Languages of Nilpotent and Solvable Groups

by

Denis Thérien
School of Computer Science
McGill University
Montréal, Québec

Research Report CS-78-44

December 1978

This research was supported by the National Research Council of Canada under a Science 67 Scholarship and under grant No. A-1617. Most of this work was done while the author was with the Computer Science Department at the University of Waterloo, Waterloo, Ontario.

Abstract

The theory of regular languages and the theory of finite monoids are closely related to each other. Many families of regular languages have been completely characterized by the corresponding family of (finite) syntactic monoids. In this paper we define, by means of congruences, a family of languages which correspond to finite nilpotent groups; the congruences are defined by counting subwords modulo some integer. By taking into account the context in which a subword appears, it is possible to define recursively a larger family of languages; it is shown that this other family corresponds to finite solvable groups. The congruences that we are using are powerful enough to characterize some important structural properties of the syntactic monoids.

Acknowledgements

My interest in regular languages has been continuously stimulated by working closely with professor J.A. Brzozowski. I thank him very much for the careful attention he gave to this paper. I owe many thanks as well to Robert Knast, with whom I had many interesting discussions.

1. INTRODUCTION

There is a deep relationship between the theory of regular languages and the theory of finite monoids. In fact, to each regular language we can associate its syntactic monoid, necessarily finite, and conversely, looking at a finite monoid as a semiautomaton, we can associate to it the set of languages, necessarily regular, which it can recognize for some choice of final states (the initial state being fixed as the unit of the monoid).

The importance of the relationship above can be seen in the fact that many families of regular languages have been characterized by the corresponding families of monoids. The most spectacular result of this kind is certainly the correspondance between the family of star-free languages and the family of group-free monoids (Schutzenberger [65]).

An approach commonly used is to define some family of congruences on A*, the free monoid generated by a finite alphabet A, and then investigate the set of languages which are unions of congruence classes for some congruence in the family. Among the interesting families of monoids that have been characterized completely by corresponding families of congruences are: "locally testable" monoids (Brzozowski & Simon [72] , McNaughton [74]), J-trivial monoids (Simon [72]), p-groups (Eilenberg [76]) and recently R-trivial and L-trivial monoids (Brzozowski & Fich [78]).

In this paper, we define by congruences the family of modulo languages and we establish the correspondence of this family with the set of finite nilpotent groups. Modulo languages can be defined by the sole operation of counting subwords modulo an integer. This serves as a basis step in the recursive definition of a family of languages which we call counting languages; this family is shown to correspond to finite solvable groups. Furthermore, the congruences we are using are powerful enough to characterize some important structural properties of the corresponding groups. Using different techniques, Straubing [78] was able to give a language characterization for these families of groups; his main result was a classification of the languages corresponding to solvable groups according to the derived length of their syntactic monoids. The results that we obtain by using congruences include this classification as a special case; other natural classifications for the same family of languages are also derived. Moreover, in Thérien [78], it is shown that the congruences used here have an analogous counterpart in the aperiodic (i.e. group-free) case.

First we introduce the definitions and the notation used in this paper. A monoid is a set M together with an associative binary operation and an element e of M such that $em = me = m$ for all $m \in M$; this element is called the unit. M is a group iff for each element m in M there exists an element m^{-1} of M such that $mm^{-1} = m^{-1}m = e$; it is customary to use the symbol 1 for the unit of a group. The operation on M can be extended to subsets of M and for $M_1, M_2 \subseteq M$ we define $M_1M_2 = \{m_1m_2 : m_1 \in M_1, m_2 \in M_2\}$; if $M_1 = \{m\}$ $(M_2 = \{m\})$ we abbreviate this to mM_2 (M_1m). We write $M_1{}^i$ for $\underbrace{M_1 \ldots M_1}_{i \text{ times}}$, $i \geq 1$, and we extend this to the case $i = 0$ by defining $M_1{}^0 = \{e\}$.

Let A be a finite set and $A^* = \bigcup_{i \geq 0} A^i$ be the free monoid generated by A with the empty word λ acting as unit. The length of $w \in A^*$ is defined by $|w| = i$ iff $w \in A^i$; note that the set of all words of length $\leq i$ is given by

$(A \cup \lambda)^i$. A language is a subset of A^*. The word x is a segment of the word w iff $w = uxv$, for some u, v in A^*. The word $x = a_1 \ldots a_m$, $a_i \in A$, is a subword of w iff $w = w_0 a_1 w_1 \ldots a_m w_m$ for some $w_0, \ldots, w_m \in A^*$. We use the convention that $a_i \ldots a_j = \lambda$ if $j < i$; we extend this notation to sequences over arbitrary sets, i.e. the sequence $(x_i, \ldots, x_j)$ of elements of X is empty whenever $j < i$.

A binary relation $\sim$ on A^* is a subset of $A^* \times A^*$; we write $x \sim y$ when $(x,y) \in \sim$. The relation $\sim$ is an equivalence of finite index iff $\sim$ partitions A^* in a finite number of disjoint classes $[x_1]_\sim, \ldots, [x_n]_\sim$ such that $A^* = \cup [x_i]_\sim$ where $[x]_\sim = \{y: \; x \sim y\}$; we write $[x]$ when $\sim$ is understood. The equivalence relation $\sim$ is a right (left) congruence iff $x \sim y$ implies $xu \sim yu$ $(ux \sim uy)$ for all $u \in A^*$; it is a congruence iff it is both a right and a left congruence or equivalently if $x_1 \sim y_1$, $x_2 \sim y_2$ implies $x_1 x_2 \sim y_1 y_2$. The set of congruence classes forms a monoid $A^*/\sim$ with multiplication $[x][y] = [xy]$ and unit $[\lambda]$. We say that $\sim$ is a group congruence iff $A^*/\sim$ is a group; in this case we use y^{-1} to denote any word $w \in [y]^{-1}$. In particular the universal congruence, $x \sim y$ for all x, $y \in A^*$, is trivially a group congruence since $A^*/\sim = \{1\}$. For a given equivalence $\sim$, L is a $\sim$language iff it is the union of classes of $\sim$. A $\sim_1$ language is regular iff there exists a congruence of finite index $\sim_2$ such that $\sim_2 \subseteq \sim_1$; thus L is also a $\sim_2$language. In particular for any language L, we define the syntactic congruence $\equiv_L$ by

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

It is always the case that $\equiv_L$ is a congruence and that L is a $\equiv_L$language. Denote $A^*/\equiv_L$ by M_L; if L is a $\sim$language for some congruence $\sim$, then $\sim \subseteq \equiv_L$ and hence $|M_L| \leq |A^*/\sim|$ where $|X|$ denotes the cardinality of the set X. Thus L is regular iff M_L if finite.

A semiautomaton is a triple $\mathcal{A} = \langle S_{\mathcal{A}}, A_{\mathcal{A}}, \delta_{\mathcal{A}} \rangle$; we use the notation S, A and δ when it is clear which semiautomaton is involved. S is the finite set of states, A is a finite alphabet and δ: $S \times A \to S$ is the transition function. We extend δ to all pairs (s,x) in $S \times A^*$ by defining

$$\delta(s,x) = \begin{cases} s & \text{if } x = \lambda \\ \delta(\delta(s,x'),a) & \text{if } x = x'a. \end{cases}$$

By choosing an initial state $s_0 \varepsilon S$ and a set of final states $S' \subseteq S$ we get an automaton $\mathcal{A} = \langle S, A, \delta, s_0, S' \rangle$ which accepts the regular language $L = \{x \varepsilon A^*: \ \delta(s_0,x) \varepsilon S'\}$.

With any semiautomaton $\mathcal{A} = \langle S, A, \delta \rangle$ we associate a monoid $\mathcal{A}^\tau = A^*/\sim$ where $\sim$ is the congruence of finite index defined by

$$x \sim y \text{ iff for all } s \varepsilon S, \ \delta(s,x) = \delta(s,y).$$

$\mathcal{A}^\tau$ is a group iff there exists an integer n such that $x^n \sim \lambda$ for all $x \varepsilon A^*$.

Conversely any finite monoid M determines a unique semiautomaton $\langle M, M, \delta \rangle$ where δ is the monoid multiplication: we call such a semiautomaton a monoid (or group) semiautomaton.

Let $\mathcal{A}_i = \langle S_i, A_i, \delta_i \rangle$ for i = 1, 2. $\mathcal{A}_1$ is a subsemiautomaton of $\mathcal{A}_2$ iff $S_1 \subsetneqq S_2$, $A_1 \subseteq A_2$ and δ_1 is the restriction of δ_2 to $S_1 \times A_1$. $\mathcal{A}_1$ is a homomorphic image of $\mathcal{A}_2$ iff $A_1 = A_2$ and there exists an epimorphism ϕ: $S_2 \to S_1$ with the property that for all $s \varepsilon S_2$, for all $a \varepsilon A_2$, $\phi(\delta_2(s,a)) = \delta_1(\phi(s),a)$. $\mathcal{A}_1$ is covered by $\mathcal{A}_2$, $\mathcal{A}_1 \prec \mathcal{A}_2$ iff $\mathcal{A}_1$ is a homomorphic image of a subsemiautomaton of $\mathcal{A}_2$. If $\mathcal{A}_i = \langle M_i, M_i, \delta_i \rangle$ is a monoid semiautomaton for i = 1, 2, this coincides with the notion of M_1

being a homomorphic image of a submonoid of M_2. The cross product of A_1, and A_2 is defined as

$$A_1 \times A_2 = \langle S_1 \times S_2,\ A_1 \cap A_2,\ \delta \rangle$$

where $\delta((s_1,s_2),a) = (\delta_1(s_1,a),\ \delta_2(s_2,a))$. If $A_2 = S_1 \times A_1$, we define the cascade connection of A_1 and A_2 to be

$$A_1 \circ A_2 = \langle S_1 \times S_2,\ A_1,\ \delta \rangle$$

where $\delta((s_1,s_2),a) = (\delta_1(s_1,a),\ \delta_2(s_2,(s_1,a)))$; if $x = a_1 \ldots a_m$, this extends to

$$\delta((s_1,s_2),x) = (\delta_1(s_1,x),\ \delta_2(s_2,\omega(x)))$$

where $\omega(x) = (t_1,a_1)(t_2,a_2)\ldots(t_m,a_m)$, $t_i = \delta_1(s_1,a_1 \ldots a_{i-1})$ for $i = 1,\ldots,m$. For more details on these concepts, see Ginzburg [68].

Finally we recall some elementary notions of modular arithmetic. Let N be the set of nonnegative integers; we write $m \mid n$ for m divides n. For $m, n, q \in N$, $q > 0$, $m \equiv n \pmod q$ iff $q \mid m - n$; in particular $m \equiv n \pmod 1$ for all integers m, n. If K is a finite subset of N, lcm K is the least common multiple of the integers in K; if $K = \phi$, lcm $K = 1$; if $K' \subseteq K$ then lcm $K' \mid$ lcm K. Also $m \equiv n \pmod{q_1}$ and $m \equiv n \pmod{q_2}$ iff $m \equiv n \pmod{\mathrm{lcm}\{q_1,q_2\}}$. If $q_2 \mid q_1$, $m \equiv n \pmod{q_1}$ implies $m \equiv n \pmod{q_2}$. We will denote by Z_q the set of equivalence classes of the integers mod q.

2. ELEMENTS OF GROUP THEORY

In this section, we state some definitions and results from group theory for later use. Unless otherwise referenced, the content of this section and further details can be found in Scott [64].

All groups considered are finite. A group G is abelian iff $gh = hg$ for all $g, h \in G$. A subset H of G is subgroup iff it forms a group under the multiplication of G; the right (left) cosets Hg (gH) are either equal or disjoint and $|H| \mid |G|$. H is normal in G, $H \lhd G$, iff $g^{-1}hg \in H$ for all $g \in G$, $h \in H$. The set of all right cosets then form a group under the multiplication $(Hg_1)(Hg_2) = H(g_1g_2)$ and we denote this group by G/H. If G has normal subgroup H such that G/H is isomorphic with K, which we denote $G/H \simeq K$, we say that G is an extension of H by K.

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

$$G_0 = G \rhd G_1 \rhd G_2 \rhd \dots \quad .$$

For a given prime integer p, G is a p-group iff each element is of order p^α for some $\alpha \geq 0$, i.e. $g^{p^\alpha} = 1$; if $|G| = p^\alpha q$ with p, q relatively prime, G has a subgroup of order p^α; any such subgroup is called a Sylow p-subgroup of G.

The center of a group G is the normal subgroup $Z(G) = \{h\colon \ gh = hg$ for all $g \in G\}$. A normal series

$$Z_0 = \{1\} \lhd Z_1 \lhd \dots \lhd Z_m = G$$

is a central series iff $Z_i/Z_{i-1} \subseteq Z(G/Z_{i-1})$ for $i = 1,\dots,m$. G is said to be nilpotent if such a series exists; it is said to be of class m, if no shorter central series exists. If $H \subseteq Z(G)$ is a normal subgroup of G and G/H is nilpotent of class m-1, then G is nilpotent of class $\leq m$. Also G is nilpotent iff it is the direct product of a set of representatives of its Sylow p-subgroups.

The commutator of g and h is $[g,h] = g^{-1}h^{-1}gh$. The derived subgroup $G_1 = [G,G]$ is the normal subgroup of G generated by the set of all commutators; it is always the case that G/G_1 is abelian. Let $G_0 = G$ and $G_i = [G_{i-1}, G_{i-1}]$ for $i \geq 1$; G_i is the i^{th} derived subgroup of G. G is solvable of derived length n iff

$$G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_n = \{1\},$$

that is if the n^{th} derived subgroup is trivial. Alternatively, G is solvable of fitting length k iff there exists a normal series

$$F_0 = \{1\} \triangleleft F_1 \triangleleft \dots \triangleleft F_k = G$$

such that F_{i+1}/F_i is nilpotent.

Let $\mathcal{G}_{ab}$, $\mathcal{G}_p$ for arbitrary prime p, $\mathcal{G}_{nil}$ and $\mathcal{G}_{sol}$ denote respectively the family of abelian groups, p-groups, nilpotent groups and solvable groups; the following chains of inclusions hold

$$\mathcal{G}_{ab} \subseteq \mathcal{G}_{nil} \subseteq \mathcal{G}_{sol}$$

$$\mathcal{G}_{p} \subseteq \mathcal{G}_{nil} \subseteq \mathcal{G}_{sol}.$$

Also each one of these families is closed under homomorphism, finite direct product and the operation of taking subgroups, i.e. each one is a variety in Eilenberg's sense (Eilenberg [76]).

An important result linking the structure of a group G and the structure of the group semiautomaton $\langle G, G, \delta \rangle$ is the following.

Lemma 2.1: If $H \triangleleft G$, then $<G, G, \delta> \prec <G_1, G_1, \delta_1> \circ <G_2, G_2, \delta_2>$ with $G_1 \simeq G/H$ and $G_2 \simeq H$.

Proof: See Ginzburg [68] or Eilenberg [76].□

Thus for any normal series

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_n = \{1\}$$

we have

$$<G, G, \delta> \prec <H_1, H_1, \delta_1> \circ \ldots \circ <H_n, H_n, \delta_n>$$

where $H_i \simeq G_{i-1}/G_i$. From this follows the fact that any solvable-group semiautomaton can be constructed with abelian-group semiautomata (or nilpotent-group semiautomata) provided cascade product and covering are available.

If $\sim_1$ is a group congruence, i.e. if $A_{\sim_1} = A^*/\sim_1$ is a group, subgroups have a particularly simple form.

Lemma 2.2: a) H is a subgroup of $A_{\sim_1}$ iff $H = \{[x]_{\sim_1} : x \sim_2 \lambda\}$ for some right congruence such that $\sim_1 \subseteq \sim_2$. We will write $H_{2,1}$ for H above.

b) $H_{2,1} \triangleleft A_{\sim_1}$ iff $\sim_2$ is a congruence; moreover $A_{\sim_1}/H_{2,1} \simeq A_2$;

c) If $\sim_1 \subseteq \sim_2 \subseteq \sim_3$ are congruences then $H_{2,1} \triangleleft H_{3,1}$ and $H_{3,1}/H_{2,1} \simeq H_{3,2}$.

Proof: a) For any right congruence $\sim_2$ containing $\sim_1$, the set $H_{2,1}$ is well-defined and it is obviously a subgroup. Conversely, if H is a subgroup, define the relation $\sim_2$ on A^* by $x \sim_2 y$ iff $Hx = Hy$; this defines a right congruence such that $\sim_1 \subseteq \sim_2$, each class being a coset; also $H = \{[x]_{\sim_1} : x \sim_2 \lambda\}$.

b) $H_{2,1} \triangleleft A_{\sim_1}$ iff $y^{-1}xy \sim_2 \lambda$ for all $x \sim_2 \lambda$ and for all y in A^*. But $y^{-1}xy$ is well defined mod $\sim_2$ iff $\sim_2$ is a congruence. In this case $y^{-1}xy \sim_2 y^{-1}y \sim_2 \lambda$ since $\sim_1 \subseteq \sim_2$. Moreover define ϕ: $A_{\sim_1}/H_{2,1} \to A_{\sim_2}$ by $\phi(H_{2,1}[x]_{\sim_1}) = [x]_{\sim_2}$.

i) ϕ is well defined; if $y_1, y_2 \in H_{2,1}$, $x_1 \sim_1 x_2$ then $y_1x_1 \sim_2 x_1 \sim_2 x_2 \sim_2 y_2x_2$

ii) ϕ is an epimorphism since, for any x in A*, $[x]_{\sim_2} = \phi(H_{2,1}[x]_{\sim_1})$

iii) ϕ is injective since $x \sim_2 y$ implies $xy^{-1} \sim_2 \lambda$; hence $xy^{-1} \in H_{2,1}$ and $H_{2,1}[x]_{\sim_1} = H_{2,1}[y]_{\sim_1}$.

c) The inclusion of the subgroups is clear since $x \sim_2 \lambda$ implies $x \sim_3 \lambda$. Also for any $y \in H_{3,1}$, and for $x \sim_2 \lambda$, $y^{-1}xy \sim_2 \lambda$ since $y^{-1}y \sim_1 \lambda$. Moreover it can be verified easily that the isomorphism defined in b) maps $H_{3,1}/H_{2,1}$ onto $H_{3,2}$.

In practice, we often make no distinction between a group and the corresponding group semiautomaton; we extend this identification to the case where a group G is given on a set of generators A, this corresponding naturally to a semiautomaton <G, A, δ> where δ is the group multiplication.

3. MODULO LANGUAGES AND NILPOTENT GROUPS

In this section, we introduce a family of equivalence relations on A*. These equivalences are defined by counting the number of times that subwords appear in words, modulo some integer. It is shown that these equivalences define a family of regular languages, which we call the family of modulo languages. A characterization of these languages is given in terms of their syntactic monoids: L is a modulo language iff M_L is a finite nilpotent group.

The following definition and proposition are borrowed from Eilenberg [76]. Let $u = a_1 \ldots a_m$, $x \in A^*$;

$$\binom{x}{u} = \begin{cases} 1 \text{ if } u = \lambda \\ \text{the number of factorizations of } x \text{ in the form} \\ x = x_0 a_1 x_1 \ldots a_m x_m \text{ otherwise} \end{cases}$$

Lemma 3.1: Let $u, x, y \in A^*$, $a \in A$. Then

a) $\displaystyle \binom{xy}{u} = \sum_{u=u_1u_2} \binom{x}{u_1}\binom{y}{u_2}$

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

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

For example, $\binom{abbab}{ab} = 4$ and $\binom{abbab}{ba} = 2$.

Let $f\colon A^+ \to N^+$, where $A^+ = A^* \setminus \{\lambda\}$ and $N^+ = N \setminus \{0\}$. We define

$$\text{supp } f = \{u\colon\ f(u) \neq 1\}$$

$$\text{im } f = \{n\colon\ f(u) = n \text{ for some } u \in A^+\};$$

(supp is for support and im for image). Also f is said to be of class m iff m is the least integer such that supp $f \subseteq (A \cup \lambda)^m \setminus \{\lambda\}$. Note that the constant function $f(u) = 1$ for all $u \in A^+$ is the only function of class 0; we denote this function by 1.

The relation $\sim_f$ is defined on A^* by

$$x \sim_f y \text{ iff for all } u \in A^+, \binom{x}{u} \equiv \binom{y}{u} \pmod{f(u)}.$$

Thus to each word x is associated a vector (finite or infinite)

$$\left(\binom{x}{u_1} \pmod{f(u_1)}, \binom{x}{u_2} \pmod{f(u_2)}, \ldots \right)$$

where supp $f = \{u_1, u_2, \ldots\}$; the pair (x,y) is in the relation $\sim_f$ iff both words have the same associated vector.

<u>Lemma 3.2</u>: Let $f\colon A^+ \to N^+$;

a) $\sim_f$ is an equivalence relation;

b) if supp f is finite, $\sim_f$ is of finite index.

Proof: a) trivial

b) If supp $f = \{u_1, \ldots, u_n\}$, the vector associated with x is an element of $Z_{f(u_1)} \times \ldots \times Z_{f(u_n)}$. Since the vector determines the equivalence class, the index of the relation is bounded by the cardinality of $Z_{f(u_1)} \times \ldots \times Z_{f(u_n)}$. □

For example, let $A = \{a,b\}$ and

$$f(u) = \begin{cases} 2 & \text{if } u = a \text{ or } u = ab \\ 1 & \text{otherwise;} \end{cases}$$

f is a function of class 2 with supp $f = \{a, ab\}$ and im $f = \{1, 2\}$; with each x is associated a vector $\left(\binom{x}{a} \pmod 2, \binom{x}{ab} \pmod 2\right)$. There are four classes corresponding to the four elements of $Z_2 \times Z_2$: they are

$[\lambda] = (0,0)$, $[a] = (1,0)$, $[ab] = (1,1)$, $[aba] = (0,1)$.

From now on we restrict ourselves to functions of finite support. Let F_i = {f: f is of class at most i}, and let $F = \bigcup_{i=0}^{\infty} F_i$.

Lemma 3.3: Let $f \in F$;

a) $\sim_f$ is a right congruence iff $x \sim_f y$ implies $\binom{x}{u'} \equiv \binom{y}{u'}$ (mod f(u)) for all x, y in A*, all u' in A^+ and for all $u \in u'A^*$;

b) $\sim_f$ is a left congruence iff $x \sim_f y$ implies $\binom{x}{u'} \equiv \binom{y}{u'}$ (mod f(u)) for all x, y in A*, all u' in A* and for all $u \in A^*u'$.

Proof: We prove only a) since b) can be obtained by symmetry.

Suppose that f is a function such that $x \sim_f y$ and $\binom{x}{u'} \equiv \binom{y}{u'}$ (mod f(u)) for all $u \in u'A^*$. We have $\binom{xz}{u} = \sum_{u=u_1u_2} \binom{x}{u_1}\binom{z}{u_2}$; but $\binom{x}{u_1} \equiv \binom{y}{u_1}$ (mod f(u)) since $u \in u_1A^*$. Hence $\binom{xz}{u} \equiv \sum_{u=u_1u_2} \binom{y}{u_1}\binom{z}{u_2}$ (mod f(u)) $\equiv \binom{yx}{u}$ (mod f(u)). Thus $xz \sim_f yz$ and $\sim_f$ is a right congruence. To prove the converse, suppose the condition does not hold. There exists x, y, u = u'u" such that $x \sim_f y$ but $\binom{x}{u'} \not\equiv \binom{y}{u'}$ (mod f(u)); choose u' such that the condition is satisfied for all prefixes of u of length greater than |u'|;

$$\binom{xu''}{u} = \sum_{u=u_1u_2} \binom{x}{u_1}\binom{u''}{u_2} = \sum_{\substack{u=u_1u_2 \\ |u_2|<|u''|}} \binom{x}{u_1}\binom{u''}{u_2} + \binom{x}{u'}\binom{u''}{u''}.$$

Similarly $\binom{yu''}{u} = \sum_{\substack{u=u_1u_2 \\ |u_2|<|u''|}} \binom{y}{u_1}\binom{u''}{u_2} + \binom{y}{u'}\binom{u''}{u''}$. Because of the maximality assumption on u', we have $\binom{x}{u_1} \equiv \binom{y}{u_1}$ (mod f(u)) when $|u_2|<|u''|$; thus

$\binom{xu''}{u} - \binom{yu''}{u} \equiv \binom{x}{u'} - \binom{y}{u'}$ (mod f(u)) $\not\equiv$ 0 (mod f(u)) and $\sim_f$ is not a right congruence. □

Lemma 3.4: Let $f \in F$, $x, y \in A^*$, $u \in A^+$; then $\sim_f$ is a congruence iff $x \sim_f y$ implies $\binom{x}{u'} \equiv \binom{y}{u'}$ (mod f(u)) for all x, y in A*, all u' in A^+ and for all $u \in A^* u'A^*$.

Proof: The proof is a replica of the proof of lemma 3.3, except that segment instead of prefix is used to establish the necessity of the condition. □

For example, observe that any function f for which $f(u) \mid f(u')$ for all prefixes (suffixes, segments) u' of u and for all $u \in A^*$, satisfies the condition of lemma 3.3a) (3.3b), 3.4). Therefore $\sim_f$ is a right congruence (left congruence, congruence). Moreover we will show that for any (right, left) congruence $\sim_f$, we can find a function f* such that $\sim_f = \sim_{f*}$ and for which the divisibility relation mentioned above is satisfied. We define the following terms:

i) f is p-closed iff $f(u) \mid f(u')$ for all $u \in u'A^*$;

ii) f is s-closed iff $f(u) \mid f(u')$ for all $u \in A^*u'$;

iii) f is p$\wedge$s-closed iff it is p-closed and s-closed.

Here p and s are meant to suggest prefix and suffix respectively.

Lemma 3.5: Let $f \in F$; f is p$\wedge$s-closed iff $f(u) \mid f(u')$ for all $u \in A^*u'A^*$.

Proof: Easily verified.

We say that a function f is full iff ($x \sim_f y$ implies $\binom{x}{u} \equiv \binom{y}{u}$ (mod k)) iff $k \mid f(u)$. As an example of a function which is not full consider A = {a} and

$$f(u) = \begin{cases} 4 & \text{if } u = a \\ 1 & \text{otherwise.} \end{cases}$$

It is easily seen that the equivalence classes of $\sim_f$ are $[\lambda]$, $[a]$, $[aa]$, $[aaa]$ and one can verify that $x \sim_f y$ implies $\binom{x}{aa} \equiv \binom{y}{aa}$ (mod 2); but 2 does not divide $f(aa) = 1$ and f is not full. We now proceed to show that for any function $f \in F$, there is a unique full function $f^* \in F$ such that $\sim_f = \sim_{f^*}$.

<u>Lemma 3.6</u>: Let $[f] = \{g \in F\colon \ \sim_f = \sim_g\}$. Then $[f]$ is finite.

Proof: Suppose $g \in [f]$; we first show that g is of class at most k for some k depending on f. Let $[x_1]_f, \ldots, [x_n]_f$ be the equivalence classes of $\sim_f$ and assume that the x_i's are of minimal length; let $k = \max\{\,|x_i|;\ i = 1,\ldots,n\}$ and let $|u| > k$; then $[u]_f = [x_i]_f$ for some i and thus $[u]_g = [x_i]_g$. But $\binom{u}{u} = 1$ and $\binom{x_i}{u} = 0$; so we must have $g(u) = 1$. Finally, let $u \in \operatorname{supp} g$; if $x \sim_f y$ implies $\binom{x}{u} = \binom{y}{u}$ then u^i cannot be equivalent to u^j if $i \neq j$ and $\sim_f$ have infinite index. Thus, there exists x, y in A^* such that $x \sim_f y$ and $\binom{x}{u} = \binom{y}{u} + k$ for some $k > 0$. Since $x \sim_g y$, it must be that $g(u) \mid k$. Altogether, this shows that there is only a finite number of possibilities for g.

<u>Lemma 3.7</u>: Let $f \in F$; there exists a unique full function f^* such that $\sim_f = \sim_{f^*}$.

<u>Proof</u>: Let $[f] = \{f_1,\ldots,f_n\}$ and let $f^*(u) = \operatorname{lcm}\{f_i(u)\ i = 1,\ldots,n\}$. We have $f(u) \mid f^*(u)$ and this clearly implies $\sim_{f^*} \subseteq \sim_f$; also

$$x \sim_f y \Rightarrow x \sim_{f_i} y \text{ for } i = 1,\ldots,n$$

$$\Rightarrow \binom{x}{u} \equiv \binom{y}{u} \pmod{f_i(u)} \text{ for } i = 1,\ldots,n$$

$$\Rightarrow \binom{x}{u} \equiv \binom{y}{u} \pmod{\operatorname{lcm}\{f_i(u)\colon\ i = 1,\ldots,n\}}$$

$$\Rightarrow x \sim_{f^*} y$$

and $\sim_f \subseteq \sim_{f^*}$. So $f^* \in [f]$. To show it is full, suppose $x \sim_{f^*} y$ implies $\binom{x}{u} \equiv \binom{y}{u}$ (mod k); then $\binom{x}{u} \equiv \binom{y}{u}$ (mod $\operatorname{lcm}\{k, f^*(u)\}$).

Define

$$f'(v) = \begin{cases} f^*(v) & \text{if } v \neq u \\ \mathrm{lcm}\{k,\ f^*(u)\} & \text{if } v = u. \end{cases}$$

It is easily verified that $f' \in [f]$ and so that $f'(u) \mid f^*(u)$; this implies that $k \mid f^*(u)$ and f^* is full. Finally suppose there is another full function $f' \in [f]$; we must have $f'(u) \mid f^*(u)$ and $f^*(u) \mid f'(u)$, hence $f' = f^*$. □

The following lemma tells us that for full functions the notions of (right, left) congruence coincide with the notions of (p-closed, s-closed) p∧s-closed. Also inclusion of equivalence relations is reduced to divisibility; we say that $g \leq f$ iff $\sim_f \subseteq \sim_g$.

<u>Lemma 3.8</u>: Let $f \in F$ be full;

i) $\sim_f$ is a right congruence iff f is p-closed

ii) $\sim_f$ is a left congruence iff f is s-closed

iii) $\sim_f$ is a congruence iff f is p∧s-closed

iv) $g \leq f$ iff $g(u) \mid f(u)$ for all $u \in A^+$.

Proof: Clear. □

We are now ready to turn our attention to the study of the languages which are $\sim_f$ languages for some $f \in F$; these languages are called modulo languages. We use the term modulo languages of class m for those languages which are $\sim_f$ languages for some $f \in F_m$. The rest of this section is devoted to the characterization of this family in terms of syntactic monoids.

<u>Lemma 3.9:</u> Modulo languages are regular.

Proof: Let L be a $\sim_f$ language for some $f \in F$. For all u in A*, let $g(u) = \mathrm{lcm}\ \{f(u') : u' \in A^*uA^*\}$. Clearly $f(u) \mid g(u)$ and thus $\sim_g \subseteq \sim_f$.

Also g is a congruence (of finite index) since it is p∧s-closed. Hence L is regular. □

Lemma 3.10: Modulo languages of class i form a boolean algebra.

Proof: Closure under complementation is obvious. Also suppose $L = L_1 \cup L_2$ where L_1 is a $\sim_{f_1}$ language, L_2 is a $\sim_{f_2}$ language, $f_1, f_2 \in \mathcal{F}_i$. Then L is a $\sim_f$ language where $f(u) = \mathrm{lcm}\{f_1(u), f_2(u)\}$ and L is a modulo language of class i. □

From the proof of lemma 3.9, we can conclude that for any modulo language L there is a p∧s-closed function f such that $M_L \prec A^*/\sim_f$. When f is p∧s-closed, $A^*/\sim_f$ is a monoid which we call A_f.

Lemma 3.11: A_f is a finite group for any p∧s-closed $f \in \mathcal{F}$.

Proof: A_f is a finite monoid since $\sim_f$ is a congruence of finite index. Suppose $f \in \mathcal{F}_m$; we show that A_f is a group by proving $x^{k^m} \sim_f \lambda$, where $k = \mathrm{lcm}\{f(u)\colon\ u \in \mathrm{supp}\ f\}$. We first need the intermediate result that $\binom{x^{k^i}}{u} \equiv 0 \pmod k$ for all u in A^+ and $i \geq |u|$; we establish this by induction on $|u|$.

Basis $|u| = 1$

We have $\binom{x^{k^i}}{u} = k^i \binom{x}{u} \equiv 0 \pmod k$ since $i \geq 1$.

Induction step $|u| > 1$

By lemma 3.1a), $\binom{x^{k^i}}{u} = \sum_{u=u_1\cdots u_k} \binom{x^{k^{i-1}}}{u_1} \cdots \binom{x^{k^{i-1}}}{u_k}$.

If $1 \leq |u_i| < |u|$ then $i-1 \geq |u_i|$ and we can apply the induction hypothesis to cancel this term. Thus

$$\binom{x^{k^i}}{u} \equiv k \cdot \binom{x^{k^{i-1}}}{u} \pmod{k}$$

$$\equiv 0 \pmod{k}.$$

and the intermediate result is established. From it follows the fact that

$\binom{x^{k^m}}{u} \equiv 0 \pmod{k}$ for all $u \in \operatorname{supp} f$ and $\binom{x^{k^m}}{u} \equiv 0 \pmod{f(u)}$ for all $u \in \operatorname{supp} f$

since $f(u) \mid k$. Hence $x^{k^m} \sim_f \lambda$. □

Corollary 3.1: If $\operatorname{im} f \subseteq \{p^\alpha: \alpha \geq 0\}$ for some prime p, then A_f is a p-group.

Proof: Immediate from the proof of lemma 3.11. □

Let $g \leq f$ be p∧s-closed; the set $\{[x]_f: x \sim_g \lambda\}$ is well defined and we denote it by $H_{g,f}$ or H_g if f is understood.

Lemma 3.12: $H_g \triangleleft A_f$.

Proof: By lemma 2.2b). □

Lemma 3.13: $A_f/H_g \simeq A_g$.

Proof: From lemma 2.2b), the isomorphism is given by $\phi(H_g[x]_f) = [x]_g$. □

Lemma 3.14: Let $g(u) = \operatorname{lcm}\{f(u_1uu_2): u_1u_2 \neq \lambda\}$; then $H_g \subseteq Z(A_f)$.

Proof: The function g is p∧s-closed and $g \leq f$. By lemma 3.12, H_g is a normal subgroup of A_f. Moreover $\binom{xy}{u} = \binom{x}{u} + \binom{y}{u} + \sum_{\substack{u=u_1u_2\\u_1\neq\lambda\\u_2\neq\lambda}} \binom{x}{u_1}\binom{y}{u_2}$;

so if $x \sim_g \lambda$, $\binom{x}{u_1} \equiv 0 \pmod{g(u_1)}$ and since $f(u) \mid g(u_1)$, we have $\binom{x}{u_1} \equiv 0 \pmod{f(u)}$, whenever $u_1 \neq \lambda$. Thus $\binom{xy}{u} \equiv \binom{x}{u} + \binom{y}{u} \pmod{f(u)}$.

Similarly $\binom{yx}{u} \equiv \binom{y}{u} + \binom{x}{u}$ (mod f(u)) and xy $\sim_f$ yx. Hence $H_g \subseteq Z(A_f)$. □

Lemma 3.15: If $f \in F_m$, A_f is nilpotent of class $\leq m$.

Proof: By induction on m.

Basis m = 0

$A_f = \{1\}$ is nilpotent of class 0.

Induction step m > 0

By lemma 3.14 $H_g \subseteq Z(A_f)$ where $g \in F_{m-1}$; by induction hypothesis A_g is nilpotent of class $\leq$ m-1. Using lemma 3.13, we conclude that A_f is the extension of a nilpotent group of class $\leq$ m-1 by a group included in its center. Hence A_f is nilpotent of class $\leq$ m. □

Corollary 3.2: If L is a modulo language of class m, M_L is a nilpotent group of class $\leq$ m.

Proof: From the proof of lemma 3.9, $M_L \prec A_f$ for some $f \in F_m$. Since A_f is nilpotent of class $\leq$ m , M_L must be nilpotent of class $\leq$ m .

Lemma 3.16 (Eilenberg): If L is a language such that M_L is a p-group, then L is a modulo language. Moreover L is a $\sim_f$ language for some f with im f = {1,p}.

Theorem 3.1: L is a modulo language iff M_L is a finite nilpotent group.

Proof: The necessity of the condition has been established in corollary 3.2. Conversely suppose M_L is nilpotent, then $M_L = G_1 \times \ldots \times G_n$ where G_i is a p_i-group. If L is over the alphabet $A = \{a_1,\ldots,a_k\}$, each $[a_j]_{\equiv_L}$ as an element of M_L has a unique representation $(g_{j1},\ldots,g_{jn}) \in G_1 \times \ldots \times G_n$ and G_i is generated by $A_i = \{g_{1i},\ldots,g_{ki}\}$ Let π_i: $A^* \to A_i^*$ be the homomorphism induced by $\pi_i(a_j) = g_{ji}$. By lemma 3.16, there exists f_i: $A_i^+ \to N^+$ such that $G_i \prec A_i^*/\sim_{f_i}$: that is, if for all $u' \in A_i^*$, $x, y \in A^*$, $\binom{\pi_i(x)}{u'} \equiv \binom{\pi_i(y)}{u'}$ (mod $f_i(u')$)

then $\pi_i(x)$ is equal to $\pi_i(y)$ in G_i. We define a function $\bar{f}_i$: $A^+ \to N^+$, by $\bar{f}_i(u) = f_i(\pi_i(u))$ for all $u \in A^+$; also let $f(u) = \mathrm{lcm}\{\bar{f}_i(u)\colon\ i = 1,\ldots,n\}$. If $x \sim_f y$ then $x \sim_{\bar{f}_i} y$ for $i = 1,\ldots,n$ and $\pi_i(x) \sim_{f_i} \pi_i(y)$ for $i = 1,\ldots,n$

since $\binom{\pi_i(x)}{u_1} = \sum_{\pi_i(u)=u_1} \binom{x}{u}$. Hence $M_L \prec A_f$. □

In corollary 3.2, we were able to prove that to a modulo language of class m corresponds a nilpotent group of class m. Theorem 3.1 does not give such a strong converse, i.e. if M_L is nilpotent of class m, the theorem does not say that L is a modulo language of class m. We conjecture that this stronger converse holds as well and we prove it in the special cases $m = 0$, $m = 1$.

Lemma 3.17: For $m \leq 1$, L is a modulo language of class m iff M_L is a nilpotent group of class $\leq m$.

Proof: The necessity of the condition was stated in corollary 3.2. Sufficiency is trivial to establish for $m = 0$. For $m = 1$ (i.e. abelian groups), let $f(a) = o(a)$, the order of a, for each $a \in A$. If $x \sim_f y$ then $x \equiv_L y \equiv_L a_1^{\alpha_1} \ldots a_k^{\alpha_k}$, $0 \leq \alpha_i < o(a_i)$ because of commutativity. □

As an example to the notions discussed in this section, consider the dihedral group D_4, which is nilpotent of class 2. One possible set of defining relations over two generators is $a^2 = b^2 = (ab)^4 = 1$. This corresponds to the representation of Fig. 1a. The group D_4 is isomorphic to A_f for

$$f(u) = \begin{cases} 2 & \text{if } u = a, b \text{ or } ab \\ 1 & \text{otherwise.} \end{cases}$$

The center of A_f is given by $\{[x]_f: \ x \sim_g \lambda\}$ for

$$g(u) = \begin{cases} 2 \text{ if } u = a, b \\ 1 \text{ otherwise} \end{cases}$$

and this corresponds to elements 0 and 4. The resulting quotient group can be verified to be the abelian group $Z_2 \times Z_2$ of Fig. 1b where we have identified the cosets by enumerating their elements.

D_4 also has the defining relations $a^2 = b^4 = (ab)^2 = 1$, and this has the representation of Fig. 2. The group D_4 is a homomorphic image of A_f with

$$f(u) = \begin{cases} 2 & u = a, b, aa, ba \\ 1 & \text{otherwise} \end{cases}$$

where to each x is associated the vector

$$(\binom{x}{a} \pmod 2, \binom{x}{b} \pmod 2, \binom{x}{aa} + \binom{x}{ba} \pmod 2)$$

The center is $\{0, 2\}$ and again it is H_g for

$$g(u) = \begin{cases} 2 & \text{if } u = a, b \\ 1 & \text{otherwise.} \end{cases}$$

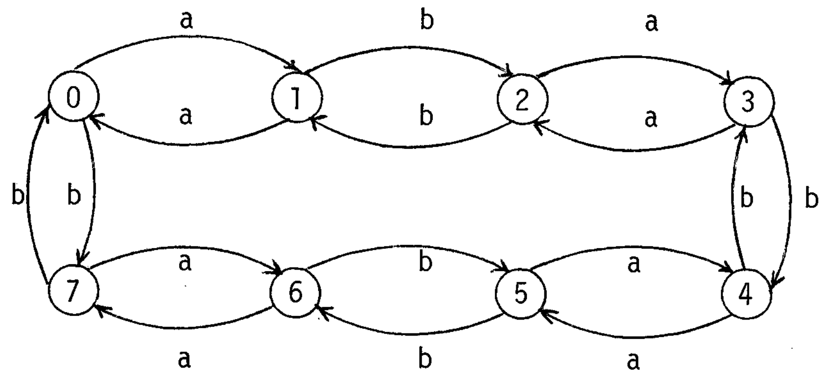

Fig. 1a

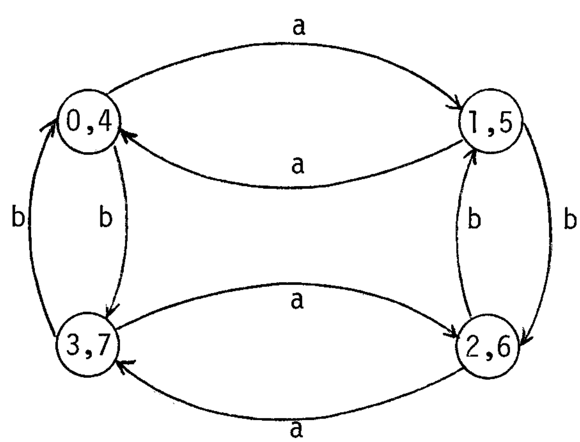

Fig. 1b

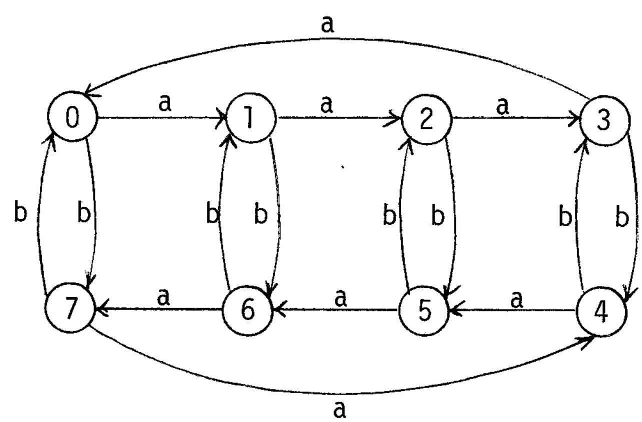

Fig. 2

4. COUNTING LANGUAGES AND SOLVABLE GROUPS

In the previous sections, we have considered factorizations of x in the form $x = x_0a_1x_1\ldots a_mx_m$ without taking the x_i's into account. Introducing the notion of counting in context, we are able to define a hierarchy of families of congruences, indexed by sequences of functions in F; this is essentially done by taking into consideration the intermediate segments $x_0,x_1,\ldots,x_m$ in the factorization above. The corresponding languages are called counting languages, and modulo languages will be seen to occur as the first nontrivial level of this hierarchy. The name counting languages is motivated by the fact that this family also corresponds to the closure of cyclic counters under the operation of cascade connection. The main result of this section asserts that L is a counting language iff M_L is a solvable group; the structure of M_L is also related to the hierarchy.

We say that $u = a_1\ldots a_m$ appears in context $X = (x_0,\ldots,x_m)$ in x iff $x = x_0a_1x_1\ldots a_mx_m$. For any equivalence relation $\sim$ on A^*, we can define a corresponding equivalence on contexts: we say that $V \sim V'$ iff $V = (v_0,\ldots v_m)$, $V' = (v_0',\ldots,v_m')$ and $v_i \sim v_i'$, $i = 0,\ldots,m$. The equivalence class containing V is denoted by $[V]_\sim$ and we can identify $[V]_\sim$ with $([v_0]_\sim,\ldots,[v_m]_\sim)$. We also define the following symbol

$$\binom{x}{u}_{[V]_\sim} = \begin{cases}\text{the number of factorizations of } x \text{ in the form}\\ x = x_0a_1x_1\ldots a_mx_m \text{ with } X \sim V\end{cases}$$

Observe that this notion is defined only in the case where V is a vector of length $|u| + 1$; in what follows, we always assume that the lengths of u and V are correctly related. Note the special case $u = \lambda$; λ always appears in context $X = (x)$ in x and $\binom{x}{\lambda}_{[V]_\sim}$ is 1 iff $x \sim v$, where $V = (v)$, and it is 0 otherwise. Finally it is clear that when $\sim$ is the universal congruence $\binom{x}{u}_{[V]_\sim} = \binom{x}{u}$. As usual we write $[V]$ for $[V]_\sim$ when it is understood which relation $\sim$ is intended. In an equation involving many $[V]_\sim$, we will usually specify the context only once and use the simplified notation for the others.

As an example of the notions introduced above, let $\sim$ be the congruence on $\{a,b\}^*$ defined by

$$x \sim y \text{ iff } |x| \equiv |y| \pmod 2.$$

Clearly any context V is equivalent to some $(v_0,\ldots,v_m)$ where $v_i = a$ or $v_i = \lambda$ for $i = 0,\ldots,m$. The reader may verify that, taking x = babaaa, we have $\binom{x}{a}_{(a,\lambda)} = 3$, $\binom{x}{a}_{(\lambda,a)} = 1$, $\binom{x}{ab}_{(a,\lambda,a)} = 1$.

Finally for any pair of contexts $V_1 = (v_{01},\ldots,v_{m1})$, $V_2 = (v_{02},\ldots v_{n2})$, we define their product V_1V_2 to be $V = (v_0,\ldots,v_{m+n})$ where $v_i = v_{i1}$, for $i = 0,\ldots,m-1$, $v_m = v_{m1}v_{02}$, and $v_j = v_{j-m2}$ for $j = m+1,\ldots,m+n$. When $\sim$ is a congruence, this multiplication of contexts can be extended to equivalence classes of contexts by defining $[V_1]_\sim[V_2]_\sim = [V_1V_2]_\sim$.

<u>Lemma 4.1</u>: Let $\sim$ be a congruence on A^*, V a context, u, x, $y \in A^*$, $a \in A$; then

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

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

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

Proof: Clear. □

Let $f \in \mathcal{F}$ and $\sim$ be a congruence on A^*. We define the following relation

$$x \sim_f y \text{ iff for all } u \text{ in } A^+ \text{ and for all contexts } V$$

$$\binom{x}{u}_{[V]_\sim} \equiv \binom{y}{u}_{[V]_\sim} \pmod{f(u)}.$$

If $\sim$ is the universal congruence, this notation is consistent with the notation of section 3.

<u>Lemma 4.2:</u> Let f, $\sim$ be as above;

a) $\sim_f$ is an equivalence;

b) if $\sim$ is of finite index, $\sim_f$ is of finite index;

c) if f is p$\wedge$s-closed, $\sim_f$ is a congruence.

Proof: a) and b) are easily verified. To prove c), we show that $x_1 \sim_f y_1$ and $x_2 \sim_f y_2$ implies $x_1x_2 \sim_f y_1y_2$. Indeed we have

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

$$\equiv \sum_{\substack{u=u_1u_2 \\ [V]=[V_1V_2]}} \binom{y_1}{u_1}_{[V_1]} \binom{y_2}{u_2}_{[V_2]} \pmod{f(u)}$$

$$\equiv \binom{y_1y_2}{u}_{[V]}$$

because $f(u) \mid f(u_1)$ and $f(u) \mid f(u_2)$. □

Let $F \in \mathcal{F}^*$ be a vector of functions which we denote by () if F is empty and by $(f_1,\ldots,f_n)$ otherwise; F is of length n iff $F \in \mathcal{F}^n$. If $F = (f_1,\ldots,f_n) \in \mathcal{F}^+$, we define $F' = (f_1,\ldots,f_{n-1})$. F is said to be p$\wedge$s-closed if f_i is p$\wedge$s-closed for $i = 1,\ldots,n$. For any congruence $\sim$ on A*, we construct by recursion the relation $\sim_F$;

$$x \sim_F y \text{ iff } \quad \text{i) } F = () \text{ and } x \sim y \text{ or}$$

$$\text{ii) } F = (f_1,\ldots,f_n),\ x \sim_{F'} y, \text{ and for all } u \in A^+, \text{ for all contexts } V$$

$$\binom{x}{u}_{[V]_{\sim_{F'}}} \equiv \binom{y}{u}_{[V]_{\sim_{F'}}} \quad (\text{mod } f_n(u)).$$

It is an easy matter to show inductively that if $\sim$ is of finite index then $\sim_F$ is of finite index, and that $\sim_F$ is a congruence when F is p$\wedge$s-closed. For the rest of this section, we investigate the languages corresponding to this new family of congruences when $\sim$ is the universal congruence. If we restrict ourselves to elements of $(\mathcal{F}_1)^*$, i.e. to vectors of functions of class at most 1, the construction of the congruence $\sim_F$ uses the same idea as the operation on languages that appeared in Straubing [78].

Let $\mathcal{C}_i = \{L\colon$ L is a $\sim_F$ language, $F \in \mathcal{F}^i\}$. It is clear that $\mathcal{C}_0 = \{\phi, A^*\}$ and that $\mathcal{C}_1$ is the family of modulo languages since we can identify $\sim_{(f)}$ and $\sim_f$. Moreover, the reader may verify that $x \sim_{(f_1,\ldots f_n)} y$ iff $x \sim_{(f_1,\ldots,f_n,1)} y$ and thus $\mathcal{C}_i \subsetneq \mathcal{C}_{i+1}$ for $i = 0,1,\ldots$. We denote by $\mathcal{C} = \bigcup_{i=0} \mathcal{C}_i$ and we call $\mathcal{C}$ the family of counting languages.

We extend the notation of the last section to the following cases: we use A_F for $A^*/\sim_F$ when F is p∧s-closed. We say that $G = (g_1,\ldots,g_r) \leq F = (f_1,\ldots,f_n)$ iff $r \leq n$ and there exists $1 \leq i_1 < \ldots < i_r \leq n$ such that $g_j \leq f_{i_j}$ for $j = 1,\ldots,r$: clearly we then have $x \sim_F y$ implies $x \sim_G y$. If $G \leq F$, we write $H_{G,F}$ (or H_G if F is understood) for the set $\{[x]_F\colon\ x \sim_G \lambda\}$.

We now proceed to give a characterization of counting languages in terms of their syntactic monoids.

<u>Lemma 4.3</u>: Let $F = (f_1,\ldots,f_n)$ and let $G = (g_1,\ldots,g_s)$ be the vector obtained from F by removing occurences of 1. Then $A_G \simeq A_F$.

Proof: Clear . □

<u>Lemma 4.4:</u> Let $F = (f_1,\ldots,f_n) \in \mathcal{F}$ be p∧s-closed; then A_F is a finite group.

Proof: By lemma 4.3, we may assume that $F \in (\mathcal{F}\setminus\{1\})^*$. A_F is a finite monoid since $\sim_F$ is a congruence of finite index. If $n = 0$, $A_{()} = \{1\}$ and the lemma holds. Otherwise let $q = \text{lcm}\,\{f_i(u)\colon\ u \in \text{supp}\ f_i,\ i = 1,\ldots,n\}$ and let $r = \sum_{j=1}^{n} m_j$, where f_j is of class m_j. We establish our result by proving $x^{q^r} \sim_F \lambda$ for all x in A^*. This happens as a consequence of the fact that

$$\binom{x^{q^i}}{u}_{[V]_{F'}} \equiv \binom{\lambda}{u}_{[V]_{F'}} \pmod q \text{ for all } i \geq |u| + \sum_{j=1}^{n-1} m_j\text{; this last}$$

statement is proved by induction on n.

<u>Basis</u> $n = 1$

This reduces to lemma 3.11.

<u>Induction step</u> $n > 1$

This we prove by induction on $|u|$.

<u>Basis</u> $|u| = 0$

$$\binom{x^{q^i}}{\lambda}_{[(v)]_{F'}} = 1 \text{ iff } x^{q^i} \sim_{F'} v;$$

but $x^{q^i} \sim_{F'} \lambda$ by the induction hypothesis; hence

$$\binom{x^{q^i}}{\lambda}_{[(v)]_{F'}} = 1 \text{ iff } \binom{\lambda}{\lambda}_{[(v)]_{F'}} = 1 \text{ and both values are 0 otherwise.}$$

<u>Induction step</u> $|u| > 0$

$$\binom{x^{q^i}}{u}_{[V]_{F'}} = \sum_{\substack{u=u_1\cdots u_q \\ [V=V_1 \ \cdots \ V_q]}} \binom{x^{q^{i-1}}}{u_1}_{[V_1]} \cdots \binom{x^{q^{i-1}}}{u_q}_{[V_q]};$$

by induction hypothesis, $\binom{x^{q^{i-1}}}{u_j}_{[V_j]} \equiv \binom{\lambda}{u_j}_{[V_j]}$ whenever $|u_j| < |u|$

since $i-1 \geq |u_j| + \sum_{k=1}^{n-1} m_k$. Also $\binom{x^{q^{i-1}}}{\lambda}_{[(v)]} = 1$ iff

$x^{q^{i-1}} \sim_{F'} v \sim_{F'} \lambda$ because of the induction hypothesis. Altogether

$$\binom{x^{q^i}}{u}_{[V]_{F'}} \equiv q \cdot \binom{x^{q^{i-1}}}{u}_{[V]_{F'}} \text{ and this is 0 (mod q); hence}$$

we have shown that $\binom{x^{q^i}}{u}_{[V]_{F'}} \equiv \binom{\lambda}{u}_{[V]_{F'}} \pmod q$. □

Corollary 4.1: Let $F = (f_1,\ldots f_n)$: if there exists a prime p such that $\text{im}(f_i) \subsetneq \{p^\alpha : \alpha \geq 0\}$ for $i = 1,\ldots,n$, then A_F is a p-group.

Proof: Clear. □

From now on, we assume that F and G are p∧s-closed elements of F^* and that $G \leq F$.

Lemma 4.5: $H_G \lhd A_F$.

Proof: By lemma 2.2b). □

Lemma 4.6: $A_F/H_G \simeq A_G$.

Proof: Following lemma 2.2b), the isomorphism is given by

$$\phi : A_F/H_G \to A_G$$
$$H_G[x]_F \mapsto [x]_G . \square$$

Lemma 4.7: Let $G \leq K \leq F$ be p∧s-closed. Then $H_{K,F} \lhd H_{G,F}$ and $H_{G,F}/H_{K,F} \simeq H_{G,K}$.

Proof: It follows from lemma 2.2c). □

Lemma 4.8: $H_{F',F}$ is nilpotent of class m if f_n is of class m.

Proof: By induction on m.

Basis m = 0, m = 1

Clearly, if m = 0, $\sim_{F'} = \sim_F$ and $H_{F',F} = \{1\}$.

For m = 1, we see that

$$\binom{xy}{a}_{[v]_{F'}} = \binom{x}{a}_{[(v_0,v_1y^{-1})]} + \binom{y}{a}_{[(x^{-1}v_0,v_1)]}$$

$$= \binom{x}{a}_{[(v_0,v_1)]} + \binom{y}{a}_{[(v_0,v_1)]}$$

$$= \binom{yx}{a}_{[v]}$$

since $y \sim_{F'} x \sim_{F'} \lambda$.

Induction step $m > 1$

Let $G = (f_1,\ldots,f_{n-1},g)$ where $g(u) = \mathrm{lcm}\,\{f_n(vuw): \ vw \neq \lambda\}$. G is p∧s-closed and $F' \leq G \leq F$; by lemma 4.6, $H_{F',F}/H_{G,F} \simeq H_{F',G,}$ which is nilpotent of class m-1 by induction hypothesis. By the usual technique, one can show that $H_{G,F} \subseteq Z(H_{F',F})$ and thus that $H_{F',F}$ is nilpotent of class m. □

Theorem 4.1: L is a counting language iff M_L is a solvable group.

Proof: If L is a counting language then by extending inductively the argument used in lemma 3.9, we can see that $M_L \prec A_F$ for some p∧s-closed F; furthermore, by lemma 4.3, we know that F can be chosen in $(\mathcal{F}\setminus\{1\})^*$. If $F = ()$ then $A_F = \{1\}$ is solvable. If $F = (f)$ then A_F is nilpotent hence solvable. Assume that the result holds for all F of length less than n and suppose that $F = (f_1,\ldots,f_n)$. By lemma 4.4 and lemma 4.5, $A_F \prec A_{F'} \circ H_{F'}$. $A_{F'}$ is solvable by induction hypothesis and $H_{F'}$ is nilpotent by lemma 4.7. This shows that A_F is covered by a solvable group since the extension of a solvable group by a nilpotent group is solvable. Hence A_F is solvable, and $M_L \prec A_F$ is solvable. Conversely let L be a language such that M_L is a solvable group. Let $H_0 = M_L \rhd H_1 \ \ldots \rhd H_n = \{1\}$ be the fitting series of M_L. If $n = 0$ then $M_L = \{1\}$ and L is a () language. If $n = 1$ then M_L is nilpotent and L is a $\sim_f$ language. Assume the theorem holds for group of fitting length less than n. Let $M_L \prec G_1 \circ G_2$ where G_1 is solvable of fitting length n-1 and G_2 is nilpotent. By induction hypothesis $G_1 \prec A_{F'}$ for some $F' = (f_1,\ldots f_{n-1})$ and $G_2 \prec (G_1 \times A)_f$. Let $F = (f_1,\ldots,f_{n-1},f)$ and suppose $x \sim_F y$; then $x \sim_{F'} y$ and $\delta_1(\lambda,x) = \delta_1(\lambda,y)$

since $G_1 \prec A_{F'}$. Also each factorization of x as $x = x_0 a_1 x_1 \ldots a_m x_m$ corresponds to a factorization of $\omega(x)$ as $\omega(x) = \omega_0 (g_1, a_1) \omega_1 \ldots (g_m, a_m) \omega_m$, $\omega_i \in (G_1 \times A)^*$ where $g_1 \sim_{F'} x_0$ and $g_i \sim_{F'} x_0 a_1 x_1 \ldots a_{i-1} x_{i-1}$ and similarly for y; since $\binom{x}{u}_{[V]_{F'}} \equiv \binom{y}{u}_{[V]_{F'}}$ (mod f(u)) it follows that $\binom{\omega(x)}{u'} \equiv \binom{\omega(y)}{u'}$ (mod f(u)) where $u' = (g_1, a_1) \ldots (g_m, a_m)$ and thus $\delta_2(\lambda, \omega(x)) = \delta_2(\lambda, \omega(y))$ since $G_2 \prec (G_1 \times A)_f$. Altogether, it implies that $M_L \prec A_F$ or that L is a $\sim_F$ language. □

<u>Corollary 4.2:</u> $L \in \mathcal{C}_n$ iff M_L is a solvable group of fitting length $\leq$ n.

Proof: Clear from the proof of the theorem. □

This last result shows a close connection between the operation of counting subwords in recursively-defined contexts and the operation of "dividing" a solvable group by a nilpotent subgroup; this extends the results of section 3 which said that counting subwords without context is closely related to nilpotent groups. Moreover if we count only words of length one in recursively-defined contexts, this corresponds to "dividing" G by an abelian subgroup just like counting subwords of length 1 was observed in section 3 to correspond to abelian groups. Let $\mathcal{D}_i = \{L$: L is a $\sim_F$ language for some F in $(\mathcal{F}_1)^i\}$; then $\mathcal{D}_0 \subseteq \mathcal{D}_1 \subseteq \ldots$; let $\mathcal{D} = \bigcup_{i \geq 0} \mathcal{D}_i$.

<u>Theorem 4.2:</u> $L \in \mathcal{D}_n$ iff M_L is a solvable group of derived length $\leq$ n.

Proof: Again we can restrict ourselves to $M_L = A_F$ otherwise $M_L \prec A_F$ and derived length cannot be increased by covering. If n = 0, $A_F = \{1\}$ and the theorem is true. If n > 0, $A_F \prec A_{F'} \circ H_{F'}$ where $A_{F'}$ is solvable of derived length $\leq$ n-1 by induction hypothesis and $H_{F'}$ is nilpotent of class 1, i.e. abelian by lemma 4.8. Hence if $L \in \mathcal{D}_n$ then M_L is a solvable group of length $\leq$ n. Conversely, if M_L is solvable of derived length $\leq$ n, then

$M_L \prec H_1 \circ \ldots \circ H_n$ where the H_i are abelian; the result is established by induction on n .

Basis $n = 0, n = 1$

If $n = 0$, $M_L = \{1\}$ and L is a $\sim_{()}$ language; if $n = 1$, then M_L is abelian and L is a $\sim_{(f)}$ language by lemma 3.17;

Induction step $n > 1$

Applying the induction hypothesis we know that $M_L \prec G_1 \circ G_2$ where $G_1 \prec A_{F'}$ for some $F' = (f_1, \ldots f_{n-1})$ and $G_2 \prec (G_1 \times A)_f$; the function $f\colon (G_1 \times A)^+ \to N^+$ can be transformed into a function $f'\colon A^+ \to N^+$ by putting $f'(a_1 \ldots a_m) = \text{lcm}\, \{f((g_1,a_1)\ldots(g_m,a_m))\colon\; g_i \in G_1\}$. Since f is of class 1, because G_2 is abelian, f' is of class 1 as well. Let $F = (f_1, \ldots f_{n-1}, f')$; an argument identical to the one used in the proof of theorem 4.1 establishes that $M_L \prec A_F$. □

This result appeared in a different form in Straubing [78]. He had also shown the equivalence of C with the family of languages recognized by cascade connection of cyclic counters. In our terminology, cascade connection of cyclic counters is an homomorphic image of A_F for some $F \in (F_1)^*$. The homomorphism corresponds to selecting sets $S_i = \{(a_{i1}, V_{i1}), \ldots, (a_{ir_i}, V_{ir_i})\}$ and integers $k_i \mid \gcd\{f_i(a_{ij})\colon\; j = 1,\ldots,r_i\}$ for $i = 1,\ldots,n$ and identifying inputs which agree on $\sum_{j=1}^{r_i} \binom{x}{a_{ij}}_{[V_{ij}]}$ (mod k_i). Moreover the k_i's can be chosen prime.

Clearly, a more general result is at hand; let $E_{ij} = \{L\colon$ L is a $\sim_F$ language for some $F \in (F_i)^j\}$ and let $E_i = \bigcup_{j \geq 0} E_{ij}$.

<u>Lemma 4.9:</u> If $L \in E_{ij}$ then M_L has a normal series of length j where each factor is nilpotent of class i.

Proof: Clear. □

Also, by an argument exactly similar to the one used in theorems 4.1 and 4.2, it is seen that if the conjecture stated in section 3 is true, then the converse of lemma 4.9 holds as well.

As an example consider the groups S_3 of all permutations of three objects. It has two different representations on two generators. The first one can be pictured as in Fig. 3; it can be checked to be isomorphic to the cascade connection of Fig. 4 with all the inputs not shown in the tail machine being identities. Thus for this representation, $S_3 \prec A_{(f_1,f_2)}$ where

$$f_1(u) = \begin{cases} 2 & \text{if } u = a \text{ or } u = b \\ 1 & \text{otherwise} \end{cases}$$

$$f_2(u) = \begin{cases} 3 & \text{if } u = b \\ 1 & \text{otherwise} \end{cases}$$

The other representation can be pictured as in Fig. 5; this one is isomorphic to the cascade connection of Fig. 6 again with the inputs not shown in the tail machine being identities. Thus for this representation, $S_3 \prec A_{(f_1,f_2)}$ where

$$f_1(u) = \begin{cases} 2 & \text{if } u = b \\ 1 & \text{otherwise} \end{cases}$$

$$f_2(u) = \begin{cases} 3 & \text{if } u = a \\ 1 & \text{otherwise} \end{cases}$$

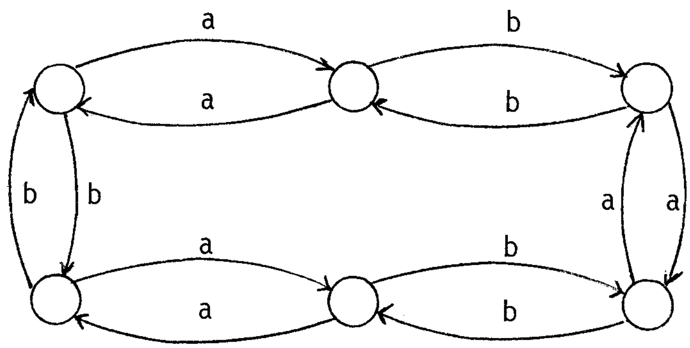

Fig. 3

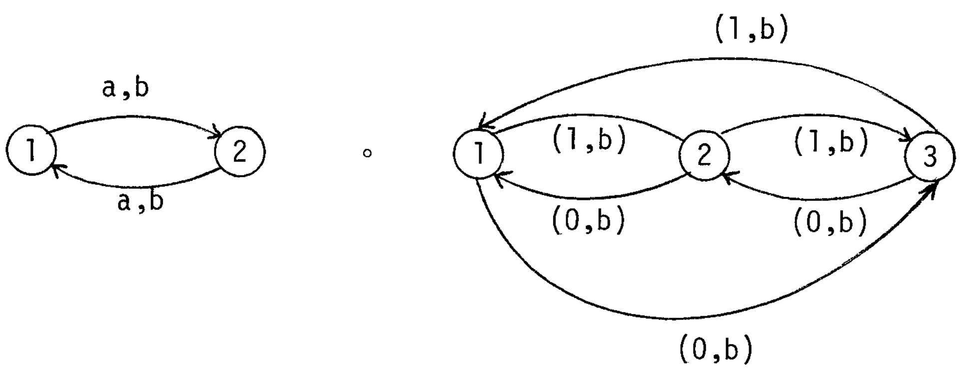

Fig. 4

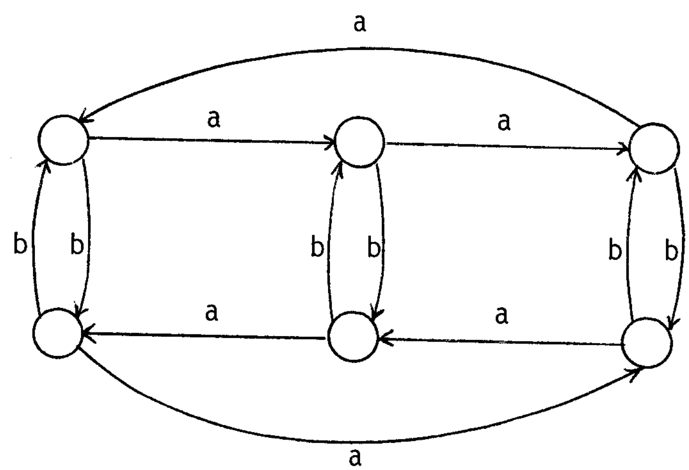

Fig. 5

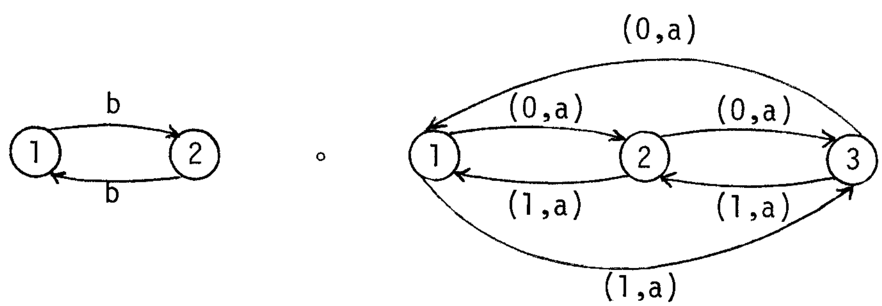

Fig. 6

BIBLIOGRAPHY

J.A. Brzozowski & I. Simon, Characterizations of locally testable events, Discrete Mathematics 4 (1973), 243-271.

J.A. Brzozowski & F.E. Fich, Languages of R-trivial monoids, Research Report CS-78-32, Department of Computer Science, University of Waterloo, Ont., Canada, 1978.

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

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

R. McNaughton, Algebraic decision procedures for local testability, Mathematical Systems Theory 8 (1974), 60-76.

M.P. Schützenberger, On finite monoids having only trivial subgroups, Information and Control 8 (1965), 190-194.

W.R. Scott, Group Theory, Prentice-Hall, 1964.

I. Simon, Piecewise testable events, in Lecture Notes in Computer Science 33, Springer-Verlag, New York, 1975.

H. Straubing, Families of regular sets corresponding to certain varieties of finite monoids, Research Report from the Department of Mathematics, University of California, Berkeley, California, 1978.

D. Thérien, Congruences for star-free languages, Research Report CS-78- , Department of Computer Science, University of Waterloo, Ont., Canada, 1978.