ON McNAUGHTON'S COUNTER FREE LANGUAGES

M. P. SCHUTZENBERGER*

LABORATORIO DI CIBERNETICA DEL C. N. R.

ARCO FELICE - NAPOLI

ON McNAUGHTON'S COUNTER FREE LANGUAGES

M. P. SCHUTZENBERGER*

Laboratorio di Cibernetica del C.N.R. - Arco Felice (Napoli)

* Permanent address: Université de Paris VII and
Institut de Recherche en Informatique et Automatique
Rocquencourt (France)

1. Introduction.

The family $\underline{A}_o$ of counter free language has been introduced long ago by Mc Naughton in connection with problems in Logic. It is the least family of subsets of the free monoid X^* that is closed under boolean operations and (set) product and that contains X^* and every subset of the alphabet X. In equivalent fashion it is the family of all subsets of X^* such that their syntactic monoid is finite and has no non trivial groups. Many further results can be found in the recent book of Mc Naughton and Pappert entitled "Counter free Automata". Some of the findings of these authors suggest generalizations and we propose here to examine one possible extension.

In what follows Π will be a fixed non empty set of positive integers that contains any divisor of its members and that is closed under the least common multiple (l.c.m.) operation. In equivalent manner Π can be defined by a partial function π into $\underset{\sim}{N}$ of the set of all primes. Then it contains every positive integer n such that for each prime p in the domain of π, the highest power of p dividing n is at most $p\pi$.

We shall denote by $\underline{M}_\Pi$ the family of all finite monoids such that the order of the cyclic group in them belongs to Π. Since any group of a quotient monoid is itself a quotient of a group in the original monoid, $\underline{M}_\Pi$ contains any quotient monoid of its member. Finally $\underline{A}_\Pi$ will denote the family of all sets

in X^* whose syntactic monoid is in $\underline{M}_\Pi$. One might may be call $\underline{A}_\Pi$ a "periodic family" (with "period set" Π) but it is probably premature to give a name to a notion whose interest remains to be demonstrated.

Let us consider some examples. If $\Pi = \{1\}$, (i.e. if $p\pi = 0$ for every prime p) we have simply Mc Naughton's family $\underline{A}_0$. At the other extreme, if Π contains every positive integers, (i.e. if the domain of the function π is empty), $\underline{A}_\Pi$ is simply Eilenberg's family $\underline{Rec}$ of all recognisable sets, i.e. of all sets whose syntactic monoid is finite. Families $\underline{M}_\Pi$ where Π is closed under multiplication have been the object of deep investigations by B. Tilson within the framework of J. Rhodes' complexity theory. However the notions we shall be using here are unable to characterise these especially interesting types of sets Π. Further, the families $\underline{M}_\Pi$ which we shall consider will fail in general to be closed under wreath product.

Anticipating upon Section 2, we give two other alternative definitions.

1.1. A recognizable set A belongs to $\underline{A}_\Pi$ iff in equivalent fashion :

(i) For any words $f,g,h \in X^*$ such that $A \cap fh^*g$ is infinite, one has $fh^p(h^r)^*g \subset A$ for somme $p \in \underset{\sim}{N}$ and $r \in \Pi$.

(ii) For any words $f,g,h \in X^*$ and positive integer t such that $f(h^t)^*g \subset A$, one has $fh^p(h^s)^*g \subset A$ for some $p \in \underset{\sim}{N}$ and divisor $s \in \Pi$ of t.

We return to our main argument. It is dear that each family $\underline{M}_\Pi$ is closed under direct product. Therefore $\underline{A}_\Pi$ is closed under boolean operations and since $\{1\} \in \Pi$ for any Π, it contains $\underline{A}_0$. Since for any recognisable set $A,B \subset X^*$ each group in $Synt(AB)$ is a subdirect product of groups in $Synt(A)$ and $Synt(B)$, we have also that each family $\underline{A}_\Pi$ is closed under product.

To proceed we need two more notions. First for each Π, we define the family $\underline{P}_\Pi$ of the submonoids P of X^* which satisfy the condition

$(\underline{P}_\Pi)$ $\quad h \in X^+$, $h^+ \cap P \neq \phi \Rightarrow h^r \in P$ for at least one $r \in \Pi$, where $X^+ = XX^* = X^*\backslash 1$, $h^+ = hh^* = h^*\backslash 1$ denotes the semigroups generated by X and by h.

This condition is vacuous iff Π contains every positive integer. When $\Pi = \{1\}$ one says at times in group theory that a subgroup which satisfies it is pure.

Second, along a different line, we recall that a subset A of X^* is a basis iff every word in X^* has at most one factorisation as a product of words from A. This requirement is satisfied when A is prefix, i.e. when $1 \notin A$ and $AX+ \cap A = \phi$.

With this terminology explained we can now state our "Main Property".

Main Property.

For each Π and any subset A of X^+ one has :

(1) $A \in \underline{A}_\Pi$, $A^* \in \underline{P}_\Pi \Rightarrow A^* \in \underline{A}_\Pi$

and, reciprocally,

(2) A , a basis, $A^* \in \underline{A}_\Pi \Rightarrow A^* \in \underline{P}_\Pi$.

Therefore, when $A \in \underline{A}_\Pi$ is prefix one has $A^* \in \underline{A}_\Pi$ iff $A^* \in \underline{P}_\Pi$. This will be verified in Section 3. In Section 4, we shall give for the sake of completeness a proof of a (weakened form of a) Theorem of Eilenberg which we state now in the manner most suitable for our present goal. Here $\underline{M}$ is an arbitrary family of finite monoids containing the quotient of its members and $\underline{A}$ is the corresponding family of sets in X^* whose syntactic monoid is in $\underline{M}$. We recall that a product AB $(A,B \in X^*)$ is unambiguous iff each word in X^* has at most one factorisation ab with $a \in A$, $b \in B$.

Theorem (Eilenberg) : Assume $\{1\} \in \underline{A}$ and that $\underline{A}$ is closed under boolean operations and product. Then $\underline{A}$ is equal to the least family $\underline{B}$ of subset of X^* that satisfies the two conditions :

(i) $\underline{B}$ contains every subset of X and it is closed under disjoint union and unambiguous product.

(ii) $\underline{B}$ contains every submonoid A^* such that $A \in \underline{B}$, A is prefix and $A^* \in \underline{A}$.

It is clear that any of our families $\underline{A}_{\pi}$ satisfies these conditions. Therefore, replacing in the theorem $\underline{A}$ by $\underline{A}_{\pi}$ and substituting in (ii), $A^* \in \underline{A}_{\pi}$ by $A^* \in \underline{P}_{\pi}$, which is allowed by the "Main Property", we get as a corollary an unambiguous expression of the members of $\underline{A}_{\pi}$.

The next section is devoted to recalling some known facts concerning cyclic groups in finite monoids and to a formal verification of 1.1 above. It will appear that some of the results do not depend upon the finiteness of Synt(A) or of its groups but only upon the finiteness of the orders of the one generators submonoids.

2. Alternative definitions.

In this section we consider a fixed recognisable set A in X^*. Its syntactic monoid will be denoted by S and we shall let $\alpha : X^* \to S$ be its syntactic morphism. We recall that for any $h,h' \in X^*$ one has $h\alpha = h\alpha'$ iff for each $f,g \in X^*$ the pair $\{fhg, fh'g\}$ is contained in A or in $X^* \setminus A$.

Therefore α is as well the syntactic morphism of $X^* \setminus A$ and all what will be said below could be dualised in this fashion. Since S is finite by hypothesis, the subsemigroup $(h\alpha)^+$ is finite for each $h \in X^*$. It contains a cyclic group H whose order will be written $\omega(h)$, or, when needed, $\omega(h,A)$.

For the same reason of finiteness, there is a number $p = p_A \in \underset{\sim}{N}$ such that $h^n\alpha$ is in its cyclic group for all $n \geq p$, irrespective of the element $h \in X^*$.

We now recall some known trivia. In what follows h is a fixed word in X^*.

2.1. For each pair $f,g \in X^*$, there is a divisor $s = \omega(h,f,g)$ of the order $\omega(h)$ such that for any $t \geq 1$ and $n \in \underset{\sim}{N}$, the relation $fh^n(h^t)^*g \subset A$ implies $fh^m(h^s)^*g$ where m is the least integer $\geq p_A$ which is congruent to n modulo $\omega(h)$.

Proof : For each positive multiple r' of $\omega(h) = r$ that is larger than p_A, $h^{r'}\alpha$ is the idempotent of the group H. Therefore for all $m \geq p_A$ one has $h^m\alpha = h^{m+r}\alpha$.

Let K be the subset of the elements $a \in H$ such that $f\alpha.a.g\alpha$ is in $A\alpha$. There is a largest subgroup G such that $KG = K$. Letting $s = (\text{Card } H)(\text{Card } G)^{-1}$ be the index of G in H, we see that s is a divisor of t and of $\omega(h)$ and the result follows. Q.E.D.

We have proved the statement (ii) in the alternative definition 1.1, since the hypothesis $A \in \underline{A}_\Pi$ is equivalent with $\omega(A) \in \Pi$ where $\omega(A)$ is the l.c.m. of the numbers $\omega(h)$, we have also proved (i). Indeed, we have shown that for each f,g,h the set of all $n \in \underset{\sim}{N}$ such that $fh^ng \in A$ is a union of a finite set and of arithmetic progressions of ratio $\omega(A)$. Because of

of the duality between A and $X^*\backslash A$ it is natural to set $\omega(h,f,g)$ when $fh^*g \cap A$ is finite.

2.2. The order $\omega(h)$ is the l.c.m. r of the numbers $\omega(h,f,g)$ overall pairs $f,g \in X^*$.

Proof : We have already seen that $\omega(h)$ is a multiple of every $\omega(h,f,g)$. It remains to check that is is exactly equal to r , i.e. that $h^m\alpha = h^{m+r}\alpha$ for all large enough m . However this is trivial because of the definition of α as the syntactic morphism of A since we have already $fh^ng \in A$ iff $fh^{n+s}g \in A$ for all large enough n , for each f,g and $s = \omega(h,f,g)$.

Q.E.D.

Another definition of $\underline{A}_{\pi}$ is suggested by Eilenberg's definition of $\underline{A}_o$.

2.3. Let A be a recognisable set. It belongs to $\underline{A}$ iff there is a $r \in \Pi$ such that for any $f,g,h \in X^*$ the set $f(h^r)^*g$ has a finite intersection with A or with $X^*\backslash A$. .

Proof : If $A \in \underline{A}_{\pi}$, we can take $r = \omega(A)$. Conversely if the condition is satisfied we have that $\omega(A) = r$ because $\omega(A)$ is the l.c.m. of the numbers $\omega(h,f,g)$ over all triples $f,g,h \in X^*$.

Q.E.D.

I submitt another similar definition. Let $\underline{\underline{S}}$ denote the family of all infinite sequences $\underline{S} = \{ s_n : n \in \underset{\sim}{N}\}$ of words $s_n \in X^*$ such that $s_n = 1$ for an infinity of $n \in \underset{\sim}{N}$.

For such a sequence let $\underline{S}^b$ denote the infinite sequence $\{t_n : n \in \underset{\sim}{N}\}$ where $t_o = s_o$. $t_{n+1} = t_n s_{n+1} t_n$ for all $n \in \underset{\sim}{N}$.

2.4. A recognisable set A belongs to $\underline{A}_\Pi$ iff there is a $r \in \Pi$ such that for any two words $f,g \in X^*$ and infinite sequence $\underline{S} \in \underline{\underline{S}}$, the set $M = \{n \in \underset{\sim}{N} : f(t_n)^r g \in A\}$ or its complement $\underset{\sim}{N} \backslash M$ is finite where $\{t_n\} = \underline{S}^b$.

Proof : Assume first $A \in \underline{A}_\Pi$. Consider an infinite sequence $\underline{S}$ and the associated sequence $\underline{S}^b$. The sequence of subsets $t_n\alpha . S . t_n\alpha = Q_n$ $(n \in \underset{\sim}{N})$ of the syntactic monoid $S = X^*\alpha$ satisfies identically $Q_{n+1} \subset Q_n$. Since S is finite, there is a set $Q \neq \phi$ such that $Q_n = Q$ for all large enough $n \in \underset{\sim}{N}$. Further any $t_n\alpha$ belongs to the minimal generating set Q' of the biideal Q . The hypothesis that $s_n = 1$ for an infinity of $n \in \underset{\sim}{N}$ implies that $t_{n+1} = t_n t_n$ for the same values of n . Therefore $Q'Q' \cap Q' \neq \phi$. By a standard argument from the theory of finite monoids, it shows that in fact Q' is a group in S . It now suffices to take $r = \omega(A) \in \Pi$.

Reciprocally, consider any set A and group G in Synt (A) . Take any $g \in G$. Since α is a surjective morphism we can choose an infinite sequence $\underline{S} \in \underline{\underline{S}}$ such that $s_{2n} = 1$, $s_{2n+1} = g^{-n'}$ where $n' = 1$ for $n = 0$ and $= 6n-5$ for n positive.

Instant computation shows that $t_{2n}\alpha = g^{2n+1}$; $t_{2n+1} = g^{4n+2}$. Therefore, $\{t_n\alpha : n \in \underset{\sim}{N}\}$ contains g itself infinitely often. Thus in order to satisfy the required condition over all triple of words we must take for r a multiple of $\omega(A)$.

Q.E.D.

Remark.

This could be applied to other questions. For instance, all the groups in the syntactic monoid of a recognisable set A are commutative iff for each infinite sequence $\underline{S} \in \underline{\underline{S}}$ there is a $m \in \underset{\sim}{N}$ such that for all $f,g \in X^*$, $n \geq m$ the set $\{ft_nt_{n+1}g\ ,\ ft_{n+1}t_ng\}$ is contained in A or in $X^*\backslash A$.

3. Verifying the "Main Property".

Let $A \subset X^*$ and $h \in X^*$ arbitrary. The set of all $n \in \underset{\sim}{N}$ such that $h^n \in A^*$ is a submonoid of the additive monoid $\underset{\sim}{N}$. As such it has a finite minimum generating set $M \subset \underset{\sim}{N}$ and we can denote it by M^* .

Further, letting d be the greatest common divisor of the numbers in M , one knows that $d\underset{\sim}{N}\backslash M^*$ is finite. Clearly, $h^* \cap A = \{1\}$ iff $M = \{d\} = \emptyset$.

3.1. Assume $A^* \in \underline{A}_{\Pi}$ and A a basis. Then A^* satisfies the condition :

$(\underline{P'}_{\Pi})$. $h \in X^*$, $s \geq 1$ $h^s \in A^* \Rightarrow h^r \in A^*$

for some factor $r \in \Pi$ of s .

Therefore $A^* \in \underline{P}_{\neg\Pi}$.

Proof : Assume $h^s \in A^*$ for some positive s . Conditions $(\underline{P'}_{\Pi})$ and $(\underline{P}_{\neg\Pi})$ are equivalent respectively with $M \subset \Pi$ and $M \cap \Pi \neq \phi$.

Because of $A^* \in \underline{A}_{\neg\Pi}$ we have $\omega(h,A^*) = p \in \Pi$, hence $h^n(h^p)^*\alpha \in A^*\alpha$ for some $n \in \underset{\sim}{N}$ where α is the syntactic morphism of A^* . Therefore $p \in d\underset{\sim}{N}$, hence $d \in \Pi$.

We recall the fact, which does not need being reproved once more, that iff A is a basis, one has the relation : $f \in X^*$, $fA^* \cap A^*f \cap A^* \neq \phi \Rightarrow f \in A^*$.

Suppose A a basis, $m,m' \in M$ and $m' = m+q$ $(q \in \underset{\sim}{N})$. We have $h^q h^m = h^m h^q = h^{m'} \in A^*$ where $h^m \in A^*$ hence $h^q \in A^*$. Since M is a minimal generating set it implies $q = 0$, i.e. that M is the singleton $\{d\} \in \Pi$. Q.E.D.

This establishes the second assertion in the "Main Property". Instead of checking the first one by the fastest method, we indulge into a longer discussion. In what follows, A,B,C are recognisable sets in X^+ , f,g and $h \neq 1$ are words in X^* . We use the notations introduced in Section 2, except that we indicate explicetely by notations such as $\omega(h,A)$ or $\omega(h,A,f,g)$ which syntactic monoid Synt (A) is involved. In particular p_A is the least number m such that the m-t^n power of any word has its syntactic image in a group in Synt (A) .

Also q denotes here a fixed positive integer.

3.2. Let $A = C^q$, $fh^ng \in A^*$, and assume that the length $|a'_i|$ of the longest word $a'_j \in A$ in some factorisation $fh^ng = a'_1a'_2 \dots a'_k$ $(a'_1,a'_2,\dots,a'_k \in A)$ satisfies

$$|a'_j| \geq q(|fg| + |h|p_C) .$$

Then $\omega(h,A^*,f,g)$ divides $\omega(h,C)$.

Proof : Because of $A = C^q$, the word fh^ng is a product of q^k words $c'_i \in C$ and because of our choice of $|a'_j|$, one of the factors c'_i of a'_j has at least $m = p_C$ factors in h, i.e., there are words $c = c'_j \in C$, $c_1,c_2 \in C^*$, $f',g' \in X^*$ such that $fh^ng = c_1cc_2 \in A^*$; $c = f'h^mg' \in C$; $c_1f' \in fh^*$; $g'c_2 \in h^*g$.

Therefore for any $t \in \underset{\sim}{N}$ we shall have $fh^{n+t}g = c_1f'h^{m+t}g'c_2$ and $fh^{n+t}g \in (C^p)^* \subset A^*$ where $f'h^{m+t}g' \in C$.

Because of our choice of $m = p_C$, this last relation is satisfied when t is a multiple of $\omega(h,C,f',g')$, hence when it is a multiple of $s = \omega(h,C)$. Therefore $fh^n(h^s)^*g \in c_1Cc_2 \subset A^*$, proving that $\omega(h,A^*,f,g)$ is a divisor of $\omega(h,C)$. Q.E.D.

3.3. Let $A^* \subset C^*$ where $C^* \in \underset{\sim}{P_{\pi}}$ and further, either $A = C^q$ or $c \in C^+$, $c^+ \cap A^* \neq \emptyset \Rightarrow c^q \in A^*$. Assume $fh^ng \in A^kA^*$ where $k \geq |fhg|$. Then $\omega(h,A^*,f,g)$ divides q^r for some $r \in \Pi$.

Proof : There is at least one factorisation $fh^n g = a_1 a a_2$, where the words $a_1, a, a_2 \in A^*$ are such that for some factorisation $h = h_1 h_2$ $(h_1, h_2 \in X^*)$ one has

$a_1 \in fh^* h_1$, $a_2 \in h_2 h^* g$ and $a \in h_2 h^* h_1 = (h_2 h_1)^+$.

Therefore for all $t \in \underset{\sim}{N}$

$$fh^{n+t} g = a_1 a (h_2 h_1)^t a_2 .$$

Because of $A^* \subset C^*$ and $C^* \in \underline{P}_\pi$; the relations $a \in A^*$, $a \in (h_2 h_1)^+$ imply $(h_2 h_1)^r = c \in C^*$ for some $r \in \Pi$. If $A = C^q$ we have instantly $c^q \in A^*$. If $A^* \subset C^*$, the same conclusion follows because of $a^+ \subset A^*$ and $a^+ \cap c^+ \neq \phi$. Therefore in both cases :

$$fh^n (h^{rq})^* g = a_1 a (c^q)^* a_2 \in A^* .$$ Q.E.D.

Let us derive some conclusions, letting Π' denote the least set containing every divisor of all numbers of the form rq with $r \in \Pi$.

3.4. Assume $A = C^q$ where $C \in \underline{A}_\pi$, $C^* \in \underline{P}_\pi$. Then $A^* \in \underline{A}_{\pi'}$.

Proof : Π' contains the least common multiple of any two of its member. Therefore, to prove $A^* \in \underline{A}_{\pi'}$, i.e. $\omega(h, A^*) \in \Pi'$ for all $h \in X^*$, it suffices to check that one has identically $\omega(h, A^*, f, g) \in A^*$.

In the situation of 3.2, this follows from $\Pi \subset \Pi'$ and the hypothesis $C \in \underline{A}_\pi$. If the hypothesis of 3.2 are not met, we are in the situation of 3.3 and the result is already stated.

Q.E.D.

Taking $q = 1$ in 3.4 gives the first assertion in the "Main Property".

3.5. Assume $A \subset B^q$, $A \in \underline{A}_\pi$ and $B^* \in \underline{P}_\pi$ where B is a basis. Then $A^* \in \underline{A}_{\pi'}$.

Proof : Taking $q = 1$ shows $\omega(h,A^*,f,g) \in \Pi'$ when in the situation of 3.3. Let us shown that we are in the situation of 3.4 (with $C = B$) when these hypothesis are not satisfied. Suppose indeed $b \in B^*$ and, say $b^r \in A^*$. We have $b = b'_1 b'_2 \ldots b'_k$ ($k \in \underset{\sim}{N}$) where all the words b'_i are in B . Therefore $b^r = b'_1 b'_2 \ldots b'_k b'_1 \ldots b'_k \ldots b'_k \in A^*$. Because of the hypothesis that B is a basis, this factorisation is unique.

Therefore $rk = qk'$ for some $k' \in \underset{\sim}{N}$ since $A \subset B^q$, and all the k' successive products of q consecutive words b_i are in A^* . Since b^q is itself a product of these last products, we have shown $b^q \in A^*$. Q.E.D.

The next remarks have no relevance to the present problem.

3.6. Assume $A \subset B$ whene B^* satisfies the condition $f \in X^*$, $B^* f B^* \cap B^* \neq \phi \Rightarrow f \in B^*$. Then for any $h \in X^*$, $\omega(h,A^*)$ divides the l.c.m. of $\omega(h,A)$ and $\omega(h,B^*)$.

Proof : Our condition on B^* implies in particular that $B^* f \cap B^* \neq \phi$ only if $f \in B^*$. Therefore B is prefix, hence

a basis. It follows that we can go directly to the case when $fh^ng = a_1aa_2$ and $a = (h_2h_1)^d \in (h_2h_1)^+$ in the notations and with the hypothesis of 3.3.

Let $s = \omega(h,B^*,f,g)$. We have $fh^nh^tg \in B^*$ iff $t \in s\underset{\sim}{N}$. Since $fh^nh^dg = a_1aaa_2 \in A^* \subset B^*$, it follows that $d \in s\underset{\sim}{N}$. Let $b = (h_2h_1)^s$. We have $fh^nh^sg = a_1aba_2 \in B^*$ where $a_1a,a_2 \in A^* \subset B^*$. Therefore $b \in B^*$ by our condition on B^* , implying as in 3.5 that $b \in A^*$, hence that $fh^n(h^s)^*g \in A^*$.

This shows that $\omega(h,A^*,f,g)$ divides $s = \omega(h,B^*,f,g)$. In fact both numbers are equal since $A^* \subset B^*$. Q.E.D.

3.7. Let the recognisable set A be such that $c \in X^+$, $c^+ \cap A^* \neq \emptyset \Rightarrow c \in A$. Then for all $h \in X^*$, $\omega(h,A^*)$ divides $\omega(h,A)$.

Proof : Take $q = 1$, hence $C = A$ in 3.2. Under the hypothesis of this statement we have that $\omega(h,A^*,f,g)$ divides $\omega(h,A)$. If they are not satisfied, take in 3.3, $C = X$; $q = 1$ and the second alternative in the hypothesis. Then we are in the same situation as in the present case. Since $X^* \in \underset{\sim}{A}_0$, we can take $\Pi = \{1\}$ and the conclusion gives $\omega(h,A^*,f,g) = 1$. Q.E.D.

In order to show some "raison d'être" to the last two assertions we verify the following final remark.

3.8. Let $\alpha : X^* \to S$ and $\beta : X^* \to T$ be two surjective morphisms onto finite monoids and assume that for each $h \in X^*$ the order $\omega(h,S)$ is a divisor of $\omega(h,T)$. Then every group G in S is a homomorphic image of a group in T.

Proof : Let $K = G\alpha^{-1}$. It is a subsemigroup of X^*. Since $K\beta$ is finite, there exists an idempotent u and a group H in T such that $u.K\beta.u = H$.

Let ρ denote the application from H into the subsets of G that sends every $b \in H$ onto $b\rho = (b\beta^{-1} \cap K)\alpha$. Since $K\alpha = G$ it is surjective and since β is a morphism one has identically $b\rho \neq \phi$ and $b\rho.b'\rho \subset (bb')\rho$ for any $b,b' \in H$. Take in particular b' to be the inverse of b in H. We have $\omega(h,T) = 1$, hence $\omega(h,S) = 1$ by hypothesis, for any $h \in (bb')\beta^{-1} \cap K$. Therefore $(bb')\rho$ is the idempotent of G, hence a singleton. Since $b\rho$ and $b\rho'$ are non empty subsets of G, it shows that each of them is a singleton, i.e. that ρ is a morphism from H to G. Q.E.D.

The example of the submonoid $\{x,xy,yx\}^*$ $(x,y \in X)$ of X^* which belongs to $\underline{A}_o$ shows that the condition of 3.7 does not imply that A^* be a free submonoid.

4. Verifying the Corollary.

We establish the theorem mentionned in the Introduction. What we give here is far from being optimal and we refer the reader to Eilenberg's theorem for deeper and more precise results. Let us recall a minimum of automatic machinery.

An automaton will be a triple $T = (Q, q_1, Q_+)$ where Q is a finite set, $q_1 \in Q$ is an initial state and $Q_+ \subset Q$ a terminal set. The set Q is provided with a morphism of X^* into the monoid of all partial applications of Q into itself. A modification of T will be another automaton $T' = (Q, q'_1, Q'_+)$ on the same set of states Q and it will be described in terms of T by indicating the initial and terminal elements q'_1 and Q'_+ and the value of the state qx for the pairs $(q,x) \in Q \times X$ such that qx is not the same in the morphisms of X^* into the monoids of action on states associated with T and with T'_o. The number of pairs $q, q' \in Q$ such that $q' \in qX$ will be denoted by $|T|$. We shall write $q^{-1}Q'$ $(q \in Q, Q' \subset Q)$ to denote the set $q^{-1}Q' = \{f \in X^* : qf \in Q'\}$. In particular, T recognises the set $q_1^{-1}Q_+$.

Any recognisable set A is recognised by at least one automaton. Among the automata who do this job there is a minimal one, say the syntactic automaton $T_A = (Q, q_1, Q_+)$ of A.

It has the following further properties :

(i) For any $q \in Q$, $Q' \subset Q$ the set $B = q^{-1}Q'$ satisfies $B\alpha^{-1}\alpha = B$ where α is the syntactic morphism of A.

(ii) $|T_A| \leq |T|$ for any other automaton T recognising A.

Let us now refer the reader to the families $\underline{A}$ and $\underline{B}$ described at the end of the Introduction. We make the observation that $X^* \in \underline{A}$ because $X^*\alpha^{-1}\alpha = X^*$ for any morphism α. Further, by hypothesis $\{1\} \in \underline{A}$, where $\underline{A}$ is closed under boolean operations. Therefore $X^+ = X^*\backslash\{1\} \in \underline{A}$ and $A \cap X^+ \in \underline{A}$ for any $A \in \underline{A}$. Also $\underline{A}$ is closed under product. Therefore $A,B \in \underline{A} \Rightarrow A\backslash BX^+ \in \underline{A}$.

We shall use repeatedly the fact that if $A \in \underline{A}$ and $B\alpha^{-1}\alpha \subset B$ (where α is the syntactic morphism of A), one has $B \in \underline{A}$. This immediately follows from the fact that by the very definition of Synt, $B\alpha^{-1}\alpha = B$ implies that Synt (B) is a quotient monoid of Synt (A) and from the hypothesis that $\underline{M}$ contains the quotient monoids of its members.

We are ready to prove that $\underline{B}$ contains any given member A of $\underline{A}$. This will be done by induction on $|T_A|$ where $T_A = (Q, q_1, Q_+)$ is the syntactic automaton of A.

First the initial case. Suppose $|T_A| = 0$. We have either $A = \emptyset$ or $A = \{1\}$. The empty set is a subset of X, therefore it is in $\underline{B}$ by the condition (i) stated in the Introduction. Also $\emptyset$ is a prefix set and since $\{\emptyset\}^* = \{1\} \in \underline{A}$

we have $\{1\} \in \underline{B}$ by condition (ii). We can henceforth assume $|T_A|$ positive.

Set $P = q_1^{-1}q_1$ and assume first $P \neq 1$. It belongs to $\underline{A}$ because $P = P\alpha\bar{\alpha}^{-1}$. Let Q' be the set of all states $q \in Q$ such that the set $X_q = q^{-1}q_1 \cap X$ is not empty. Modify the automaton T_A into a new automaton T' by letting $qX_q = \phi$ for every $q \in Q'$. If we take successively each $q \in Q'$ as a final state we obtain a set $B_q \subset X^*$ and the union of $B_q X_q$ over all $q \in Q'$ is a prefix set B such that $B^x = P$. Therefore by our induction hypothesis and $B_q\alpha^{-1}\alpha = B_q$, we have $P \in \underline{B}$.

Now we have the unambigous product $A = PA'$ where A' is the set accepted by T' when restoring Q_+ as the set of final states. Therefore to conclude the argument we have only to show $A' \in \underline{B}$. This is already done by the induction hypothesis unless $T' = T_A$, i.e. unless $P = \{1\}$, and also $A' \neq 1$. Take any state q_2 such that $q_1^{-1}q_2 = X' \neq \phi$ and modify $T' = T_A$ to T'' by letting $q_1X' = \phi$, keeping the same final set of states.

We have that A' is the disjoint union of $q_1^{-1}Q_+$ and of $X'q_2^{-1}Q_+$; Both sets are in B by the induction hypothesis.

Q.E.D.

References.

[1] R. Mc Naughton and S. Pappert, Counter free automata. MIT Press 1971.

[2] S.W. Golomb and B. Gordon (1965), Codes with Bounded synchronisation delay. Information and Control (8), pp; 355-372.

[3] S. Eilenberg, Forth coming book.

[4] Bret R. Tilson, p-length of p-solvable semigroups, in Semigroups, K.W. Folley Ed. Academic Press, 1969.