

By the induction hypothesis and corollary 1(a), $r(u\xi,\sigma w) = r(u\sigma,\xi w)$; hence the claim follows from (17) and (18). Finally, if $\eta = \xi$, the claim follows by a similar argument. □

Now we define the relation C_m^*.

Definition 7. Let $x,y \in \Sigma^*$, $m > 0$. Define $x\ C_m\ y$ iff there exist $u,w \in \Sigma^*$ and $\sigma,\xi \in \Sigma$ such that $x = u\sigma\xi w$, $y = u\xi\sigma w$, $r(u,\sigma) = r(u\sigma,\xi) = p$, $\ell(\xi,w) = \ell(\sigma,\xi w) = q$ and $p + q = m - 1$. Let C_m^* be the reflexive and transitive closure of C_m.

Proposition 12. C_m^* is an equivalence relation. If x is m-reduced and $x\ C_m^*\ y$ then y is m-reduced.

Proof. This follows from proposition 11, its dual and by theorem 1. We leave the proof to the reader. □

Proposition 13. If $x\ C_m^*\ y$ then $x\ E_m^*\ y$.

Proof. It is sufficient to consider the case $x\ C_m\ y$. Then there exist $u,w \in \Sigma^*$ and $\sigma,\xi \in \Sigma$, such that $x = u\sigma\xi w$, $y = u\xi\sigma w$, $r(u,\sigma) = r(u\sigma,\xi) = p$, $\ell(\xi,w) = \ell(\sigma,\xi w) = q$ and $p + q = m - 1$. Let $z = u\sigma\xi\sigma w$. By proposition 11 $\sigma \neq \xi$; hence by proposition 7 and its dual $r(u\sigma\xi,\sigma) = p + 1$ and $\ell(\sigma,\xi\sigma w) = q + 1$. Thus $r(u,\sigma) + \ell(\sigma,\xi\sigma w) = p + q + 1 = m$. Then $z\ R_m\ u\xi\sigma w = y$, hence $z\ E_m\ y$. Also $r(u\sigma\xi,\sigma) + \ell(\sigma,w) = p + q + 1 = m$, hence $z\ R_m\ u\sigma\xi w = x$, and $z\ E_m\ x$. Then, since E_m is symmetric, $x\ E_m^*\ y$. □

Corollary 4. If $x\ C_m^*\ y$ then $x \underset{m}{\sim} y$.

Proof. This follows from the proposition above, corollary 3 and the definition of E_m^*. □

To illustrate the development to this point, we represent a portion of the relation C_m^*, in figure 2. The words are from

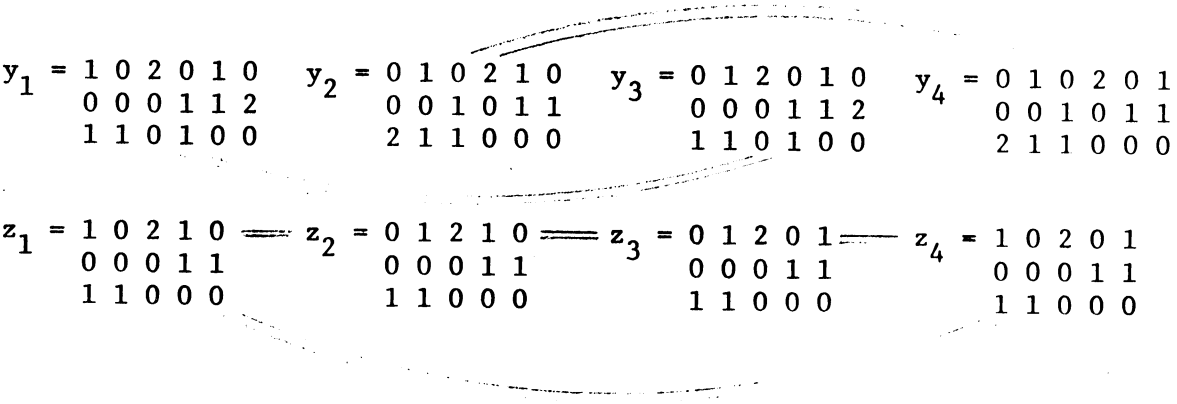


Figure 2 A portion of C_2^*.

figure 1, and we draw a double line between u and v iff $u\ C_m\ v$. Note that one does not need an arrow, since C_m is symmetric.

The converse of corollary 4 clearly does not hold, since C_m^* is a length preserving relation. However, we will be able to prove the partial converse, when x and y are m-reduced. The next three lemmas will be used in that proof.

Lemma 1. Let $x = u\sigma v$ and $y = uw$ for some $u,v,w \in \Sigma^*$ and $\sigma \in \Sigma$. If x and y are m-reduced and $x \underset{m}{\sim} y$, then there exist $v_1,v_2 \in \Sigma^*$ such that

(a) $y = uv_1\sigma v_2$,

(b) $v \underset{m-1-p}{\sim} v_2$ and $u \underset{m-1-q}{\sim} uv_1$, where $p = r(u,\sigma)$ and $q = \ell(\sigma,v)$,

(c) $r(uv_1,\sigma) = r(u,\sigma)$ and $\ell(\sigma,v_2) = \ell(\sigma,v)$.

Proof. Let $p = r(u,\sigma)$ and $q = \ell(\sigma,v)$. Since $x = u\sigma v$ is m-reduced, we have, by theorem 1,

$$p + q \leq m - 1. \tag{20}$$

By proposition 8, there is a p-tuple $\underline{a}$ in u such that $(\underline{a},\sigma)$ does not occur in u. It follows from (20), that $p + 1 \leq m$; hence $(\underline{a},\sigma)$ occurs in y, since $x \underset{m}{\sim} y$. Thus σ occurs in w. Let $v_1,v_2 \in \Sigma^*$ be such that $w = v_1\sigma v_2$, and σ does not occur in v_1. Then $y = uw = uv_1\sigma v_2$, proving (a). Now we claim that

$$v \underset{m-1-p}{\sim} v_2. \tag{21}$$

Let $\underline{t}$ be a ($\leq$ m-1-p)-tuple in v. Then $(\underline{a},\sigma,\underline{t})$ is a ($\leq$ m)-tuple in x. Since $x \underset{m}{\sim} y$, it follows that $(\underline{a},\sigma,\underline{t})$ occurs in y. Since σ does not occur in v_1, it follows that $(\underline{a},\sigma)$ does

not occur in uv_1; hence $\underline{t}$ occurs in v_2. Thus $U_{m-1-p}(v) \subseteq U_{m-1-p}(v_2)$. The reverse inclusion is proved similarly and (21) follows. By the dual of proposition 8, there is a q-tuple $\underline{b}$ in v, such that $(\sigma,\underline{b})$ does not occur in v. From (20) $q \leq m - 1 - p$; hence it follows from (21) that $\underline{b}$ occurs in v_2. Now we claim that

$$u_{m-1-q} \sim uv_1. \tag{22}$$

To prove this, it is sufficient to prove that $U_{m-1-q}(uv_1) \subseteq U_{m-1-q}(u)$. Let $\underline{t}$ be a ($\leq$ m-1-q)-tuple in uv_1. Then $(\underline{t},\sigma,\underline{b})$ is a ($\leq$ m)-tuple in y, since $\underline{b}$ occurs in v_2, and hence it is a ($\leq$ m)-tuple in x. Since $(\sigma,\underline{b})$ does not occur in v, it follows that $\underline{t}$ occurs in u. Hence (22) holds.

Finally, let $p_1 = r(uv_1,\sigma)$ and $q_1 = \ell(\sigma,v_2)$. We now will prove that $p = p_1$ and $q = q_1$. Since y is m-reduced, it follows that

$$p_1 + q_1 \leq m - 1. \tag{23}$$

From (20) $p \leq m - 1 - q$, hence, from (22) $u_p \sim uv_1$. Since $u_p \sim u\sigma$, it follows that $uv_{1\,p} \sim uv_1\sigma$; hence

$$p \leq p_1. \tag{24}$$

From this, $m - 1 - p_1 \leq m - 1 - p$, and from (23), $q_1 \leq m - 1 - p_1$. Thus $q_1 \leq m - 1 - p$, and from (21), $v_{q_1} \sim v_2$. Since $v_{2\,q_1} \sim \sigma v_2$, it follows that $v_{q_1} \sim \sigma v$, hence $q_1 \leq q$. One can show similarly that $q \leq q_1$ and $p_1 \leq p$. Thus $p = p_1$ and $q = q_1$. □

Lemma 2. Let $\sigma,\xi \in \Sigma$ be such that $\sigma \neq \xi$, and let $x = u\sigma z_1$, and $y = u\xi z_2$. If x and y are m-reduced, and $x \underset{m}{\sim} y$, then there exist $v,w \in \Sigma^*$ such that $x = u\sigma v\xi w$, and $r(u,\sigma v\xi) + \ell(\sigma v\xi,w) = m - 1$.

Proof. Let $r(u,\sigma) = p_1$, $r(u,\xi) = p_2$, $\ell(\sigma,z_1) = q_1$ and $\ell(\xi,z_2) = q_2$. By lemma 1 and the fact that $\sigma \neq \xi$, there exist $v,w \in \Sigma^*$ such that $x = u\sigma v\xi w$, and

$$r(u\sigma v,\xi) = r(u,\xi) = p_2, \tag{25}$$

$$\ell(\xi,w) = \ell(\xi,z_2) = q_2, \tag{26}$$

$$u \underset{m-1-q_2}{\sim} u\sigma v, \tag{27}$$

and

$$w \underset{m-1-p_2}{\sim} z_2. \tag{28}$$

Applying lemma 1 again, there exist $v_1,w_1 \in \Sigma^*$ such that $y = u\xi v_1\sigma w_1$, and

$$r(u\xi v_1,\sigma) = r(u,\sigma) = p_1, \tag{29}$$

$$\ell(\sigma,w_1) = \ell(\sigma,z_1) = q_1, \tag{30}$$

$$u \underset{m-1-q_1}{\sim} u\xi v_1, \tag{31}$$

and

$$w_1 \underset{m-1-p_1}{\sim} z_1. \tag{32}$$

Clearly $z_1 = v\xi w$ and $z_2 = v_1\sigma w_1$, thus (26), (28), (30) and (32) become

$$\ell(\xi,w) = \ell(\xi,v_1\sigma w_1) = q_2, \tag{26'}$$

$$w \underset{m-1-p_2}{\sim} v_1\sigma w_1, \tag{28'}$$

$$\ell(\sigma,w_1) = \ell(\sigma,v\xi w) = q_1, \tag{30'}$$

and

$$w_1 \underset{m-1-p_1}{\sim} v\xi w. \tag{32'}$$

We represent the situation in figure 3. The cross in the middle means to suggest the equivalences (27), (28'), (31) and (32').

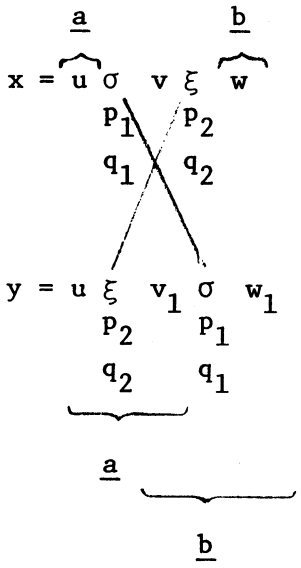


Figure 3.

Since x is m-reduced, we have from theorem 1

$$p_1 + q_1 \leq m - 1, \tag{33}$$

and

$$p_2 + q_2 \leq m - 1. \tag{34}$$

Now we claim that

$$m - 1 \leq p_1 + q_2. \tag{35}$$

In fact, by proposition 8, there exist p_1 and q_2-tuples $\underline{a}$ and $\underline{b}$, in $u\xi v_1$ and $v_1\sigma w_1$, such that $(\underline{a},\sigma)$ and $(\xi,\underline{b})$ do not occur in $u\xi v_1$ and $v_1\sigma w_1$, respectively. (See figure 3.) From (33)

$p_1 \leq m - 1 - q_1$; hence, from (31), $u \underset{p_1}{\sim} u\xi v_1$. Thus $\underline{a}$ occurs in u. Similarly, from (34) and (28'), $\underline{b}$ occurs in w. Thus, the $(p_1 + q_2 + 2)$-tuple $\underline{t} = (\underline{a},\sigma,\xi,\underline{b})$ occurs in x, but it clearly does not occur in y. Hence, $x \not\underset{p_1+q_2+2}{\sim} y$, and $m < p_1 + q_2 + 2$. Now (35) follows. Similarly,

$$m - 1 \leq p_2 + q_1. \tag{36}$$

From (33) and (35), $q_1 \leq m - 1 - p_1 \leq q_2$. From (34) and (36) $q_2 \leq m - 1 - p_2 \leq q_1$. Thus $q_1 = q_2$. Similarly $p_1 = p_2$; then from (33) and (35),

$$p_1 + q_1 = m - 1. \tag{37}$$

Finally, let $p = r(u,\sigma v\xi)$. Then $u \underset{p}{\sim} u\sigma v\xi$, and by corollary 1 $p \leq p_1$. From (37) and (31), $u \underset{p_1}{\sim} u\xi v_1$, and from (37) and (27), since $q_1 = q_2$, $u \underset{p_1}{\sim} u\sigma v$. It follows that $u \underset{p_1}{\sim} u\sigma v\xi v_1$, and from proposition 4, $u \underset{p_1}{\sim} u\sigma v\xi$. Hence $p_1 \leq p$. Thus $p_1 = p$. Similarly $q_1 = \ell(\sigma v\xi,w)$ and the proposition follows from (37). □

Lemma 3. Let $u,v,w \in \Sigma^*$ and $\xi \in \Sigma$ be such that $uv\xi w$ is m-reduced, and $r(u,v\xi) + \ell(v\xi,w) = m - 1$. Then $uv\xi w \; C^*_m \; u\xi vw$.

Proof. Let $p = r(u,v\xi)$ and $q = \ell(v\xi,w)$. We will first show that for all $z_1,z_2 \in \Sigma^*$ and $\eta \in \Sigma$, $z_1\eta z_2 = v\xi$ implies

$$r(uz_1,\eta) = p \quad \text{and} \quad \ell(\eta,z_2w) = q. \tag{38}$$

In fact, from corollary 1(a), and its dual, we have:

$$r(uz_1,\eta) \geq p \quad \text{and} \quad \ell(\eta,z_2w) \geq q. \tag{39}$$

From theorem 1, since $uv\xi w$ is m-reduced,

$$r(uz_1,\eta) + \ell(\eta,z_2w) < m. \tag{40}$$

Since $p + q = m - 1$, it follows, from (39) and (40), that

$r(uz_1,\eta) \leq m - 1 - \ell(\eta,z_2w) \leq p + q - \ell(\eta,z_2w) \leq p + q - q = p.$

Thus, from (39), $r(uz_1,\eta) = p$. Similarly $\ell(\eta,z_2w) = q$.

Now we prove the lemma by induction on $|v|$. For $v = \lambda$ we have nothing to prove, so let us suppose $v = v_1\sigma$, for some $\sigma \in \Sigma$. By (38), $r(uv_1,\sigma) = r(uv_1\sigma,\xi) = p$ and $\ell(\xi,w) = \ell(\sigma,\xi w) = q$.

Since $p + q = m - 1$, it follows that $x = uv_1\sigma\xi w \; C_m \; uv_1\xi\sigma w = y$.

From proposition 11 and its dual, x and y have the same r-vectors and ℓ-vectors. Thus y is m-reduced and, from (38), $r(u,v_1\xi) + \ell(v_1\xi,\sigma w) = m - 1$. By the induction hypothesis $uv_1\xi\sigma w \; C_m^* \; u\xi v_1\sigma w$. Hence $uv_1\sigma\xi w \; C_m^* \; u\xi v_1\sigma w$. □

Now we prove the main result of this subsection.

Theorem 3. Let x,y be m-reduced. Then $x \underset{m}{\sim} y$ iff $x \; C_m^* \; y$.

Proof. The if part holds by corollary 4. To prove the only if part, let u be the longest common prefix of x and y, and let $x_1,y_1 \in \Sigma^*$ be such that $x = ux_1$ and $y = uy_1$. We proceed by induction on $|x_1y_1|$. If $|x_1y_1| = 0$ then $x = y = u$ and $x \; C_m^* \; y$. Consider then the case when $|x_1y_1| > 0$. It follows from lemma 1, that $|x_1| = 0$ iff $|y_1| = 0$, hence $x_1,y_1 \in \Sigma^+$. By the choice of u, there exist $\sigma,\xi \in \Sigma$ and $z_1,z_2 \in \Sigma^*$, such that $\sigma \neq \xi$,

$x = u\sigma z_1$ and $y = u\xi z_2$. By lemma 2, there exist $v,w \in \Sigma^*$, such that $x = u\sigma v\xi w$ and $r(u,\sigma v\xi) + \ell(\sigma v\xi,w) = m - 1$. By lemma 3 $x = u\sigma v\xi w \; C_m^* \; u\xi\sigma vw = z$. By corollary 4 $x \sim_m z$; hence $z \sim_m y$. By proposition 12 z is m-reduced. Since, z and y have a common prefix longer than u, it follows, by the induction hypothesis, that $z \; C_m^* \; y$. Hence $x \; C_m^* \; y$. □

As a byproduct of the development to this point, we show how to obtain the "efficient" algorithm, mentioned earlier, to decide whether $x_1 \sim_m y_1$. First we apply the reduction procedure, described in section 21, to x_1 and y_1. Thus we obtain two reduced words, say x and y, such that $x_1 \sim_m y_1$ iff $x \sim_m y$. To decide the latter problem, one has to carry out the construction described in the proof of the only if part of theorem 3. If the construction succeeds then $x \; C_m^* \; y$, hence $x \sim_m y$. If it fails, $x \not\sim_m y$. We illustrate this by an example. Let $x = 10210$, $y = 01201$ and $m = 2$. The longest common prefix u is λ, hence $\sigma = 1$, $\xi = 0$, $z_1 = 0210$ and $z_2 = 1201$. To find v and w, we have to go back to lemma 2, and from there to lemma 1. By that proof, if $x \sim_m y$ then ξ occurs in x. This is the case and thus $v = \lambda$ and $w = 210$. Now $x = u\sigma v\xi w$. Lemma 2 says that if $x \sim_m y$, then $r(u,\sigma v\xi) + \ell(\sigma v\xi,w) = m - 1$. This clearly holds. Then by lemma 3, $x = u\sigma v\xi w \; C_m^* \; u\xi\sigma vw = z$. The construction in lemma 3 reduces in this case to $x = 10210 \; C_2 \; 01210 = z$. Now we apply the construction of theorem 3 to z and y, which longest common prefix is $u = 012$. We will have $z = 01210 \; C_2 \; 01201 = y$. Hence, $x \sim_2 y$. If any of the above steps would fail, we could conclude that $x \not\sim_m y$. In fact, the proofs of lemmas 1 and 2 would exhibit the $(\cdot\, m)$-tuple in x which does not occur in y, or vice-versa.

Finally, we have the following corollary of theorem 3.

Corollary 5. If x and y are m-reduced, then $x \overset{\sim}{}_{m+1} y$ iff $x = y$.

Proof. By theorem 1, x and y are also (m+1)-reduced. Hence, by theorem 3, $x \overset{\sim}{}_{m+1} y$ iff $x\ C^*_{m+1}\ y$. Since x and y are m-reduced $x\ C^*_{m+1}\ y$ iff $x = y$, by theorem 1 and the definition of C^*_{m+1}. □

23. Characterization.

Here we combine the results of the last two subsections, to get the main theorem of section 2.

Theorem 4. Let $x,y \in \Sigma^*$, $m > 0$. The following are equivalent:

(a) $x \overset{\sim}{}_m y$.

(b) There exist $x_1,y_1 \in \Sigma^*$, such that $x\ R^*_m\ x_1$, $y\ R^*_m\ y_1$, and $x_1\ C^*_m\ y_1$.

(c) $x\ E^*_m\ y$.

Proof. (a) implies (b) by theorems 2 and 3.

(b) implies (c) by proposition 13.

(c) implies (a) by corollary 3 and the definition of E^*_m. □

3. $\mathcal{J}$-trivial semigroups.

In this section we study semigroups in which the Green equivalence relations are trivial. Our main interest is in finite $\mathcal{J}$-trivial semigroups; however, at the end of the section we make some comments about infinite semigroups.

Recall that, given a semigroup S, $S^1 = S$ if S has an identity, and $S^1 = S \cup \Lambda$ otherwise, where Λ is an identity for S^1 and multiplication in S is unchanged. We have:

Definition 9. Let S be a semigroup and let $a,b \in S$. The Green equivalence relations are:

(a) $a \mathcal{R} b$ iff $aS^1 = bS^1$

(b) $a \mathcal{L} b$ iff $S^1a = S^1b$,

(c) $a \mathcal{J} b$ iff $S^1aS^1 = S^1bS^1$,

(d) $a \mathcal{H} b$ iff $a \mathcal{L} b$ and $a \mathcal{R} b$,

(e) $a \mathcal{D} b$ iff $a \mathcal{R} c$ and $c \mathcal{L} b$ for some $c \in S$.

It is well known (e.g. see Clifford and Preston's book [CP]) that $\mathcal{H} \subseteq \mathcal{L} \subseteq \mathcal{D} \subseteq \mathcal{J}$ and $\mathcal{H} \subseteq \mathcal{R} \subseteq \mathcal{D}$. We represent these inclusions in figure 4.

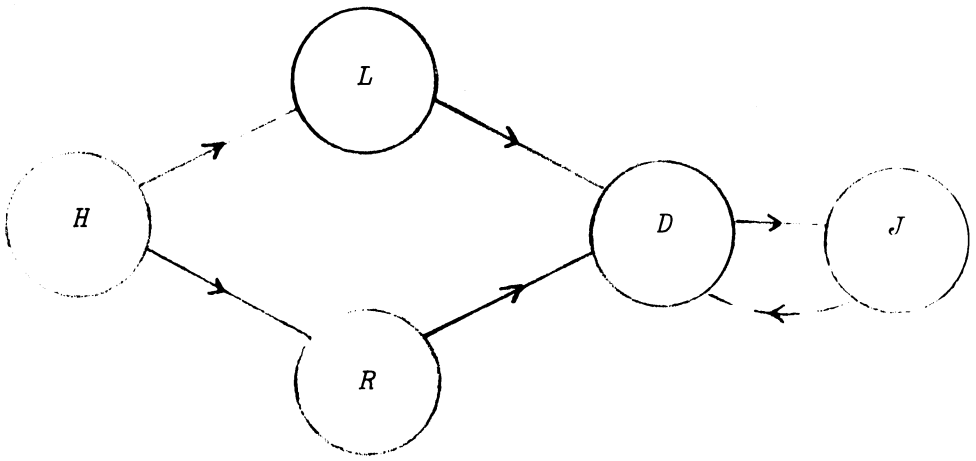


Figure 4 Inclusion among the Green relations.

Furthermore, for finite semigroups $\mathcal{J} \subseteq \mathcal{D}$ also holds (see Rhodes and Tilson [RT] Fact 1.15), hence in this case $\mathcal{J} = \mathcal{D}$.

Now we have:

Definition 10. Let ρ be any of $\mathcal{R}$, $\mathcal{L}$, $\mathcal{J}$, $\mathcal{H}$ or $\mathcal{D}$. A ρ-class is an equivalence class mod ρ. A semigroup S is ρ-trivial iff every ρ-class of S is trivial, i.e. for $a,b \in S$, $a \rho b$ implies $a = b$.

From the above mentioned inclusions it follows that, for instance, a $\mathcal{J}$-trivial semigroup is also $\mathcal{D}$, $\mathcal{L}$, $\mathcal{R}$ and $\mathcal{H}$-trivial. It is well known that every subgroup of S is contained in an $\mathcal{H}$-class of S. Thus, it follows that, if S is $\mathcal{H}$-trivial, then S is group-free. (The converse is true for finite semigroups, see [RT] Fact 2.32). Thus, for $\rho = \mathcal{R}$, $\mathcal{L}$ and $\mathcal{J}$, if S is ρ-trivial, then it is group-free.

We extend the duality introduced in section 34 to semigroups, by replacing every semigroup product ab by ba. Thus, $\mathcal{L}$ and $\mathcal{R}$ are duals, while $\mathcal{J}$, $\mathcal{H}$ and $\mathcal{D}$ are self-dual concepts.

Before proceeding, we need the following notation.

Notation. Let S be a semigroup. S^+ (S^*) denotes the free semigroup (monoid) generated by the set S. In order to avoid confusion, we denote by $\circ$ the concatenation in S^+. If $u \in S^+$, say $u = a_1 \circ a_2 \circ \ldots \circ a_k$, for $a_i \in S$, then $\P u$ denotes the semigroup element $a_1 a_2 \ldots a_k$.

Now we have the following two theorems.

Theorem 5. Let S be a finite semigroup. The following are equivalent.

(a) S is $\mathcal{R}$-trivial.

(b) For all $a,b,c \in S$, $abc = a$ implies $ab = a$.

(c) There exists an integer $m > 0$, such that for all $u,v \in S^+$, $u \underset{m}{\sim} u\circ v$ implies $\P(u\circ v) = \P u$.

(d) There exists an integer $m > 0$, such that for all $a,b \in S$, $(ab)^m = (ab)^m a$.

Proof. (a) implies (b). If $abc = a$, then clearly $a \mathrel{R} ab$. Since S is R-trivial, $a = ab$.

(b) implies (c). Let $m = \#S + 1$. By proposition 10, $u \underset{m}{\sim} uv$ implies that there exist $u_1,u_2,\ldots,u_m \in S^+$, such that $u = u_1u_2\ldots u_m$, and

$$\mu_1(u_1) \supseteq \mu_1(u_2) \supseteq \ldots \supseteq \mu_1(u_m) \supseteq \mu_1(v). \tag{41}$$

Let $a_i \in S$ be such that $a_i = \P(u_1\circ u_2\circ\ldots\circ u_i)$, for $i = 1,2,\ldots,m$. By the choice of m, there exist j and k, $1 \le j < k \le m$, such that $a_j = a_k$. It is easy to see that, from (b), it follows that

$$\text{for all } b \in \mu_1(u_{j+1}),\ a_j = a_jb. \tag{42}$$

On the other hand (41) implies that

$$\mu_1(u_{j+1}) = \mu_1(u_{j+1}\circ\ldots\circ u_m) = \mu_1(u_{j+1}\circ\ldots\circ u_m\circ v).$$

Then, from (42),

$$a_j = a_j(\P(u_{j+1}\circ\ldots\circ u_m)) = a_j(\P(u_{j+1}\circ\ldots\circ u_m\circ v)).$$

Since $a_j = \P(u_1\circ\ldots\circ u_j)$, we have that $a_j = \P u = \P(u\circ v)$.

(c) implies (d). Let $u = (a\circ b)^m$ and $v = a$. By proposition 3(d) $u \underset{m}{\sim} u\circ v$. Then, by (c), $\P u = \P(u\circ v)$. Since $\P u = (ab)^m$ and $\P(u\circ v) = (ab)^m a$, the implication follows.

(d) implies (a). Let $a,b \in S$ be such that $a \mathrel{R} b$. Then, for some $c,d \in S^1$, $ac = b$ and $bd = a$. If either c or d is the identity in S^1, then $a = b$, otherwise $c,d \in S$. Now, we have that $acd = a$

and hence $a(cd)^m = a$. By (d), $(cd)^m = (cd)^m c$; hence $a(cd)^m c = a$. Also $a(cd)^m c = ac$; thus $a = ac = b$. □

Theorem 6. Let S be a finite semigroup. The following are equivalent:

(a) There exists an integer $m > 0$, such that for all $x,y \in S^+$, $x \, R_m \, y$ implies $\P x = \P y$.

(b) There exists an integer $m > 0$, such that for all $x,y \in S^+$, $x \underset{m}{\sim} y$ implies $\P x = \P y$.

(c) There exists an integer $m > 0$, such that for all $a,b \in S$, $(ab)^m = (ab)^m a = b(ab)^m$.

(d) There exists an integer $m > 0$, such that for all $a,b \in S$, $a^m = a^{m+1}$ and $(ab)^m = (ba)^m$.

(e) S is J-trivial.

(f) S is R-trivial and L-trivial.

Proof. For reasons which will become apparent later, we prove the theorem by establishing the following implications: (a) iff (b), (b) implies (c), (c) iff (d), (c) implies (e), (e) implies (f), and (f) implies (a). Note that all proofs, but the last one, are valid for arbitrary semigroups, i.e. finite or infinite.

(a) implies (b). Let $x,y \in S^+$ be such that $x \underset{m}{\sim} y$. By theorem 4(c), $x \, E_m^* \, y$. Since $u \, E_m \, v$ iff either $u \, R_m \, v$ or $v \, R_m \, u$, it follows from (a) that $\P u = \P v$. By induction, $\P x = \P y$.

(b) implies (a). Let $x,y \in S^+$ be such that $x \, R_m \, y$. By corollary 3 $x \underset{m}{\sim} y$, hence $\P u = \P v$ by (b).

(b) implies (c). Let $a,b \in S$. By proposition 3(d) and its dual, $(a\circ b)^m \underset{m}{\sim} (a\circ b)^m \circ a \underset{m}{\sim} b\circ(a\circ b)^m$. Hence, by (b), $(ab)^m = (ab)^m a = b(ab)^m$.

(c) implies (d). Let $p = 2m$. Taking $a = b$ in (c), we have $a^p = a^{p+1}$. Now, using (c) in the second and fourth equalities, $(ab)^p = (ab)^m(ab)^m = =(ab)^m(ab)^m a = a(ba)^m(ba)^m = (ba)^m(ba)^m = (ba)^p$. Hence p is the desired integer.

(d) implies (c). Let $a,b \in S$. Then $(ab)^m = (ba)^m = (ba)^{m+1} = = b(ab)^m a$; i.e. $(ab)^m = b(ab)^m a$. It follows that $(ab)^m = b^m(ab)^m a^m$. Thus, since $a^m = a^{m+1}$, $(ab)^m = (ab)^m a$. Similarly, $(ab)^m = b(ab)^m$.

(c) implies (e). Let $x,y \in S$ be such that $x \mathcal{J} y$. Then there exist $a,b,c,d \in S^1$, such that $ayd = x$ and $bxc = y$. It follows that $abxcd = x$. We now claim that $x = bx$. Let Λ be the identity in S^1. If $b = \Lambda$, we have nothing to prove; otherwise $b \in S$. If $a = \Lambda$, then $bxcd = x$. It follows that $b^{2m}x(cd)^{2m} = x$. By (c) $b^{2m} = b^{2m+1}$, hence $bx = x$. The remaining case is when $a,b \in S$. Then $(ab)^m x(cd)^m = x$. By (c) $(ab)^m = b(ab)^m$, hence $x = bx$. Similarly $x = xc$. Since $y = bxc$, it follows that $y = x$. Hence S is $\mathcal{J}$-trivial.

(e) implies (f). This follows from $L \subseteq J$ and $R \subseteq J$.

(f) implies (a). Since S is R-trivial, by theorem 5(c), there exists an integer $m_1 > 0$, such that for all $u,v \in S^+$, $u \sim_{m_1} u\circ v$ implies $\P(u\circ v) = \P u$. Since $u \sim_{m_1} u\circ v$ iff $r(u,v) \geq m_1$, it follows that, for all $u,v \in S^+$, $r(u,v) \geq m_1$ implies that $\P(u\circ v) = \P u$. By a dual argument, since S is L-trivial, there exists an integer $m_2 > 0$, such that for all $u,v \in S^+$, $\ell(v,u) \geq m_2$ implies $\P(v\circ u) = \P u$. Let $m = m_1 + m_2$. If $x R_m y$, then there exist $u,v \in S^*$ and $\sigma \in S$,

such that $x = u\circ\sigma\circ v$, $y = u\circ v$ and $r(u,\sigma) + \ell(\sigma,v) \geq m$. If $r(u,\sigma) \geq m_1$, then, since $m_1 > 0$, it follows that $u \in S^+$. Thus $\P(u\circ\sigma) = \P u$. Similarly, if $\ell(\sigma,v) \geq m_2$, then $\P(\sigma\circ v) = \P v$. In both cases it follows that $\P x = \P y$. The remaining case is when $r(u,\sigma) < m_1$ and $\ell(\sigma,v) < m_2$. But then $r(u,\sigma) + \ell(\sigma,v) < m_1 + m_2 = m$, a contradiction. □

It is interesting to verify what happens with theorem 6 for semigroups in general, i.e. finite or infinite. Let $\mathcal{S}_F$ denote the family of finite semigroups satisfying the properties in theorem 6. Let $\mathcal{S}_a,\mathcal{S}_b,\ldots,\mathcal{S}_f$ denote the families of semigroups (finite or infinite) satisfying properties a,b,...,f respectively. As noted in the proof of theorem 6, all implications, but the last one, are also valid for infinite semigroups. Hence

$$\mathcal{S}_F \subseteq \mathcal{S}_a = \mathcal{S}_b \subseteq \mathcal{S}_c = \mathcal{S}_d \subseteq \mathcal{S}_e \subseteq \mathcal{S}_f.$$

We will show that every inclusion in the above chain is a proper one.

Let $A = \{a_i \mid i = 1,2,\ldots\}$ and let S_1 be the family of finite subsets of A. Define the following multiplication in S_1: for $x,y \in S_1$ $xy = (x \cup y)$. Clearly we have an infinite semigroup which is idempotent and commutative. It follows that $S_1 \in \mathcal{S}_b$ (for m = 1). Hence $\mathcal{S}_F \subsetneq \mathcal{S}_b$.

Let $\Sigma = \{0,1,2\}$, and let S_2 be the semigroup generated by Σ, subject to the generating relations: for all $a,b \in S_2$ $a^2 = a^3$ and $(ab)^2 = (ba)^2$. Clearly $S_2 \in \mathcal{S}_d$, for m = 2. Since the set of words in Σ^* which are not of the form uv^2w is infinite (see for

instance [BCG]), it follows that S_2 is infinite. On the other hand S_2 is finitely generated by Σ. Since $\underset{m}{\sim}$ is of finite index for any m over a finite alphabet Σ, it follows that $S_2 \notin \mathcal{S}_b$. Hence $\mathcal{S}_b \subsetneq \mathcal{S}_d$.

Let S_3 be Σ^+ for $\Sigma = \{0\}$. Clearly S_3 is $\mathcal{J}$-trivial, but $S_3 \notin \mathcal{S}_d$. Hence $\mathcal{S}_d \subsetneq \mathcal{S}_e$.

Let $A = \{a_i \mid i = 1,2,\ldots\}$, $B = \{b_i \mid i = 1,2,\ldots\}$ and $C = \{c_i \mid i = 0,\pm1,\pm2,\ldots\}$. Let $S_4 = A \cup B \cup C \cup \{0\}$. Multiplication in S_4 is defined by $x0 = 0x = 0$ for all $x \in S_4$, and the following table (e.g. $a_i b_j = c_{i-j}$):

	a_j	b_j	c_j
a_i	a_{i+j}	c_{i-j}	c_{i+j}
b_i	0	b_{i+j}	0
c_i	0	c_{i-j}	0

It is tedious but straightforward to verify associativity. Perhaps the easiest way is to verify that S_4 is isomorphic to the syntactic semigroup of $\{a_1^n b_1^n \mid n = 1,2,\ldots\}$. We leave the proof to the reader. One can also verify that if $n = 0,1,2,\ldots$, then

$$a_i S_4^1 = \{a_{i+n}\} \cup C \cup \{0\}$$

$$b_i S_4^1 = \{b_{i+n}\} \cup \{0\}$$

$$c_i S_4^1 = \{c_{i-n}\} \cup \{0\}$$

$$S_4^1 a_j = \{a_{j+n}\} \cup \{0\}$$

$$S_4^1 b_j = \{b_{j+n}\} \cup C \cup \{0\}$$

$$S_4^1 c_j = \{c_{j+n}\} \cup \{0\}.$$

It follows now, that S_4 is R-trivial and L-trivial. On the other hand

$$S_4^1 c_i S_4^1 = C \cup \{0\}.$$

Hence, for all $u,v \in C$ $u \mathcal{J} v$, and S_4 is not J-trivial. Thus $S_e \subsetneq S_f$.

4. Characterization of γ_1.

In this section we prove the main theorem of the chapter. To do this, we need the following:

Definition 11. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton. A is partially ordered if for all $q \in Q$ and for all $x,y \in \Sigma^*$, $q(xy)^A = q$ implies $qx^A = q$.

Partially ordered semiautomata have been studied by Meyer and Thompson [MT], Stiffler [S3] and Zalcstein [Z2]. They prove that A is partially ordered iff it can be covered by a cascade of semi-resets

We leave the proof of the following proposition to the reader:

Proposition 14. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton. The following are equivalent:

(a) A is partially ordered.

(b) The relation $\rightarrow$ is a partial order on Q, where $p \rightarrow q$ iff $px^A = q$ for some $x \in \Sigma^*$.

(c) S_A is R-trivial.

Now we have:

Theorem 7. Let $\hat{A} = (Q,\Sigma,M,q_0,F)$ and $\hat{B} = (R,\Sigma,N,r_0,G)$ be reduced automata, accepting the events E and E^T respectively. The following are equivalent:

(a) E is (-,1)-testable, i.e. $E \in \gamma_1$.

(b) A and B are partially ordered semiautomata.

(c) A is a partially ordered semiautomaton, such that for all $q \in Q$, and for all $x,y \in \Sigma^*$, $qx^A = q(xx)^A = q(xy)^A$ and $qy^A = q(yy)^A = q(yx)^A$ imply $qx^A = qy^A$.

(d) S_A is J-trivial.

Proof. (a) implies (b). Let $m \geq 0$ be such that E is $(m,1)$-testable. Suppose that A is not partially ordered, i.e. there exist $q \in Q$, and $x,y \in \Sigma^*$ such that $px^A = q$, $qy^A = p$ and $p \neq q$. Let $u = (xy)^m$ and $v = (xy)^m x$. By proposition 3(d) $u \underset{m}{\sim} v$. Since $\hat{A}$ is reduced and accepts an $(m,1)$-testable event, it follows, by proposition 1.1, that $u^A = v^A$. Hence $p = pu^A = pv^A = q$, a contradiction; thus A is partially ordered. By proposition 3.3 it follows that E^T is also $(m,1)$-testable. Hence, by the previous argument, B is partially ordered.

(b) implies (c). The semiautomaton A is partially ordered by hypothesis; hence we only have to prove the second part of (c). Now, B is partially ordered and this clearly implies that B is permutation-free. By lemma 1.1, for all $x \in \Sigma^*$,

$$(x^n)^B = (x^{n+1})^B, \tag{43}$$

where $n = \#R$. Suppose then, that for some $q \in Q$, and for some $x,y \in \Sigma^*$ the condition in (c) does not hold; i.e. we have $qx^A = q(xx)^A = q(xy)^A$, $qy^A = q(yy)^A = q(yx)^A$ and $qx^A \neq qy^A$. Since $\hat{A}$ is reduced, there exist $u,v \in \Sigma^*$, such that $q_0 u^A = q$ and $q(xv)^A \in F$ iff $q(yv)^A \notin F$. It follows that $u(xy)^n v \in E$ iff $u(yx)^n yv \notin E$. Hence $z_1 = v^T(y^T x^T)^n u^T \in E^T$ iff $z_2 = v^T y^T (x^T y^T)^n u^T \notin E^T$. Let $r_0(v^T(y^T x^T)^n)^B = r \in R$. It follows from (43) that $r(y^T x^T)^B = r$. Since B is partially ordered, $r(y^T)^B = r$. Then $r_0 z_1^B = r_0 z_2^B$, and $z_1 \in E^T$ iff $z_2 \in E^T$, a contradiction. Hence (c) holds.

(c) implies (d). Since A is partially ordered, it follows that A is permutation-free. Thus, by lemma 1.1, for all $x \in \Sigma^*$,

$$(x^n)^A = (x^{n+1})^A, \tag{44}$$

where $n = \#Q$. Let $u,v \in \Sigma^*$. Then, by (44) $((uv)^n)^A = ((uv)^{n+1})^A$. Since A is partially ordered, it follows that $((uv)^n)^A = ((uv)^n u)^A$. Thus, also $((uv)^n)^A = ((uv)^n v)^A$. It follows that

$$((uv)^n)^A = ((uv)^n(uv)^n)^A = ((uv)^n(vu)^n)^A. \tag{45}$$

Interchanging u and v, we have

$$((vu)^n)^A = ((vu)^n(vu)^n)^A = ((vu)^n(uv)^n)^A. \tag{46}$$

Taking $x = (uv)^n$ and $y = (vu)^n$, (45), (46) and (c) imply that $((uv)^n)^A = ((vu)^n)^A$. Hence, by theorem 6(d), S_A is J-trivial.

(d) implies (a). By theorem 6(b), there exists an integer $m > 0$, such that for all $u,v \in S_A^+$, $u \overset{m}{\sim} v$ implies $\P u = \P v$. Let $x = \sigma_1\sigma_2\ldots\sigma_k$ and $y = \xi_1\xi_2\ldots\xi_\ell$, for $\sigma_i,\xi_i \in \Sigma$, be such that $x \overset{m}{\sim} y$. Let $u = \sigma_1^A \circ \sigma_2^A \circ \ldots \circ \sigma_k^A$, $v = \xi_1^A \circ \xi_2^A \circ \ldots \circ \xi_\ell^A$. Clearly $u \overset{m}{\sim} v$. Since $\P u = x^A$ and $\P v = y^A$, it follows that $x^A = y^A$. Thus $x \in E$ iff $y \in E$, and E is $(m,1)$-testable. □

It might be helpful at this point, to review the proof of (d) implies (a) in the last theorem. Our hypothesis is that $\hat{A}$ is a reduced automaton, accepting the event E, such that S_A is J-trivial. We want to prove that E is $(m,1)$-testable for some m. In view of proposition 1.1, this is equivalent to proving that there exists an integer m, such that for all $x,y \in \Sigma^*$

$$x \overset{m}{\sim} y \text{ implies } x^A = y^A. \tag{47}$$

Let $m = 2(\#S_A + 1)$. According to theorem 4, if $x \overset{m}{\sim} y$ then there exist $z_1,z_2,\ldots,z_n \in \Sigma^*$ such that $z_1 = x$, $z_n = y$ and for all i, $1 \leq i < n$, $z_i \; E_m \; z_{i+1}$, that is to say, either $z_i \; R_m \; z_{i+1}$ or

$z_{i+1}\ R_m\ z_i$. We obtained the sequence of z_i's by m-reducing x and y to x_r and y_r respectively (section 21), and then commuting appropriate letters of x_r until we obtain y_r (section 22). We also showed (proposition 13), that the commuting of two letters can be obtained by using the relation R_m twice. Thus, in order to establish (47), it is sufficient to prove that for all $x,y \in \Sigma^*$

$$x\ R_m\ y \text{ implies } x^A = y^A. \tag{48}$$

Now, by definition of R_m, if $x\ R_m\ y$ then there exist u,v and σ, such that $x = u\sigma v$, $y = uv$ and $r(u,\sigma) + \ell(\sigma,v) \geq m = 2(\#S_A + 1)$. The latter inequality implies that either $r(u,\sigma) \geq \#S_A + 1$ or $\ell(\sigma,v) \geq \#S_A + 1$. On the other hand, if S_A is J-trivial, then it is also R-trivial and L-trivial. Thus, if $r(u,\sigma) \geq \#S_A + 1$, then $u\ {}^{\#S_A+1}\!\sim u\sigma$ and since S_A is R-trivial, it follows (via proposition 10) that $u^A = (u\sigma)^A$ (theorem 5). Thus, $x^A = (u\sigma v)^A = (uv)^A = y^A$. The other case follows by duality. This completes the proof of (48) and hence (d) implies (a) is established.

The proof above is long and complicated, but our attempts to simplify it have failed. It is likely that the concept of m-reduced words and the method of computing $r(u,x)$ are unnecessary, i.e. we feel that the above mentioned z_i's can be obtained by some other method. On the other hand we also feel that propositions 5 and 7, which show how to compute $r(u,x)$, do clarify our understanding of the relation $\overset{m}{\sim}$ and that they play an important role if one is interested in obtaining an efficient algorithm to decide whether $x \overset{m}{\sim} y$. In what follows we give, in an informal manner, another condition equivalent to those in theorem 7. This in turn suggests a substantially different

approach to obtain the desired result, i.e. (d) implies (a). Again, we were unable to carry out this approach, except in the very simple case of idempotent and commutative semiautomata. We omit this proof here; it is in fact an easy consequence of Schützenberger's method of proving that an event is star-free iff its syntactic semigroup is group-free [S1 and S2].

First we give the following definition.

Definition 12. A chain-reset is a connected semiautomaton $D = (Q,\Sigma,M,q_0)$ for which there is a linear ordering $q_0,q_1,\ldots,q_m$ of Q, such that for all $q_i \in Q - \{q_m\}$ and for all $\sigma \in \Sigma$, $q_i\sigma^D$ is either q_i or q_{i+1}, and $q_m\sigma^D = q_m$ for all $\sigma \in \Sigma$.

Now, in view of propositions 1 and 2, each congruence class $_m[x]$ can be denoted by a star-free expression which is a Boolean combination of events of the form $I\sigma_1I\sigma_2\ldots I\sigma_pI$, for some $p \leq m$. It follows that any (m,1)-testable event can be denoted by such expressions. On the other hand, an event of the form $I\sigma_1I\sigma_2\ldots I\sigma_pI$, for $p \leq m$, is clearly (m,1)-testable; thus the family $\alpha_{m,1}$ of (m,1)-testable events is precisely the family of events which can be denoted by Boolean combinations of events of the form $I\sigma_1I\sigma_2\ldots I\sigma_pI$, $p \leq m$. This is in fact equivalent to saying that

$$\alpha_{m,1} = B(C^m),$$

where C is the family

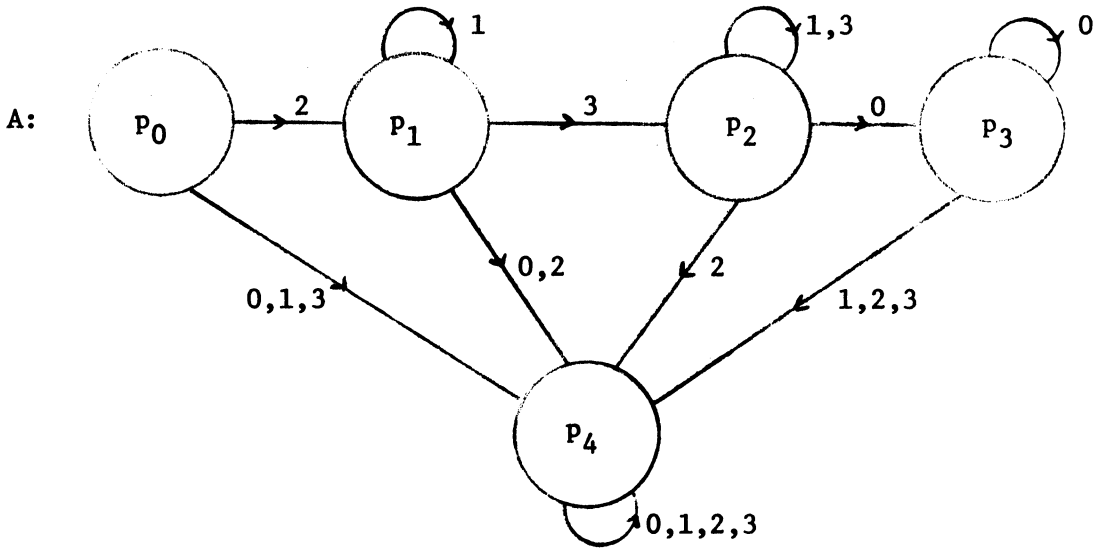
$$C = \{\lambda\} \cup \{I\sigma I \mid \sigma \in \Sigma\}.$$

Now, it is easy to see that if $\hat{D}$ is a reduced automaton accepting an event of the form $I\sigma_1I\sigma_2\ldots I\sigma_mI$, then D is a chain-reset with

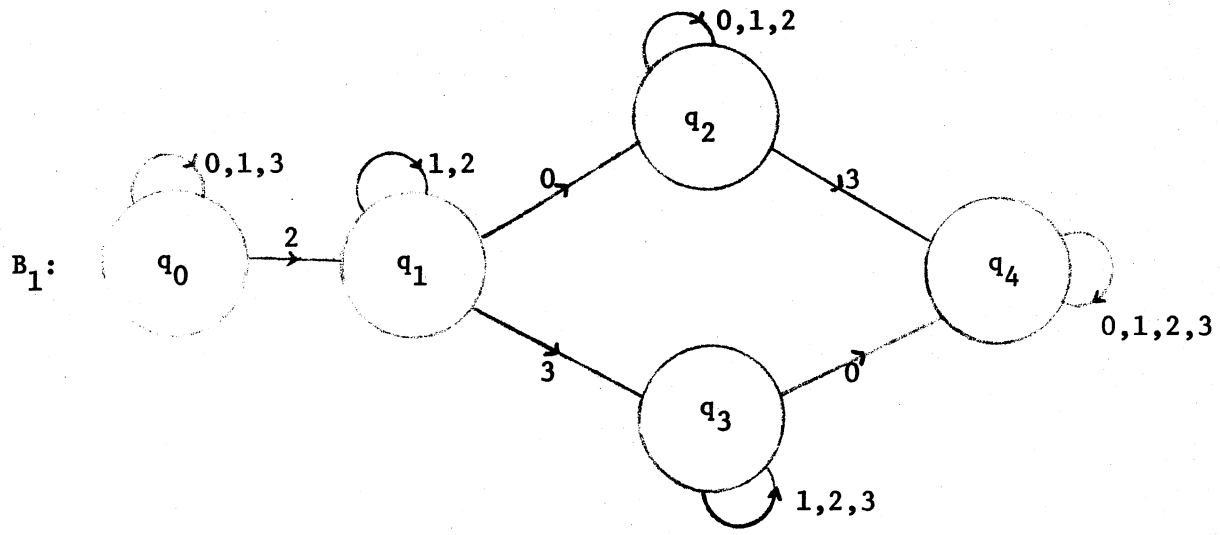
$m + 1$ states. It follows that if $\hat{A}$ is the reduced automaton accepting the (m,1)-testable event E, then there exist chain-resets $D_1, D_2, \ldots D_\ell$, with at most $m + 1$ states, such that $A \leq D_1 \times D_2 \times \ldots \times D_\ell$. It is also easy to see that if $D = (Q,\Sigma,M,q_0)$ is a chain-reset with at most $m + 1$ states, then for any $F \subseteq Q$, the event accepted by $\hat{D} = (Q,\Sigma,M,q_0,F)$ is (m,1)-testable. Thus, <u>if $\hat{A}$ is the reduced automaton accepting the event E, then E is (m,1)-testable iff A can be covered by a direct product of chain-resets with at most $m + 1$ states</u>. It follows now, from theorem 7, that <u>if $\hat{A}$ is a reduced automaton then A can be covered by a direct product of chain-resets iff S_A is J-trivial</u>. The proposed approach consists of finding chain-resets $D_1, D_2, \ldots, D_\ell$ such that $A \leq D_1 \times D_2 \times \ldots \times D_\ell$, given $\hat{A}$, such that S_A is J-trivial. We point out that our proof implies that A is covered by the direct product of all chain-resets (over Σ) with $m + 1$ states, where $m = 2(\#S_A + 1)$, since clearly $x \underset{m}{\sim} y$ iff $q_0x^D = q_0y^D$ for all chain-resets D, with $m + 1$ states. However, in general there exist fewer and smaller chain-resets, such that $A \leq D_1 \times D_2 \times \ldots \times D_\ell$.

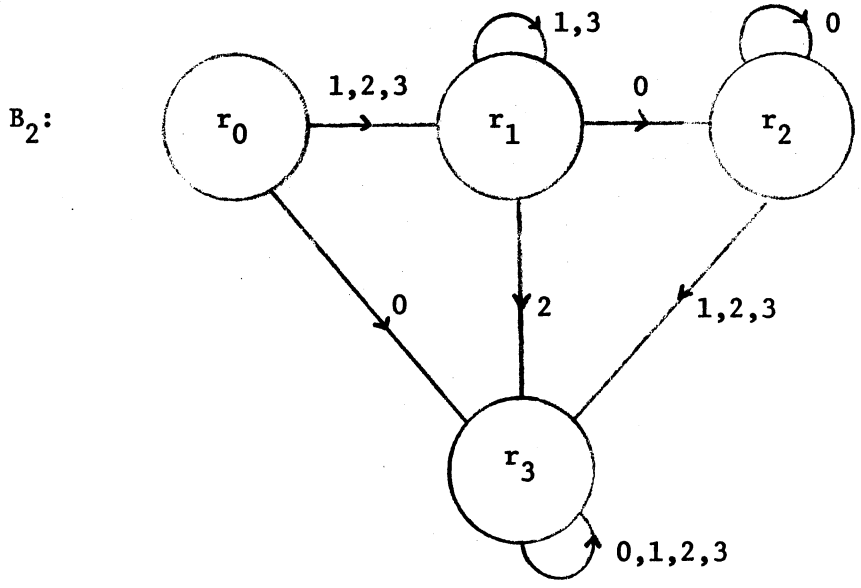
To illustrate this, we give an example in figure 5. The automaton $\hat{A}$ in figure 5(a), where p_4 is the only final state, is reduced. In figure 5(b) we exhibit two semiautomata B_1 and B_2, and in 5(c) we have the connected part of $B_1 \times B_2$. It is easy to see that $A \leq B_1 \times B_2$. In figures 5(d) and 5(f) we exhibit chain-resets D_1, D_2, D_3 and D_4; in 5(e) and 5(g) we have the connected parts of $D_1 \times D_2$ and $D_3 \times D_4$ respectively. It is easy to see that $B_1 \leq D_1 \times D_2$ and $B_2 \leq D_3 \times D_4$; hence $A \leq D_1 \times D_2 \times D_3 \times D_4$. It

follows that the event E accepted by $\hat{A}$ is (2,1)-testable. Incidentally, the reader can verify that the semiautomaton A is 2-testable (chapter 2); hence E is also locally testable, in fact (1,2)-testable.

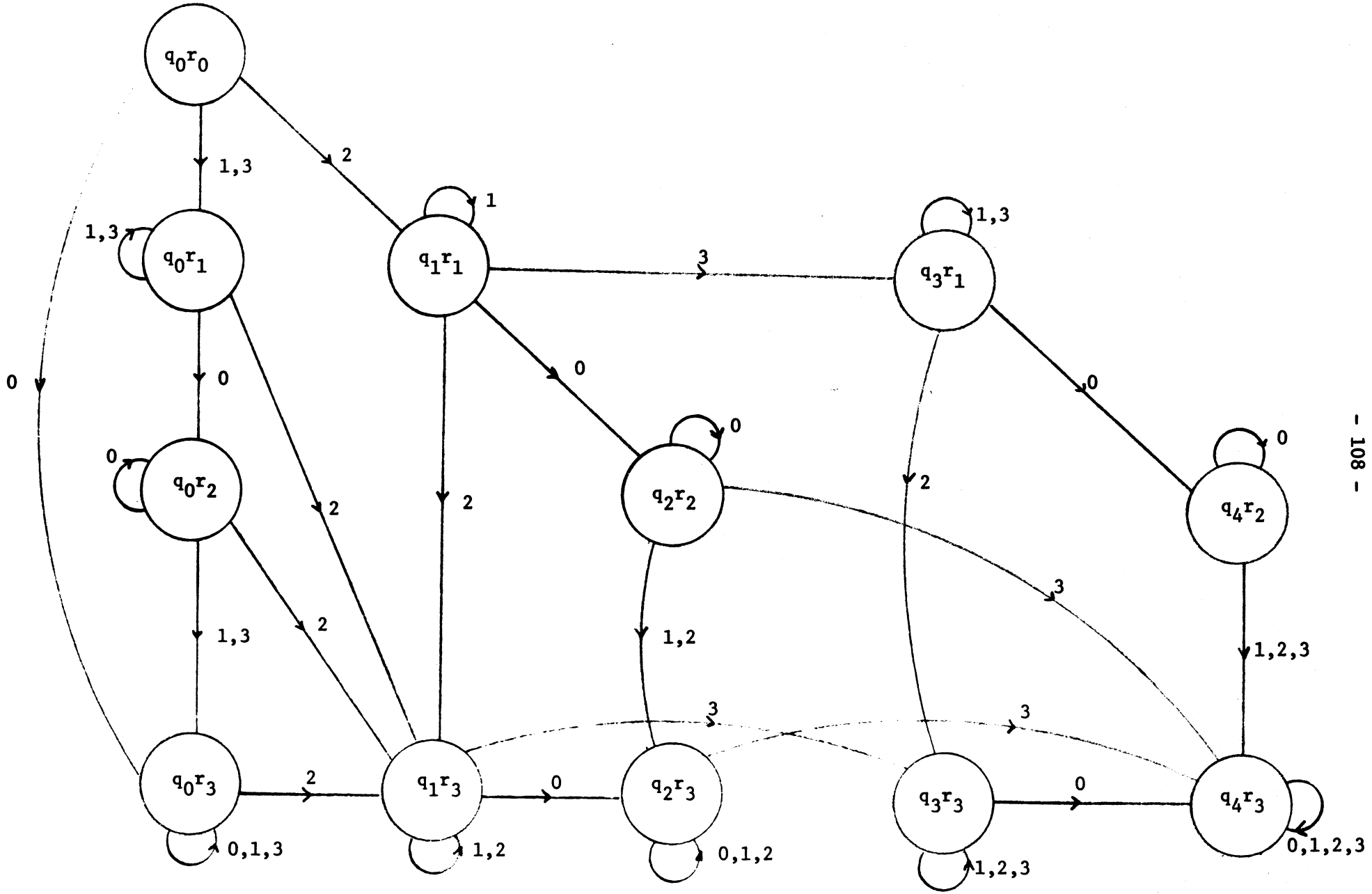


5(a) Semiautomaton A.

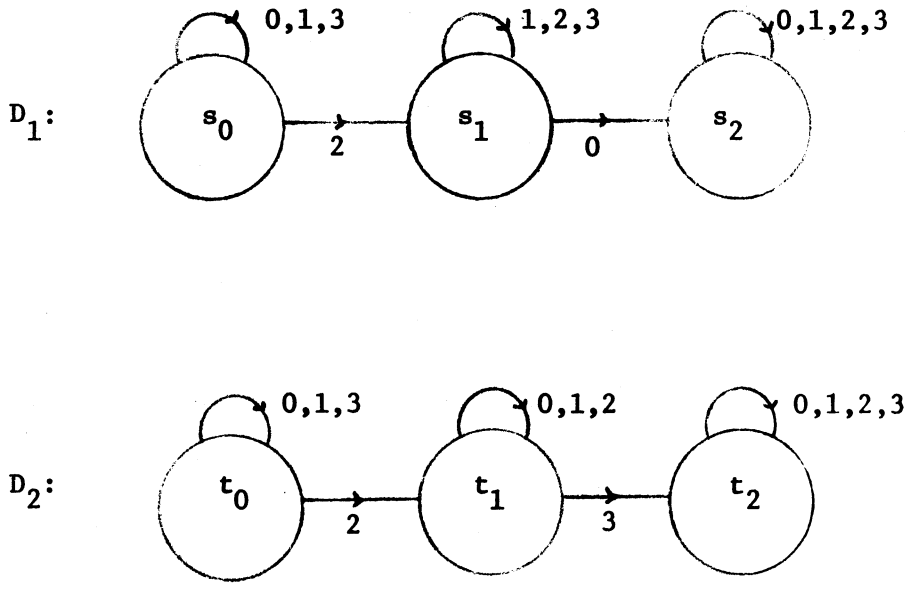




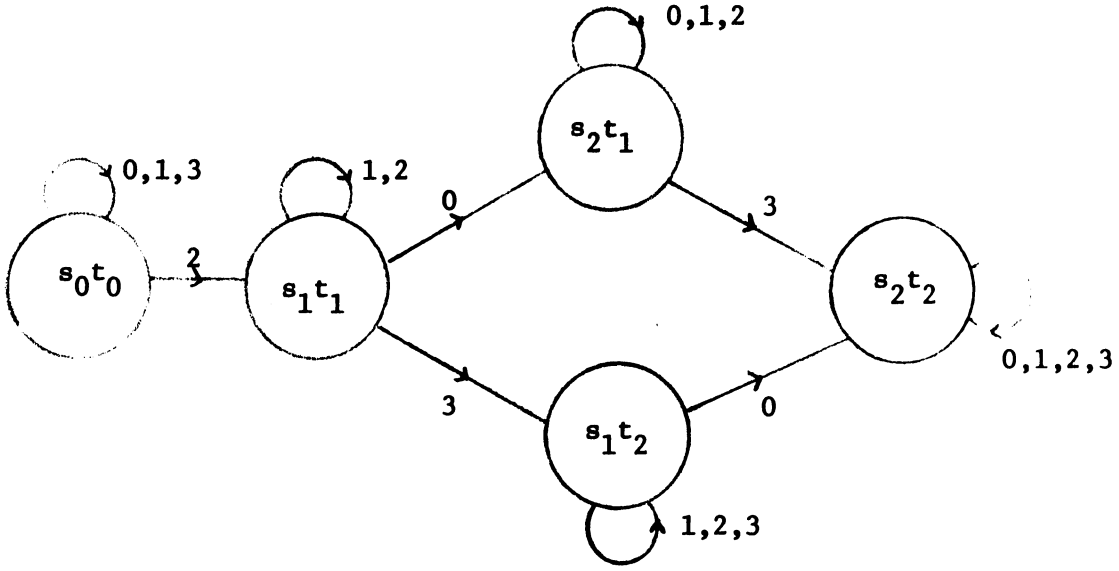
5(b) Semiautomata B_1 and B_2.



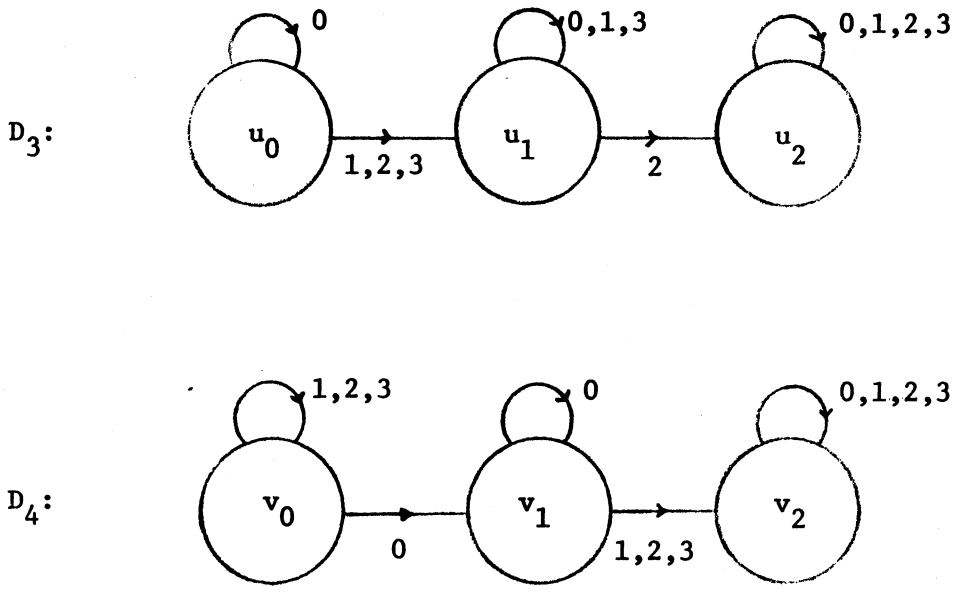
5(c) Semiautomaton $B_1 \times B_2$.



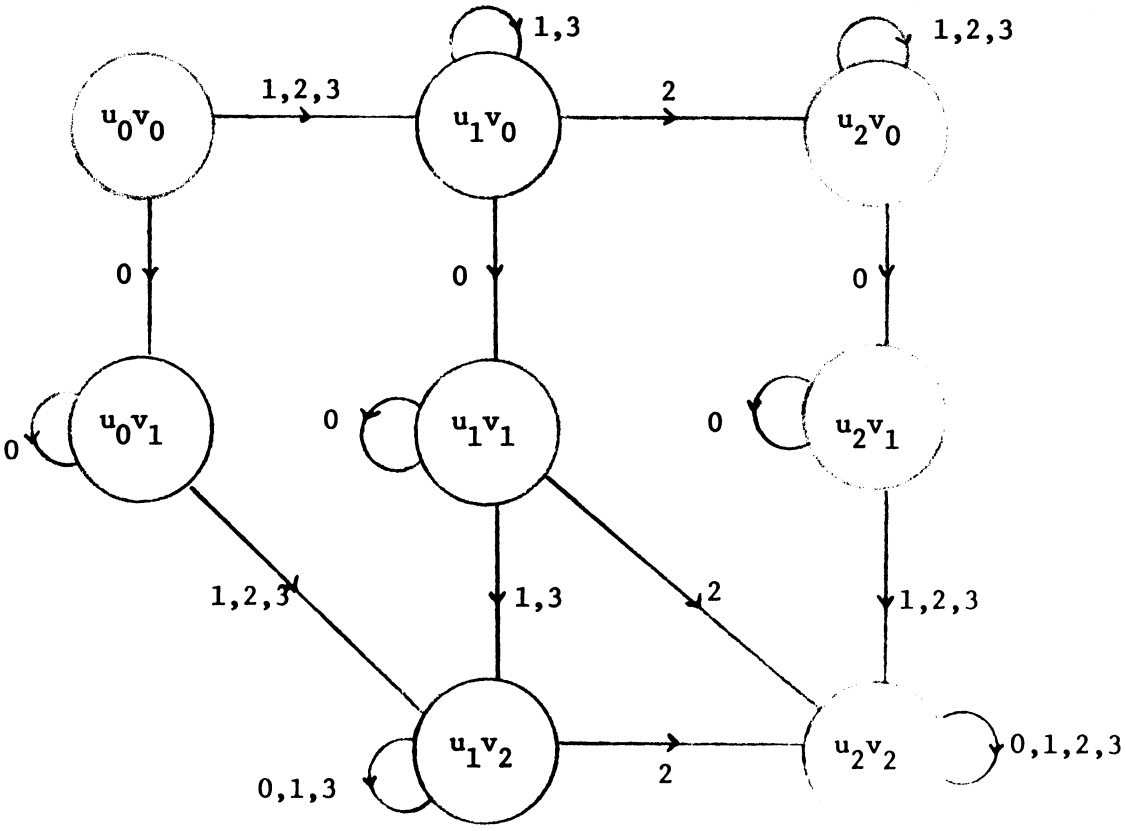
5(d) Chain-resets D_1 and D_2.



5(e) Semiautomaton $D_1 \times D_2$.



5(f) Chain-resets D_3 and D_4.



5(g) Semiautomaton $D_3 \times D_4$.

Figure 5 An Example.

Finally we wish to comment on statement (c) in theorem 7. Note that (c) and (d) are equivalent, even without the restriction that $\hat{A}$ is reduced. Indeed, we have:

Proposition 15. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton. Then S_A is J-trivial iff A is partially ordered and for all $q \in Q$ and $x,y \in \Sigma^*$, $qx^A = q(xx)^A = q(xy)^A$ and $qy^A = q(yy)^A = q(yx)^A$ imply $qx^A = qy^A$.

Proof. The if part is proved by (c) implies (d) in theorem 7. To see the converse, assume that S_A is J-trivial. Then S_A is R-trivial by theorem 6; hence A is partially ordered by proposition 14. Further, by theorem 6, there exists an integer $m > 0$, such that for all $x,y \in \Sigma^+$,

$$((xy)^m)^A = (y(xy)^m)^A. \tag{49}$$

Let $q \in Q$ and $x,y \in \Sigma^*$ be such that $qx^A = q(xx)^A = q(xy)^A$ and $qy^A = q(yy)^A = q(yx)^A$. If either $x = \lambda$ or $y = \lambda$, then clearly $qx^A = qy^A$. Otherwise $q((xy)^m)^A = qx^A$ and $q(y(xy)^m)^A = qy^A$. It follows from (49), that $qx^A = qy^A$. □

Now, (c) has been included in theorem 7 because of proposition 15 and because it is unpleasant (and maybe even uninformative) to test an automaton $\hat{A}$ for (b), since (b) involves the automata accepting E and E^T. On the other hand, (c) involves only A. The question then arises: how to test for the condition in (c)? We give an answer in proposition 16, but first we need the following definitions.

Definition 13. Let $A = (Q,\Sigma,M,q_0)$ be a semiautomaton. A component of A is a minimal nonempty subset P of Q, such that for all $q \in Q$ and for all $\sigma \in \Sigma$, $q\sigma^A \in P$ iff $q \in P$. Let θ be a nonempty subset of Σ. The restriction of A to θ is the semiautomaton

$A|\theta = (Q,\theta,N,q_0)$, where $\sigma^{A|\theta} = \sigma^A$ for all $\sigma \in \theta$. A dead state of A is a state $q \in Q$, such that for all $\sigma \in \Sigma$, $q\sigma^A = q$.

Now we have:

Proposition 16. Let $A = (Q,\Sigma,M,q_0)$ be a partially ordered semi-automaton. The following are equivalent.

(a) For all $q \in Q$ and for all $x,y \in \Sigma^*$, $qx^A = q(xx)^A = q(xy)^A$ and $qy^A = q(yy)^A = q(yx)^A$ imply $qx^A = qy^A$.

(b) For every nonempty subset θ of Σ, each component of $A|\theta$ contains exactly one dead state of $A|\theta$.

(c) Each component of $A|\theta$ contains exactly one dead state of $A|\theta$, for every subset θ of Σ satisfying (1) $\#\theta \geq 2$ and (2) there exist $r,s \in Q$, such that $r \neq s$ and $\theta = \{\sigma \mid r\sigma^A = r \text{ and } s\sigma^A = s\}$.

Proof. (a) implies (b). Let $P \subseteq Q$ be a component of $A|\theta$. Since A is partially ordered, so is $A|\theta$ and it is clear that P contains at least one dead state of $A|\theta$. Let r and s be dead states of $A|\theta$ in P, and assume that $r \neq s$. Let

$$R = \{p \in Q \mid px^{A|\theta} = r \text{ for some } x \in \theta^*\}.$$

It is easy to see that $R \subseteq P$; in fact R is a proper subset of P, since $s \notin R$. This and the minimality of P imply that there exist $q \in Q$ and $\sigma \in \theta$, such that $q\sigma^{A|\theta} \in R$ iff $q \notin R$. Now, by definition of R, $q\sigma^{A|\theta} \in R$ implies $q \in R$ for all $q \in Q$; hence it follows that there exist $q \in Q$ and $\sigma \in \theta$, such that $q \in R$ and $q\sigma^{A|\theta} \notin R$. Since $A|\theta$ is partially ordered, there exists a $y \in \theta^*$ such that $q(\sigma y)^{A|\theta} = t$ is a dead state of $A|\theta$. Clearly $t \notin R$. Now, since $q \in R$, it follows that $qx^{A|\theta} = r$ for some $x \in \theta^*$.

Since r and t are dead states of $A|\theta$, and $A|\theta$ is a restriction of A, it follows that

$$qx^A = q(xx)^A = q(x\sigma y)^A = r$$

and $$q(\sigma y)^A = q(\sigma y\sigma y)^A = q(\sigma yx)^A = t.$$

By (a), $r = t$, which is a contradiction, since $r \in R$ and $t \notin R$.

(b) implies (c). This is obvious.

(c) implies (a). Let $q \in Q$ and $x,y \in \Sigma^*$ be such that

$$qx^A = q(xx)^A = q(xy)^A = r$$

and $$qy^A = q(yy)^A = q(yx)^A = s.$$

Assume that $r \neq s$. Now, clearly $rx^A = ry^A = r$ and $sx^A = sy^A = s$. Since A is partially ordered, it follows that

$$\psi = \mu_1(x) \cup \mu_1(y) \subseteq \{\sigma \mid r\sigma^A = r \text{ and } s\sigma^A = s\} = \theta.$$

Assume now, that $\#\theta \leq 1$; then also $\#\psi \leq 1$; i.e. $x = \sigma^n$ and $y = \sigma^m$ for some $\sigma \in \Sigma$ and integers $n,m \geq 0$. Thus, $q(xy)^A = q(yx)^A$; hence $r = s$, a contradiction. Then $\#\theta \geq 2$. By (c), each component of $A|\theta$ contains exactly one dead state of $A|\theta$. On the other hand, clearly q, r and s are in the same component of $A|\theta$, and by construction, r and s are both dead states of $A|\theta$. This is a contradiction, hence $r = s$. □

Note that combining propositions 15 and 16, one can test whether S_A is J-trivial, for a given semiautomaton A, without constructing the semigroup S_A.

We illustrate proposition 16 by an example. Consider the semiautomaton A in figure 5(a). The only subset of Σ, satisfying (1) and (2) in (c) is $\theta = \{1,3\}$, for $r = p_2$ and $s = p_4$. The

restriction of A to θ is shown in figure 6. It contains two components: $\{p_0,p_3,p_4\}$ and $\{p_1,p_2\}$. Each contains exactly one

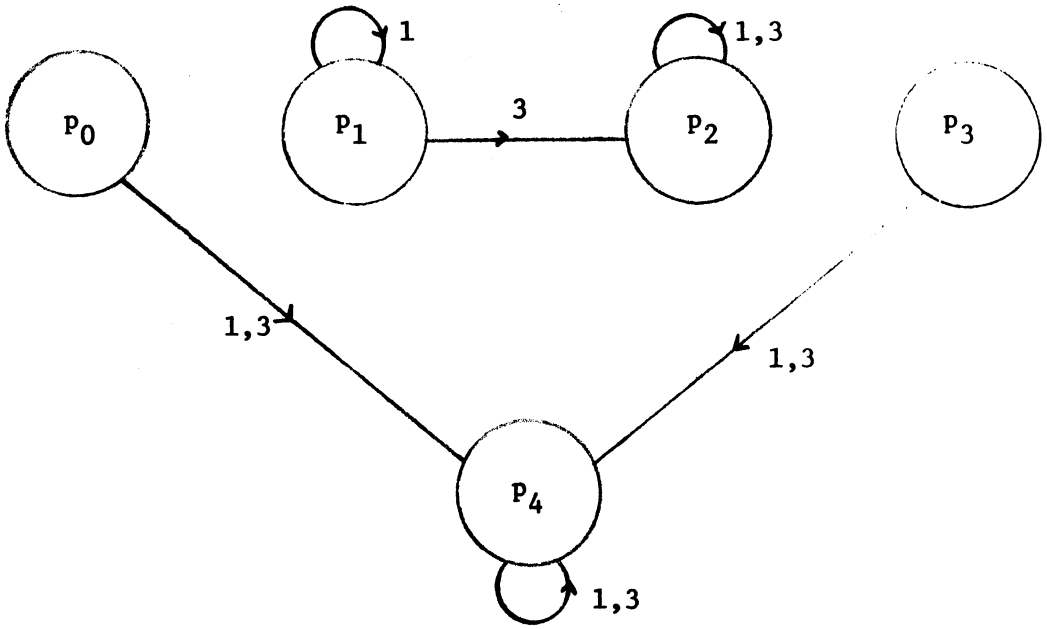


Figure 6 An example.

dead state, p_4 and p_2 respectively. Note that if, for example, $p_0 1^A = p_4$ is replaced by $p_0 1^A = p_2$, the resulting semiautomaton does not satisfy (c), hence its semigroup is not J-trivial.

CHAPTER 5

A Necessary Condition for Events of Dot-Depth One

In this chapter we derive a necessary condition for membership in B_2. We also comment on the structural characterization of the families of events introduced in chapter 3, as well as that of B_2 itself.

We begin with the following remark. Let S be a semigroup and let e be an idempotent S. Then eSe is a subsemigroup of S, in fact, it is a monoid with identity e. Let J_S and J_e denote the relation J in the semigroups S and eSe respectively. We claim that for $a,b \in eSe$ $a\ J_e\ b$ iff $a\ J_S\ b$. It follows that it is sufficient to consider the relation J_S; we will denote it by J. Let us now prove the claim. Clearly $a\ J_e\ b$ implies $a\ J_S\ b$. Assume now that $a\ J_S\ b$; i.e. there exist $s,t,u,v \in S^1$, such that $a = sbt$ and $b = uav$. Since $a,b \in eSe$, it follows that $a = eae$ and $b = ebe$. This implies that $a = esebete$ and $b = eueaeve$; hence $a\ J_e\ b$.

Now we have the following.

Proposition 1. Let $\hat{A}$ be the reduced automaton accepting the event E. If E is in B_2, then for every idempotent e in S_A, eS_Ae is a J-trivial subsemigroup of S_A.

Proof. Since $E \in B_2$, it follows from corollary 3.1 that $E \in \alpha_{m,k}$ for some integers $m,k > 0$. Thus, it follows from proposition 1.1 and 3.2(b) that for all $x,y,z \in \Sigma^*$, such that $|x| = k - 1$,

$$(x(yxzx)^m)^A = (x(yxzx)^m yx)^A. \qquad (1)$$

Let e, a and b be in S_A, e an idempotent. In view of theorem 4.6(c), to prove that eS_Ae is J-trivial, it is sufficient to show that

$$(eaeebe)^m = (eaeebe)^m eae \tag{2}$$

and

$$(eaeebe)^m = ebe(eaeebe)^m. \tag{3}$$

Let $u,v,w \in \Sigma^+$ be such that $e = u^A$, $a = v^A$ and $b = w^A$. Since $u \in \Sigma^+$, it follows that $|u^k| \geq k$; hence $u^k = tx$ for some $t,x \in \Sigma^*$, such that $|x| = k - 1$. Since e is idempotent, it follows that $e = (tx)^A$. Further, let $y = vt$ and $z = wt$. Then we have

$$(eaeebe)^m = e(aebe)^m = (tx(yxzx)^m)^A. \tag{4}$$

From (1) it follows that

$$(tx(yxzx)^m)^A = (tx(yxzx)^m yx)^A. \tag{5}$$

Now, $(tx(yxzx)^m yx)^A = e(aebe)^m ae = (eaeebe)^m eae$; hence (2) follows from (4) and (5). By a dual argument one can prove (3); hence eS_Ae is J-trivial. □

Note that the necessary condition in proposition 1 is effective. It follows that one can produce examples of events which are not in B_2. In fact, the event E = 2*0I over $\Sigma = \{0,1,2\}$ is not in B_2. The reduced automaton $\hat{A}$, accepting E is represented in figure 1. The semigroup S_A has an identity element $e = 2^A$. Since

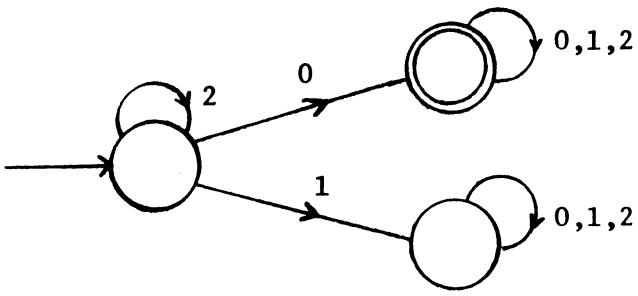


Figure 1. Automaton accepting 2*0I.

$eS_Ae = S_A$ is not J-trivial, it follows that E is not in B_2. Note that this has been proved by Cohen and Brzozowski [CB]. Now, clearly $E = 2^*0I = \overline{I(1 \cup 0)I}0I$; hence $E \in B_3$ and the dot-depth of E is 2. Another such example is given by the event $E = (01 \cup 10)^*$, mentioned in section 1.2. We have seen there that

$$E = \overline{\overline{I0} \; X \; \overline{0I} \cup \overline{I1} \; Y \; \overline{1I}},$$

where $X = 1(01)^* = 1I \cap I1 \cap \overline{I00I} \cap \overline{I11I}$, and $Y = 0(10)^* = 0I \cap I0 \cap \overline{I00I} \cap \overline{I11I}$. We represent in figure 2 the reduced automaton $\hat{A}$ accepting E. We leave it to the reader to

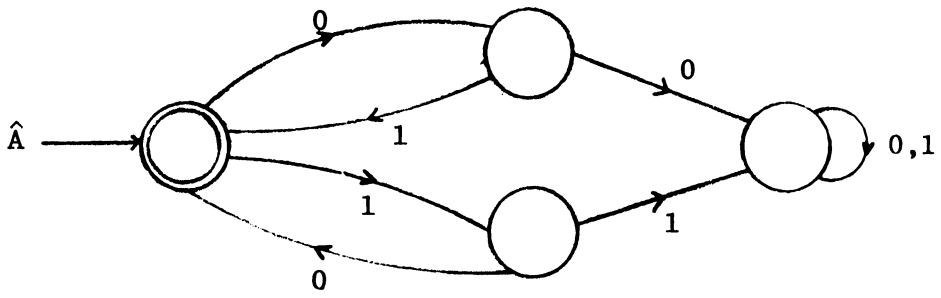


Figure 2. Automaton $\hat{A}$ accepting $(01 \cup 10)^*$.

verify the following:

(a) $e = (01)^A = (0101)^A$; hence e is an idempotent in S_A,

(b) $a = (001)^A = (0100101)^A = eae$, $b = (0011)^A = (01001101)^A = ebe$ and $a \neq b$. Hence $a,b \in eS_Ae$.

(c) $a1^A = b$ and $b0^A = a$; hence $a \; J \; b$.

It follows that eSe is not J-trivial and thus $E \notin B_2$. On the other hand, the star-free expression for E implies that $E \in B_3$; hence the dot-depth of E is 2.

We now have the following corollary to proposition 1 and theorem 4.7.

Corollary 1. Let $\hat{A}$ be the reduced automaton accepting the event E. If S_A has an identity, then E is in B_2 iff S_A is J-trivial.

Proof. Let $E \in B_2$. Since S_A has an identity, say e, it follows from proposition 1, that $eS_Ae = S_A$ is J-trivial. Conversely, if S_A is J-trivial then $E \in \gamma_1$ by theorem 4.7; hence $E \in B_2$. □

We conjecture that the necessary condition in proposition 1 is sufficient as well, that is to say we have:

Conjecture. Let $\hat{A}$ be the reduced automaton accepting the event E. Then E is in B_2 iff for every idempotent e in S_A, eS_Ae is a J-trivial subsemigroup of S_A.

Note that we have proved in chapters 2 and 4 the if part of the conjecture in two particular cases. In chapter 2 we proved that if for every idempotent e in S_A, eS_Ae is idempotent and commutative, (hence eS_Ae is J-trivial) then E is locally testable; hence E is $(1,-)$-testable and it is in B_2. In chapter 4 we proved that if S_A is J-trivial, then E is $(-,1)$-testable; hence E is in B_2.

Finally, we wish to comment on the structure of (reduced) automata accepting events in $\alpha_{m,k}$, for $m,k \geq 1$. Let A be a semiautomaton; we say that A is of type (m,k) if there exist semi-automata B and C, such that

(1) B is $(k-1)$-definite,

(2) C can be covered by a direct product of chain-resets with at most $m+1$ states,

(3) $A \leq B \circ C$.

We will outline a proof of the following proposition. Let $m,k \geq 1$ and let $\hat{A}$ be the reduced automaton accepting the event E. Then E is (m,k)-testable iff A is of type (m,k).

Let us first consider the following five assertions:

(a) If $|u| = k-1$ and $\hat{A}$ is the reduced automaton accepting Iu (uI respectively), then A is of type (1,k); hence A is also of type (m,k).

(b) Let $\underline{w} \in (\Sigma^k)^m$; and let $\hat{A}$ be the reduced automaton accepting the event $L(\underline{w})$ (see section 3.2). Then A is of type (m,k).

(c) If A_1 and A_2 are semiautomata of type (m,k), then so is $A_1 \times A_2$.

(d) Let A, B and C be semiautomata. Then $A \circ (B \times C) \prec (A \circ B) \times (A \circ C)$.

(e) If B is a (k-1)-definite semiautomaton and C is a chain-reset with at most (m+1) states, then for all $x,y \in \Sigma^*$, $x \underset{m}{\sim}_k y$ implies $x^{B \circ C} = y^{B \circ C}$.

The proofs of these assertions are tedious but straightforward, and we omit them here. Now, the only if part of the proposition follows from assertions (a), (b) and (c) and the expressions obtained for ${}_m[x]_k$ in the proof of theorem 3.1. The if part follows from assertions (d) and (e). As a corollary of the above proposition, we have the following. Let $\hat{A}$ be the reduced automaton accepting the event E. Then E is in γ_k $(k \geq 1)$ iff there exist a (k-1)-definite semiautomaton B and a semiautomaton C which can be covered by a direct product of chain-resets, such that $A \leq B \circ C$. Also E is in δ_m $(m \geq 1)$ iff there exist a definite semiautomaton B and a semiautomaton C

which can be covered by a direct product of chain-resets with at most m+1 states, such that $A \leq B \circ C$. Finally, E is in B_2 iff there exist a definite semiautomaton B and a semiautomaton C which can be covered by a direct product of chain-resets, such that $A < B \circ C$. Note that the last statement does characterize B_2, however it is not an effective characterization, in the sense that it is not clear how to test whether there exist semiautomata B and C satisfying the given properties.

Finally, we point out that the structural characterization for B_2 shows that the role played by semiautomata, whose semigroups are J-trivial, in the characterization of B_2 is similar to that of idempotent and commutative semiautomata in the characterization of locally testable events. (cf. first paragraph in section 2.2). Indeed, we proved that an event E is in γ_1 iff the semigroup S_A of the reduced automaton $\hat{A}$ accepting E is J-trivial. On the other hand, these semiautomata are used as tail machines in the structural characterization of automata accepting events in B_2.

CHAPTER 6

Conclusion and Further Research

In this thesis we have defined two hierarchies of Boolean algebras; the union of the families in each hierarchy is the family B_2 of star-free events with dot-depth at most one. We showed that both hierarchies are infinite and that they are incomparable. Each family in the hierarchies, as well as B_2, has been characterized by means of structural decompositions in terms of definite semiautomata and semiautomata whose semigroups are J-trivial. We also characterized effectively the first two families of the δ-hierarchy and the first family of the γ-hierarchy, in the sense that we gave algorithms to decide whether a given event is in one of these families. Our technique consisted of defining congruence relations $\underset{m}{\sim}_k$ over Σ^* for each $m \geq 0$ and $k > 0$. Then we considered families of events which are unions of congruence classes. Loosely speaking, our characterizations of δ_1 and γ_1, in chapters 2 and 4 respectively, were obtained by finding certain properties of the respective congruence relations (propositions 2.4 and 4.3(d) and its dual). These properties gave rise, via proposition 1.1, to necessary conditions for membership in those families. Then we showed that these conditions are sufficient as well. The proofs of sufficiency turned out to be long and difficult arguments. By a similar method, starting with proposition 3.2 and its dual, we obtained an effective necessary condition for membership in B_2; but we were unable to prove the sufficiency in this case.

Now we mention a few open problems which arise from this thesis. Of course, the most important of these, is to prove or disprove the conjecture in chapter 5, regarding the family B_2. This problem proved to be difficult and it is possible that the investigation of some of the following open problems might be useful in answering that conjecture.

We have proved, in a number of cases, the existence of structural decompositions with properties P_1 for semiautomata satisfying properties P_2. Examples of this, can be found in sections 2.2, 2.3 and 4.4 for the case of idempotent and commutative semiautomata, k-testable semiautomata and semiautomata whose semigroups are J-trivial, respectively. We have done this by considering (implicitly or explicitly) the largest possible (free) semiautomaton over a fixed alphabet Σ, satisfying properties P_2 and proving that these admit a structural decomposition with properties P_1. Our approach succeeded because the free semiautomata turned out to be finite in every case. However, in general, we were unable to find constructions which yield smaller decompositions with properties P_1. The open problem consists of finding these constructions. This is, of course, related to the problem of writing "reasonable" regular expressions of a restricted type for events accepted by automata satisfying P_2.

In chapter 2 [4] we found an upper bound for $k\,[m]$, such that an event E is locally testable [(-,1)-testable], iff it is k-testable [(m,1)-testable] for $k = \#S_A + 2$ [$m = 2(\#S_A + 1)$]. We believe that these bounds are not tight and hence we propose the

problem of finding better bounds for k and m. Note that this problem might be related to the previous one.

In chapter 3 we defined the families γ_k and δ_m. In section 4.4 we gave an example (figure 5) of an event E which is both (2,1)-testable and (1,2)-testable, hence $E \in \delta_1 \cap \gamma_1$. However it is easy to see that $E \notin \alpha_{1,1}$, since A is not idempotent and commutative. This leads to the interesting question of investigating and possibly characterizing the Boolean algebras $\delta_m \cap \gamma_k$. Clearly $\alpha_{m,k} \subseteq \delta_m \cap \gamma_k$; however it is easy to see that the inclusion is proper. Indeed, the family $\beta_1 = F \cup C$ is contained in $\delta_m \cap \gamma_k$ for every m and k. It follows that $\delta_m \cap \gamma_k$ is an infinite Boolean algebra. In view of the structural characterizations in chapter 5, this problem corresponds to investigating the existing trade-off between the complexity of the definite front machines (giving k) and that of the J-trivial tail machines (giving m). The example in figure 4.5 and the fact that $\beta_1 \subseteq \delta_m \cap \gamma_k$ do prove the existence of such a trade-off. On the other hand, the fact that both the γ- and δ-hierarchies are infinite show that this trade-off is limited.

Finally, we propose the problem of finding an algebraic characterization of semigroups S_A, corresponding to automata A accepting (m,1)-testable events. In a sense this problem is solved by theorem 4.4; however it is likely that more natural characterizations exist. We cite for example the case $m = 1$ which corresponds to idempotent and commutative semigroups. For $m = 2$, we can prove the

following: Let $\hat{A}$ be the reduced automaton accepting the event E. Then E is (2,1)-testable iff for all $u,v,x \in S_A$ $xuvx = xuxvx$ and $(uv)^2 = (vu)^2$.

References

[B] Brzozowski, J. A., Canonical Regular Expressions and Minimal State Graphs for Definite Events, in "Proc. of the Symp. of Math. Theory of Automata", Polytechnic Institute of Brooklyn, Brooklyn, New York, 1962, 529-561.

[BCG] Brzozowski, J. A., Culik II, K. and Gabrielian, A., Classification of Noncounting Events, J. of Computer and System Sciences 5 (1971), 41-53.

[BS] Brzozowski, J. A. and Simon, I., Characterizations of Locally Testable Events, in "Conference Record 1971 Twelfth Annual Symp. on Switching and Automata Theory", IEEE Computer Society, 1971, 166-176.

[CB] Cohen, R. S. and Brzozowski, J. A., Dot-depth of Star-Free Events, J. of Computer and System Sciences 5 (1971), 1-16.

[CP] Clifford, A. H. and Preston, G. B., "The Algebraic Theory of Semigroups", Vol. I, Math. Surveys 7, Amer. Math. Soc., Providence, R.I., 1961.

[G1] Ginzburg, A., "Algebraic Theory of Automata", Academic Press, New York, 1968.

[G2] Ginzburg, A., About Some Properties of Definite, Reverse-Definite and Related Automata, IEEE Trans. on Electronic Computers EC-15 (1966), 806-810.

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

[KR] Krohn, K. and Rhodes, J. L., Algebraic Theory of Machines I. Prime Decomposition Theorem for Finite Semigroups and Machines, Trans. Amer. Math. Soc. 116 (1965), 450-464.

[KRT] Krohn, K., Rhodes, J. L. and Tilson, B. R., The Prime Decomposition Theorem of the Algebraic Theory of Machines, in "Algebraic Theory of Machines, Languages and Semigroups", M. A. Arbib (ed.), Academic Press, N.Y., 1968, 81-125.

[M1] McNaughton, R., Algebraic Decision Procedures for Local Testability, Tech. Report, Rensselaer Polytechnic Institute, Troy, N.Y., 1971, to appear in Math. Systems Theory.

[M2] Meyer, A. R., A Note on Star-Free Events, J. of the Assoc. for Computing Machinery 16 (1969), 220-225.

[MP] McNaughton, R. and Papert, S., "Counter-Free Automata" Research Monograph No. 65, The MIT Press, Cambradge, Mass., 1971.

[MZ] McNaughton, R. and Zalcstein, Y., Abstract 71T-C16, Notices Amer. Math. Soc. 18 (1971), p. 657.

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

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

[RT] Rhodes, J. L. and Tilson, B. R., Local Structure Theorems for Finite Semigroups, in "Algebraic Theory of Machines, Languages and Semigroups", M. A. Arbib (ed.), Academic Press, N.Y., 1968, 147-189.

[S1] Schützenberger, M. P., On Finite Monoids Having Only Trivial Subgroups, Information and Control 8 (1965), 190-194.

[S2] Schützenberger, M. P., On a Family of Sets Related to McNaughton's L-language, in "Automata Theory", E. R. Caianiello (ed.), Academic Press, N.Y., 1966, 320-324.

[S3] Stiffler, Jr., P. E., "Extension of the Fundamental Theorem of Finite Semigroups", Ph.D. thesis, University of California, Berkeley, 1970.

[Z1] Zalcstein, Y., Locally Testable Languages, J. of Computer and System Sciences 6 (1972), 151-167.

[Z2] Zalcstein, Y., Remarks on Automata and Semigroups, Unpublished manuscript, 1971.

[Z3] Zeiger, H. P., Yet Another Proof of the Cascade Decomposition Theorem for Finite Automata, Math. Systems Theory 1 (1967), 225-228.

[Z4] Zeiger, H. P., Cascade Decomposition of Automata Using Covers, in "Algebraic Theory of Machines, Languages and Semigroups", M. A. Arbib (ed.), Academic Press, N.Y., 1968, 55-80.