Enumeration of nondeterministic automata for a given language: a technique that avoids the universal automaton

J.-M. Champarnaud and F. Coulon

LIFAR, University of Rouen, France,
{Jean-Marc.Champarnaud,Fabien.Coulon}@univ-rouen.fr

Abstract. Our aim is to enumerate all NFAs (nondeterministic finite automata) that recognize a given regular language $\mathcal{L}$. More precisely, we produce a set $\mathbb{A}$ of automata such that each automaton A recognizing $\mathcal{L}$ appears in $\mathbb{A}$ up to the merging of some states and the addition of some transitions, that is, there is a surjective morphism that maps A onto an automaton of $\mathbb{A}$. We provide a common theoretical framework, based on morphism properties, to previous works of Kameda and Weiner (1970), and of Sengoku (1992), whose issue is the minimization of NFAs. Our paper gives two non comparable enumeration techniques. Both proceed by enumerating a specific class of grid covers of the automaton map. The first one is related to the canonical automaton introduced by Carrez. The second one is based on new outcomes related to the relationship between grid covers and their projections.

Introduction

Nondeterministic automata engineering is at the origins of a flood of applications in computer science, such as pattern matching, software verification and many others. This paper deals with the enumeration of all NFAs (nondeterministic finite automata) that recognize a given regular language. This problem plays a significant role in NFA algorithmics and it involves specific structures related to automata such as grid covers [8] that are widely studied here. This problem derives from a former one that is the search of minimal NFAs (minimal w.r.t. number of states) for a regular language. Contrary to deterministic automata (DFAs), there may be several non isomorphic automata being minimal w.r.t. number of states. We distinguish the minimization from the reduction problem. The reduction consists in finding an automaton smaller than the one given as input. Minimization is known to be a NP-hard problem [7], even though many ways of reduction have been investigated, like some polynomial heuristics in [4].

However, a full minimization is possible for a given language as soon as we have some practical means of enumerating NFAs that recognize it, and heuristics can use a process of partial enumeration.

Our study draws a parallel between automata and grid covers of the language's reduced automaton map (RAM), which have been described by Kameda

and Weiner in [8]. The underlying idea is to associate each automaton with one grid cover of the language's RAM. The automaton can be recovered with no ambiguity from its associated grid cover (up to the merging of some states and the addition of some transitions). So, one can enumerate automata recognizing a given language by enumerating all the grid covers of its RAM. Unfortunately, this process is prohibitive, or at least, inefficient. Hence we are searching for particular classes of grid covers, as small as possible, which enable the enumeration of all the NFAs recognizing the language. More precisely, if $\mathbb{A}$ is the set of produced automata, then for all automata A recognizing the language, there exists a surjective morphism that maps A onto an automaton of $\mathbb{A}$.

In this paper, we give two classes of such grid covers. The first one is related to the canonical automaton, and the second one is based on new outcomes concerning the relationship between grid covers and their projections. The first part concerning the canonical automaton is a reminder of already known outcomes from Carrez [3], and Arnold *et al.* [1]. The canonical automaton is also underlying in the early work of Kameda and Weiner [8]. Their specific approach is the main link between the canonical automaton and our second class of grid covers. This second class is our main contribution. We give a specification on right projections of grid covers that fully characterizes the class of enumeration. This specification is easily implementable and does not require to build the entire canonical automaton, whose space complexity is exponential. The possibility to bypass the exponential complexity is the main difference between our work and the work of Sylvain Lombardy *et al.* [9] concering the canonical automaton. The idea of using a right projection of grid covers appears in the thesis of Sengoku [11].

Sections 1 and 2 introduce a general background for studying the relationship between automata and grid covers. Sections 3 and 4 provide two enumeration techniques based on two different classes of grid covers.

1 Definitions and Properties

We assume that the reader is familiar with regular languages and automata theory [12]. We just introduce some notations.

We consider a finite alphabet Σ. Let $A = <Q, \Sigma, \delta, I, F>$ be an automaton. The *left language* of a state $q \in Q$ is denoted $\overleftarrow{\mathcal{L}}^A(q)$ and defined by $\overleftarrow{\mathcal{L}}^A(q) = \{w \in \Sigma^* \mid q \in \delta(I, w)\}$. The *right language* of a state $q \in Q$ is denoted $\overrightarrow{\mathcal{L}}^A(q)$ and defined by $\overrightarrow{\mathcal{L}}^A(q) = \{w \in \Sigma^* \mid \delta(q, w) \cap F \neq \emptyset\}$.

Let $w = a_1 a_2 \cdots a_n$ be a word of Σ^n, we define $\overline{w} = a_n a_{n-1} \cdots a_1$. We also define the *reverse* of A as $\overline{A} = <Q, \Sigma, \overline{\delta}, F, I>$, where $q' \in \overline{\delta}(q, a) \Leftrightarrow q \in \delta(q', a)$ ($\forall q, q' \in Q, a \in \Sigma$).

Let $A = <Q, \Sigma, \delta, I, F>$ and $A' = <Q', \Sigma, \delta', I', F'>$ be two automata. A morphism from A to A' is a mapping φ from Q to Q' such that $\varphi(I) \subseteq I'$, $\varphi(F) \subseteq F'$, and for all $q, p \in Q$ and $a \in \Sigma$, $p \in \delta(q, a) \Longrightarrow \varphi(p) \in \delta'(\varphi(q), a)$.

1.1 Characteristic events

All the notions that appear in this Section are from [8] with slight modifications.

We consider a regular language $\mathcal{L}$. Let $\mathcal{A} = < Q_\mathcal{A}, \Sigma, \delta_\mathcal{A}, 1, F_\mathcal{A} >$ be the minimal complete DFA of $\mathcal{L}$, where $Q_\mathcal{A} = \{1, \ldots, n\}$ is the set of states. Let $\mathcal{B} = < Q_\mathcal{B}, \Sigma, \delta_\mathcal{B}, q_1, F_\mathcal{B} > = Det(\overline{\mathcal{A}})$ obtained from the reverse of $\mathcal{A}$ by subset determinization. The automaton $\mathcal{B}$ is made complete by eventually adding a sink state, so that it is also a minimal complete DFA [2]. States of $\mathcal{B}$ are arbitrarily ordered and named q_i ($1 \leq i \leq n_b$). Each q_i is a subset of $Q_\mathcal{A}$, and q_1 is initial. As in [8], we define the RAM of the language $\mathcal{L}$, that is unique up to a permutation of rows and columns:

Definition 1 ([8]) *The reduced automaton map (RAM) associated with $\mathcal{L}$, denoted M, contains n rows and n_b columns. The element at the intersection of the ith row and the jth column is defined by*

$$M_{i,j} = 1 \ if \ i \in q_j$$
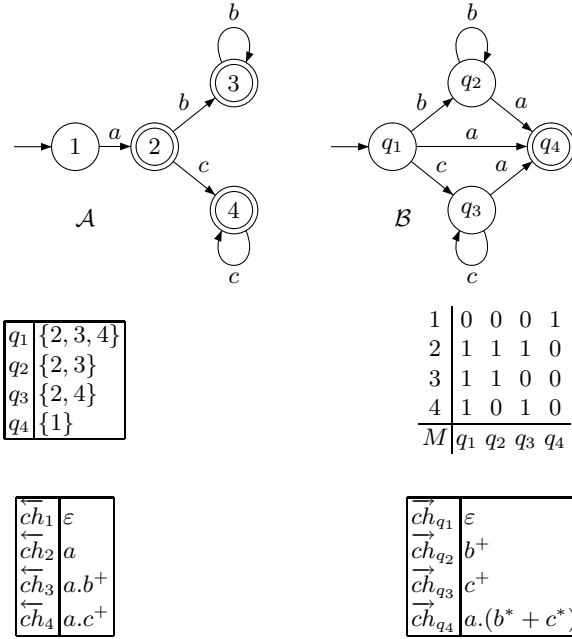$$= 0 \ otherwise$$

Fig. 1. Automata $\mathcal{A}$ and $\mathcal{B}$ for the language $a(b^* + c^*)$, the associated RAM M, and the associated characteristic events.

Definition 2 ([8]) Characteristic left events *of the language $\mathcal{L}$ are the languages $\overleftarrow{ch}_i = \overleftarrow{\mathcal{L}}^\mathcal{A}(i)$ ($1 \leq i \leq n$), while* characteristic right events *of $\mathcal{L}$ are*

the languages $\overrightarrow{ch}_{q_j} = \overline{\overleftarrow{\mathcal{L}}^{\mathcal{B}}(q_j)}$ $(1 \leq j \leq n_b)$. Let $L \subseteq \{1, \ldots, n\}$ and $R \subseteq \{q_1, \ldots, q_{n_b}\}$, we note $\overleftarrow{ch}_L$ (resp. $\overrightarrow{ch}_R$) instead of $\bigcup_{l \in L} \overleftarrow{ch}_l$ (resp. $\bigcup_{r \in R} \overrightarrow{ch}_r$).

Proposition 1 ([8])

1. Left (resp. right) characteristic events of $\mathcal{L}$ are pairwise disjoint.
2. Let $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, n_b\}$, we have $\overleftarrow{ch}_i \cdot \overrightarrow{ch}_{q_j} \subseteq \mathcal{L} \Longleftrightarrow M_{i,j} = 1$.

Definition 3 *Let q be a state of an automaton A that recognizes $\mathcal{L}$. A set $\lambda(q)$ of characteristic left events and a set $\rho(q)$ of characteristic right events are associed with q by letting:*

$$\lambda(q) = \{i \in \{1, \ldots, n\} \mid \overleftarrow{ch}_i \cap \overleftarrow{\mathcal{L}}^A(q) \neq \emptyset\}$$

$$\rho(q) = \{q_j \in \{q_1, \ldots, q_{n_b}\} \mid \overrightarrow{ch}_{q_j} \cap \overrightarrow{\mathcal{L}}^A(q) \neq \emptyset\}$$

Definition 4 ([8]) *A grid in the RAM M is a pair $[L, R]$ where L is a subset of $\{1, \ldots, n\}$, R is a subset of $\{q_1, \ldots, q_{n_b}\}$, and for all $i \in L$ and $q_j \in R$, we have $M_{i,j} = 1$. The set of all grids in M is denoted $\mathcal{G}_M$.*

Definition 5 *Let us define some external operations over the states of $\mathcal{A}$ and $\mathcal{B}$. Let $L \subseteq \{1, \ldots, n\}$, $R \subseteq \{q_1, \ldots, q_{n_b}\}$, and $a \in \Sigma$,*

$$L.a = \delta_{\mathcal{A}}(L, a), \quad L.a^{-1} = \delta_{\mathcal{A}}^{-1}(L, a)$$
$$a.R = \delta_{\mathcal{B}}(R, a), \quad a^{-1}.R = \delta_{\mathcal{B}}^{-1}(R, a)$$

The transitions of automata $\mathcal{A}$ and $\overline{\mathcal{B}}$ can be considered as inclusion relations between characteristic events:

Proposition 2 ([8]) *Let $q, p \in \{1, \ldots, n\}$ and $a \in \Sigma$, there exists a transition $q \xrightarrow{a} p$ in $\mathcal{A}$ if and only if $\overleftarrow{ch}_q \cdot a \subseteq \overleftarrow{ch}_p$. The transition $q_i \xrightarrow{a} q_j$ exists in $\mathcal{B}$ if and only if $a \cdot \overrightarrow{ch}_{q_i} \subseteq \overrightarrow{ch}_{q_j}$.*

Proof — In the one hand, we have

$$\overleftarrow{ch}_q \cdot a \subseteq \overleftarrow{ch}_p \Longleftrightarrow \overleftarrow{\mathcal{L}}^A(q) \cdot a \subseteq \overleftarrow{\mathcal{L}}^A(p)$$

Since $\mathcal{A}$ is deterministic, this is equivalent to $p \in \delta(q, a)$.

In the other hand,

$$a \cdot \overrightarrow{ch}_{q_i} \subseteq \overrightarrow{ch}_{q_j} \Longleftrightarrow \overleftarrow{\mathcal{L}}^{\mathcal{B}}(q_i) \cdot a \subseteq \overleftarrow{\mathcal{L}}^{\mathcal{B}}(q_j)$$

Since $\mathcal{B}$ is deterministic, this is equivalent to $q_j \in \delta_{\mathcal{B}}(q_i, a)$. ∎

2 Grid covers

Definition 6 *A grid cover of the RAM M is a set C of grids that covers M in the sense that for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, n_b\}$ such that $M_{i,j} = 1$, there exists $[L, R] \in C$ with $i \in L$ and $q_j \in R$.*

2.1 Relationship between automata and grid covers

Definition 7 *Let $A = <Q, \Sigma, \delta, I, F>$ be an automaton that recognizes $\mathcal{L}$. We define the grid cover $G(A)$ associated with A by letting $G(A) = \{[\lambda(q), \rho(q)] \mid q \in Q\}$.*

Conversely, there exist different ways to define an automaton associated with a grid cover. In particular, Kameda and Weiner achieve their aim by using an operation that is a reverse of the subset determinization, namely, the *intersection rule*. It consists in creating a transition labelled by a from the grid $[L_1, R_1]$ to the grid $[L_2, R_2]$ if $L_1.a \subseteq L_2$. That is, only the left parts of grids are considered. We shall see that we obtain very coherent results by simultaneously considering left and right parts of the grids.

Definition 8 *Let C be a grid cover of the RAM M. We let $\overrightarrow{C}$ be the automaton associated with C, defined by $\overrightarrow{C} = <C, \Sigma, \delta_C, I_C, F_C>$, where*

1. *$(\ \forall [L_1, R_1] \in C, a \in \Sigma\ )\quad \delta_C([L_1, R_1], a) = \{[L_2, R_2] \in C \mid a.R_2 \subseteq R_1 \wedge L_1.a \subseteq L_2\}$,*
2. *$I_C = \{[L, R] \in C \mid 1 \in L\}$,*
3. *$F_C = \{[L, R] \in C \mid q_1 \in R\}$.*

Notice that the left (resp. right) language of a grid $[L, R]$ in $\overrightarrow{C}$ is not necessarily equal to $\overleftarrow{ch}_L$ (resp. $\overrightarrow{ch}_R$). Nevertheless, the following inclusion holds.

Proposition 3 ([8]) *Let C be a grid cover of the RAM M. For each grid $[L, R] \in C$, we have $\overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R]) \subseteq \overleftarrow{ch}_L$ and $\overrightarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R]) \subseteq \overrightarrow{ch}_R$.*

Proof — From the definition of $\overrightarrow{C}$, $\varepsilon \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R])$ implies $1 \in L$, and we get $\varepsilon \in \overleftarrow{ch}_L$. We shall prove by induction on the length of the word w that $w \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R])$ implies $w \in \overleftarrow{ch}_L$. Let $n \in \mathbb{N}$, and $wa \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R]) \cap \Sigma^{n+1}$, where $w \in \Sigma^n$ and $a \in \Sigma$. Hence there exists $[L_1, R_1] \in C$ with $w \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L_1, R_1])$ such that $[L_1, R_1] \xrightarrow{a} [L, R]$ in $\overrightarrow{C}$, thence $L_1.a \subseteq L$. By induction, we have $w \in \overleftarrow{ch}_{L_1}$, then $wa \in \overleftarrow{ch}_{L_1.a}$ and yet $wa \in \overleftarrow{ch}_L$.

We go about things in a symmetrical way for the second condition. ∎

Proposition 4 *Let A be an automaton that recognizes $\mathcal{L}$. The automaton $\overrightarrow{G(A)}$ is equivalent to A. Moreover, the function that maps each state q of A to the grid $[\lambda(q), \rho(q)]$, considered as a state of $\overrightarrow{G(A)}$, is a surjective automaton morphism.*

Proof — Suppose there exists a transition $q_1 \xrightarrow{a} q_2$ in A. We necessarily have $\overleftarrow{\mathcal{L}}(q_1) \cdot a \subseteq \overleftarrow{\mathcal{L}}(q_2)$ and $a \cdot \overrightarrow{\mathcal{L}}(q_2) \subseteq \overrightarrow{\mathcal{L}}(q_1)$. Let us prove that the transition $[\lambda(q_1), \rho(q_1)] \xrightarrow{a} [\lambda(q_2), \rho(q_2)]$ exists in $\overrightarrow{G(A)}$, that is, we have to prove $\lambda(q_1).a \subseteq \lambda(q_2)$ and $a.\rho(q_2) \subseteq \rho(q_1)$. Indeed, let $ch_1 \in \lambda(q_1)$. By definition of λ, ch_1 intersects $\overleftarrow{\mathcal{L}}(q_1)$: there is a $w \in ch_1 \cap \overleftarrow{\mathcal{L}}(q_1)$. Then $wa \in \overleftarrow{\mathcal{L}}(q_2) \cap ch_1.a$. There is

a unique characteristic event ch_1' that contains $ch_1.a$ because of Proposition 2, so that $ch_1' \in \lambda(q_2)$. This proves $\lambda(q_1).a \subseteq \lambda(q_2)$. Now let $ch_2 \in rho(q_2)$. There is a $w \in ch_2 \cap \overrightarrow{\mathcal{L}}(q_2)$. Then $aw \in \overrightarrow{\mathcal{L}}(q_1)$, and the unique characteristic right event ch_2' that contains $a.ch_2$ is in $\rho(q_1)$.

It can also be seen that the set of initial (resp. final) states of A is mapped into the set of initial (resp. final) states of $\overrightarrow{G(A)}$. Then the mapping is a morphism, and $\mathcal{L}(A) \subseteq \mathcal{L}(\overrightarrow{G(A)})$. The reverse inclusion is deduced from Proposition 3. ■

Definition 9 *Let A be an NFA recognizing $\mathcal{L}$, A is said to be a* saturated *NFA if it is isomorphic to $\overrightarrow{G(A)}$.*
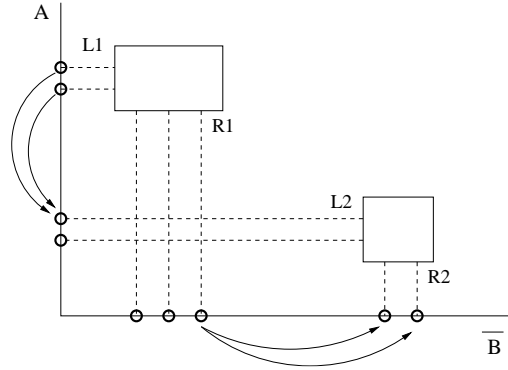

Fig. 2. Representation of two grids linked by a transition.

Now, let us give an intuitive representation of all these objects. Figure 2 represents two grids of a RAM M. The different positions on the vertical axis are the states of $\mathcal{A}$: remind that they are bijectively associated with left characteristic events. Moreover, we have a transition $q \xrightarrow{a} p$ in $\mathcal{A}$ if and only if $\overleftarrow{ch_q}.a \subseteq \overleftarrow{ch_p}$. The different positions on the horizontal axis are the states of $\overline{\mathcal{B}}$: they are bijectively associated with the right characteristic events, and we have a transition $q_i \xrightarrow{a} q_j$ in $\overline{\mathcal{B}}$ if and only if $a \cdot \overrightarrow{ch_{q_j}} \subseteq \overrightarrow{ch_{q_i}}$. The condition $L_1.a \subseteq L_2$ (resp. $a.R_2 \subseteq R_1$) is visualized on Figure 2 by the fact that each transition outgoing from L_1 is entering L_2 (resp. each transition entering R_2 is outgoing from R_1).

2.2   Different classes of covers

The following definition of legitimate covers is close to the one given by Kameda and Weiner. Together with legitimate covers, we introduce the class of tight covers and the class of prime covers.

Definition 10

1. *A cover C is said to be* legitimate *if $\overrightarrow{C}$ recognizes $\mathcal{L}$.*
2. *A cover C is said to be* tight *if $G(\overrightarrow{C}) = C$.*
3. *A cover C is said to be* prime *if every grid $[L, R]$ in C is prime, that is, if*

$$(\ \forall [L', R'] \in \mathcal{G}_M \ ) \quad L \subseteq L' \wedge R \subseteq R' \Longrightarrow [L, R] = [L', R']$$

Proposition 5

1. *A tight cover is legitimate.*
2. *A cover C is tight if and only if*

$$(\ \forall [L, R] \in C \ ) \quad \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R]) = \overleftarrow{ch}_L \ \wedge \ \overrightarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R]) = \overrightarrow{ch}_R$$

3. *A cover C is tight if and only if the two following conditions are satisfied:*
   (i) For all grids $[L_2, R_2] \in C$ and all $a \in \Sigma$, for all $l \in L_2.a^{-1}$, there exists $[L, R] \in C$ such that $l \in L$, $L.a \subseteq L_2$ and $a.R_2 \subseteq R$,
   (ii) For all grids $[L, R] \in C$ and all $a \in \Sigma$, for all $r' \in a^{-1}.R$, there exists $[L_2, R_2] \in C$ such that $r' \in R_2$, $L.a \subseteq L_2$ and $a.R_2 \subseteq R$.

Proof — (1) Let C be a tight cover and $uv \in \mathcal{L}$. Their exists $i \in \{1, \ldots, n\}$ and $j \in \{q_1, \ldots, q_{n_b}\}$ such that $u \in \overleftarrow{ch}_i$ and $v \in \overrightarrow{ch}_{q_j}$. Since $G(\overrightarrow{C}) = C$, there exists $[L, R] \in G(\overrightarrow{C})$ such that $i \in L$ and $j \in R$, hence $u \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R])$ and $v \in \overrightarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R])$.

(2) The mapping $[L, R] \mapsto (\overleftarrow{ch}_L, \overrightarrow{ch}_R)$ is clearly injective: the characteristic events are pairwise disjoint. Hence we have $G(\overrightarrow{C}) = C$ iff for all $[L, R] \in C$, $\overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R]) = \overleftarrow{ch}_L$ and $\overrightarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R]) = \overrightarrow{ch}_R$.

(3) Let C be a tight grid cover, $[L_2, R_2] \in C$, $a \in \Sigma$ and $l \in L_2.a^{-1}$. Then $\overleftarrow{ch}_l.a \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L_2, R_2])$. Hence there necessarily exists a state $[L, R]$ such that $l \in L$ and such that $[L, R] \xrightarrow{a} [L_2, R_2]$ in $\overrightarrow{C}$. The second necessary condition is obtained by a symmetric way.

Suppose the first condition is verified. We shall prove by induction on the length of the word w that for all $[L, R] \in C$, $w \in \overleftarrow{ch}_L \Rightarrow w \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R])$. The equality is then deduced from Proposition 3.

The case $|w| = 0$ is given by the definition of $\overrightarrow{C}$. Now, let $n \in \mathbb{N}$, $[L_2, R_2] \in C$ and $wa \in \overleftarrow{ch}_{L_2}$, where $w \in \Sigma^n$ and $a \in \Sigma$. Hence there exists $l \in L_2.a^{-1}$ such that $w \in \overleftarrow{ch}_L$. By induction, we have $w \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L, R])$. Moreover, the first condition implies that $[L, R] \xrightarrow{a} [L_2, R_2]$ exists in $\overrightarrow{C}$. Hence $wa \in \overleftarrow{\mathcal{L}}^{\overrightarrow{C}}([L_2, R_2])$. The second sufficient condition is obtained in a symmetric way. ∎

Proposition 5.3 is, in a different framework, the characterization given by Courcelle, Niwinski and Podelski [6] for rectangular decompositions deduced from an automaton. Notice that for all grid covers C, the automaton $\overrightarrow{C}$ recognizes a subset of $\mathcal{L}$. Thus, proving that C is legitimate is equivalent to proving that $\mathcal{L} \subseteq \mathcal{L}(\overrightarrow{C})$. For all automata A, the grid cover $G(A)$ is a tight grid cover — by definition. However, there exist legitimate covers that are not tight.

As a consequence of Proposition 4, tight grid covers are good candidates for enumerating automata, since this class of grid covers is associated with the class of saturated automata and since for each automaton A recognizing $\mathcal{L}$, there exists a surjective morphism from A onto a saturated automaton. Indeed, the enumeration of NFAs and the enumeration of tight grid covers are equivalent problems by definition. Hence there is no straightforward enumeration technique of tight grid covers. The following sections present two different approaches for this problem.

3   Grid cover extensions and automaton morphisms

The process described in this section consists in extending horizontally and then vertically a given cover in order to get a prime cover.

Definition 11 *Let $[L, R]$ be a grid of M. We define R_L and L_R by letting $R_L = \max\{R' \subseteq \{q_1, \ldots, q_{n_b}\} \mid [L, R'] \in \mathcal{G}_M\}$ and $L_R = \max\{L' \subseteq \{1, \ldots, n\} \mid [L', R] \in \mathcal{G}_M\}$.*

Let C be a grid cover of M, the horizontal extension of C is the cover $H(C) = \{[L, R_L] \mid [L, R] \in C\}$ while its vertical extension is $V(C) = \{[L_R, R] \mid [L, R] \in C\}$. A grid cover is said to be vertically (resp. horizontally) prime if it is equal to its own vertical (resp. horizontal) extension.

Lemma 1 *Let C be a cover whose grids are horizontally prime. Let $[L, R]$ and $[L_2, R_2]$ be two grids of C, and let $a \in \Sigma$, we have*

$$L.a \subseteq L_2 \Longrightarrow a.R_2 \subseteq R$$

Symmetrically, if C is a cover whose grids are vertically prime, then we have

$$a.R_2 \subseteq R \Longrightarrow L.a \subseteq L_2$$

Proof — Suppose that $L.a \subseteq L_2$. For all $r_2 \in R_2$, we have $L.a \subseteq L_2 \subseteq r_2$ where r_2 is considered as a subset of $Q_\mathcal{A}$. Hence, $L \subseteq \delta_{\overline{\mathcal{A}}}(r_2, a)$. Through subset determinization, we get $L \subseteq \delta_\mathcal{B}(r_2, a)$. And since R is maximal for the property $[L, R] \in \mathcal{G}_M$, that is for the property $L \subseteq r$ ($\forall r \in R$), we have $\delta_\mathcal{B}(r_2, a) \in R$, that is, $a.r_2 \in R$. ∎

Lemma 2 *Let C be a grid cover of M. The mapping $\varphi_h : [L, R] \mapsto [L, R_L]$ is a surjective morphism that maps $\overrightarrow{C}$ onto $\overrightarrow{H(C)}$. In a same way, the mapping $\varphi_v : [L, R] \mapsto [L_R, R]$ is a surjective morphism from $\overrightarrow{C}$ onto $\overrightarrow{V(C)}$.*

Proof — Let $[L_1, R_1], [L_2, R_2] \in C$ and $a \in \Sigma$ such that the transition $[L_1, R_1] \xrightarrow{a} [L_2, R_2]$ exists. Since we have $L_1.a \subseteq L_2$ and since $H(C)$ is horizontally prime, Lemma 1 implies that the transition $[L_1, R_{L_1}] \xrightarrow{a} [L_2, R_{L_2}]$ exists in $\overrightarrow{H(C)}$. In addition, it is clear that φ_1 maps initial and final states of $\overrightarrow{C}$ respectively into the initial and final states of $\overrightarrow{H(C)}$.

On the other hand, $\varphi_v(M) = \overline{\varphi_h(\overline{M})}$, hence φ_v is also a surjective automaton morphism. ∎

Theorem 1 *Let C be a grid cover of the RAM M. There exists a prime grid cover C' and a surjective morphism that maps $\overrightarrow{C}$ into $\overrightarrow{C'}$.*

3.1 The canonical automaton

Consider the language $\mathcal{L}$ and its associated RAM M. We have a particular case where a prime grid cover is a tight grid cover.

Definition 12 *Let $\mathcal{C}_\mathcal{L}$ denote the grid cover of M that consists of all prime grids of M. The automaton $\overrightarrow{\mathcal{C}_\mathcal{L}}$ is said to be the* canonical automaton *of $\mathcal{L}$.*

Proposition 6 *The prime grid cover $\mathcal{C}_\mathcal{L}$ is tight.*

Proof — We have to prove that $\mathcal{C}_\mathcal{L}$ satisfies the Property 3 of Proposition 5.
  Let $[L_2, R_2] \in \mathcal{C}_\mathcal{L}$, $a \in \Sigma$ and $l \in L_2.a^{-1}$. Let $L = L_2.a^{-1}$ and $R = R_L$. We have $l \in L$, and L is nonempty. On the other hand, $\overleftarrow{ch}_L \cdot \overrightarrow{ch}_{a.R_2} \subseteq \mathcal{L}$, which shows that R is also nonempty.
  The grids $[L, R]$ and $[L_2, R_2]$ are both horizontally prime. Because of the Lemma 1, we just have to verify that $L.a \subseteq L_2$, which is trivial.
  Now let $[L, R] \in \mathcal{C}$, $a \in \Sigma$ and $r' \in a^{-1}.R$. Let $R_2 = a^{-1}.R$ and $L_2 = L_{R_2}$. We have $r' \in R_2$, and R_2 is nonempty. On the other hand, $\overleftarrow{ch}_{L.a} \cdot \overrightarrow{ch}_{R_2} \subseteq L$, which shows that L_2 is also nonempty.
  The grids $[L, R]$ and $[L_2, R_2]$ are both vertically prime. Because of the Lemma 1, we just have to verify that $aR_2 \subseteq R$, which is trivial. ∎

Corollary 1 (of Theorem 1) *Let A be an automaton recognizing $\mathcal{L}$, there exists a morphism from A into $\overrightarrow{\mathcal{C}_\mathcal{L}}$. Moreover, every minimal NFA of $\mathcal{L}$ is isomorphic to a subautomaton of the canonical automaton $\overrightarrow{\mathcal{C}_\mathcal{L}}$.*

Proof — Let A be a minimal NFA of $\mathcal{L}$. There exists a morphism φ that maps A into $\overrightarrow{\mathcal{C}_\mathcal{L}}$. The image of A through φ is an automaton recognizing $\mathcal{L}$, that has at least as many states as A. This proves that φ is injective. ∎

  Hence the canonical automaton is a means of enumerating NFAs recognizing $\mathcal{L}$. It also provides a first technique to search the minimal NFAs of $\mathcal{L}$ [1, 3, 10]. A comparison between the fundamental automaton[10] and the canonical automaton can be found in [5], where their calculations are shown to have a same complexity.

4 Enumerating tight prime grid covers

Another approach for enumerating NFAs is to enumerate tight prime grid covers, which is natural since each automaton is associated with a unique tight grid cover. In this case, we shall see that the relevant information for a given grid cover is contained in either its right projection (i.e. on the horizontal axis) or its left projection. We choose the right one. The underlying minimization technique is the one described by Hiroaki Sengoku [11].

Definition 13 *A* right cover *of the RAM M is a family $\mathcal{R}$ of subsets of $\{q_1, \ldots, q_{n_b}\}$ that covers the first row of M in the sense that for all $j \in \{q_1, \ldots, q_{n_b}\}$ such that $M_{1,j} = 1$, we have $j \in R$ for some $R \in \mathcal{R}$.*

As for grid covers, we can associate a right cover with each automaton.

Definition 14 *Let $A = <Q, \Sigma, \delta, I, F>$ be an automaton that recognizes $\mathcal{L}$. We define the right cover $\mathcal{R}(A)$ associated with A by letting $\mathcal{R}(A) = \{\rho(q) \mid q \in Q\}$. Let C be a grid cover, we also define its associated right cover $\mathcal{R}(C) = \{R \subseteq \{q_1, \ldots, q_{n_b}\} \mid (\ \exists L \subseteq \{1, \ldots, n\}\ )\ [L, R] \in C\}$.*

Of course, for all automata A, we have $\mathcal{R}(G(A)) = \mathcal{R}(A)$. Conversely, we associate an automaton with each right cover as follows.

Definition 15 *Let $\mathcal{R}$ be a right cover, its associated automaton is $\overrightarrow{\mathcal{R}} = < \mathcal{R}, \Sigma, \delta_{\mathcal{R}}, I_{\mathcal{R}}, F_{\mathcal{R}} >$ defined by $\delta_{\mathcal{R}}(R, a) = \{R' \in \mathcal{R} \mid aR' \subseteq R\}$ for all $R \in \mathcal{R}$ and $a \in \Sigma$, $I_{\mathcal{R}} = \{R \in \mathcal{R} \mid 1 \in r,\ \forall r \in R\}$, $F_{\mathcal{R}} = \{R \in \mathcal{R} \mid q_1 \in R\}$.*

Now, let us introduce the class of legitimate (resp. tight) right covers.

Definition 16

1. *The right cover $\mathcal{R}$ is legitimate if $\overrightarrow{\mathcal{R}}$ recognizes $\mathcal{L}$.*
2. *The right cover $\mathcal{R}$ is tight if $\mathcal{R}(\overrightarrow{\mathcal{R}}) = \mathcal{R}$.*

Definition 17 *Let $\mathcal{R}$ be a right cover, we define its associated grid cover as $G(\overrightarrow{\mathcal{R}})$.*

Lemma 3 is significant since it proves that tight covers and tight right covers are bijectively associated, and that each tight right cover is the horizontal projection of its associated tight grid cover, which justifies Definition 15.

Lemma 3 *Let C be a grid cover of the RAM M. The automaton $\overrightarrow{V(C)}$ is isomorphic to $\overrightarrow{\mathcal{R}(C)}$. In addition, the function φ that maps a state $[L, R]$ of $\overrightarrow{V(C)}$ to the state R of $\overrightarrow{\mathcal{R}(C)}$, is an isomorphism.*

Proof — Since the automaton $\overrightarrow{V(C)}$ is vertically prime, Lemma 1 implies that the transition $[L, R] \xrightarrow{a} [L_2, R_2]$ exists in $\overrightarrow{V(C)}$ if and only if $a.R_2 \subseteq R$, that is iff the transition $R \xrightarrow{a} R_2$ exists in $\overrightarrow{\mathcal{R}(C)}$. A state $[L, R]$ in $\overrightarrow{V(C)}$ is initial iff $1 \in L$, that is iff $1 \in r$ for all $r \in R$ (L is maximal), that is iff R is initial in $\overrightarrow{\mathcal{R}(C)}$. A state $[L, R]$ in $\overrightarrow{V(C)}$ is final iff $q_1 \in R$, that is iff R is final in $\overrightarrow{\mathcal{R}(C)}$.   ∎

Some properties about right covers are rather similar to Proposition 5. The following proposition is a consequence of Lemma 3.

Proposition 7 *Let $\mathcal{R}$ be a right cover of the RAM M.*

1. *If $\mathcal{R}$ is tight, then $\mathcal{R}$ is legitimate.*

2. $\mathcal{R}$ is tight if and only if

$$(\ \forall R \in \mathcal{R} \ )(\ \forall a \in \Sigma \ )(\ \forall r' \in a^{-1}.R \ )(\ \exists R_2 \in \mathcal{R} \mid r' \in R_2 \ ) \quad a.R_2 \subseteq R$$

Lemma 4 *Let C be a tight grid cover of the RAM M. The function that maps each state $[L, R]$ of $\overrightarrow{C}$ to the state $V([L, R])$ of $\overrightarrow{V(C)}$ is a surjective automaton morphism.*

Proof — We still apply Lemma 1, since $V(C)$ is vertically prime. If the transition $[L, R] \xrightarrow{a} [L_2, R_2]$ exists in $\overrightarrow{C}$, then $aR_2 \subseteq R$ and the related transition exists in $\overrightarrow{V(C)}$. If $[L, R]$ is initial in $\overrightarrow{C}$, then $1 \in L$ and if we let $[L_2, R_2] = V([L, R])$, then it comes $1 \in L_2$ and $V(C)$ is initial in $\overrightarrow{V(C)}$. The same reasoning works for final states. ∎

Now, let us define automata that are associated with tight right covers.

Definition 18 *Let A be an automaton recognizing $\mathcal{L}$. A is said to be right saturated if A is isomorphic to $\overrightarrow{V(G(A))}$.*

According to Lemma 4, right saturated automata are good candidates for enumeration, since for each automaton A recognizing $\mathcal{L}$, there exists a surjective morphism that maps A onto a right saturated automaton.

Theorem 2 *Right saturated automata are bijectively associated with tight right covers of the RAM M. Indeed,*

1. Let A be a right saturated automaton, then A is isomorphic to $\overrightarrow{\mathcal{R}(A)}$.
2. Let $\mathcal{R}$ be a tight right cover of M, then $\overrightarrow{\mathcal{R}}$ is right saturated.
3. Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two distinct tight right covers of M, then $\overrightarrow{\mathcal{R}_1}$ and $\overrightarrow{\mathcal{R}_2}$ are not isomorphic.

Proof — (1) is a consequence of Definition 18 and Lemma 3.

(2) Let $\mathcal{R}$ be a tight right cover. We have $\mathcal{R}(\overrightarrow{\mathcal{R}}) = \mathcal{R}$. Hence, $\overrightarrow{\mathcal{R}}$ is isomorphic to $\overrightarrow{\mathcal{R}(\overrightarrow{\mathcal{R}})}$, which is itself isomorphic to $\overrightarrow{V(G(\overrightarrow{\mathcal{R}}))}$ from Lemma 3. Hence $\overrightarrow{\mathcal{R}}$ is right saturated.

(3) Two isomorphic automata have the same set of right languages. ∎

As a result, the enumeration of right saturated NFAs recognizing $\mathcal{L}$ can be achieved by enumerating the tight right covers of the RAM M. We now give a characterization of tight right covers which provides an algorithmic approach.

Proposition 8 *A family $\mathcal{R}$ of subsets of $\{q_1, \ldots, q_{n_b}\}$ is a tight right cover of the RAM M if and only if:*

1. $(\ \forall j \in \{q_1, \ldots, q_{n_b}\} \mid M_{1,j} = 1 \ )(\ \exists R \in \mathcal{R} \ ) \quad j \in R$.
2. $(\ \forall R \in \mathcal{R} \ )(\ \forall a \in \Sigma \ ) \quad \delta_{\overline{\mathcal{B}}}(R, a) = \bigcup\{R' \in \mathcal{R} \mid \delta_{\mathcal{B}}(R', a) \subseteq R\}$.

Proof — Let $\mathcal{R}$ be a right cover of M. Then, $\mathcal{R}$ is tight if and only if for all $R \in \mathcal{R}$, for all $r \in R$, for all $a \in \Sigma$ and $r' \in \delta_{\overline{\mathcal{B}}}(R, a)$, there exists $R' \in \mathcal{R}$ such that $a.R' \subseteq R$, that is $\delta_{\mathcal{B}}(R', a) \subseteq R$. ∎

Proposition 8 gives a mathematical characterization of tight right covers. In practical terms, the enumeration of all tight right covers consists in walking along an exploration tree. At the root of the exploration tree, one chooses a cover of $M_{1,j}$. Then, for each block R already in the cover, some blocks $R' \subseteq \delta_{\overline{\mathcal{B}}}(R, a)$ are added so that $\delta_{\overline{\mathcal{B}}}(R, a)$ is covered by such blocs R', that is, condition (2) holds for this block R.

Thence, an alternative method for searching minimal NFAs consists in applying this enumeration technique and searching the smallest tight right covers. From a practical point of view, this is the technique described by Sengoku in [11].

5   Conclusion

Let us conclude by stating that, contrary to an assertion of Sengoku in [11], searching minimal NFAs cannot be achieved by only considering tight right covers that are projections of a prime grid cover. It is true that prime grid covers are maximal in terms of surjective automaton morphisms. Unfortunately, there is no reason for the horizontal projection of a prime cover to be tight.

Then we have two distinct and *a priori* non comparable enumeration techniques. Is there one technique better than the other to enumerate *all* NFAs remains an open question that could be investigated by practical tests. Whatever, the enumeration of tight right covers has a crucial advantage over the canonical automaton as it permits a partial enumeration, avoiding the obstacle of the exponential complexity.

References

1. A. Arnold, A. Dicky, and M. Nivat. A note about minimal non-deterministic automata. *Bulletin of the EATCS, number 47*, pages 166–169, June 1992.
2. J. A. Brzozowski. Canonical regular expressions and minimal state graphs for definite events. *Mathematical Theory of Automata, MRI Symposia Series*, 12:529–561, 1962.
3. C. Carrez. On the minimalization of non-deterministic automaton. Technical report, Laboratoire de Calcul de la Faculté des Sciences de l'Université de Lille, 1970.
4. J.-M. Champarnaud and F. Coulon. NFA reduction algorithms by means of regular inequalities. In *Proc. of DLT 2003, Lecture Notes in Computer Science*, 2710, pages 194–205. Springer, 2003.
5. J.-M. Champarnaud and F. Coulon. Theoretical study and implementation of the canonical automaton. *Fundamenta Informaticae*, 55(1):23–38, 2003.
6. B. Courcelle, D. Niwinski, and A. Podelski. A geometrical view of the determinization and minimization of finite-state automata. *Mathematical Systems Theory 24*, pages 117–146, 1991.

7. T. Jiang and B. Ravikumar. Minimal NFA problems are hard. *SIAM J. Comput. Vol 22, No 6*, pages 1117–1141, 1993.

8. T. Kameda and P. Weiner. On the state minimization of nondeterministic finite automata. *IEEE Trans. Comp.*, C(19):617–627, 1970.

9. S. Lombardy, R. Poss, Y. Regis-Gianas, and J. Sakarovitch. Introducing Vaucanson. In *Proc. of CIAA 2003, Lecture Notes in Computer Science*, 2759, pages 96–107. Springer, 2003.

10. O. Matz and A. Potthoff. Computing small nondeterministic finite automata. *Tools and Algorithms for the Construction and Analysis of Systems – TACAS 95, volume NS-95-2*, pages 74–88, 1995.

11. H. Sengoku. Minimization of nondeterministic finite automata. Master's thesis, Kyoto University, 1992.

12. S. Yu. Regular languages. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages, Volume I, Word, Language, Grammar*, pages 41–110. Springer, Berlin, 1997.