# Theoretical Informatics and Applications 

Theoret. Informatics Appl. 36 (2002) 359-384
DOI: 10.1051/ita:2003002

# ON SHUFFLE IDEALS* 

Pierre-Cyrille Héam ${ }^{1}$


#### Abstract

A shuffle ideal is a language which is a finite union of languages of the form $A^{*} a_{1} A^{*} \cdots A^{*} a_{k} A^{*}$ where $A$ is a finite alphabet and the $a_{i}$ 's are letters. We show how to represent shuffle ideals by special automata and how to compute these representations. We also give a temporal logic characterization of shuffle ideals and we study its expressive power over infinite words. We characterize the complexity of deciding whether a language is a shuffle ideal and we give a new quadratic algorithm for this problem. Finally we also present a characterization by subwords of the minimal automaton of a shuffle ideal and study the complexity of basic operations on shuffle ideals.


Mathematics Subject Classification. 68Q45, 68Q70.

## 1. Preliminaries

### 1.1. Introduction

The shuffle product is an operation on languages which is strongly connected to combinatorics on words and which was widely studied in the literature $[4,18$, 21, 24, 26].

The main topic of this paper is the algorithmic study of shuffle ideals which are rational languages of the form $\cup A^{*} a_{1} A^{*} \cdots A^{*} a_{k} A^{*}$ where $A$ is a finite alphabet and the $a_{i}$ 's are letters. This is an interesting class of languages which is both connected to combinatorics on words $[11,17]$ and to the algebraic classification of rational languages: indeed it represents the first half level of a hierarchy of starfree languages which was introduced by Straubing [29] and Thérien [30] and which is still intensively studied $[2,3,9,10,23,25,27,28,31]$.

[^0]In this paper, we first show that a rational language is a shuffle ideal if and only if it can be represented by a finite automaton whose strongly connected components are complete and reduce to one state. Next we prove that computing such an automaton accepting the shuffle ideal $K$ generated by a language given by a finite automaton can be done in polynomial time, while computing a rational expression $\cup A^{*} a_{1} A^{*} \cdots A^{*} a_{k} A^{*}$ (where the union is finite) representing $K$ is exponential in the worst case. Moreover we give a quadratic algorithm to test whether a language given by a deterministic automaton is a shuffle ideal (the best algorithm known previously works approximately in time $O\left(n^{6}\right)$ [23]). We also consider the complexity of this problem by proving that it is NLOGSPACE-complete and that it becomes PSPACE-complete when the language is given by a nondeterministic automaton. In Section 5, we present a connection between the minimal automaton of a shuffle ideal and combinatorics on words: we show how to construct this automaton using properties on subwords. We also study the complexity of computing the union, the intersection and the product of two shuffle ideals. Finally, it is known $[8,14,15]$ that star-free languages are exactly the languages which can be represented by a linear temporal logic formula (some fragments of this logic are studied in $[6,32,33])$. In the last section, we give a temporal logic characterization of shuffle ideals and we prove that this restricted temporal logic evaluated over infinite words defines exactly the languages of the form $L A^{\omega}$, where $L$ is a shuffle ideal.

### 1.2. Some background

For more information on combinatorics on words we refer the reader to [17]. For a general reference on automata theory the reader is referred to $[5,7,13]$, and for basic results on complexity see [19].

For a finite set $K$, we denote its cardinality by $|K|$.
Recall that an alphabet is a finite set whose elements are called letters. A word is a finite sequence of letters. A language is a set of words and the set of all words over the alphabet $A$ is denoted by $A^{*}$. If $L$ is a language of $A^{*}, L^{c}$ denotes the complement of $L$ relatively to $A^{*}$. Any subsequence $v$ of $u$ is called a subword of $u$ and we denote this by $v \prec u$. We denote by $|u|$ the length of a word $u$, by $\varepsilon$ the empty word and by $A^{+}$the language $A^{*} \backslash\{\varepsilon\}$.

Recall that a finite automaton is a 5 -tuple $\mathcal{A}=(Q, A, E, I, F)$ where $Q$ is a finite set of states, $A$ is the alphabet, $E \subseteq Q \times A \times Q$ is the set of transitions, $I \subseteq Q$ is the set of initial states and $F \subseteq Q$ is the set of final states. With the above notation, if $p \in Q$ and $u \in A^{*}, p \cdot u \subseteq Q$ denotes the set of states $q$ of $\mathcal{A}$ such that there exists a path in $\mathcal{A}$ from $p$ to $q$ labeled by $u$. A finite automaton is said to be complete if for every state $q$ and every letter $a, q \cdot a \neq \emptyset$. If $\mathcal{A}$ is a finite automaton, then $L(\mathcal{A})$ denotes the language accepted by $\mathcal{A}$. In this paper, minimal automata are deterministic but not necessary complete and all considered automata are finite. In general, in this paper, automata are nondeterministic.

If $L$ is a language and $u$ a word, then $u^{-1} L$ denotes the language $\left\{v \in A^{*} \mid u v\right.$ $\in L\}$ and is called a quotient of $L$. It is known that $L$ is rational if and only if $L$ has
a finite number of quotients. Furthermore, in this case, the minimal automaton of $L$ has as many states as quotients of $L$.

A rational expression is a finite expression using the empty set, the letters and the symbols union, product and star. We recursively define the size of a rational expression $E$, denoted $\tau(E)$ by:

- $\tau(\emptyset)=1$;
- $\tau(E)=1$ if $E=a$ with $a \in A$;
- $\tau(E F)=\tau(E)+\tau(F)+1$;
- $\tau\left(E^{*}\right)=\tau(E)+1$;
- $\tau(E \cup F)=\tau(E)+\tau(F)+1$.

The size of a rational expression represents the number of symbols occurring in it. A language which can be represented by a rational expression is rational. Kleene's theorem [16] states that a language is rational if and only if it is recognizable by a finite automaton. In this paper, we shall make no distinction between a rational expression and the language it represents. Moreover we need the following result [12]:

Theorem 1.1. Let $E$ be a rational expression of size $n$. One can compute in time $O\left(n \log ^{2}(n)\right)$ a corresponding automaton with $O(n)$ states and $O\left(n \log ^{2}(n)\right)$ transitions.

Recall that the shuffle of two words $u$ and $v$ is the language of all words $w$ such that $w=u_{1} v_{1} u_{2} v_{2} \cdots u_{n} v_{n}$ with $u_{i}, v_{i} \in A^{*}, u_{1} u_{2} \cdots u_{n}=u$ and $v_{1} v_{2} \cdots v_{n}=v$. The shuffle of $u$ and $v$ is denoted $u \sqcup v$. This notion can be extended to languages as follows:

$$
L \amalg K=\bigcup_{u \in L, v \in K} u \amalg v .
$$

A language $L$ is a shuffle ideal if $L \amalg A^{*}=L$. For any language $L, L \amalg A^{*}$ is the smallest (for the inclusion) shuffle ideal containing $L$; it is called the shuffle ideal generated by $L$. We need the following important result due to Higman [11] (see also [17], Chap. 6).

Theorem 1.2. A language $L$ is a shuffle ideal if and only if there exists a finite set $K$ such that $L=K \amalg A^{*}$.

In particular, since the shuffle operator preserves rational languages, every shuffle ideal is a rational language. Moreover, it is known [23] that the class of shuffle ideals is a positive variety of languages. In particular, we have the following proposition [23]:

Proposition 1.3. The union and the intersection of two shuffle ideals is a shuffle ideal and left and right quotients of a shuffle ideal are shuffle ideals.

Finally we need the following result which leads to an algorithm to test whether a rational language is a shuffle ideal [23].

Proposition 1.4. Let $\mathcal{A}=(Q, A, E, i, F)$ be a deterministic complete automaton. The language $L(\mathcal{A})$ is a shuffle ideal if and only if there are no states $p$ and $q$ and words $u$, $v, w$ such that $i \cdot w=p, p \cdot u=q, p \cdot v \in F$ and $q \cdot v \notin F$.

We denote by $A^{\omega}$ the set of infinite words over $A$ and a set of infinite words is called $\omega$-language. If $\mathcal{A}=(Q, A, E, I, F)$ is an automaton, we denote by $L_{\omega}(\mathcal{A})$ the set of infinite words which are the label of an infinite path of $\mathcal{A}$ visiting infinitly often a state of $F$. In this case $\mathcal{A}$ is said to be a Büchi automaton.

## 2. Representing shuffle ideals

An automaton $\mathcal{A}=(Q, A, E, I, F)$ is called saturated if for all states $p \in Q$ and all letters $a \in A,(p, a, p) \in E$. An automaton is said to be locally trivial if each of its strongly connected components is reduced to one state. A rational expression is called polynomial if it is a finite union of expressions of the form $A^{*} A_{1} A^{*} \cdots A^{*} A_{k} A^{*}$ where $A_{i} \subseteq A$.
Theorem 2.1. Let $L$ be a language of $A^{*}$. The following assertions are equivalent:
(1) $L$ is a shuffle ideal;
(2) $L$ can be described by a polynomial expression;
(3) $L$ is recognizable by a saturated automaton;
(4) $L$ is recognizable by an automaton that is saturated and locally trivial.

Proof. Let $K$ be a finite set. Since

$$
K \amalg A^{*}=\bigcup_{a_{0} a_{1} \cdots a_{k} \in K} A^{*} a_{0} A^{*} a_{1} A^{*} \cdots A^{*} a_{k} A^{*}
$$

$(1) \Rightarrow(2)$ is a direct consequence of Theorem 1.2.
Each language of the form $A^{*} A_{1} A^{*} \cdots A^{*} A_{k} A^{*}$ is accepted by the automaton

which is saturated and locally trivial. Since a disjoint union of saturated, locally trivial automata is a saturated, locally trivial automaton, we have $(2) \Rightarrow(4)$.

The condition (4) is stronger than the condition (3), thus we have $(4) \Rightarrow(3)$.
Now, let $\mathcal{A}=(Q, A, E, I, F)$ be a saturated automaton and let $w \in L(\mathcal{A}) \amalg A^{*}$. By definition of the shuffle product, we have $w=u_{1} v_{1} \cdots u_{k} v_{k}$ where $u_{1} \cdots u_{k}=$ $u \in L(\mathcal{A})$ and $v_{i} \in A^{*}$. Thus, considering an accepting path in $\mathcal{A}$ labeled by $u$, each time we finish to read $u_{i}$, we can use transitions of the form $(p, a, p)$ to
read $v_{i}$. So we construct an accepting path in $\mathcal{A}$ labeled by $w$. It follows that $L(\mathcal{A}) \amalg A^{*} \subseteq L(\mathcal{A})$. Consequently $L(\mathcal{A})$ is a shuffle ideal and $(3) \Rightarrow(1)$.

## 3. Computing generated shuffle ideals

In this section we study the following problem: given a rational language, we want to compute one of the representations of Theorem 2.1 of its generated shuffle ideal. We first study how to compute a saturated automaton accepting the shuffle ideal of a given rational language. Secondly we study the same question for the computation of a locally trivial, saturated automaton. Finally we study the complexity of computing a polynomial expression representing the shuffle ideal of a given rational language.

### 3.1. Computing saturated automata

We need the following algorithm called Saturate which applies to an automaton $\mathcal{A}=(Q, A, E, I, F)$.

## Algorithm 3.1. Saturate

1. $E^{\prime}=E$.
2. For all $p \in Q$ and for all letter $a \in A$,

$$
E^{\prime}=E^{\prime} \cup\{(p, a, p)\}
$$

3. Return $\mathcal{A}^{\prime}=\left(Q, A, E^{\prime}, I, F\right)$.

Graphically, during the algorithm, we just add on each state of the automaton a loop labeled by $A$.
Proposition 3.2. If $\mathcal{A}$ is an automaton, then $\mathcal{A}^{\prime}=\underline{\operatorname{Saturate}}(\mathcal{A})$ is a saturated automaton which recognizes $L(\mathcal{A})$ ш $A^{*}$.

Proof. The automaton $\mathcal{A}^{\prime}$ is saturated because we precisely add the missing transitions to make it saturated.

By Theorem 2.1, $L\left(\mathcal{A}^{\prime}\right)$ is a shuffle ideal. Moreover, by construction, $L(\mathcal{A}) \subseteq$ $L\left(\mathcal{A}^{\prime}\right)$. It follows that $L(\mathcal{A}) \amalg A^{*} \subseteq L\left(\mathcal{A}^{\prime}\right)$. Conversely, let $w$ be in $L\left(\mathcal{A}^{\prime}\right)$ : there exists a successful path in $\mathcal{A}^{\prime}$

$$
\left(p_{0}, a_{1}, p_{1}\right),\left(p_{1}, a_{2}, p_{2}\right), \cdots,\left(p_{k-1}, a_{k}, p_{k}\right)
$$

labeled by $w$. If we delete in this path all the transitions of the form $(p, a, p)$ we obtain a new path which is both successful in $\mathcal{A}^{\prime}$ and in $\mathcal{A}$. Let $u$ be the label of this new path. Since $u \in L(\mathcal{A})$ and since $w \in\{u\} ш A^{*}, w \in L(\mathcal{A}) \amalg A^{*}$. It follows that $L\left(\mathcal{A}^{\prime}\right)=L(\mathcal{A})$ ш $A^{*}$.

For example the shuffle ideal generated by the language $\left(b^{*}(a b)^{*}\right)^{*}$ whose minimal automaton is $\mathcal{A}_{0}$ (see below), is accepted by the saturated automaton $\mathcal{A}_{1}$.

$\mathcal{A}_{0}$

$\mathcal{A}_{1}$

Proposition 3.3. Let $L$ be a rational language given by an $n$-state, $m$-transition automaton. Then one can compute in time $O(m+n|A|)$ an n-state, saturated automaton with at most $m+n|A|$ transitions, accepting the shuffle ideal generated by $L$.

Proof. By Proposition 3.2, it is sufficient to apply the algorithm Saturate.
As a direct consequence, using Theorem 1.1, one has the following corollary:
Corollary 3.4. Let $L$ be a rational language given by a rational expression of size $k$. One can compute in $O\left(k \log ^{2}(k)\right)$ time an $O(k)$-state saturated automaton accepting the shuffle ideal generated by $L$.

### 3.2. Computing locally trivial, saturated automata

Lemma 3.5. Let $L$ be a shuffle ideal accepted by a saturated $n$-state automaton and $K$ be the set of words of $L$ of length less than or equal to $n$. Then

$$
L=K \amalg A^{*}
$$

Proof. Since $K \subseteq L, K \amalg A^{*} \subseteq L \amalg A^{*}=L$. Now, let $w$ be in $L, \mathcal{A}$ be a saturated $n$-state automaton accepting $L$ and $m$ be a successful path in $\mathcal{A}$ labeled by $w$. We consider now a successful path in $\mathcal{A}$ obtained from $m$ by deleting the loops. We denote by $u$ the label of this new path. By construction $u \in K$. Furthermore, $w \in\{u\} \amalg A^{*}$. Consequently, $w \in K \amalg A^{*}$, proving the lemma.

The following algorithm has as input an $n$-state finite automaton $\mathcal{A}=(Q, A$, $E, I, F)$ and computes an automaton accepting precisely the shuffle ideal generated by $L(\mathcal{A})$.

## Algorithm 3.6. LTSaturate

1. $Q^{\prime}=Q \times\{0, \ldots, n\}$
2. $E^{\prime}=\{((p, i-1), a,(q, i)) \mid(p, a, q) \in E, i \in\{1, \ldots, n\}\}$
3. $I^{\prime}=I \times\{0\}$
4. $F^{\prime}=F \times\{0, \ldots, n\}$
5. $\mathcal{A}^{\prime}=\left(Q^{\prime}, A, E^{\prime}, I^{\prime}, F^{\prime}\right)$
6. Return Saturate $\left(\mathcal{A}^{\prime}\right)$.

Proposition 3.7. Let $\mathcal{A}$ be an n-state automaton. Then LTSaturate $(\mathcal{A})$ is a saturated, locally trivial, $O\left(n^{2}\right)$-state automaton with $O\left(m n+|A| n^{2}\right)$ transitions accepting the shuffle ideal generated by $L(\mathcal{A})$.

Proof. The automaton $\mathcal{A}^{\prime}$ is the product of $\mathcal{A}$ by the minimal automaton accepting the set of words of length less than or equal to $n$. It follows that $\mathcal{A}^{\prime}$ accepts the set of words of $L(\mathcal{A})$ of length less or equal to $n$. Thus, by Lemma 3.5 and Proposition 3.2, the automaton LTSaturate $(\mathcal{A})$ recognizes the shuffle ideal generated by $L(\mathcal{A})$.

Moreover, by construction, the automaton LTSaturate $(\mathcal{A})$ is saturated and has $n(n+1)$ states. Now, we claim that $\mathcal{A}^{\prime}$ is locally trivial. Indeed, assume that we have a non trivial loop in $\mathcal{A}^{\prime}$, i.e. there exist two distinct states $(p, i)$ and $(q, j)$ in $Q^{\prime}$ and words $u$ and $v$ such that $(p, i) \in(q, j) \cdot v$ and $(q, j) \in(p, i) \cdot u$. By definition of $E^{\prime}$, it means that $i<j$ and $j<i$, a contradiction. Since the algorithm Saturate does not change the strongly connected components, it follows that LTSaturate $(\mathcal{A})$ is locally trivial.

For example the shuffle ideal generated by the language $\left(b^{*}(a b)^{*}\right)^{*}$ whose minimal automaton is $\mathcal{A}_{0}$ (see below) and which is accepted by the saturated and locally trivial automaton $\mathcal{A}_{1}=$ LTSaturate $\left(\mathcal{A}_{0}\right)$.


Proposition 3.8. Let $L$ be a rational language given by an $n$-state, $m$-transition automaton. Then one can compute in time $O\left(|A| n^{2}+m n\right)$ a saturated, locally trivial automaton accepting the shuffle ideal generated by $L$.

Proof. This is a direct consequence of Proposition 3.7.
As a consequence of the above proposition and Theorem 1.1, one has the following corollary:

Corollary 3.9. Let $L$ be a rational language given by a rational expression of size $k$. Then one can compute in time $O\left(k^{2} \log ^{2} k\right)$ an $O\left(k^{2}\right)$-state saturated, locally trivial automaton accepting the shuffle ideal generated by $L$.

### 3.3. Computing polynomial expressions

Proposition 3.10. Let $\mathcal{A}$ be an n-state automaton. Then one can compute in time $O\left((|A|+1)^{n}\right)$ a polynomial expression of size $O\left((|A|+1)^{n}\right)$ accepting the shuffle ideal generated by $L(\mathcal{A})$.

Proof. By Lemma 3.5, one has

$$
\begin{equation*}
L(\mathcal{A}) \amalg A^{*}=\bigcup_{\substack{a_{1} \cdots a_{k} \in L(\mathcal{A}) \\ a_{i} \in A, k \leq n}} A^{*} a_{1} A^{*} a_{2} \cdots A^{*} a_{k} A^{*} \tag{1}
\end{equation*}
$$

Since $\tau(A)=\tau\left(\bigcup_{a \in A} a\right)=2|A|-1$, we have $\tau\left(A^{*} a_{1} A^{*} a_{2} \cdots A^{*} a_{k} A^{*}\right)=(k+$ 1) $\tau\left(A^{*}\right)+k+2 k=2|A|(k+1)+3 k$. It follows that the size of the expression (1) is at most $|A|^{n+1}[2|A|(n+1)+3 n]=O\left((|A|+1)^{n}\right)$.

Now we shall prove that computing a polynomial rational expression representing a given language is exponential in the worst case. Let $L$ be a rational language. We denote by $m(L)$ the number of states of the minimal automaton of $L$ and by $M(L)$ the minimal number of states of an automaton accepting $L$. Obviously $m(L) \geq M(L)$. We also denote by $e(L)$ the minimal size of a rational expression representing $L$.

We introduce the following invariants (with the convention $\inf \emptyset=0$ ):

$$
\begin{aligned}
& R(n)=\max _{L: m(L) \leq n}\left[\inf _{E: E=L}\{\tau(E) \mid E \text { polynomial }\}\right] \\
& S(n)=\max _{L: M(L) \leq n}\left[\inf _{E: E=L}\{\tau(E) \mid E \text { polynomial }\}\right] \\
& T(n)=\max _{L: e(L) \leq n}\left[\inf _{E: E=L}\{\tau(E) \mid E \text { polynomial }\}\right] .
\end{aligned}
$$

## Theorem 3.11.

$$
\Omega\left(2^{n / 3}\right)=R(n) \leq S(n)=O\left((|A|+1)^{n}\right)
$$

Proof. Since $m(L) \geq M(L)$, we have $R(n) \leq S(n)$. Moreover, by Proposition 3.10, one has $S(n)=O\left((|A|+1)^{n}\right)$.

To prove the lower bound, we consider the alphabet $A=\{a, b\}$ and the language $L=A^{*} a A^{*} b A^{*} \cup A^{*} b A^{*} a A^{*}$ which is a shuffle ideal. Since the class of shuffle ideals
is closed under product, for all $n, L^{n}$ is a shuffle ideal. Moreover, the minimal automaton of $L^{n}$ has the following form:


It follows that $m\left(L^{n}\right)=3 n+1$. Now let $E$ be a polynomial expression accepting $L^{n}$. Assume that $A^{*} A_{1} A^{*} \cdots A_{k} A^{*}$ is an expression appearing in $E$. Then the word $u=a_{1} a_{2} \cdots a_{k}$, with $a_{i} \in A_{i}$ belongs to $L^{n}$. Since each word of $L^{n}$ has length $2 n$, we have that $k \geq 2 n$.

Let $K=\{a b, b a\}$. Each word $u$ in $K^{n}$ belongs to $L^{n}$. Consequently there exists an expression

$$
E_{0}=A^{*} A_{1} A^{*} \cdots A_{k} A^{*}
$$

appearing in $E$ such that $u \in E_{0}$. But $k \geq 2 n$, hence $k=2 n$. It follows that $u \in A_{1} A_{2} \cdots A_{2 n}$.

Now we claim that if $A_{1} \cdots A_{2 n} \subseteq L^{n}$ (with $\left.A_{i} \neq \emptyset\right)$, then for all $i,\left|A_{i}\right|=1$. Indeed assume there exists an $i$ such that $A_{i}=\{a, b\}$. In this case, there exist $x$ and $y$ in $A^{*}$ such that $|x|=i-1,|x|+|y|=2 n-1$ and xay, xby $\in K^{n}$. Thus, when we read xay and $x b y$ in the minimal automaton of $L^{n}$, we do not use any loop. Thus $|x|$ must be odd (otherwise after reading $x a$ we must read $b$, and after reading $x b$ we must read $a$ : the first letter of $y$ should be both $a$ and $b$ ). Starting from the final state, the same argument leads to conclude that $|y|$ is odd, which is in contradiction with $|x|+|y|=2 n-1$.

It follows that each expression of the form

$$
A^{*} a_{1} A^{*} a_{2} A^{*} \cdots a_{2 n} A^{*}
$$

with $a_{1} \cdots a_{2 n} \in K^{n}$ appears in $E$. But

$$
\tau\left(A^{*} a_{1} A^{*} a_{2} A^{*} \cdots a_{2 n} A^{*}\right)=2|A|(2 n+1)+6 n=14 n+4
$$

and there are $\left|K^{n}\right|=2^{n}$ expressions of this kind in $E$. Thus

$$
\tau(E) \geq 14 n 2^{n}
$$

Since $R(n)$ is an increasing function and since $m\left(L^{n}\right)=3 n+1$, one can conclude that

$$
R(n)=\Omega\left(2^{n / 3}\right)
$$

Proposition 3.12. There exists a constant $\alpha \in \mathbb{N}$ such that

$$
\Omega\left(2^{n / 15}\right)=T(n) \leq S(\alpha n)=O\left((|A|+1)^{\alpha n}\right)
$$

Proof. By Theorem 1.1, there exists a constant $\alpha \in \mathbb{N}$ such that for all rational language $L, M(L) \leq \alpha e(L)$. Consequently $T(n) \leq S(\alpha n)$. The equality $S(\alpha n)=$ $O\left((|A|+1)^{\alpha n}\right)$ has been already proved.

To prove the lower bound we use the languages $L^{n}$ defined in the proof of Theorem 3.11. Since

$$
L^{n}=\left(a a^{*} b \cup b b^{*} a\right)^{n}\{a, b\}^{*}
$$

and since

$$
\tau\left(a a^{*} b \cup b b^{*} a\right)=6+1+6=13
$$

we have, for all $n \geq 4$,

$$
e\left(L^{n}\right) \leq 14 n+4 \leq 15 n
$$

Furthermore, we have seen that

$$
\inf _{E: E=L}\{\tau(E) \mid E \text { polynomial }\} \geq 14 n 2^{n}
$$

It follows that

$$
T(n) \geq \frac{14}{15} n 2^{n / 15}
$$

Consequently, $T(n)=\Omega\left(2^{n / 15}\right)$.

## 4. Testing whether a Language is a shuffle ideal

In this section we consider the complexity of testing whether a rational language is a shuffle ideal.

### 4.1. Deterministic automata

In [23], an algorithm based on Proposition 1.4 is proposed to test whether a language given by a deterministic $n$-state automaton is a shuffle ideal. This algorithm requires to compute the transitive closure of a graph with $|A|^{2} n^{2}$ vertices
and its time complexity is about $O\left(|A|^{6} n^{6}\right)$. We propose here an $O\left(|A|^{2} n^{2}\right)$ algorithm. We call our algorithm TestShuffle. Its input is a deterministic complete automaton $\mathcal{A}=(Q, A, E, i, F)$.

```
Algorithm 4.1. TestShuffle
    1. \(\mathcal{A}_{0}=\left(Q_{0}, A, E_{0}, i_{0}, F_{0}\right)=\) Saturate \((\mathcal{A})\).
    2. \(Q_{1}=Q_{0} \times Q\).
    3. \(E_{1}=\left\{\left(\left(p_{0}, p\right), a,\left(q_{0}, q\right)\right) \mid(p, a, q) \in E,\left(p_{0}, a, q_{0}\right) \in E_{0}\right\}\).
    4. \(i_{1}=\left(i_{0}, i\right)\).
    5. \(F_{1}=F_{0} \times(Q \backslash F)\).
    6. \(\mathcal{A}_{1}=\left(Q_{1}, A, E_{1}, i_{1}, F_{1}\right)\).
    7. If \(L\left(\mathcal{A}_{1}\right)=\emptyset\) return true, else return false.
```

Let us note that the automaton $\mathcal{A}_{0}$ has a unique initial state: indeed the algorithm Saturate does not change the initial states and $\mathcal{A}$ is deterministic and has hence a unique initial state.

Proposition 4.2. Let $\mathcal{A}$ be a deterministic complete $n$-state automaton. The algorithm TestShuffle $(\mathcal{A})$ returns true if and only if $L(\mathcal{A})$ is a shuffle ideal. Moreover the answer is given in time $O\left(|A|^{2} n^{2}\right)$.
Proof. By Proposition 3.2, $L\left(\mathcal{A}_{0}\right)=L(\mathcal{A}) ш A^{*}$. Moreover, by construction, $L\left(\mathcal{A}_{1}\right)=L(\mathcal{A})^{c} \cap L\left(\mathcal{A}_{0}\right)$. Consequently the algorithm returns true if and only if $L\left(\mathcal{A}_{0}\right) \subseteq L(\mathcal{A})$, if and only if $L\left(\mathcal{A}_{0}\right)=L(\mathcal{A})$, if and only if $L(\mathcal{A})$ is a shuffle ideal.

Assume that $\mathcal{A}$ has $m$ transitions. The first step of the algorithm can be done in time $O(n|A|+m)$ by Proposition 3.3 and the automaton $\mathcal{A}_{0}$ has $n$ states and $O(m+n|A|)$ transitions. It follows that computing $\mathcal{A}_{1}$ can be done in time $O\left(n^{2}+m^{2}+m n|A|\right)$ and $\mathcal{A}_{1}$ has $n^{2}$ states and $O\left(m^{2}+m n|A|\right)$ transitions. Now one can test whether $L\left(\mathcal{A}_{1}\right)$ is empty by testing whether a final state of $\mathcal{A}_{1}$ is accessible from $i_{1}$. It can be done by computing a spanning tree of $\mathcal{A}_{1}$ rooted on $i_{1}$ (for example by a depth-first search from $i_{1}$ ) and by testing whether this tree contains a final state. Hence, testing whether $L\left(\mathcal{A}_{1}\right)$ is empty can be done in time $O\left(n^{2}+m^{2}+m n|A|\right)$. Since $\mathcal{A}$ is deterministic and complete, $m=|A| n$. Consequently the algorithm works in time $O\left(n^{2}+2 n^{2}|A|^{2}\right)=O\left(n^{2}|A|^{2}\right)$.
Lemma 4.3. Let $\mathcal{A}=(Q, A, E, i, Q \backslash\{q\})$ be a complete deterministic automaton such that there is only one state $q \neq i$ which is not final. There is no path in $\mathcal{A}$ from $i$ to $q$ if and only if $L(\mathcal{A})$ is a shuffle ideal.

Proof. According to Proposition 1.4, if $L(\mathcal{A})$ is a shuffle ideal then there is no path from $i$ to $q$.

Conversely, if there is no path from $i$ to $q, L(\mathcal{A})=A^{*}$ because $\mathcal{A}$ is complete and all accessible states are final.

Theorem 4.4. Testing whether a rational language over A given by a deterministic automaton is a shuffle ideal is a NLOGSPACE-complete problem if $|A| \geq 2$.

Proof. Let $\mathcal{A}$ be a deterministic automaton whose initial state is $i$. By Proposition $1.4, L(\mathcal{A})$ is not a shuffle ideal if and only if there exist three words $w, u$
and $v$ and two states $p$ and $q$ such that $i \cdot w=p, p \cdot u=q, p \cdot v$ is final and $q \cdot v$ is not final. This can be tested in NLOGSPACE by guessing $p$ and $q$ and successively the letters of $u$ and $v$. Since NLOGSPACE=co-NLOGSPACE, testing whether a rational language given by a deterministic automaton is a shuffle ideal is an NLOGSPACE problem.

Now, let $G=(V, E)$ be a finite directed graph such that there are no more than two edges starting from each vertex. Let $p$ and $q$ be two distinct vertices of $G$. It is known that testing whether there is a path from $p$ to $q$ is an NLOGSPACEcomplete problem. Now consider a deterministic automaton $\mathcal{A}_{0}=\left(V, A, E_{0}, p, V \backslash\right.$ $\{q\})$ such that $(r, a, s) \in E_{0}$ if and only if $(r, s) \in E$ : we put labels on the edges of $G$ to make it a deterministic automaton (there are several ways to do it). If $\mathcal{A}_{0}$ is not complete we make it complete by adding a state $t \notin V$ : we consider the automaton

$$
\mathcal{A}_{1}=\left(V \cup\{t\}, A, E_{0} \cup E_{1}, p, V \cup\{t\} \backslash\{q\}\right)
$$

where $E_{1}=\left\{(s, a, t) \mid s \in V \cup\{t\}, a \in A\right.$ and $\left.(\{s\} \times\{a\} \times V) \cap E_{0}=\emptyset\right\}$. If $\mathcal{A}_{0}$ is complete we define $\mathcal{A}_{1}=\mathcal{A}_{0}$. Now, by Lemma 4.3, there is no path from $p$ to $q$ in $G$ if and only if $L\left(\mathcal{A}_{1}\right)$ is a shuffle ideal. Thus, testing whether a rational language given by a deterministic automaton is a shuffle ideal is a NLOGSPACEhard problem.

### 4.2. Nondeterministic automata

It is known that testing whether a rational language over $A$ given by a finite nondeterministic automaton accepts $A^{*}$ is a PSPACE-complete problem [1]. Since it is NLOGSPACE decidable whether the empty word belongs to a rational language given by a finite automaton (just guess a state which is both initial and final), testing whether a rational language containing the empty word and given by a finite automaton accepts every word is a PSPACE-complete problem.

Theorem 4.5. If $|A| \geq 2$, then testing whether a rational language given by $a$ finite automaton is a shuffle ideal is a PSPACE-complete problem.

Proof. Testing the equality of two rational languages given by finite automata is a PSPACE problem. Thus, using Proposition 3.3, testing whether a rational language given by a finite automaton is a shuffle ideal is a PSPACE problem.

Let $\mathcal{A}$ be a finite automaton containing the empty word. Then $L(\mathcal{A})$ is a shuffle ideal if and only if $L(\mathcal{A})=A^{*}$. Thus, testing whether a rational language given by a finite automaton is a shuffle ideal is PSPACE-hard.

## 5. On the minimal automaton of a shuffle ideal

In this section we first study properties of the minimal automaton of a shuffle ideal. Next, since the class of shuffle ideals is closed under union, intersection and product we study the complexity of computing the union, the intersection and the
product of two shuffle ideals given by their minimal automata (for a survey on these problems for finite languages or for rational languages see [34]).

### 5.1. Properties of the minimal automaton of a shuffle ideal

The following proposition is proved in [28].
Proposition 5.1. The minimal automaton of a shuffle ideal is complete and locally trivial.

Moreover, the following lemma will be useful later:
Lemma 5.2. The minimal automaton of a shuffle ideal has a unique final state.
Proof. Let $\mathcal{A}=(Q, A, E, i, F)$ be the minimal automaton of a shuffle ideal $L$ and $f$ and $g$ be two final states. There exist $u$ and $v$ such that $i \cdot u=f$ and $i \cdot v=g$. Since $L$ is a shuffle ideal, for all $w \in A^{*}, u w$ and $v w$ are both in $L$. It follows that $f=g$. Moreover, we proved that $f \cdot A^{*}=f$.

The minimal automaton of the shuffle ideal generated by a language can be much smaller than the minimal automaton of that language. For instance, $m\left(A^{n} \cup\right.$ $\{\varepsilon\})=n+1$ and $m\left(\left(A^{n} \cup\{\varepsilon\}\right) \amalg A^{*}\right)=1$ because $\left(A^{n} \cup\{\varepsilon\}\right) \amalg A^{*}=A^{*}$.

Proposition 5.3. Let $L$ be a language. There exists a unique finite language, denoted $S_{\min }(L)$, such that

- $S_{\text {min }}(L) \amalg A^{*}=L ш A^{*}$;
- If $u, v \in S_{\min }(L)$ and if $u$ is a subword of $v$, then $u=v$.

Proof. By Theorem 1.2, there exists a finite language $K$ such that $K ш A^{*}=$ $L \amalg A^{*}$. Assume there exist $u$ and $v$ in $K$ such that $u$ is a subword of $v$ and $u \neq v$. Then $v ш A^{*} \subseteq u ш A^{*}$. It follows that $K \backslash\{v\} ш A^{*}=L ш A^{*}$. In this way, one can build a finite language $S$ satisfying the hypotheses of the proposition. Assume now that there are two such finite languages $S_{1}$ and $S_{2}$. Let $u \in S_{1}$. Since $S_{1} \subseteq L ш A^{*}=S_{2} \amalg A^{*}$, there exists $v \in S_{2}$ such that $v \prec u$. By a symmetric argument, there exists $w \in S_{1}$ such that $w \prec v$. It follows that $w \prec v \prec u$. Thus, by hypotheses on $S_{1}$, we have $u=w$. Hence $u=v$, proving that $S_{1} \subseteq S_{2}$. In the same way, we prove that $S_{2} \subseteq S_{1}$. It follows that $S_{1}=S_{2}$.

Let us note that in the above proposition we do not require $L$ to be a shuffle ideal. Moreover, for each language $L, S_{\min }(L)=S_{\min }\left(L \amalg A^{*}\right)$.

Proposition 5.4. Let $L$ be a non empty language and $\ell=\min \{|u| \mid u \in L\}$. Set $K_{0}=L \cap A^{\ell}$ and, by induction, for $i \geq 1$,

$$
K_{i}=K_{i-1} \cup\left(\left(L \cap A^{\ell+i}\right) \cap\left(K_{i-1} \amalg A^{*}\right)^{c}\right) .
$$

It holds that

$$
S_{\min }(L)=\bigcup_{i \in \mathbb{N}} K_{i} .
$$

Proof. Let $K=\bigcup_{i \in \mathbb{N}} K_{i}$. By a direct induction, for all $i \in \mathbb{N}, K_{i} \subseteq L$. Thus $K \subseteq L$ and, therefore, $K ш A^{*} \subseteq L ш A^{*}$. Conversely, assume that $u \in L ш A^{*}$. There exists $v \in L$ such that $v \prec u$. If $v \in K_{|v|-\ell}$, then $u \in K_{|v|-\ell} ш A^{*} \subseteq K$ ш $A^{*}$. If $v \notin K_{|v|-\ell}$, then there exists $w \in K_{|v|-\ell-1}$ such that $w \prec v$. In this case $w \prec u$ and $u \in K_{|v|-\ell-1} \amalg A^{*} \subseteq K \amalg A^{*}$. It follows that

$$
L \amalg A^{*}=K ш A^{*}
$$

Now assume that $u$ and $v$ are two distinct words of $K$ such that $u \prec v$. Thus $|u|<|v|$. Since all words of $K$ of length $\ell+i$ are in $K_{i}$, it follows that $u \in$ $K_{|u|-\ell} \subseteq K_{|v|-\ell-1}$ and that $v \in K_{|v|-\ell}$. Moreover all words of $K_{i}$ have length less than or equal to $\ell+i$, thus $v \in K_{|v|-\ell} \backslash K_{|v|-\ell-1}$. By definition of $K_{|v|-\ell}$, $v \notin K_{|v|-\ell-1} \amalg A^{*}$. It means that $u$ is not a subword of $v$, a contradiction. Therefore, by Theorem 1.2, $K$ is finite, which concludes the proof.

For each language $L$ we define the mapping $\phi_{L}$ from $A^{*}$ into the set of finite languages by letting $\phi_{L}(u)=S_{\min }\left(u^{-1}\left(L \amalg A^{*}\right)\right)$.

Let $Q_{L}=\left\{\phi_{L}(u) \mid u \in A^{*}\right\} \quad$ and $\quad E_{L}=\left\{\left(\phi_{L}(u), a, \phi_{L}(u a)\right) \mid a \in A, u \in A^{*}\right\}$.
Proposition 5.5. Let $L$ be a non empty language. The set $Q_{L}$ is finite and the automaton $\mathcal{A}_{L}=\left(Q_{L}, A, E_{L}, S_{\min }(L),\{\varepsilon\}\right)$ is the minimal automaton of $L \amalg A^{*}$.

Proof. Since there are finitely many $u^{-1}\left(L \amalg A^{*}\right)$, the set $Q_{L}$ is finite. Moreover $\left|Q_{L}\right| \leq\left|\left\{u^{-1}\left(L \amalg A^{*}\right) \mid u \in A^{*}\right\}\right|=m\left(L \amalg A^{*}\right)$. Furthermore, by construction, $\mathcal{A}_{L}$ is deterministic.

Now we claim that $\mathcal{A}_{L}$ accepts $L \amalg A^{*}$. Indeed assume that $u \in L\left(\mathcal{A}_{L}\right)$. Then, by definition of $\mathcal{A}_{L}, S_{\min }\left(u^{-1}\left(L \amalg A^{*}\right)\right)=\{\varepsilon\}$. It follows that $\varepsilon \in u^{-1}\left(L \amalg A^{*}\right)$, proving that $u \in L ш A^{*}$. Conversely, if $u \in L \amalg A^{*}$, then $\varepsilon \in u^{-1}\left(L ш A^{*}\right)$. But the only shuffle ideal containing $\varepsilon$ is $A^{*}$ and, by Proposition 1.3, $u^{-1}\left(L \amalg A^{*}\right)$ is a shuffle ideal. It follows that $u^{-1}\left(L \amalg A^{*}\right)=A^{*}$. Therefore $S_{\min }\left(u^{-1}\left(L \amalg A^{*}\right)\right)=$ $\{\varepsilon\}$, proving the claim.

The automaton $\mathcal{A}_{L}$ is deterministic, accepts $L \amalg A^{*}$ and has at most $m(L$ ш $\left.A^{*}\right)$ states. Thus it is the minimal automaton of $L ш A^{*}$.

Now we explain how to recursively compute $\phi_{L}(u)$. We need three lemma
Lemma 5.6. Let $L$ be a shuffle ideal, $a \in A$ and $u \in A^{*}$. If

$$
u \in a^{-1} S_{\min }(L) \cup \bigcup_{b \neq a} b\left(b^{-1} S_{\min }(L)\right)
$$

then $u \in a^{-1} L$.
Proof. If $u \in a^{-1} S_{\min }(L)$, then $a u \in S_{\min }(L) \subseteq L$. It follows that $u \in a^{-1} L$. If $u \in b\left(b^{-1} S_{\min }(L)\right)$, then $u=b w$, with $b \neq a$ and $w \in b^{-1} S_{\min }(L)$. Consequently $u \in S_{\min }(L) \subseteq L$. Since $L$ is a shuffle ideal, $a u \in L$. Thus $u \in a^{-1} L$.

Lemma 5.7. Let $L$ be a shuffle ideal, $a \in A$ and $u \in A^{*}$. If $L \neq A^{*}$ and if $u \in a^{-1} L$, then there exists

$$
z \in a^{-1} S_{\min }(L) \cup \bigcup_{b \neq a} b\left(b^{-1} S_{\min }(L)\right)
$$

such that $z \prec u$.
Proof. Since $a u \in L$ and since $L$ is a shuffle ideal, there exists $v \in S_{\min }(L)$ such that $v \prec a u$. Two cases arise:
$v \in a A^{*}$ : there exists $z \in A^{*}$ such that $v=a z$. Since $a z \prec a u$, one has $z \prec u$.
Moreover, since $v \in S_{\text {min }}(L)$, one has $z \in a^{-1} S_{\text {min }}(L)$;
$v \notin a A^{*}$ : if $v=\varepsilon$, then $L=A^{*}$. Thus, by hypothesis $v \neq \varepsilon$. Therefore there exists $w \in A^{*}$ such that $v=b w$ with $b \neq a$. Since $b w$ is a subword of $a u, b w$ also is a subword of $u$. Consequently $z=b w \prec u$ and $z \in b\left(b^{-1} S_{\min }(L)\right)$.

Lemma 5.8. Let $L$ be a shuffle ideal distinct of $A^{*}, a \in A$ and

$$
K=\left(a^{-1} S_{\min }(L) \cup \bigcup_{b \neq a} b\left(b^{-1} S_{\min }(L)\right)\right)
$$

We have $a^{-1} L=K$ ш $A^{*}$.
Proof. If $u \in a^{-1} L$, then, by Lemma 5.7, there exists $z \in K$ such that $z \prec u$. Thus $u \in K \amalg A^{*}$.

If $u \in K \amalg A^{*}$, then there exists $v \in K$ such that $v \prec u$. By Lemma 5.6, $v \in a^{-1} L$. Since $a^{-1} L$ is a shuffle ideal, we have $u \in a^{-1} L$, proving the lemma.

The next proposition provides a recursive and constructive method to compute $\phi_{L}(u)$ when $S_{\min }(L)$ is known:

Proposition 5.9. Let $L$ be a language. We have $\phi_{L}(\varepsilon)=S_{\min }(L)$ and, for all $u \in A^{*}$ and $a \in A$, if $\phi_{L}(u) \neq\{\varepsilon\}$, then

$$
\phi_{L}(u a)=S_{\min }\left(a^{-1} \phi_{L}(u) \cup \bigcup_{b \in A \backslash\{a\}} b\left(b^{-1} \phi_{L}(u)\right)\right) .
$$

Proof. According to the definition of $\phi_{L}, \phi_{L}(\varepsilon)=S_{\min }\left(L \amalg A^{*}\right)$. But, by definition of $S_{\min }, S_{\min }\left(L \amalg A^{*}\right)=S_{\min }(L)$. Thus $\phi_{L}(\varepsilon)=S_{\min }(L)$.

Assume that $\phi_{L}(u) \neq\{\varepsilon\}$. Then $u^{-1}\left(L \amalg A^{*}\right) \neq A^{*}$. Moreover, by Proposition 1.3, $u^{-1}\left(L \amalg A^{*}\right)$ is a shuffle ideal. Thus, by Lemma 5.8, we have

$$
\begin{aligned}
& a^{-1} u^{-1}\left(L \amalg A^{*}\right)= \\
& \\
& \qquad\left(a^{-1} S_{\min }\left(u^{-1}\left(L \amalg A^{*}\right)\right) \cup \bigcup_{b \neq a} b\left(b^{-1} S_{\min }\left(u^{-1}\left(L \amalg A^{*}\right)\right)\right)\right) \amalg A^{*} .
\end{aligned}
$$

By definition of $\phi_{L}$, it follows that

$$
\phi_{L}(u a)=S_{\min }\left(a^{-1} \phi_{L}(u) \cup \bigcup_{b \in A \backslash\{a\}} b\left(b^{-1} \phi_{L}(u)\right)\right)
$$

Moreover, if $\phi_{L}(u)=\{\varepsilon\}$, then $u^{-1}\left(L \amalg A^{*}\right)=A^{*}$. Consequently, for evrey $a \in A, \phi_{L}(u a)=S_{\min }\left(a^{-1} u^{-1}\left(L \amalg A^{*}\right)\right)=S_{\min }\left(a^{-1} A^{*}\right)=S_{\min }\left(A^{*}\right)=\{\varepsilon\}$.

For example, consider the language $L$ given by the following automaton:


By Lemma 3.5, the shuffle ideal generated by $L$ is also generated by the words of $L$ of length less than or equal to 6 . Consequenlty $S_{\min }(L)=S_{\min }(\{b a b, b b a, a a b a$, $a a a b, b a b a b, b a b b a, b b a a b a, b b a a a b, b a b a b a, b a b a a b, a a a b a b, a a a b b a, b a a a a b, b a a a b a\})$. Now, according to Proposition 5.4, one has $S_{\min }(L)=\{b a b, b b a, a a b a, a a a b\}$.

By Proposition 5.9, we have

- $\phi_{L}(\varepsilon)=\{b a b, b b a, a a b a, a a a b\} ;$
- $\phi_{L}(a)=S_{\text {min }}(\{a b a, a a b, b a b, b b a\})=\{a b a, a a b, b a b, b b a\} ;$
- $\phi_{L}(b)=S_{\min }(\{a b, b a, a a b a, a a a b\})=\{a b, b a\} ;$
- $\phi_{L}(a a)=S_{\min }(\{a b, b a, b a b, b b a\})=\{a b, b a\} ;$
- $\phi_{L}(a b)=S_{\min }(\{b a, a b, a b a, a a b\})=\{a b, b a\} ;$
- $\phi_{L}(b a)=\phi_{L}(a a a)=\phi_{L}(a b a)=S_{\min }(\{b, b a\})=\{b\} ;$
- $\phi_{L}(b b)=\phi_{L}(a a b)=\phi_{L}(a b b)=S_{\min }(\{a, a b\})=\{a\}$;
- For all $k>0 ; \phi_{L}\left(b a a^{k}\right)=\phi_{L}\left(a^{k+3}\right)=\phi_{L}\left(a b a a^{k}\right)=S_{\min }(\{b\})=\{b\} ;$
- For all $k>0 ; \phi_{L}\left(b b b^{k}\right)=\phi_{L}\left(a a b b^{k}\right)=\phi_{L}\left(a b b b^{k}\right)=S_{\min }(\{a\})=\{a\} ;$
- For all $k>0$ and for all $u \in A^{*} ; \phi_{L}\left(b a a^{k} b u\right)=\phi_{L}\left(a^{k+3} b u\right)=\phi_{L}\left(a b a a^{k} b u\right)=$ $S_{\text {min }}(\{\varepsilon\})=\{\varepsilon\} ;$
- For all $k>0$ and for all $u \in A^{*} ; \phi_{L}\left(b b b^{k} a u\right)=\phi_{L}\left(a a b b^{k} a u\right)=\phi_{L}\left(a b b b^{k} a u\right)=$ $S_{\text {min }}(\{\varepsilon\})=\{e\} ;$
- For all $u \in A^{*} ; \phi_{L}(b a b u)=\phi_{L}(b b a u)=S_{\min }(\{\varepsilon\})=\{\varepsilon\}$.

It follows that $\mathcal{A}_{L}$ is the following automaton:


We introduce the following invariant:

$$
U(n)=\max _{L: m(L) \leq n}\left[m\left(L \amalg A^{*}\right)\right] .
$$

Proposition 5.10. One has $U(n)=O\left(2^{n}\right)$ and $U(n)=\Omega\left(\left(\frac{n}{|A|}\right)^{|A|}\right)$.
Proof. Let $\mathcal{A}$ be an $n$-state minimal automaton. The automaton Saturate $(\mathcal{A})$ has also $n$ states and accepts $L(\mathcal{A}) \amalg A^{*}$. It follows that $m\left(L(\mathcal{A}) \amalg A^{*}\right) \leq 2^{n}$. Consequently $U(n)=O\left(2^{n}\right)$.

Consider now the language $L=\bigcup_{a \in A}\left\{a^{N}\right\}$. One has $m(L)=(N-1)|A|+2$. Let $A=\left\{a_{1}, a_{2}, \cdots, a_{n}\right\}$. We claim that if $\left(k_{1}, k_{2}, \cdots, k_{n}\right)$ and $\left(\ell_{1}, \ell_{2}, \cdots, \ell_{n}\right)$ are two distinct $n$-tuples of positive integers less than or equal to $N-1$, then

$$
\left(a_{1}^{k_{1}} a_{2}^{k_{2}} \cdots a_{n}^{k_{n}}\right)^{-1}\left(L \amalg A^{*}\right) \neq\left(a_{1}^{\ell_{1}} a_{2}^{\ell_{2}} \cdots a_{n}^{\ell_{n}}\right)^{-1}\left(L \amalg A^{*}\right)
$$

Indeed, assume for example that $k_{i}>\ell_{i}$. Then $a_{i}^{N-\ell_{i}}$ belongs to the second quotient and not to the first one, proving the claim. It follows that

$$
m\left(L \amalg A^{*}\right) \geq(N-1)^{|A|}
$$

Consequently, one has $U(n)=\Omega\left(\left(\frac{n}{|A|}\right)^{|A|}\right)$.
Proposition 5.11. If $|A| \geq 2$, then $U(n)=\Omega\left(r^{\sqrt{n}}\right)$, where $r=\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{\sqrt{2}}{2}} \geq 1.39$.
Proof. Let $a$ and $b$ be two distinct letters of $A$ and $n \geq 4$. If $u$ is a word on $A$, we denote by $u^{R}$ its reverse (i.e. the word obtained by reading $u$ from the right to the left) and by $|u|_{a}$ (resp. $|u|_{b}$ ) the number of $a$ (resp. $b$ ) in $u$. We consider the following languages:

$$
L=\left\{u u^{R}\left|u \in\{a, b\}^{*},|u|_{a}=1,|u|=n\right\} \quad \text { and } \quad K=L \amalg A^{*} .\right.
$$

Since $|L|=n$ and since each word of $L$ has length $2 n$ we have $m(L) \leq 2 n^{2}$.
Now we prove that $m(K) \geq \frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n}$. Let $u$ and $v$ be two distinct words of $\{a, b\}^{*} \cap\left(\{a, b\}^{*} a a\{a, b\}^{*}\right)^{c}$ such that $|u|=|v|=n$ and $|u|_{a} \geq 2$ and $|v|_{a} \geq 2$. We claim that $u^{-1} K \neq v^{-1} K$. We may assume that $|u|_{b} \geq|v|_{b}$. One of the following cases arises:
$|u|_{b}>|v|_{b}$ : let $w=b^{n-1-|u|_{b}} a a b^{n-1} \in\left(b^{|u|_{b}}\right)^{-1} L$. Since $b^{|u|_{b}} w \in L, u w \in L$ ש $A^{*}$. Thus $w \in u^{-1} K$. Assume that $w \in v^{-1} K$. Then, $v w \in L ш A^{*}$. Thus there exists $z \prec v w$ such that $z \in L$. Consequently $|z|_{b}=2 n-2$. It follows that $|v w|_{b} \geq 2 n-2$. Therefore $|v|_{b} \geq 2 n-2-|w|_{b}=|u|_{b}$, a contradiction;
$|u|_{b}=|v|_{b}:$ since $u \neq v$, there exist $w, u_{0}$ and $v_{0}$ such that $u=w b u_{0}$ and $v=w a v_{0}$. The word $b^{|w|_{b}} a b^{|u|_{b}-|w|_{b}}$ is a subword of $v$. Let $s=$ $b^{2 n-2-|u|_{b}-|w|_{b}} a b^{|w|_{b}}$. Since $b^{|w|_{b}} a b^{|u|_{b}-|w|_{b}} s \in L, s \in v^{-1} K$. Assume that $s \in u^{-1} K$. There exists a subword $z$ of us such that $z \in L$. Since $z \in L, z$ is of the form $b^{i} a b^{2 n-2-2 i} a b^{i}$.


But $|u s|_{b}=2 n-2=|z|_{b}$, thus, since $z \prec u s, z$ is obtained from $u s$ only by deleting some $a$ 's.

Since $|u s|_{b}=|z|_{b}$, if the second $a$ of $z$ corresponds to the last $a$ of $u s$, then $i=|w|_{b}$; otherwise $i \geq 2 n-2-|u|_{b}$, which is not possible since $i \leq n-1(z \in L)$ and since $|u|_{b} \leq|u|-2 \leq n-2$. Thus $i=|w|_{b}$. Now, two cases arise:
$w \neq \varepsilon$ : since $v$ does not contain the factor $a a$, the last letter of $w$ is $b$. If the first $a$ of $z$ corresponds to an $a$ of $w$, then $i<|w|_{b}$; otherwise $i>|w|_{b}$, a contradiction;
$w=\varepsilon$ : in this case, $u s=b u_{0} b^{2 n-2-|u|_{b}} a$. Since $z$ is obtained from $u s$ only by deleting some $a$ 's, the first letter of $z$ is a $b$. But we proved that $i=|w|_{b}$, thus $z=a b^{2 n-2} a$, a contradiction.

Now we evaluate $\left|\left(\{a, b\}^{*} a a\{a, b\}^{*}\right)^{c} \cap\{a, b\}^{*} a\{a, b\}^{*} a\{a, b\}^{*} \cap\{a, b\}^{n}\right|$. For $d \in$ $\{a, b\}$, let

$$
R_{n}(d)=\left(\{a, b\}^{*} a a\{a, b\}^{*}\right)^{c} \cap\{a, b\}^{*} a\{a, b\}^{*} a\{a, b\}^{*} \cap\{a, b\}^{n} \cap\{a, b\}^{*} d
$$

We have $R_{n}(b) a \subseteq R_{n+1}(a)$ and $R_{n+1}(b)=R_{n}(a) b \cup R_{n}(b) b$ (this union is disjoint). Consequently,

$$
\begin{align*}
\left|R_{n+1}(b)\right| & =\left|R_{n}(a) b\right|+\left|R_{n}(b) b\right| \\
& =\left|R_{n}(a)\right|+\left|R_{n}(b)\right| \\
& \geq\left|R_{n-1}(b) a\right|+\left|R_{n}(b)\right| \\
& \geq\left|R_{n-1}(b)\right|+\left|R_{n}(b)\right| . \tag{*}
\end{align*}
$$

Since

$$
\left|R_{4}(b)\right|=|\{a b a b\}|=1 \geq \frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{4} \approx 0.98
$$

and since

$$
\left|R_{5}(b)\right|=|\{a b a b b, b a b a b, a b b a b\}|=3 \geq \frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{5} \approx 1.58
$$

we have, for all $n \geq 4, R_{n}(b) \geq \frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n}$. Indeed this result holds for $n=4$ and $n=5$. Moreover, by induction, for all $n \geq 5$,

$$
\begin{aligned}
\left|R_{n+1}(b)\right| & \geq\left|R_{n-1}(b)\right|+\left|R_{n}(b)\right| \quad(\text { by }(*)) \\
& \geq \frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}+\frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n} \quad(\text { by induction) } \\
& \geq \frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(1+\left(\frac{1+\sqrt{5}}{2}\right)\right) \\
& =\frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+\sqrt{5}}{2}\right)^{2} \\
& =\frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} .
\end{aligned}
$$

It follows that $m(K) \geq \frac{1}{7}\left(\frac{1+\sqrt{5}}{2}\right)^{n}$.
Since $U(n)$ is an increasing function and since $m(L) \leq 2 n^{2}$, we have

$$
U(n)=\Omega\left(r^{\sqrt{n}}\right)
$$

### 5.2. UnION AND INTERSECTION OF SHUFFLE IDEALS

Proposition 5.12. For all $n, m \geq 0$ it holds that

$$
\max _{L_{1}, L_{2}} \text { shuffle ideals }\left\{m\left(L_{1} \cup L_{2}\right) \mid m\left(L_{1}\right) \leq n, m\left(L_{2}\right) \leq m\right\}=\Theta(m n)
$$

Proof. It is a general result for regular languages that $m\left(L_{1} \cup L_{2}\right) \leq m\left(L_{1}\right) m\left(L_{2}\right)$.
For the lower bound consider the languages $L_{1}=a^{n} \amalg A^{*}$ and $L_{2}=b^{m} ш A^{*}$. One has $m\left(L_{1}\right)=n+1$ and $m\left(L_{2}\right)=m+1$.

Let $k, k^{\prime} \in\{0, \ldots, n-1\}$ and $\ell, \ell^{\prime} \in\{0, \ldots, m-1\}$. Assume that $(k, \ell) \neq\left(k^{\prime}, \ell^{\prime}\right)$. One has, for example, $k>k^{\prime}$. In this case,

$$
a^{n-k} \in\left(a^{k} b^{\ell}\right)^{-1}\left(L_{1} \cup L_{2}\right) \quad \text { and } \quad a^{n-k} \notin\left(a^{k^{\prime}} b^{\ell^{\prime}}\right)^{-1}\left(L_{1} \cup L_{2}\right)
$$

It follows that $L_{1} \cup L_{2}$ has at least $m n$ right quotients. It follows that $m\left(L_{1} \cup L_{2}\right) \geq m n$.
Proposition 5.13. For all $n, m \geq 0$ it holds that

$$
\max _{L_{1}, L_{2} \text { shuffle ideals }}\left\{m\left(L_{1} \cap L_{2}\right) \mid m\left(L_{1}\right) \leq n, m\left(L_{2}\right) \leq m\right\}=\Theta(m n)
$$

Proof. It is a general result for regular languages that $m\left(L_{1} \cap L_{2}\right) \leq m\left(L_{1}\right) m\left(L_{2}\right)$.
For the lower bound consider the languages $L_{1}=a^{n} \amalg A^{*}$ and $L_{2}=b^{m} ш A^{*}$. One has $m\left(L_{1}\right)=n+1$ and $m\left(L_{2}\right)=m+1$. Let $k, k^{\prime} \in\{1, \ldots, n\}$ and $\ell, \ell^{\prime} \in$ $\{1, \ldots, m\}$. Assume that $(k, \ell) \neq\left(k^{\prime}, \ell^{\prime}\right)$. One has, for example, $k>k^{\prime}$. In this case,

$$
a^{n-k} b^{m-\ell} \in\left(a^{k} b^{\ell}\right)^{-1}\left(L_{1} \cap L_{2}\right) \quad \text { and } \quad a^{n-k} b^{m-\ell} \notin\left(a^{k^{\prime}} b^{\ell^{\prime}}\right)^{-1}\left(L_{1} \cap L_{2}\right)
$$

It follows that $L_{1} \cap L_{2}$ has at least $m n$ right quotients. Consequently $m\left(L_{1} \cap L_{2}\right)$ $\geq m n$.

### 5.3. Product and star of shuffle ideals

Proposition 5.14. If $L$ is a shuffle ideal, then $m\left(L^{*}\right) \leq m(L)+1$.
Proof. We claim that $L^{2} \subseteq L$. Indeed if $u \in L^{2}$, one has $u=v w$ with $v \in L$ and $w \in L$. It follows that $u \in v \amalg A^{*} \subseteq L$, proving the claim.

By a direct induction, one can prove that $L^{*}=\{\varepsilon\} \cup L$. Let $\mathcal{A}=(Q, A, E, i, F)$ be the minimal automaton of $L$ and $p \notin Q$. The automaton $\mathcal{A}^{\prime}=\left(Q^{\prime}, A, E^{\prime}, p, F^{\prime}\right)$ where

$$
\begin{aligned}
& \text { - } Q^{\prime}=Q \cup\{p\} ; \\
& \text { - } E^{\prime}=E \cup\{(p, a, q) \mid(i, a, q) \in E\} \\
& \text { - } F^{\prime}=F \cup\{p\}
\end{aligned}
$$

accepts $L \cup\{\varepsilon\}$, is deterministic and has $m(L)+1$ states. It follows that $m\left(L^{*}\right)$ $\leq m(L)+1$.

We may have $m\left(L^{*}\right)<m(L)$. For example, if $L=A^{*} a A^{*} \cup A^{*} b A^{*}$ and if $A=\{a, b\}$, then $m(L)=2$. But $L^{*}=A^{*}$ and so $m\left(L^{*}\right)=1$.

Proposition 5.15. If $L_{1}$ and $L_{2}$ are non empty shuffle ideals, then

$$
m\left(L_{1} L_{2}\right)=m\left(L_{1}\right)+m\left(L_{2}\right)-1
$$

Proof. Recall that by Lemma 5.2, the minimal automaton of a shuffle ideal has a unique final state. Now let $\mathcal{A}_{1}=\left(Q_{1}, A, E_{1}, i_{1}, f_{1}\right)$ and $\mathcal{A}_{2}=\left(Q_{2}, A, E_{2}, i_{2}, f_{2}\right)$ be the minimal automata of $L_{1}$ and $L_{2}$. We may assume that $Q_{1} \cap Q_{2}=\emptyset$. Let

$$
\mathcal{A}_{3}=\left(Q_{1} \cup Q_{2} \backslash\left\{i_{2}\right\}, A, E_{3}, i_{1}, f_{2}\right)
$$

where

$$
\begin{aligned}
E_{3}= & E_{1} \backslash\left\{\left(f_{1}, a, p\right) \mid\left(f_{1}, a, p\right) \in E_{1}\right\} \\
& \cup E_{2} \backslash\left\{\left(i_{2}, a, p\right) \mid\left(i_{2}, a, p\right) \in E_{2}\right\} \\
& \cup\left\{\left(f_{1}, a, p\right) \mid\left(i_{2}, a, p\right) \in E_{2}\right\} .
\end{aligned}
$$

We claim that $\mathcal{A}_{3}$ is the minimal automaton of $L_{1} L_{2}$.

- By construction, $\mathcal{A}_{3}$ is deterministic.
- By construction $L\left(\mathcal{A}_{3}\right) \subseteq L_{1} L_{2}$. Let $u=v w \in L_{1} L_{2}$, with $v \in L_{1}$ and $w \in L_{2}$ and let $v^{\prime}$ be the shortest prefix of $v$ which is in $L_{1}$. We have $u=v^{\prime} z w$ with $v=v^{\prime} z$. Since $L_{2}$ is a shuffle ideal, $w^{\prime}=z w \in L_{2}$. By construction, one can read $v^{\prime}$ in $\mathcal{A}_{1}$ by using transitions in $E_{1} \backslash\left\{\left(f_{1}, a, p\right) \mid\left(f_{1}, a, p\right) \in E_{1}\right\}$. It follows that $v^{\prime} w^{\prime} \in L\left(\mathcal{A}_{3}\right)$, proving that $L\left(\mathcal{A}_{3}\right)=L_{1} L_{2}$.
- Now we shall prove that $\mathcal{A}_{3}$ is minimal. Let $p$ and $q$ be two states of $\mathcal{A}_{3}$ such that $p \cdot u=f_{2}$ if and only if $q \cdot u=f_{2}$ for all $u \in A^{*}$. The following cases arise:
case (1): $p$ and $q$ are in $Q_{2} \cup\left\{f_{1}\right\}$. Since $\mathcal{A}_{2}$ is minimal, $p=q$;
case (2): $p \in Q_{1}$ and $q=f_{1}$. Let $v$ be a word of $L_{2}$ of minimal length. We have $q \cdot v=f_{2}$. Thus $p \cdot v=f_{2}$. Since all paths from $p$ to $f_{2}$ go through $q$ and by the minimality of $v, p \cdot v=f_{2}$ implies $p=q$;
case (3): $p$ and $q$ are both in $Q_{1}$. Assume that there exists $u$ such that $p \cdot u=f_{1}$ and $q \cdot u \neq f_{1}$. If $q \cdot u \in Q_{1}$ we are in case (2) and $p=q$. If $q \cdot u \in Q_{2}$ we are in case (1) and $p=q$. Now if $p \cdot u=f_{1}$ if and only if $q \cdot u=f_{1}$, we have $p=q$ by minimality of $\mathcal{A}_{1}$;
case (4): $p \in Q_{1}$ and $q \in Q_{2}$. Let $v$ be a word such that $p \cdot v=f_{1}$. Using case (1), we have $q \cdot v=f_{1}$. Hence, by Proposition 5.1, we have $q=f_{1}$. Now, using case (2), we have $p=q$.
It follows that $p=q$, proving that $\mathcal{A}_{3}$ is minimal.


## 6. Shuffle ideals and Linear temporal logic

In this section we first present a temporal logic characterization of shuffle ideals. Next we study the expressive power of this fragment of temporal logic over infinite words.

### 6.1. Temporal logic on finite words

Linear temporal logic (LTL for short) on an alphabet $A$ is defined as follows [22]. The vocabulary consists of
(1) an atomic proposition $p_{a}$ for each letter $a \in A$ and the atomic propositions true and false;
(2) connectives $\vee$ and $\neg$;
(3) temporal operators X ("next"); $\mathcal{U}$ ("until");
and the formulas are constructed according to the rules
(1) atomic propositions are formulas;
(2) if $\varphi$ and $\psi$ are formulas, so are $\varphi \vee \psi, \neg \varphi, \mathrm{X} \varphi, \varphi \mathcal{U} \psi$.

The semantics is defined by induction. Given a word $u \in A^{+}$, and $n \in\{1, \ldots,|u|\}$, we say that $u$ satisfies $\varphi$ at position $n$ (denoted $(u, n) \models \varphi)$ as follows
(1) $(u, n) \models p_{a}$ if the $n$-th letter $u(n)$ of $u$ is an $a$;
(2) $(u, n) \models \varphi \vee \psi$ if $(u, n) \models \varphi$ or $(u, n) \models \psi$;
(3) $(u, n) \models \neg \varphi$ if ( $u, n$ ) does not satisfy $\varphi$;
(4) $(u, n) \models \mathrm{X} \varphi$ if $n<|u|$ and $(u, n+1) \models \varphi$;
(5) $(u, n) \models \varphi \mathcal{U} \psi$ if there exists $m$ such that $n \leq m \leq|u|,(u, m) \models \psi$ and, for every $k$ such that $n \leq k<m,(u, k) \models \varphi$.
Moreover, for all $u \in A^{+}$and all $n \in\{1, \ldots,|u|\}$ we have $(u, n) \models$ true and ( $u, n$ ) does not satisfy false.

Finally, we denote by $L(\varphi)$ the language of words $u$ such that $(u, 1)$ satisfies $\varphi$. It is known $[8,14,15,20]$ that a language $L$ is LTL-definable (i.e. there exists a LTL formula $\varphi$ such that $L=L(\varphi)$ ) if and only if $L$ is star-free. Reference [6] also gives a characterization of languages accepted by LTL formulas defined without the symbol $\mathcal{U}$.

Now we give a temporal logic characterization of shuffle ideals. For each letter $a$, we define a new temporal operator $\mathrm{F}_{a}$ and we define SLTL (Shuffle Linear Temporal Logic) formulas according to the rules
(1) true is a SLTL-formula;
(2) if $\varphi$ and $\psi$ are formulas, so are $\varphi \vee \psi, \varphi \wedge \psi, \mathrm{X} \varphi, \mathrm{F} \varphi$ and $\mathrm{F}_{a} \varphi$.

The semantics is defined as for LTL and by letting:

$$
\begin{aligned}
& (u, n) \models \varphi \wedge \psi \text { if }(u, n) \models \neg(\neg \varphi \vee \neg \psi) ; \\
& (u, n) \models \mathrm{F} \varphi \text { if }(u, n) \models \operatorname{true} \mathcal{U} \varphi ; \\
& (u, n) \models \mathrm{F}_{a} \varphi \quad \text { if } \quad(u, n) \models \mathrm{F}\left(p_{a} \wedge(\mathrm{X} \varphi)\right) .
\end{aligned}
$$

A SLTL ${ }^{-}$-formula is a SLTL-formula that uses true and the operators $\vee$ and $\mathrm{F}_{a}$. A language $L$ is SLTL-definable [resp. SLTL--definable] if there exists a SLTLformula (resp. SLTL $^{-}$-formula) $\varphi$ such that $L=L(\varphi)$.

Theorem 6.1. Let $L \subseteq A^{+}$. The following assertions are equivalent.
(1) L is SLTL-definable.
(2) $L$ is $S L T L^{-}$-definable.
(3) $L$ is a shuffle ideal.

To prove this theorem we need the following lemma:
Lemma 6.2. If $L$ is a shuffle ideal, then $A L$ and $A^{*} L$ are shuffle ideals.
Proof. Since the product of two shuffle ideals is a shuffle ideal, $A^{*} L$ is a shuffle ideal.

Since $A A^{*}=A^{*} A A^{*}$, by Theorem $1.2, A L$ is a shuffle ideal. The same argument holds for $L A$.

We can now prove Theorem 6.1.

Proof. It is clear that (2) implies (1).
Now we shall prove that (1) implies (3). Let $\psi$ be a SLTL-formula. We prove by induction on $\psi$ that $L(\psi)$ is a shuffle ideal.

- $L$ (true $)=A^{+}=A^{*} A A^{*}$ is a shuffle ideal.
- If $\psi=\varphi_{1} \vee \varphi_{2}$ (resp. $\psi=\varphi_{1} \wedge \varphi_{2}$ ) where $L\left(\varphi_{1}\right)$ and $L\left(\varphi_{2}\right)$ are shuffle ideals, then $L(\psi)$ is a shuffle ideal because the union (resp. intersection) of two shuffle ideals is a shuffle ideal.
- If $\psi=\mathrm{F} \varphi$ where $L(\varphi)$ is a shuffle ideal, then $L(\psi)=A^{*} L(\varphi)$ is a shuffle ideal (by Lem. 6.2).
- If $\psi=\mathrm{X} \varphi$ where $L(\varphi)$ is a shuffle ideal, then $L(\psi)=A L(\varphi)$ is a shuffle ideal (by Lem. 6.2).
- If $\psi=\mathrm{F}_{a} \varphi$ where $L(\varphi)$ is a shuffle ideal, then $L(\psi)=A^{*}\left(a A^{*} \cap A L(\varphi)\right)=$ $A^{*} a L(\varphi)$ is a shuffle ideal.
To finish the proof, we prove that (3) implies (2). Let $a$ be in $A$. We have $L\left(\mathrm{~F}_{a}\right.$ true $)=A^{*} a A^{*}$. By a direct induction we have

$$
L\left(\mathrm{~F}_{a_{1}} \mathrm{~F}_{a_{2}} \cdots \mathrm{~F}_{a_{k}} \text { true }\right)=A^{*} a_{1} A^{*} a_{2} A^{*} \cdots A^{*} a_{k} A^{*}
$$

It follows that every shuffle ideal of $A^{+}$is SLTL ${ }^{-}$-definable.

The above proof is constructive: given a shuffle ideal by a polynomial rational expression, one can compute a SLTL--formula representing it, and given a SLTLformula one can construct the shuffle ideal it represents.

### 6.2. TEMPORAL LOGIC OVER INFINITE WORDS

One can also define a semantic for LTL for infinite words. If $\sigma$ is an infinite word, we denote by $\sigma(i)$ its $i$-th letter. The semantic for LTL is the following:
(1) $(\sigma, n) \models p_{a}$ if $\sigma(n)=a$. Moreover $(\sigma, n) \models$ true and $(\sigma, n)$ does not satisfy false;
(2) $(\sigma, n) \models \varphi \vee \psi$ if $(\sigma, n) \models \varphi$ or $(\sigma, n) \models \psi$;
(3) $(\sigma, n) \models \neg \varphi$ if ( $\sigma, n$ ) does not satisfy $\varphi$;
(4) $(\sigma, n) \models \mathrm{X} \varphi$ if $(\sigma, n+1) \models \varphi$;
(5) $(\sigma, n) \models \varphi \mathcal{U} \psi$ if there exists $m$ such that $n \leq m,(\sigma, m) \vDash \psi$ and, for every $k$ such that $n \leq k<m,(\sigma, k) \models \varphi$;
Finally, we denote by $L_{\omega}(\varphi)$ the language of infinite words $\sigma$ such that $(\sigma, 1)$ satisfies $\varphi$. As for languages of finite words, we say that an $\omega$-language $L$ is SLTL (resp. SLTL ${ }^{-}$) recognizable if there exists a SLTL-formula (resp. a SLTL ${ }^{-}$formula) $\varphi$ such that $L=L_{\omega}(\varphi)$.

Proposition 6.3. Let $\psi$ be a SLTL-formula. Then

$$
L_{\omega}(\psi)=L(\psi) A^{\omega} .
$$

Proof. We proceed by induction on the formula $\psi$.

- $L_{\omega}($ true $)=A^{\omega}=A^{*} A^{\omega}=L($ true $) A^{\omega}$.
- If $\psi=\varphi_{1} \vee \varphi_{2}$ where $L_{\omega}\left(\varphi_{1}\right)=L\left(\varphi_{1}\right) A^{\omega}$ and $L_{\omega}\left(\varphi_{2}\right)=L\left(\varphi_{2}\right) A^{\omega}$, then $L_{\omega}(\psi)=L_{\omega}\left(\varphi_{1}\right) \cup L_{\omega}\left(\varphi_{2}\right)=L\left(\varphi_{1}\right) A^{\omega} \cup L\left(\varphi_{2}\right) A^{\omega}=\left(L\left(\varphi_{1}\right) \cup L\left(\varphi_{2}\right)\right) A^{\omega}=$ $L(\psi) A^{\omega}$.
- If $\psi=\mathrm{F} \varphi$ where $L_{\omega}(\varphi)=L(\varphi) A^{\omega}$, then $L_{\omega}(\psi)=A^{*} L_{\omega}(\varphi)=A^{*} L(\varphi) A^{\omega}=$ $L(\mathrm{~F} \varphi) A^{\omega}=L(\psi) A^{\omega}$.
- If $\psi=\mathrm{X} \varphi$ where $L_{\omega}(\varphi)=L(\varphi) A^{\omega}$, then $L_{\omega}(\psi)=A L_{\omega}(\varphi)=A L(\varphi) A^{\omega}=$ $L(\mathrm{X} \varphi) A^{\omega}=L(\psi) A^{\omega}$.
- If $\psi=\varphi_{1} \wedge \varphi_{2}$ where $L_{\omega}\left(\varphi_{1}\right)=L\left(\varphi_{1}\right) A^{\omega}$ and $L_{\omega}\left(\varphi_{2}\right)=L\left(\varphi_{2}\right) A^{\omega}$, then $L_{\omega}(\psi)=L_{\omega}\left(\varphi_{1}\right) \cap L_{\omega}\left(\varphi_{2}\right)=L\left(\varphi_{1}\right) A^{\omega} \cap L\left(\varphi_{2}\right) A^{\omega}=\left[L\left(\varphi_{1}\right) A^{*} \cap L\left(\varphi_{2}\right)\right] A^{\omega} \cup$ $\left[L\left(\varphi_{1}\right) \cap L\left(\varphi_{2}\right) A^{*}\right] A^{\omega}$. But $L\left(\varphi_{1}\right) A^{*}=L\left(\varphi_{1}\right)$ and $L\left(\varphi_{2}\right) A^{*}=L\left(\varphi_{2}\right)$. Consequently $L_{\omega}(\psi)=L(\psi) A^{\omega}$.
- If $\psi=\mathrm{F}_{a} \varphi$ where $L_{\omega}(\varphi)=L(\varphi) A^{\omega}$, then $L_{\omega}(\psi)=A^{*} L_{\omega}\left(p_{a} \wedge \mathrm{X} \varphi\right)=$ $A^{*} a L_{\omega}(\varphi)=A^{*} a L(\varphi) A^{\omega}=L\left(\mathrm{~F}_{a} \varphi\right) A^{\omega}=L(\psi) A^{\omega}$.

Lemma 6.4. Let $\mathcal{A}=(Q, A, E, I, F)$ be a saturated automaton. We have

$$
L_{\omega}(\mathcal{A})=L(\mathcal{A}) A^{\omega}
$$

Proof. For an automaton we always have $L_{\omega}(\mathcal{A}) \subseteq L(\mathcal{A}) A^{\omega}$.
Let $u$ be in $L(\mathcal{A})$ and $\sigma$ in $A^{\omega}$. There exist $i \in I$ and $f \in F$ such that $f \in i \cdot u$. Since $\mathcal{A}$ is saturated, for each prefix $s$ of $\sigma, f \in i \cdot u s$. Consequently $u \sigma \in L_{\omega}(\mathcal{A})$, proving that $L(\mathcal{A}) A^{\omega} \subseteq L_{\omega}(\mathcal{A})$.

Theorem 6.5. Let $K$ be an $\omega$-language of $A^{\omega}$. The following conditions are equivalent:
(1) $K$ is SLTL-recognizable;
(2) $K$ is $S L T L^{-}$-recognizable;
(3) There exists a shuffle ideal $L$ such that $K=L A^{\omega}$;
(4) $K$ is accepted by a locally trivial, saturated Büchi-automaton ;
(5) $K$ is accepted by a saturated Büchi-automaton.

Proof. By Theorem 6.1 and Proposition 6.3, (1) implies (3).
It is clear that (2) implies (1).
Now let $L$ be a shuffle ideal such that $K=L A^{\omega}$. By Theorem 6.1, there exists a SLTL $^{-}$-formula $\varphi$ such that $L=L(\varphi)$. Thus, by Proposition 6.3, $L_{\omega}(\varphi)=L A^{\omega}=$ $K$. Therefore, (3) implies (2).

The equivalence between $(3,4)$ and $(5)$ is a direct consequence of Lemma 6.4 and Theorem 2.1.

Acknowledgements. The author wishes to thank Ines Klimann and Anca Muscholl for many contributions and comments about this paper. The author also wishes to thank the anonymous referees for helpful and constructive suggestions.

## References

[1] A. Aho, J. Hopcroft and J. Ullman, The design and analysis of computer algorithms. Addison-Wesley (1974) 395-400.
[2] J. Almeida, Implicit operations on finite $\mathcal{J}$-trivial semigroups and a conjecture of I. Simon. J. Pure Appl. Algebra 69 (1990) 205-218.
[3] M. Arfi, Opération polynomiales et hiérarchies de concaténation. Theoret. Comput. Sci. 91 (1991) 71-84.
[4] J. Berstel and L. Boasson, Shuffle factorization is unique, Technical Report. LIAFA, Université Paris 7 (1999).
[5] J. Berstel, Transductions and context-free languages. Teubner (1979) Verlag.
[6] J. Cohen, D. Perrin and J.-E. Pin, On the expressive power of temporal logic for finite words. J. Comput. System Sci. 46 (1993) 271-294.
[7] S. Eilenberg, Automata, Languages and Machines, Vol. A. Academic Press (1974).
[8] D. Gabbay, A. Pnueli, S. Shelah and J. Stavi, On the temporal analysis of fairness, in 12 th ACM Symp. on Principles of Programming Languages (1980) 163-180.
[9] C. Glasser and H. Schmidt, Level 5/2 of the straubing-thérien hierarchy for two-letter alphabets, in Conference on Developments in Language Theory (DLT). Vienna (2001).
[10] P.-C. Héam, Some complexity results for polynomial rational expressions. Theoret. Comput. Sci. (to appear).
[11] G. Higman, Ordering by divisibility in abstract algebras, in Proc. of the London Mathematical Society, Vol. 2 (1952) 326-336.
[12] C. Hagenah and A. Muscholl, Computing $\epsilon$-free nfa from regular expressions in $O\left(n \log ^{2}(n)\right)$ time. RAIRO: Theoret. Informatics Appl. 34 (2000) 257-277.
[13] J. Hopcroft and J. Ullman, Introduction to automata theory, languages, and computation. Addison-Wesley (1980).
[14] J.A. Kamp, Tense logic and the theory of linear order, Ph.D. Thesis. University of California, Los Angeles (1968).
[15] O. Katai, Completeness and the expressive power of next time temporal logical system by semantic tableau method, Technical Report RR-0109. Inria, Institut National de Recherche en Informatique et en Automatique (1981).
[16] S.C. Kleene, Representation of events in nerve nets and finite automata. Princeton University Press, Automata Studies (1956) 3-42.
[17] M. Lothaire, Combinatorics on words. Cambridge Mathematical Library (1983).
[18] M. Nivat, G.D.S. Ramkumar, C. Pandu Rangan, A. Saoudi and R. Sundaram, Efficient parallel shuffle recognition. Parallel Process. Lett. 4 (1994) 455-463.
[19] C.H. Papadimitriou, Computational complexity. Addison Wesley (1994).
[20] M. Parigot, Automates, réseaux, formules, in Actes des journées "Informatiques et Mathématiques". Luminy (1984).
[21] B. Pradeep, C. Murthy and S. Ram, A constant time string shuffle algorithm on reconfigurable meshes. Int. J. Comput. Math. 68 (1998) 251-259.
[22] A. Pnueli, The temporal logic of programs, in 18th FOCS (1977) 46-57.
[23] J.-E. Pin and P. Weil, Polynomial closure and unambiguous product. Theory Comput. Systems 30 (1997) 1-39.
[24] D.E. Radford, A natural ring basis for shuffle algebra and an application to group schemes. J. Algebra 58 (1979) 432-454.
[25] I. Simon, Piecewise testable events, in GI Conf. Springer-Verlag, Lecture Notes in Comput. Sci. 33 (1975) 214-222.
[26] J.-C. Spehner, Le calcul rapide des mélanges de deux mots. Theoret. Comput. Sci. 47 (1986) 181-203.
[27] H. Straubing and D. Thérien, Partially ordered finite monoids and a theorem of I. Simon. J. Algebra 119 (1985) 161-183.
[28] J. Stern, Characterization of some classes of regular events. Theoret. Comput. Sci. 35 (1985) 17-42.
[29] H. Straubing, Finite semigroups varieties of the form V $*$ D. J. Pure Appl. Algebra 36 (1985) 53-94.
[30] D. Thérien, Classification of finite monoids: The language approach. Theoret. Comput. Sci. 14 (1981) 195-208.
[31] W. Thomas, Classifying regular events in symbolic logic. J. Comput. System Sci. 25 360375.
[32] D. Thérien and Th. Wilke, Temporal logic and semidirect products: An effective characterization of the until hierarchy, in Proc. of the 37th Annual Symposium on Foundations of Computer Science. IEEE (1996) 256-263.
[33] Th. Wilke, Classifying discrete temporal properties, in STACS'99. Springer-Verlag, Lecture Notes in Comput. Sci. 1563 (1999) 32-46.
[34] S. Yu, State complexity of regular languages, in Proc. of the International Workshop on Descriptional Complexity of Automata, Grammars and Related Structures (1999) 77-88.

Communicated by J.-E. Pin.
Received November, 2001. Accepted October, 2002.

[^1]
[^0]:    * This work was done while the author was at LIAFA, Université Paris 7.
    ${ }^{1}$ Laboratoire d'Informatique de Franche-Comté, Université de Franche-Comté, 16 route de Gray, 25030 Besancon Cedex, France; e-mail: heampc@lifc.univ-fcomte.fr
    (C) EDP Sciences 2003

[^1]:    To access this journal online:
    www.edpsciences.org

