CLASSIFICATION OF REGULAR LANGUAGES BY CONGRUENCES

by

Denis Thérien

RESEARCH REPORT CS-80-19

University of Waterloo
Department of Computer Science
Waterloo, Ontario, Canada

April 1980

CLASSIFICATION OF REGULAR LANGUAGES BY CONGRUENCES

by

Denis Thérien

A thesis
presented to the University of Waterloo
in partial fulfilment of the
requirements for the degree of
Doctor of Philosophy
in
Computer Science

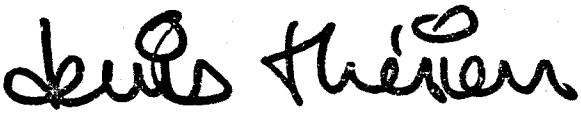
Waterloo, Ontario, 1980

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

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

Signature 

I further authorize the University of Waterloo to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Signature 

The University of Waterloo requires the signatures of all persons using or photocopying this thesis. Please sign below, and give address and date.

Abstract

In this thesis, we consider the problem of providing an algebraic classification of regular languages. An abstract monoid M recognizes the language $L \subseteq A^*$ iff there exists a surjective morphism $\phi: A^* \to M$ such that $L = S\phi^{-1}$ for some $S \subseteq M$. Given a family $\underline{M}$ of abstract monoids, it is a natural problem to try to characterize the languages recognized by the monoids in $\underline{M}$. Conversely, given a family of languages $\mathcal{L}$, we can ask for a characterization of the smallest family of monoids which are needed to recognize all the languages in $\mathcal{L}$.

A family $\underline{M}$ of finite monids is a variety iff it is closed under morphic images, submonoids and finite direct products. A family $\mathcal{L}$ of regular languages is a *-variety iff it is closed under boolean operations, derivatives and inverse morphisms. Eilenberg's theorem indicates that there exists a 1-1 correspondence between varieties of monoids and *-varieties of languages.

Our approach makes use of congruences of finite index. The conditions defining varieties are first expressed in terms of these objects. We then present a method for constructing congruences which generates *-varieties in a systematic manner. The languages produced in this way have the property that the membership of a word x can be determined by counting occurrences of subwords of length $\leq m$ with respect to a congruence of finite index on $\mathbb{N}$, taking into account the context in which these subwords appear with respect to a previously

given congruence γ. This scheme is recursively applied, using as basis the universal congruence $x \omega y$ for all $x, y \in A^*$. Noting the fact that every congruence of finite index on $\mathbb{N}$ is the intersection of a threshold t counting congruence and a modulo q counting congruence, our *-varieties of congruences are characterized by four parameters: the t and q of the congruence on $\mathbb{N}$ with respect to which the counting is done, the length m of the subwords that are counted and the depth i of the recursion. Algebraic properties of the corresponding monoids are then investigated in terms of these four indices.

For all values of m and i, if only threshold t counting is used (i.e. q is fixed to 1), the generated monoids are aperiodic, and if only modulo q counting is used (i.e. t is fixed to 0), the generated monoids are groups. The following table summarizes some characterizations that have been obtained.

$i = 1, m = 1, t \geq 0, q = 1$	commutative aperiodic monoids
$i = 1, m = 1, t = 0, q \geq 1$	commutative groups
$i = 1, m = 1, t \geq 0, q \geq 1$	commutative monoids
$i = 1, m \geq 0, t \geq 0, q = 1$	J-trivial monoids
$i = 1, m \geq 0, t = 0, q \geq 1$	nilpotent groups
$i = n, m = 1, t = 0, q \geq 1$	solvable groups of derived length $\leq n$
$i = n, m \geq 0, t = 0, q \geq 1$	solvable groups of fitting length $\leq n$
$i \geq 0, m = 1, t \geq 0, q = 1$	aperiodic monoids
$i \geq 0, m = 1, t = 0, q \geq 1$	solvable groups
$i \geq 0, m = 1, t \geq 0, q \geq 1$	monoids containing only solvable groups.

For the last three entries, the monoids are the same if we replace $m = 1$ by $m \geq 0$. In several other cases partial characterizations are presented. In addition, tradeoffs between the various parameters are analyzed and some families of languages are investigated from the point of view of Kleene's operations. Finally, modifying the construction to take into account one-sided contexts only, it is shown that R- and L-trivial monoids are generated when threshold t counting is used.

Acknowledgements

I wish to thank my supervisor Janusz Brzozowski for stimulating my interest in the algebraic theory of regular languages. His encouragement was often much needed. I also thank the members of the examining committee: Dominique Perrin, Tom Maibaum, Karel Culik and Denis Higgs. Faith Fich and Howard Straubing made useful comments on preliminary versions of this work.

The difficult task of typing my manuscript was well handled by Mrs. Maura Crilly. Various other contributions, not necessarily of a mathematical nature, were made by Louise, Danielle, Jean-Philippe, Mary Jane, Herman and Bill.

The financial assistance of the National Science and Engineering Research Council of Canada, by means of a Science 67 scholarship and grant A-1617, is gratefully acknowledged.

Table of Contents

Index of definitions

Index of symbols

Congruences and counting factorizations

Languages

H^i	languages of *-height $\leq i$, 66
L^ρ	reverse of the language L, 7
$\mathcal{L}B$	boolean closure of $\mathcal{L}$, 116
$\mathcal{L}M$	monoid closure of $\mathcal{L}$, 116
$\mathcal{L}_{t,q}^{m,i}$	*-variety of languages associated with $\Delta(\Delta_{t,q}^{m,i})$, 116

Semiautomata

A_γ	semiautomaton associated with the congruence γ, 89
A_M	semiautomaton associated with the monoid M, 89
$A_1 \overset{\circ}{g} A_2$	cascade g-connection of A_1 and A_2, 89

Semigroups

S^ρ	reverse of the semigroup S, 7
U	monoid, 96
U_1	monoid, 108
Z(G)	center of the group G, 19
$H \lhd G$	H is a normal subgroup of G, 19
$S \simeq T$	S is isomorphic with T, 5

*-varieties of congruences

Γ	congruences of finite index, 5
Γ_+	aperiodic congruences, 10
$\Gamma_\times$	group congruences, 10
$\Delta_{t,q}$	*-variety generated by $\alpha_{t,q}$, 26
$\Delta_{t,q}^{m,i}$	*-variety generated by $\alpha_{t,q}^{m,i}$, 46

$\overrightarrow{\Delta^{m,i}_{t,q}}$ *-variety generated by $\overrightarrow{\alpha^{m,i}_{t,q}}$, 85

$\Delta(\Delta^{m}_{t,q})$ *-variety generated by $\gamma(\alpha^{m}_{t,q})$, $\gamma \in \Delta$, 37

$\Delta(\Delta^{m,i}_{t,q})$ *-variety generated by $\gamma(\alpha^{m,i}_{t,q})$, $\gamma \in \Delta$, 39

$\overrightarrow{\Delta(\Delta^{m,i}_{t,q})}$ *-variety generated by $\gamma(\overrightarrow{\alpha^{m,i}_{t,q}})$, $\gamma \in \Delta$, 84

$\Delta^{m,*}_{t,q}$ $\bigcup_{i\geq 0} \Delta^{m,i}_{t,q}$, 23

Ω *-variety generated by ω, 26

Varieties of monoids

$\underline{Ap}$ aperiodic monoids, 17

$\underline{CM}$ monoids satisfying the equations defining $\underline{M}$ in context, 100

$\overrightarrow{\underline{CM}}$ monoids satisfying the equations defining $\underline{M}$ in one-sided context, 109

$\underline{G}$ groups, 17

$\underline{G_{ab}}$ abelian groups, 20

$\underline{G_{der,i}}$ solvable groups of derived length $\leq i$, 88

$\underline{G_{der,i,q}}$ subvariety of $\underline{G_{der,i}}$, 92

$\underline{G_{fit,i}}$ solvable groups of fitting length $\leq i$, 88

$\underline{G_{fit,i,q}}$ subvariety of $\underline{G_{fit,i}}$, 92

$\underline{G_{nil}}$ nilpotent groups, 20

$\underline{G_{nil,m}}$ nilpotent groups of class $\leq m$, 55

$\underline{G_{p}}$ p-groups, 20

$\underline{G_{sol}}$ solvable groups, 20

$\underline{G_{\Pi}}$ Π-groups, 19

$\underline{J}$ J-trivial monoids, 74

$\underline{LM}$	localization of $\underline{M}$, 103
$\underline{M}_{com}$	commutative monoids, 28
$\underline{M}_{der,i,q}$	monoids containing groups in $\underline{G}_{der,i,q}$, 112
$\underline{M}_{sol}$	monoids containing solvable groups, 112
$\underline{M}_{t,q}$	monoids satisfying $m^t = m^{t+q}$, 28
$\underline{M}(\underline{S})$	variety of monoids, 100
$\underline{M}(\underline{S}^i)$	variety of monoids, 100
$\underline{R}$	R-trivial monoids, 107
$\underline{1}$	trivial variety of monoids, 26

Miscellaneous

λ	empty word, 6
$[x]_\alpha$	congruence class of x, 5
x^ρ	reverse of the word x, 7
V_1V_2	product of contexts, 34
$\overrightarrow{V_1}\overrightarrow{V_2}$	product of one-sided contexts, 82
$\lfloor n \rfloor$	floor function, 52
$\lceil n \rceil$	ceiling function, 42
$(m)_p$	highest power of p dividing m, 51
deg f	degree of a polynomial f, 61
deg F	degree of a set of polynomials F, 61
supp f	support of a polynomial f, 61
$\vee$	join operator on varieties, 114
$\Delta \to L$	11
$L \to \Delta$	12
$\Delta \to \underline{M}$	16
$\leftrightarrow$, $\to$	17

I. INTRODUCTION

The notion of regular language arises by considering finite machines processing finite sequences of inputs. The original motivation for this type of work came through attempts to model the behaviour of the brain, but it was soon realized that the theory of regular languages could be an important tool in the study of finite circuits and digital computers (cf: Kleene [54], McNaughton [61]).

Connections with classical algebra were also established. A semigroup S generated by a set A can be viewed as a machine over input alphabet A, the states being the elements of S, where processing a sequence of inputs means applying the semigroup operation. The proper formalization of this idea gives rise to a correspondence between regular languages and finite semigroups. Consideration of the empty sequence leads to a similar relationship between regular languages and finite monoids (cf: Myhill [57], Rabin and Scott [59]).

This algebraic characterization was refined over the years, as several subclasses of regular languages were shown to correspond to families of semigroups or monoids. For example, definite languages (Perles, Rabin and Shamir [59]), star-free languages (Schützenberger [65]), locally testable languages (Brzozowski and Simon [73]) and piecewise testable languages (Simon [72]) were all characterized by algebraic methods. This approach was formalized in the theory of

varieties presented by Eilenberg [76]: the essential result of Eilenberg exhibits a 1-1 correspondence between *-varieties (+ - varieties) of regular languages and varieties of monoids (semigroups).

In view of the central role played by regular languages in modeling finite computations, it appears to be a worthwhile problem to study possible classification schemes that would induce a measure of complexity applicable to those languages. Original attempts to provide such a systematic classification centered on regular expressions. The restricted *-height of Eggan [63] and the extended *-height presented in McNaughton and Papert [71] were measures of complexity related to the presence of the * operator in expressions representing languages. The family of star-free languages (i.e. those languages of extended *-height 0) was subdivided according to the dot-depth measure introduced by Cohen and Brzozowski [71]. Simon [72] further refined this classification in his study of dot-depth one languages.

More recently, a different approach was used by Straubing [79]. He introduced a new operation on languages by counting certain factorizations of words. He thus obtained a characterization of those regular languages corresponding to solvable groups. Furthermore, his operation can be used to define hierarchies of families of languages which correspond to natural hierarchies of families of monoids. Combining his operation with concatenation, he was able to generate $\underline{M_{sol}}$, the variety of all monoids which contain only solvable groups.

In this thesis, Straubing's operation is extended in several directions. By using only this generalized counting method, we are able to systematically generate hierarchies of regular languages. Moreover, it is shown that several well-known families of monoids can be recovered by our construction. In particular, the limit of these hierarchies is the family of languages corresponding to $\underline{M_{sol}}$.

In this introduction, we first present some definitions and notation that will be used. This is followed by a section on varieties in which basic results on the relationship between languages, congruences and monoids are stated. Another section deals more specifically with monoids. Finally a summary of the results of this thesis is included.

I.1 Definitions and notation

We denote by $\mathbb{N}$ the infinite set $\{0,1,\ldots\}$ and by $|A|$ the cardinality of the set A. The set of all functions from B to A is A^B. The image of x under the function f is written (x)f (or xf for short) and functions compose from left to right, i.e. (x)fg = ((x)f)g. The set xff^{-1} is denoted by $[x]_f$.

For any $n \geq 0$, the set of all sequences of length n over a set A is written A^n; individual sequences are denoted by $(a_1,\ldots,a_n)$ if $n \geq 1$, and by () if n = 0. A^+ (A*) represents the set of all sequences of length ≥ 1 (≥ 0). For $x \in A^*$, we define $|x| = n$ iff $x \in A^n$.

A <u>semigroup</u> is a set S together with an associative binary operation which is often denoted simply by juxtaposition. This operation can be extended to subsets of S by defining $S_1S_2 = \{s_1s_2 : s_1 \in S_1, s_2 \in S_2\}$ for any $S_1, S_2 \subseteq S$. For convenience sS_1 and S_1s are written instead of $\{s\}S_1$ and $S_1\{s\}$, where $s \in S$ and $S_1 \subseteq S$. A <u>monoid</u> M is a semigroup with an <u>identity</u>, i.e. an element 1 such that 1m = m1 = m for all $m \in M$. A <u>group</u> G is a monoid in which every element g has an <u>inverse</u> g^{-1} satisfying $gg^{-1} = g^{-1}g = 1$; if G is finite this is equivalent to requiring the existence of an integer n such that $g^n = 1$ for all $g \in G$.

For any semigroup S, $T \subseteq S$, $s \in S$, the <u>left</u> (<u>right</u>) <u>derivative</u> of T by s is defined as $s^{-1}T = \{t \in S : st \in T\}$ ($Ts^{-1} = \{t \in S : ts \in T\}$). This notation is formal and does not imply that the element s is invertible but if it is then $s^{-1}T = \{s^{-1}\}T$ and $Ts^{-1} = T\{s^{-1}\}$.

For two semigroups S and T, $\phi \in T^S$ is a morphism if $(ss')\phi = (s\phi)(s'\phi)$ for all $s, s' \in S$. The morphism ϕ is surjective if $S\phi = T$. If S and T are monoids and $1\phi = 1$, ϕ is a monoid morphism: in this case, if S is a group, then $S\phi$ is also a group and $(s\phi)^{-1} = (s^{-1})\phi$. S is isomorphic with T, $S \simeq T$, if there exists a 1-1 surjective morphism from S to T.

An equivalence α on a set S is a binary relation (i.e. a subset of S^2) which is reflexive, symmetric, and transitive. α partitions S into disjoint equivalence classes and we write S/α for the set of those classes; $|S/\alpha|$ is the index of α. We will also use α to denote the natural projection from S onto S/α. We thus have $[s]_\alpha = s\alpha\alpha^{-1} = \{t : s \alpha t\}$. Conversely any function ϕ having S as domain induces an equivalence on S, also denoted by ϕ, defined by $s \phi t$ iff $s\phi = t\phi$.

If S is a semigroup, the equivalence α is a right (left) congruence iff $s \alpha t$ implies $su \alpha tu$ ($us \alpha ut$) for all $s, t, u \in S$; this is equivalent to requiring that $[s]_\alpha u^{-1}$ ($u^{-1}[s]_\alpha$) be a union of classes of α for all $u, s \in S$. α is a congruence iff it is both a right and a left congruence. The function $\alpha : S \to S/\alpha$ is then a morphism with the operation on S/α defined by $[s]_\alpha[t]_\alpha = [st]_\alpha$. Conversely if ϕ is a morphism having S as domain, then the equivalence ϕ is a congruence. The symbol $S\Gamma$ denotes the set of all congruences of finite index over S and ω_S (or ω if S is understood) represents the universal congruence, that is $s \omega_S t$ for all $s, t \in S$.

If α is a right congruence on a semigroup S, the following common representation will be used; classes of α are associated with vertices of a graph and there is an arrow labelled s from the vertex $[x]_\alpha$ to the vertex $[y]_\alpha$ iff $xs\ \alpha\ y$; normally only arrows labelled with some set of generators of S are given. If S is a monoid, the vertex corresponding to $[1]_\alpha$ is designated by an arrow coming out of no vertex.

Let A be any finite set. A^+ (A^*) becomes a semigroup (monoid) under the operation of concatenation defined by $(a_1,\ldots,a_n)(b_1,\ldots,b_m) = (a_1,\ldots,a_n,b_1,\ldots,b_m)$ (with () being the identity). In this context sequences are called words; we write $a_1\ldots a_n$ for $(a_1,\ldots,a_n)$ and λ for (). A language L over A^* is a subset of A^*. L is an α language iff L is a union of classes of α for some equivalence α on A^*, i.e. $L = L\alpha\alpha^{-1}$. Any language L is an α_L language where α_L is the congruence defined by

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

α_L is called the syntactic congruence and $M_L = A^*/\alpha_L$ is the syntactic monoid of L. Corresponding notions are defined when we consider languages to be subsets of A^+ instead of A^*; the syntactic semigroup, which may or may not be a monoid, is $S_L = A^+/\alpha_L$. A language L over A^* (A^+) is regular iff M_L (S_L) is finite. If L is regular then $x^{-1}L$ and Lx^{-1} are regular for any x in A^*; indeed one easily verifies that they are α_L languages.

For any semigroup S generated by a set A, there exists a natural surjective morphism $\alpha_S : A^+ \to S$ defined by $(a_1,\ldots,a_n)\alpha_S = a_1\ldots a_n$, with the operation on the right being that of S.

If S is a monoid we obtain a surjective monoid morphism $\alpha_S : A^* \to S$ by defining $\lambda\alpha_S = 1$. Observe that for all $s \in S$, $s\alpha_S^{-1}$ is a language over A^+ (or A^*) which consists of all sequences $(a_1,\ldots,a_n)$ which "multiply" to s.

A subset T of S is a subsemigroup of S iff $T^2 \subseteq T$. If T has an identity e then T is said to be a monoid in S; in this case e is necessarily an idempotent, i.e. $e^2 = e$. T is a submonoid of S if S is a monoid, T is a monoid in S, and the identity in T coincides with that of S. Every monoid in S is a submonoid of the monoid eSe for some idempotent e. We say that S is group-free (or aperiodic) if every group in S is a trivial one-element group. The notation $T \prec S$, read T is covered by S, will be used to indicate that T is an image of a subsemigroup of S under a morphism.

The reverse S^ρ of a semigroup is the set S together with the multiplication defined by $s \circ t = ts$. The reverse α^ρ of a congruence α on A^* is defined by $x\ \alpha^\rho\ y$ iff $x^\rho\ \alpha\ y^\rho$ where $\lambda^\rho = \lambda$ and $(xa)^\rho = ax^\rho$ for all $x \in A^*$, $a \in A$. The reverse L^ρ of a language L is $L^\rho = \{x^\rho : x \in L\}$.

For $m, n \in \mathbb{N}$, we write $m|n$ if m divides n. If K is a finite subset of $\mathbb{N}$, lcm K and max K are the least common multiple and the maximum respectively of the elements in K. If $K = \emptyset$, we define lcm K = 1 and max K = 0; if $K' \subseteq K$, lcm K' | lcm K and max K' $\leq$ max K. Observe that $\mathbb{N}$ is a monoid under the operation of addition. It can be viewed as a free monoid generated by the integer 1. There are essentially only two types of congruences in $\mathbb{N}$. For any $t \geq 0$, $q \geq 1$, let

$m \equiv n$ (thresh t) iff ((m < t and m = n) or (m ≥ t and n ≥ t))

and $m \equiv n$ (mod q) iff $q \mid m-n$.

One can verify that every congruence of finite index on $\mathbb{N}$ is the intersection of a threshold t congruence and a modulo q congruence. We will write $\theta_{t,q}$ for such a congruence on $\mathbb{N}$: $\mathbb{N}/\theta_{t,q}$ is represented in figure I.1 on the generator 1; it is a group iff t = 0 and it is a group-free monoid iff q = 1.

Proposition 1.1: Let $m,n,t_1,t_2 \geq 0$, $q_1,q_2 \geq 1$;

a) If $n \neq m$ there are a finite number of congruences $\theta \in \mathbb{N}\Gamma$ such that $n \theta m$;

b) for all $\theta \in \mathbb{N}\Gamma$ $0 \theta 1$ iff $\theta = \omega$;

c) $\theta_{t_1,q_1} \cap \theta_{t_2,q_2} = \theta_{\max\{t_1,t_2\},\mathrm{lcm}\{q_1,q_2\}}$;

d) $\theta_{t_1,q_1} \supseteq \theta_{t_2,q_2}$ iff $t_1 \leq t_2$ and $q_1 \mid q_2$.

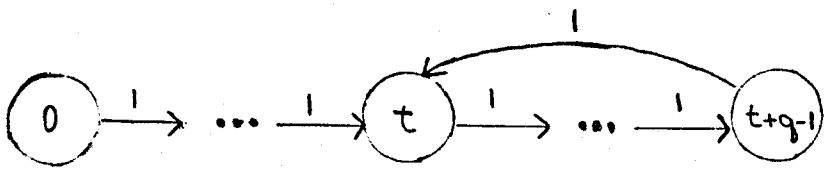


Fig. I.1: The cyclic monoid $\mathbb{N}/\theta_{t,q}$

I.2. Varieties

This section presents elementary notions that are relevant to the classification of regular languages by algebraic methods; it is largely inspired by Eilenberg [76]. The main result is Eilenberg's theorem giving conditions under which a family of regular languages can be characterized by the corresponding monoids. We express these conditions in terms of congruences since these will play a central role in our approach. In the sequel, all languages are regular, all congruences are of finite index, and all semigroups except A^+, A^*, $\mathbb{N}$ are finite. The concepts that follow are presented in terms of monoids but can be expressed in terms of semigroups.

A solution to the classification problem is most satisfying if we can arrange families of languages in hierarchies of increasing "complexity". Intuitively, the complexity of a congruence is related to its power of discriminating between words. Inclusion thus provides a natural order relation on $A^*\Gamma$, the largest element being ω. Note that, as congruences on A^*, $\alpha' \supseteq \alpha$ iff the corresponding morphisms are related by $\alpha' = \alpha\phi$, for some surjective monoid morphism $\phi : A^*/\alpha \to A^*/\alpha'$; we will use both notions interchangeably at our convenience. Also renaming the elements of a finite set B with elements of A^*, i.e. setting up a function $\phi : B \to A^*$, yields a natural renaming of the words in B^*, by extending ϕ to a monoid morphism $\phi : B^* \to A^*$. Any congruence α on A^* can then be used to discriminate between $u\phi$ and $v\phi$, for any $u, v \in B^*$ such that $u\phi \neq v\phi$. The induced congruence $\phi\alpha$ on B^* is no more complex than α in the intuitive sense that $\phi\alpha$ can discriminate between two words u and v in B^* iff α can discriminate between their

respective renamings $u\phi$ and $v\phi$ in A^*. Finally it is convenient to use a measure of complexity on congruences which is independent of the operation of finite intersection.

Now consider, for each finite set A, a family of congruences $A^*\Delta \subseteq A^*\Gamma$ and let Δ be the union over all A of these families. We say that Δ is a *-variety of congruences iff the following properties hold:

i) closure under composition by morphisms, i.e. if $\alpha \in A^*\Delta$, $\phi : B^* \to A^*$, $\phi' : A^*/\alpha \to T$ are monoid morphisms, then $\phi\alpha\phi' \in B^*\Delta$;

ii) closure under finite intersection, i.e. if $\alpha_1, \alpha_2 \in A^*\Delta$, then $\alpha_1 \cap \alpha_2 \in A^*\Delta$.

Example: Let Γ_x be defined by

$$A^*\Gamma_x = \{\alpha \in A^*\Gamma : \text{ there exists n such that } x^n \alpha \lambda \text{ for all } x \in A^*\} .$$

Let Γ_+ be defined by

$$A^*\Gamma_+ = \{\alpha \in A^*\Gamma : \text{ there exists n such that } x^n \alpha x^{n+1} \text{ for all } x \in A^*\} .$$

It is easily verified that Γ_x and Γ_+ form *-varieties of congruences. We refer to the elements of Γ_x and Γ_+ as group and aperiodic congruences respectively.

Proposition 2.1: Let $\alpha, \alpha' \in A^*\Gamma$, and $\phi : B^* \to A^*$ be a morphism:

a) if $\alpha' \supseteq \alpha$ then $|A^*/\alpha'| \leq |A^*/\alpha|$;

b) $|B^*/\phi\alpha| \leq |A^*/\alpha|$

c) $|A^*/(\alpha \cap \alpha')| \leq |A^*/\alpha| \cdot |A^*/\alpha'|$.

Proof: Clear. □

This last proposition shows that congruences of infinite index cannot be introduced by the operations mentioned above.

We can view Δ as defining a family of languages $\mathcal{L}$ which is the union, over all finite sets A, of

$$A^*\mathcal{L} = \{L \subseteq A^* : L \text{ is an } \alpha \text{ language, } \alpha \in A^*\Delta\}:$$

the notation $\Delta \to \mathcal{L}$ indicates that $\mathcal{L}$ is so defined.

Proposition 2.2: Let $L \subseteq A^*$; L is an α language iff $\alpha \subseteq \alpha_L$.

Proof: Clear. □

Proposition 2.3: Let $L, L_1, L_2 \subseteq A^*$, $\bar{L} = \{x \in A^* : x \notin L\}$, $z \in A^*$, and $\phi : B^* \to A^*$:

a) $\alpha_{\bar{L}} = \alpha_L$;

b) $\alpha_{L_1} \cap \alpha_{L_2} \subseteq \alpha_{(L_1 \cup L_2)}$;

c) $\alpha_L \subseteq \alpha_{z^{-1}L}$ and $\alpha_L \subseteq \alpha_{Lz^{-1}}$;

d) $\phi\alpha_L \subseteq \alpha_{L\phi^{-1}}$.

Proof: a) and b) are clear. To show c) suppose $x \alpha_L y$; then $uxv \in L$ iff $uyv \in L$ for all u, v in A*. In particular $zuxv \in L$ iff $zuyv \in L$, i.e. $uxv \in z^{-1}L$ iff $uyv \in z^{-1}L$. The second inclusion in c) follows by symmetry. To prove d) suppose $x \phi\alpha_L y$ for some x, y in B*; then $x\phi \alpha_L y\phi$ and for any u, v in B* $(uxv)\phi \alpha_L (uyv)\phi$. This implies that $(uxv)\phi \in L$ iff $(uyv)\phi \in L$ and thus $uxv \in L\phi^{-1}$ iff $uyv \in L\phi^{-1}$. It follows that $x \alpha_{L\phi^{-1}} y$. □

Proposition 2.4: Let $\Delta \to L$ where Δ is a *-variety of congruences; then L is closed under boolean operations, left and right derivatives and inverse morphisms.

Proof: This follows from proposition 2.3. □

Conversely let L be the union, over all finite sets A, of given families A^*L of languages over A*. L is said to be a *-variety of languages if it satisfies the properties stated in proposition 2.4. For any L, we write $L \to \Delta$ if Δ is the smallest *-variety of congruences containing the syntactic congruences of all languages in L.

A congruence $\alpha \in A^*\Gamma$ is syntactic iff there exists $L \subseteq A^*$ such that $\alpha = \alpha_L$.

Example: For $i \geq 1$, let $A_i = \{a_1,\ldots,a_i\}$ and let $\alpha_i \in A_i^*\Gamma$ be the congruence that partitions A_i^* as $\{\{\lambda\}, A_i^*a_1,\ldots,A_i^*a_i\}$.

If $i = 1,2, \alpha_i$ can be verified to be syntactic by taking $L = A_i^* a_1$. If $i \geq 3$, for any $I \subseteq \{1,\ldots,i\}$ let $L_I = \bigcup_{j \in I} A_i^* a_j$ and $L'_I = L_I \cup \{\lambda\}$. Any α_i language is equal to L_I or L'_I for some I; but $\alpha_{L_I} = \alpha_{L'_I}$ partitions A_i^* into $\{\{\lambda\}, \bigcup_{j \in I} A_i^* a_j , \bigcup_{j \notin I} A_i^* a_j\}$ thereby proving that α_i is not syntactic.

On the other hand, one can verify that every group congruence $\alpha \in A^* \Gamma_x$ is syntactic; indeed $\alpha = \alpha_L$ for $L = [x]_\alpha$ for any x in A^*.

A *-variety Δ of congruences is said to be <u>generated</u> by a subset Δ' if Δ is the smallest *-variety containing Δ'.

<u>Proposition 2.5</u>: *-varieties of congruences are generated by their syntactic elements.

Proof: Let $\alpha \in A^* \Delta$ and let $A^*/\alpha = \{[x_1],\ldots,[x_n]\}$. Since $[x_i]$ is an α language, $\alpha_{[x_i]} \supseteq \alpha$ and thus $\alpha_{[x_i]} \in A^* \Delta$ for $i = 1,\ldots,n$. If $x \alpha y$ does not hold for a pair of words x, y then neither does $x \alpha_{[x]} y$. Hence $\alpha_{[x_1]} \cap \ldots \cap \alpha_{[x_n]} \subseteq \alpha$ and therefore $\alpha_{[x_1]} \cap \ldots \cap \alpha_{[x_n]} = \alpha$. □

<u>Proposition 2.6</u>: If Δ is a *-variety of congruences and $\Delta \to L$ then $L \to \Delta$.

Proof: Suppose $L \to \Delta'$. To prove that $\Delta \subseteq \Delta'$ it is sufficient to show that some set of generators of Δ is contained in Δ' and this clearly holds for the set of syntactic congruences of Δ .

Conversely, Δ' is generated by the congruences α_L , $L \in \mathcal{L}$.
Since $\Delta \to \mathcal{L}$, L is an α language for some $\alpha \in A^*\Delta$ and $\alpha_L \in A^*\Delta$ as well since Δ is a *-variety and $\alpha \subseteq \alpha_L$. This implies that $\Delta = \Delta'$. □

Proposition 2.7: Let $\mathcal{L} \to \Delta$. Then $\alpha \in A^*\Delta$ iff there exists $L_i \in A_i^*\mathcal{L}$, $n \in \mathbb{N}$, $\phi_i : A^* \to A_i^*$ for $i = 1,\ldots,n$ such that $\alpha \supseteq \alpha_1 \cap \ldots \cap \alpha_n$ where $\alpha_i = \phi_i \alpha_{L_i}$.

Proof: The sufficiency of the condition is obvious. To see the converse suppose $\alpha \in A^*\Delta$: then α can be constructed from syntactic congruences of languages in $\mathcal{L}$ by using morphisms and intersections. We prove the result by induction on k, the number operations that are used. If $k = 0$, then $\alpha = \alpha_L$ for some $L \in \mathcal{L}$ and the result follows.

If $k > 0$, we consider three cases according to the last operator that is used.

i) $\alpha \supseteq \alpha'$ for some $\alpha' \in A^*\Delta$. We can apply the induction hypothesis on α', so that $\alpha' \supseteq \alpha_1 \cap \ldots \cap \alpha_n$, for some congruences α_i as defined in the proposition. Then $\alpha \supseteq \alpha_1 \cap \ldots \cap \alpha_n$ is seen to satisfy the condition.

ii) $\alpha = \phi\beta$ for some $\phi : A^* \to B^*$, $\beta \in B^*\Delta$. Applying the induction hypothesis on β, we have $\beta \supseteq \beta_1 \cap \ldots \cap \beta_n$ for appropriate β_i. Then $\alpha \supseteq \phi\beta_1 \cap \ldots \cap \phi\beta_n$ also has the correct form.

iii) $\alpha = \alpha_1 \cap \alpha_2$ for some $\alpha_1, \alpha_2 \in A^*\Delta$. Applying the induction hypothesis on α_1 and α_2, we have $\alpha_1 \supseteq \alpha_{11} \cap \ldots \cap \alpha_{1n}$, $\alpha_2 \supseteq \alpha_{21} \cap \ldots \cap \alpha_{2m}$ for appropriate α_{1i}, α_{2j}. Then $\alpha \supseteq \alpha_{11} \cap \ldots \cap \alpha_{1n} \cap \alpha_{21} \cap \ldots \cap \alpha_{2m}$ is again in correct form. □

If L is a *-variety of languages and $L \to \Delta$, the following stronger result can be derived: $\beta \in B^*\Delta$ iff $\beta = \phi_1(\alpha_{L_1} \cap \ldots \cap \alpha_{L_n})\phi_2$ for some $\phi_1 : B^* \to A^*$, $L_i \in A^*L$, $\phi_2 : A^*/(\alpha_{L_1} \cap \ldots \cap \alpha_{L_n}) \to M$.

Proposition 2.8: If L is a *-variety of languages and $L \to \Delta$ then $\Delta \to L$.

Proof: Let $\Delta \to L'$. If $L \in A^*L$ then $\alpha_L \in A^*\Delta$ and then $\Delta \to L'$ implies that $L \in A^*L'$; thus $L \subseteq L'$. Conversely suppose L is in A^*L'; L is an α language for some $\alpha \in A^*\Delta$ and by proposition 2.7 there exists $L_i \in A_i^*L$, $\phi_i : A^* \to A_i^*$ for $i = 1,\ldots,n$, so that $\alpha \supseteq \alpha_1 \cap \ldots \cap \alpha_n$ where $\alpha_i = \phi_i \alpha_{L_i}$. Hence $L = \bigcup_{x \in L} \bigcap_{i=1}^{n} [x]_{\alpha_i}$ and it is sufficient to show that $[x]_{\alpha_i} \in A^*L$ since L is closed under boolean operations. But $[x]_{\alpha_i} = ([x\phi_i]_{\alpha_{L_i}})\phi_i^{-1}$ and we only have to show that $[y]_{\alpha_{L_i}} \in A_i^*L$, for an arbitrary y in A_i^*. Now $z \, \alpha_{L_i} \, y$ iff $(uzv \in L_i$ iff $uyv \in L_i$ for all u, v in $A_i^*)$; thus $[y]_{\alpha_{L_i}} = \bigcap_{\substack{u,v \in A^* \\ uyv \in L_i}} u^{-1}L_iv^{-1} \cap \bigcup_{\substack{u,v \in A^* \\ uyv \notin L_i}} u^{-1}L_iv^{-1}$.

Closure of L under boolean operations and derivatives imply the result. □

The propositions 2.6 and 2.8 together prove that there is a 1-1 correspondence between *-varieties of congruences and *-varieties of languages given by $\Delta \to L$ and $L \to \Delta$.

Given a family of congruences Δ, we can also look at Δ from a more algebraic point of view, i.e. by considering the abstract monoids that correspond to congruences in Δ. Define $\Delta \to \underline{M}$ if $\underline{M} = \{M : M \simeq A^*/\alpha, \alpha \in A^*\Delta, \text{ for some } A\}$; conversely for any family of finite monoids $\underline{M}$ define $\underline{M} \to \Delta$ iff $A^*\Delta = \{\alpha \in A^*\Gamma : A^*/\alpha \simeq M, M \in \underline{M}\}$. Clearly $\underline{M} \to \Delta$ implies $\Delta \to \underline{M}$.

Conversely let $\Delta \to \underline{M}$ and $\underline{M} \to \Delta'$. It is clear that $\Delta \subseteq \Delta'$. Also if $\alpha \in A^*\Delta'$, there must exist $\beta \in B^*\Delta$ such that $B^*/\beta \simeq A^*/\alpha$ and then $\alpha = \phi\beta$, where, for any $x \in A^*$, $x\phi = w$ for some $w \in B^*$ such that $[w]_\beta$ is related to $[x]_\alpha$ by the isomorphism between B^*/β and A^*/α . Thus if Δ is a *-variety, $\Delta' = \Delta$.

The following relations between congruences and monoids are stated without proof.

Proposition 2.9: Let $\alpha, \alpha_1, \alpha_2 \in A^*\Gamma$, $\beta \in B^*\Gamma$ and $\phi : B^* \to A^*$;

a) if $\alpha_1 \supseteq \alpha_2$ then A^*/α_1 is a morphic image of A^*/α_2;

b) $B^*/\phi\alpha$ is isomorphic to a submonoid of A^*/α ;

c) $A^*/(\alpha_1 \cap \alpha_2) \prec A^*/\alpha_1 \times A^*/\alpha_2$.

Proposition 2.10: If Δ is a *-variety of congruences and $\Delta \to \underline{M}$ then $\underline{M}$ is closed under morphic images, submonoids and finite direct products.

Proposition 2.11: If $\underline{M}$ is closed under morphic images, submonoids and finite direct products, then $\underline{M} \to \Delta$ implies that Δ is a *-variety of congruences.

A family of monoids satisfying the properties stated in proposition 2.11 is called a variety of monoids. Proposition 2.10 and 2.11 together with the remarks preceding proposition 2.9 indicate that *-varieties of congruences and varieties of monoids are in 1-1 correspondence, given by $\Delta \to \underline{M}$ and $\underline{M} \to \Delta$, which we abbreviate as $\Delta \leftrightarrow M$. We also write $\Delta \hookrightarrow \underline{M}$ ($\underline{M} \hookrightarrow \Delta$) if $\Delta \to \underline{M}'$ for some $\underline{M}' \subseteq \underline{M}$ (if $\underline{M} \to \Delta'$ for some $\Delta' \subseteq \Delta$).

Example: Let $\underline{G} = \{M : M \text{ is a group}\}$ and $\underline{Ap} = \{M : M \text{ is group-free}\}$. $\underline{G}$ and $\underline{Ap}$ are varieties of monoids and $\underline{G} \leftrightarrow \Gamma_{\times}$, $\underline{Ap} \leftrightarrow \Gamma_{+}$.

Proposition 2.12: $\Delta \leftrightarrow \underline{M}$ iff $\Delta \hookrightarrow \underline{M}$ and $\underline{M} \hookrightarrow \Delta$.

Proof: The necessity of the condition follows directly from the definitions. Conversely $\Delta \hookrightarrow \underline{M}$ and $\underline{M} \leftrightarrow \Delta'$ imply $\Delta \subseteq \Delta'$. But $M \hookrightarrow \Delta$ implies $\Delta' \subseteq \Delta$ so that $\Delta = \Delta'$ and $M \leftrightarrow \Delta$. □

I.3 Elements of semigroup theory

In this section, more properties of monoids and groups are presented. References for the material of this section are Clifford and Preston [61] for results on semigroups and Hall [59], for properties specific to groups. Let M be an arbitrary monoid, $s, t \in M$; define the following preorders on M:

i) $s \leq_J t$ iff $MsM \subseteq MtM$

ii) $s \leq_R t$ iff $sM \subseteq tM$

iii) $s \leq_L t$ iff $Ms \subseteq Mt$

iv) $s \leq_H t$ iff $s \leq_R t$ and $s \leq_L t$.

For any preorder $\leq$ on M, we have an induced equivalence $s \equiv t$ iff $s \leq t$ and $t \leq s$. For any equivalence α on M, we say that M is <u>α-trivial</u> if $s \alpha t$ implies $s = t$. For example, $s \equiv_J t$ iff $MsM = MtM$ and M is <u>J-trivial</u> iff $MsM = MtM$ implies $s = t$. The notions above first appeared in Green [51].

M is a <u>commutative monoid</u> iff $st = ts$ for all $s,t \in M$. If M is commutative, the four order relations defined above coincide. The reader may observe that in the monoid $\langle \mathbb{N}, + \rangle$, the preorder $n \leq_J m$ (and thus each of the preorders $\leq_R$, $\leq_L$ and $\leq_H$) is the ordering $n \geq m$ of the integers.

Any group in M is a subset of a class of the equivalence $\equiv_H$.

If G is a group, any subgroup H induces a right (left) congruence on G defined by $g \alpha g'$ iff $Hg = Hg'$ ($gH = g'H$); note that $H = [1]_\alpha$. If, for all $g \in G$, $gH = Hg$, the subgroup H is said to be normal in G, which we write $G \triangleright H$ or $H \triangleleft G$, and α is a congruence. The image G/α is usually denoted G/H and if $G/H \simeq K$ then G is an extension of H by K.

A normal series of G is a sequence of nested subgroups of G such that

$$G_0 = G \triangleright G_1 \triangleright \ldots \quad .$$

Let Π be a set of primes: q is a Π-integer iff $q = p_1^{c_1} \ldots p_n^{c_n}$, $c_i \geq 1$, $p_i \in \Pi$. The element g of G has Π-order iff $g^q = 1$ for some Π-integer q. G is a Π-group iff every element of G has Π-order iff $|G|$ is a Π-integer. It may be verified that G_Π, the family of Π-groups is a variety. If $|G| = p^c q$ with p prime and p, q relatively prime, G has a subgroup (not necessarily normal) of cardinality p^c; any such subgroup is called a Sylow p-subgroup.

Commutative groups are also called abelian. The center of G is the normal subgroup

$$Z(G) = \{h : gh = hg \text{ for all } g \text{ in } G\} .$$

A normal series

$$Z_0 = \{1\} \triangleleft Z_1 \triangleleft \ldots \triangleleft Z_m = G$$

is a central series iff $Z_i/Z_{i-1} \subseteq Z(G/Z_{i-1})$ for $i = 1,\ldots,m$. If equality holds for each i, the resulting series is the upper central series and it is of shortest length among all central series of G. G is nilpotent of class m iff the upper central series has length m. Equivalently G is nilpotent iff it is the direct product of its Sylow p-subgroups.

The commutator of g and H is $[g,h] = g^{-1}h^{-1}gh$. For $H, K \subseteq G$ $[H,K]$ is the subgroup generated by all commutators of the form $h^{-1}k^{-1}hk$ $h \in H$, $k \in K$. The derived subgroup is $G_1 = [G, G]$; it is always the case that G/G_1 is abelian. The derived series of G is

$$G_0 = G \triangleright G_1 \triangleright \ldots$$

where $G_i = [G_{i-1},G_{i-1}]$. G is solvable of derived length n if n is the smallest integer such that $G_n = \{1\}$. In this case there also exists an integer $k \leq n$ and a series

$$G_0 = \{1\} \triangleleft G_1 \triangleleft \ldots \triangleleft G_k = G$$

such that G_i/G_{i-1} is the maximal nilpotent subgroup of G/G_{i-1} for $i = 1,\ldots,k$; G is then solvable of fitting length k.

Let G_{ab}, G_p for an arbitrary prime p, G_{nil} and G_{sol} denote respectively the family of abelian groups, p-groups, nilpotent groups and solvable groups. The following chains of inclusion hold:

$$\underline{G_{ab}} \subseteq \underline{G_{nil}} \subseteq \underline{G_{sol}}$$

$$\underline{G_{p}} \subseteq \underline{G_{nil}} \ .$$

Each of these families is a variety.

Often we will need to express properties of groups in terms of congruences. For any $\alpha,\beta \in A^*\Gamma_x$, $\alpha \subseteq \beta$, define $H_{\beta,\alpha} = \{[x]_\alpha : x \ \beta \ \lambda\}$.

Proposition 3.1: Let $\alpha \subseteq \beta \subseteq \gamma \in A^*\Gamma_x$;

i) $H_{\beta,\alpha} \lhd A^*/\alpha$

ii) $H_{\beta,\alpha} \lhd H_{\gamma,\alpha}$

iii) $H_{\gamma,\alpha}/H_{\beta,\alpha} \simeq H_{\gamma,\beta}$

Proof: Left to the reader. □

The terminology of semigroups will be applied to congruences whenever the context is clear. Thus we will speak of nilpotent congruences, J-trivial congruences, etc.

I.4 Synopsis

The correspondence between languages and monoids leads to the problem of establishing the translation between language properties and algebraic properties. One approach, much used in particular by Brzozowski and his collaborators, is to construct, in a systematical way, hierarchies of congruences and then investigate the corresponding families of languages and monoids. The constructions that have been used generally involve considering specific factorizations, i.e. we consider how a word is built from the letters of the underlying alphabet. Two words are then congruent iff they have similar factorizations. It is this approach that is taken in this thesis.

In chapter II, we introduce a construction that generates *-varieties of congruences. This construction is based on counting occurrences of subwords of length m with respect to a congruence $\theta_{t,q}$ on $\mathbb{N}$ and taking into account the context in which a subword appears with respect to a previously given congruence γ. Starting with $\gamma = \omega$ and applying the scheme recursively, our *-varieties are thus characterized by four parameters: the length m of subwords that are considered, the depth i of the recursion and the parameters t and q of the congruence on $\mathbb{N}$ with respect to which the counting is done; such a variety is denoted by $\Delta_{t,q}^{m,i}$. This is a natural approach as the simplest non-trivial *-varieties occur in the first step of this construction (i.e. by taking $m = i = 1$). It is also shown that, if $t = 0$, only group congruences are generated and, if $q = 1$, we obtain

only aperiodic congruences. In the general case, properties of $\Delta_{t,q}^{m,i}$ can be inferred by combining results on $\Delta_{0,q}^{m,i}$ and $\Delta_{t,1}^{m,i}$.

The following chapters investigate properties of the *-varieties introduced in chapter II. We adopt the convention that unless explicitly specified otherwise, m,i,t,q represents fixed, but arbitrary integers, $m,i,t \geq 0$, $q \geq 1$. Also we define $\Delta_{t,q}^{m,*} = \bigcup_{i \geq 0} \Delta_{t,q}^{m,i}$, and similarly for m, t and q.

In chapter III, we show that $\Delta_{0,*}^{*,1} \leftrightarrow \underline{G_{nil}}$ and we relate the intermediate $\Delta_{0,*}^{m,1}$ to the variety of nilpotent groups of class m. A method for constructing large families of normal subgroups of G from the corresponding congruences is indicated. Bounds on the *-height of the languages are derived. In chapter IV, the relation $\Delta_{*,1}^{*,1} \leftrightarrow \underline{J}$ is proved where $\underline{J}$ is the variety of J-trivial monoids. These congruence characterizations for $\underline{G_{nil}}$ and $\underline{J}$ complete results of Eilenberg [76] and Simon [72] respectively. We also examine the existing tradeoff between the various indices.

Chapters V and VI study the congruences in $\Delta_{0,q}^{m,i}$ and $\Delta_{t,1}^{m,i}$ respectively, for $i > 1$. It is shown that $\Delta_{0,*}^{*,*} \leftrightarrow \underline{G_{sol}}$ and $\Delta_{*,1}^{*,*} \leftrightarrow \underline{Ap}$. The intermediate *-varieties $\Delta_{0,*}^{1,i}$ and $\Delta_{0,*}^{*,i}$ are characterixed in terms of the derived length and fitting length respectively. Partial results on the corresponding aperiodic congruences $\Delta_{*,1}^{1,i}$ and $\Delta_{*,1}^{*,i}$ are given, which parallel those obtained in the group case. Also the original construction of congruences is modified to consider one-sided contexts only. It is shown that this modified construction still yields solvable

groups if modulo counting is used, but in the aperiodic case, R-trivial monoids are now generated.

In chapter VII, the general case is investigated. It is proved that $\Delta^{*,*}_{*,*} \leftrightarrow \underline{M_{sol}}$, the variety of monoids in which all groups are solvable. A relationship between threshold 1 counting of subwords in context and concatenation of languages is indicated.

Finally, we outline in the conclusion, a number of problems that remain unsolved.

II. GENERATING *-VARIETIES OF CONGRUENCES

In this chapter, various families of congruences are introduced and shown to be *-varieties. The congruences arise from counting the number of certain factorizations of words. The simplest congruences are those which count occurrences of letters (i.e. subwords of length 1) in words. These are generalized to count subwords of arbitrary length and to take into account the context in which the subword appears.

II.1 Letter counting congruences

In this section, it is shown that the simplest non-trivial *-varieties of congruences consist of congruences counting the number of occurrences of letters, with respect to a congruence of finite index on $\mathbb{N}$.

The family of congruences Ω defined by $A^*\Omega = \{\omega_{A^*}\}$ forms a *-variety which is in correspondence with $\underline{1}$, the variety of monoids consisting of the trivial monoid alone.

For any $\alpha \in A^*\Gamma$, $x \in A^*$, there exists $t \geq 0$, $q \geq 1$, such that $x^t \alpha x^{t+q}$. Let Δ be any *-variety such that $\alpha \in A^*\Delta$. For any alphabet B, $b \in B$, consider the morphism $\phi : B^* \to A^*$ defined by $b\phi = x$ and $b'\phi = \lambda$ for all $b' \in B - \{b\}$. Two words $y_1, y_2 \in B^*$ are $\phi\alpha$ congruent iff $\binom{y_1}{b} \theta_{t,q} \binom{y_2}{b}$ where $\binom{y}{b} \in \mathbb{N}$ is the number of occurrences of the letter b in y. Thus for any A the family $A^*\Delta$ must contain congruences that can count (with respect to $\theta_{t,q}$) occurrences of letters.

Let $\alpha_{t,q} \in A^*\Gamma$ be defined by:

$$x \ \alpha_{t,q} \ y \ \text{ iff } \binom{x}{a} \ \theta_{t,q} \ \binom{y}{a} \quad \text{for all } a \in A .$$

We will use the notation $\beta_{t,q}$ for the corresponding congruence over B^* . Let $\Delta_{t,q}$ be defined by $A^*\Delta_{t,q} = \{\alpha : \alpha \supseteq \alpha_{t,q}\}$.

Theorem 1.1: For any $t \geq 0$, $q \geq 1$, $\Delta_{t,q}$ is a *-variety of congruences.

Proof: It follows from the definition that for any $\alpha, \alpha' \in A^*\Delta_{t,q}$, $\phi : A^*/\alpha \to M$, we have $\alpha \cap \alpha' \in A^*\Delta_{t,q}$ and $\alpha\phi\varepsilon\ A^*\Delta_{t,q}$. Let $\phi : B^* \to A^*$, $\alpha \in A^*\Delta_{t,q}$; it must be shown that $\phi\alpha \supseteq \beta_{t,q}$. Since $\alpha \supseteq \alpha_{t,q}$, it is sufficient to show that $\phi\alpha_{t,q} \supseteq \beta_{t,q}$. It is easily seen that for any $x, y \in B^*$,

$$\binom{x\phi}{a} = \sum_{b \in B} \binom{x}{b} \binom{b\phi}{a}$$

$$\binom{y\phi}{a} = \sum_{b \in B} \binom{y}{b} \binom{b\phi}{a} \quad .$$

Assuming $x\ \beta_{t,q}\ y$, we have $\binom{x}{b}\ \theta_{t,q}\ \binom{y}{b}$ for all $b \in B$. Thus $\binom{x}{b}\binom{b\phi}{a}\ \theta_{t,q}\ \binom{y}{b}\binom{b\phi}{a}$ and $\binom{x\phi}{a}\ \theta_{t,q}\binom{y\phi}{a}$. Hence $\Delta_{t,q}$ is a *-variety. □

It is easily verified that for any $x,y \in A^*$, $a \in A$, $\binom{xy}{a} = \binom{x}{a} + \binom{y}{a}$. In particular $\binom{x^n}{a} = n\binom{x}{a}$ and consequently $x^t\ \alpha_{t,q}\ x^{t+q}$ for all $x \in A^*$; by considering the case $x = a \in A$, it is seen that these exponents are the best possible.

Lemma 1.1 : i) $\Delta_{0,1} = \Omega$

ii) $\Delta_{t,q} \subseteq \Gamma_x$ iff $t = 0$;

iii) $\Delta_{t,q} \subseteq \Gamma_+$ iff $q = 1$;

iv) $\Delta_{t,q} \subseteq \Delta_{t',q'}$ iff $t \leq t'$ and $q|q'$.

Proof: The first three statements follow from the property $x^t \alpha_{t,q} x^{t+q}$ for all $x \in A^*$. To prove iv) we have $\Delta_{t,q} \subseteq \Delta_{t',q'}$ iff $A^*\Delta_{t,q} \subseteq A^*\Delta_{t',q'}$ for any A : this holds iff $\alpha_{t,q} \supseteq \alpha_{t',q'}$, iff $\theta_{t,q} \supseteq \theta_{t',q'}$, iff $t \leq t'$, $q|q'$. □

Lemma 1.2 : If Δ is any non-trivial *-variety of congruences, then $\Delta_{0,p} \subseteq \Delta$ for some prime p or $\Delta_{1,1} \subseteq \Delta$.

Proof: Let $\alpha \neq \omega \in A^*\Delta$. There exists $x \in A^*$, $t \geq 0$, $q \geq 1$, $(t,q) \neq (0,1)$, such that $x^t \alpha x^{t+q}$. The argument preceding theorem 1.1 can be used to imply that for any B, $\beta_{t,q} \in B^*\Delta$. Thus $\Delta_{t,q} \subseteq \Delta$. If $t = 0$, it must be that $q > 1$; for any prime p dividing q we then have $\Delta_{0,p} \subseteq \Delta_{t,q} \subseteq \Delta$. If $t > 0$, $\Delta_{1,1} \subseteq \Delta_{t,q} \subseteq \Delta$. □

Monoid characterization for the varieties $\Delta_{t,q}$ are easily derived. Let $\underline{M_{com}}$ be the variety of commutative monoids and $\underline{M_{t,q}}$ be the variety of all monoids M in which $m^{t+q} = m^t$ for all $m \in M$.

Theorem 1.2: For all $t \geq 0$, $q \geq 1$, $\Delta_{t,q} \leftrightarrow \underline{M_{com}} \cap \underline{M_{t,q}}$.

Proof: Let $\alpha \in A^*\Delta_{t,q}$. Then $\alpha \supseteq \alpha_{t,q}$. Thus $x^{t+q}\ \alpha\ x^t$ for all $x \in A^*$. Also $\binom{xy}{a} = \binom{x}{a} + \binom{y}{a} = \binom{yx}{a}$ so that $xy\ \alpha_{t,q}\ yx$ and $xy\ \alpha\ yx$. This shows that $\Delta_{t,q} \hookrightarrow \underline{M_{com}} \cap \underline{M_{t,q}}$.

Conversely let $M \in \underline{M_{com}} \cap \underline{M_{t,q}}$ be generated by the set A. It is sufficient to show that $\alpha_M \in A^*\Gamma$ is in $\Delta_{t,q}$. Using the commutativity of M, we have, for any $x \in A^*$, $x\ \alpha_M\ a_1^{\binom{x}{a_1}} \ldots a_n^{\binom{x}{a_n}}$ where $A = \{a_1,\ldots,a_n\}$. Using the second property of M, it is seen that $x\ \alpha_M\ a_1^{c_1} \ldots a_n^{c_n}$ where $c_i = [\binom{x}{a_i}]_{\theta_{t,q}}$ for $i = 1,\ldots,n$. Thus if $x\ \alpha_{t,q}\ y$, we have $x\ \alpha_M\ a_1^{c_1} \ldots a_n^{c_n}\ \alpha_M\ y$. Hence $\alpha_M \in A^*\Delta_{t,q}$ and $\underline{M_{com}} \cap \underline{M_{t,q}} \hookrightarrow \Delta_{t,q}$. By proposition I.2.12 we conclude that $\Delta_{t,q} \leftrightarrow \underline{M_{com}} \cap \underline{M_{t,q}}$. □

Corollary 1.1 : i) $\Delta_{*,1} \leftrightarrow \underline{Ap} \cap \underline{M_{com}}$

ii) $\Delta_{0,*} \leftrightarrow \underline{G_{ab}}$;

iii) $\Delta_{*,*} \leftrightarrow \underline{M_{com}}$.

A complete description of all *-varieties of commutative congruences can be obtained. Let $\{p_1,p_2,\ldots\}$ be an enumeration of all prime numbers, and extend the order relation $\leq$ on $\mathbb{N}$ to the set $\mathbb{N}\cup\{*\}$ by defining $n \leq *$ for all $n \in \mathbb{N}$. Consider the set $N = \{(n_0,n_1,\ldots) : n_i \in \mathbb{N}\cup\{*\}\}$, and for $N = (n_0,n_1,\ldots)$, $N' = (n_0',n_1',\ldots) \in N$, define $N\leq N'$ iff $n_j \leq n_j'$ for all $j\geq 0$. Also define

$A^*\Delta_N = \{\alpha : \alpha \supseteq \alpha_{t,q}$ such that $q = p_{i_1}^{c_1}\ldots p_{i_r}^{c_r}$, $t\leq n_0$, $c_j \leq n_{i_j}$ for $j=1,\ldots,r\}$.

Lemma 1.3: Let $N, N' \in N$;

i) Δ_N is a *-variety of congruences;

ii) $\Delta_N \subseteq \Gamma_+$ iff $n_j=0$ for all $j\geq 1$;

iii) $\Delta_N \subseteq \Gamma_\times$ iff $n_0=0$;

iv) $\Delta_N \subseteq \Delta_{N'}$ iff $N\leq N'$;

v) if Δ is a *-variety of abelian congruences, then $\Delta = \Delta_N$ for some $N \in N$.

Proof: The proof is straightforward and it is omitted. □

This lemma provides a complete description of the lattice of *-varieties of commutative congruences ordered by inclusion.

II.2 Generating *-varieties of congruences by counting subwords in context.

In this section, we first extend the concept of counting letters to counting subwords of arbitrary length. We further refine this notion by taking into consideration the context in which a given subword appears in a word. This is shown to lead to *-varieties of congruences and basic properties of this construction are investigated.

The following definition and lemma are borrowed from Eilenberg [76].

Let $u = a_1 \ldots a_m$, $a_i \in A$, $m \geq 0$, $x \in A^*$;

$$\binom{x}{u} = \begin{cases} 1 & \text{if } u = \lambda \text{ (i.e. } m = 0) \\ \text{the number of factorizations of } x \text{ of the form} & \\ x = x_0 a_1 x_1 \ldots a_m x_m \text{ , } x_i \in A^* \text{ , otherwise.} & \end{cases}$$

This notation agrees with our definition of $\binom{x}{a}$ when $m = 1$.

Lemma 2.1: Let $u, x, y \in A^*$, $a \in A$. Then

i) $$\binom{xy}{u} = \sum_{u=u_1u_2} \binom{x}{u_1}\binom{y}{u_2} \text{ ;}$$

ii) $$\binom{a}{u} = \begin{cases} 1 & \text{if } u=\lambda \text{ or } u = a \\ 0 & \text{otherwise;} \end{cases}$$

iii)
$$\binom{\lambda}{u} = \begin{cases} 1 & \text{if } u=\lambda \\ 0 & \text{otherwise .} \end{cases}$$

Example: If x = abbab, u = ab, then

$$\binom{x}{u} = 4 \quad \text{since} \quad x = \lambda\, \underline{a}\, \lambda\, \underline{b}\, bab\ ,$$
$$x = \lambda\, \underline{a}\, b\, \underline{b}\, ab\ ,$$
$$x = \lambda\, \underline{a}\, bba\, \underline{b}\, \lambda\ ,$$
$$\text{and} \quad x = abb\, \underline{a}\, \lambda\, \underline{b}\, \lambda\ .$$

As the notation suggests, this concept constitutes an extension of the binomial coefficients to free monoids on more than one generator. Indeed for words in $\{a\}^*$ we have $\binom{a^n}{a^m} = \binom{n}{m}$. Many properties of the binomial coefficients have direct counterparts in this more general setting. For example the familiar identity

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

becomes

$$\binom{xb}{ua} = \begin{cases} \binom{x}{ua} + \binom{x}{u} & \text{if } b = a \\ \binom{x}{ua} & \text{otherwise .} \end{cases}$$

If $A = \{a_1,\ldots,a_n\}$, the notion above gives rise to a morphism from A^* into the multiplicative monoid of $\mathbb{N}[A]$, the semiring of polynomials in the non-commuting variables $a_1,\ldots,a_n$ with coefficients in $\mathbb{N}$. The morphism is induced by the mapping $a\phi = 1+a$ for all $a \in A$, and for any $x \in A^*$ we have $x\phi = \sum_{u\in A^*} \binom{x}{u} u$.

We now introduce congruences related to subword counting. For any $m \geq 0$, $t \geq 0$, $q \geq 1$, $x, y \in A^*$, let

$$x\ \alpha^m_{t,q}\ y \text{ iff } \text{ for all } u \in (A\cup\lambda)^m,\ \binom{x}{u}\ \theta_{t,q}\ \binom{y}{u} .$$

Lemma 2.2: For any $m \geq 0$, $t \geq 0$, $q \geq 1$, $\alpha^m_{t,q} \in A^*\Gamma$.

Proof: Let $x_1\ \alpha^m_{t,q}\ y_1$, $x_2\ \alpha^m_{t,q}\ y_2$. Then for any $u \in (A\cup\lambda)^m$, by lemma 2.1,

$$\binom{x_1x_2}{u} = \sum_{u=u_1u_1} \binom{x_1}{u_1}\binom{x_2}{u_2} .$$

Since for any $u_1, u_2 \in (A\cup\lambda)^m$, we have $\binom{x_1}{u_1}\ \theta_{t,q}\ \binom{y_1}{u_1}$ and $\binom{x_2}{u_2}\ \theta_{t,q}\ \binom{y_2}{u_2}$, it follows that $\binom{x_1x_2}{u}\ \theta_{t,q}\ \binom{y_1y_2}{u}$. Also the index of $\alpha^m_{t,q}$ is bounded by $|\mathbb{N}/\theta_{t,q}|\ |(A\cup\lambda)^m| = (t+q)\ |(A\cup\lambda)^m|$, so that $\alpha^m_{t,q} \in A^*\Gamma$. □

It is clear that $\alpha^1_{t,q} = \alpha_{t,q}$ as defined in section 1.

We now show how to refine this notion of subword counting by taking into account the context in which u appears in x, i.e. by considering the intermediate segments $x_0,\ldots,x_m$ in the factorization $x = x_0a_1x_1 \cdots a_mx_m$.

Let $\gamma \in A^*\Gamma$, $u = a_1\ldots a_m$, $x \in A^*$, $V = ([v_0]_\gamma,\ldots,[v_m]_\gamma) \in (A^*/\gamma)^{|u|+1}$. Define

$$\binom{x}{u}_V = \begin{cases} 1 \text{ if } u = \lambda \text{ and } x\ \gamma\ v_0 , \\ \text{the number of factorizations of } x \text{ in the form} \\ x = x_0a_1x_1 \cdots a_mx_m \text{ , with } x_i\ \gamma\ v_i \text{ for } i = 0, \\ \ldots,m \text{ otherwise.} \end{cases}$$

For any $n \geq 1$, we call the elements of $(A^*/\gamma)^n$ <u>γ-contexts</u>. We introduce the following operation on <u>γ-contexts</u>. If

$V = ([v_0]_\gamma,\ldots,[v_m]_\gamma) \in (A^*/\gamma)^{m+1}$ and $V' = ([v'_0]_\gamma,\ldots,[v'_n]_\gamma) \in (A^*/\gamma)^{n+1}$,

then

$$VV' = ([v_0]_\gamma,\ldots,[v_{(m-1)}]_\gamma,\ [v_mv'_0]_\gamma\ ,\ [v'_1]_\gamma,\ldots,[v'_n]_\gamma) \in (A^*/\gamma)^{m+n+1} .$$

<u>Lemma 2.3</u>: Let $u, x, y \in A^*$, $a \in A$, $\gamma \in A^*\Gamma$, $V \in (A^*/\gamma)^{|u|+1}$. Then

i) $$\binom{xy}{u}_V = \sum_{\substack{u=u_1u_2 \\ V=V_1V_2}} \binom{x}{u_1}_{V_1} \binom{y}{u_2}_{V_2} ;$$

ii) $\binom{a}{u}_V = \begin{cases} 1 & \text{if } (u=\lambda \text{ and } V=([a]_\gamma)) \\ & \text{or } (u=a \text{ and } V=([\lambda]_\gamma,[\lambda]_\gamma)) \\ 0 & \text{otherwise ;} \end{cases}$

iii) $\binom{\lambda}{u}_V = \begin{cases} 1 & \text{if } u=\lambda \text{ and } V = ([\lambda]_\gamma) \\ 0 & \text{otherwise .} \end{cases}$

Proof: Left to the reader. □

Counting subwords in context induces the following equivalence on A^*. Let $\gamma \in A^*\Gamma$, $m \geq 0$, $t \geq 0$, $q \geq 1$, $x, y \in A^*$: define

$$x \ \gamma(\alpha^m_{t,q}) \ y \text{ iff for all } u \in (A \cup \lambda)^m \text{ , for all } V \in (A^*/\gamma)^{|u|+1} \text{ ,}$$

$$\binom{x}{u}_V \ \theta_{t,q} \ \binom{y}{u}_V \ .$$

Lemma 2.4: For any $\gamma \in A^*\Gamma$, $m \geq 0$, $t \geq 0$, $q \geq 1$, $\gamma(\alpha^m_{t,q}) \in A^*\Gamma$.

Proof: Let $x_1 \ \gamma(\alpha^m_{t,q}) \ y_1$, $x_2 \ \gamma(\alpha^m_{t,q}) \ y_2$.

Then for any $u \in (A \cup \lambda)^m$, $V \in (A^*/\gamma)^{|u|+1}$, we have

$$\binom{x_1x_2}{u}_V = \sum_{\substack{u=u_1u_2 \\ V=V_1V_2}} \binom{x_1}{u_1}_{V_1} \binom{x_2}{u_2}_{V_2}$$

by lemma 2.3. Since $\binom{x_1}{u_1}_{V_1} \theta_{t,q} \binom{y_1}{u_1}_{V_1}$ and $\binom{x_2}{u_2}_{V_2} \theta_{t,q} \binom{y_2}{u_2}_{V_2}$, it follows that $\binom{x_1x_2}{u}_V \theta_{t,q} \binom{y_1y_2}{u}_V$. Also the index of $\gamma(\alpha^m_{t,q})$ is bounded by $|\mathbb{N}/\theta_{t,q}|(\sum_{u\in(A\cup\lambda)^m} |A^*/\gamma|^{|u|+1}) = (t+q)(\sum_{u\in(A\cup\lambda)^m} |A^*/\gamma|^{|u|+1})$, so that $\gamma(\alpha^m_{t,q}) \in A^*\Gamma$. □

The reader may verify that, for any $\gamma \in A^*\Gamma$, $t \geq 0$, $q \geq 1$, $(t,q) \neq (0,1)$, $m \geq 0$, we have $\gamma(\alpha^0_{t,q}) = \gamma$ and $\gamma(\alpha^m_{0,1}) = \omega$. Also $\omega(\alpha^m_{t,q})$ can be identified with our previous definition of $\alpha^m_{t,q}$.

Lemma 2.5: Let $\gamma \supseteq \gamma' \in A^*\Gamma$, $0\leq t\leq t'$, $1 \leq q|q'$ and $0\leq m\leq m'$. Then $\gamma(\alpha^m_{t,q}) \supseteq \gamma'(\alpha^{m'}_{t',q'})$.

Proof: Let $x\ \gamma'(\alpha^{m'}_{t',q'})\ y$. Also let $u \in (A\cup\lambda)^m$,

$V = ([v_0]_\gamma,\ldots,[v_{|u|}]_\gamma) \in (A^*/\gamma)^{|u|+1}$

and $V' = \{([v'_0]_{\gamma'},\ldots,[v'_{|u|}]_{\gamma'}) : v'_i\ \gamma\ v_i,\ i=0,\ldots,|u|\}$; the set V' is well defined because $\gamma \supseteq \gamma'$. Now $\binom{x}{u}_V = \sum_{V'\in V'} \binom{x}{u}_{V'}$ and $\binom{y}{u}_V = \sum_{V'\in V'} \binom{y}{u}_{V'}$. Since $\binom{x}{u}_{V'}\ \theta_{t',q'}\ \binom{y}{u}_{V'}$ for all $V' \in V'$, it follows that $\binom{x}{u}_{V'}\ \theta_{t,q}\ \binom{y}{u}_{V'}$ and $\binom{x}{u}_V\ \theta_{t,q}\ \binom{y}{u}_V$. Thus $x\ \gamma(\alpha^m_{t,q})\ y$. □

Corollary 2.1: Let $\gamma, \gamma' \in A^*\Gamma$, $0 \le t,t'$, $1 \le q,q'$, $0 \le m,m'$, $\max\{t,t'\} \le t''$, $\mathrm{lcm}\{q,q'\} \mid q''$, and $\max\{m,m'\} \le m''$. Then

$$\gamma(\alpha^m_{t,q}) \cap \gamma'(\alpha^{m'}_{t',q'}) \supseteq (\gamma \cap \gamma')\ (\alpha^{m''}_{t'',q''}) \ .$$

Proof: From lemma 2.5, it follows that $\gamma(\alpha^m_{t,q})$ and $\gamma'(\alpha^{m'}_{t',q'})$ both contain $(\gamma \cap \gamma')(\alpha^{m''}_{t'',q''})$. □

We extend the construction to *-varieties of congruences. For any *-variety Δ, m, $t \ge 0$, $q \ge 1$, define $\Delta(\Delta^m_{t,q})$ by

$$A^*\Delta(\Delta^m_{t,q}) = \{\alpha : \alpha \supseteq \gamma(\alpha^m_{t,q}) \ , \ \gamma \in A^*\Delta\} \ .$$

Lemma 2.6: For any *-variety Δ , m, $t \ge 0$, $q \ge 1$, $\Delta(\Delta^m_{t,q})$ is a *-variety of congruences.

Proof: If $\alpha \supseteq \alpha'$ and $\alpha' \in A^*\Delta(\Delta^m_{t,q})$, then $\alpha \in A^*\Delta(\Delta^m_{t,q})$. If $\alpha \supseteq \gamma(\alpha^m_{t,q})$ and $\alpha' \supseteq \gamma'(\alpha^m_{t,q})$ for some $\gamma, \gamma' \in A^*\Delta$ then $\alpha \cap \alpha' \supseteq \gamma(\alpha^m_{t,q}) \cap \gamma'(\alpha^m_{t,q}) \supseteq (\gamma \cap \gamma')(\alpha^m_{t,q})$ by corollary 2.1 . Thus $\alpha \cap \alpha' \in \Delta(\Delta^m_{t,q})$ since $\gamma \cap \gamma' \in \Delta$. Now let $\phi : B^* \to A^*$ and $\alpha \in A^*\Delta(\Delta^m_{t,q})$; thus $\alpha \supseteq \gamma(\alpha^m_{t,q})$ for some $\gamma \in A^*\Delta$, and $\phi\alpha \supseteq \phi(\gamma(\alpha^m_{t,q}))$. To show that $\phi\alpha \in B^*\Delta(\Delta^m_{t,q})$, it is sufficient to establish that $\phi(\gamma(\alpha^m_{t,q})) \supseteq (\phi\gamma)(\alpha^m_{t,q})$. If $t = 0$, $q = 1$, there is nothing to prove as both congruences are ω . Otherwise let $x\ (\phi\gamma)(\alpha^m_{t,q})\ y$ for some $x, y \in B^*$ and let $u = a_1 \ldots a_r \in (A \cup \lambda)^m$, $V = ([v_0]_\gamma, \ldots, [v_r]_\gamma) \in (A^*/\gamma)^{|u|+1}$. We must show that

$\binom{x\phi}{u}_V \ \theta_{t,q} \ \binom{y\phi}{u}_V$. If $u = \lambda$, $\binom{x\phi}{u}_V = 1$ iff $x\phi \ \gamma \ v_0$ and $\binom{x\phi}{u}_V = 0$ otherwise; but $x\phi \ \gamma \ y\phi$ so that $\binom{y\phi}{\lambda}_V = 1$ iff $y\phi \ \gamma \ v_0$ and $\binom{y\phi}{\lambda} = 0$ otherwise. Thus $\binom{x\phi}{\lambda}_V \ \theta_{t,q} \ \binom{y\phi}{\lambda}_V$. If $u \in A^+$, any factorization of $x\phi = (b_1\phi)\ldots(b_n\phi)$ as $x\phi = z_0a_1z_1\ldots a_rz_r$ determines uniquely a factorization of u as $u = u_1\ldots u_s$, $u_i \in A^+$ for $i = i,\ldots,s$, such that u_i is a subword of $b_{j_i}\phi$, for $1 \le j_1 < j_2 < \ldots < j_s \le n$. Moreover if $V_i = ([v_{i0}]_\gamma,\ldots[v_{i|u_i|}]_\gamma)$ denotes the context in which u_i appears in $b_{j_i}\phi$, we have

$$([(b_1\phi) \ \ldots \ (b_{j_1-1}\phi)]_\gamma)V_1([b_{j_1+1}\phi) \ \ldots \ (b_{j_2-1}\phi)]_\gamma)\ldots V_s([(b_{j_s+1})\phi \ \ldots \ (b_n\phi)]_\gamma) =$$

$$([z_0]_\gamma \ ,\ldots, \ [z_r]_\gamma) \ .$$

Conversely any factorization of u as $u = u_1\ldots u_s$, $u_i \in A^+$ a subword of $b_{j_i}\phi$ for $i = 1,\ldots, s$, determines a unique occurrence of u in $x\phi$ with the contexts satisfying the property above. Thus

$$\binom{x\phi}{u}_V = \sum_{s=1}^{|u|} \sum \binom{x}{b_{j_1}\ldots b_{j_s}}_{V'} \binom{b_{j_1}\phi}{u_1}_{V_1} \ \ldots \ \binom{b_{j_s}\phi}{u_s}_{V_s}$$

where the inner sum extends over all $u = u_1\ldots u_s$, $u_i \in A^+$, $b_{j_1}\ldots b_{j_s} \in B^s$, $V' = ([w_0]_{\phi\gamma} \ ,\ldots, \ [w_s]_{\phi\gamma}) \in (B^*/\phi\gamma)^{s+1}$, $V_i \in (A^*/\gamma)^{|u_i|+1}$ for $i = 1,\ldots, s$, such that $V = ([w_0\phi]_\gamma)V_1([w_1\phi]_\gamma)\ldots V_s([w_s\phi]_\gamma)$. Note that $w \ \phi\gamma \ w'$ implies $w\phi \ \gamma \ w'\phi$ so that the sum is well-defined. Since $x \ (\phi\gamma)(\alpha^m_{t,q}) \ y$, we have

$$\binom{x}{b_{j_1}\ldots b_{j_s}}_{V'} \quad \theta_{t,q} \quad \binom{y}{b_{j_1}\ldots b_{j_s}}_{V'}$$

for any $b_{j_1} \ldots b_{j_s} \in B^s$, $V' \in (B^*/\phi\gamma)^{s+1}$. This in turn implies that

$$\binom{x\phi}{u}_V \quad \theta_{t,q} \quad \binom{y\phi}{u}_V \ . \ \square$$

The definition of counting subwords in context is now applied recursively. For any *-variety Δ , m, $t \geq 0$, $q \geq 1$, let

$$\Delta(\Delta^{m,0}_{t,q}) = \begin{cases} \Omega & \text{if } t = 0 \text{ and } q = 1 \\ \Delta & \text{otherwise} , \end{cases}$$

and for $i \geq 1$, $\Delta(\Delta^{m,i}_{t,q}) = (\Delta(\Delta^{m,i-1}_{t,q}))(\Delta^{m}_{t,q})$

Theorem 2.1: For any Δ , m , i, $t \geq 0$, $q \geq 1$, $\Delta(\Delta^{m,i}_{t,q})$ is a *-variety of congruences.

Proof: The result trivially holds for $i = 0$ and arbitrary m, $t \geq 0$, $q \geq 1$. The proof is completed by induction on i, using lemma 2.6 . $\square$

Lemma 2.7: For any *-variety Δ , m, i, $t \geq 0$, $q \geq 1$,

$$A^*\Delta(\Delta^{m,i}_{t,q}) = \{\alpha : \alpha \supseteq \gamma(\alpha^{m,i}_{t,q}) \ , \ \gamma \in A^*\Delta\} \ ,$$

where $\gamma(\alpha^{m,0}_{t,q}) = \begin{cases} \omega & \text{if } t=0 \text{ and } q=1 \\ \gamma & \text{otherwise} \end{cases}$

and $\gamma(\alpha_{t,q}^{m,i}) = (\gamma(\alpha_{t,q}^{m,i-1}))(\alpha_{t,q}^{m})$.

Proof: The lemma is easily established when $i = 0,1$. For $i > 1$, $\alpha \in A^*\Delta(\Delta_{t,q}^{m,i})$ iff $\alpha \supseteq \gamma'(\alpha_{t,q}^{m})$ for some $\gamma' \in A^*\Delta(\Delta_{t,q}^{m,i-1})$. Assuming inductively that $\gamma' \supseteq \gamma(\alpha_{t,q}^{m,i-1})$ for some $\gamma \in A^*\Delta$, it follows from lemma 2.5 that $\alpha \supseteq (\gamma(\alpha_{t,q}^{m,i-1}))(\alpha_{t,q}^{m}) = \gamma(\alpha_{t,q}^{m,i})$. □

We now proceed to show that counting subwords of length m can always be simulated by counting subwords of length 1, provided we are willing to increase the recursive depth at which the contexts are taken.

Lemma 2.8: Let $\gamma \in A^*\Gamma$, $u = u_0 a u_1 \in A^+$, $x \in A^*$,

$V = ([v_0]_\gamma, \ldots, [v_{|u|}]_\gamma) \in (A^*/\gamma)^{|u|+1}$,

$V_0 = ([v_0]_\gamma, \ldots, [v_{|u_0|}]_\gamma) \in (A^*/\gamma)^{|u_0|+1}$,

$V_1 = ([v_{|u_0|+1}]_\gamma, \ldots, [v_{|u|}]_\gamma) \in (A^*/\gamma)^{|u_1|+1}$. Then

$$\binom{x}{u}_V = \sum_{x=x_0 a x_1} \binom{x_0}{u_0}_{V_0} \binom{x_1}{u_1}_{V_1} .$$

Proof: Left to the reader. □

Lemma 2.9: For any *-variety Δ , i, $t \geq 0$, $q \geq 1$, $\Delta(\Delta_{t,q}^{2^i-1,1}) \subseteq \Delta(\Delta_{t,q}^{1,i})$.

Proof: If $t = 0$, $q = 1$, then $\Delta(\Delta_{t,q}^{2^i-1,1}) = \Delta(\Delta_{t,q}^{1,i}) = \Omega$ for all $i \geq 0$. Suppose now that $t > 0$ or $q > 1$. If $i = 0$, then $\Delta(\Delta_{t,q}^{2^i-1,1}) = \Delta(\Delta_{t,q}^{1,i}) = \Delta$.

Now let $i > 0$ and assume inductively that $\Delta(\Delta_{t,q}^{2^{i-1}-1,1}) \subseteq \Delta(\Delta_{t,q}^{1,i-1})$. Let $\alpha \in A^*\Delta(\Delta_{t,q}^{2^i-1,1})$. By lemma 2.7, $\alpha \supseteq \gamma(\alpha_{t,q}^{2^i-1})$ for some $\gamma \in A^*\Delta$, and it is sufficient to show that $\gamma(\alpha_{t,q}^{2^i-1}) \supseteq \gamma(\alpha_{t,q}^{1,i})$ since $\gamma(\alpha_{t,q}^{1,i}) \in A^*\Delta(\Delta_{t,q}^{1,i})$. Let $x\ \gamma(\alpha_{t,q}^{1,i})\ y$ for some $x, y \in A^*$. Let $u \in A^*$ be of length $\leq 2^i-1$ and let $V = ([v_0]_\gamma, \ldots, [v_{|u|}]_\gamma) \in (A^*/\gamma)^{|u|+1}$. If $u = \lambda$, then $\binom{x}{u}_V\ \theta_{t,q}\ \binom{y}{u}_V$ iff $x\ \gamma\ y$; but $\gamma = \gamma(\alpha_{t,q}^{1,0}) \supseteq \gamma(\alpha_{t,q}^{1,i})$. Thus $x\ \gamma(\alpha_{t,q}^{1,i})\ y$ implies $\binom{x}{\lambda}_V\ \theta_{t,q}\ \binom{y}{\lambda}_V$. If $u \in A^+$, there exists a factorization of u as $u = u_0 a u_1$, $a \in A$, $|u_0|, |u_1| \leq 2^{i-1}-1$; then let $V_0 = ([v_0]_\gamma, \ldots, [v_{|u_0|}]_\gamma)$ and $V_1 = ([v_{|u_0|+1}]_\gamma, \ldots, [v_{|u|}]_\gamma)$. With these fixed V_0 and V_1, let, for any $0 \leq k_0, k_1 \leq q + t$,

$$V_{k_0,k_1} = \{([w_0]_{\gamma(\alpha_{t,q}^{1,i-1})}, [w_1]_{\gamma(\alpha_{t,q}^{1,i-1})}) : \binom{w_0}{u_0}_{V_0}\ \theta_{t,q}^{k_0}\ , \binom{w_1}{u_1}_{V_1}\ \theta_{t,q}^{k_1}\}.$$

Observe that by the induction hypothesis $\gamma(\alpha_{t,q}^{2^{i-1}-1}) \supseteq \gamma(\alpha_{t,q}^{1,i-1})$ so that the set V_{k_0,k_1} is well defined. By lemma 2.8, $\binom{x}{u}_V = \sum_{x=x_0 a x_1} \binom{x_0}{u_0}_{V_0} \binom{x_1}{u_1}_{V_1}$ and $\binom{y}{u}_V = \sum_{y=y_0 a y_1} \binom{y_0}{u_0}_{V_0} \binom{y_1}{u_1}_{V_1}$. Thus

$$\binom{x}{u}_V = \sum_{0\le k_0,k_1^{}\le t+q} \sum_{V'\in V_{k_0,k_1}} k_0 k_1 \binom{x}{a}_{V'} ,$$

and similarly for $\binom{y}{u}_V$.

Since $x\ \gamma(\alpha_{t,q}^{1,i})\ y$ we have $\binom{x}{a}_{V'}\ \theta_{t,q}\ \binom{y}{a}_{V'}$ for any $V' \in (A^*/\gamma(\alpha_{t,q}^{1,i-1}))^2$

and therefore $\binom{x}{u}_V\ \theta_{t,q}\ \binom{y}{u}_V$. This establishes that $\gamma(\alpha_{t,q}^{2^i-1}) \supseteq \gamma(\alpha_{t,q}^{1,i})$. □

Corollary 2.2: For any *-variety Δ, $m,i,\ t\ge 0$, $q \ge 1$, $\Delta(\Delta_{t,q}^{m,i}) \subseteq \Delta(\Delta_{t,q}^{1,i\lceil\log(m+1)\rceil})$, where the log is taken to base 2, and $\lceil n\rceil$ is least integer greater or equal to n.

Proof: The result is true when i=0 . If i>0 then $\Delta(\Delta_{t,q}^{m,i}) = (\Delta(\Delta_{t,q}^{m,i-1}))(\Delta_{t,q}^{m})$. We can assume inductively that $\Delta(\Delta_{t,q}^{m,i-1}) \subseteq \Delta(\Delta_{t,q}^{1,(i-1)\lceil\log(m+1)\rceil})$.

Applying lemma 2.9, we get

$$\Delta(\Delta_{t,q}^{m,i}) \subseteq (\Delta(\Delta_{t,q}^{1,(i-1)\lceil\log(m+1)\rceil}))(\Delta_{t,q}^{m})$$

$$\subseteq (\Delta(\Delta_{t,q}^{1,(i-1)\lceil\log(m+1)\rceil}))(\Delta_{t,q}^{1,\lceil\log(m+1)\rceil}) .$$

$$= \Delta(\Delta_{t,q}^{1,i\lceil\log(m+1)\rceil}) . \square$$

We next proceed to show that mod q counting of letters in context preserves the property of being a group and that thresh t counting of letters in context preserves the property of being group-free.

Lemma 2.10: If $\gamma \in A^*\Gamma_x$ then $\gamma(\alpha_{0,q}) \in A^*\Gamma_x$ for any $q \geq 1$.

Proof: Let k be such that $x^k \gamma \lambda$ for all $x \in A^*$. We show that $x^{qk} \gamma(\alpha_{0,q}) \lambda$ for all $x \in A^*$. Since $x^{kq} \gamma \lambda$, we have

$$\binom{x^{kq}}{\lambda}_{([v_0]_\gamma)} = \binom{\lambda}{\lambda}_{([v_0]_\gamma)} = 1 \quad \text{iff} \quad v_0 \gamma \lambda \text{, and both quantities are 0}$$

otherwise. Also,

$$\binom{x^{kq}}{a}_V = \sum_{\substack{a=u_1\ldots u_q \\ V=V_1\ldots V_q}} \binom{x^k}{u_1}_{V_1} \cdots \binom{x^k}{u_q}_{V_q} .$$

All terms containing a factor $\binom{x^k}{\lambda}_{V'}$ with $V' \neq ([\lambda]_\gamma)$ vanish.

Thus $\binom{x^{kq}}{a}_V = q\binom{x^k}{a}_V \theta_{0,q} \; 0 = \binom{\lambda}{a}_V$. □

Lemma 2.11: If $\gamma \in A^*\Gamma_+$ then $\gamma(\alpha_{t,1}) \in A^*\Gamma_+$ for any $t \geq 0$.

Proof: Let k be such that $x^k \gamma x^{k+1}$ for all $x \in A^*$. We show that $x^{2k+t} \gamma(\alpha_{t,1}) x^{2k+t+1}$ for all $x \in A^*$. We have $\binom{x^{2k+t}}{\lambda}_V = 1$ iff $V = ([x^{2k+t}]_\gamma)$: since $x^{2k+t} \gamma x^{2k+t+1}$ this shows that $\binom{x^{2k+t}}{\lambda}_V = 1$ iff $\binom{x^{2k+t+1}}{\lambda}_V = 1$. Next let $a \in A$, $V = ([v_0]_\gamma, [v_1]_\gamma) \in (A^*/\gamma)^2$

$$V_0 = \{([v_0]_\gamma, [v_1']_\gamma) \; : \; v_1'x^k \gamma v_1\}$$

$$V_1 = \{([v_0']_\gamma, [v_1']_\gamma) \; : \; x^k v_0' \gamma v_0, v_1'x^k \gamma v_1\}$$

and $V_2 = \{([v_0']_\gamma , [v_1]_\gamma) : x^k v_0' \ \gamma \ v_0\}$.

Then $\binom{x^{2k+t}}{a}_V = V_0 \overset{\Sigma}{\varepsilon} V_0 \binom{x^k}{a}_{V_0} + V_1 \overset{\Sigma}{\varepsilon} V_1 \binom{x^t}{a}_{V_1} + V_2 \overset{\Sigma}{\varepsilon} V_2 \binom{x^k}{a}_{V_2}$,

and $\binom{x^{2k+t+1}}{a}_V = V_0 \overset{\Sigma}{\varepsilon} V_0 \binom{x^k}{a}_{V_0} + V_1 \overset{\Sigma}{\varepsilon} V_1 \binom{x^{t+1}}{a}_{V_1} + V_2 \overset{\Sigma}{\varepsilon} V_2 \binom{x^k}{a}_{V_2}$.

If there exists $V_1 \varepsilon V_1$ such that $\binom{x^t}{a}_{V_1} \geq 1$, then $x^t = x^i x_0 a x_1 x^{t-i-1}$ with $x^i x_0 \ \gamma \ v_0'$ and $x_1 x^{t-i-1} \ \gamma \ v_1'$. Then, for $j = 0,\ldots,t-1$, we have $x^t = x^j x_0 a x_1 x^{t-j-1}$ with $([x^j x_0]_\gamma , [x_1 x^{t-j-1}]_\gamma) \varepsilon V_1$ and $x^{t+1} = x^j x_0 a x_1 x^{t-j}$ with $([x^j x_0]_\gamma , [x_1 x^{t-j}]_\gamma) \varepsilon V_1$. Thus

$$V_1 \overset{\Sigma}{\varepsilon} V_1 \binom{x^t}{a}_{V_1} \geq t \quad \text{and} \quad V_1 \overset{\Sigma}{\varepsilon} V_1 \binom{x^{t+1}}{a}_{V_1} \geq t .$$

We can reverse the argument if there exists $V_1 \varepsilon V_1$ such that $\binom{x^{t+1}}{a}_{V_1} \geq 1$. Therefore $\binom{x^{2k+t}}{a}_V \ \theta_{t,1} \ \binom{x^{2k+t+1}}{a}_V$. □

Our next result deals with reversal of congruences.

Lemma 2.12: If $\gamma \varepsilon A^*\Gamma$, $t \geq 0$, $q \geq 1$, $m \geq 0$, then $(\gamma(\alpha^m_{t,q}))^\rho = \gamma^\rho(\alpha^m_{t,q})$.

Proof: Let $x \ (\gamma(\alpha^m_{t,q}))^\rho \ y$, i.e. $x^\rho \ \gamma(\alpha^m_{t,q}) \ y^\rho$. Any factorization of x^ρ as $x^\rho = x_0 a_1 x_1 \ldots a_m x_m$ with $x_i \ \gamma \ v_i$ for $i = 0,\ldots, m$, induces a factorization of x as $x = x_m^\rho a_m x_{m-1}^\rho \ldots a_1 x_0^\rho$ with $x_i^\rho \ \gamma^\rho \ v_i^\rho$ for $i = 0,\ldots, m$, and similarly for y . Thus $x^\rho \ \gamma(\alpha^m_{t,q}) \ y^\rho$

implies $x\ \gamma^{\rho}(\alpha^{m}_{t,q})\ y$ and $\gamma^{\rho}(\alpha^{m}_{t,q}) \supseteq (\gamma(\alpha^{m}_{t,q}))^{\rho}$. Replacing γ by γ^{ρ} we also have $\gamma(\alpha^{m}_{t,q}) \supseteq (\gamma^{\rho}(\alpha^{m}_{t,q}))^{\rho}$, and reversing both sides $(\gamma(\alpha^{m}_{t,q}))^{\rho} \supseteq \gamma^{\rho}(\alpha^{m}_{t,q})$. This completes the proof of the lemma. □

The final lemma of this chapter summarizes basic properties of the *-varieties $\Delta(\Delta^{m,i}_{t,q})$.

Lemma 2.13: For any *-variety Δ , m,i , $t \geq 0$, $q \geq 1$:

i) $\Delta(\Delta^{m,i}_{t,q}) = \Omega$ iff $(t = 0$ and $q = 1)$ or

$$(\Delta = \Omega \text{ and } (m = 0 \text{ or } i = 0));$$

ii) if $m \leq m'$, $i \leq i'$, $t \leq t'$, $q \mid q'$, then

$$\Delta(\Delta^{m,i}_{t,q}) \subseteq \Delta(\Delta^{m',i'}_{t',q'}) ;$$

iii) if $\Delta \subseteq \Gamma_{\times}$ then $\Delta(\Delta^{m,i}_{0,q}) \subseteq \Gamma_{\times}$;

iv) if $\Delta \subseteq \Gamma_{+}$ then $\Delta(\Delta^{m,i}_{t,1}) \subseteq \Gamma_{+}$;

v) if $\Delta = \Delta^{\rho}$ then $(\Delta(\Delta^{m,i}_{t,q}))^{\rho} = \Delta(\Delta^{m,i}_{t,q})$, where $A^{*}\Delta^{\rho} = \{\alpha^{\rho} : \alpha \in A^{*}\Delta\}$

Proof: The easy proofs of i) and ii) are left to the reader. To prove iii), we have $\Delta(\Delta_{0,q}^{m,i}) \subseteq \Delta(\Delta_{0,q}^{1,i\lceil\log(m+1)\rceil})$ by corollary 2.2. It is thus sufficient to show that $\Delta(\Delta_{0,q}^{1,i}) \subseteq \Gamma_x$ for all $i \geq 0$. This trivially holds when $i = 0$. The proof may then be completed by induction using lemma 2.10 . The proof of iv) is similar to iii) except that lemma 2.11 is used in the induction step. For v), the result is easily seen to be true when $i = 0$. Again, an inductive argument, using lemma 2.12 , may be applied to establish the result for arbitrary i. □

In the following chapters, we will investigate in more detail the hierarchies of *-varieties of congruences obtained by starting with $\Delta = \Omega$. We will use the notation $\Delta_{t,q}^{m,i}$ for $\Omega(\Delta_{t,q}^{m,i})$. Also the superscript i is dropped when it is 1 . From lemma 2.7 , we have that $A*\Delta_{t,q}^{m,i}$ is generated (under $\supseteq$) by the congruence $\alpha_{t,q}^{m,i}$. Unless explicitly specified otherwise, we assume throughout the following chapters that m , i , $t \geq 0$ and $q \geq 1$ are fixed but arbitrary integers.

III. COUNTING SUBWORDS MOD Q AND NILPOTENT GROUPS.

In this chapter, the *-variety $\Delta^*_{0,*}$ is shown to correspond to the variety $\underline{G_{nil}}$. Partial results on the intermediate $\Delta^m_{0,q}$ are also given. Some properties of nilpotent groups are examined with respect to this congruence characterization. In particular, information on the subgroups of $A^*/\alpha^m_{0,q}$ is obtained in terms of counting subwords. Finally a bound on the star-height of $\alpha^m_{0,q}$ languages is derived.

III.1 Monoid characterization of $\Delta^*_{0,*}$.

In this section we generalize a result of Eilenberg [76] on p-groups to characterize the variety of monoids corresponding to $\Delta^*_{0,*}$.

Lemma 1.1 : $\Delta^m_{0,q} \subseteq \Gamma_x$.

Proof: This follows from lemma II.2.13 iii) since $\Omega \subseteq \Gamma_x$. □

We can use the results of chapter II to derive a bound on the order of the elements of the groups A^*/α , $\alpha \in A^*\Delta^m_{0,q}$.

Lemma 1.2 : Let $\alpha \in A^*\Delta^m_{0,q}$, $k = \lceil \log(m+1) \rceil$. Then $x^{q^k} \alpha \lambda$ for all $x \in A^*$.

Proof: For our choice of k, we have $\Delta^m_{0,q} \subseteq \Delta^{2^k-1}_{0,q}$. By lemma II.2.9, $\Delta^{2^k-1}_{0,q} \subseteq \Delta^{1,k}_{0,q}$. Therefore $\alpha \supseteq \alpha^{1,k}_{0,q}$, where $\alpha^{1,k}_{0,q}$ is the generator of $A^*\Delta^{1,k}_{0,q}$, and it is sufficient to show that $x^{q^k} \alpha^{1,k}_{0,q} \lambda$ for all $x \in A^*$. This clearly holds when $k = 0$. The proof is completed by induction on k using the argument in the proof of lemma II.2.10 . □

Corollary 1.1 : If p is prime, $c \geq 0$,

$$\Delta^m_{0,p^c} \hookrightarrow G_p$$

Proof: By lemma 1.2, every element of the group A^*/α , $\alpha \in A^*\Delta^m_{0,p^c}$ has order p^r for some $r \geq 0$. □

Corollary 1.2 : $\Delta^m_{0,q} \hookrightarrow G_{nil}$

Proof: Let $q = p_1^{c_1} \ldots p_n^{c_n}$, p_i prime for $i = 1,\ldots,n$. Then $\theta_{0,q} = \theta_{0,p_1^{c_1}} \cap \ldots \cap \theta_{0,p_n^{c_n}}$ and consequently $\alpha^m_{0,q} = \alpha^m_{0,p_1^{c_1}} \cap \ldots \cap \alpha^m_{0,p_n^{c_n}}$.

By proposition I.2.9 c),

$$A^*/\alpha^m_{0,q} \hookrightarrow A^*/\alpha^m_{0,p_1^{c_1}} \times \ldots \times A^*/\alpha^m_{0,p_n^{c_n}} .$$

The i^{th} factor of the direct product is a p_i-group by corollary 1.1 so that $A^*/\alpha^m_{0,q}$ is covered by a nilpotent group. Hence $\alpha^m_{0,q}$ is a nilpotent congruence. □

The key result needed to characterize $\Delta^*_{0,*}$ is the following theorem of Eilenberg.

Lemma 1.3 : If G is a p-group and $G \simeq A^*/\alpha_G$ then $\alpha_G \in A^*\Delta^*_{0,p}$.

Lemma 1.4 : If G is a nilpotent group, $G \simeq G_1 \times \ldots \times G_n$ with G_i a p_i-group, and $G \simeq A^*/\alpha_G$, then $\alpha_G \in A^*\Delta^*_{0,q}$ for $q = p_1 \cdots p_n$.

Proof: Let $\phi_i = \alpha_G \pi_i$ where π_i is the natural projection $\pi_i : A^*/\alpha_G \to G_i$. Then $\phi_i \in A^*\Gamma$ is a p_i-group congruence; hence $\phi_i \in A^*\Delta^{m_i}_{0,p_i}$ for some $m_i \geq 0$ by lemma 1.3 . Let $m = \max\{m_i : i = 1, \ldots, n\}$. Then $\phi_i \supseteq \alpha^m_{0,p_i}$ for $i = 1, \ldots, n$. Then $\alpha_G = \bigcap_{i=1}^n \phi_i \supseteq \bigcap_{i=1}^n \alpha^m_{0,p_i} = \alpha^m_{0,q}$, where $q = p_1 \cdots p_n$. Hence $\alpha_G \in A^*\Delta^*_{0,q}$. □

Theorem 1.1 : i) Let $\Pi_q = \{p : p \text{ is prime, } p|q\}$ and $I_q = \{i \geq 1 : i \text{ is a } \Pi_q \text{ integer}\}$. Then

$$\Delta^*_{0,q} \leftrightarrow \underline{G_{nil}} \cap \left(\bigcup_{i \in I_q} \underline{M_{0,i}}\right)$$

ii) $$\Delta^*_{0,*} \leftrightarrow \underline{G_{nil}}$$

Proof: By corollary 1.2 $\Delta^*_{0,q} \hookrightarrow \underline{G_{nil}}$ and it follows from lemma 1.2 that $\Delta^m_{0,q} \hookrightarrow \underline{M_{0,q}^{\lceil \log(m+1) \rceil}}$ for every $m \geq 0$. Thus $\Delta^*_{0,q} \hookrightarrow \underline{G_{nil}} \cap \left(\bigcup_{i \in I_q} \underline{M_{0,i}}\right)$. Conversely if $G \in \underline{G_{nil}} \cap \left(\bigcup_{i \in I_q} \underline{M_{0,i}}\right)$ then $G \cong G_1 \times \cdots \times G_n$, G_i a p_i-group for some $p_i \in \Pi_q$. If $G \cong A^*/\alpha_G$, by lemma 1.4 $\alpha_G \in \Delta^*_{0,q}$. Thus $\underline{G_{nil}} \cap \left(\bigcup_{i \in I_q} \underline{M_{0,i}}\right) \hookrightarrow \Delta^*_{0,q}$ and thus $\Delta^*_{0,q} \leftrightarrow \underline{G_{nil}} \cap \left(\bigcup_{i \in I_q} \underline{M_{0,i}}\right)$. The second part follows directly. □

III.2 Congruence description of some properties of nilpotent groups.

From theorem 1.1, we obtain a "combinatorial" description of nilpotent groups. Indeed if G is a nilpotent group generated by A, i.e. $G \simeq A^*/\alpha_G$, then G is covered by $A^*/\alpha^m_{0,q}$ for some $m \geq 0$, $q \geq 1$. Eilenberg's proof of lemma 1.3 may be adapted to show that we can always take $m = |G|$ and $q = p_1 \ldots p_n$ where $\{p_1,\ldots,p_n\} = \{p : p \text{ prime}, p||G|\}$. Since the definition of $\alpha^m_{0,q}$ is in terms of counting, one can describe the monoid $A^*/\alpha^m_{0,q}$ as a set which is a cross-product of cyclic counters with the operation on this set modeling counting of subwords. This is an extension of the fundamental theorem on abelian groups since counting subwords of length 1 can be modeled by the usual direct product.

Theorem 1.1 also implies that $\Delta^*_{0,q} = \Delta^*_{0,q'}$, whenever $\{p : p \text{ prime}, p|q\} = \{p : p \text{ prime}, p|q'\}$. On the other hand, it is not true in general that $\Delta^m_{0,q} = \Delta^m_{0,q'}$ for all m. For example, consider the cyclic group $\{a\}^*/\alpha_{0,p^2}$; it may be verified that $\alpha_{0,p^2} \in \{a\}^*\Delta^1_{0,p^2}$, but $\alpha_{0,p^2} \notin \{a\}^*\Delta^1_{0,p}$. We now examine the trade off between m and q in the simple case of abelian congruences.

Lemma 2.1 : Let p be prime, c, $d \geq 1$ $m \geq 1$; if $p^d \geq m$ then $p^c \left| \binom{p^d}{m} \right.$ iff $d \geq c + (m)_p$ where $(m)_p$ is the highest power of p dividing m .

Proof: The lemma is easily verified when $m = 1$. If $m \geq 2$, then $p^c \left| \binom{p^d}{m} \right.$ iff

$$(*)\quad p^c m(m-1)\ldots 2 \mid p^d(p^d-1) \ldots (p^d-m+1) .$$

Since $p^d \geq m$, $m(m-1)\ldots 2 \mid p^d(p^d-1) \ldots (p^d-m+1)$. Also $(j)_p = (p^d-j)_p$ for $j = 1,\ldots,m-1$. Thus (*) holds iff $(p^c m)_p = c+(m)_p \leq (p^d)_p = d$. □

Lemma 2.2 : Let p be prime, $c \geq 1$, $m \geq 1$. If $k \geq m$ then $p^c | \binom{k}{i}$ for $i = 1,\ldots,m$ iff $(k)_p \geq c + \lfloor \log_p m \rfloor$, where $\lfloor n \rfloor$ is the largest integer less than or equal to n.

Proof: Consider $\alpha^m_{0,p^c} \in \{a\} * \Delta^m_{0,p^c}$. By lemma 1.2, $[a]\alpha^m_{0,p^c}$ has order p^d for some $d \geq 0$. On the other hand $a^{p^d} \alpha^m_{0,p^c} \lambda$ iff $p^c | \binom{a^{p^d}}{a^i} = \binom{p^d}{i}$ for $i = 1,\ldots,m$. If $p^d < m$ then p^c cannot divide $\binom{p^d}{p^d} = 1$ so that $p^d \geq m$. By lemma 2.1, it must be that $d \geq c + (i)_p$ for $i = 1,\ldots,m$. But $p^c | \binom{k}{i}$ for $i = 1,\ldots,m$ iff $a^k \alpha^m_{0,p^c} \lambda$ iff $p^d | k$ iff $(k)_p \geq d$. It remains to show that $\max\{(i)_p : i = 1,\ldots,m\} = \lfloor \log_p m \rfloor$. If there exists $r \leq m$ such that $(r)_p = j$, then $p^j \leq m$.. Thus $\max\{(i)_p : i = 1,\ldots,m\} \leq \lfloor \log_p m \rfloor$. Conversely $p^{\lfloor \log_p m \rfloor} \leq m$ so that $\lfloor \log_p m \rfloor \leq \max\{(i)_p : i = 1,\ldots,m\}$. □

Lemma 2.3 : Let p be prime, $1 \leq c \leq d$, $m \geq 1$. Then $\Delta^1_{0,p^d} \subseteq \Delta^m_{0,p^c}$ iff $d \leq c + \lfloor \log_p m \rfloor$.

Proof: Suppose $d > c + \lfloor \log_p m \rfloor$. By lemma 2.2, we know that $a^{p^{c+\lfloor \log_p m \rfloor}} \alpha^m_{0,p^c} \lambda$ for $\alpha^m_{0,p^c} \in \{a\} * \Delta^m_{0,p^c}$. But $p^d \nmid p^{c+\lfloor \log_p m \rfloor}$ hence $a^{p^{c+\lfloor \log_p m \rfloor}} \alpha^1_{0,p^d} \lambda$ does not hold. Thus $\Delta^1_{0,p^d} \subseteq \Delta^m_{0,p^c}$ implies $d \leq c + \lfloor \log_p m \rfloor$. Conversely suppose $d \leq c + \lfloor \log_p m \rfloor$, and let $x \alpha^m_{0,p^c} \lambda$ for $x \in A^*$, $\alpha^m_{0,p^c} \in A^* \Delta^m_{0,p^c}$. Then $p^c | \binom{x}{a^i} = \binom{\binom{x}{a}}{i}$ for $i = 1,\ldots,m$. By lemma 2.2, $c + \lfloor \log_p m \rfloor \leq (\binom{x}{a})_p$, that is $p^d | \binom{x}{a}$.

Hence $x\ \alpha^1_{0,p}{}^d\ \lambda$. Now $x\ \alpha^m_{0,p}{}^c\ y$ iff $xw\ \alpha^m_{0,p}{}^c\ \lambda$ for some w such that wy $\alpha^m_{0,p}{}^c\ \lambda$. Then $xw\ \alpha^1_{0,p}{}^d\ \lambda$ and $wy\ \alpha^1_{0,p}{}^d\ \lambda$. Therefore $x\ \alpha^1_{0,p}{}^d\ y$ and $\alpha^1_{0,p}{}^d \supseteq \alpha^m_{0,p}{}^c$. Since A was arbitrary this shows that $\Delta^1_{0,p}{}^d \subseteq \Delta^m_{0,p}{}^c$. □

Lemma 2.4 : Let p be prime, $1 \leq d$.. Then $\Delta^1_{0,p}{}^d \subseteq \Delta^m_{0,q}$ iff $m \geq 1$, $(q)_p \geq 1$ and $d \leq (q)_p + \lfloor \log_p m \rfloor$.

Proof: Let $x \in A^*$ be such that $\binom{x}{a} \geq m$ and $x\ \alpha^m_{0,q}\ \lambda$. In particular $q \mid \binom{x}{a^i}$ for $i = 1,\ldots,m$. This implies that $p^{(q)_p} \mid \binom{\binom{x}{a}}{i}$ for $i = 1,\ldots,m$. By lemma 2.2, we have then $(q)_p + \lfloor \log_p m \rfloor \leq \left(\binom{x}{a}\right)_p$. If $m \geq 1$, $(q)_p \geq 1$ and $d \leq (q)_p + \lfloor \log_p m \rfloor$, we then conclude that $p^d \mid \binom{x}{a}$, i.e. $x\ \alpha^1_{0,p}{}^d\ \lambda$. Using the same reasoning as in the previous lemma, this implies that $\Delta^1_{0,p}{}^d \subseteq \Delta^m_{0,q}$. Conversely, if $m = 0$ then $\Delta^m_{0,q} = \Omega$ and $\Delta^1_{0,p}{}^d \subseteq \Omega$ does not hold. If $(q)_p = 0$, then we have in $\{a\}^*$ $a^{q^k}\ \alpha^m_{0,q}\ \lambda$ for some $k \geq 1$ but since p^d does not divide $q^k, a^{q^k}\ \alpha^1_{0,p}{}^d\ \lambda$ does not hold. Hence $\alpha^1_{0,p}{}^d \not\ni \alpha^m_{0,p}{}^c$, i.e. $\Delta^1_{0,p}{}^d \not\subseteq \Delta^m_{0,p}{}^c$. Suppose now $d > (q)_p + \lfloor \log_p m \rfloor$. We have $q \mid \binom{k}{i}$ for $i = 1,\ldots,m$ iff $p^{(q)_p} \mid \binom{k}{i}$ for $i = 1,\ldots,m$, for all p dividing q . It can be verified that $x = a^{q'(p^{(q)_p + \lfloor \log_p m \rfloor})}\ \alpha^m_{0,q}\ \lambda$ where $(q')_p = 0$. But $x\ \alpha^1_{0,p}{}^d\ \lambda$ does not hold since p^d does not divide $q'(p^{(q)_p + \lfloor \log_p m \rfloor})$. Again this establishes that $\Delta^1_{0,p}{}^d \not\subseteq \Delta^m_{0,q}$. □

Corollary 2.1 : For any $q \geq 1$, $\Delta^1_{0,q} \subseteq \Delta^m_{0,q'}$ iff $(q)_p \geq 1$ implies $(q')_p \geq 1$ for any prime p , $m \geq 1$, and $(q)_p \leq (q')_p + \lfloor \log_p m \rfloor$.

Proof: If $q = p_1^{c_1} \ldots p_n^{c_n}$, then $\Delta^1_{0,q} \subseteq \Delta^m_{0,q'}$ iff $\Delta^1_{0,p_i^{c_i}} \subseteq \Delta^m_{0,q'}$ for $i = 1,\ldots,n$. The result follows from lemma 2.4 . □

The problem of finding conditions under which $\Delta^m_{0,q} \subseteq \Delta^{m'}_{0,q'}$ remains unsolved in the general case.

Lemma 2.2 can also be used to determine the minimal integer k satisfying $x^k \alpha^m_{0,q} \lambda$ for all x in A* .

Lemma 2.5 : Let $q = p_1^{c_1} \ldots p_n^{c_n}$, p_i prime, $m \geq 1$. Then $x^k \alpha^m_{0,q} \lambda$ for all x in A* iff $p_1^{d_1} \ldots p_n^{d_n} | k$ with $d_j = c_j + \lfloor \log_{p_j} m \rfloor$, for $j = 1,\ldots,n$.

Proof: Consider the identity

$$\binom{a^k}{u} = \begin{cases} \binom{k}{i} & \text{if} \quad u = a^i \\ 0 & \text{otherwise .} \end{cases}$$

Thus $a^k \alpha^m_{0,q} \lambda$ iff $q \mid \binom{k}{i}$ for $i = 1,\ldots,m$. This is true iff $p_j^{c_j} \mid \binom{k}{i}$ for $i = 1,\ldots,m$, and $j = 1,\ldots,n$. By lemma 2.2, $(k)_{p_j} \geq c_j + \lfloor \log_{p_j} m \rfloor$ for $j = 1,\ldots,n$. Thus, the first condition is seen to imply the

second. For the converse, we will use the following identity whose proof we leave to the reader:

$$\binom{x^k}{u} = \sum_{r=1}^{|u|} \sum_{\substack{u=u_1\cdots u_r \\ u_i \in A^+}} \binom{k}{r} \binom{x}{u_1} \cdots \binom{x}{u_r} \quad .$$

Using once more lemma 2.2, we have that $p_j^{c_j} \mid \binom{k}{r}$ for $r = 1,\ldots,m$, $j = 1,\ldots,n$. Thus $q \mid \binom{k}{r}$ for $r = 1,\ldots,m$ and $q \mid \binom{x^k}{u}$ so that $x^k \alpha_{0,q}^m \lambda$. □

We now turn our attention to the variety of nilpotent groups of class $\leq m$, for fixed $m \geq 0$, which we denote by $\underline{G_{nil,m}}$. If G is nilpotent of class m, recall that the upper central series is given by

$$Z_0(G) = \{1\} \lhd Z_1(G) \lhd \ldots \lhd Z_n(G) = G$$

where, for $i \geq 1$, $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$.

Since $\underline{G_{nil,0}} = \{1\}$, $\Delta_{0,q}^0 \leftrightarrow \underline{G_{nil,0}}$ for any $q \geq 1$. Also $\underline{G_{nil,1}} = \underline{G_{ab}}$ so that by corollary II.1.1 ii) $\Delta_{0,*}^1 \leftrightarrow \underline{G_{nil,1}}$. If $|A| = 1$, A^*/α is a cyclic group for any $\alpha \in A^*\Gamma_x$. Hence A^*/α is nilpotent of class ≤ 1. We now consider the case of an alphabet of cardinality ≥ 2.

Lemma 2.6 : Let $\alpha^m_{0,q} \in A^*\Delta^m_{0,q}$. Then $Z_i(A^*/\alpha^m_{0,q}) = \{[x]_{\alpha^m_{0,q}} : x\ \alpha^{m-i}_{0,q}\ \lambda\}$ for $i = 0,\ldots,m$.

Proof: The lemma clearly holds when $i = 0$. For $i > 0$, we can assume inductively that $Z_{i-1}(A^*/\alpha^m_{0,q}) = \{[x]_{\alpha^m_{0,q}} : x\ \alpha^{m-i+1}_{0,q}\ \lambda\}$. Then $(A^*/\alpha^m_{0,q})/Z_{i-1}(A^*/\alpha^m_{0,q}) \simeq A^*/\alpha^{m-i+1}_{0,q}$. We claim that $Z(A^*/\alpha^{m-i+1}_{0,q}) \simeq \{[x]\alpha^{m-i+1}_{0,q} : x\ \alpha^{m-i}_{0,q}\ \lambda\}$. Suppose $x\ \alpha^{m-i}_{0,q}\ \lambda$. Then, for any $y \in A^*$, $u \in (A \cup \lambda)^{m-i+1}$, $\binom{xy}{u} = \sum_{u=u_1u_2} \binom{x}{u_1}\binom{y}{u_2}\ \theta_{0,q}\ \binom{x}{u} + \binom{y}{u}$, since $q \mid \binom{x}{u_1}$ whenever $1 \le |u_1| \le m - i$. Similarly $\binom{yx}{u}\ \theta_{0,q}\ \binom{y}{u} + \binom{x}{u}$ so that $xy\ \alpha^{m-i+1}_{0,q}\ yx$. Conversely if $x\ \alpha^{m-i}_{0,q}\ \lambda$ does not hold, there exists $u = u'a$, $a \in A$, $1 \le |u| \le m-i$ such that q does not divide $\binom{x}{u}$. Since $|A| \ge 2$, we can choose $b \in A$, $b \neq a$. Then

$$\binom{xb}{bu} = \binom{x}{bu} \quad \text{and} \quad \binom{bx}{bu} = \binom{x}{bu} + \binom{x}{u} .$$

Therefore q does not divide $\binom{xb}{bu} - \binom{bx}{bu}$, i.e. $xb\ \alpha^{m-i+1}_{0,q}\ bx$ does not hold. Thus $Z(A^*/\alpha^{m-i+1}_{0,q}) = \{[x]_{\alpha^{m-i+1}_{0,q}} : \alpha^{m-i}_{0,q}\ \lambda\}$ as was claimed. Now,

$$\{[x]_{\alpha^m_{0,q}} : x\ \alpha^{m-i}_{0,q}\ \lambda\}/\{[x]_{\alpha^m_{0,q}} : x\ \alpha^{m-i+1}_{0,q}\lambda\}$$

$$\simeq \{[x]_{\alpha^{m-i+1}_{0,q}} : x\ \alpha^{m-i}_{0,q}\ \lambda\}$$

by proposition I.3.1. This establishes that $Z_i(A^*/\alpha^m_{0,q}) = \{[x]_{\alpha^m_{0,q}} : x\ \alpha^{m-i}_{0,q}\ \lambda\}$, completing the induction step. □

Corollary 2.2 : $\Delta^m_{0,q} \hookrightarrow G_{nil,m}$ and for $q > 1$, $\Delta^m_{0,q} \not\hookrightarrow G_{nil,m-1}$.

Proof: By lemma 2.6, $A^*/\alpha^m_{0,q}$ is a nilpotent group of class exactly m , when $|A| \geq 2$. □

We now present a detailed analysis in terms of subword counting of a well-known family of groups.

Example: Let D_r , $r \geq 3$, denote the group of rigid transformations of an r-gon onto itself. Numbering the vertices 1, 2, ..., r , vertex 1 can be mapped onto any other vertex and the remaining vertices may be placed in either clockwise or counterclockwise manner. Thus D_r has order 2r ; it can be shown that the group D_r on two generators is determined by the relations $a^2 = b^2 = (ab)^r = 1$.

Let γ_n , $n \geq 2$, be the right congruence on $\{a,b\}^*$ represented in figure II.1 . The congruence γ'_n generated by γ_n can be found by a well-known algorithm and is represented in figure II.2 . From this figure, it is seen that the relations $a^2 = b^2 = (ab)^{2^n} = 1$ hold in A^*/γ'_n so that $A^*/\gamma'_n \prec D_{2^n}$. Also $|A^*/\gamma'_n| = 2^{n+1} = |D_{2^n}|$ and thus $A^*/\gamma'_n \simeq D_{2^n}$.

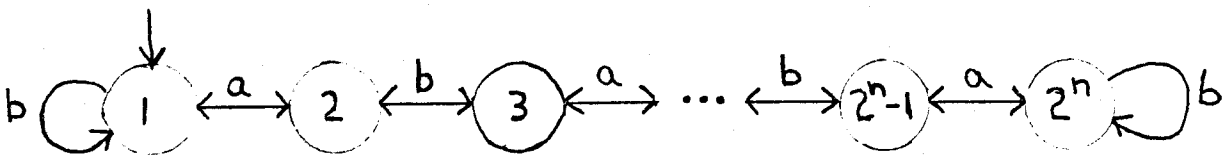


Figure II.1 : Representation of the right congruence γ_n on {a,b}* .

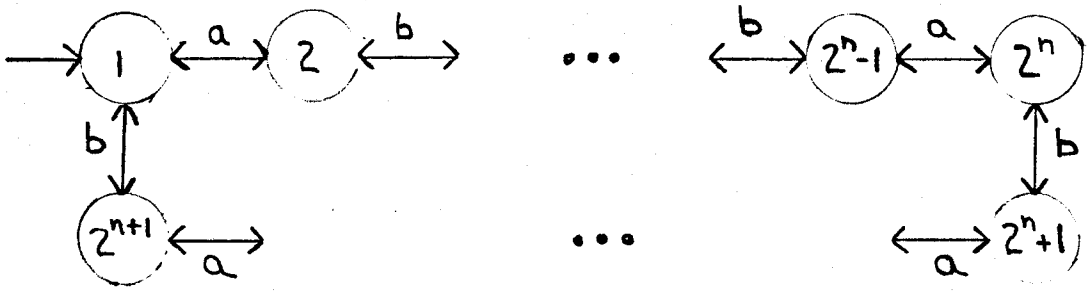


Figure II.2 : Representation of the congruence γ_n' generated by γ_n .

The following are claimed to be equivalent.

For all x, y $\in$ A* , n $\geq$ 2 ,

i) $x \gamma_n y$;

ii) $\binom{x}{u} \theta_{0,2} \binom{y}{u}$ for all u such that $(ab)^{2^{n-1}} = uu'$, $u' \in A^+$;

iii) $\binom{x}{u} \theta_{0,2} \binom{y}{u}$ for $u = a$, $(ab)^{2^i}$ $i = 0,\ldots,n-2$.

<u>i) implies ii)</u>

The claim is proved by induction on n .

n = 2 : It can be verified directly that $x \gamma_2 y$ implies $\binom{x}{u} \theta_{0,2} \binom{y}{u}$ for u = a , ab , aba . Using the numbering given by figure II.1 , we also have that $\binom{x}{ab} \theta_{0,2} 1$ iff $[x]_{\gamma_2} \geq 3$ and $\binom{x}{aba} \theta_{0,2} 1$ iff

$[x]_{\gamma_2} = 4$.

$n > 2$: We assume inductively that the claim holds for $n - 1$ and also that for $u = (ab)^{2^{n-2}-1}a$, $\binom{x}{u}\ \theta_{0,2}\ 1$ iff $[x]_{\gamma_{n-1}} = 2^{n-1}$.

Identifying all pairs of states i and $2^n + 1 - i$, it is seen that $\gamma_{n-1} \supseteq \gamma_n$ and that $\binom{x}{u}\ \theta_{0,2}\ 1$ iff $[x]_{\gamma_n} = 2^{n-1}$ or $[x]_{\gamma_n} = 2^{n-1} + 1$, for $u = (ab)^{2^{n-2}-1}a$. Also, using the formulas

$$\binom{\lambda}{vb} = 0$$

$$\binom{x}{vb} = \begin{cases} \binom{x'}{vb} + \binom{x'}{v} & \text{if } x = x'b \\ \binom{x'}{v} & \text{if } x = x'a , \end{cases}$$

we have that $\binom{x}{(ab)^{2^{n-2}}}\ \theta_{0,2}\ 1$ iff $[x]_{\gamma_n} \geq 2^{n-1} + 1$. The proof will be complete if one shows that $[x]_{\gamma_n} = i$ implies

$$\binom{x}{(ab)^{2^{n-2}}u} = \begin{cases} 0 & \text{if } i \leq 2^{n-1} \\ \binom{y}{u} & \text{for } y \text{ such that} \\ & [y]_{\gamma_n} = i - 2^{n-1} \text{ otherwise,} \end{cases}$$

and this for all u such that $(ab)^{2^{n-2}} = uu'$, $u' \in A^+$. An easy argument by induction on $|u|$ is left to the reader.

ii) implies iii)

The subwords which are counted in iii) form a subset of the set of subwords which are counted in ii). The claim follows.

iii) implies i)

By induction on n .

n = 2 It may be directly verified.

n > 2 We have shown that $\gamma_{n-1} \supseteq \gamma_n$ by identifying the states i and 2^n+1-i . It was also indicated that $\left(\overset{x}{(ab)^{2^{n-2}}}\right) \theta_{0,2}\ 1$ iff $[x]_{\gamma_n} \geq 2^{n-1} + 1$. Combining these observations with the induction hypothesis yields the result. □

Now consider the group A^*/γ_n' of figure II.2. One verifies that $Z(A^*/\gamma_n') = \{1 , 2^n+1\}$, that $(A^*/\gamma_n')/Z(A^*/\gamma_n') \simeq A^*/\gamma_{n-1}'$ for $n \geq 3$, and that A^*/γ_2' is a nilpotent group of class 2 . Hence A^*/γ_n' is nilpotent of class n . On the other hand, the best subword counting representation that we are able to get involves counting subwords of length 2^{n-1} . We conjecture that this is best possible and that $\gamma_n' \in \{a,b\}^* \Delta_{0,q}^{2^{n-1}} - \{a,b\}^* \Delta_{0,q}^{2^{n-1}-1}$, for any $q = 2^r$, $r \geq 1$.

As an intermediate step in obtaining a congruence characterization for $G_{nil,m}$, we also propose the conjecture that $G_{nil,m} \hookrightarrow \Delta_{0,*}^{2^{m-1}}$.

We close this section by considering the problem of describing more explicitely the congruences in $\Delta^m_{0,q}$.

Let $f = \Sigma\, k_u\, u$ be a polynomial in $\mathbb{N}[A]$. The <u>support</u> of f is $\operatorname{supp} f = \{u : k_u \neq 0\}$ and the <u>degree</u> of f is $\deg f = \min \{r : \operatorname{supp} f \subseteq (A \cup \lambda)^r\}$. Any such polynomial induces a function $f : A^* \to \mathbb{N}$ given by $(x)f = \Sigma\, k_u \binom{x}{u}$.

Let F be a finite collection of polynomials such that $1 \cdot \lambda \in F$. With each f of degree ≥ 1 , we associate an arbitrary congruence $\theta_f \in \mathbb{N}\Gamma_\times$. These notions lead to the following equivalence on A^* :

$$x\ \alpha_F\ y \text{ iff } (x)f\ \theta_f\ (y)f \quad \text{for all } f \text{ in } F \text{ of degree} \geq 1 .$$

For any $f \in \mathbb{N}[A]$, $\deg f \geq 1$, $a \in A$, define

$$f^R_a = \sum_{u = u'a} k_u\ u'$$

$$f^L_a = \sum_{u = au'} k_u\ u' \quad .$$

Observe that f^R_a (f^L_a) is a polynomial of degree $\deg f - 1$.

Let $\deg F = \max \{\deg f : f \in F\}$. We say that f is a <u>linear</u>

combination of $f_1, \ldots, f_n$ iff there exists $k_1, \ldots, k_n \in \mathbb{N}$ such that $f = \sum_{i=1}^{n} k_i f_i$. We define F to be complete iff the following conditions hold:

i) for each $f \in F$ with $\deg f \geq 1$, for all $a \in A$, f_a^R and f_a^L are linear combinations of elements of F ;

ii) if $f_a^R = k_1 f_1 + \ldots + k_n f_n$ and $\theta_{0,q}$, θ_{0,q_i} are the congruences associated with f and f_i respectively, then $q \mid q_i k_i$ for $i = 1, \ldots, n$; the same condition is required to hold on f_a^L .

Lemma 2.7 : If F is complete then $\alpha_F \in A^*\Gamma$.

Proof: Let $x \, \alpha_F \, y$. We show that $xa \, \alpha_F \, ya$ for any $a \in A$. We have

$$(xa)f = \sum k_u \binom{xa}{u}$$

$$= \sum k_u \binom{x}{u} + \sum_{u=u'a} k_u \binom{x}{u'}$$

$$= (x)f + (x)f_a^R$$

$$= (x)f + k_1(x)f_1 + \ldots + k_n(x)f_n ,$$

where $k_i \in \mathbb{N}$, $f_i \in F$. Since $x \, \alpha_F \, y$, $(x)f_i \, \theta_{0,q_i} \, (y)f_i$ for $i = 1, \ldots, n$, where $\theta_{0,q_i} = \theta_{f_i}$. If $\theta_f = \theta_{0,q}$ we have, because F is complete, that

$q|k_i q_i$ for $i = 1,\ldots,n$. Thus $k_i(x)f_i\ \theta_f\ k_i(y)f_i$ for $i = 1,\ldots,n$, and $(xa)f\ \theta_f\ (ya)f$. By induction on the length of z it follows that $xz\ \alpha_F\ yz$ for any $z \in A^*$. A symmetric argument, using f_a^L instead of f_a^R , shows that $zx\ \alpha_F\ zy$ for all $z \in A^*$. Thus $\alpha_F \in A^*\Gamma$. □

Lemma 2.8 : Let $F, F' \subseteq \mathbb{N}[A]$ be such that each $f \in F$ is a linear combination of elements of F' . Furthermore if $f = \sum_{i=1}^{n} k_i f_i'$, $\theta_f = \theta_{0,q}$, $\theta_{f_i'} = \theta_{0,q_i}$, assume that $q|k_i q_i$. Then $\alpha_F \supseteq \alpha_{F'}$.

Proof: Let $x\ \alpha_{F'}\ y$. Then $(x)f_i'\ \theta_{0,q_i}\ (y)f_i'$ for $i = 1,\ldots,n$, and $k_i(x)f_i'\ \theta_{0,q}\ k_i(y)f_i'$ for $i = 1,\ldots,n$. Hence $(x)f\ \theta_{0,q}\ (y)f$ for any $f \in F$ so that $x\ \alpha_F\ y$. □

Lemma 2.9 : Let $F \in \mathbb{N}[A]$ with $\deg F \leq m$ have the property that it is complete and that for each $f \in F$ of degree ≥ 1 , $f = \Sigma\ k_u u$ and $\theta_f = \theta_{0,q_f}$ imply that $q_f|k_u q$ for all $u \in \operatorname{supp} f$. Then $\alpha_F \supseteq \alpha_{0,q}^m$.

Proof: $\alpha_{0,q}^m = \alpha_{F'}$ for $F' = \{1\cdot u : |u| \leq m\}$ and $\theta_{f'} = \theta_{0,q}$ for all $f' \in F'$. The conditions of lemma 2.8 are satisfied and $\alpha_F \supseteq \alpha_{0,q}^m$. □

Corollary 2.3 : Let F satisfy the condition of lemma 2.9 . Then $H = \{[x]_{\alpha_{0,q}^m} : x\ \alpha_F\ \lambda\} \lhd A^*/_{\alpha_{0,q}^m}$.

Proof: It follows from the fact that α_F is a congruence containing $\alpha^m_{0,q}$. □

Thus we have provided a description in terms of counting subwords of congruences in $\Delta^m_{0,q}$. This consequently gives us a description of normal subgroups in $A^*/\alpha^m_{0,q}$. If $m = 1$, it can be shown that every element of $A^*\Delta^m_{0,q}$ is of the form α_F as given in lemma 2.9 . It is an interesting problem to determine if there exists congruences in $A^*\Delta^m_{0,q}$, when $m > 1$, other than those of the form α_F .

Example: For any $u \in A^*$, $|u| \leq m$, let $F_u = \{1 \cdot u' : u \in A^*u'A^*\}$ and let $\theta_f = \theta_{0,q}$ for all $f \in F$. Thus $x \; \alpha_{F_u} \; y$ iff $\binom{x}{u'} \; \theta_{0,q} \binom{y}{u'}$ for all segments u' of u . It can be verified that the hypothesis of corollary 2.3 are satisfied so that $H = \{[x]_{\alpha^m_{0,q}} : x \; \alpha_{F_u} \; \lambda\} \lhd A^*/\alpha^m_{0,q}$. Also let $F_{p(u)} = \{1 \cdot u' : u \in u'A^*\}$, $F_{s(u)} = \{1 \cdot u' : u \in A^*u'\}$ and for any $U = \{u_1, \ldots, u_r\}$ such that $u = u_1u_2$ implies $u_1 \in U$ or $u_2 \in U$ let $F_U = \{1 \cdot u_i : u_i \in U\}$. The sets

$$H_1 = \{[x]_{\alpha^m_{0,q}} : x \; \alpha_{F_{p(u)}} \; \lambda\}$$

$$H_2 = \{[x]_{\alpha^m_{0,q}} : x \; \alpha_{F_{s(u)}} \; \lambda\}$$

and $$H_3 = \{[x]_{\alpha^m_{0,q}} : x \; \alpha_{F_U} \; \lambda\}$$

form (non-normal) subgroups of $A^*/\alpha^m_{0,q}$. Moreover the largest normal subgroup of $A^*/\alpha^m_{0,q}$ which is contained in H_1 (H_2) is H .

III.3 Star-height of $\alpha^{m}_{0,q}$ -languages.

From a famous theorem of Kleene [56], it is known that the family of regular languages over A* is the closure of {{a} : a ε A} under boolean operations, concatenation and star. This theorem may be used to provide a description of any regular language by an expression indicating in which order the operations mentioned above may be applied to the letters to generate the language.

The problem of finding "simplest" regular expressions for languages is notably difficult, specially when the star operator is involved (see Brzozowski [79]). For any regular language L , let the star-height of L , denoted Lh , be the minimum number of nested * operators that are required to generate L . This induces a hierarchy of languages

$$H_0 \subseteq H_1 \subseteq \quad \cdots$$

where $H_i = \{L : Lh \leq i\}$.

It is known that $L \in H_0$ iff M_L is aperiodic (Schutzenberger [65]) and thus $H_0 \subsetneq H_1$. It is not known at present if $H_1 \neq H_2$. The following lemma appeared in Henneman [72] .

Lemma 3.1 : Let $L \subseteq A^*$; if M_L is a group and $H \lhd M_L$ is abelian, then

$Lh \leq L'h + 1$ where L' is a language of maximal star-height such that $M_{L'} \simeq M_L/H$.

For any $m \geq 0$, $q \geq 1$, let $\Delta^m_{0,q} \leftrightarrow L^m_{0,q}$. Trivially $L^0_{0,q} \subseteq H_0$ and $L^m_{0,1} \subseteq H_0$. Since $\Delta^1_{0,q}$ consists of abelian congruences, lemma 3.1 implies that $L^1_{0,q} \subseteq H_1$.

Lemma 3.2 (K. Culik): Let $L \in A^*H_0$ and $L' = (L + (aL^*)^{q-1}a)^*$ for some $a \in A$, $q \geq 1$. Suppose that any word $x \in L'$ can be uniquely written as $x = x_1 \ldots x_r$, $x_i = a$ or $x_i \in L$ for $i = 1,\ldots,r$. Then $L \in A^*H_1$.

Proof: Clearly $x \in L'$ iff $x = x_1 \ldots x_r$, $r \geq 0$, with $x_i \in L$ or $x_i = a$, and the number of indices such that $x_i = a$ is $\theta_{0,q}$ congruent to 0 . For fixed r , this will hold iff the number of indices such that $x_i \in L$ is $\theta_{0,q}$ congruent to r . Hence

$$L' = \bigcup_{r=0}^{q-1} (((a + L)^q)^*(a + L)^r \cap (a^*L)^r(a + (La^*)^{q-1}L)^*) .$$

Indeed for each fixed r , the first term of the intersection determines that x can be written as $x = x_1 \ldots x_s$, $x_i \in L$ or $x_i = a$ for $i = 1,\ldots, s$ and $s\ \theta_{0,q}\ r$; the second term determines that s' of the indices are such that $x_i \in L$ for $s'\ \theta_{0,q}\ r$. Since $a^* = \bigcap_{b \in A-\{a\}} \overline{\emptyset\ b\ \emptyset}$, this shows that $L' \in A^*H_1$. □

Lemma 3.3 : $L^2_{0,q} \subseteq H_1$

Proof: Let $\alpha \supseteq \alpha^2_{0,q} \in A^*\Delta^2_{0,q}$. Any α language is also a $\alpha^2_{0,q}$

language and it is sufficient to show that $[x]^2_{\alpha_{0,q}} \in A^*H_1$ for arbitrary $x \in A^*$. Now $[x]^2_{\alpha_{0,q}} = \bigcap_{1\le|u|\le 2} \{y : \binom{y}{u} \theta_{0,q} \binom{x}{u}\}$. From lemma 2.3, we can infer that $\{y : \binom{y}{a^i} \theta_{0,q} k\}$ is an $\alpha^1_{0,q'}$ language if q' is chosen large enough. Thus, for any k, $\{y : \binom{y}{a^2} \theta_{0,q} k\} \in A^*H_1$. It remains to show that $\{y : \binom{y}{ab} \theta_{0,q} k\} \in A^*H_1$ when $a \neq b$. Let $y = y_0 b y_1$; we say that the occurrence of b which is singled out has a-weight k' iff $\binom{y_0}{a} \theta_{0,q} k'$. Such an occurrence of b will contribute k' to $\binom{y}{ab}$ since $\binom{y}{ab} = \sum_{y=y_0 b y_1} \binom{y_0}{a}$. Let

$$K = \{(k_1,\ldots,k_{q-1}) : k_i \in \mathbb{N}/\theta_{0,q}, \sum_{i=1}^{q-1} ik_i \; \theta_{0,q} \; k\}.$$

Then

$$\{y : \binom{y}{ab} \theta_{0,q} k\} =$$

$$\bigcup_{(k_1,\ldots,k_{q-1}) \in K} \bigcap_{i=1}^{q-1} \{y : y \text{ has } k_i \text{ occurrences of b of a-weight i}\} :$$

denote by L_{i,k_i} the sets occurring on the right hand side. First consider the case when $k_i \neq 0$. Let

$$L = (a\ \overline{A^*aA^*})^{q-1}\ a$$

$$L_1 = ((\overline{A^*aA^*}\ a\ \overline{A^*aA^*})^q)^*\ (\overline{A^*aA^*}\ a\ \overline{A^*aA^*})^i$$

$$L_2 = (bL^*)^{q-1}\ b + L$$

$$L_3 = (bL^*)^{k_i-1}\ \overline{bL^*bA^*}\ .$$

We claim that

$$L_{i,k_i} = (L_1 - L_1bA^*)L_2^*L_3 \cdot$$

Let x be in the language on the right hand side. Then $x = x_1x_2x_3$ with $x_1 \in L_1 - L_1bA^*$, $x_2 \in L_2^*$, $x_3 \in L_3$. From the definition of L_1 , it follows that $\binom{x_1}{a} \theta_{0,q}\, i$; also x_1 does not contain any b of a-weight i since $x_1 \notin L_1bA^*$. Furthermore $x_2 \in L_2$ implies that x_2 contributes 0 (modulo q) b of a-weight i and $x_3 \in L_3$ implies that x_3 contributes exactly k_i b of a-weight i . This shows that $(L_1 - L_1bA^*)L_2^*L_3 \subseteq L_{i,k_i}$. Conversely $x \in L_{i,k_i}$ implies that $x=x_1x_2x_3$ where x_i is the longest prefix of x not containing any b of a-weight i and $x_3 = bx_3'$ contains exactly k_i b of a-weight i , the initial letter of x_3 being such an occurrence of b . It follows that x_2 must contain 0 (modulo q) occurrences of b of a-weight i . These observations imply that $x_1 \in L_1 - L_1bA^*$, $x_2 \in L_2^*$, $x_3 \in L_3$; hence $L_{i,k_i} \subseteq (L_1-L_ibA^*)L_2^*L_3$. If $k_i = 0$, we replace L_3 above by $L_4 = (bL^*)^{q-1}\overline{bL^*bA^*}$ and $L_{i,k_i} = (L_1 - L_1bA^*)L_2^*L_4 \cup \overline{L_1bA^*}$. The first term of the union takes care of those words having rq occurrences of b of a-weight i when $r > 0$, and the second term takes care of those words having no such b . Now, since $A^* = \overline{\emptyset}$, L_1 , L_3 and $L_4 \in A^*H_1$. Also $L_2^* \in A^*H_1$ by lemma 3.2 . Thus $L_{i,k_1} \in A^*H_1$ and this is sufficient to insure that $[x]_{\alpha}{}^2_{0,q} \in A^*H_1$ for any $x \in A^*$. □

Lemma 3.4 : If $\alpha_{0,q}^m \in A^*\Delta_{0,q}^m$, then $H = \{[x]_{\alpha_{0,q}^m} : x\, \alpha_{0,q}^{\lfloor m/2 \rfloor} \lambda\}$ is an abelian normal subgroup of $A^*/\alpha_{0,q}^m$.

Proof: $H \triangleleft A^*/\alpha_{0,q}^m$ since $\alpha_{0,q}^{\lfloor m/2 \rfloor} \supseteq \alpha_{0,q}^m$. Also suppose $[x]_{\alpha_{0,q}^m}$, $[y]_{\alpha_{0,q}^m} \in H$ and let $u \in (A \cup \lambda)^m$. Then $\binom{xy}{u} = \sum_{u=u_1u_2} \binom{x}{u_1}\binom{y}{u_2}$.

If $u_1 \neq \lambda$, $u_2 \neq \lambda$, either $1 \leq |u_1| \leq \lfloor \frac{m}{2} \rfloor$ or $1 \leq |u_2| \leq \lfloor \frac{m}{2} \rfloor$, so that either $\binom{x}{u_1} \theta_{0,q} 0$ or $\binom{y}{u_2} \theta_{0,q} 0$. Thus $\binom{xy}{u} \theta_{0,q} \binom{x}{u} + \binom{y}{u}$ and similarly $\binom{yx}{u} \theta_{0,q} \binom{y}{u} + \binom{x}{u}$. This establishes that H is abelian. □

Corollary 3.2 : Let $m > 2$: then $L_{0,q}^m \subseteq H_{2+\lfloor \log \frac{m}{3} \rfloor}$.

Proof: By lemma 3.3 , $L_{0,q}^2 \subseteq H_1$. Applying lemma 3.1 and lemma 3.4 inductively, it can be verified that for $m > 2$, $L_{0,q}^m \subseteq H_{i+1}$ when $2^i+2^{i-1} \leq m < 2^{i+1}+2^i$, i.e. when $3\cdot 2^{i-1} \leq m < 3\cdot 2^i$. It follows that $L_{0,q}^m \subseteq H_{2+\lfloor \log \frac{m}{3} \rfloor}$. □

IV. COUNTING SUBWORDS THRESHOLD T AND J-TRIVIAL MONOIDS.

In this chapter, we complete a result of Simon to characterize the variety of monoids corresponding to $\Delta^*_{*,1}$. It is shown that $\Delta^*_{t,1} = \Delta^*_{1,1}$ for any $t \geq 1$. Simon had obtained the characterization $\Delta^*_{1,1} \leftrightarrow \underline{J}$, where $\underline{J}$ denotes the variety of J-trivial monoids. We also prove that threshold t counting of subwords of length m can be done by threshold 1 counting of subwords of length m+t-1. Finally a description of congruences in $\Delta^m_{t,1}$ is given, which parallels our description for congruences in $\Delta^m_{0,q}$.

IV.1 Monoid characterization of $\Delta^{*}_{*,1}$.

It is known from lemma II.2.13 that $\Delta^{m}_{t,1} = \Omega(\Delta^{m}_{t,1}) \subseteq \Gamma_{+}$, since $\Omega \subseteq \Gamma_{+}$. Indeed, using the fact that $\Delta^{m}_{t,1} \subseteq \Delta^{1,\lceil\log(m+1)\rceil}_{t,1}$ and applying lemma II.2.10 inductively, it is seen that $x^{k} \alpha x^{k+1}$ for all $x \in A^{*}$, $\alpha \in A^{*}\Delta^{m}_{t,1}$, $k = (2^{\lceil\log(m+1)\rceil} - 1)t$. We are able to determine a smaller value of k such that $x^{k} \alpha x^{k+1}$ holds for all $x \in A^{*}$, $\alpha \in A^{*}\Delta^{m}_{t,1}$.

Lemma 1.1: Let $\alpha \in A^{*}\Delta^{m}_{t,1}$. Let

$$k = \begin{cases} 0 & \text{if} \quad t = 0 \text{ or } m = 0 \\ m & \text{if} \quad t = 1 \\ m+1 & \text{if} \quad 1 < t \leq m \\ t & \text{if} \quad 0 < m < t \, . \end{cases}$$

Then $x^{k} \alpha x^{k+1}$ for all $x \in A^{*}$.

Proof: Since $\alpha \supseteq \alpha^{m}_{t,1}$, it is sufficient to show that $\binom{x^{k}}{u} \theta_{t,1} \binom{x^{k+1}}{u}$ for all $x \in A^{*}$, $u \in (A \cup \lambda)^{m}$. The case when $t = 0$ or $m = 0$ is trivial since $\alpha = \omega$. Suppose now $t > 0$, $m > 0$. If $u = \lambda$, then $\binom{x^{k}}{\lambda} = \binom{x^{k+1}}{\lambda} = 1$. We also observe that for any $u \in (A \cup \lambda)^{m}$, $\binom{x^{|u|+r}}{u} = 0$ iff $\binom{x^{|u|}}{u} = 0$, for all $r \geq 0$. Now let $|u| \geq 1$ and $\binom{x^{|u|}}{u} \geq 1$;it is claimed that

$$(*) \quad \binom{x^{|u|+r}}{u} \geq \binom{|u|+r}{|u|} \quad \text{for all } r \geq 0 \, .$$

If $|u| = 1$, then $\binom{x}{u}^{|u|+r} \geq |u|+r = \binom{|u|+r}{|u|}$. Suppose $u = u'a$, $u' \in A^+$; since we assume that $\binom{x}{u}^{|u|} > 0$, we must have $\binom{x}{a} > 0$. The equation (*) trivially holds when $r = 0$. For $r > 0$, we have

$$\binom{x}{u}^{|u|+r} \geq \binom{x}{u}^{|u|+r-1} + \binom{x}{u'}^{|u|+r-1}$$

Assuming inductively that (*) holds for $|u'| < |u|$ and $r' < r$, we have

$$\binom{x}{u}^{|u|+r} \geq \binom{|u|+r-1}{|u|} + \binom{|u|+r-1}{|u'|} = \binom{|u|+r}{|u|}$$

and the induction step is complete. Consider now $\binom{x}{u}^{k}$. In all three cases left to deal with, the relation $k \geq m$ holds, hence $k \geq |u|$. Thus, in all three cases, $\binom{x}{u}^{k} = 0$ iff $\binom{x}{u}^{k+1} = 0$. If $\binom{x}{u}^{k} > 0$, we can use (*) to imply $\binom{x}{u}^{k} \geq \binom{k}{|u|}$. If $t = 1$, then $k = m$ and $\binom{k}{|u|} \geq \binom{k}{m} = 1$. If $1 < t \leq m$, then $k = m+1$ and therefore $\binom{x}{u}^{k} \geq \binom{m+1}{|u|} \geq m \geq t$. If $m < t$, then $k = t$ and $\binom{x}{u}^{k} \geq \binom{k}{|u|} \geq \binom{t}{t-1} = t$. Thus in all cases $\binom{x}{u}^{k} \geq t$, and since $\binom{x}{u}^{k+1} \geq \binom{x}{u}^{k}$, it follows that $\binom{x}{u}^{k+1} \theta_{t,1} \binom{x}{u}^{k}$. □

It can be verified that the values for k given in lemma 1.1 cannot be lowered for arbitrary alphabets. Indeed, for a fixed value of $m > 0$, let $A = \{a_1,\ldots,a_m\}$, $x = a_1 \ldots a_m$, $u = a_m \ldots a_1$. If $t = 1$, then m is

the smallest integer with the property that $\binom{x^m}{u} \theta_{1,1} \binom{x^{m+r}}{u}$ for all $r \geq 0$. Similarly, if $1 < t \leq m$, $m+1$ is the smallest integer with the property above. Finally if $m < t$, considering $u = a_1$, the reader may verify that t is the minimum integer satisfying $\binom{x^t}{a_1} \theta_{t,1} \binom{x^{t+1}}{a_1}$.

Let $\underline{J}$ denote the variety of J-trivial monoids. It is known that $M \in \underline{J}$ iff M and M^ρ are partially ordered, i.e. M (M^ρ) satisfies the property

$$m_1 m_2 m_3 = m_1 \quad \text{implies} \quad m_1 m_2 = m_1$$

for all $m_1, m_2, m_3 \in M$ (M^ρ) .

Lemma 1.2: Let $\alpha \in A^* \Delta^m_{t,1}$. Then α is a J-trivial congruence.

Proof: It is sufficient to show that $\alpha^m_{t,1}$ is a J-trivial congruence. Clearly, for any u, x, y, z $\in A^*$, $\binom{x}{u} \leq \binom{xy}{u} \leq \binom{xyz}{u}$. Hence $\binom{xyz}{u} \theta_{t,1} \binom{x}{u}$ implies $\binom{xy}{u} \theta_{t,1} \binom{x}{u}$, so that $x \; \alpha^m_{t,1} \; xyz$ implies $x \; \alpha^m_{t,1} \; xy$. This shows that $A^*/\alpha^m_{t,1}$ is a partially ordered monoid. A symmetric argument establishes that $(A^*/\alpha^m_{t,1})^\rho$ is partially ordered as well. □

The following deep result has been proved by Simon [72].

Lemma 1.3: If M is a J-trivial monoid generated by A, then $\alpha_M \in A^* \Delta^*_{1,1}$.

Theorem 1.1: i) For any $t \geq 1$, $\Delta^*_{t,1} \leftrightarrow \underline{J}$

ii) $\Delta^*_{*,1} \leftrightarrow \underline{J}$

Proof: By lemma 1.2, $\Delta^*_{t,1} \hookrightarrow \underline{J}$, for all $t \geq 0$. Conversely $\underline{J} \hookrightarrow \Delta^*_{1,1}$ by Simon's theorem. Since $\Delta^*_{1,1} \subseteq \Delta^*_{t,1}$ for all $t \geq 1$, we also have $\underline{J} \hookrightarrow \Delta^*_{t,1}$ for any $t \geq 1$. Hence $\Delta^*_{t,1} \leftrightarrow \underline{J}$. The second result follows directly. □

IV.2 More properties of $\Delta^*_{t,1}$.

Theorem 1.1 indicates that threshold t counting of subwords can always be implemented by threshold 1 counting since $\Delta^*_{t,1} = \Delta^*_{1,1}$. Of course it is not true that $\Delta^m_{t,1} = \Delta^m_{1,1}$ for all m. There thus exists a tradeoff between t and m. This situation is similar to the case investigated in chapter III, where $\Delta^*_{0,p_1^{c_1}\ldots p_n^{c_n}}$ was seen to be equal to $\Delta^*_{0,p_1\ldots p_n}$, though for any fixed m, only $\Delta^m_{0,p_1^{c_1}\ldots p_n^{c_n}} \supseteq \Delta^m_{0,p_1\ldots p_n}$ need hold. But unlike the situation of chapter III, we are this time able to determine a precise bound on the length of the subwords that must be considered when counting threshold 1 instead of threshold t.

Lemma 2.1: $\Delta^m_{t,1} \subseteq \Delta^{m+t-1}_{1,1}$

Proof: We want to prove that for any A, $\alpha^m_{t,1} \supseteq \alpha^{m+t-1}_{1,1}$. It is sufficient to show that $[x]_{\alpha^m_{t,1}}$ is a $\alpha^{m+t-1}_{1,1}$ language for an arbitrary $x \in A^*$.

Since $[x]_{\alpha^m_{t,1}} = \bigcap_{|u|\le m} \{y : \binom{y}{u} \theta_{t,1} \binom{x}{u}\}$ and

$$\{y : \binom{y}{u} \theta_{t,1} t\} = \overline{\bigcup_{j=0}^{t-1} \{y : \binom{y}{u} = j\}} ,$$

it needs only to be shown that $\{y : \binom{y}{u} = j\}$ is an $\alpha^{m+t-1}_{1,1}$ language for $j = 0,\ldots,t-1$. To complete the argument, we will prove that $\{y : \binom{y}{u} = j\}$, $j=0,\ldots,t-1$, can be expressed as a boolean function of sets in the family

$$\{\{z : \binom{z}{u} = 0\} , \{z : \binom{z}{u} \ge 1\} : |u| \le m+j\} .$$

This result clearly holds for j=0. If j>0, assume inductively that $\{y : \binom{y}{u} = j-1\} = \bigcup_{v\in Y_{j-1}} \{z : \binom{z}{v} \geq 1\} \cap \bigcap_{v\in N_{j-1}} \{z : \binom{z}{v} = 0\}$. (In particular, $Y_0 = \emptyset$, $N_0 = \{u\}$). Let $Y_j = \{v \in N_{j-1} : \binom{v}{u} = j\}$, $N_j = (N_{j-1} - Y_j) \cup \{v_0 a v_1 : v_0 v_1 \in Y_j, a \in A, \binom{v_0 a v_1}{u} > j\}$. Observe that $\max\{|v| : v \in Y_j\} = m+j-1$, $\max\{|v| : v \in N_j\} = m+j$. Thus the induction step will be complete if we show that

$$(*) \quad \{y : \binom{y}{u} = j\} = \bigcup_{v\in Y_j} \{z : \binom{z}{v} \geq 1\} \cap \bigcap_{v\in N_j} \{z : \binom{z}{v} = 0\} .$$

If z is in the set defined on the right-hand side of (*), then $\binom{z}{v} \geq 1$ for some v such that $\binom{v}{u} = j$. Hence $\binom{z}{u} \geq j$. If $\binom{z}{u} > j$, let v be any subword of z such that $\binom{v}{u} > j$ but no proper subword of v has this property. Then $|v| > |u| \geq 1$ and there exists a factorization of v as $v = v_0 a v_1$, such that $v_0 v_1 \in Y_k$ for some $k \leq j$. This implies that $v \in N_k$ and also that $v \in N_n$ for $k \leq n \leq j$. Thus (*) implies that $\binom{z}{v} = 0$, a contradiction. This proves that $\binom{z}{u} = j$. Conversely if $z \in \{y : \binom{y}{u} = j\}$ then clearly $z \in \bigcap_{v\in N_j} \{z : \binom{z}{v} = 0\}$. Again let v be any subword of z such that $\binom{v}{u} = \binom{z}{u} = j$ but no proper subword of v has this property. If j = 1, then $v = u \in Y_1$ since it was in N_0 . Otherwise there exists a such that $v = v_0 a v_1$ and $1 \leq \binom{v_0 v_1}{u} = k < j$. Hence $v_0 a v_1 \in N_n$ for $n = k,\ldots,j-1$ and $v \in Y_i$. Thus $z \in \bigcap_{v\in Y_j} \{z : \binom{z}{v} \geq 1\}$. □

It is easily seen that equality does not hold in lemma 2.1 Indeed let $L = \{x : \binom{x}{ab} = 0\} \subseteq \{a,b\}^*$. Then $\alpha_L \in \{a,b\}^* \Delta^2_{1,1}$; on the other hand $\alpha_L \notin \{a,b\}\Delta^1_{2,1}$ since $ba\ \alpha^1_{2,1}\ ab$ but $ba \in L$ and $ab \notin L$.

We now consider the problem of determining explicitly the congruences of $\Delta^*_{t,1}$. We use the same terminology as in the last part of III.2; f is a polynomial in $\mathbb{N}[A]$ and F is a finite family of such polynomials containing $1\cdot\lambda$. This time, to each $f \in F$ is associated a congruence θ_f in $\mathbb{N}\Gamma_+$. The definitions of α_F , f_a^R and f_a^L are as in III.2 .

We say that F is complete if the following properties hold:

i) f_a^R and f_a^L are linear combinations of elements of F, for each $f \in F$ of degree ≥ 1;

ii) if $f_a^R = k_1 f_1 + \ldots + k_n f_n$ and $\theta_{t,1}$, $\theta_{t_i,1}$ are the congruences associated with f and f_i respectively, then $t \leq k_i t_i$ for $i=1,\ldots,n$; the same condition is required to hold for f_a^L .

Lemma 2.2: Let F be complete. Then $\alpha_F \in A^*\Gamma$.

Proof: Let $x \,\alpha_F\, y$. Then, for any $a \in A$,

$$(xa)f = xf + xf_a^R = xf + k_1(x)f_1 + \ldots + k_n(x)f_n$$

and $(ya)f = yf + yf_a^R = yf + k_1(y)f_1 + \ldots + k_n(y)f_n$. Since $xf_i \;\theta_{t_i,1}\; yf_i$ and $t \leq k_i t_i$ we have $k_i(x)f_i \;\theta_{t,1}\; k_i(y)f_i$, so that $(xa)f \;\theta_{t,1}\; (ya)f$. Hence $xa \;\alpha_F\; ya$. By induction on the length of z, we then conclude that $xz \;\alpha_F\; yz$ for all $z \in A^*$. A symmetric argument, using f_a^L instead of f_a^R , proves that $zx \;\alpha_F\; zy$. The index of α_F is bounded by $\prod_{f \in F} |A^*/\alpha_f|$. Hence $\alpha_F \in A^*\Gamma$. □

Lemma 2.3: Let F, $F' \subseteq \mathbb{N}[A]$ be such that each $f \in F$ is a linear

combination of elements of F' . Furthermore if $f = k_1 f_1' + \ldots + k_n f_n'$, and $\theta_{t,1}$, $\theta_{t_i,1}$ are the congruences associated with f and f_i' respectively, assume that $t \leq k_i t_i$ for $i=1,\ldots,n$. Then $\alpha_F \supseteq \alpha_{F'}$.

Proof: Similar to the proof of lemma III.2.8 . □

Lemma 2.4: Let $F \in \mathbb{N}[A]$ with $\deg F \leq m$ have the property that it is complete and that for each $f \in F$ of degree ≥ 1, $f = \Sigma k_u u$ and $\theta_f = \theta_{t_f,1}$ implies $t_f \leq k_u t$ for all $u \in \operatorname{supp} f$. Then $\alpha_F \supseteq \alpha^m_{t,1}$.

Proof: Similar to the proof of lemma III.2.9 . □

The construction above thus provides a description of congruences in $A^*\Delta^m_{t,1}$ in terms of counting subwords. If $m=1$, all congruences in $A^*\Delta^m_{t,1}$ are of the form α_F for some F . This raises the problem of determining if there exists congruences in $A^*\Delta^m_{t,1}$, $m > 1$, other than those given by the α_F .

We close this chapter with the following observation. If $\alpha^m_{t,1} \in A^*\Delta^m_{t,1}$, then $\{x : \binom{x}{u} \geq t \text{ for all } u \in (A \cup \lambda)^m\}$ is a two-sided 0 of $A^*/\alpha^m_{t,1}$. Thus every J-trivial monoid contains a two-sided 0 . If M is $\underline{J}$-trivial and $\phi : M \to M'$ is a monoid morphism, then $0\phi^{-1} = I$ is a two-sided ideal of M , i.e. $MIM = I$. If F satisfies the properties of lemma 2.4, then the set $I = \{[x]_{\alpha^m_{t,1}} : (x)f \geq t_f \text{ for all } f \in F \text{ , where } \theta_f = \theta_{t_f,1}\}$ is a

two-sided ideal of $A^*/\alpha_{t,1}^m$ since $I = 0\phi^{-1}$ where 0 is the two-sided zero of A^*/α_F . We conjecture that all ideals of $A^*/\alpha_{t,1}^m$ can be described as above for suitable F .

V. MODULO COUNTING OF SUBWORDS IN CONTEXT AND SOLVABLE GROUPS

In this chapter, we characterize the monoids corresponding to the *-variety $\Delta_{0,*}^{*,*}$. It is shown that all solvable groups can be obtained by counting subwords in context, modulo some integer q. We also derive monoid characterizations for the intermediate varieties $\Delta_{0,q}^{1,i}$ and $\Delta_{0,q}^{*,i}$. But we first introduce congruences defined by one-sided contexts. It will be shown that in the group case, one-sided and two-sided contexts are equivalent. This property makes groups essentially easier to characterize.

V.1 One-sided context

In this section we introduce the notion of counting subwords in one-sided context.

Let $\gamma \in A^*\Gamma$, $u = a_1 \ldots a_m$, $x \in A^*$, $\vec{V} = ([v_0]_\gamma, \ldots, [v_m]_\gamma) \in (A^*/\gamma)^{m+1}$. Define

$$\binom{x}{u}_{\vec{V}} = \begin{cases} 1 & \text{if } u = \lambda \text{ (i.e. } m=0) \text{ and } x \,\gamma\, v_0 \\ \text{the number of factorizations of } x \text{ in the form} & \\ x = x_0 a_1 x_1 \ldots a_m x_m \text{ with } x_0 a_1 x_1 \ldots x_i \,\gamma\, v_i \text{ for } i=0,\ldots,m & \\ \text{otherwise.} & \end{cases}$$

$\vec{V}$ will be called a <u>left context</u>. We introduce the following operation on left contexts. If $\vec{V} = ([v_0]_\gamma, \ldots, [v_m]_\gamma) \in (A^*/\gamma)^{m+1}$, and $\vec{V}' = ([v_0']_\gamma, \ldots, [v_n']_\gamma) \in (A^*/\gamma)^{n+1}$, then

$$\vec{V}\,\vec{V}' = ([v_0]_\gamma, \ldots, [v_{m-1}]_\gamma, [v_m v_0']_\gamma, [v_m v_1']_\gamma, \ldots, [v_m v_n']_\gamma) \in (A^*/\gamma)^{m+n+1} .$$

The following lemma enables us to compute $\binom{x}{u}_{\vec{V}}$.

<u>Lemma 1.1</u>: Let $\gamma \in A^*\Gamma$, $u,x,y \in A^*$, $a \in A$, $\vec{V} \in (A^*/\gamma)^{|u|+1}$:

i) $$\binom{xy}{u}_{\vec{V}} = \sum_{\substack{u=u_1u_2 \\ \vec{V}=\vec{V}_1\vec{V}_2}} \binom{x}{u_1}_{\vec{V}_1} \binom{y}{u_2}_{\vec{V}_2} ;$$

ii)
$$\binom{a}{u}_{\vec{V}} = \begin{cases} 1 \text{ if } u=a \text{ , } \vec{V} = ([\lambda]_\gamma, [a]_\gamma) \\ \text{or } u=\lambda \text{ , } \vec{V} = ([a]_\gamma) \\ 0 \text{ otherwise} \end{cases}$$

iii)
$$\binom{\lambda}{u}_{\vec{V}} = \begin{cases} 1 \text{ if } u=\lambda \text{ , } \vec{V} = ([\lambda]_\gamma) \\ 0 \text{ otherwise.} \end{cases}$$

Proof: Left to the reader. □

Counting subwords in left context induces equivalences on A^* in a natural way. Define for any $x, y \in A^*$, $\gamma \in A^*\Gamma$,

$x \; \gamma(\overrightarrow{\alpha^m_{t,q}}) \; y$ iff, for all $u \in (A \cup \lambda)^m$, for all $\vec{V} \in (A^*/\gamma)^{|u|+1}$,

$$\binom{x}{u}_{\vec{V}} \; \theta_{t,q} \; \binom{y}{u}_{\vec{V}}$$

We extend this construction to varieties of congruences. Let Δ be any *-variety: then $\Delta(\overrightarrow{\Delta^m_{t,q}})$ is defined by

$$A^*\Delta(\overrightarrow{\Delta^m_{t,q}}) = \{\alpha : \alpha \supseteq \gamma(\overrightarrow{\alpha^m_{t,q}}) \text{ , } \gamma \in A^*\Gamma\} \text{ .}$$

Applying the construction recursively, we also define

$$\Delta(\overrightarrow{\Delta^{m,0}_{t,q}}) = \begin{cases} \Omega \text{ if } t=0 \text{ , } q=1 \\ \Delta \text{ otherwise} \end{cases}$$

and for $i>0$, $\Delta(\overrightarrow{\Delta^{m,i}_{t,q}}) = (\Delta(\overrightarrow{\Delta^{m,i-1}_{t,q}}))(\overrightarrow{\Delta^{m}_{t,q}})$.

It is clear that $A^*\Delta(\overrightarrow{\Delta^{m,i}_{t,q}}) = \{\alpha : \alpha \supseteq \gamma(\overrightarrow{\alpha^{m,i}_{t,q}}) \text{ for some } \gamma \in A^*\Delta\}$, where

$$\gamma(\overrightarrow{\alpha^{m,0}_{t,q}}) = \begin{cases} \omega \text{ if } t=0 \text{ and } q=1 \\ \gamma \text{ otherwise} \end{cases}$$

$$\gamma(\overrightarrow{\alpha^{m,i}_{t,q}}) = (\gamma(\overrightarrow{\alpha^{m,i-1}_{t,q}}))(\overrightarrow{\alpha^{m}_{t,q}}) .$$

The proof of the following results are similar to the corresponding ones on two-sided contexts and they are omitted here.

Lemma 1.2: If $\gamma \in A^*\Gamma$, then $\gamma(\overrightarrow{\alpha^{m}_{t,q}}) \in A^*\Gamma$.

Lemma 1.3: $\Delta(\overrightarrow{\Delta^{m,i}_{t,q}})$ is a *-variety of congruences.

Lemma 1.4: $\Delta(\overrightarrow{\Delta^{m,1}_{t,q}}) \subseteq \Delta(\overrightarrow{\Delta^{1,m}_{t,q}})$.

Lemma 1.5: i) If $x^k \gamma \lambda$ for all $x \in A^*$, then $x^{kq} \gamma(\overrightarrow{\alpha_{0,q}}) \lambda$ for all $x \in A^*$;

ii) If $\Delta \subseteq \Gamma_x$, then $\Delta(\overrightarrow{\Delta^{m,i}_{0,q}}) \subseteq \Gamma_x$.

Lemma 1.6: i) If $x^k \gamma x^{k+1}$ for all $x \in A^*$, then $x^{k+t} \gamma(\overrightarrow{\alpha_{t,1}}) x^{k+t+1}$ for all $x \in A^*$;

ii) If $\Delta \subseteq \Gamma_+$, then $\Delta(\overrightarrow{\Delta^{m,i}_{t,1}}) \subseteq \Gamma_+$.

Lemma 1.7: If $m \leq m'$, $i \leq i'$, $t \leq t'$, $q|q'$, then $\Delta(\overrightarrow{\Delta^{m,i}_{t,q}}) \subseteq \Delta(\overrightarrow{\Delta^{m',i'}_{t',q'}})$.

By duality, all the definitions and lemmas of this section can be restated in terms of right context. It is verified that the following result holds true.

Lemma 1.8: $(\Delta(\overrightarrow{\Delta^{m,i}_{t,q}}))^{\rho} = \Delta^{\rho}(\overleftarrow{\Delta^{m,i}_{t,q}})$.

We will write $\overrightarrow{\Delta^{m,i}_{t,q}}$ for $\Omega(\overrightarrow{\Delta^{m,i}_{t,q}})$ and $\overrightarrow{\alpha^{m,i}_{t,q}}$ for $\omega(\overrightarrow{\alpha^{m,i}_{t,q}})$.

Lemma 1.9: $\Delta(\overrightarrow{\Delta^{m}_{t,q}}) \subseteq \Delta(\Delta^{m}_{t,q})$.

Proof: It is sufficient to show that for any A^*, $\gamma \in A^*\Delta$, we have $\gamma(\overrightarrow{\alpha^{m}_{t,q}}) \supseteq \gamma(\alpha^{m}_{t,q})$. Suppose $x\ \gamma(\alpha^{m}_{t,q})\ y$ and consider $u=a_1 \ldots a_r \in (A \cup \lambda)^m$, $\vec{V} = ([v_0]_\gamma, \ldots, [v_{|u|}]_\gamma) \in (A^*/\gamma)^{|u|+1}$. Let

$$V = \{([v'_0]_\gamma, \ldots, [v'_{|u|}]_\gamma) : v'_0 a_1 v'_1 \ldots a_i v'_i\ \gamma\ v_i \text{ for } i=0,\ldots,|u|\} .$$

It is verified that

$$\binom{x}{u}_{\vec{V}} = \bigcup_{V' \in V} \binom{x}{u}_{V'} \quad \text{and} \quad \binom{y}{u}_{\vec{V}} = \bigcup_{V' \in V} \binom{y}{u}_{V'} .$$

Since $\binom{x}{u}_{V'}\ \theta_{t,q}\ \binom{y}{u}_{V'}$ for all $V' \in V$, we thus conclude that $\binom{x}{u}_{\vec{V}}\ \theta_{t,q}\ \binom{y}{u}_{\vec{V}}$. Therefore $x\ \gamma(\overrightarrow{\alpha^{m}_{t,q}})\ y$. □

Corollary 1.1: $\Delta(\overrightarrow{\Delta^{m,i}_{t,q}}) \subseteq \Delta(\Delta^{m,i}_{t,q})$

Thus, in general, counting subwords in one-sided context only can be done by counting subwords in two-sided contexts. We now show that the converse of lemma 1.9 holds when we are dealing with groups.

Lemma 1.10: Let $\Delta \subseteq \Gamma_x$. Then $\Delta(\Delta^m_{t,q}) \subseteq \Delta(\overrightarrow{\Delta^m_{t,q}})$.

Proof: It must be shown that for any A^*, $\gamma \in A^*\Delta$, we have $\gamma(\alpha^m_{t,q}) \supseteq \gamma(\overrightarrow{\alpha^m_{t,q}})$. Suppose $x\ \gamma(\overrightarrow{\alpha^m_{t,q}})\ y$ and consider $u=a_1\ldots a_r \in (A\cup\lambda)^m$, $V=([v_0]_\gamma,\ldots,[v_r]_\gamma)\in(A^*/\gamma)^{|u|+1}$. If $t=0$ and $q=1$, there is nothing to prove as both congruences are ω. Otherwise $x\ \gamma(\overrightarrow{\alpha^m_{t,q}})\ y$ implies $x\ \gamma\ y$. Let

$$\overrightarrow{V'} = ([v_0]_\gamma,[v_0a_1]_\gamma^{-1}[v_1],\ldots,[v_0a_1v_1\ldots a_r]_\gamma^{-1}[v_r]_\gamma) \in (A^*/\gamma)^{|u|+1}.$$

Then $\binom{x}{u}_V = \binom{x}{u}_{\overrightarrow{V'}}$ and $\binom{y}{u}_V = \binom{y}{u}_{\overrightarrow{V'}}$. Since $\binom{x}{u}_{\overrightarrow{V'}}\ \theta_{t,q}\ \binom{y}{u}_{\overrightarrow{V'}}$ then $\binom{x}{u}_V\ \theta_{t,q}\ \binom{y}{u}_V$ as well. Thus $x\ \gamma(\alpha^m_{t,q})\ y$. □

Corollary 1.2: If $\Delta \subseteq \Gamma_x$, then $\Delta(\Delta^{m,i}_{0,q}) = \Delta(\overrightarrow{\Delta^{m,i}_{0,q}})$.

The congruence $\overrightarrow{\alpha^{1,i}_{0,q}}$ is closely related to an operation on sets introduced in Straubing [79].

V.2 Monoid characterization of $\Delta^{*,*}_{0,*}$.

In this section, we characterize the varieties of monoids corresponding to the *-varieties $\Delta^{1,i}_{0,q}$, $\Delta^{*,i}_{0,q}$ for arbitrary $i\geq 0$, $q\geq 1$. This is done by showing that modulo counting of letters (subwords) in context is closely related to extensions of an abelian (nilpotent) group H by a group K.

Lemma 2.1: For any $q\geq 1$, let $\Pi_q = \{p : p \text{ is prime, } p|q\}$ and $I_q = \{n : n \text{ is a } \Pi_q \text{ integer}\}$. $\Delta^{m,i}_{0,q} \hookrightarrow \bigcup_{n\in I_q} \underline{M_{0,n}}$

Proof: By corollary II.2.2, $\Delta^{m,i}_{0,q} \subseteq \Delta^{1,i\lceil \log_2(m+1)\rceil}_{0,q}$. Applying lemma II.2.10 inductively, it is clear from the proof of the lemma that for all $x \in A^*$, $\alpha \in A^*\Delta^{1,i\lceil \log_2(m+1)\rceil}_{0,q}$, $x^{q^r}\ \alpha\ \lambda$ for some $r\geq 0$. Hence $\Delta^{m,i}_{0,q} \hookrightarrow \bigcup_{n\in I_q} \underline{M_{0,n}}$. □

Note that the *-varieties $\Delta^{m,i}_{0,q}$ are closed under reversal, by lemma II.2.13v).

Next we extend corollary II.2.2.

Lemma 2.2: Let $\gamma \in A^*\Gamma_x, q>1$. Then $H = \{[x]_{\gamma(\alpha^m_{0,q})} : x\ \gamma\ \lambda\} \in \underline{G_{nil,m}}$.

Proof: It follows from proposition I.3.1 i) that H is a normal subgroup of $A^*/\gamma(\alpha^m_{0,q})$ since $\gamma \supseteq \gamma(\alpha^m_{0,q})$. Consider the sequence of subgroups $H_n = \{[x]_{\gamma(\alpha^m_{0,q})} : x\ \gamma(\alpha^{m-n}_{0,q})\ \lambda\}$ for $n=0,\ldots,m$. By proposition I.3.1 ii),

we have $H_0 \simeq \{1\} \lhd H_1 \lhd \ldots \lhd H_m = H$. The result will follow if we show that $H_n/H_{n-1} \subseteq Z(H/H_{n-1})$. Using proposition I.3.1 iii), $H_n/H_{n-1} \simeq \{[x]_{\gamma(\alpha_{0,q}^{m-n+1})} : x\ \gamma(\alpha_{0,q}^{m-n})\ \lambda\}$ and $H/H_{n-1} \simeq \{[x]_{\gamma(\alpha_{0,q}^{m-n+1})} : x\ \gamma\ \lambda\}$. Thus it is sufficient to establish that $x\ \gamma(\alpha_{0,q}^{m-n})\ \lambda$, $y\ \gamma\ \lambda$ imply $xy\ \gamma(\alpha_{0,q}^{m-n+1})\ yx$. For any $u \in (A \cup \lambda)^{m-n+1}$, $V \in (A^*/\gamma)^{|u|+1}$, we have

$$\binom{xy}{u}_V = \sum_{\substack{u=u_1u_2 \\ V=V_1V_2}} \binom{x}{u_1}_{V_1} \binom{y}{u_2}_{V_2} .$$

Using the hypothesis on x and y, this yields $\binom{xy}{u}_V\ \theta_{0,q}\ \binom{x}{u}_V + \binom{y}{u}_V$. Similarly $\binom{yx}{u}_V\ \theta_{0,q}\ \binom{y}{u}_V + \binom{x}{u}_V$ and the proof is complete. □

Let $\underline{G_{der,i}}$ denote the family of solvable groups of derived length $\leq i$ and $\underline{G_{fit,i}}$ denote the family of solvable groups of fitting length $\leq i$. It can be shown that $\underline{G_{der,i}}$ and $\underline{G_{fit,i}}$ are varieties of monoids for any $i \geq 0$.

Lemma 2.3: Let $\alpha \in A^*\Delta_{0,q}^{1,i}$. Then $A^*/\alpha \in \underline{G_{der,i}}$.

Proof: It is sufficient to show that $A^*/\alpha_{0,q}^{1,i} \in \underline{G_{der,i}}$. This trivially holds if i=0 or q=1. Let i>0 and q>1, and consider the sequence of subgroups $H_n = \{[x]_{\alpha_{0,q}^{1,i}} : x\ \alpha_{0,q}^{1,n}\ \lambda\}$ for n=0,...,i. It follows from proposition I.3.1 that $H_0 = A^*/\alpha_{0,q}^{1,i} \rhd H_1 \rhd \ldots \rhd H_i = \{[\lambda]_{\alpha_{0,q}^{1,i}}\}$, and that $H_n/H_{n+1} \simeq \{[x]_{\alpha_{0,q}^{1,n+1}} : x\ \alpha_{0,q}^{1,n}\ \lambda\}$ for n=0,...,i-1. By lemma 2.2, H_n/H_{n+1} is abelian and thus $A^*/\alpha_{0,q}^{1,i}$ is solvable of derived length $\leq i$. Note also that $x \in H_n$ implies $x^q \in H_{n+1}$. □

Lemma 2.4: Let $\alpha \in A^*\Delta_{0,q}^{m,i}$. Then $A^*/\alpha \in G_{fit,i}$.

Proof: This proof is similar to that of lemma 2.3. Note that the series of subgroups obtained is such that H_n/H_{n+1} is a direct product of p_j-groups for p_j dividing q . □

To complete the results of this section, we will use notions from automata theory. We adapt the exposition of Ginzburg [68] to our needs.

A semiautomaton A is a triple (R,A,δ) where R is the finite set of states, A is the finite input alphabet and $\delta : R \times A \to R$ is the transition function; this induces a transition function $\delta : R \times A^* \to R$ by letting $(r,\lambda)\delta=r$, $(r,xa)\delta = ((r,x)\delta,a)\delta$, for all $r \in R$, $x \in A^*$, $a \in A$. The semiautomaton $A = (R,A,\delta)$ is covered by the semiautomaton $A' = (R',A,\delta')$ iff there exists $P \subseteq R'$ and a surjective function $h : P \to R$ such that for all $p \in P$, $a \in A$, $(ph,a)\delta = (p,a)\delta'h$; this relation is denoted $A \prec A'$. Any congruence $\gamma \in A^*\Gamma$ determines a semiautomaton in a natural way by letting $A_\gamma = (A^*/\gamma,A,\delta)$ with $([x]_\gamma,a)\delta = [xa]_\gamma$. For γ, $\gamma' \in A^*\Gamma$ we have $A_\gamma \prec A_{\gamma'}$ iff $A^*/\gamma \prec A^*/\gamma'$. For any monoid M, we also define $A_M = (M,M,\delta)$ where $(m,m')\delta = mm'$.

Given two semiautomata $A_1 = (R_1,A_1,\delta_1)$ and $A_2 = (R_2,A_2,\delta_2)$, and a function $g : R_1 \times A_1 \to A_2$, we define the cascade g-connection of A_1 and A_2 to be $A_1 \overset{g}{\circ} A_2 = (R_1 \times R_2, A_1,\delta)$ where

$$((r_1,r_2),a)\delta = ((r_1,a)\delta_1,(r_2,(r_1,a)g)\delta_2) .$$

Of particular importance in the sequel will be the case when $A_1 = A_\gamma$ for some $\gamma \in A_1^*\Gamma$. Note that, for any $x = a_1 \ldots a_n \in A_1^*$, $z \in A_1^*$, $r_2 \in R_2$, we have

$$(([z]_\gamma, r_2), x)\delta = ([zx]_\gamma, (r_2, ([z]_\gamma, a_1)g([za_1]_\gamma, a_2)g \ldots ([za_1 \ldots a_{n-1}]_\gamma, a_n)g)\delta_2) .$$

Lemma 2.5: Let $\gamma \in A^*\Gamma$, $H \in G_{ab} \cap M_{0,q}, q>1$. Then $A_\gamma \underset{g}{\circ} A_H \prec A_{\gamma(\alpha^1_{0,q})}$.

Proof: Let r be an arbitrary state of $A_\gamma \underset{g}{\circ} A_H$ and δ be its transition function. It is sufficient to show that $x \; \gamma(\alpha^1_{0,q}) \; y$ implies $(r,x)\delta = (r,y)\delta$, for any $x, y \in A^*$. But $r = ([z]_\gamma, h)$ for some $z \in A^*$, $h \in H$. Using the remark preceding the lemma and the properties of H, it follows that $(r,x)\delta = ([zx]_\gamma, hh_1^{c_1} \ldots h_n^{c_n})$ and $(r,y)\delta = ([zy]_\gamma, hh_1^{d_1} \ldots h_n^{d_n})$, where

$$H = \{h_1, \ldots, h_n\} , \; c_i \; \theta_{0,q} \sum_{([zv_0]_\gamma, a)g = h_i} \binom{x}{a} ([v_0]_\gamma, [v_1]_\gamma) ,$$

$$d_i = \sum_{([zv_0]_\gamma, a)g = h_i} \binom{y}{a}_{([v_0]_\gamma, [v_1]_\gamma)} . \text{ Since } x \; \gamma(\alpha^1_{0,q}) \; y , \text{ we have}$$

$zx \; \gamma \; zy$ and $c_i = d_i$ for $i = 1, \ldots, n$. Hence $(r,x)\delta = (r,y)\delta$. □

Lemma 2.6: Let $\gamma \in A^*\Gamma$ and $H \in G_{nil}$. Then there exists $q \geq 1$, $m \geq 0$, such that $A_\gamma \underset{g}{\circ} A_H \prec A_{\gamma(\alpha^m_{0,q})}$.

Proof: If $H = \{1\}$, then $A_\gamma \underset{g}{\circ} A_H$ is isomorphic to A_γ and, for any $q > 1$, $A_\gamma \prec A_{\gamma(\alpha^0_{0,q})} = A_\gamma$. Otherwise let $q = p_1 \ldots p_s$ where $\{p_1, \ldots, p_s\} = \{p : p \text{ is prime and } p \,||\, |H|\}$. By lemma III.1.4, there

exists $m \geq 0$ such that $\alpha_H \supseteq \eta^m_{0,q}$, $\eta^m_{0,q} \in H^*\Delta^m_{0,q}$ where α_H is the congruence corresponding to the natural morphism $\alpha_H : H^* \to H$. Let $x = a_1 \ldots a_n$, $y = a'_1 \ldots a'_j \in A^*$. Then for any $z \in A^*$, $h \in H$, we get $(([z]_\gamma,h),x)\delta = ([zx]_\gamma, hh_1 \ldots h_n)$ and $([z]_\gamma,h),y)\delta = ([zy]_\gamma, hh'_1 \ldots h'_j)$ where δ is the transition function of $A_\gamma \underset{g}{\circ} A_H$, $h_i = ([za_1 \ldots a_{i-1}]_\gamma, a_i)g$ for $i=1,\ldots,n$ and $h'_i = ([za'_1 \ldots a'_{i-1}]_\gamma, a'_i)g$ for $i=1,\ldots,j$. Viewing $h_1 \ldots h_n$ as a string in H^* , we have, for any $w \in (H \cup \lambda)^m$,

$$\binom{h_1 \ldots h_n}{w} = \sum_{\substack{u \in A^{|w|} \\ V \in V_u}} \binom{x}{u}_V ,$$

where

$$V_{b_1 \ldots b_k} = \{([v_0]_\gamma, \ldots, [v_k]_\gamma) \in (A^*/\gamma)^{k+1} : ([zv_0 b_1 v_1 \ldots v_{i-1}]_\gamma, b_i)g = h_i \text{ for } i = 1,\ldots,k\} .$$

Similarly $\binom{h'_1 \ldots h'_j}{w} = \sum_{\substack{u \in A^{|w|} \\ V \in V_u}} \binom{y}{u}_V$. Suppose $x \; \gamma(\alpha^m_{0,q}) \; y$. Then $x \; \gamma \; y$ and $[zx]_\gamma = [zy]_\gamma$. Also $\binom{x}{u}_V \; \theta_{0,q} \binom{y}{u}_V$ so that $\binom{h_1 \ldots h_n}{w} \theta_{0,q} \binom{h'_1 \ldots h'_j}{w}$. Since $\alpha_H \supseteq \eta^m_{0,q}$, it follows that $h_1 \ldots h_n = h'_1 \ldots h'_j$ and therefore $hh_1 \ldots h_n = hh'_1 \ldots h'_j$. Altogether, this proves that $A_\gamma \underset{g}{\circ} A_H \prec A_{\gamma(\alpha^m_{0,q})}$. □

Lemma 2.7 (Ginzburg [68]): Let $H \lhd G$, where G is a group generated by a set A. Let $\alpha_G \in A^*\Gamma_\times$ and $\alpha_{G/H} \in A^*\Gamma_\times$ be the congruences corresponding to the morphisms $\alpha_G : A^* \to G$, $\alpha_{G/H} : A^* \to G/H$ respectively. Then $A_{\alpha_G} \prec A_{\alpha_{G/H}} \underset{g}{\circ} A_H$ for some function $g : A^*/\alpha_{G/H} \times A \to H$.

Let $\underline{G_{der,i,q}}$ denote the variety of groups G for which there exists a normal series $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_i = \{1\}$ where $G_i/G_{i+1} \in \underline{G_{ab}} \cap \underline{M_{0,q}}$. Let $\underline{G_{fit,i,q}}$ denote the variety of groups G for which there exists a normal series $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_i = \{1\}$ where G_i/G_{i+1} is a nilpotent group which is the direct product of p_j-groups for p_j dividing q.

Lemma 2.8: Let $G \in \underline{G_{der,i,q}}$ be generated by A. Then $\alpha_G \in A^*\Delta^{1,i}_{0,q}$.

Proof: If i=0 or q=1, then $G = \{1\}$; thus $\alpha_G = \omega \supseteq \alpha^{1,i}_{0,q} = \omega$. If $i > 0$ and $q > 1$, there exists $H \triangleleft G$ such that $H \in \underline{G_{ab}} \cap \underline{M_{0,q}}$ and $G/H \in \underline{G_{der,i-1,q}}$. By lemma 2.7, $A_{\alpha_G} \prec A_{\alpha_{G/H}} \underset{g}{\circ} A_H$. Assuming inductively that $\alpha_{G/H} \supseteq \alpha^{1,i-1}_{0,q}$, $A_{\alpha_G} \prec A_{\alpha^{1,i-1}_{0,q}} \underset{g}{\circ} A_H$. By lemma 2.5 and transitivity of covering, we conclude that $A_{\alpha_G} \prec A_{\alpha^{1,i}_{0,q}}$. Hence $A^*/\alpha_G \prec A^*/\alpha^{1,i}_{0,q}$ and $\alpha_G \in A^*\Delta^{1,i}_{0,q}$. □

Lemma 2.9: Let $G \in \underline{G_{fit,i,q}}$ be generated by A. Then $\alpha_G \in A^*\Delta^{*,i}_{0,q}$.

Proof: If $i = 0$ or $q = 1$, then $G = \{1\}$ and $\alpha_G = \omega \supseteq \alpha^{0,i}_{0,q} = \omega$. If $i > 0$ and $q > 1$, there exists $H \triangleleft G$ such that $G/H \in \underline{G_{fit,i-1,q}}$ and H is a direct product of p_j-groups for p_j dividing q. The rest of the proof parallels that of lemma 2.8 with lemma 2.6 being used in the induction step. □

Theorem 2.1: i) $\Delta^{1,i}_{0,q} \leftrightarrow \underline{G_{der,i,q}}$

ii) $\Delta^{1,i}_{0,*} \leftrightarrow \underline{G_{der,i}}$

iii) $\Delta_{0,q}^{*,i} \leftrightarrow \underline{G_{fit,i,q}}$

iv) $\Delta_{0,*}^{*,i} \leftrightarrow \underline{G_{fit,i}}$

v) $\Delta_{0,*}^{1,*} = \Delta_{0,*}^{*,*} \leftrightarrow \underline{G_{sol}}$

Proof: By lemma 2.3, $\Delta_{0,q}^{1,i} \hookrightarrow \underline{G_{der,i,q}}$. By lemma 2,8, $\underline{G_{der,i,q}} \hookrightarrow \Delta_{0,q}^{1,i}$. Thus i) holds. Taking the union of these respective families over all $q \geq 1$ yields ii). The proof of iii) and iv) is similar, this time using lemmas 2.4 and 2.9. Finally v) is obtained from ii) and iv) by taking the union over all $i \geq 0$. □

Straubing [79] obtained characterizations of the family of languages corresponding to $\underline{G_{der,i}}$ and $\underline{G_{sol}}$. As we have mentioned earlier, he made use of an operation on sets which is the language equivalent of our congruences $\overrightarrow{\alpha_{0,q}^{1,i}}$.

VI. THRESHOLD COUNTING OF SUBWORDS IN CONTEXT AND APERIODIC MONOIDS

Having considered the case of modulo counting in the last chapter, we now characterize the monoids corresponding to the *-variety $\Delta_{*,1}^{*,*}$. It is shown that $\Delta_{*,1}^{*,*} \leftrightarrow \underline{Ap}$. We also obtain information on the intermediate *-varieties $\Delta_{t,1}^{1,i}$ and $\Delta_{t,1}^{*,i}$, though no complete characterization has been established. Finally we carry out the same investigation when one-sided contexts are considered. We show that $\overrightarrow{\Delta_{*,1}^{*,*}} \leftrightarrow \underline{R}$, the variety of R-trivial monoids.

VI.1 Monoid characterization of $\Delta^{*,*}_{*,1}$.

In chapter V, it was seen that many well-known families of groups could be characterized in terms of our congruences. This indicates that the operation of counting subwords in context is a natural one from the algebraic point of view. In this section, we consider the aperiodic equivalent of the families of group congruences that were studied in the last chapter. First it is shown that globally the *-variety $\Delta^{*,*}_{*,1}$ is in correspondence with the family of all aperiodic monoids. Then we obtain some partial results on the intermediate *-varieties $\Delta^{1,i}_{t,1}$ and $\Delta^{*,i}_{t,1}$. These results parallel those obtained in the case where modulo q counting was used.

Lemma 1.1: $\Delta^{*,*}_{*,1} \hookrightarrow \underline{Ap}$.

Proof: Since $\Omega \subseteq \Gamma_+$, it follows from lemma II.2.13 iv) that $\Delta^{m,i}_{t,1} \subseteq \Gamma_+$, for all $m,i,t \geq 0$. Hence $\Delta^{*,*}_{*,1} \subseteq \Gamma_+$, or equivalently $\Delta^{*,*}_{*,1} \hookrightarrow \underline{Ap}$. □

Using the fact that $\Delta^{m,i}_{t,1} \subseteq \Delta^{1,i}_{t,1}$ and lemma II.2.11 inductively, we see that for $k = (2^{i\lceil \log(m+1) \rceil} - 1)t$, we have $x^k \alpha x^{k+1}$ for all $x \in A^*$, $\alpha \in A^*\Delta^{m,i}_{t,1}$. Note also that by lemma II.2.13 v), each family $\Delta^{m,i}_{t,1}$ is closed under reversal.

Let U be the monoid represented in figure VI.1 .

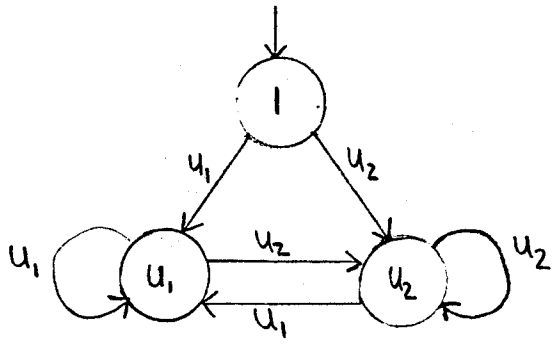


Figure VI.1 Representation of the monoid U .

Lemma 1.2: If $\gamma \in A^*\Gamma$, then $A_\gamma \underset{g}{o} A_U \prec A_{\gamma(\alpha_{1,1}^{1,2})}$.

Proof: Let $([z]_\gamma,m)$ be an arbitrary state of $A_\gamma \underset{g}{o} A_U$ and let δ be its transition function. We must show that $x\ \gamma(\alpha_{1,1}^{1,2})\ y$ implies $(([z]_\gamma,m),x)\delta = (([z]_\gamma,m),y)\delta$. For any $v \in A^*$, $a \in A$, define $W_{v,a} = \{[v']_{\gamma(\alpha_{1,1}^{1,1})} : \binom{v'}{a'}_{([v_0]_\gamma,[v_1]_\gamma)}\ \theta_{1,1}\ 0$ for any $v_0 \in A^*$, $a' \in A$ such that $([zvav_0]_\gamma,a') \notin 1g^{-1}\}$.

Suppose $x = a_1\ldots a_k$ and $y = a_1'\ldots a_n'$. Then $(([z]_\gamma,m),x)\delta = ([zx]_\gamma,mm_1\ldots m_k)$ and $(([z]_\gamma,m),y)\delta = ([zy]_\gamma,mm_1'\ldots m_n')$ where $m_j = ([za_1\ldots a_{j-1}]_\gamma,a_j)g$ for $j=1,\ldots,k$ and $m_j' = ([za_1'\ldots a_{j-1}']_\gamma,a_j')g$ for $j=1,\ldots,n$. Since $\gamma \supseteq \gamma(\alpha_{1,1}^{1,2})$, $x\ \gamma(\alpha_{1,1}^{1,2})\ y$ implies $[zx]_\gamma = [zy]_\gamma$. If $mm_1\ldots m_k = 1$, it must be that $m=1$ and $m_j \in 1g^{-1}$ for $j=1,\ldots,k$. This is possible iff

$$([zv_0]_\gamma,a) \notin 1g^{-1} \overset{\Sigma}{a\in A} \binom{x}{a}_{([v_0]_\gamma,[v_1]_\gamma)}\ \theta_{1,1}\ 0 .$$

Since $\gamma(\alpha_{1,1}^{1,1}) \supseteq \gamma(\alpha_{1,1}^{1,2})$ we have $\binom{x}{a}_V\ \theta_{1,1}\ \binom{y}{a}_V$ for all $a \in A$, $V \in (A^*/\gamma)^2$. Therefore

$$([zv_0]_\gamma,a) \notin \mathrm{lg}^{-1} \binom{x}{a}_{([v_0]_\gamma,[v_1]_\gamma)}^{\sum_{a\in A}} \theta_{1,1} ([zv_0]_\gamma,a) \notin \mathrm{lg}^{-1} \binom{y}{a}_{([v_0]_\gamma,[v_1]_\gamma)}^{\sum_{a\in A}}$$

and $mm_1\ldots m_k = 1$ iff $mm_1'\ldots m_n' = 1$. If $mm_1\ldots m_k = u_1$, there must exist an index j, $0\le j\le k$ such that $m_j = u_1$ and $m_s \in \mathrm{lg}^{-1}$ for s=j+1,...,k (we take m_0 to be m). This is possible iff

$$\sum_{\substack{a\in A \\ V\in V_a}} \binom{x}{a}_V \theta_{1,1} 1$$

where $V_a = \{([v_0]_{\gamma(\alpha_{1,1}^{1,1})}, [v_1]_{\gamma(\alpha_{1,1}^{1,1})}) :$

$$([zv_0]_\gamma,a) \in u_1\mathrm{g}^{-1}, [v_1]_{\gamma(\alpha_{1,1}^{1,1})} \in W_{v_0,a}\},$$

or $m = u_1$ and $([zv_0]_\gamma,a) \notin \mathrm{lg}^{-1} \binom{x}{a}_{([v_0]_\gamma,[v_1]_\gamma)}^{\sum_{a\in A}} \theta_{1,1} 0$.

Again, the fact that $x\ \gamma(\alpha_{1,1}^{1,2})\ y$ implies that $mm_1\ldots m_k = u_1$ iff $mm_1'\ldots m_n' = u_1$. The case $mm_1\ldots m_k = u_2$ is handled similarly. □

Lemma 1.3 (Krohn-Rhodes [65]): If $\alpha \in A^*\Gamma_+$, then $A_\alpha \prec U \circ_{g_1} \ldots \circ_{g_n} U$ for some $n\ge 0$.

Lemma 1.4: Let $M \in \underline{Ap}$ be generated by A. Then $\alpha_M \in A^*\Delta_{1,1}^{1,*}$.

Proof: By lemma 1.3, $A_{\alpha_M} \prec U \circ_{g_1} \ldots \circ_{g_n} U$ for some $n\ge 0$. Equivalently $A_{\alpha_M} \prec A_\omega \circ_{g_0} U \circ_{g_1} \ldots \circ_{g_n} U$ and applying inductively lemma 1.2,

$A_{\alpha_M} \prec A_{\alpha^{1,2n}_{1,1}}$. Therefore $\alpha_M \in A^*\Delta^{1,2n}_{1,1}$. □

Theorem 1.1: $\Delta^{1,*}_{1,1} = \Delta^{*,*}_{*,1} \leftrightarrow \underline{Ap}$.

Proof: By lemma 1.1, $\Delta^{*,*}_{*,1} \hookrightarrow \underline{Ap}$. By lemma 1.4, $\underline{Ap} \hookrightarrow \Delta^{1,*}_{1,1}$. The conclusion follows from the inclusion $\Delta^{1,*}_{1,1} \subseteq \Delta^{*,*}_{*,1}$. □

From theorem 1.1, it is seen that the sequence of varieties $\Delta^{m,i}_{t,1}$ ultimately equals the sequence of varieties $\Delta^{1,i}_{1,1}$. This raises the problem of analyzing the trade-off between the various indices.

Lemma 1.5: $\Delta^{1,i}_{t,1} \subseteq \Delta^{t,i}_{1,1}$.

Proof: The lemma trivially holds when i=0. We establish the case i>0 by showing that the set $\{x : \binom{x}{a}_V \theta_{t,1} j\}$ is an $\alpha^{t,i}_{1,1}$ language for all $a \in A$, $V \in (A^*/\alpha^{1,i-1}_{t,1})^2$, $j = 0,\ldots,t$. Let $V = ([v_0]_{\alpha^{1,i-1}_{t,1}}, [v_1]_{\alpha^{1,i-1}_{t,1}})$, and $V' = \{([v'_0]_{\alpha^{t,i-1}_{1,1}}, [v'_1]_{\alpha^{t,i-1}_{1,1}}) : v'_0 \; \alpha^{1,i-1}_{t,1} \; v_0, v'_1 \; \alpha^{1,i-1}_{t,1} \; v_1\}$. The set V' is well defined, since we can assume inductively that $\alpha^{1,i-1}_{t,1} \supseteq \alpha^{t,i-1}_{1,1}$. Then $\{x : \binom{x}{a}_V \theta_{t,1} 0\} = \{x : \bigcup_{V' \in V} \binom{x}{a}_{V'} \theta_{1,1} 0\}$

Let $0<j<t$ and consider a fixed $a \in A$, $V = ([v_0]_{\alpha^{1,i-1}_{t,1}}, [v_1]_{\alpha^{1,i-1}_{t,1}})$. Let $V_0 = \{([v'_0]_{\alpha^{t,i-1}_{t,1}}, \ldots, [v'_j]_{\alpha^{t,i-1}_{t,1}}) : v'_0 a v'_1 \ldots a v'_k \; \alpha^{1,i-1}_{t,1} \; v_0$,

$$v'_{k+1} a v'_{k+2} \ldots a v'_j \; \alpha^{1,i-1}_{t,1} \; v_1 \text{ , } k=0,\ldots,j-1\}$$

and $V_1 = \{([v_0']_{\alpha_{1,1}^{t,i-1}}, \ldots, [v_{j+1}']_{\alpha_{1,1}^{t,i-1}}) : v_0'av_1'\ldots av_k' \ \alpha_{t,1}^{1,i-1} \ v_0 ,$

$v_{k+1}'av_{k+2}'\ldots av_{j+1}' \ \alpha_{t,1}^{1,i-1} \ v_1 , \ k=0,\ldots,j\}$.

Again the induction hypothesis implies that V_0 , V_1 are well-defined.

But $\{x : \binom{x}{a}_V \ \theta_{t,1} \ j\} = \bigcup_{V_0 \in V_0} \{y : \binom{y}{a^j}_{V_0} \ \theta_{1,1} \ 1\}$

$\bigcap \bigcap_{V_1 \in V_1} \{y : \binom{y}{a^{j+1}}_{V_1} \ \theta_{1,1} \ 0\}$.

Hence $\{x : \binom{x}{a} \ \theta_{t,1} \ j\}$ is an $\alpha_{1,1}^{t,1}$ language. Finally, we note that

$$\{x : \binom{x}{a}_V \ \theta_{t,1} \ t\} = \overline{\bigcup_{j=0}^{t-1} \{x : \binom{x}{a}_V \ \theta_{t,1} \ j\}} ,$$

and the proof is complete. □

Corollary 1.1: $\Delta_{t,1}^{m,i} \subseteq \Delta_{1,1}^{1,i\lceil \log_2(m+1)\rceil \lceil \log_2(t+1)\rceil}$

Proof: By corollary II.2.2, the inclusion $\Delta_{t,1}^{m,i} \subseteq \Delta_{t,1}^{1,i\lceil \log_2(m+1)\rceil}$ holds. By lemma 1.5, we obtain $\Delta_{t,1}^{m,i} \subseteq \Delta_{1,1}^{t,i\lceil \log_2(m+1)\rceil}$. Applying corollary II.2.2 again, the result follows. □

We have not been able to characterize completely the *-varieties $\Delta_{t,1}^{1,i}$ and $\Delta_{*,1}^{*,i}$ in terms of monoids. We now present partial results in that direction.

The approach taken here has been introduced by Straubing [80]. Let $\phi : M_1 \to M_2$ be a monoid morphism. For any idempotent $e \in M_2$, the set $e\phi^{-1}$ is a subsemigroup of M_1. If $\underline{S}$ is a family of semigroups, ϕ is said to be an $\underline{S}$-morphism iff $e\phi^{-1} \in \underline{S}$ for any idempotent $e \in M_2$. If $\underline{M}$ is a variety of monoids and $\underline{S}$ a variety of semigroups, let $\underline{M}(\underline{S}) = \{M : M \prec M_1$ and there exists an $\underline{S}$-morphism $\phi : M_1 \to M_2$, $M_2 \in \underline{M}\}$. Straubing used the notation $\underline{S}(\underline{M})$ for this concept: we have reversed the order to be consistent with our notation for the *-varieties $\Delta(\Delta^m_{t,q})$. We also define $\underline{M}(\underline{S}^0) = \underline{M}$ and for $i \geq 1$, $\underline{M}(\underline{S}^i) = (\underline{M}(\underline{S}^{i-1}))(\underline{S})$. It can be verified that $\underline{M}(\underline{S}^i)$ is a variety of monoids for all $i \geq 0$.

We now describe a method by which one can induce a variety of semigroups from a variety of monoids. It is known that any variety of monoids (semigroups) can be described by equations (see Eilenberg [76]). For example, the pair of equations $mm' = m'm$ and $m^t = m^{t+1}$ defines the variety $\underline{M_{com}} \cap \underline{M_{t,1}}$; another example is the variety $\underline{J}$ which is characterized by the family of equations $m^t = m^{t+1}$, $(mm')^t = (m'm)^t$ for some $t \geq 0$ (i.e. $M \in \underline{J}$ iff there exists $t \geq 0$ such that the above pair of equations is satisfied for all $m, m' \in M$). If $E = \{e_1 = e_1', \ldots, e_n = e_n'\}$ is a set of equations defining the variety $\underline{M}$, let $\underline{CM}$ be the variety of semigroups defined by the equations $z_0e_1z_1 = z_0e_1'z_1, \ldots, z_0e_nz_1 = z_0e_n'z_1$. Thus a semigroup is in $\underline{CM}$ iff the equations defining $\underline{M}$ are satisfied in any context (z_0, z_1). Note that the family of monoids contained in $\underline{CM}$ is precisely $\underline{M}$ (take $z_0 = z_1 = 1$).

Lemma 1.6: Let $\Delta \leftrightarrow \underline{M}$. Then $\Delta(\Delta_{t,1}) \hookrightarrow \underline{M}\ (C(M_{com} \cap M_{t,1}))$.

Proof: Let $\gamma \in A^*\Delta$ and $\phi : A^*/\gamma(\alpha_{t,1}) \to A^*/\gamma$. It needs to be shown that ϕ is a $C(M_{com} \cap M_{t,1})$-morphism. Let $e = [w]_\gamma$ be an idempotent in A^*/γ and let $z_0, z_1, x, y \in A^*$ be such that their respective $\gamma(\alpha_{t,1})$ class is in $e\phi^{-1}$. We must show that $z_0xyz_1\ \gamma(\alpha_{t,1})\ z_0yxz_1$ and $z_0x^tz_1\ \gamma(\alpha_{t,1})\ z_0x^{t+1}z_1$. It is clear that $z_0xyz_1\ \gamma\ z_0yxz_1$ and $z_0x^tz_1\ \gamma\ z_0x^{t+1}z_1$ so that

$$\begin{pmatrix} z_0xyz_1 \\ \lambda \end{pmatrix} \theta_{t,1} \begin{pmatrix} z_0yxz_1 \\ \lambda \end{pmatrix} \text{ and } \begin{pmatrix} z_0x^tz_1 \\ \lambda \end{pmatrix} \theta_{t,1} \begin{pmatrix} z_0x^{t+1}z_1 \\ \lambda \end{pmatrix}.$$

Let $a \in A$, $V = ([v_0]_\gamma , [v_1]_\gamma) \in (A^*/\gamma)^2$.

Let $V_0 = \{([v_0]_\gamma , [v_1']_\gamma) : v_1'w\ \gamma\ v_1\}$,

$V_1 = \{([v_0']_\gamma , [v_1']_\gamma) : wv_0'\ \gamma\ v_0 , v_1'w\ \gamma\ v_1\}$,

and

$V_2 = \{([v_0']_\gamma , [v_1]_\gamma) : wv_0'\ \gamma\ v_0\}$.

Then

$$\begin{pmatrix} z_0xyz_1 \\ a \end{pmatrix}_V = V_0 \overset{\Sigma}{\varepsilon} V_0 \begin{pmatrix} z_0 \\ a \end{pmatrix}_{V_0} + V_1 \overset{\Sigma}{\varepsilon} V_1 \begin{pmatrix} x \\ a \end{pmatrix}_{V_1} + V_1 \overset{\Sigma}{\varepsilon} V_1 \begin{pmatrix} y \\ a \end{pmatrix}_{V_1} + V_2 \overset{\Sigma}{\varepsilon} V_2 \begin{pmatrix} z_1 \\ a \end{pmatrix}_{V_2}$$

and similarly for $\begin{pmatrix} z_0yxz_1 \\ a \end{pmatrix}_V$. Thus $\begin{pmatrix} z_0xyz_1 \\ a \end{pmatrix}_V \theta_{t,1} \begin{pmatrix} z_0yxz_1 \\ a \end{pmatrix}_V$, and $z_0xyz_1\ \gamma(\alpha_{t,1})\ z_0yxz_1$. Also $\begin{pmatrix} z_0x^tz_1 \\ a \end{pmatrix}_V = V_0 \overset{\Sigma}{\varepsilon} V_0 \begin{pmatrix} z_0 \\ a \end{pmatrix}_{V_0} + \overset{t\Sigma}{V_1 \varepsilon V_1} \begin{pmatrix} x \\ a \end{pmatrix}_{V_1} + V_2 \overset{\Sigma}{\varepsilon} V_2 \begin{pmatrix} z_1 \\ a \end{pmatrix}_{V_2}$

and $\binom{z_0 x^{t+1} z_1}{a}_V = V_0 \overset{\Sigma}{\varepsilon} V_0 \binom{z_0}{a}_{V_0} + (t+1)\ V_1 \overset{\Sigma}{\varepsilon} V_1 \binom{x}{a}_{V_1} + V_2 \overset{\Sigma}{\varepsilon} V_2 \binom{z_1}{a}_{V_2}$.

Thus $\binom{z_0 x^t z_1}{a}_V \theta_{t,1} \binom{z_0 x^{t+1} z_1}{a}_V$ and $z_0 x^t z_1\ \gamma(\alpha_{t,1})\ z_0 x^{t+1} z_1$. □

Corollary 1.1:

i) $\Delta^{1,i}_{t,1} \hookrightarrow \underline{1}\ (C(M_{com} \cap M_{t,1})^i)$

ii) $\Delta^{1,i}_{*,1} \hookrightarrow \underline{1}\ (C(M_{com} \cap \underline{Ap})^i)$

Proof: We can apply lemma 1.6 inductively to get i). The second assertion follows directly. □

Note the special case i=1. The morphism $\phi : A^*/\alpha^{1,1}_{t,1} \to A^*/\omega$ has the property that $e\phi^{-1} = A^*/\alpha^{1,1}_{t,1}$. Thus $e\phi^{-1}$ is a monoid and $\underline{1}\ (C(M_{com} \cap M_{t,1})) = \underline{M_{com}} \cap \underline{M_{t,1}}$. In this case, we know that the converse of lemma 1.6 holds true.

This property of congruences in $\Delta^{1,i}_{t,1}$ is an aperiodic equivalent of the property of congruences in $\Delta^{1,i}_{0,q}$ described in theorem V.2.1. If G is a group and $\phi : G \to G'$ is a CM-morphism, then $e\phi^{-1} \varepsilon$ CM for each idempotent e of G'. But the only idempotent of G' is 1 and $1\phi^{-1}$ contains the identity of G, i.e. it is a monoid (in fact a subgroup of G). Thus theorem V.2.1 i) could be restated as $\Delta^{1,i}_{0,q} \leftrightarrow \underline{1}\ (C(M_{com} \cap M_{0,q})^i)$, which makes clear the parallel between threshold and modulo counting.

Lemma 1.7: $\underline{Ap} = \bigcup_{i\geq 0} \underline{1}\,(C(M_{com} \cap M_{t,1})^i)$ for any $t > 0$.

Proof: By theorem 1.1 $\underline{Ap} \leftrightarrow \Delta^{1,*}_{t,1}$ for any $t > 0$. It thus follows from corollary 1.1 that $\underline{Ap} \subseteq \bigcup_{i\geq 0} \underline{1}\,(C(M_{com} \cap M_{t,1})^i)$. To establish the converse inclusion, it is sufficient to show that $\underline{M}(C(M_{com} \cap M_{t,1})) \subseteq \underline{Ap}$ whenever $\underline{M} \subseteq \underline{Ap}$. Let $\phi : M_1 \to M_2$ be a $C(M_{com} \cap M_{t,1})$ - morphism and $M_2 \in \underline{M}$. If G is a group in M_1 then $G\phi$ is a group in M_2; hence $G\phi = e = e^2$ since $M_2 \in \underline{Ap}$. Thus $G \subseteq e\phi^{-1} \in C(M_{com} \cap M_{t,1})$. It is easily seen that every monoid in $C(M_{com} \cap M_{t,1})$ is aperiodic. Hence G is trivial and the result follows. □

The result we have been able to derive for the *-varieties $\Delta^{*,i}_{t,1}$ is weaker. For any variety of monoids $\underline{M}$, let $\underline{LM} = \{S : eSe \in \underline{M}$ for each idempotent e of S$\}$. It can be verified that $\underline{LM}$ is a variety of semigroups and that $\underline{CM} \subseteq \underline{LM}$.

Lemma 1.8: Let $\gamma \in A^*\Gamma$, $x, y, z \in A^*$. If $x\,\gamma\, y\,\gamma\, z\,\gamma\, x^2$ and $z\,\gamma(\alpha^m_{t,1})z^2$, then

i) $(zxz)^{m+t-1}\,\gamma(\alpha^m_{t,1})\,(zxz)^{m+t}$

ii) $(zxzyz)^{m+t-1}\,\gamma(\alpha^m_{t,1})\,(zyzxz)^{m+t-1}$.

Proof: i) Let $u \in (A \cup \lambda)^m$, $V = ([v_0]_\gamma, \ldots, [v_m]_\gamma) \in (A^*/\gamma)^{|u|+1}$. It must be shown that $\left(\begin{smallmatrix}(zxz)^{m+t-1}\\ u\end{smallmatrix}\right)_V \theta_{t,1} \left(\begin{smallmatrix}(zxz)^{m+t}\\ u\end{smallmatrix}\right)_V$. This holds if $u=\lambda$ since $(zxz)^{m+t-1} \gamma (zxz)^{m+t}$. Let $|u|>0$. If, for some $r>0$, $(zxz)^{m+r} = z_0 a_1 z_1 \ldots a_n z_n$, there must exist an index j such that $z_j = z_j' x z_j''$. Then $w = z_0 a_1 z_1 \ldots a_j z_j' z z_j'' a_{j+1} \ldots a_n z_n$ is a factorization of w such that $z_j' z z_j'' \gamma z_j$ and $w \gamma(\alpha^m_{t,1}) (zxz)^{m+r-1}$. Thus $\left(\begin{smallmatrix}(zxz)^{m}\\ u\end{smallmatrix}\right)_V = 0$ implies $\left(\begin{smallmatrix}(zxz)^{m+t-1}\\ u\end{smallmatrix}\right)_V = 0$ and $\left(\begin{smallmatrix}(zxz)^{m+t}\\ u\end{smallmatrix}\right)_V = 0$. Suppose $\left(\begin{smallmatrix}(zxz)^{m}\\ u\end{smallmatrix}\right)_V > 0$. Equivalently $\left(\begin{smallmatrix}(z^m x z^m)^m\\ u\end{smallmatrix}\right)_V > 0$ and $(z^m x z^m)^m = z_0 a_1 z_1 \ldots a_n z_n$. If there exist two indices $0 \le j < k \le n$ such that $z_j = z_j' z z_j''$ and $z_k = z_k' z z_k''$, then, for $s=0,\ldots,t-1$,

$$w = z_0 a_1 z_1 \ldots a_{j-1} z_j' z (zxz)^s z_j'' a_j \ldots a_{k-1} z_k' z (zxz)^{t-1-s} z_k'' a_k \ldots a_n z_n = w_0 a_1 w_1 \ldots a_n w_n$$

is a factorization of w such that $w_i \gamma z_i$ for $i=0,\ldots,n$ and $w \gamma(\alpha^m_{t,1}) (zxz)^{m+t-1}$. Hence $\left(\begin{smallmatrix}(zxz)^{m+t-1}\\ u\end{smallmatrix}\right)_V \theta_{t,1} t$ and similarly $\left(\begin{smallmatrix}(zxz)^{m+t}\\ u\end{smallmatrix}\right)_V \theta_{t,1} t$. If no two such indices exist, then $(zxz)^m = z_0 a_1 z_1 \ldots a_n z_n$ has the property that there exists $0 \le j \le n$ such that $z = z_0 a_1 z_1 \ldots a_j z_j'$, $z = z_j'' a_{j+1} z_{j+1} \ldots a_n z_n$ and $z_j = z_j' x z (zxz)^{m-2} z x z_j''$; moreover $[z_i]_\gamma \notin A^*/\gamma [z]_\gamma A^*/\gamma$ for $i \neq j$. It can be verified that this implies $\left(\begin{smallmatrix}(zxz)^{m+t-1}\\ u\end{smallmatrix}\right)_V = \left(\begin{smallmatrix}(zxz)^{m+t}\\ u\end{smallmatrix}\right)_V = \left(\begin{smallmatrix}(zxz)^{m}\\ u\end{smallmatrix}\right)_V$. This completes the proof that $\left(\begin{smallmatrix}(zxz)^{m+t-1}\\ u\end{smallmatrix}\right)_V \theta_{t,1} \left(\begin{smallmatrix}(zxz)^{m+t}\\ u\end{smallmatrix}\right)_V$.

ii) The proof of the second assertion is obtained by the same kind of analysis as in part i) and it is omitted. □

Lemma 1.9: Let $\Delta \leftrightarrow \underline{M}$. Then $\Delta(\Delta^{m}_{t,1}) \hookrightarrow \underline{M}(\underline{LJ})$.

Proof: Let $\gamma \in A^*\Gamma$ and $\phi : A^*/\gamma(\alpha^{m}_{t,1}) \to A^*/\gamma$. Lemma 1.8 implies that ϕ is a $\underline{LJ}$-morphism. □

Corollary 1.2: $\Delta^{*,i}_{t,1} \hookrightarrow \underline{1}(\underline{LJ}^{i})$.

Proof: Apply lemma 1.9 inductively. □

The remarks following corollary 1.1 apply in the case of $\underline{LJ}$-morphisms. That is, corollary 1.2 implies that $\Delta^{*,1}_{t,1} \hookrightarrow \underline{J}$ and by theorem IV.1.1 the converse also holds in this case. Also corollary 1.2 constitutes an aperiodic equivalent of theorem V.2.1 iv) (though, unlike the group case, the characterization is not complete). The corresponding result for groups could be stated as $\Delta^{*,i}_{0,*} \leftrightarrow \underline{1}(\underline{LG_{nil}}^{i})$.

Lemma 1.10: $A = \bigcup_{i \geq 0} \underline{1}\,(\underline{LJ}^{i})$.

Proof: As in lemma 1.7 . □

This result has originally been obtained by Straubing, using a different approach. Straubing also made the following remark. Let L be an α language, $\alpha \in A^*\Delta_{t,1}^{1,i}$. Lemma 1.6 cannot be used to imply the existence of a series $M_L \xrightarrow{\phi_1} M_1 \xrightarrow{\phi_2} \ldots \xrightarrow{\phi_i} M_i = \{1\}$, where ϕ_j would be a $\underline{C(M_{com} \cap M_{t,1})}$-morphism for j=1,...,i. It is known only that M_L is covered by a monoid for which such a series exists. If the same property could be inferred for M_L, this would provide an effective criterion for determining if L is an α language, $\alpha \in A^*\Delta_{t,1}^{1,i}$. No such criterion is known at present. The same is true for $\Delta_{t,1}^{*,1}$ in connection with lemma 1.9.

VI.2 Monoid characterization of $\overrightarrow{\Delta^{*,*}_{*,1}}$

In this section we characterize the monoids corresponding to the *-variety $\overrightarrow{\Delta^{*,*}_{*,1}}$. Also a one-sided version of lemma 1.6 is given.

Let $\underline{\mathbf{R}}$ denote the variety of R-trivial monoids. A monoid M is in $\underline{\mathbf{R}}$ iff $m_1m_2m_3 = m_1$ implies $m_1m_2 = m_1$ for all $m_1,m_2,m_3 \in M$.

Lemma 2.1: $\overrightarrow{\Delta^{m,i}_{t,1}} \hookrightarrow \underline{\mathbf{R}}$.

Proof: Using lemma V.1.4, it is seen that $\overrightarrow{\Delta^{m,i}_{t,1}} \subseteq \overrightarrow{\Delta^{1,mi}_{t,1}}$. Hence the lemma will follow if we show that $\overrightarrow{\alpha^{1,i}_{t,1}}$ is a R-trivial congruence for all $i\geq 0$. This trivially holds when $i=0$. Let $xyz\ \overrightarrow{\alpha^{1,i}_{t,1}}\ x$ for some $x, y, z \in A^*$. Then $xyz\ \overrightarrow{\alpha^{1,i-1}_{t,1}}\ x$ and, assuming inductively that $\alpha^{1,i-1}_{t,1}$ is an R-trivial congruence, we have $xy\ \overrightarrow{\alpha^{1,i-1}_{t,1}}\ x$. Hence $\binom{xy}{\lambda}_{\vec{V}}\ \theta_{t,1}\ \binom{x}{\lambda}_{\vec{V}}$ for all $\vec{V} \in A^*/\overrightarrow{\alpha^{1,i-1}_{t,1}}$. Also, for any $a' \in A$, if $x\ \overrightarrow{\alpha^{1,i-1}_{t,1}}\ xa'$, then $\binom{x}{a}_{\vec{V}} \leq \binom{xa'}{a}_{\vec{V}}$ for all $\vec{V} \in (A^*/\overrightarrow{\alpha^{1,i-1}_{t,1}})^2$. Thus $\binom{x}{a}_{\vec{V}} \leq \binom{xy}{a}_{\vec{V}} \leq \binom{xyz}{a}_{\vec{V}}$. If $\binom{x}{a}_{\vec{V}}\ \theta_{t,1}\ \binom{xyz}{a}_{\vec{V}}$, it must be that $\binom{x}{a}_{\vec{V}}\ \theta_{t,1}\ \binom{xy}{a}_{\vec{V}}$. Therefore $x\ \overrightarrow{\alpha^{1,i}_{t,1}}\ xy$ as required. □

Let U_1 be the monoid represented in figure VI.2 .

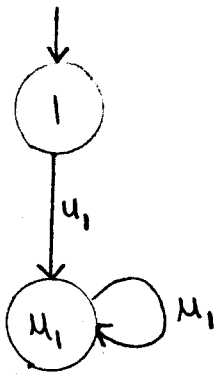


Figure VI.2 Representation of the monoid U_1 .

Lemma 2.2: If $\gamma \in A^*\Gamma$, then $A_\gamma \circ_g A_{U_1} \prec A_{\gamma(\overrightarrow{\alpha^{1,1}_{1,1}})}$.

Proof: Let $([z]_\gamma,m)$ be a state of $A_\gamma \circ_g A_{U_1}$ and let δ be its transition function. We must show that $x\ \gamma(\overrightarrow{\alpha^{1,1}_{1,1}})\ y$ implies $(([z]_\gamma,m),x)\delta = (([z]_\gamma,m),y)\delta$. Suppose $x = a_1\ldots a_k$ and $y = a'_1\ldots a'_n$. Then $(([z]_\gamma,m),x)\delta = ([zx]_\gamma,mm_1\ldots m_k)$ and $(([z]_\gamma,m),y)\delta = ([zy]_\gamma,mm'_1\ldots m'_n)$ where $m_j = ([za_1\ldots a_{j-1}]_\gamma,a_j)g$ for $j=1,\ldots,k$, and $m'_j = ([za'_1\ldots a'_{j-1}]_\gamma,a'_j)g$ for $j=1,\ldots,n$. Since $\gamma \supseteq \gamma(\overrightarrow{\alpha^{1,1}_{1,1}})$, we have $[zx]_\gamma = [zy]_\gamma$. Also $mm_1\ldots m_k = 1$ iff $m=1$ and $m_j \in 1g^{-1}$ for $j=1,\ldots,k$. This is possible iff

$$([zv_0]_\gamma,a) \in u_1g^{-1} \sum_{a\in A} \binom{x}{a}_{\overrightarrow{([v_0]_\gamma,[v_1]_\gamma)}} \theta_{1,1}\ 0 .$$

Since $\binom{x}{a}_{\vec{V}}\ \theta_{1,1}\ \binom{y}{a}_{\vec{V}}$ for all $\vec{V} \in (A^*/\gamma)^2$, $a \in A$, $mm_1\ldots m_k = 1$ iff $mm'_1\ldots m'_n = 1$. Finally $mm_1\ldots m_k = u_1$ iff $m=u_1$ or

$$([zv_0]_\gamma,a) \in u_1g^{-1} \sum_{a\in A} \binom{x}{a}_{\overrightarrow{([v_0]_\gamma,[v_1]_\gamma)}} \theta_{1,1}\ 1 .$$

Again $mm_1 \ldots m_k = u_1$ iff $mm'_1 \ldots m'_n = u_1$. □

Lemma 2.3 (Meyer-Thompson [69]): If $\alpha \in A^*\Gamma$ is such that $A^*/\alpha \in \underline{R}$, then $A_\alpha \prec U_1 \circ_{g_1} \ldots \circ_{g_n} U_1$ for some $n \geq 0$.

Lemma 2.4: If $M \in \underline{R}$ is generated by A, then $\alpha_M \in A^*\overrightarrow{\Delta^{1,*}_{1,1}}$.

Proof: By lemma 2.3, $A_{\alpha_M} \prec U_1 \circ_{g_1} \ldots \circ_{g_n} U_1$ for some $n \geq 0$. Equivalently $A_{\alpha_M} \prec A_\omega \circ_{g_0} U_1 \circ_{g_1} \ldots \circ_{g_n} U_1$ and applying inductively lemma 2.2, $A_{\alpha_M} \prec A_{\overrightarrow{\alpha^{1,n}_{1,1}}}$. Therefore $\alpha_M \in A^*\overrightarrow{\Delta^{1,n}_{1,1}}$. □

Theorem 2.1: $\overrightarrow{\Delta^{1,*}_{1,1}} = \overrightarrow{\Delta^{*,*}_{*,1}} \leftrightarrow \underline{R}$.

Proof: By lemma 2.1, $\overrightarrow{\Delta^{*,*}_{*,1}} \hookrightarrow \underline{R}$. By lemma 2.4, $\underline{R} \hookrightarrow \overrightarrow{\Delta^{1,*}_{1,1}}$. The conclusion follows from the inclusion $\overrightarrow{\Delta^{1,*}_{1,1}} \subseteq \overrightarrow{\Delta^{*,*}_{*,1}}$. □

We close this chapter by giving the one-sided equivalent of lemma 1.6. If $\underline{M}$ is a variety of monoids defined by a set of equations $E = \{e_1 = e'_1, \ldots, e_n = e'_n\}$, let $\overrightarrow{\underline{CM}}$ be the variety of semigroups defined by the equations $ze_1 = ze'_1, \ldots, ze_n = ze'_n$.

Lemma 2.5: Let $\Delta \leftrightarrow \underline{M}$. Then $\Delta(\overrightarrow{\Delta_{t,1}}) \hookrightarrow \underline{M}\ (\overrightarrow{C(M_{com} \cap M_{t,1})})$.

Proof: The proof is similar to that of lemma 1.6 . □

Corollary 2.1: i) $\overrightarrow{\Delta^{1,i}_{t,1}} \hookrightarrow \underline{1}\ (\underline{\overrightarrow{C(M_{com} \cap M_{t,1})}^{i}})$

ii) $\overrightarrow{\Delta^{1,i}_{*,1}} \hookrightarrow \underline{1}\ (\underline{\overrightarrow{C(M_{com} \cap \underline{Ap})}^{i}})$.

Proof: This follows from lemma 2.5 . □

Other congruence characterizations of R-trivial monoids have been obtained by Fich [79].

VII COUNTING SUBWORDS IN CONTEXT: THE GENERAL CASE.

In this chapter, we combine results of the previous chapters to derive a monoid characterization of $\Delta^{*,*}_{*,*}$. It is shown to correspond to $\underline{M_{sol}}$, the variety of monoids in which all groups are solvable. In the second section, we relate threshold 1 counting of subwords and concatenation of languages.

VII.1 Monoid characterization of $\Delta^{*,*}_{*,*}$.

Lemma 1.1: Let $\Delta \leftrightarrow \underline{M}$. Then $\Delta(\Delta_{t,q}) \hookrightarrow \underline{M}\ (C(M_{com} \cap M_{t,q}))$.

Proof: The proof is similar to that of lemma VI.1.6 . □

Let $\phi : M \to M'$ be a monoid morphism. If G is group in M, then $G\phi \simeq G/H$ is a group in M' and H is a group in $e\phi^{-1}$ where e is the unit of $G\phi$. Thus G is an extension of a group in $e\phi^{-1}$ by a group in M' .

Let $\underline{M_{der,i,q}} = \{M : \text{all groups in M are in } \underline{G_{der,i,q}}\}$.

Lemma 1.2: $\Delta^{1,i}_{t,q} \hookrightarrow \underline{M_{der,i,q}}$

Proof: The lemma trivially holds when i=0 . Let i>0 and G be a group in $A^*/\alpha^{1,i}_{t,q}$. There exists a morphism $\phi : A^*/\alpha^{1,i}_{t,q} \to A^*/\alpha^{1,i-1}_{t,q}$. By the remark preceding the lemma, G is an extension of a group H in $e\phi^{-1}$, for some idempotent e of $A^*/\alpha^{1,i-1}_{t,q}$, by a group G' in $A^*/\alpha^{1,i-1}_{t,q}$. We can assume inductively that $G' \in \underline{M_{der,i-1,q}}$. Let f be the identity of H. By lemma 1.1, $h_1h_2=fh_1h_2f=fh_2h_1f=h_2h_1$, and $f=fh_1{}^qf=h_1{}^q$ for any $h_1,h_2 \in H$. Hence $G \in \underline{M_{der,i,q}}$. □

Let $\underline{M_{sol}} = \{M : \text{all groups in M are solvable}\}$.

Lemma 1.3 (Krohn-Rhodes [65]): If $A^*/\alpha \in \underline{M_{sol}}$, then $A_\alpha \prec A_1 \underset{g_1}{\circ} \cdots \underset{g_{n-1}}{\circ} A_n$ where $A_i = A_U$ or $A_i = A_H$ for some abelian group H.

Lemma 1.4: If $M \in \underline{M_{sol}}$ is generated by A, then $\alpha_M \in \Delta^{*,*}_{*,*}$.

Proof: By lemma 1.3, $A_{\alpha_M} \prec A_1 \overset{\circ}{g_1} \cdots \overset{\circ}{g_{n-1}} A_n$ with $A_i = A_U$ or $A_i = A_H$ for some abelian group H. Using lemma V.2.5 and lemma VI.1.2 inductively, the result follows. □

Theorem 1.1: $\Delta^{1,*}_{*,*} = \Delta^{*,*}_{*,*} \leftrightarrow \underline{M_{sol}}$

Proof: By lemma 1.2, $\Delta^{1,*}_{*,*} \hookrightarrow \underline{M_{sol}}$. By lemma 1.4, $\underline{M_{sol}} \hookrightarrow \Delta^{1,*}_{*,*}$. Hence $\Delta^{1,*}_{*,*} \leftrightarrow \underline{M_{sol}}$. Also $\Delta^{1,*}_{*,*} \subseteq \Delta^{*,*}_{*,*}$ and $\Delta^{m,i}_{t,q} \subseteq \Delta^{1,i\lceil \log_2(m+1)\rceil}_{t,q}$ implies $\Delta^{*,*}_{*,*} = \Delta^{1,*}_{*,*}$. □

Corollary 1.1: $\underline{M_{sol}} = \bigcup_{i\geq 0} \underline{1}\,(\underline{CM_{com}}^{i})$

Proof: By lemma 1.1 and theorem 1.1, it follows that $\underline{M_{sol}} \subseteq \bigcup_{i\geq 0} (\underline{CM_{com}}^{i})$. Conversely it is easily verified that every monoid in $\underline{1}(\underline{CM_{com}}^{i})$ contains only solvable groups of derived length $\leq i$. □

For completeness, we give results concerning $\Delta^{*,i}_{*,*}$.

Lemma 1.5: If $\gamma \in A^*\Gamma$, then ϕ: $A^*/\gamma(\alpha^m_{0,q}) \to A^*/\gamma$ is an $\underline{LG_{nil}}$-morphism.

Proof: Left to the reader. □

For two varieties of monoids $\underline{M}_1$ and $\underline{M}_2$, define their join $\underline{M}_1 \vee \underline{M}_2 = \{M : M \prec M_1 \times M_2, M_1 \in \underline{M}_1, M_2 \in \underline{M}_2\}$. In other words $\underline{M}_1 \vee \underline{M}_2$ is the smallest variety containing $\underline{M}_1$ and $\underline{M}_2$. The same definition can be made for varieties of semigroups.

Lemma 1.6: Let $\underline{M}$ be a variety of monoids, $\underline{M}_1$, $\underline{M}_2$ be varieties of monoids or varieties of semigroups. Then $\underline{M}(M_1) \vee \underline{M}(M_2) \subseteq \underline{M}(M_1 \vee M_2)$.

Proof: Let $M \in \underline{M}(M_1) \vee \underline{M}(M_2)$. Then $M \prec M_1 \times M_2$ where $M_1 \in \underline{M}(M_1)$ and $M_2 \in \underline{M}(M_2)$. There then exists N_1, $N_2 \in \underline{M}$, $\phi_1 : M_1 \to N_1$ a $\underline{M}_1$-morphism and $\phi_2 : M_2 \to N_2$ a $\underline{M}_2$-morphism. Since $\underline{M}$ is a variety, $N_1 \times N_2 \in \underline{M}$. Let $\phi : M_1 \times M_2 \to N_1 \times N_2$ be defined by $(m_1,m_2)\phi = (m_1\phi_1, m_2\phi_2)$. It must be shown that ϕ is a $\underline{M}_1 \vee \underline{M}_2$-morphism. If (e_1,e_2) is an idempotent of $N_1 \times N_2$, it must be that e_1 is an idempotent of N_1 and similarly for e_2. If $(m_1,m_2) \in (e_1,e_2)\phi^{-1}$, then $m_1\phi_1 = e_1$, $m_2\phi_2 = e_2$. Thus $(e_1,e_2)\phi^{-1}$ is a subsemigroup of $e_1\phi_1^{-1} \times e_2\phi_2^{-1}$ and therefore $(e_1,e_2)\phi^{-1} \in \underline{M}_1 \vee \underline{M}_2$. □

Lemma 1.7: Let $\Delta \leftrightarrow \underline{M}$. If $\gamma \in A^*\Delta$, then $A^*/\gamma(\alpha^m_{t,q}) \in \underline{M}(\underline{LJ} \vee \underline{LG}_{nil})$.

Proof: From the definition of $\gamma(\alpha^m_{t,q})$ it follows that $\gamma(\alpha^m_{t,q}) = \gamma(\alpha^m_{t,1}) \cap \gamma(\alpha^m_{0,q})$. Thus $A^*/\gamma(\alpha^m_{t,q}) \prec A^*/\gamma(\alpha^m_{t,1}) \times A^*/\gamma(\alpha^m_{0,q})$. From lemma VI.1.9, we infer that $A^*/\gamma(\alpha^m_{t,1}) \in \underline{M}(\underline{LJ})$. From lemma 1.5, it is seen that $A^*/\gamma(\alpha^m_{0,q}) \in \underline{M}(\underline{LG}_{nil})$. Hence $A^*/\gamma(\alpha^m_{t,q}) \in \underline{M}(\underline{LJ}) \vee \underline{M}(\underline{LG}_{nil})$. By lemma 1.6, $\underline{M}(\underline{LJ}) \vee \underline{M}(\underline{LG}_{nil}) \subseteq \underline{M}(\underline{LJ} \vee \underline{LG}_{nil})$, completing the proof. □

Corollary 1.2: $\underline{M}_{sol} = \bigcup_{i\geq 0} \underline{1}\,((\underline{LJ} \vee \underline{LG}_{nil})^{i})$.

Proof: Let $\alpha \in A^*\Delta^{m,i}_{t,q}$. Then $A^*/\alpha \prec A^*/\alpha^{m,i}_{t,q}$. Iterating lemma 1.7, it follows that $\Delta^{*,*}_{*,*} \hookrightarrow \bigcup_{i\geq 0} \underline{1}\,((\underline{LJ} \vee \underline{LG}_{nil})^{i})$. Conversely it may be verified that every monoid in $\underline{1}\,((\underline{LJ} \vee \underline{LG}_{nil})^{i})$ contains only solvable groups of fitting length $\leq i$. □

VII.2 Threshold counting of subwords and concatenation.

In chapter VI, it was shown that $\Delta_{1,1}^{*,*} \leftrightarrow \underline{Ap}$. A famous theorem of Schutzenberger [65] indicates that the corresponding family of languages consists, for each alphabet A, of the closure of the family $\{\{a\} : a \in A\}$ under boolean operations and concatenation. This result is extended to $\Delta(\Delta_{1,1}^{*,*})$ for an arbitrary *-variety of congruences Δ .

The following notation will be used. If $\Delta \leftrightarrow L$, we denote by $L_{t,q}^{m,i}$ the *-variety of languages corresponding to $\Delta(\Delta_{t,q}^{m,i})$. For any L, LM denotes the smallest family of languages containing $L \cup \{\lambda\}$ and closed under concatenation; LB will stand for the smallest family of languages containing L and closed under boolean operations.

Lemma 2.1: If $\Delta \leftrightarrow L$ then $A^*L_{1,1}^{*,1} \subseteq (A^*L \cup \{\{a\} : a \in A\})MB$.

Proof: Let $\gamma \in A^*\Delta$; we have to show that for any $x \in A^*$, $[x]_{\gamma(\alpha_{1,1}^m)} \in (A^*L \cup \{\{a\} : a \in A\})MB$. Let

$Y_x = \{(u,V) : |u| \leq m \text{ and } \binom{x}{u}_V \theta_{1,1} 1\}$ and

$N_x = \{(u,V) : |u| \leq m \text{ and } \binom{x}{u}_V \theta_{1,1} 0\}$. Then

$$[x]_{\gamma(\alpha_{1,1}^m)} = \bigcap_{(a_1 \ldots a_r, ([v_0]_\gamma, \ldots, [v_r]_\gamma)) \in Y_x} [v_0]_\gamma a_1 [v_1]_\gamma \ldots a_r [v_r]_\gamma$$

$$\bigcap \bigcap_{(a_1 \ldots a_r, ([v_0]_\gamma, \ldots, [v_r]_\gamma)) \in N_x} \overline{[v_0]_\gamma a_1 [v_1]_\gamma \ldots a_r [v_r]_\gamma} \quad .$$

Since $[v]_\gamma \in A^*L$ for all $v \in A^*$, this proves the lemma . □

Lemma 2.2: If $\{\lambda\} \in A^*L$ then $(A^*L \cup \{\{a\} : a \in A\})MB \subseteq A^*L^{*,1}_{1,1}$.

Proof: Since $A^*L^{*,1}_{1,1}$ is closed under boolean operations, it is sufficient to show that $L_1 \ldots L_k \in (A^*L \cup \{\{a\} : a \in A\})M$ implies that $L_1 \ldots L_k \in A^*L^{*,1}_{1,1}$. For $L_1 \ldots L_k$ as above, then, for $i=1,\ldots,k$, either $L_i = \{a\}$ or L_i is a union of γ_i-classes for some $\gamma_i \in A^*\Delta$ where $L \leftrightarrow \Delta$. Let $I = \{i : L_i \neq \{a\}, a \in A\}$ and $\gamma = \bigcap_{i\in I} \gamma_i \cap \alpha_{\{\lambda\}}$. Then each L_i is either $\{a\}$ or a γ language. Distributing concatenation over union, and using the fact that $A^*L^{*,1}_{1,1}$ is closed under boolean operations, it is seen that it is sufficient to show that $L_1 \ldots L_k \in A^*L^{*,1}_{1,1}$ when $L_i = \{a\}$ or $L_i = [x]_\gamma$ for some $\gamma \in A^*\Delta$, $i=1,\ldots,k$. If $L_1 = \{a\}$, we replace L_1 by $\{\lambda\}L_1$. If for some $1 \leq i \leq k-1$ L_i and L_{i+1} are both in $\{\{a\} : a \in A\}$, we replace L_iL_{i+1} by $L_i\{\lambda\}L_{i+1}$; if $L_i = [x]_\gamma$ and $L_{i+1} = [y]_\gamma$, we can replace L_iL_{i+1} by $L_i(\bigcup_{a\in A} a\, a^{-1}L_{i+1})$. Note that $a^{-1}L_{i+1}$ is a γ-language. Finally if $L_k \in \{\{a\} : a \in A\}$, we replace it by $L_k\{\lambda\}$. Noting that $\{\lambda\}$ is a γ-language and distributing concatenation over union, $L_1 \ldots L_k$ is seen to be a boolean function of languages of the form $L = [v_0]_\gamma a_1 [v_1]_\gamma \ldots a_r [v_r]_\gamma$ for some $r \leq k$. Since $L = \{x : \binom{x}{a_1 \ldots a_r}_{([v_0]_\gamma, \ldots, [v_r]_\gamma)} \theta_{1,1}\, 1\}$, it follows that $L \in A^*L^{*,1}_{1,1}$ and $L_1 \ldots L_k \in A^*L^{*,1}_{1,1}$. □

Lemma 2.3: Let $\Delta \leftrightarrow L$. Then $A^*L^{*,1}_{1,1}$ is the closure of $(A^*L \cup \{\{a\} : a \in A\})$ under boolean operations and concatenation.

Proof: By iterating lemma 2.1, $A^*L^{*,i}_{1,1} \subseteq (A^*L \cup \{\{a\} : a \in A\})(MB)^i$, and thus $A^*L^{*,*}_{1,1} \subseteq \bigcup_{i\geq 0} (A^*L \cup \{\{a\} : a \in A\})(MB)^i$. To prove the converse, observe that $\{\lambda\} = \bigcap_{a\in A} \overline{A^*aA^*}$ is a γ-language for $\gamma \in \Delta(\Delta^{1,1}_{1,1})$. Clearly $(A^*L \cup \{\{a\} : a \in A\}) \subseteq (A^*L^{*,1}_{1,1} \cup \{\{a\} : a \in A\})$ and the hypothesis of lemma 2.2 is satisfied for $A^*L^{*,1}_{1,1}$. Hence

$$(A^*L \cup \{\{a\} : a \in A\})MB \subseteq (A^*L^{*,1}_{1,1} \cup \{\{a\} : a \in A\})MB$$

$$\subseteq A^*L^{*,2}_{1,1} .$$

Iterating this result, we get $(A^*L \cup \{\{a\} : a \in A\})(MB)^i \subseteq A^*L^{*,i+1}_{1,1}$, and this completes the proof. Note that our proof indicates that $(A^*L \cup \{\{a\} : a \in A\})(MB)^i$ lies between $A^*L^{*,i}_{1,1}$ and $A^*L^{*,i+1}_{1,1}$. □

VIII SUMMARY AND OPEN PROBLEMS

The goal of this thesis was to obtain an algebraically meaningful classification of regular languages. This problem has two aspects. First it is necessary to design a method for generating families of languages, and then, these families must be characterized by the properties of the induced monoids.

Eilenberg's theorem gives conditions under which an algebraic characterization is possible for a family of languages. In chapter I, we expressed these conditions in terms of congruences of finite index.

In chapter II, we presented a method for generating regular languages, where membership of a word x is determined by counting certain factorizations; that is,we counted occurrences of subwords of length m with respect to a congruence $\theta_{t,q}$ on $\mathbb{N}$, recursively taking into account the context in which these subwords appear. This membership criterion was expressed in congruence form and it was shown that *-varieties of congruences were produced. These *-varieties are thus defined by four parameters: the length m of the subwords that are counted, the depth i of the recursion, and the indices t and q of the congruence on $\mathbb{N}$ with respect to which the counting is done. Moreover these families of congruence $\Delta_{t,q}^{m,i}$ can be ordered by inclusion according to the values of m, i, t and q, thus providing hierarchies of increasing complexity.

This is a convenient approach in many respects. For each $\Delta_{t,q}^{m,i}$ and each alphabet A, there exists a unique congruence $\alpha_{t,q}^{m,i}$ on A* such that $\alpha \in A^*\Delta_{t,q}^{m,i}$ iff $\alpha \supseteq \alpha_{t,q}^{m,i}$. Also, the Krohn-Rhodes decomposition theorem indicates that the structure of any finite monoid can be described by appropriate combinations of groups and aperiodic monoids. For our construction, we showed that groups were generated iff t=0 and aperiodic monoids were obtained iff q=1. In the general case, properties of $\Delta_{t,q}^{m,i}$ can be inferred by combining properties of $\Delta_{0,q}^{m,i}$ and $\Delta_{t,1}^{m,i}$. Finally, it was shown that the simplest instance of our construction, i.e. taking m=i=1, led to the smallest varieties of monoids, i.e. to varieties of commutative monoids (figure VIII.1). In section II.1, a complete characterization of all varieties of commutative monoids was given along these lines.

In subsequent chapters, we studied the families of monoids corresponding to the congruences in $\Delta_{t,q}^{m,i}$.

In chapter III, the correspondence $\Delta_{0,*}^{*,1} \leftrightarrow \underline{G_{nil}}$ was established. The hierarchy of *-varieties of congruences $\Delta_{0,*}^{0,1} \subseteq \Delta_{0,*}^{1,1} \subseteq \ldots \subseteq \Delta_{0,*}^{m,1} \subseteq \ldots \subseteq \Delta_{0,*}^{*,1}$ was related to the hierarchy of varieties of groups $\underline{G_{nil,0}} \subseteq \underline{G_{nil,1}} \subseteq \ldots \subseteq \underline{G_{nil,m}} \subseteq \ldots \subseteq \underline{G_{nil}}$, which is the natural algebraic hierarchy leading to nilpotent groups (figure VIII.2). Also an attempt was made to characterize all congruences in $\Delta_{0,q}^{m,1}$ in terms of counting subwords.

In chapter IV, we proved that $\Delta^{*,1}_{*,1} \leftrightarrow \underline{J}$. We suspect the existence of an aperiodic equivalent to the notion of nilpotent groups of class m, i.e. a hierarchy $J_0 \subseteq J_1 \subseteq \ldots \subseteq J_m \subseteq \ldots \subseteq \underline{J}$ which would relate to the hierarchy $\Delta^{0,1}_{*,1} \subseteq \Delta^{1,1}_{*,1} \subseteq \ldots \subseteq \Delta^{m,1}_{*,1} \subseteq \ldots \subseteq \Delta^{*,1}_{*,*}$ in a way similar to the group case (figure VIII.3). We again discussed a characterization of congruences in $\Delta^{m,1}_{t,1}$ in terms of counting subwords.

In chapter V, we established that $\Delta^{1,*}_{0,*} = \Delta^{*,*}_{0,*} \leftrightarrow \underline{G_{sol}}$. The intermediate *-varieties $\Delta^{1,i}_{0,*}$ and $\Delta^{*,i}_{0,*}$ were also characterized exactly by the structure of the induced monoids (figure VIII.4). More specific results were given when modulo q counting was considered, for a fixed integer q.

In chapter VI, it was shown that $\Delta^{1,*}_{*,1} = \Delta^{*,*}_{*,1} \leftrightarrow \underline{Ap}$. Necessary conditions on the monoids were derived for the intermediate *-varieties $\Delta^{1,i}_{*,1}$ and $\Delta^{*,i}_{*,1}$ (figure VIII.5).

Finally, in chapter VII, previous results were combined to yield the characterization $\Delta^{1,*}_{*,*} = \Delta^{*,*}_{*,*} \leftrightarrow \underline{M_{sol}}$. Partial results concerning $\Delta^{1,i}_{*,*}$ were also given (figure VIII.6).

Throughout this work, we also considered the trade-off between the various indices. Our results show that $\Delta^{*,*}_{*,*} = \bigcup \Delta^{1,*}_{1,q}$ where the union ranges over all those q which are product of distinct primes. Thus to generate $\underline{M_{sol}}$, it is sufficient to count letters in context, using threshold 1 and modulo p counting for p prime. It is easily seen that no further restriction can be made on the set of indices. We also

provided a modification of the initial construction which would take into account one-sided contexts only. Nothing was lost in the group case, but, with threshold counting, this modification led to the varieties of R- and L-trivial monoids (figure VIII.7). Finally, some study of the languages defined by our congruences was made from the point of view of Kleene's operations. A bound on the *-height of $\alpha_{0,q}^{m,1}$ languages was given (section III.3) and a relationship between concatenation and threshold counting of subwords in context was indicated (section VII.2).

We now conclude by stating some problems that remain open and suggestions for further research.

The most important problem to solve is certainly to extend our classification to all regular languages. The idea of counting factorizations of specific types has proved extremely fruitful from the algebraic point of view. Counting subwords in context is sufficient to generate all monoids containing only solvable groups. Left out of this classification are all non-cyclic simple groups, and consequently, the monoids containing such groups. In view of the fact that any group contains (not necessarily normal) cyclic subgroups, it seems that the idea of counting some kind of factorizations might play a role in generating congruences of finite index for arbitrary monoids. We suggest the extension of our approach to counting segments. Preliminary investigations indicate that a proper formalization of this idea will generate hierarchies of varieties of semigroups. It also seems that this approach can define in a systematic way sequences of increasingly complex congruences where each member of the sequence can be reduced to the previous one, by using a generalization of the notion of morphism.

A second problem of importance is to complete the monoid characterization for the *-varieties $\Delta^{1,i}_{*,*}$ and $\Delta^{*,i}_{*,*}$. A natural approach to the solution of this problem is to characterize the monoids corresponding to $\Delta^{1,i}_{*,1}$ and $\Delta^{*,i}_{*,1}$, and to combine these results with those concerning $\Delta^{1,i}_{0,*}$ and $\Delta^{*,i}_{0,*}$, which are already available. This solution should respect the similarity in the construction leading to aperiodic and group congruences. Indeed, we believe that the "algebraic meaning" of the indices m and i can be analyzed independently of the type of counting which is done. In other words if $\Delta^{m,i}_{*,*}$ corresponds to all monoids having property P, then $\Delta^{m,i}_{*,1}$ should correspond to all aperiodic monoids having property P and $\Delta^{m,i}_{0,*}$ should correspond to all groups having property P. This is exemplified in the initial level of the hierarchy where the values m=i=1 determines the property of commutativity.

We recall that corollary VI.1.1 ii) indicates that $\Delta^{1,i}_{*,1} \subsetneq \underline{M}$, where $M \in \underline{M}$ iff M is covered by a monoid M' for which there exists a sequence of i $\underline{C(M_{com} \cap Ap)}$-morphisms $M' \xrightarrow{\phi_1} \ldots \xrightarrow{\phi_i} \{1\}$. We suggest that this property implies that there exists a sequence of mappings $M \xrightarrow{\phi_1} \ldots \xrightarrow{\phi_i} \{1\}$, where the ϕ_j would be generalized morphisms having some property closely related to commutativity. To be interesting, the existence of such a chain would have to be decidable; hence relational morphisms as defined by Tilson in Eilenberg [76] are not suitable for the task.

Another set of problems deals with the operation of counting subwords when the context is not considered. Although we have characterizations for the monoids corresponding to $\Delta^{*,1}_{*,1}$ and $\Delta^{*,1}_{0,*}$, it is not clear how these

characterizations are related. Following the discussion above, we feel that J-trivialness is the aperiodic equivalent of nilpotency of groups: it would be helpful to have a more exact description of this statement.

Also in the variety of nilpotent groups, we are presented with two hierarchies; one more natural from the algebraic standpoint (classifying by the length of the central series), the other more natural from the language point of view (classifying by the length of the subwords that must be counted). Our analysis of the dihedral groups seems to indicate that the two hierarchies do not coincide. Establishing the exact relationship between them would be a useful result. A more general problem is to characterize the set of all varieties of nilpotent congruences. Using the notation of section II.1, we know that $\Delta_N^{m,1}$ is a *-variety of nilpotent congruences for all $N = (0,n_1,n_2,\ldots)$, $n_j \in \mathbb{N} \cup \{*\}$ for $j \geq 1$. Results on this problem would certainly include a solution to the previous one. We also mention two problems of lesser importance concerning this family. The first one is to characterize the tradeoff between m and q, i.e. to find the minimal m' such that $\Delta_{0,p_1^{c_1}\ldots p_n^{c_n}}^{m} \subseteq \Delta_{0,p_1\ldots p_n}^{m'}$. The result we got for m = 1 says that $\Delta_{0,q}^{m} \subseteq \Delta_{0,q'}^{m'}$ iff $\{p : p \text{ prime and } p|q\} \subseteq \{p : p \text{ prime and } p|q'\}$ and $mq|m'q'$. We conjecture that it is true for arbitrary m. This result and conjecture are to be related to the corresponding result in the aperiodic case which says that $\Delta_{t,1}^{m} \subseteq \Delta_{1,1}^{m'}$ when $m+t \leq m'+1$. Another problem is to determine if there exist other congruences in $\Delta_{0,q}^{m,1}$ than those given by α_F .

Continuing on the similarity between nilpotent groups and J-trivial monoids, we conjecture the existence of an algebraic property paralleling central series; this property would define a hierarchy $\underline{J}_0 \subseteq \underline{J}_1 \subseteq \ldots \subseteq \underline{J}_m \subseteq \ldots \subseteq \underline{J}$, with $\underline{J}_0 = \underline{1}$ and $\underline{J}_1 = \underline{M}_{com} \cap \underline{Ap}$. It is felt that understanding this property could help in simplifying the proof of Simon's theorem. Closely related is the problem of determining all *-varieties of J-trivial congruences.

Finally, we make some remarks on the longstanding *-height problem. The definitions of our congruences yield precise descriptions of languages in terms of counting certain factorizations and these in turn can be readily expressed in terms of regular expressions. We are thus in presence of a convenient framework for studying *-height. It is known that any α language, $\alpha \in \Delta_{0,q}^{1,1}$, has *-height 1. Two natural ways for getting hard languages (from the *-height point of view) are to count letters in deeper context and to count longer subwords. Going in the first direction, the following example is a simple candidate for a *-height 2 language. Let $A = \{a,b,c\}$, $x \gamma y$ iff $\binom{x}{u} \theta_{0,2} \binom{y}{u}$ for u=a,b and $L_1 = \{x : \binom{x}{c}_{([\lambda]_\gamma, [v]_\gamma)} \theta_{0,2} 0\}$. Thus L_1 consists of those words which contain an even number of c's, where we count only those c's appearing after even number of a's and even number of b's. The syntactic right congruence that recognizes L_1 is represented in figure VIII.8. Going in the second direction, we have shown in chapter III that any α language, $\alpha \in \Delta_{0,q}^{2,1}$, has *-height 1. We are thus led to counting subwords of length 3 as the next level of difficulty. It can be shown that $\{x : \binom{x}{a_1 a_2 a_3} \theta_{0,q} k\}$ has *-height 1 whenever the

three letters a_1 , a_2 and a_3 are not all different. The next candidate for a *-height 2 language is thus $L_2 = \{x : \binom{x}{abc} \theta_{0,2}\ 0\} \subseteq \{a,b,c\}^*$. The syntactic right congruence recognizing this language is represented in figure VIII.9. A final example can be produced along different lines. The language L_3 = (b(ab*a)*b+ab*a)* is recognized by the right congruence represented in figure VIII.10. It can be shown that L_3 is an $\alpha_{0,2}^{2,1}$ language and thus that it has *-height 1. Consider L_4 = (ba*b(ab*a)*ba*b+ab*a)*, accepted by the right congruence represented in figure VIII.11. L_4 is an example of a language of *-height $\leq$ 2 whose syntactic monoid is a solvable group of derived length 3. It is not known if a *-height 1 expression can be found for L_4.

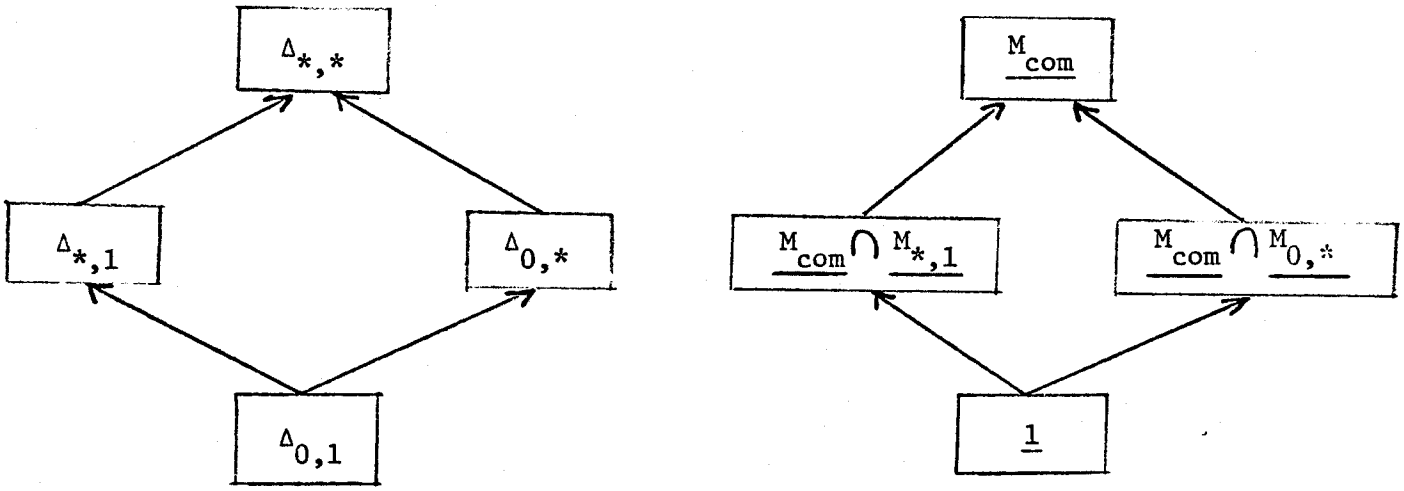


Fig. VIII.1 : Counting letters and related monoids

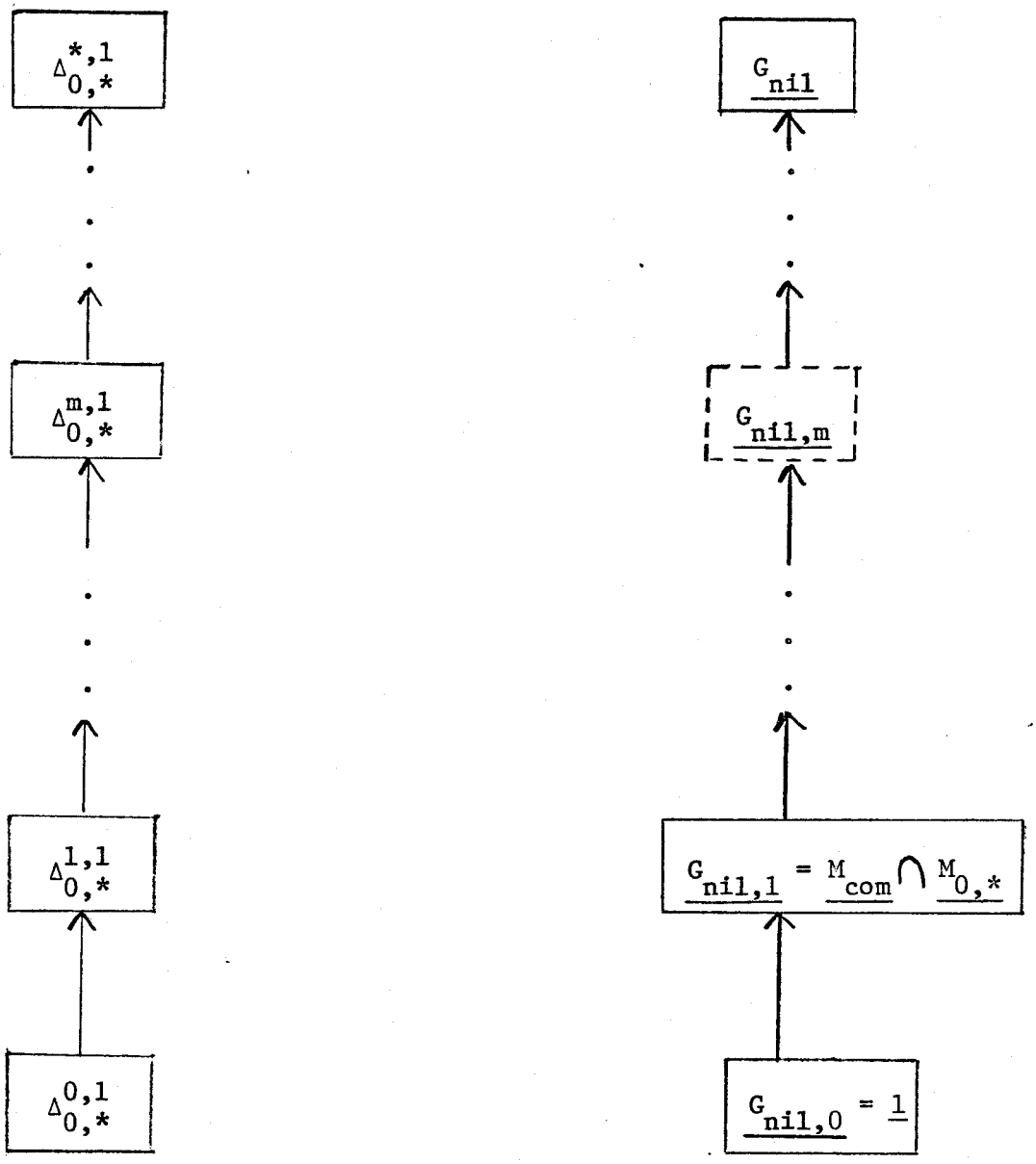


Fig. VIII.2 : Modulo counting of subwords and related monoids

Note: $\boxed{\underline{M}}$ means that $\Delta \hookrightarrow \underline{M}$ has been established but not the converse.

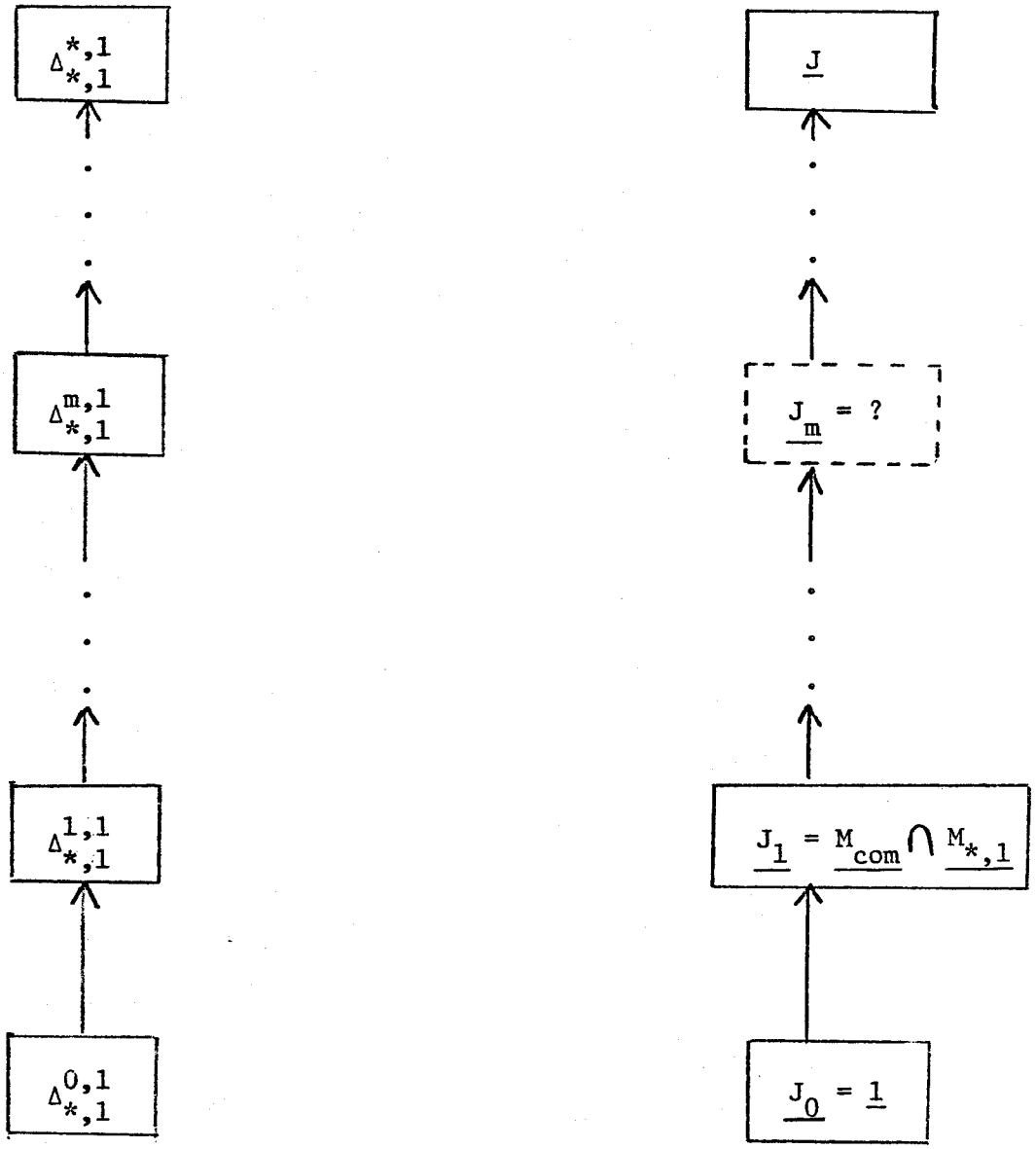


Fig. VIII.3 : Threshold counting of subwords and related monoids

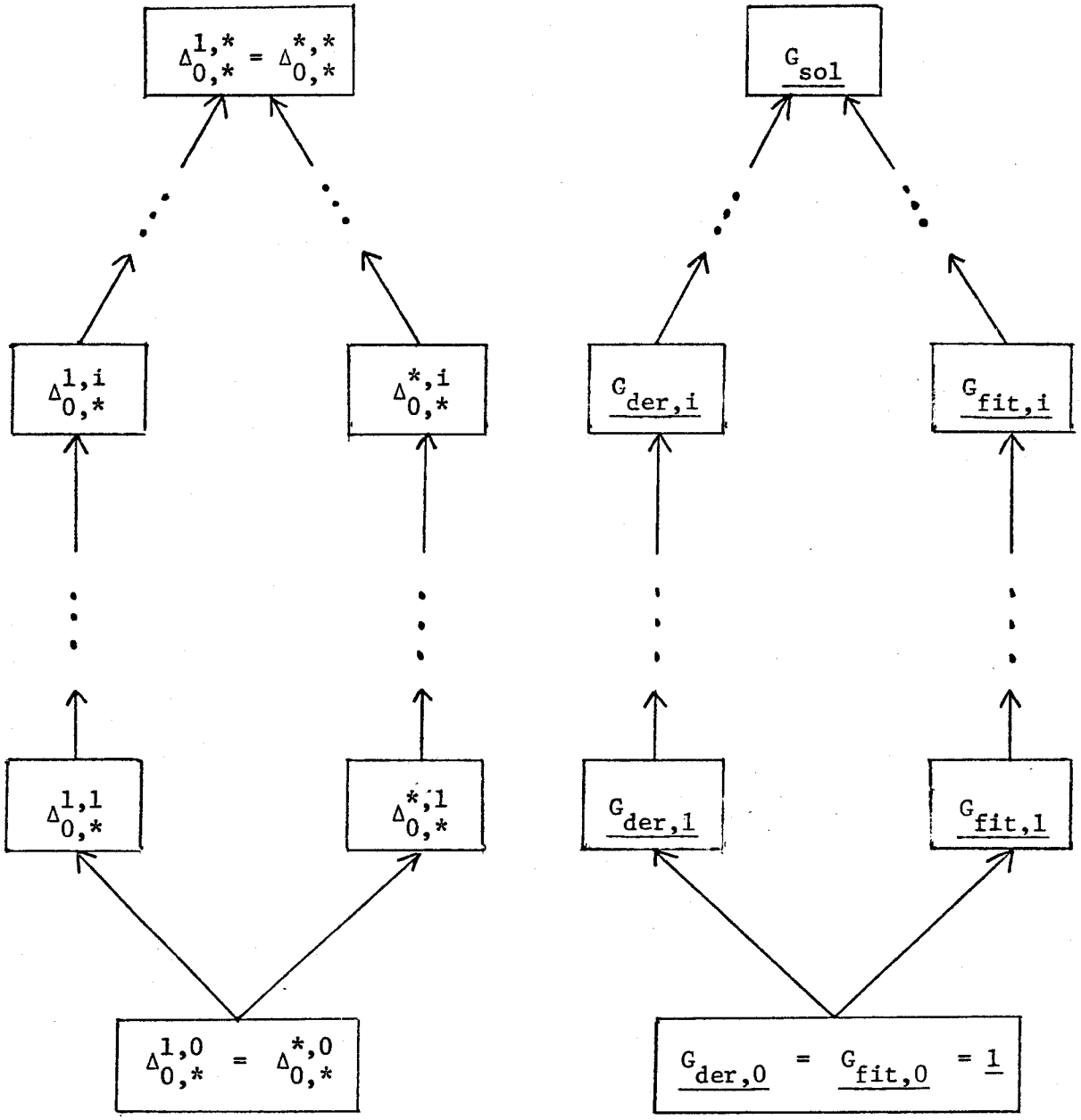


Fig. VIII.4 : Modulo counting of subwords in context and related monoids

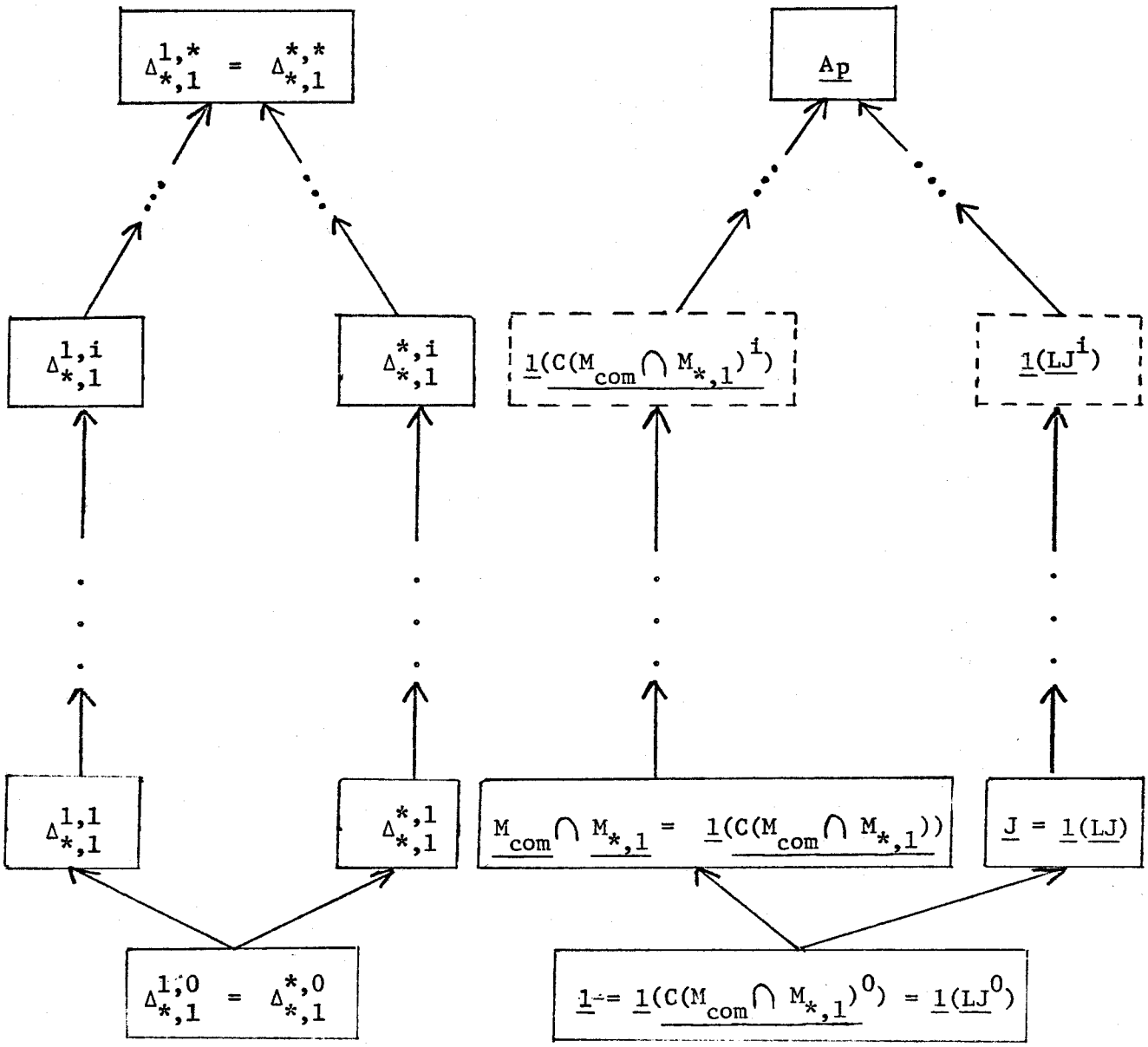


Fig. VIII.5 : Threshold counting of subwords in context and related monoids

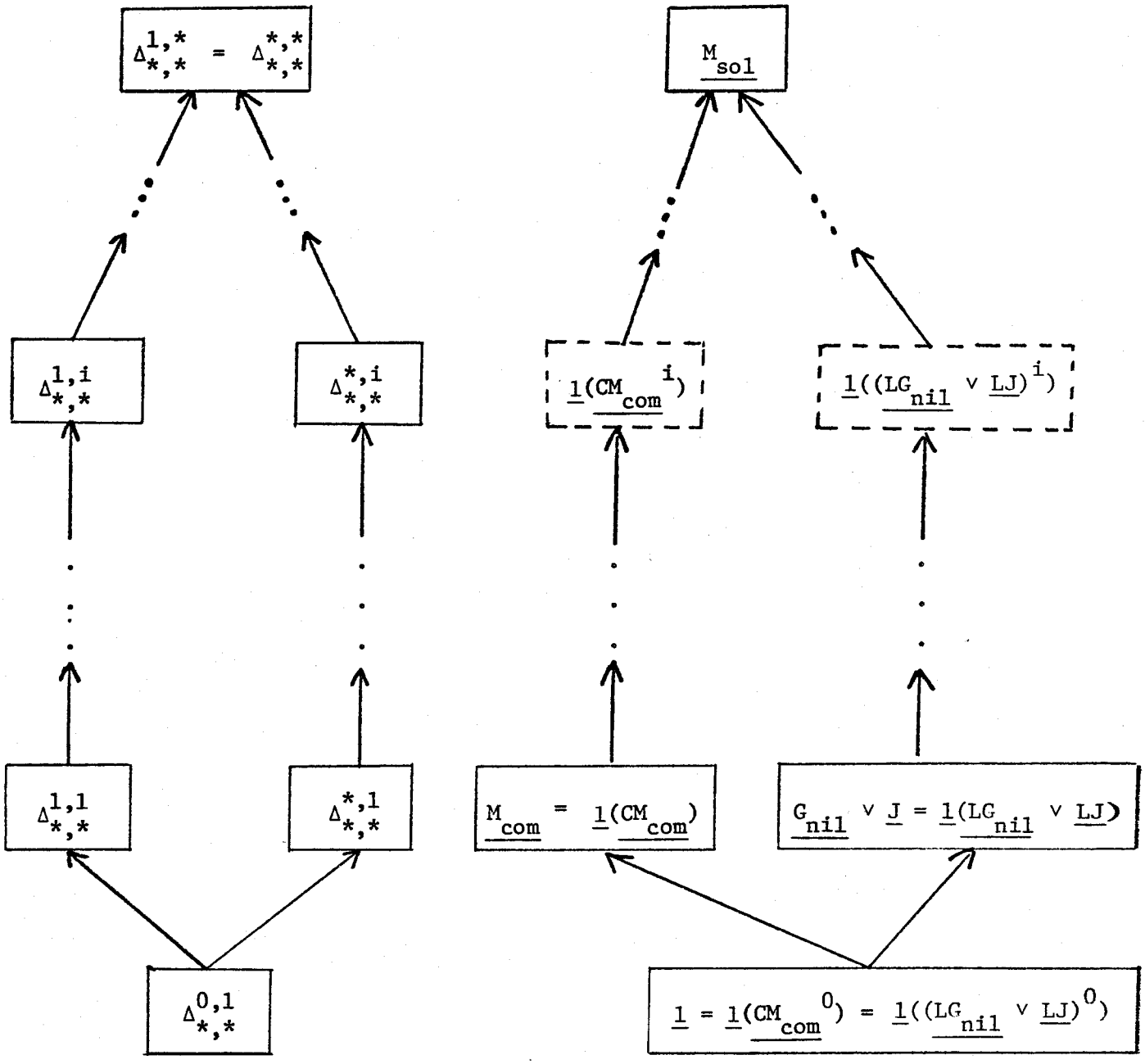


Fig. VIII.6 : Counting subwords in context and related monoids

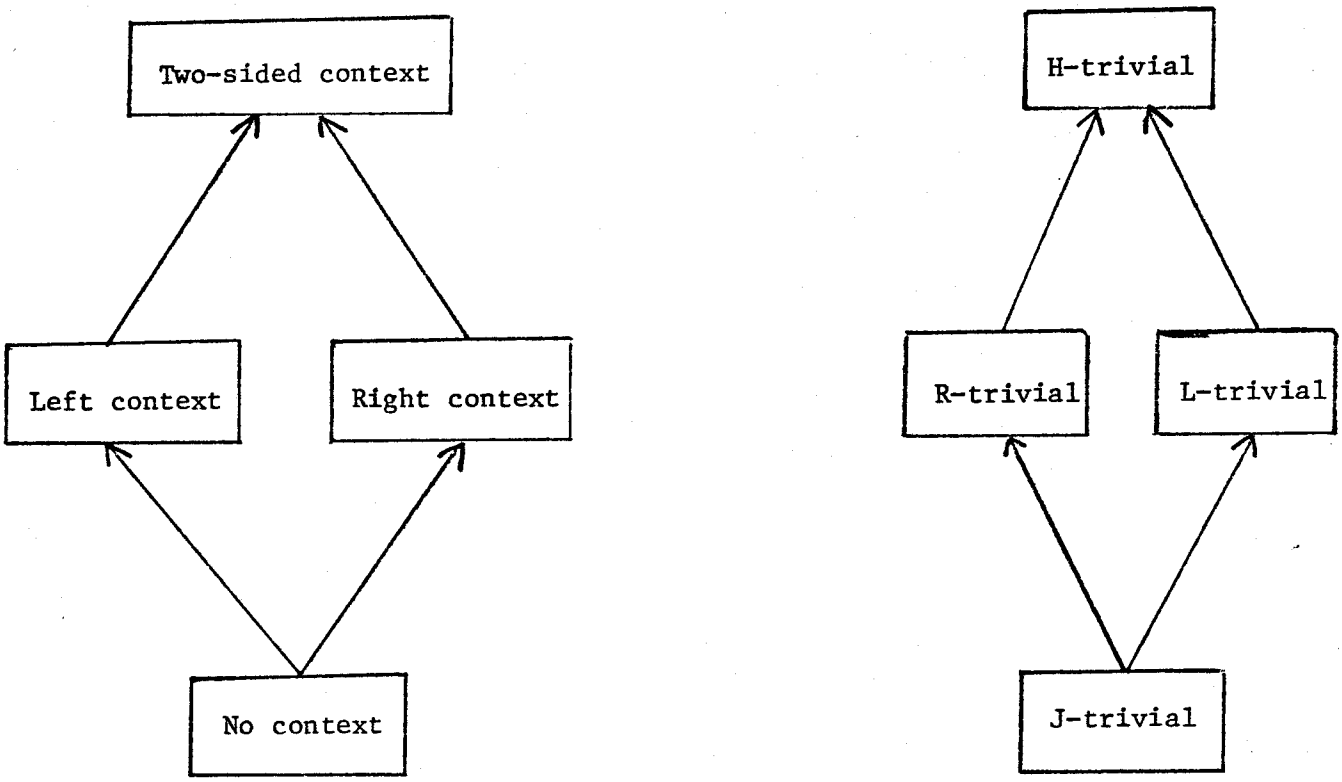


Fig. VIII.7: Threshold counting of subwords in context and Green's equivalences.

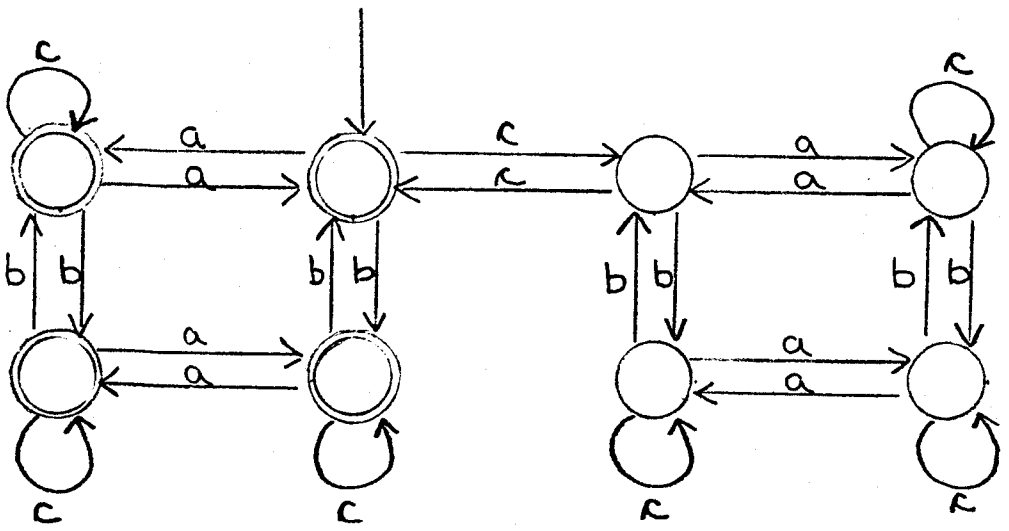


Fig. VIII.8 : Representation of the syntactic right congruence of L_1

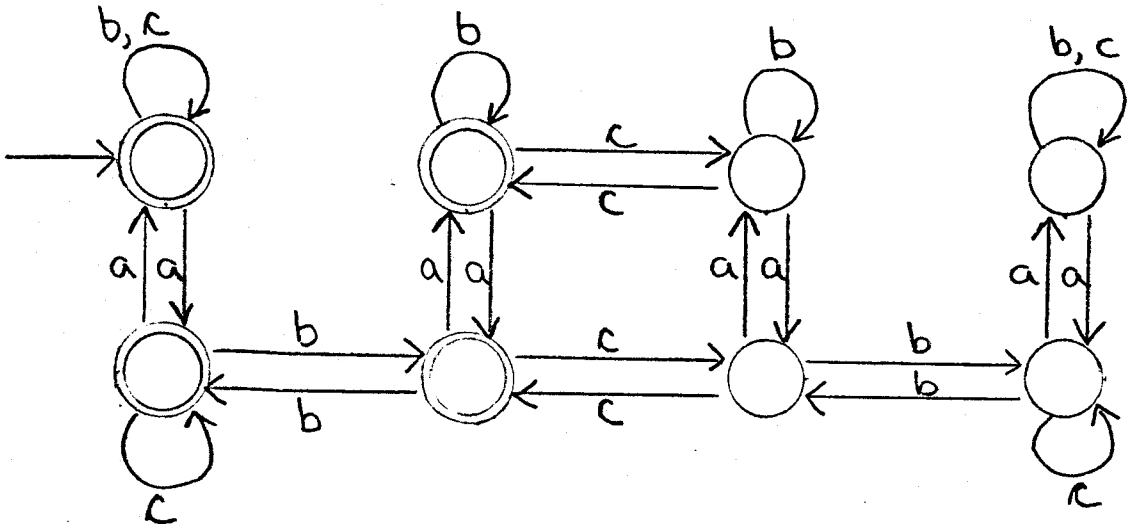


Fig. VIII.9 : Representation of the syntactic right congruence of L_2

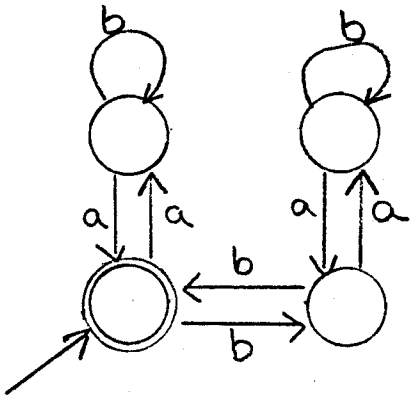


Fig. VIII.10: Representation of the syntactic right congruence of L_3

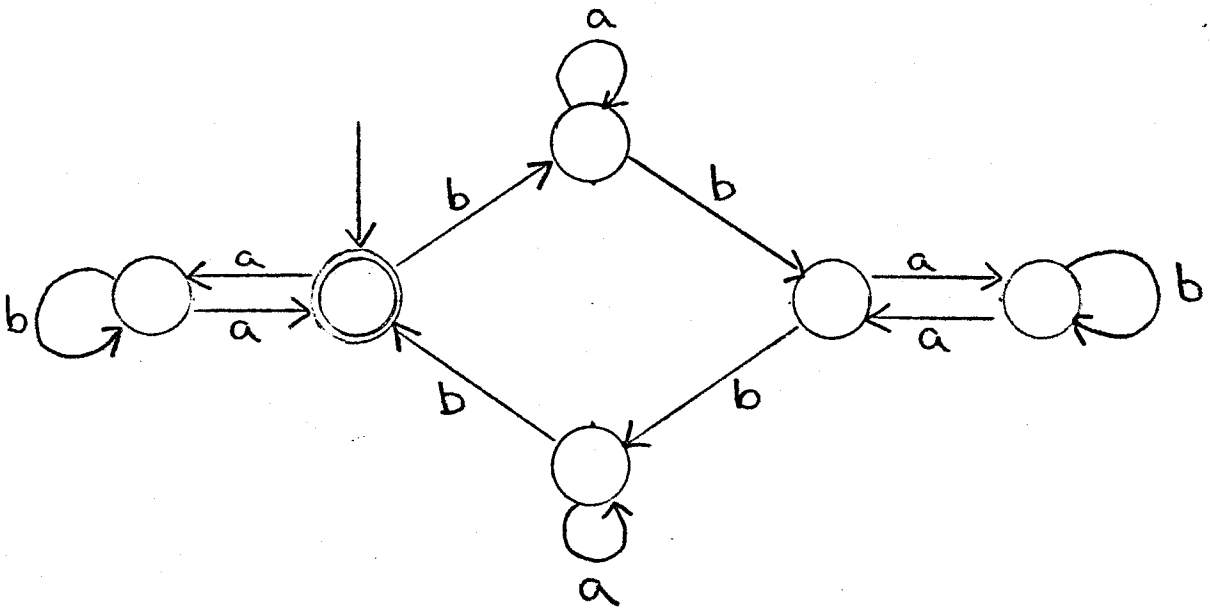


Fig. VIII.11: Representation of the syntactic right congruence of L_4

References

Brzozowski, J.A., Open Problems About Regular Languages, Proceedings of the Symposium on Formal Language Theory, Santa Barbara, 1979.

Brzozowski, J.A. and Fich, F.E., Languages of R-Trivial Monoids, Research Report CS-78-32, Department of Computer Science, University of Waterloo, 1978.

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

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

Cohen, R.S., and Brzozowski, J.A., Dot-depth of star-free events, J. Computer and Systems Sciences, vol. 5, 1971, 1-15.

Eggan, L.C., Transition graphs and the star-height of regular events, Michigan Math. J., 10 (1963), 385-397.

Eilenberg, S., "Automata, Languages, and Machines", Volume B, Academic Press, New York, 1976.

Fich, F.E., Languages of R-Trivial and Related Monoids, Research Report, CS-79-18, Department of Computer Science, University of Waterloo, 1979.

Ginzburg, A., "Algebraic Theory of Automata", Academic Press, New York, 1968.

Green, J.A., On the Structure of Semigroups, Annals of Math. 54 (1951, 163-172.

Hall, M., "The Theory of Groups", Chelsea Publishing Company, New York, 1959.

Henneman, W.H., Algebraic Theory of Automata, Ph.D. Dissertation, Massachusetts Institute of Technology, 1971.

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

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.

McNaughton, R., The theory of automata, a survey, Advan. Computing, vol. 2, 1961.

McNaughton, R., and Papert, S., "Counter-free automata", MIT Press, Cambridge, 1971.

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

Myhill, J., Finite automata and the representation of events, WADD Technical Report 57-624, Wright-Patterson Air Force Base, Nov. 1957.

Perles, M., Rabin, M.O., and Shamir, E., The theory of definite automata, IEEE Trans. Electronic Computer, vol. EC-12, 1963, 233-243.

Rabin, M.O., and Scott, D., Finite automata and their decision problems, IBM J. Res. and Dev., vol. 3, 1959, 114-125.

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

Simon, I., Hierarchies of Events with Dot-Depth One, Ph.D. thesis, Department of Computer Science, University of Waterloo, Waterloo, Onatrio, Canada, 1972.

Straubing H., Families of recognizable sets corresponding to certain varieties of finite monoids, J. Pure and Applied Algebra, vol. 15 (1979), 305-318.

Straubing H., A Generalization of the Schützenberger Product of Finite Monoids, to appear in Theoretical Computer Science, 1980.