I. Litovsky

Minimal generators of submonoids of $A^\infty$

*Informatique théorique et applications*, tome 25, n° 1 (1991), p. 3-17

<http://www.numdam.org/item?id=ITA_1991__25_1_3_0>
MINIMAL GENERATORS OF SUBMONOIDS OF $A^\infty$ (*)

by I. Litovsky (*)

Communicated by J. Berstel

Abstract. — In the monoid $A^\infty$ (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 $A^\infty$ may be obtained from the single submonoid $x^* + (x^*y)\infty$ through a composition of non-erasing morphisms and non-erasing inverse morphisms.

Résumé. — Dans le monoïde $A^\infty$ (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 $x^* + (x^*y)\infty$ permet d’obtenir tout sous-monoïde rationnel de $A^\infty$ 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 $\text{Root}(M)$ (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 $\text{Root}(M)$].

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

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

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

Given $M$ a submonoid of $A^\infty$, 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 smallest 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 $A^\infty$ may be obtained through the single submonoid $(x^* + (x^* y)^*)$.

I. PRELIMINAIRES

Let $A$ be an alphabet, $A^*$ is the set of all (finite) words over $A$, the empty word is denoted by $\varepsilon$, $A^* - \{\varepsilon\}$ 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.

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

Informatique théorique et Applications/Theoretical Informatics and Applications
The concatenation over $A^*$ is extended over $A^\omega$ by:
\[
\forall w \in A^\omega, \quad \forall \alpha \in A^\omega : w\alpha = w.
\]
\[
\forall u \in A^*, \forall w \in A^\omega : uw \text{ is such that}
\]
\[
(uw)(n) = u(n), \quad \forall n \leq |u|
\]
\[
(uw)(n) = w(n - |u|), \quad \forall n > |u|.
\]
So $A^\omega$ is a monoid. As usual the concatenation is extended to the languages, and for any language $L$:
\[
L^0 = \{\varepsilon\}
\]
\[
\forall n \geq 1, \quad L^n = L \cdot L^{n-1}
\]
\[
L^* = \bigcup_{n \geq 0} L^n = (L_{\text{fin}})^* \cup (L_{\text{inf}})^* L_{\text{inf}}.
\]

Let $u$ be a word in $A^+$, the $\omega$-word $u \ldots u \ldots$ is denoted by $u^\omega$ and is said to be periodic. Let $L$ be a language in $A^+$, as in [2], $L^0$ denotes the following $w$-language $\{u^\omega/u \in L\}$. An $\omega$-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 $v^\omega$ a periodic right-factor of $w$. A language $L$ is ultimately periodic if and only if every $\omega$-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 $A^\omega$ if and only if $M_{\text{fin}} = M_{\text{fin}}^*$ and $M_{\text{inf}} = M_{\text{inf}} M_{\text{inf}}$. Let $M$ be a submonoid of $A^\omega$, $G$ is called a generator of $M$ whenever $G^* = M$. Clearly $G$ is a generator of $M$ if and only if $G_{\text{fin}}^* = M_{\text{fin}}$ and $G_{\text{fin}}^* G_{\text{inf}} = M_{\text{inf}}$. The family of all generators of $M$ is denoted by $\text{Gen}(M)$.

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 $\text{Gen}(M)$, the basic following definitions. Let $M$ be submonoid of $A^\omega$, $L$ is the smallest generator of $M$ if and only if $L \in \text{Gen}(M)$ and for each $G \in \text{Gen}(M)$, $L \subset G$. $G$ is a minimal generator of $M$ if and only if $G \in \text{Gen}(M)$ and for each $G' \in \text{Gen}(M)$, $G' \subset G$ implies $G = G'$.

The language $(M - \varepsilon) - (M - \varepsilon)^2$ is denoted by $\text{Root}(M)$. It is well-known that, when $M$ is a submonoid of $A^*$, $\text{Root}(M)$ is the smallest generator of $M$. In [3] it is shown that, when $M$ is a submonoid of $A^\omega$, $\text{Root}(M)$ 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 $(a+b)^* (e+(ab)^*)$. $G = a+b+(ab)^*$ and $G' = a+b+(ba)^*$ 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 $A^\infty$. First let us note that of course for each $G \in \text{Gen}(M)$, $\text{Root}(M)$ is included in $G$. But unlike $A^*$, $\text{Root}(M)$ 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 $A^\infty$). For example, $\text{Root}(A^\infty) = A$ which is not a generator of $A^\infty$.

We need the three following definitions [3].

Definition 1: Let $M$ be a submonoid of $A^\infty$. 
\( \forall \, w, \, w' \in M, \, w \succ w' \) if and only if $w \in (M_{\text{fin}} - \varepsilon)w'$.

We say $w$ is factorizable in $M$ by $w'$.

As usual $(w \succ w'$ or $w = w'$) is denoted by $w \succeq w'$.

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

Definition 2: Let $M$ be a submonoid of $A^\infty$. Let $w \in M$.

$w$ is non-factorizable (in $M$) if and only if 
\[ \forall \, w' \in M, \, w \succ w'. \]

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

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

Definition 3: Let $M$ be a submonoid of $A^\infty$. Let $w \in M$.

$w$ is self-factorizable (in $M$) if and only if 
\[ \forall \, w' \in M, \, w \succ w' \Rightarrow w' = w. \]

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

For our study, we give another definition.

Definition 4: Let $M$ be a submonoid of $A^\infty$. Let $w \in M$.
w is weakly-factorizable (in M) if and only if
\[ \forall w' \in M, \quad w > w' \Rightarrow w' > w. \]

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

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

**Exemple 2:** Let \( M \) be the submonoid
\[
(aaba + ab)^* [\varepsilon + (ab)^\omega + (ba)^\omega + (aba)^\omega + a(ab)^\omega].
\]
\[
\text{nf}(M) = aaba + ab + (ba)^\omega
\]
\[
\text{sf}(M) = \text{nf}(M) + (ab)^\omega
\]
\[
\text{wf}(M) = \text{sf}(M) + (aba)^\omega + a(ab)^\omega
\]

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

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

**Lemma 1:** Let \( M \) be a submonoid of \( A^\omega \).

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

**Proof:** The first inclusion holds for any generator.

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

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

As \( G \) is a generator of \( M \), \( \exists g' \in G/w \geq g' \).

Hence \( g > g \) and \( g \not= g' \), it follows that \( (G - g)^* = G^* \). ■

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

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

\[
\text{wf}(M) = a+b, \quad \text{which is not a generator of } M. \quad \blacksquare
\]

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

**Proposition 2:** Let \( M \) be a submonoid of \( A^\omega \).

(1) The smallest generator of \( M \) is \( \text{Root}(M) \) 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 $\omega$-words in $M_{\text{inf}}$.
$(u_n)$ 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 $i \geq 0$, $u_i > u_{i+1}$.

**Lemma 3:** Let $M$ a submonoid of $A^\infty$.
$M$ does not satisfy $C_w$ implies: $\forall G \in \text{Gen}(M)$, there exists a strictly decreasing sequence in $G_{\text{inf}}$.

**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 $w' \not\geq w$.

We are going to construct a strictly decreasing sequence in $G_{\text{inf}}$ 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 $w' \not\geq w_n$ (hence $w_n \neq w'$).
As for each $i < n$, $w_i > w_{i+1}$, we have $w_i \neq w'$.
As $w' \geq g$ 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 $\geq$, i.e. $w \sim v$ if and only if $(u \geq v$ or $v \geq u)$. It is easy to verify that $\sim$ saturates $\text{wf}(M)$. For each $w$ in $M_{\text{inf}}$, 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 $\{ w' \in \text{wf}(M) / w \geq w' \}$ and $\text{cl}(w)$ is a finite language (indeed $w > w'$ and $w' \geq w$ imply $w$ is a periodic $\omega$-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 Root($M_{\text{inf}}$)]. Concerning the generators of $M$, we can state both following results:

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

**Lemma 5:** Let $M$ be a submonoid of $A^\infty$ satisfying the condition $C_w$.
\( \forall G \in \text{Gen}(M), G \text{ is a minimal generator if and only if} \)

(a) \( G \subseteq \text{wf}(M) \) and

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

**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 \( G_{\text{inf}} \cap (\text{wf}(M) - \text{sf}(M)) \).

Let \( w' \) be an \( \omega \)-word in \( \text{cl}(w) \cap G_{\text{inf}} \).

\( \forall w'' \in M_{\text{inf}} / w'' \geq ' \), we have \( w'' \geq w \), 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 \( G_{\text{fin}} \) is the smallest generator of \( M_{\text{fin}} \).

Conditions (b) implies that \( M_{\text{fin}} \text{wf}(M) = M_{\text{fin}} G_{\text{inf}}, \) 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 \( A^\infty \) 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 \( \text{wf}(M) \), \( \text{cl}(w) = \{ w \} \);

- a proof of equivalence (1) of proposition 2, indeed Root(\( M \)) is the smallest generator of \( M \) if and only if condition \( C_s \) is satisfied and for each \( w \) in \( \text{wf}(M) \), \( w \triangleright w \).

**Example 4**: Let \( M \) be the monoid \( A^\infty \).

\[
\begin{align*}
\text{nf}(M) &= a + b \\
\text{sf}(M) &= a + b + a^* + b^* \\
\text{wf}(M) &= a + b + (A^+)\Omega.
\end{align*}
\]

Since \( A^\infty \) is not included in \( A^*(A^+)\Omega \), \( A^\infty \) does not have minimal generators. 

vol. 25, n° 1, 1991
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 $(a+b)^*\{e + \mathcal{U}\{a+\}b\}^\omega$.

\[
\begin{align*}
\text{nfr}(M) &= a + b \\
\text{sfr}(M) &= a + b + b^\omega \\
\text{wfr}(M) &= \bigcup_{i \geq 0} \{a^i b (a^i b)^\omega/0 \leq j \leq i\}.
\end{align*}
\]

There are infinitely many $\sim$-classes:

$$\forall i \geq 0, \quad \text{cl}_i = \{a^i b (a^i b)^\omega/0 \leq j \leq i\}.$$  

Hence $M$ has infinitely many minimal generators. \[\square\]

III. **RATIONAL CASE**

Now we assume that $M$ is a rational submonoid of $A^\omega$ (i.e. $M_{\text{fin}}$ is a rational language of $A^*$ and $M_{\text{inf}}$ is a rational language of $A^\omega$). Let us recall that a $\omega$-language is rational if and only if it is a finite union of $\omega$-languages such as $XY^\omega$ where $X$ and $Y$ are rational languages of $A^*$. We also know [1] that rational $\omega$-languages are characterized as $\omega$-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 $C$, $u C^\omega \cap v C^\omega \neq \emptyset$ 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 $|u| \leq |v|$.

So we can write $v = u^n u'$ for some integer $n \geq 0$ 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 $u (u + v)^\omega \cap v (u + v)^\omega \neq \emptyset$ (i.e. $u + v$ is not an ifl-code), we have necessarily: $u^n u' u'' u' = u u^n u' u'' u'$.
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 \( L^\omega \) is an ultimately periodic \( \omega \)-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 \( \omega \)-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 \( C_\omega \) raises no problem since \( \text{nf}(M) \) [i.e. \( \text{Root}(M) \)] is a rational language. But neither \( \text{sf}(M) \) nor \( \text{wf}(M) \) are rational languages as shown by the following example.

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

\[
\begin{align*}
\text{nf}(M) &= a^* b \\
\text{sf}(M) &= a^* b + (a^* b)^\Omega \\
\text{wf}(M) &= \text{sf}(M) + ((a^* b) +)^\Omega - ((a^* b)^\Omega).
\end{align*}
\]

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

Now we are going to propose a way for deciding, given a rational submonoid, \( M \), whether \( M \) satisfies the condition \( C_\omega \).

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

Then the condition \( C_\omega \) can be reformulated by:

**Lemma 9:** Let \( M \) be a submonoid of \( A^\omega \).

\( M \) satisfies the condition \( C_\omega \) if and only if \( M_{\text{inf}} - M_{\text{fin}} \text{nf}(M) \) is included in \( M_{\text{fin}} \text{Psf}(M) \).

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

**Lemma 10:** Let \( M \) be a submonoid of \( A^\omega \).

If \( M \) satisfies the condition \( C_\omega \) then \( M_{\text{inf}} - M_{\text{fin}} \text{nf}(M) \) 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 $A^\omega$. On can decide whether $M$ is an ultimately periodic language.

**Proof:** Let $M$ be a rational language of $A^\omega$ 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 $B_i^\omega$ 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. $lacklozenge$

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

**Lemma 13:** Let $M$ be a submonoid of $A^\omega$. Given a periodic $\omega$-word (by a period), one can construct all $\omega$-words $w'$ in $(M_{\text{fin}})\Omega$ satisfying $w > w'$.

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

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

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

That closes the proof. $lacklozenge$

**Corollary 14:** Let $M$ be a rational submonoid of $A^\omega$. Given a periodic $\omega$-word (by a period), one can decide whether $w$ belongs to $\text{Psf}(M)$.

**Proof:**

algorithm:

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

**Proposition 15:** Given $M$ a rational submonoid of $A^\infty$, 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 $A^\infty$, 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 $A^\infty$, 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 $A^\infty$, $M$ is finitely generated if and only if $M$ has a finite generator.

**Proposition 18:** Let $M$ be a submonoid of $A^\infty$.  

vol. 25, n° 1, 1991
\( M \) is finitely generated if and only if

(a) \( \text{wf}(M) \) 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 \( \text{wf}(M) \), \( \text{cl}(w) \) is a finite set and \( \text{wf}(M) \) 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 \( A^\infty \).

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 \( A^\infty \) WITH NON-ERASING MORPHISMS**

In this last part we prove that the submonoid \( x^* + (x^* y)^\infty \) 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 \( h(A) \subseteq B^+ \).

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

**Proposition 20:** Let \( M \) be a language of \( A^\infty \).

\( M \) is a rational language of \( A^\infty \) if and only if

\[
M = h_1 \circ h_2 \circ h_3 (x^* z + (x^* y)^\infty)
\]

for some non-erasing morphisms \( h_1, h_2, h_3 \).

**Proof:** The “\( \text{if} \)”-part is clear since \( x^* z + (x^* y)^\infty \) is a rational language.

The “\( \text{only if} \)”-part is adapted from the proof of proposition 3.1 in [6].

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

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

Informatique théorique et Applications/Theoretical Informatics and Applications
Let $\mathcal{A'} = (A, Q', q'_0, T', \delta')$ be a Büchi automaton recognizing $M_{\text{inf}}$ and having a single initial state $q'_0$.

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

We consider the automaton $\mathcal{A} \cup \mathcal{A'}$ where $q_0$ and $q'_0$ are merged.

In the automaton $\mathcal{A} \cup \mathcal{A'}$, the states of $\mathcal{A}$ range in $0, \ldots, k$ and the states of $\mathcal{A'}$ range in $0, \ldots, n$.

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

Let $F$ be the following set

$$F = \{t^i a^j \mid a \in A, q_j \in \delta(q_i, a) \} \cup \{t^i \bar{a}t^n \mid a \in A, \delta(q_i, a) \in T' \} \cup \{t^i \hat{a}t^n \mid a \in A, q_j \in \delta(q_i, a) \cap T' \}.$$

Let $h$ be the morphism defined by:

$$\forall a \in A, \quad h(a) = h(\bar{a}) = h(\hat{a}) = a \quad \text{and} \quad h(t) = \varepsilon$$

So we have:

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

(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:

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

then we have:

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

So it follows:

$$M = h \circ k_1 \circ k_1^{-1}((A t^n)^* \bar{A} t^n + [(A t^n)^* \hat{A} t^n]^w)$$

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

On the other hand:

$$(A t^n)^* \bar{A} t^n + [(A t^n)^* \hat{A} t^n]^w = k_2^{-1} \circ h_3(x^* y \cup (x^* z)^o)$$

vol. 25, n° 1, 1991
where \( k_2 \) is a strictly alphabetic morphism defined by:

\[
k_2(t) = t \quad \text{and} \quad \forall a \in A : k_2(a) = x, k_2(\bar{a}) = z, k_2(\hat{a}) = y
\]

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 \( A^\omega \), indeed: if \( m \) belongs to \((h_1 \circ h_2^{-1} \circ h_3)(x^*y)\) then \( m^\omega \) belongs to \((h_1 \circ h_2^{-1} \circ h_3)((x^*y)^\omega)\). That is, \((M_{\text{fin}})^\omega\) is included in \( M_{\text{inf}} \).

Now in the same way, we characterize the rational submonoids of \( A^\omega \).

**Proposition 21:** Let \( M \) be a language of \( A^\omega \).

\( M \) is a rational submonoid of \( A^\omega \) 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 \( A^\omega \) 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 \( M_{\text{inf}} \) and such that \( q_0' \) is the single initial state and \( q_0' \notin \delta(Q', A) \).

Replacing letter \( \bar{a} \) 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:

\[
\begin{align*}
    h(a) &= h(c) = a \\
    h(b) &= h(d) = b
\end{align*}
\]

\( h(M) = (a + b)^\omega \) which does not satisfy \( C_n \). □

**Example 8:** Let \( M \) be the submonoid \((a + b + bc)^* [c + ca^*(bca^*)^\omega] \).
MINIMAL GENERATORS OF SUBMONOIDS OF $A^\infty$

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

\begin{align*}
h(x) &= a \\
h(y) &= bc
\end{align*}

$h^{-1}(M) = (x + y)^*(\varepsilon + (yx^*)^\omega)$ 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

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

do not satisfy $C_w$. ■

REFERENCES


