to appear in:
Actes du Seminaire D'Informatique
Theoretique. Universités Paris 6 et 7.
Ed. M. Fontet. I. Guessarian

pp 203-218
1981-82

About the Universality of the Ring $R<X^{(*)}>$.

GÜNTER HOTZ

Universität des Saarlandes

ABSTRACT : As we have shown in an earlier paper it is possible to imbed each finite dimensional algebra $\mathcal{A}_R$ over R with unit monomorph into the ring $R<X^{(*)}>$ where $X^{(*)}$ is the polycyclic monoid generated by X, cardX $\geq$ 2. Important for the theory of c.f. languages was the possibility to represent infinite dimensional algebras $\mathcal{A}_R(G)$ which reflect the derivation structure belonging to context-free grammars G by a homomorphism $\varphi : \mathcal{A}_R(G) \to R<X^{(*)}>$. From this fact one easily derives the well known important representation theorems of c.f. language theory. Here we continue in working out, that $R<X^{(*)}>$ is suitable to play a fundamental role not only in c.f. language theory but also in the general theory of computation. We especially show that sets of algebraic expressions defining elements of $R<X^{(*)}>$ or residual classes in $R<X^{(*)}>$ are hardest languages in the category of homorphic reductions for recursively enumerable sets, context sensitive languages and the intersection closure of c.f. languages.

This research partially was done while the author was visiting the "Institut de Programmation de Université Paris VI".

1. INTRODUCTION

Let R be a semi ring and X,Y,Z finite sets and X^* the free monoid generated by X. $\overline{X}$ is a set with $X \cap \overline{X} = \emptyset$ and $x \rightarrow \overline{x}$ defines a bijection between X and $\overline{X}$. The polycyclic monoid $X^{(*)}$ is the quotient of $(X \cup \overline{X})^*$ by the congruences generated by the relations

$$x \cdot \overline{x} = 1, \; x \cdot \overline{y} = o \text{ for } x,y \in X, \; x \neq y.$$

$R<X^*>$ and $R<X^{(*)}>$ are the free R-bimodules with base X^* resp. $X^{(*)}$. This means that the elements $f \in R<X^*>$ are finite sums

$$f = \sum_{u \in X^*} <f,u> \cdot u, \; <f,u> \in R.$$

For $v \in (X \cup \overline{X})^*$ $|v|$ is the length of v and red(v) the uniquely determined word which can be derived from v by deleting all pairs $x\overline{x}$ in v and which may appear in this process. If red(v) contains a pair $x\overline{y}$ with $x \neq y$, then we put red(v) = o.

In [Ho.1][Ho.2] it has been shown that there exist ring-monomorphisms from the ring of (nxn)-matrices over R into $R<X^{(*)}>$ if card$X \geq 2$. More general to each finite dimensional algebra $\mathcal{A}$ over R with unit there exists an injectiv representation $\psi : \mathcal{A} \rightarrow R<X^{(*)}>$.

In the same papers to each c.f. grammar G in chomsky normal (CNF) form there is assigned an algebra $\mathcal{A}_R(G)$ which we describe now.

Nearly without loss of generality one may assume for the grammar $G = (X,T,P,S)$, $X = X_1 \cap X_r$, $X_1 \cap X_r = \emptyset$, $P \subset X \times X_1 \cdot X_r \cup X \cdot T$.
The only restriction is, that always $1 \notin L(G)$. Each c.f. grammar G' in CNF can be transformed in a grammar G of this type, such that the following properties are invariant under this transformation

multiplicity of words relativ to G
LL(k) - property
LR(k) - property.

The multiplication in $\mathcal{A}_R(G)$ then is defined by the rule

$$x \cdot y = \sum \alpha^u_{x,y} \cdot u, \quad \alpha^u_{x,y} = \begin{cases} 1 & (u,xy) \in P \\ o & \text{else.} \end{cases}$$

$\mathcal{A}_R(G)$ is assoziativ and has a representation

$$\varphi : \mathcal{A}_R(G) \to R\langle B^{(*)}\rangle, \ \mathrm{card}B = 2,$$

which "preserves" the multiplicity of words.
This representation is formally similar to the representation $\tilde{\varphi} : R\langle X^*\rangle \to R\langle H(B)\rangle$ where $H(B)$ is the free half-group generated by B, which has been used by Nivat [Ni] in his proof of the theorem of Shamir [Sh]. But he needs in his proof the normal form theorem of Greibach [Gr.1]. In our case we derive from our representation φ the theorems of Shamir, Chomsky-Schützenberger and of Greibach directly. In this paper we continue in showing that $R\langle X^{(*)}\rangle$ is suited to play an universal role in language theory in general.

2. SYNTACTICAL CONGRUENCES AND THE REPRESENTATION

Let be $L \subset T^*$ and $u =_r v(L)$ resp. $u = v(L)$ the syntactical right resp. syntactical congruence modulo L defined as usually. These congruences transform itself in a natural way into right congruences resp. congruences of our algebra $\mathcal{A}_R(G)$. The quotient of $\mathcal{A}$ by the two sided congruence seems to be the syntactical algebra of Reutenauer. The classes $\mathfrak{A}_r$ resp. $\mathfrak{A}$ of this congruences which contain the o are right sided resp. two sided ideals. The word problem $p \in \mathfrak{A}_r$ can be decided by means of an easy modification of φ. It holds $\varphi^{-1}(o) \subset \mathfrak{A}$. But it is open if there exists a representation $\psi : \mathcal{A} \to R\langle X^{(*)}\rangle$ such that kernel $\psi = \mathfrak{A}$. This question is of practical interest, because such a homomorphism ψ would lead us to a simple procedure for error location in syntactically incorrect programs. One could hope, that one could find such a ψ by prolongating φ by an homomorphism $\sigma : R\langle X^{(*)}\rangle \to R\langle Y^{(*)}\rangle$ with suitable Y. This idea is the motivation for this section.

Theorem 1 : $\mathcal{A} = R\langle X^{(*)}\rangle$ is a simple algebra for card$X \geq 2$.

Proof : We have to show that from $\mathcal{A}\mathfrak{a}\mathcal{A} \subset \mathfrak{a}$ it follows that $\mathfrak{a} = o$ or $\mathfrak{a} = i\langle X^{(*)}\rangle$, where i is an ideal of R.

1) If $\alpha \in R$ and $\alpha\, \bar{u} \cdot v$ with $u, v \in X^*$ in $\mathfrak{a}$ then
$\alpha = u \cdot \alpha\, \bar{u}\, v \cdot \bar{v} \in \mathcal{A}\, \mathfrak{a}\, \mathcal{A} \subset \mathfrak{a}$.

2) From $p = \alpha\, \bar{u}\, v + q \in \mathfrak{a}$ it follows $p' = \alpha + q' \in \mathfrak{a}$,
where q' has not more monoms as q.

3) Let be $p = \alpha + \beta\, \bar{u}\, v + q \in \mathfrak{a}$.

a) If $u\, \bar{v} = o$ then $u\, p\, \bar{v} = \beta + q'$ where
$u\, p\, \bar{v}$ is shorter then q.

b) Let be $u \cdot \bar{v} \neq o$. We may assume $u\, \bar{v} = u' \in X^*$, $u' \neq 1$.
Then we form $u\, p\, \bar{v} = \alpha\, u' + \beta + u\, q\, \bar{v}$
and choose $y \in X$, $y \neq$ last u' and have
$u\, p\, \bar{v}\, \bar{y} = \beta\, \bar{y} + u\, q\, \bar{v}\, \bar{y}$
again $u\, p\, \bar{v}\, \bar{y}$ is shorter than p.

4) Thus we have shown that together with $p \neq o$ and $p \in \mathfrak{a}$
there exists $\alpha \in R$, $\alpha \neq o$ such that $\alpha \in \mathfrak{a}$.
Let be $i = R \cap \mathfrak{a}$, then $\mathfrak{a} = i\langle X^{(*)}\rangle$.
In the case that R is a field we have $\mathfrak{a} = \mathcal{A}$

This theorem shows that the idea to define $\psi = \sigma \circ \varphi$ does not work. But it could be, that there exist prolongations of φ by a σ defined on a sub algebra $\mathcal{A}' \subset R\langle X^{(*)}\rangle$. Therefore it is of interest to have conditions under which a mapping $\sigma' : E \to R\langle Y^{(*)}\rangle$ may be extended to a morphism on the sub algebra $\langle E\rangle$ of $R\langle X^{(*)}\rangle$ generated by E.

Let be E^+ the free semi-group generated by $E \subset R\langle X^{(*)}\rangle$, then there exists always an extension of σ' to a morphism $\sigma'' : R\langle E^+\rangle \longrightarrow R\langle Y^{(*)}\rangle$. Let

$$\mu : R\langle E^+\rangle \longrightarrow R\langle X^{(*)}\rangle$$

the canonical morphism and $\mathcal{E} = \mu\,(R\langle E^+\rangle)$.

One easily proves then

<u>Lemma 1 :</u> There exists an uniquely determined extension $\sigma : \mathcal{E} \rightarrow R\langle Y^{(*)}\rangle$ of σ' if $1 \notin \mathcal{E}$ and if $\mu^{-1}(o) \subset \sigma''^{-1}(o)$.

But generell there is no decidable condition that guarantees that σ' may be extended to a ring morphism. This follows from the subsequent lemmata.

<u>Lemma 2 :</u> Let be $E \subset X^* \times X^*$ and $\langle E\rangle$ the submonoid of $X^* \times X^*$ generated by E. There does not exist any procedure with parameter E to decide if the canonical monoid morphism $\mu : E^* \rightarrow \langle E\rangle$ is an isomorphism.

A proof of this theorem one can find in [Ho.Cl.].

<u>Lemma 3 :</u> There does exist a set Y and a monoid monomorphism $\mu : X^* \times X^* \rightarrow R\langle Y^{(*)}\rangle$.

<u>Proof :</u> Let be $y, z \notin X$ and $Y = X \cup \{y, z\}$.

We define

$$\mu'(x_1, x_2) = \bar{y}x_1y + \bar{z}x_2z \quad \text{for } x_1, x_2 \in X.$$

μ' defines uniquely the monoid morphism μ.
Obviously μ is injectiv.

From Lemma 2 and Lemma 3 it follows

<u>Theorem 2 :</u> For $E \subset R\langle X^{(*)}\rangle$ and $\mu' : E \rightarrow R\langle Y^{(*)}\rangle$ it is not generally decidable if there is an extension of μ' to a ring morphism $\mu : \langle E\rangle \rightarrow R\langle Y^{(*)}\rangle$.

3. RATIONAL SETS OVER $R<X^{(*)}>$.

Here we use the terminology introduced by Eilenberg [Ei]. The rational sets of an algebra are the sets generated from finite sets by application of the operations of the algebra, the union of sets and the algebraic closure operation. In the case of the free monoid the rational sets are identical with the sets accepted by finite automata. The reader not familiar with this theory be refered to [Ei] or [Be]. But the reader of [Be] should registrate, that $X^{(*)}$ there designates the free group generated by X. We use here F(X) for the free group generated by X. Benoit [Ben], [Be] has shown that the rational sets of F(X) transform by reduction of the words to short words in the rational sets over $(X \cup X^{-1})^*$. In [Ho.Es] it has been shown that the analog results for $X^{(*)}$.

Theorem 3 : $\mathrm{Rat}\ (X^{(*)}) := \mathrm{red}\ \mathrm{Rat}\ (X \cup \overline{X})^* \subset \mathrm{Rat}\ (X \cup \overline{X})^* \cup \{o\}$.

One could think that this theorem shows that the rational sets because of this result don't deserve no special interest. But if we are not only interested in the generated sets, but in the generating process too, then there is a essential difference between Rat (X^*), Rat F(X) and Rat $(X^{(*)})$. This difference concerns the starhight [Be], which in the case of X^* and F(X) may be any integer.

Theorem 4 : For the starhight $\sigma(L)$ of $L \in \mathrm{Rat}\ (X^{(*)})$ it holds $\sigma(L) \leq 1$.

Proof : Let be $L \in \mathrm{Rat}\ (X^*)$ and $G = (V,E)$ the state graph of a finite non-deterministic automaton, which accepts L. Let be $\alpha : E \to X^*$ the labelling of the edges of G by the input alphabet and $\mathfrak{Pth}(G)$ the category of paths of G. S is the initial and F the final state of the automaton. $\mathfrak{Pth}(S,F)$ is the set of paths from S to F. Then we have $L = \alpha(\mathfrak{Pth}(S,F))$.
Now we form $Y = V \cup E$ and $Y^{(*)}$.
We define

$$f = \{\overline{v}_1 s v_2 \mid s \in E,\ v_1 = \mathrm{source}\ (s),\ v_2 = \mathrm{sink}\ (s)\}.$$

Then we have $\mathfrak{M}\mathfrak{S}(S,F) = S <f> \overline{F}$, where $<f>$ is the submonoid of $Y^{(*)}$ generated by f. We put

$$g = \{\overline{v}_1\alpha(s)v_2 \mid \overline{v}_1 s v_2 \in f\}$$

and get

$$L = S <g> \overline{F}.$$

The expression $S <g> \overline{F}$ has only one star:"< >". Therefore $\sigma(L) \leq 1$.

By putting

$$\tilde{g} = \sum_{u \in g} u \in R<Y^{(*)}>$$

and assuming $\alpha(s) \neq 1$ for $s \in E$ we get with

$$1 + \tilde{g} + \tilde{g}^2 + \ldots$$

a formal power series for which we formally write $\frac{1}{1-\tilde{g}}$.

Then the series

$$S \frac{\tilde{g}}{1-\tilde{g}} \overline{F}$$

has L as support.
We extend our theorem 4 to

<u>Theorem 5 :</u> For each $L \in \mathrm{Rat}\,(R(X^{(*)}))$ we have $\sigma(L) \leq 1$.

<u>Proof :</u> We show that it is possible to move the star from the inner to the outside of rational expressions. We write in this proof A* for the subalgebra generated by A in $R<X^{(*)}>$.

Let be $y,z \in X^{(*)}$. Then we have

(1) $(y+z)(\bar{y}Ay \cup \bar{z}Bz)^*(\bar{y}+\bar{z}) = A^* \cup B^*$,

(2) $(y+z)(\bar{y}Ay+\bar{z}Bz)^*(\bar{y}+\bar{z}) = A^* + B^*$,

(3) $(\bar{y}Ay \cup \bar{z}Bz \cup \bar{y}z)^*y = A^* \cdot B^*$,

(4) $(A^*)^* = A^*$.

From (1), (2), (3) and (4) theorem 5 follows.

One can give to this theorem a program theoretic interpretation. Instead of

m_1 : do f_1; goto m_{i_1};

$\vdots$

m_k : do f_k; goto m_{i_k};

write

$$p = \sum_{i=1}^{k} \bar{m}_i \text{do } f;\ m_{i_1}.$$

Then $m_1 p^* m_2$ gives all possible computation paths from m_1 to m_2 of the program p.
We will not go in details, but one easily sees, that our theorem 5 can be interpreted in the following way: Procedures do not increase the computing power of the programming language, because each computation may be reduced to the iteration of one single program.
Let be $E \subset R\langle X^{(*)}\rangle$ and $\langle E\rangle$ the <u>submonoid</u> generated by E in $R\langle X^{(*)}\rangle$. The rational sets of $R\langle X^{(*)}\rangle$ relative to the multiplikation be $\dot{R}at\ (R\langle X^{(*)}\rangle$.

<u>Theorem 6 :</u> The word problem $u \in L$ for $L \in \text{Rat } R\langle X^{(*)}\rangle$ is not decidable for $\text{card}X \geq 2$.

<u>Proof :</u> To proof this theorem we reduce the modified correspondence problem of Post (MPCP) on the word problem considered in

our theorem. Let be Q a finite set and

$$a,b : Q^* \longrightarrow T^*$$

be monoid homomorphisms. The theorem of Post states :
It is not decidable if there exists a $q \in Q^*$ such that $a(q) = b(q)$.
This result holds in the following modified version of the PCP too : Does there exist a $q = q' \cdot q_1$, $q' \in Q^*$ and $q_1 \in Q$ such that $a(q) = b(q)$ (q_1 fixed for all cases).
Let x,y,z be new symbols not contained in $Q \cup T$ and $Q \cap T = \emptyset$. We define

$$u(q) = \overline{y}a(q)y + q, \quad v(q) = \overline{z}\overline{b(q)}z + q \qquad \text{for } q \in Q$$

and

$$u_o = \overline{y}a(q_1)x + 1, \quad v_o = \overline{x}\overline{b(q_1)}z + 1.$$

We put $X = T \cup Q \cup \{x,y,z\}$ and extend u to a monoid homomorphism $u : Q^* \longrightarrow R\langle X^{(*)}\rangle$ and v to an anti homomorphism $v : Q^* \longrightarrow R\langle X^{(*)}\rangle$.
Then from the existence of $q \in Q^*$ such that $a(q \cdot q_1) = b(q \cdot q_1)$ it follows

$$u(q) \cdot u_o \cdot v_o \cdot v(q) = \overline{y}z + 1.$$

Conversely if we have

$$\overline{y}z + 1 \in \langle \{u(q), v(q), u_o, v_o \mid q \in Q\} \rangle$$

then a and b have a solution of the MPCP.

<u>Open problem :</u> Is the word problem $w \in L$ for $L \in \mathrm{Rat}\, R\langle X^{(*)}\rangle$ decidable? Our construction for the proof of theorem 6 leads to the following modification of the PCP.
Do there exist $q,q' \in Q^*$, $|q| = |q'|$ such that $a(q) = a(q')$. In [Gr.2] this problem has shown to be decidable.

4. THREE HARDEST LANGUAGES UNDER HOMOMORPHIC REDUCTION

We are going to construct hardest languages in the category of homomorphic reductions.
We start with a TM with an input tape and a working tape. The actual working space is between two end markers \$ and #. The inscription of the working tape \$ v # we represent by two words $\bar{\$}\ v_1\ \$$ and $\bar{\#}\ v_2\ \bar{\#}$ with $v = v_1 \cdot \text{reversal}(v_2)$. We assume the head of the working tape on the position of the last element of $\$v_1$. This means we simulate our TM by a two-tape pda.
This model we simulate by the following one: Let be G = (V,E) a graph

$$\alpha : E \to T^*,\ \gamma : E \to R\langle X^{(*)}\rangle$$

two labellings of the edges of G. T is the input alphabet, X the working alphabet. A vertex $S \in V$ is the starting state, a vertex $F \in V$ the final state. A computation is a path $w \in \mathcal{M}(S,V_1)$.
The start konfiguration is \$ + #. If $w \in \mathcal{M}(F,V_1)$ then the configuration after the computation w is $(\$ + \#)\gamma(w)$. The input beeing read after the computation w is $\alpha(w)$. $u \in T^*$ will be accepted by our machine, if there is a computation $w \in \mathcal{M}(S,F)$ such that

$$\alpha(w) = u,\ (\bar{\$}\$ + \bar{\#}\#)\cdot\gamma(w) = \bar{\$}\$ + \bar{\#}\#$$

This means we accept words only after a computation with empty working tape. We now explain how this model simulates the two tape pda. We do this only for two characteristic cases.

We assume our machine to be in state V_1, it reads t on the input tape. The inscription is $v_1x\$ + v_2y\#$. The machine writes z on the place of x and moves to the right. V_2 is the new state. This action we represent by the edge $V_1 \overset{s}{\text{---}} V_2$ with
$V_1 \xrightarrow{s} V_2$ with

$$\alpha(s) = t \quad \text{and} \quad \gamma(s) = \bar{\$}\bar{x}zy\$ + \bar{\#}\bar{y}\#.$$

We see if w was the path from S to V_1 with
$(\bar{\$}\$ + \bar{\#}\#)\gamma(w) = v_1 x\$ + v_2 y\#$ and $\alpha(w) = u'$, then we have after the computation ws

$$(\bar{\$}\$ + \bar{\#}\#)\gamma(ws) = v_1 zy\$ + v_2\#, \quad \alpha(ws) = u'\cdot t.$$

This action did not increase the working space on the tape. We look at a second example, where the working space increases and the mashine does not read a new input symbol.

Then α and γ could be defined as follows:

$$\alpha(s) = 1, \quad \gamma(s) = \bar{\$}\bar{x}xz\$ + \bar{\#}\#.$$

This action puts depending from the state and the top element x of the \$-tape a new symbol z on the top of the stack.

This examples are sufficient to understand our computational model.
Now we respresent G by the sum

$$\sum_{s \in E} \bar{V}_1 \, s \, V_2$$

and we put

$$f_\varepsilon = \sum_{\substack{s \in E \\ \alpha(s)=1}} \bar{V}_1 \, s \, V_2, \quad \gamma(V_1) = V_1 \quad \text{for } V_1 \in V.$$

f_E represents the single ε-moves of the TM on the input tape. The sequences of all ε-computations will be represented by $\frac{1}{1-f_\varepsilon}$.
We put

$$r_t = \frac{1}{1-f_\varepsilon} \left(\sum_{\substack{\alpha(s)=t \\ V_1 \xrightarrow{s} V_2}} \bar{V}_1 \gamma(s) \, V_2 \right) \cdot \frac{1}{1-f_\varepsilon}$$

r_t is a rational set. According to theorem 4 we find a polynomial g_t such that

$$r_t = \frac{1}{1-g_t} .$$

Now let $R\langle\langle R^{(*)}\rangle\rangle_{rat}$ the ring of the rational power series over R. We define the monoid homomorphism $\varphi : T^* \rightarrow R\langle\langle X^{(*)}\rangle\rangle_{rat}$

$$\varphi(t) = \frac{1}{1-g_t} \quad \text{for } t \in T.$$

Then we have the

<u>Theorem 7 :</u> For each rec.en. set $L \subset T^*$ one can construct a monoid homomorphism $\varphi : T^* \rightarrow R\langle\langle X^{(*)}\rangle\rangle_{rat}$ such that

$$u \in L \iff (\bar{S}S + \bar{\#}\#)\, S\, \varphi(u)\bar{F} = \bar{S}S + \bar{\#}\#$$

holds.

If we would take a non-deterministic TM instead of the deterministic one we used, then we would get with the same construction

<u>Theorem 8 :</u> For each rec.en. set $L \subset T^*$ one can construct a monoid homomorphism $\varphi : T^* \rightarrow R\langle\langle X^{(*)}\rangle\rangle$ such that

$$u \in L \iff (\bar{\$}\$ + \bar{\#}\#) S\varphi(u)\bar{F} = \bar{\$}\$ + \bar{\#}\# + R\langle\langle X^{(*)}\rangle\rangle_{rat}$$

If we restrict our machine in such a way that ε- moves do not increase the tape space, then the accepted sets are deterministic context sensitiv (dcs) languages resp. context sensitiv (cs) languages.

The two last theorems and these remarks lead to the construction of hardest languages. The construction is analogous to the construction of the hardest c.f. language of Greibach from the representation theorem of Shamir.

We define for $q_o = \bar{S}S + \bar{\#}\#$

$$\tilde{L}_{r.e.} = \{|\frac{1}{1-f_1}|\frac{1}{1-f_2}|\ldots| \;\Big|\; q_oS\,\frac{1}{1-f_1}\cdot\frac{1}{1-f_2}\cdot\;\ldots\;\cdot\frac{1}{1-f_n}\,\bar{F} = q_o$$
$$\text{for } f_i \in R<X^{(*)}>,\ n \in \mathbb{N}\}.$$

In this definition

$$|\frac{1}{1-f_1}|\frac{1}{1-f_2}|\ldots|\frac{1}{1-f_n}|$$

is an expression. By a suitable coding

$$c : R<X^{(*)}> \rightarrow R<B^{(*)}>,\ B = \{x,y\}$$

applying some standard tricks we get a language $L_{r,e} \subset B^*$ and for L a homomorphism $h : T^* \rightarrow B^*$ such that $L = h^{-1}(L_{r.e})$.

Thus we have

Theorem 9 : To each recursivelly enumerable set $L \subset T^*$ there exists a monoid homomorphism h such that $L = h^{-1}(L_{r.e})$.

We define

$$\tilde{L}_{d.c.s.} = \{w \in L_{r.e} \mid f_i \text{ increases the tape space by } 1\}.$$

From the non-deterministic version of the TM we derive in a similar way a set $L_{c.s.}$. By standard coding tricks we get hardest context sensitiv resp. deterministic context sensitiv languages $L_{c.s.}$ resp. $L_{d.c.s.}$.

Theorem 10 : To each c.s. (d.c.s.) language L there exists a homomorphism $h : T^* \rightarrow B^*$ such that $L = h^{-1}(L_{c.s.})$ $(L = h^{-1}$ $(L = h^{-1}(L_{d.c.s.}))$.

Complete proofs are in [Fis].

We define now another hardest language.

Let be $q_o \in R<X^{(*)}>$, $R = \mathbb{N}$ and

$$\tilde{H}_{BNP}(q_o)=\{|p_1|p_2|\dots p_n| \mid p_i \in R\langle X^{(*)}\rangle,\ p_1\cdot p_2\cdots p_n \in q_o+R\langle X^{(*)}\rangle\}.$$

For each $q_o \in R\langle X^{(*)}\rangle$ the set $H_{BNP}(q_o)$ is a language which can be represented by the intersection of c.f. languages. If k is the number of different monomes in q_o, then $H_{BNP}(q_o)$ is the intersection of k c.f. languages. If we use the theorem of Book - Nivat - Paterson [B.N.P], which states the fact, that each such language can be represented as the intersection of only three c.f. languages, then we are able to prove the following theorem easily.

Theorem 11 : There exists a polynom $q \in \mathbb{N}\langle B^{(*)}\rangle$ and to each language $L \subset T^*$ out of the intersection closure of c.f. there exists a monoid homomorphism $h : T^* \rightarrow \mathbb{N}\langle B^{(*)}\rangle$ such that $L = h^{-1}(q + \mathbb{N}\langle B^{(*)}\rangle)$.

The idea of the proof: Let be h_1, h_2, h_3 representations of L_1, L_2 resp. L_3 as in the theorem of Shamir. Then one forms a sum

$$h = \bar{x}_1 h_1 x_1 + \bar{x}_2 h_2 x_2 + \bar{x}_3 h_3 x_3$$

with suitable $x_1, x_2, x_3 \in B^*$. h leads us to representation of theorem 11.

Now if we code $\tilde{H}_{BNP}(q)$ in $(B \cup \bar{B} \cup \{+,|\})^*$ with standard tricks then we get a language $H_{BNP}(q)$ for which we can proof the

Corollary to theorem 11 : $H_{BNP}(q)$ is a hardest language under homomorphic reduction in the intersection closure of c.f. languages.

Detailed proofs the reader may find in the Dipl. Thesis [Fis].

Acknowledgement : The author wishes to thank J. Berstel, J. Sakarovitch and C. Reutenauer for valuable discussions. U. Fissgus I thank for critical reading of this paper.

Literatur :

[Be] J. Berstel: "Transductions and Context-Free Languages". Teubner Studienbücher, Stuttgart (1979).

[Ben] M. Benois: Parties rationelles du groupe libre. C. R. Acad Sci. Paris, Sér. A 269 (1969).

[BNP] R. Book, M. Nivat, M. Paterson: "Reversal-Bounded Acceptors and Intersections of Linear Languages". SIAM J. Com. Vol. 3 (1974).

[Ei] S. Eilenberg: "Automata, Languages and Machines". New York - San Francisco - London (1974).

[Fis] U. Fissgus: "Darstellungssätze für Ch-O und Ch-1 Sprachen" Diplomarbeit an der Universität des Saarlandes.

[Gr 1] S. Greibach: "The Hardest Context-Free Language". SIAM J. of Computing 2 (1973).

[Gr 2] S. Greibach: "A Remark on Code Sets and Context-Free Languages". IEEE Trans. Comput. C-24 (1975).

[Ho 1] G. Hotz: "Ein Darstellungssatz über unendliche dimensional Algebren und Anwendungen in der Theorie der Formalen Sprachen". Tech. Bericht der Angewandten Mathematik und Informatik. Universität des Saarlandes (1982).

[Ho 2] G. Hotz: "A representation theorem for infinite dimensiona associativ algebras and applications in Formal language theory". Actes de l'école de printemps de theorie des langages. Ed. Maurice BLAB LITP 82-14.

[Ho-Cl] G. Hotz, V. Claus: "Automatentheorie und formale Sprachen" III. Mannheim - Wien - Zürich (1972) B.I. Hochschultaschen bücher.

[Ho-E] G. Hotz, K. Estenfeld: "Formale Sprachen, eine automatentheoretische Einführung". Mannheim - Wien - Zürich (1981) Bi-Reihe Informatik.

[Ni] M. Nivat: "Transductions des Languages des Chomsky". Ann. de l'Inst. Fourier 18 (1968).

[Pe] J.-F. Perrot: "Contribution à l'étude des monoides syntactiques et de certains groupes associés aux automates finis". Thèse Sc. Math., Univ. Paris VI (1972).

[Re] C. Reutenauer: "Series rationelles et algèbres syntactique Thèse de Doctorat d'Etat à l'Université de Paris VI (1980)

[Sal] A. Salomaa, M. Soittola: "Automata-Theoretic Aspects of Formal Power Series". Berlin - Heidelberg - New York (1978)