INFORMATIQUE THÉORIQUE ET APPLICATIONS

I. LITOVSKY

Minimal generators of submonoids of A^∞

Informatique théorique et applications, tome 25, nº 1 (1991), p. 3-17
<http://www.numdam.org/item?id=ITA_1991__25_1_3_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 25, n° 1, 1991, p. 3 à 17)

MINIMAL GENERATORS OF SUBMONOIDS OF A^∞ (*)

by I. LITOVSKY [1]

Communicated by J. BERSTEL

Abstract. – *In the monoid A^∞ (unlike the monoid A^*) some submonoids do not have minimal generators with respect to inclusion; here we characterize these submonoids. Next we give algorithms to decide, in the rational case, whether a submonoid has either one smallest generator or minimal generators of finite generators. Finally we prove that every rational submonoid of A^∞ may be obtained from the single submonoid $x^*+(x^*y)^\omega$ through a composition of non-erasing morphisms and non-erasing inverse morphisms.*

Résumé. – *Dans le monoïde A^∞ (à la différence du monoïde A^*) certains sous-monoïdes n'ont pas de générateurs minimaux par rapport à l'inclusion; nous caractérisons ici ces sous-monoïdes. Puis dans le cas rationnel nous proposons des algorithmes pour décider si un sous-monoïde a soit un plus petit générateur, soit des générateurs minimaux, soit des générateurs finis. Pour finir nous montrons que le seul sous-monoïde $x^*+(x^*y)^\omega$ permet d'obtenir tout sous-monoïde rationnel de A^∞ par composition de morphismes et morphismes inverses non effaçants.*

INTRODUCTION

Given an alphabet A, the free monoid A^* is the set of all finite words over A with concatenation. Let M be a submonoid of A^* (*i.e.* a subset of A^* containing the empty word and closed under the concatenation), a subset G is called a generator of M if and only if $G^*=M$. It is well-known that Root (M) (*i.e.* the set of words non-factorizable by using two nonempty words of M) is the smallest generator of M [*i.e.* each generator of M contains Root (M)].

When we deal furthermore with infinite words, we consider the set, denoted by A^∞, of all finite or infinite words over A. A^∞ endowed with a natural extension of the concatenation is a monoid and then A^* is a submonoid of

---

(*) Received May 1989, final version in August 1989.

(1) C.N.R.S. U.R.A. 1304, Université de Bordeaux-I, L.A.B.R.I., 351, cours de la Libération, 33405 Talence Cedex, France.

A^∞. However the property, $vu=u$ implies v is the empty word, holds in A^* but not in A^∞. We shall see here a few consequences concerning the generators of submonoids of A^∞.

Given M a submonoid of A^∞, the aim of this paper is to look for the "little" generators of M with respect to inclusion. In [3] it is proved that some submonoids do not have a smallest generator and two characterizations are given, one of "Root (M) is the smallest generator" and the other "M has one smallet generator [possibly not Root (M)]". In view of these results, it has seemed interesting to study more generally the minimal generators of M. First we note that some submonoids do not have minimal generators. Next by defining three kinds of "minimal" elements for the following transitive relation over M "u is factorizable in M by v", we find again both previous characterizations and we obtain a third one for "M has minimal generators".

Then we prove that for the rational case, these three above characterizations are effective, that is to say, assuming that M is a rational submonoid, one can decide whether any one of them is satisfied. That allows us to decide whether M has a finite set as generator.

In a last part we try to generate the rational submonoids no longer with the $*$-operation, but through morphisms and inverse morphisms from the simplest possible submonoid. We start from a result of [5] which states that, for any alphabet A, every rational submonoid of A^* may be obtained, from the single submonoid x^* through a composition of two non-erasing morphisms and one inverse non-erasing morphism. In a same way as in [5, 6], we state that every rational submonoid of A^∞ may be obtained through the single submonoid $(x^*+(x^*y)^\omega)$.

I. PRELIMINARIES

Let A be an alphabet, A^* is the set of all (finite) words over A, the empty word is denoted by ε, $A^*-\{\varepsilon\}$ is denoted by A^+ (we use $-$ to denote the difference between two subsets), $|u|$ denotes the length of the word u. A^* with concatenation is a monoid.

A^ω is the set of all infinite words over A (*i.e.* sequences with value in A), and A^∞ denotes A^*+A^ω. Any infinite word is called an $\omega-$word and any subset of A^∞ is called a language. Let M be a language of A^∞, $M\cap A^*$ is denoted by M_{fin} and $M\cap A^\omega$ is denoted by M_{inf}.

The concatenation over A^* is extended over A^∞ by:

$$\forall w \in A^\omega, \qquad \forall \alpha \in A^\infty : w\alpha = w.$$

$\forall u \in A^*$, $\forall w \in A^\omega$: uw is such that

$$(uw)(n) = u(n), \qquad \forall n \leqq |u|$$
$$(uw)(n) = w(n - |u|), \qquad \forall n > |u|.$$

So A^∞ is a monoid. As usual the concatenation is extended to the languages, and for any language L:

$$L^0 = \{\varepsilon\}$$
$$\forall n \geqq 1, \qquad L^n = \mathrm{L}.\mathrm{L}^{n-1}$$
$$L^* = \bigcup_{n \geqq 0} L^n = (L_{\mathrm{fin}})^* \cup (L_{\mathrm{fin}})^* L_{\mathrm{inf}}.$$

Let u be a word in A^+, the ω-word $u \ldots u \ldots$ is denoted by u^ω and is said to be periodic. Let L be a language in A^+, as in [2], L^Ω denotes the following w-language $\{u^\omega / u \in L\}$. An ω-word w is ultimately periodic if and only if $w = uv^\omega$ for some u in A^* and v in A^+, then v is called a period of w, and v^ω a periodic right-factor of w. A language L is ultimately periodic if and only if every ω-word of L is ultimately periodic.

A language M is a submonoid of A^* if and only if $M^* = M$. Moreover for any language L, L^* is the smallest submonoid containing L. Clearly M is a submonoid of A^∞ if and only if $M_{\mathrm{fin}} = M^*_{\mathrm{fin}}$ and $M_{\mathrm{inf}} = M_{\mathrm{inf}} M_{\mathrm{inf}}$. Let M be a submonoid of A^∞, G is called a generator of M whenever $G^* = M$. Clearly G is a generator of M if and only if $G^*_{\mathrm{fin}} = M_{\mathrm{inf}}$ and $G^*_{\mathrm{fin}} G_{\mathrm{inf}} = M_{\mathrm{inf}}$. The family of all generators of M is denoted by Gen(M).

In the following we study the minimal languages of this family with respect to the inclusion. Let us recall, in the particular case of the family Gen(M), the basic following definitions. Let M be submonoid of A^∞, L is the smallest generator of M if and only if $L \in$ Gen(M) and for each $G \in$ Gen(M), $L \subset G$. G is a minimal generator of M if and only if $G \in Gen(M)$ and for each $G' \in$ Gen(M), $G' \subset G$ implies $G = G'$.

The language $(M - \varepsilon) - (M - \varepsilon)^2$ is denoted by Root(M). It is well-known that, when M is a submonoid of A^*, Root(M) is the smallest generator of M. In [3] it is shown that, when M is a submonoid of A^∞, Root(M) may not be the smallest generator of M and that furthermore some submonoids may have no smallest generator, as shown below.

Example 1: Let M be the submonoid $(a+b)^* (\varepsilon+(ab)^\omega)$.

$G=a+b+(ab)^\omega$ and $G'=a+b+(ba)^\omega$ are two generators of M, but $G \cap G'=a+b$ is not. So M does not have a smallest generator (the smallest generator would be contained in $a+b$!). ■

Hence it is natural to investigate the minimal generators of M.

II. MINIMAL GENERATORS OF SUBMOIDS OF A^∞

Let M be a submonoid of A^∞. First let us note that of course for each $G \in \mathrm{Gen}(M)$, $\mathrm{Root}(M)$ is included in G. But unlike A^*, $\mathrm{Root}(M)$ is not always a generator of M (the reason being that the concatenation is a right-regular operation in A^* (*i.e.* for each $x, y, u \in A^*$, $xu=yu$ implies $x=y$) but it is not a right-regular operation in A^∞). For example, $\mathrm{Root}(A^\infty)=A$ which is not a generator of A^∞.

We need the three following definitions [3].

DEFINITION 1: Let M be a submonoid of A^∞.

$\forall w, w' \in M$, $w > w'$ if and only if $w \in (M_{\mathrm{fin}}-\varepsilon)\, w'$.

We say w is factorizable in M by w'.

As usual ($w > w'$ or $w=w'$) is denoted by $w \geqq w'$.

Recall that the previous relation $>$ is only transitive.

DEFINITION 2: Let M be a submonoid of A^∞. Let $w \in M$.

w is non-factorizable (in M) if and only if

$$\forall w' \in M, \qquad w \not> w'.$$

The set of all non-factorizable words of M is denoted by $\mathrm{nf}(M)$.

Remark: $\mathrm{nf}(M)=\mathrm{Root}(M)$ [notation $\mathrm{nf}(M)$ is here convenient, see both following definitions].

DEFINITION 3: Let M be a submonoid of A^∞. Let $w \in M$.

w is self-factorizable (in M) if and only if

$$\forall w' \in M, \qquad w > w' \Rightarrow w'=w.$$

The set of all self-factorizable words of M is denoted by $\mathrm{sf}(M)$.

For our study, we give another definition.

DEFINITION 4: Let M be a submonoid of A^∞. Let $w \in M$.

w is weakly-factorizable (in M) if and only if

$$\forall w' \in M, \qquad w > w' \Rightarrow w' > w.$$

The set of all weakly-factorizable words of M is denoted by $\mathrm{wf}(M)$.

In A^* where $w > w'$ implies $w' \not> w$, we have $\mathrm{nf}(M) = \mathrm{sf}(M) = \mathrm{wf}(M) = \{w/w$ is minimal with respect to $>\}$. But in A^∞, we have generally: $\mathrm{nf}(M) \subset \mathrm{sf}(M) \subset \mathrm{wf}(M)$.

Exemple 2: Let M be the submonoid

$$(aaba + ab)^* [\varepsilon + (ab)^\omega + (ba)^\omega + (aba)^\omega + a(aba)^\omega].$$

$$\mathrm{nf}(M) = aaba + ab + (ba)^\omega$$

$$\mathrm{sf}(M) = \mathrm{nf}(M) + (ab)^\omega$$

$$\mathrm{wf}(M) = \mathrm{sf}(M) + (aba)^\omega + a(aba)^w$$

(indeed $(aba)^\omega = ab(a(aba)^\omega)$ and $a(aba)^\omega = aaba(aba)^\omega$ furthermore there are not other factorizations). ■

However $\mathrm{nf}(M_{\mathrm{inf}}) = \mathrm{nf}(M)_{\mathrm{fin}} = \mathrm{sf}(M)_{\mathrm{fin}} = \mathrm{wf}(M)_{\mathrm{fin}}$.

LEMMA 1: *Let M be a submonoid of A^∞.*

Let G be a minimal generator of M, then we have: $\mathrm{sf}(M) \subset G \subset \mathrm{wf}(M)$ (*and* a fortiori $\mathrm{Root}(M_{\mathrm{fin}}) = (G_{\mathrm{fin}})$.

Proof :The first inclusion holds for any generator.

Let us assume that g is in G-$\mathrm{wf}(M)$.

For some $w \in M$, we have: $g > w$ and $w \not> g$.

As G is a generator of M, $\exists g' \in G/w \geqq g'$.

Hence $g > g$ and $g \neq g'$, it follows that $(G - g)^* = G^*$. ■

But let us note that $\mathrm{wf}(M)$ is not necessarily a generator of M as shown by the following example.

Exemple 3: Let M be the submonoid $(a+b)^* (\varepsilon + \bigcup_{i \geqq 0} a^i b a^{i+1} b \ldots)$

$$\mathrm{wf}(M) = a + b, \quad \text{which is not a generator of } M. \ ■$$

Notation: For $x \in \{n, s, w\}$, we say that a submonoid M satisfies the condition C_x iff $M_{\mathrm{inf}} \subset M_{\mathrm{fin}}\, \mathrm{xf}(M)$.

PROPOSITION 2: *Let M be a submonoid of A^∞.*

(1) *The smallest generator of M is* $\mathrm{Root}(M)$ *iff M satisfies C_n.*

(2) *M has one smallest generator iff M satisfies* C_s.

(3) *M has minimal generators iff M satisfies* C_w.

Both first equivalences are proved in [3]. For the third one, we take:

DEFINITION 5: Let (u_n) be a sequence of ω-words in M_{inf}.

(u_n) is strictly decreasing (with respect to $>$) iff (u_n) is an injective sequence (*i. e.* $i \neq j \Rightarrow u_i \neq u_j$) such that for each $i \geqq 0$, $u_i > u_{i+1}$.

LEMMA 3: *Let M a submonoid of* A^∞.

M does not satisfy C_w *implies:* $\forall G \in \text{Gen}(M)$, *there exists a strictly decreasing sequence in* G_{inf}.

Proof: As M does not satisfy C_w, the set $M_{\text{inf}} - M_{\text{fin}} \text{wf}(M)$ denoted by L is nonempty.

We have for each w in L:

(*a*) $\forall w' \in M_{\text{inf}}, w > w' \Rightarrow w' \in L$,

(*b*) $w' \in L / w > w'$ and $w' \not> w$.

We are going to construct a strictly decreasing sequence in G_{inf} by induction.

– Let w_1 be in $L \cap G$ [according to (*a*), w_1 exists].

– Let us assume that $w_1, \ldots, w_n$ are constructed.

As $w_n \in L$, there exists $w' \in L$ such that $w_n > w'$ and $w' \not> w_n$ (hence $w_n \neq w'$). As for each $i < n$, $w_i > w_n$, we have $w_i \neq w'$.

As $w' \geqq g$ for some g in $G \cap L$, according to (*a*), by keeping $w_{n+1} = g$, we obtain the $(n+1)$ th term of a strictly decreasing sequence in $G \cap L$. ■

Now to prove that not C_w implies that M does not have minimal generators, let us note that $(G - w_1)^* = G^*$.

Suppose now that $M_{\text{inf}} = M_{\text{fin}} \text{wf}(M)$ (*i.e.* M satisfies the condition C_w). Let $\sim$ be the equivalence associated with the preorder $\geqq$, *i. e.* $\sim$ is defined over M by $u \sim v$ if and only if ($u \geqq v$ or $v \geqq u$). It is easy to verify that $\sim$ saturates $\text{wf}(M)$. For each w in M_{inf}, the $\sim$-class of w is denoted by $\text{cl}(w)$.

Hence, for each w in $\text{wf}(M)$, $\text{cl}(w)$ is equal to $\{ w' \in \text{wf}(M) / w \geqq w' \}$ and $\text{cl}(w)$ is a finite language (indeed $w > w'$ and $w' \geqq w$ imply w is a periodic ω-word). Let us remark that in $\text{wf}(M)$ the words w of $\text{sf}(M)$ are characterized by $\text{cl}(w) = \{ w \}$ [that holds in particular for w in $\text{Root}(M_{\text{inf}})$]. Concerning the generators of M, we can state both following results:

LEMMA 4: $\forall G \in \text{Gen}(M)$, $\forall w \in \text{wf}(M)$, $\text{card}(\text{cl}(w) \cap G) \geqq 1$.

LEMMA 5: *Let M be a submonoid of* A^∞ *satisfying the condition* C_w.

$\forall G \in \mathrm{Gen}(M)$, G is a minimal generator if and only if

(a) $G \subset \mathrm{wf}(M)$ and

(b) $\forall w \in \mathrm{wf}(M)$, $\mathrm{card}(G \cap \mathrm{cl}(w)) = 1$.

Proof: Let G be a minimal generator of M.

Conditions (*a*) is given by lemma 1.

For condition (*b*), in view of lemma 4, it remains to consider every w in $G_{\mathrm{inf}} \cap (\mathrm{wf}(M) - \mathrm{sf}(M))$.

Let w' be an ω-word in $\mathrm{cl}(w) \cap G_{\mathrm{inf}}$.

$\forall w'' \in M_{\mathrm{inf}} / w'' \geqq '$, we have $w'' \geqq w$, hence $w' = w$ otherwise G is not a minimal generator (this implication holds even if M does not satisfy C_w).

Reciprocally, conditions (*a*) and (*b*) imply that G_{fin} is the smallest generator of M_{fin}.

Conditions (*b*) implies that $M_{\mathrm{fin}}\, \mathrm{wf}(M) = M_{\mathrm{fin}}\, G_{\mathrm{inf}}$, hence in view of condition C_w, G is a generator of M.

Now conditions (*a*) and (*b*) imply that G is a minimal generator of M. ■

The previous lemma closes the proof of the third equivalence of Proposition 2.

COROLLARY 6 : *Let M be a submonoid of A^{∞} satisfying the condition C_w. Each generator of M contains at least one minimal generator of M.*

Remark: We find again:

– a proof of equivalence (2) of proposition 2, indeed M has one smallest generator if and only if condition C_w is satisfied and for each w in $\mathrm{wf}(M)$, $\mathrm{cl}(w) = \{w\}$;

– a proof of equivalence (1) of proposition 2, indeed $\mathrm{Root}(M)$ is the smallest generator of M if and only if condition C_s is satisfied and for each w in $\mathrm{wf}(M)$, $w \not> w$.

Example 4: Let M be the monoid A^{∞}.

$$\mathrm{nf}(M) = a + b$$

$$\mathrm{sf}(M) = a + b + a^{\omega} + b^{\omega}$$

$$\mathrm{wf}(M) = a + b + (A^{+})^{\Omega}.$$

Since A^{ω} is not included in $A^{*}(A^{+})^{\Omega}$, A^{∞} does not have minimal generators. ■

We end this part with an example where M has infinitely many minimal generators (which is not possible whenever M is a rational submonoid, as shown in the following part).

Example 5: Let M be the submonoid $(a+b)^*[\varepsilon + \bigcup_{i \geqq 0} (a^i b)^\omega]$.

$$\mathrm{nf}(M) = a+b$$

$$\mathrm{sf}(M) = a+b+b^\omega$$

$$\mathrm{wf}(M) = \bigcup_{i \geqq 0} \{a^j b (a^i b)^\omega / 0 \leqq j \leqq i\}.$$

There are infinitely many $\sim$-classes:

$$\forall i \geqq 0, \qquad \mathrm{cl}_i = \{a^j b (a^i b)^\omega / 0 \leqq j \leqq i\}.$$

Hence M has infinitely many minimal generators. ■

III. RATIONAL CASE

Now we assume that M is a rational submonoid of A^∞ (*i.e.* M_{fin} is a rational language of A^* and M_{inf} is a rational language of A^ω). Let us recall that a ω-language is rational if and only if it is a finite union of ω-languages such as XY^ω where X and Y are rational languages of A^*. We also know [1] that rational ω-languages are characterized as ω-languages recognized by a Büchi automaton.

We are going to prove that one can decide, given a rational submonoid M, whether M satisfies or not a condition C_x. But we first recall the definition of ifl-codes [9] and give two preliminary results.

DEFINITION: Let C be a language, C is an ifl-code if and only if for each u, v in C, $u C^\omega \cap v C^\omega \neq \varnothing$ or $u = v$.

LEMMA 7: *Let u, v be two words in A^+.*

If the language $(u+v)$ is a code, then it is an ifl-code.

Proof: We can assume that $|u| \leqq |v|$.

So we can write $v = u^n u'$ for some integer $n \geqq 0$ and some word u' which is not a prefix of u.

– If u' is a proper prefix of u (*i.e.* $u = u' u''$ for some u'' in A^+) and $u(u+v)^\omega \cap v(u+v)^\omega \neq \varnothing$ (*i.e.* $u+v$ is not an ifl-code), we have necessarily: $u^n u' u' u'' = u u^{n-1} u' u'' u'$.

Hence $u' u'' = u'' u'$, it follows that $u+v$ is not a code.

– If u' is not a prefix of u, then $u+v$ is an ifl-code. ■

LEMMA 8: *Let L be a language of* A^+.

If L^ω *is an ultimately periodic* ω*-language then any word m in L satisfies* $\{m^\omega\} = L^\omega$.

Proof: Let u be a fixed word in L and let v be any word in L.

The w-word $w = uv \ldots u^n v^n \ldots$ being ultimately periodic, it is easy to see that $w = m' m^\omega$ for some m, m' in $(u+v)^+$.

Hence $u+v$ is not an ifl-code.

By using the previous lemma, $u+v$ is not a code, the result follows. ■

To decide whether a rational submonoid M satisfies C_n raises no problem since $\mathrm{nf}(M)$ [*i.e.* $\mathrm{Root}(M)$] is a rational language. But neither $\mathrm{sf}(M)$ nor $\mathrm{wf}(M)$ are rational languages as shown by the following example.

Example 6: Let M be the submonoid $(a^* b)^* (\varepsilon + (a^* b)^\omega)$.

$$\mathrm{nf}(M) = a^* b$$

$$\mathrm{sf}(M) = a^* b + (a^* b)^\Omega$$

[$(a^* b)^\Omega$ is not a rational ω-language]

$$\mathrm{wf}(M) = \mathrm{sf}(M) + ((a^* b) +)^\Omega - ((a^* b)^\Omega). \quad ■$$

Now we are going to propose a way for deciding, given a rational submonoid, M, whether M satisfies the condition C_s.

Notation: An ω-word w is properly self-factorizable if and only if $w \in \mathrm{sf}(M) - \mathrm{nf}(M)$. The set $\mathrm{sf}(M) - \mathrm{nf}(M)$ is denoted by $\mathrm{Psf}(M)$.

Then the condition C_s can be reformulated by:

LEMMA 9: *Let M be a submonoid of* A^∞.

M satisfies the condition C_s *if and only if* $M_{\mathrm{inf}} - M_{\mathrm{fin}}\,\mathrm{nf}(M)$ *is included in* $M_{\mathrm{fin}}\,\mathrm{Psf}(M)$.

Now we note that $\mathrm{Psf}(M)$ is a periodic language included in $(M_{\mathrm{fin}})^\Omega$, so we have:

LEMMA 10: *Let M be a submonoid of* A^∞.

If M satisfies the condition C_s *then* $M_{\mathrm{inf}} - M_{\mathrm{fin}}\,\mathrm{nf}(M)$ *is an ultimately periodic language (note that the converse does not hold).*

On the other hand:

LEMMA 11: *Let M be a rational language of A^ω.*

On can decide whether M is an ultimatley periodic language.

Proof: Let M be a rational language of A^ω given by a rational expression such as $\bigcup_{1 \leq i \leq n} A_i B_i^\omega$, where all A_i and B_i are rational languages of A^*.

If M is an ultimately periodic language, then B_i^ω is also one. By using lemma 8, we obtain: $\forall b_i \in B_i$, $B_i^\omega = b_i^\omega$.

Hence M is an ultimately periodic language if and only if for each $i \in \{1, \ldots, n\}$, $B_i^\omega = b_i^\omega$ for any word b_i in B_i (the sense "if" is trivial).

Consequently one can decide whether M is an ultimately periodic language. ■

COROLLARY 12: *Each rational and ultimately periodic language has a finite number of periodic right-factors. Furthermore everyone is a constructible ω-word (a periodic ω-word is constructible means that one can construct a (finite) period of this ω-word).*

LEMMA 13: *Let M be a submonoid of A^∞.*

Given a periodic ω-word (by a period), one can construct all ω-words w' in $(M_{\text{fin}})^\Omega$ satisfying $w > w'$.

Proof: Let $w = u^\omega$ be a periodic ω-word.

First the number of w' such that $w > w'$ is less than $|u|$.

Let $w' = \hat{u}^\omega$ be a periodic w-word in $(M_{\text{fin}})^\Omega$ such that $w > w'$. So there exists $v \in M_{\text{fin}} - \varepsilon$ such that $w = vw'$.

Let Q be the set of states of the minimal automaton recognizing M_{fin}.

One can check that $u^\omega = v\hat{u}^\omega$ for some v and $\hat{u}$ in M_{fin} if and only if $u^\omega = \alpha\beta^\omega$ for some α and β in $M_{\text{fin}} \cap \{m \in A^* / |m| \leq 1 + |u| . \text{Card}(Q)\}$.

That closes the proof. ■

COROLLARY 14: *Let M be a rational submonoid of A^∞.*

Given a periodic ω-word (by a period), one can decide whether w belongs to $\text{Psf}(M)$.

Proof:

algorithm:
. decide whether w belongs to M_{inf}
. if yes then
. . construct the set E of all w' in $(M_{\text{fin}})^\Omega$ such that $w > w'$

. . check whether $E \cap M_{\text{inf}} = \{ w \}$
. . if yes then w belongs to $\text{Psf}(M)$
else w does not belong to $\text{Psf}(M)$. ■

Now we can state:

PROPOSITION 15: *Given* M a rational submonoid of A^{∞}, one can decide whether M has a smallest generator.

Proof:
algorithm:
. decide whether $M_{\text{inf}} - M_{\text{fin}}\, \text{nf}(M)$ is an ultimately periodic language { lemma 11 }
. if yes then
. . construct the set E of all periodic factors of $M_{\text{inf}} - M_{\text{fin}}\, \text{nf}(M)$ { corollary 12 }
. . construct $E \cap \text{Psf}(M)$ { corollary 14 }
. . decide whether $M_{\text{inf}} - M_{\text{fin}}\, \text{nf}(M)$ is included in $M_{\text{fin}}\, (E \cap \text{Psf}(M)$
. . if yes then M satisfies C_s
else M does not satisfy C_s { lemma 9 }
else M does not satisfy C_s { lemma 10 }. ■

As $\text{Psf}(M)$ is included in $M_{\text{inf}} - M_{\text{fin}}\, \text{nf}(M)$, in the previous algorithm, $E \cap \text{Psf}(M)$ is equal to $\text{Psf}(M)$, hence we obtain:

COROLLARY 16: *Let M be a rational submonoid of A^{∞}, the smallest generator (if any) is equal to* $\text{sf}(M)$ *which is a rational and constructible language.*

In the same way, one can prove that:

PROPOSITION 17: *Given M a rational submonoid of A^{∞}, one can decide whether M has minimal generators. Furthermore these minimal generators are in finite number, rational and constructible languages.*

Remark: Example 5 shows that, when M is not a rational language, it may have infinitely many minimal generators.

Finally we are interested in the submonoids having a finite set for generator.

DEFINITION: Let M be a submonoid of A^{∞}, M is finitely generated if and only if M has a finite generator.

PROPOSITION 18: *Let M be a submonoid of A^{∞}.*

M is finitely generated if and only if

(a) wf (M) *is a finite language and (b) M satisfies condition* C_w.

Proof: If M is finitely generated, we have:

– condition (*a*) since, for each w in wf(M), cl(w) is a finite set and wf(M) is then a finite union of finite sets.

– condition (*b*) indeed M having a finite generator has *a fortiori* minimal generators (but not necessarily one smallest generator, *see* example 1).

The converse is immediate. ■

COROLLARY 19: *Let M be a rational submonoid of* A^∞.

One can decide whether M is finitely generated.

If so, then M has a finite number of finite generators and furthermore all minimal generators are finite and have the same cardinality.

IV. CHARACTERIZATION OF RATIONAL SUBMONOIDS OF A^∞ WITH NON-ERASING MORPHISMS

In this last part we prove that the submonoid $x^*+(x^*y)^\omega$ enable us to obtain every rational submonoid over some alphabet A through a composition of two non-erasing morphisms and one inverse non-erasing morphism.

DEFINITION [5]: Let A, B be two alphabets, a morphism h mapping A^* to B^* is said to be non-erasing if and only if $h(A)\subset B^+$.

We first give a characterization of rational languages of A^∞ which is similar to the ones of rational languages either of A^* or of A^ω [5, 6].

PROPOSITION 20: *Let M be a language of* A^∞.

M is a rational language of A^∞ *if and only if*

$$M=h_1\circ h_2\circ h_3^1(x^*z+(x^*y)^\omega)$$

for some non-erasing morphisms h_1, h_2, h_3.

Proof: The "if"-part is clear since $x^*z+(x^*y)^\omega$ is a rational language.

The "only if"-part is adapted from the proof of proposition 3.1 in [6].

Let $@=(A, Q, q_0, T, \delta)$ be an automaton recognizing M_{fin} (where A is an alphabet, Q is a finite set of states, q_0 is the initial state, δ is the transition relation and T is the set of recognizing states).

We can assume that $q_0\notin\delta(Q, A)$.

Let $@'=(A, Q', q'_0, T', \delta')$ be a Büchi automaton recognizing M_{inf} and having a single initial state q'_0.

We can assume that $q'_0 \notin \delta'(Q', A)$.

We consider the automaton $@ \cup @'$ where q_0 and q'_0 are merged.

In the automaton $@ \cup @'$, the states of $@$ range in $0, \ldots, k$ and the states of $@'$ range in $0, k+1, \ldots, n$.

Let $\ddot{A}$ be the alphabet $\{\ddot{a}/a \in A\}$, $\mathring{A}$ be the alphabet $\{\mathring{a}/a \in A\}$ and t be a new letter.

Let F be the following set

$$F=\{t^i a t^{n-j}/a \in A,\ q_j \in \delta(q_i, a)\} \cup \{t^i \ddot{a} t^n/a \in A,\ \delta(q_i, a) \in T\} \cup$$
$$\{t^i a t^{n-j}/a \in A,\ q_j \in \delta(q_i, a)-T'\} \cup \{t^i \mathring{a} t^{n-j}/a \in A,\ q_j \in \delta(q_i, a) \cap T'\}.$$

Let h be the morphism defined by:

$$\forall a \in A, \qquad h(a)=h(\ddot{a})=h(\mathring{a})=a \quad \textit{and} \quad h(t)=\varepsilon$$

So we have:

$$M_{\text{fin}}=h(F^* \cap (A\,t^n)^* \ddot{A}\,t^n) \quad \textit{and} \quad M_{\text{inf}}=h(F^w \cap [(A\,t^n)^* \mathring{A}\,t^n]^w)$$

(the assumption $q_0 \notin \delta(Q, A)$ and $q_0 \notin \delta'(Q', A)$ is here necessary).

We denote by $f_1, \ldots f_p$ the elements of F and let Y be a new alphabet $\{y_1, \ldots, y_p\}$.

Let k_1 be the non-erasing morphism defined by:

$$\forall i \in \{1, \ldots, p\}, \qquad k_1(y_i)=f_i$$

then we have:

$$\forall L \subset A^\infty, \qquad L \cap (F^* \cup F^w)=k_1 \circ k_1^{-1}(L).$$

So it follows:

$$M=h \circ k_1 \circ k_1^{-1}((A\,t^n)^* \ddot{A}\,t^n+[(A\,t^n)^* \mathring{A}\,t^n]^\omega)$$

where $(h \circ k_1)$ is a strictly alphabetic morphism.

On the other hand:

$$(A\,t^n)^* \ddot{A}\,t^n+[(A\,t^n)^* \mathring{A}\,t^n]^\omega=k_2^{-1} \circ h_3(x^* y+(x^* z)^\omega)$$

where k_2 is a strictly alphabetic morphism defined by:

$$k_2(t)=t \quad \textit{and} \quad \forall a \in A : k_2(a)=x,\ k_2(\ddot{a})=z,\ k_2(\mathring{a})=y$$

and h_1 is a non-erasing morphism defined by:

$$h_3(x)=xt^n,\ h_3(y)=yt^n,\ h_3(z)=zt^n.$$

Now by denoting $h_2=k_2 \circ k_1$ and $h_1=k \circ k_1$, we have the result. ■

Note that $(x^* y+(x^* y)^\omega$ does not enable us to obtain all rational languages of A^∞, indeed: if m belongs to $(h_1 \circ h_2^{-1} \circ h_3)(x^* y)$ then m^ω belongs to $(h_1 \circ h_2^{-1} \circ h_3)((x^* y)^\omega)$. That is, $(M_{\text{fin}})^\omega$ is included in M_{inf}!

Now in the same way, we characterize the rational submonoids of A^∞.

PROPOSITION 21: *Let M be a language of A^∞.*

M is a rational submonoid of A^∞ if and only if

$$M=h_1 \circ h_2^{-1} \circ h_3 (x^* + (x^* y)^\omega)$$

for some non-erasing morphisms h_1, h_2, h_3.

Proof: The "if"-part holds since the family $\text{Rat}(A^\omega)$ and the family of all submonoids of A^∞ are closed under morphisms and inverse morphisms.

For the "only if"-part, let $@=(A, Q, q_0, T, \delta)$ be the minimal automaton recognizing $\text{Root}(M_{\text{fin}})$.

Let $@=(A, Q', q'_0, T', \delta)$ be a Büchi automaton recognizing M_{inf} and such that q'_0 is the single initial state and $q'_0 \notin \delta(Q', A)$.

Replacing letter $\ddot{a}$ by a and hence removing the letter z in the above construction, we obtain the result. ■

Finally we note that none of the families of submonoids satisfying some condition C_x is closed under either morphism, inverse morphism or intersection as shown by the three following examples.

Example 7: Let M be the submonoid $(a+b)^* + [(a+b)^* (c+d)]^\omega$.

M satisfies the condition C_n, but with the morphism h defined by:

$$h(a)=h(c)=a$$
$$h(b)=h(d)=b$$

$h(M)=(a+b)^\infty$ which does not satisfy C_w. ■

Example 8: Let M be the submonoid $(a+b+bc)^* [\varepsilon + ca^* (bca^*)^\omega]$.

M satisfies the condition C_n, but with the morphism h defined by:

$$h(x)=a$$
$$h(y)=bc$$

$h^{-1}(M)=(x+y)^*(\varepsilon+(yx^*)^\omega)$ which does not satisfy C_w. ■

Example 9: Let M be the submonoid $(a+b+bcd)^*[\varepsilon+cda^*(bcda^*)^\omega]$.

Let M' be the submonoid $(a+bc+bcd)^*[\varepsilon+da^*(bcda^*)^\omega]$.

M and M' satisfy the condition C_n, but the submonoid

$M\cap M'=(a+bcd)^*[\varepsilon+(bcda^*)^w]$

does not satisfy C_w. ■

REFERENCES

1. J. R. Büchi, On Decision Method in Restricted Second-Order Arithmetics, *Proc. Congr. Logic, Method. and Philos. Sci.*, Stanford Univ. Press, Stanford, 1962, pp. 1-11.
2. P. Darondeau and L. Kott, A Formal Proof System for Infinitary Rational Expression; *I.R.I.S.A. Rept.*, No. 199, 1983.
3. Do Long Van, Sur les ensembles générateurs minimaux des sous-monoïdes de A^∞; *C. R. Acad. Sci. Paris*, 300, série I, No. 13, 1985.
4. S. Eilenberg, Automata, Languages and Machines; *A*, *Academic Press*, New York, 1974.
5. M. Latteux and J. Leguy, On the Composition of Morphisms and Inverse Morphisms, *Lect. Notes Comput. Sci.*, 1983, *154*, pp. 420-432.
6. M. Latteux and E. Timmerman, Two Characterizations of Rational Adherences, *Theor. Comput. Sci.*, 1986, *46*, pp. 101-106.
7. I. Litovsky and E. Timmerman, On Generators of Rational ω-Power Languages, *Theor. Comput. Sci.*, 1987, *53*, pp. 187-200.
8. E. Timmerman, The Three Subfamilies of Rational ω-Languages Closed under ω-Transduction (to appear).
9. L. Staiger, On Infinitary Finite Lenght Codes; *Theoretical Informatics and Applications*, 1986, *20*, No. 4, pp. 483-494.
10. L. Staiger, Reasearch in Theory of ω-Languages, *J. Inf. Process. Cybern.*, EIK 23, 1987, *8/9*, pp. 415-439.