Five lectures in the theory of
Weighted Automata and Transducers

Jacques Sakarovitch

IRIF/CNRS–Université Paris Diderot & Telecom-ParisTech

December 2018 – January 2019

Lectures notes of the Master Parisien de Recherche en Informatique

Course 2.16 — Finite automata based computation models

Contents

These lectures notes are intended to be as self-contained as possible. However, many complements — sometimes in a slightly different setting, as my point of view has evolved — are to be found in my book *Elements of Automata Theory* (Cambridge University Press, 2009). References to this work are indicated in marginal notes.

Every lecture ends with an exercise section.

Lecture III

Reduction of weighted automata

Controllability and observability

Given a (finite) $\mathbb{K}$-automaton over A^*, we want to build equivalent ones, hopefully of smaller dimension. In this lecture, we base this construction upon the *behaviour* of the automaton, in contrast with the preceding lecture where we have addressed the same question by considering the *structure* of the automaton.

Contents

We first define a process, that we call the *universal determinisation process*, and that yields a possibly infinite automaton, but a *deterministic* one and with no multiplicity on the transitions but in the final function. We then explain how to work in that framework.

In the next section, we introduce the notion of *quotient* of a series, show a characterisation of recognisable series in terms of quotients, and relate the quotients with the previous construction.

Finally, we combine the two approaches to set up the theory for reduction in the case where the multiplicity semiring is a field, or a subsemiring of a field, and turn the theory into a polynomial algorithm.

As a preliminary, let us recall the main result of Lecture I: finite $\mathbb{K}$-automata over A^* and $\mathbb{K}$-representations of A^* are one and the same thing and we use the most convenient form; here, the representation. Before all, let us introduce the notion of *action* that will be ubiquitous in that lecture.

1 Actions and representations

The notion of *action* is central in this lecture. We first define it and then describe how it relates to the one of representation.

Contrary to what we have done in Lecture I (where we have defined $\mathbb{K}$-automata over free monoids and then extended the notion to $\mathbb{K}$-automata over general (graded) monoids), we first define actions of arbitrary monoids and then consider in the following sections actions of free monoids only.

1.1 Action of a monoid on a set

Definition 1. Let S be a set — finite or infinite — and M a monoid. An *action* δ of M on S is a map from $S \times M$ to S, denoted by $s \cdot m$ rather than by $\delta(s, m)$, which meets the two conditions:

$$\begin{aligned} &\forall s \in S && s \cdot 1_M = s\,, \\ &\forall s \in S\,,\ \forall m, m' \in M && (s \cdot m) \cdot m' = s \cdot (m\,m')\ . \end{aligned} \tag{1.1}$$

The *orbit* of an element s of S under the action δ is the subset of S that can be reached from s by the actions of all elements of M, that is, the set $\{s \cdot m \mid m \in M\}$.

When necessary, we write $s \mathbin{\dot{\delta}} m$ in order to differentiate between two different actions of a monoid or from the matrix product symbol.

Examples 2. (i) Permutation groups are examples of monoid actions; even more, one may say that monoid actions are generalisation of permutation groups.

(ii) Every monoid M defines an *action on itself* by multiplication on the right:

$$\forall p, m \in M \qquad p \cdot m = pm \ ;$$

this action is called the *right translation* or the *(right) regular representation* of M over itself. It is denoted (when necessary) by ρ.

(iii) Likewise, every morphism $\alpha \colon M \to N$ defines an action of M on N:

$$\forall n \in N\,,\ \forall m \in M \qquad n \cdot m = n\,(\alpha\,(m)) \ . \tag{1.2}$$

This map satisfies (1.1) because α is a morphism and multiplication in N is associative. (The regular representation above corresponds to the identity morphism ι from M onto itself.[1])

Right and left actions The actions we have thus defined are *right* actions. We could have defined in a dual manner a *left* action of M on S as a map from $M \times S$ to S that satisfies the conditions:

$$\begin{aligned} &\forall s \in S && 1_M \cdot s = s\,, \\ &\forall s \in S\,,\ \forall m, m' \in M && m' \cdot (m \cdot s) = (m'\,m) \cdot s \ . \end{aligned} \tag{1.3}$$

Actions on structured sets An action of M on S is a morphism from M into the monoid of maps from S into itself. If S has a structure (*e.g.*being a group, a ring, *etc.*), we want an action to be a morphism from M into the monoid of *endomorpisms* of S. In the sequel, S is a $\mathbb{K}$-module and an action of M on S is 'linear':

$$\begin{aligned} &\forall s, t \in S\,,\ \forall m, m' \in M && (s+t) \cdot m = s \cdot m + t \cdot m\,, \\ &\forall k \in \mathbb{K} && (k\,s) \cdot m = k\,(s \cdot m) \ . \end{aligned}$$

Examples 3. (i) A special case of Example 2 (ii) is the regular representation of A^* over itself, which extends by linearity to an action of A^* on the $\mathbb{K}$-*module* $\mathbb{K}\langle A^*\rangle$, and which we call the *right translation* by A^*.

(ii) Any $\mathbb{K}$-representation (or morphism) $\mu \colon M \to \mathbb{K}^{Q \times Q}$ of dimension Q defines an action of M on the *(left)* $\mathbb{K}$-*module* $\mathbb{K}^Q$ (on $\mathbb{K}^{1 \times Q}$, indeed), also denoted by μ:

$$\forall x \in \mathbb{K}^Q\,,\ \forall m \in M \qquad x \underset{\mu}{\cdot} m = x \cdot \mu\,(m) \ . \tag{1.4}$$

Since $\mathbb{K}$ is not supposed to be commutative, it is important to specify that $\mathbb{K}^{1 \times Q}$ is a left module.

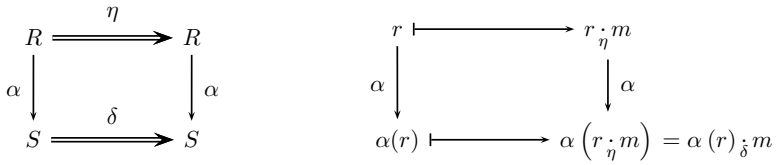
[1] But is not denoted as such, as it is misleading to denote by ι a map which is not the identity.

Action morphisms Let R and S be two structures (in the sequel, they will be $\mathbb{K}$-modules) and suppose that M acts on both R and S, by η and δ respectively.

A morphism $\alpha\colon R \to S$ is an *action morphism* if

$$\forall r \in R\,,\ \forall m \in M \qquad \alpha\,(r) \mathbin{\dot{\delta}} m = \alpha\left(r \mathbin{\dot{\eta}} m\right)\ ,$$

that is, if the following diagram is commutative (for every m in M).



1.2 Actions and deterministic automata

If we distinguish an element s_0 in S, that will play the role of an initial state, and a subset T of S, that will play the role of the set of final states, any action δ of M on S defines an automaton $\mathcal{A}_\delta = \langle\, M, S, \{s_0\}, \delta, T\,\rangle$.

If M is a free monoid A^*, $\mathcal{A}_\delta$ is a *deterministic* Boolean automaton. And conversely any (complete) deterministic Boolean automaton $\mathcal{A}$ over A^* determines an action of A^* on the state set of $\mathcal{A}$. If M is not a free monoid, the notion of action is indeed *the* way to generalise the one of deterministic automaton.

exercice to be written

If we replace the subset T by a *function* T from S to $\mathbb{K}$ (the former being a function from S to $\mathbb{B}$) the action δ, together with s_0 and T, now defines a $\mathbb{K}$-automaton, which we call again deterministic in which the weight of every transition is $1_\mathbb{K}$ and the final function is T. The behaviour of $\mathcal{A}_\delta$ is then defined by $\langle\!|\mathcal{A}_\delta|\!, m\rangle = T(s_0 \cdot m)$ for every m in M.

1.3 Closed sets

In this section, S is a (left) $\mathbb{K}$-module (later, it will be $\mathbb{K}^{1\times Q}$ or $\mathbb{K}\langle\langle A^*\rangle\rangle$). We first take some notations that prove to be (very) convenient.

Notations for submodules Any finite subset G of S induces a morphim

$$\alpha_G\colon \mathbb{K}^G \to S\ ,$$

whose image is $\langle G \rangle$, the sub(-$\mathbb{K}$-)module of S generated by G:

$$\forall x \in \mathbb{K}^G \qquad \alpha_G\,(x) = \sum_{g\in G} x_g\, g\ .$$

We also write

$$\alpha_G\,(x) = x \cdot G$$

which implicitely means that G is viewed as a *column-vector* of dimension G of elements of S.

Conversely, let $\beta_G \colon \langle G \rangle \to \mathbb{K}^G$ be a map that performs, for every v in $\langle G \rangle$, *a choice* of a decomposition of v over the elements of G and hence, for every v in $\langle G \rangle$:

$$\alpha_G(\beta_G(v)) = v \ . \tag{1.5}$$

Such a decomposition *is not unique* in general; that is, when G is not a *basis* of $\langle G \rangle$) and $\beta_G(\alpha_G(x))$ and x are not necessarily equal (but $\alpha_G(\beta_G(\alpha_G(x))) = \alpha_G(x)$ holds.

It is natural, even though not necessary, to assume that for every g in G, $\beta_G(g)$ is the vector whose all entries are $0_{\mathbb{K}}$ but the g-th one which is $1_{\mathbb{K}}$. In other words, $\beta_G(G)$ is the identity matrix of dimension G. *Is this alinea useful?*

Definition 4. Let S be a (left) $\mathbb{K}$-module and δ a (right) action of A^* on S. A subset G of S is said to be δ-*closed* if the orbit of G is contained in $\langle G \rangle$, that is, if

$$\forall g \in G\,,\ \forall w \in A^* \qquad g \mathbin{\dot{\delta}} w \in \langle G \rangle \ ,$$

which amounts to say that $\langle G \rangle$ itself is closed, or *stable*, under the action of δ:

$$\forall v \in \langle G \rangle\,,\ \forall w \in A^* \qquad v \mathbin{\dot{\delta}} w \in \langle G \rangle \ .$$

If v is in $\langle G \rangle$, there exists x in $\mathbb{K}^G$ such that $v = \alpha_G(x) = x \cdot G$ and then:

$$v \mathbin{\dot{\delta}} w = x \cdot \left(G \mathbin{\dot{\delta}} w \right) \ .$$

1.4 Closed sets and representations

The core of this section is to show that an action on a finite closed set can be lifted into a representation. We give indeed two versions of this construction: the lifting of actions and the lifting of representations.

1.4.1 Lifting of actions

Proposition 5. *Let S be a (left) $\mathbb{K}$-module, δ a (right) action of A^* on S and G a finite subset of S.*

If G is δ-closed, then there exists a $\mathbb{K}$-representation κ_G (not necessarily unique) of A^* of dimension G such that α_G is an action morphism between the action of A^* on $\mathbb{K}^G$ defined by κ_G and δ, that is, such that the following diagram commutes.

$$\begin{array}{ccc} \mathbb{K}^G & \xrightarrow{\kappa_G} & \mathbb{K}^G \\ {\scriptstyle \alpha_G}\downarrow & & \downarrow{\scriptstyle \alpha_G} \\ S \supseteq \langle G \rangle & \xrightarrow{\delta} & \langle G \rangle \subseteq S \end{array} \tag{1.6}$$

Proof. Let $\beta_G \colon \langle G \rangle \to \mathbb{K}^G$ be a fixed map defined as above. Since G is δ-closed, for every g in G and every a in A, $g \mathbin{\dot{\delta}} a$ is in $\langle G \rangle$ and hence $\beta_G \left(g \mathbin{\dot{\delta}} a \right)$ is in $\mathbb{K}^G$. Let κ_G be defined by

$$\forall a \in A \qquad \kappa_G (a) = \beta_G \left(G \mathbin{\dot{\delta}} a \right) \ ,$$

that is, since we see G as a column-vector of dimension G, $\beta_G \left(G \mathbin{\dot{\delta}} a \right)$ is a $G \times G$-matrix (with entries in $\mathbb{K}$) the g-th row of which is $\beta_G \left(g \mathbin{\dot{\delta}} a \right)$. Hence every map β_G defines a representation κ_G, possibly distinct from the others.

If we instanciate diagram (1.6) for x in $\mathbb{K}^G$ and a in A, it comes:

$$\begin{array}{ccc} x & \longmapsto & x \cdot \kappa_G (a) = x \cdot \beta_G \left(G \mathbin{\dot{\delta}} a \right) \\ {\scriptstyle \alpha_G} \downarrow & & \downarrow {\scriptstyle \alpha_G} \\ x \cdot G = \alpha_G (x) & \longmapsto & \alpha_G (x) \mathbin{\dot{\delta}} a = x \cdot \left(G \mathbin{\dot{\delta}} a \right) \end{array} \tag{1.7}$$

on which we read the following sequence of equalities:

$$\alpha_G (x) \mathbin{\dot{\delta}} a = (x \cdot G) \mathbin{\dot{\delta}} a = x \cdot (G \mathbin{\dot{\delta}} a) \qquad \text{as } \delta \text{ is } \mathbb{K}\text{-linear.} \tag{1.8}$$

$$\begin{aligned} \text{On the other hand} \qquad x \cdot \kappa_G (a) &= x \cdot \beta_G \left(G \mathbin{\dot{\delta}} a \right) && \text{by definition} \\ \alpha_G (x \cdot \kappa_G (a)) = \alpha_G \left(x \cdot \beta_G \left(G \mathbin{\dot{\delta}} a \right) \right) &= x \cdot \alpha_G \left(\beta_G \left(G \mathbin{\dot{\delta}} a \right) \right) && \text{as } \alpha_G \text{ is } \mathbb{K}\text{-linear,} \\ &= x \cdot (G \mathbin{\dot{\delta}} a) && \text{by (1.5).} \end{aligned} \tag{1.9}$$

The equality between the right hand-sides of (1.8) and (1.9) expresses that the diagram (1.6) commutes. ∎

1.4.2 Lifting of representations

Let Q be any finite set. We study the preceding case when $S = \mathbb{K}^Q$ and δ is the action on $\mathbb{K}^Q$ defined by a representation $\mu \colon A^* \to \mathbb{K}^{Q \times Q}$.

Let G be a finite subset of $\mathbb{K}^Q$. We denote by M_G the $G \times Q$-matrix (with entries in $\mathbb{K}$) the g-th row of which is the *row-vector* g of $\mathbb{K}^Q$. In this context, to say that G is a column-vector amounts to say that G is in $\left(\mathbb{K}^{1 \times Q} \right)^{G \times 1} = \mathbb{K}^{G \times Q}$ that is, that G *is the matrix* $M_G = \alpha_G (\mathrm{Id})$, where Id is the identity matrix of dimension G.

Proposition 6. *Let $\mathcal{A} = \langle I, \mu, T \rangle$ be a $\mathbb{K}$-representation of A^* of dimension Q. Any finite subset G of $\mathbb{K}^Q$, that is μ-closed and that decomposes I, determines (not uniquely) a $\mathbb{K}$-representation $\langle J, \kappa_G, U \rangle$ of dimension G that is conjugate to $\mathcal{A}$ by M_G (hence equivalent to $\mathcal{A}$).*

Proof. Let us come back to diagram (1.6) of Proposition 5:

$$\begin{array}{ccc} \mathbb{K}^G & \xrightarrow{\kappa_G} & \mathbb{K}^G \\ {\scriptstyle \alpha_G}\downarrow & & \downarrow{\scriptstyle \alpha_G} \\ \mathbb{K}^{1\times Q} \supseteq \langle G \rangle & \xrightarrow{\mu} & \langle G \rangle \subseteq \mathbb{K}^{1\times Q} \end{array}$$

If we replace in the proof of Proposition 5 the action δ by the action μ determined by $\mathcal{A}$ and G by M_G, it comes

$$G \mathbin{\dot{\delta}} a = M_G \cdot \mu(a) \qquad \text{and} \qquad \forall x \in \mathbb{K}^G \qquad \alpha_G(x) = x \cdot M_G \ .$$

The above diagram instanciated for $\mathtt{Id}$ and any letter a of A yields

$$\begin{array}{ccc} \mathtt{Id} & \longmapsto & \kappa_G(a) \\ {\scriptstyle \alpha_G}\downarrow & & \downarrow{\scriptstyle \alpha_G} \\ M_G & \longmapsto & M_G \cdot \mu(a) = \kappa_G(a) \cdot M_G \end{array}$$

which shows that for every a in A, $\kappa_G(a)$ is conjugate to $\mu(a)$ by M_G.

Furthermore, to say that G decomposes I, that is, $I \in \langle\!\langle G \rangle\!\rangle$, implies that there exists J in $\mathbb{K}^G$ such that $I = \alpha_G(J) = J \cdot M_G$. If we write $U = M_G \cdot T$, we have built the $\mathbb{K}$-representation we wanted. ∎

2 Control

Starting from a $\mathbb{K}$-automaton, we paradoxically begin our search for small equivalent automata by the definition and idealistic constuction of two automata that are infinite (in the general case). In this section, we start from the given automaton itself, in the next one from its behaviour. In some sense, we thus begin with the *effective* level as the (finite) automaton (or representation) is effectively given; since the computations may lead to an *infinite* automaton, this effectivity is somewhat relative. Linear algebra will then allow to fold these infinite automata into finite ones, hopefully, and when possible, optimally.

For the rest of this section, $\mathcal{A} = \langle I, \mu, T \rangle$ is a $\mathbb{K}$-representation of A^*, of dimension Q.

2.1 The reachability set

The representation $\mathcal{A}$, the morphism μ indeed, determines an *action* of A^* on $\mathbb{K}^Q$, called μ again, by

$$\forall x \in \mathbb{K}^Q \qquad x \mathbin{\dot{\mu}} w = x \cdot \mu(w) \ .$$

Definition 7. The *reachability set* $\mathbf{R}_\mathcal{A}$ of $\mathcal{A}$ is the orbit of I under the action μ:

$$\mathbf{R}_\mathcal{A} = \{ I \cdot \mu(w) \mid w \in A^* \} \ .$$

This set $\mathbf{R}_\mathcal{A}$ may well be, and in general is, infinite.

Determinisation The set $\mathbf{R}_{\mathcal{A}}$ is closed under the action μ and this action of A^* on $\mathbf{R}_{\mathcal{A}}$ can be seen as a *deterministic automaton*, denoted by $\widehat{\mathcal{A}}$, and called the *determinisation* of $\mathcal{A}$ as it is defined by $\mathcal{A}$:

$$\widehat{\mathcal{A}} = \left\langle A, \mathbf{R}_{\mathcal{A}}, \{I\}, \mu, \widehat{T} \right\rangle \ .$$

Its transitions are defined by: $[I \cdot \mu(w)] \cdot_{\mu} a = I \cdot \mu(w) \cdot \mu(a) = I \cdot \mu(wa)$ and its final function by: $\widehat{T}(x) = x \cdot T$. The automaton $\widehat{\mathcal{A}}$, a priori infinite, is equivalent to $\mathcal{A}$.

Example 8. Let $\mathcal{A}_2$ and $\mathcal{A}_3$ be the $\mathbb{N}$-automata over a^* of dimension 1 and 2 defined by $\mathcal{A}_2 = \left\langle \begin{pmatrix}1\end{pmatrix}, \begin{pmatrix}2\end{pmatrix}, \begin{pmatrix}1\end{pmatrix} \right\rangle$ and by $\mathcal{A}_3 = \left\langle \begin{pmatrix}1 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}, \begin{pmatrix}1\\ 1\end{pmatrix} \right\rangle$ respectively. Their determinisations are shown at Figure 1. The determinisation of $\mathcal{B}_1$ (*cf.*Example I.3) is shown at Figure 2.

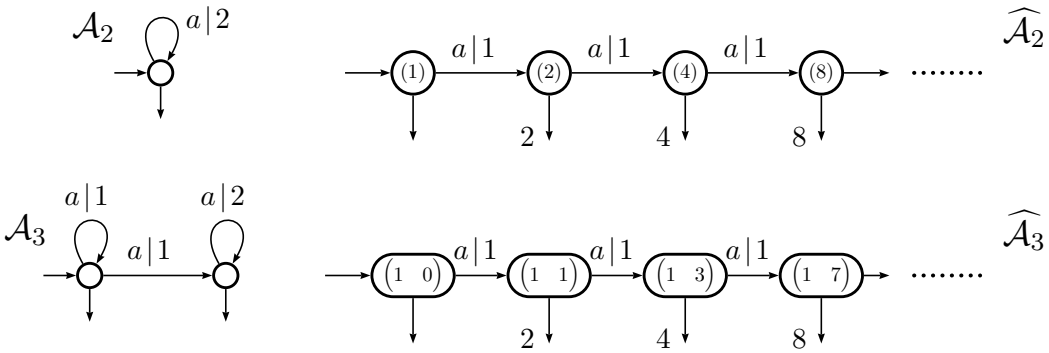


Figure 1: Two (equivalent) $\mathbb{N}$-automata and their (equal) determinisations

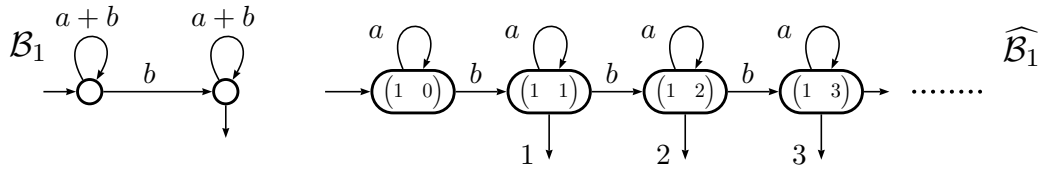


Figure 2: The determinisation of the $\mathbb{N}$-automaton $\mathcal{B}_1$

The Boolean case The use of the word determinisation, as in the case of classical Boolean automata, is not a coincidence: if $\mathbb{K} = \mathbb{B}$ the construction we have described *is* the so-called *subset construction*. Every Boolean vector of $\mathbb{B}^Q$ can be identified with a subset of Q , and conversely. The initial state I *is* the set of initial states of $\mathcal{A}$, and $(I \cdot \mu(w)) \cdot \mu(a)$ *is* the set of states reached by the letter a from the set of states $I \cdot \mu(w)$.

2.2 The state-space

So far, $\mathbb{K}^Q$, and thus $\mathbf{R}_{\mathcal{A}}$, have been considered as sets without any structure. We now bring into play the fact that $\mathbb{K}^Q = \mathbb{K}^{1\times Q}$ is a *(left) module over* $\mathbb{K}$.

Definition 9. We call *state-space* of $\mathcal{A}$ the $\mathbb{K}$-module $\mathbb{K}^Q$.

Definition 10. We call *control morphism* of $\mathcal{A}$ the morphism of $\mathbb{K}$-modules $\Psi_\mathcal{A}$:

$$\Psi_\mathcal{A} \colon \mathbb{K}\langle A^* \rangle \longrightarrow \mathbb{K}^Q \ ,$$

defined by $\Psi_\mathcal{A}(w) = I \cdot \mu(w)$ for every w in A^* and extended to $\mathbb{K}\langle A^* \rangle$ by linearity.

With these definition and notation, it holds:

$$\mathbf{R}_\mathcal{A} = \Psi_\mathcal{A}(A^*) \qquad \text{and} \qquad \mathsf{Im}\,\Psi_\mathcal{A} = \Psi_\mathcal{A}(\mathbb{K}\langle A^* \rangle) = \langle \mathbf{R}_\mathcal{A} \rangle \ .$$

and the following statement is almost a tautology.

Proposition 11. *The control morphism $\Psi_\mathcal{A}$ is an action morphism from the right translation by A^* on $\mathbb{K}\langle A^* \rangle$ to the action μ of A^*.*

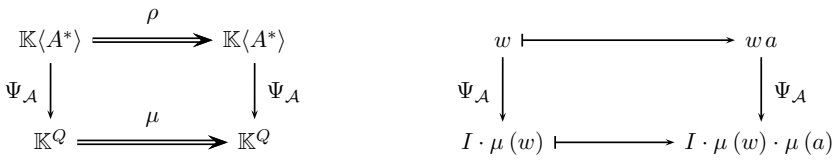


Figure 3: The control morphism is a morphism of actions

Definition 12. A $\mathbb{K}$-representation (or $\mathbb{K}$-automaton) $\mathcal{A}$ is said to be *controllable*[2] if $\Psi_\mathcal{A}$ is *surjective*.

The automaton $\mathcal{A}$ is controllable if for every point in the state space, there exists at least one linear combination of input that leads $\mathcal{A}$ to that point.

3 Observation

We now define a third action of A^*, on $\mathbb{K}\langle\langle A^* \rangle\rangle$ this time. It allows to *characterise* recognisable series and to associate with every such series a *minimal* deterministic automaton.

3.1 Quotient of series

The quotient of a series is the generalisation to series of the quotient of a subset of a monoid (of a free monoid in this case).

[2] *commandable* in French.

Definition 13. Let s be in $\mathbb{K}\langle\langle A^*\rangle\rangle$ and w in A^*. The (left) quotient of s by w is the series denoted by $w^{-1}s$ and defined by:

$$w^{-1}s = \sum_{v\in A^*} \langle s, w\,v\rangle\, v\,, \qquad \text{that is,} \qquad \forall v \in A^* \quad \langle w^{-1}s, v\rangle = \langle s, w\,v\rangle\,. \tag{3.1}$$

$$\text{In particular,} \qquad \forall w \in A^* \qquad \langle w^{-1}s, 1_{A^*}\rangle = \langle s, w\rangle \quad . \tag{3.2}$$

For every w, the operation $s \mapsto w^{-1}s$ is an *endomorphism* of the $\mathbb{K}$-module $\mathbb{K}\langle\langle A^*\rangle\rangle$: it is *additive*:

$$w^{-1}(s+t) = w^{-1}s + w^{-1}t\,,$$

and *commutes with the exterior multiplications* of $\mathbb{K}$ on $\mathbb{K}\langle\langle A^*\rangle\rangle$:

$$w^{-1}(k\,s) = k\,(w^{-1}s) \qquad \text{and} \qquad w^{-1}(s\,k) = (w^{-1}s)\,k\,.$$

Moreover, it is *continuous*. These three properties ensure that the quotient by w is entirely defined on $\mathbb{K}\langle\langle A^*\rangle\rangle$ by its values on A^*.

The associativity of concatenation implies then that

$$\forall u, v \in A^* \qquad (u\,v)^{-1}s = v^{-1}\left[u^{-1}s\right]\,,$$

that is, thanks to the preceding properties:

Proposition 14. *The (left) quotient is a (right) action of A^* on the (left) $\mathbb{K}$-module $\mathbb{K}\langle\langle A^*\rangle\rangle$.*[3]

The orbit of a series s under the quotient action is denoted by $\mathbf{R}_s$:

$$\mathbf{R}_s = \left\{ w^{-1}\,s \;\middle|\; w \in A^* \right\} \quad .$$

Example 15. Let $s_2 = (\underline{a^*})^2 = \sum_{n\in\mathbb{N}} (n+1)\,a^n$ in $\mathbb{N}\mathrm{Rat}\,a^*$. For every integer k, it holds:

$$(a^k)^{-1}s_2 = \sum_{n\in\mathbb{N}} (k+n+1)\,a^n = s_2 + k\,\underline{a^*} \quad .$$

All quotients of s_2 are distinct and $\mathbf{R}_{s_2} = \{s_2 + k\,\underline{a^*} \mid k \in \mathbb{N}\}$.

Example 15 shows that, in general, and in contrast with the case for (recognisable) languages, the family of quotients of a rational, and thus recognisable, series is not necessarily finite. On the other hand, and despite its simplicity, it exhibits the property that we seek: there are infinitely many quotients, but they can all be expressed as the linear combination of a *finite number* of suitably chosen series.

3.2 The minimal deterministic automaton

Let again $\mathcal{A} = \langle\, I, \mu, T\,\rangle$ be a $\mathbb{K}$-representation of A^*, of dimension Q.

[3] In diagrams, the quotient action will be denoted by $\triangleright$.

Observability

Definition 16. We call *observation morphism* of $\mathcal{A}$ the morphism of $\mathbb{K}$-modules $\Phi_{\mathcal{A}} \colon \mathbb{K}^Q \longrightarrow \mathbb{K}\langle\langle A^* \rangle\rangle$ defined by:

$$\forall x \in \mathbb{K}^Q \quad \Phi_{\mathcal{A}}(x) = \big|\langle x, \mu, T \rangle\big| = \sum_{w \in A^*} (x \cdot \mu(w) \cdot T)\, w \ .$$

The definition of quotient (Equation (3.1)) directly implies that if $s = \big|\langle I, \mu, T \rangle\big|$, then, for every w in A^*, $w^{-1}s = \big|\langle I \cdot \mu(w), \mu, T \rangle\big|$, that is:

Property 17. *For every w in A^*, and every x in $\mathbb{K}^Q$, $w^{-1}\Phi_{\mathcal{A}}(x) = \Phi_{\mathcal{A}}(x \cdot \mu(w))$.*

In other words:

Proposition 18. *The observation morphism $\Phi_{\mathcal{A}}$ is an action morphism from the action μ of A^* on $\mathbb{K}^Q$ to the quotient action of A^* on $\mathbb{K}\langle\langle A^* \rangle\rangle$.*

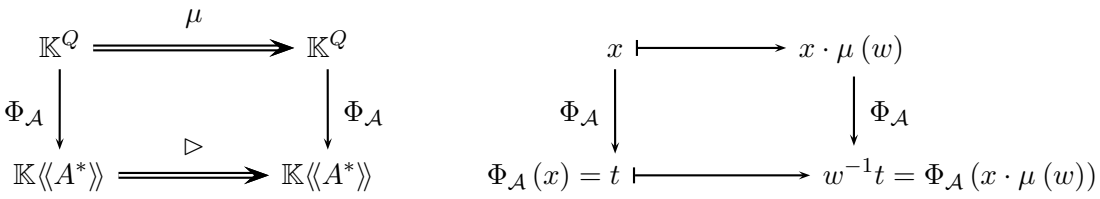


Figure 4: The observation morphism is a morphism of actions

From Property 17 also follows:

Property 19. $\mathbf{R}_s = \Phi_{\mathcal{A}}(\Psi_{\mathcal{A}}(A^*)) = \Phi_{\mathcal{A}}(\mathbf{R}_{\mathcal{A}})$.

Definition 20. A $\mathbb{K}$-representation (or $\mathbb{K}$-automaton) $\mathcal{A}$ is said to be *observable* if $\Phi_{\mathcal{A}}$ is *injective*.

That is, $\mathcal{A}$ is observable if no two distinct starting points in the state-space yield the same behaviour for $\mathcal{A}$.

The minimal automaton The set $\mathbf{R}_s$ is closed under the quotient action and this action of A^* on $\mathbf{R}_s$ can be seen as a *deterministic automaton*, denoted by $\mathcal{A}_s$:

$$\mathcal{A}_s = \langle A, \mathbf{R}_s, \{s\}, \triangleright, \mathsf{c} \rangle \ .$$

Its transitions are defined by

$$[w^{-1}s] \triangleright a = a^{-1}w^{-1}s = (w\,a)^{-1}s \,,$$

its unique initial state is s, and its final function c maps every state $w^{-1}s$ to its *constant term*, that is, $\mathsf{c}(w^{-1}s) = \langle w^{-1}s, 1_{A^*} \rangle = \langle s, w \rangle$.

The automaton $\mathcal{A}_s$, a priori infinite, is equivalent to $\mathcal{A}$: every word w labels a unique path with multiplicity $1_{\mathbb{K}}$ from the initial state s to the state $w^{-1}s$ and the final function gives that computation the weight $\langle s, w\rangle$ by definition.

If s is a $\mathbb{B}$-series, that is, if s is a language L, then $\mathcal{A}_L$ is the *minimal automaton* of L. The well-known relation between the determinisation of an automaton and the minimal automaton of the recognised language generalises to series.

Strictly writing, we have defined *Out-morphisms* and *quotients* for finite ($\mathbb{K}$)-automata only but in the same way we have defined *the weight of a word* for finite automata and noted that it could be defined for infinite deterministic automata (Note I.3, p. 6), Out-morphisms and quotients are easily defined also for infinite deterministic $\mathbb{K}$-automata since the definition coincide with the one for finite deterministic automata: two states can be merged if they have the same transitions to the other (merged) states, and give the final function the same value.

Proposition 21. *Let s be a $\mathbb{K}$-recognisable series and $\mathcal{A}$ any finite $\mathbb{K}$-automaton that realises s. Then $\mathcal{A}_s$ is the* minimal quotient *of $\widehat{\mathcal{A}}$.*

Proof. By Property 19, we already know that $\mathbf{R}_s = \Phi_{\mathcal{A}}(\mathbf{R}_{\mathcal{A}})$. Stating that $\Phi_{\mathcal{A}}$ is a morphism of actions is exactly the same thing as saying that $\Phi_{\mathcal{A}}$ is an Out-morphism between the deterministic automata induced by these actions, here, from $\widehat{\mathcal{A}}$ onto $\mathcal{A}_s$.

Conversely, every state of $\mathcal{A}_s$ corresponds to the series that is accepted by this state taken as the initial state. Thus, two *distinct* states of $\mathcal{A}_s$ cannot be mapped by a morphism onto the same state of a proper quotient since they would correspond to the *same* series. ∎

3.3 Stability

The notion of quotient allows an intrinsic characterisation of recognisable series, via the one of stability.

Definition 22. A subset U of $\mathbb{K}\langle\langle A^*\rangle\rangle$ is called *stable* if it is closed under quotient; that is, for every s in U and every w in A^*, $w^{-1}s$ is in U.

Theorem 23 (Fliess–Jacob)**.** *A series of $\mathbb{K}\langle\langle A^*\rangle\rangle$ is $\mathbb{K}$-recognisable if and only if it is contained in a* stable *finitely generated submodule of $\mathbb{K}\langle\langle A^*\rangle\rangle$.*

Proposition 24. *If s is a series realised by $\mathcal{A}$, then $\mathsf{Im}\,\Phi_{\mathcal{A}}$ is a stable (finitely generated) submodule of $\mathbb{K}\langle\langle A^*\rangle\rangle$ that contains s.*

Proof. The submodule $\mathsf{Im}\,\Phi_{\mathcal{A}}$ is finitely generated since $\mathbb{K}^Q$ is, is stable since $\Phi_{\mathcal{A}}$ is a morphism of actions, and contains $s = \Phi_{\mathcal{A}}(I)$. ∎

Proposition 25. *Let U be a stable submodule of $\mathbb{K}\langle\langle A^*\rangle\rangle$ generated by a finite set G. Then, every series in U is realised by a $\mathbb{K}$-representation of dimension G.*

Proof. Proposition 5, applied to the case where $S = \mathbb{K}\langle\langle A^* \rangle\rangle$ and δ is the quotient, yields a $\mathbb{K}$-representation κ_G of dimension G. Every g in G is a series in $\mathbb{K}\langle\langle A^* \rangle\rangle$; let us denote by $T = \langle G, 1_{A^*} \rangle$ the (column) vector whose g-th entry is $\langle g, 1_{A^*} \rangle$.

If a series s is in U, there exists an x in $\mathbb{K}^G$ such that $s = x \cdot G$. By definition of κ_G, for every w in A^*, $w^{-1}s = x \cdot \kappa_G(w) \cdot G$ and then

$$\langle s, w \rangle = \langle w^{-1}s, 1_{A^*} \rangle = \langle x \cdot \kappa_G(w) \cdot G, 1_{A^*} \rangle = x \cdot \kappa_G(w) \cdot \langle G, 1_{A^*} \rangle = x \cdot \kappa_G(w) \cdot T \ .$$

Hence s is realised by $\langle x, \kappa_G, T \rangle$. ∎

Propositions 24 and 25 together prove Theorem 23. ∎

4 Reduction of representations in a field

We now suppose that $\mathbb{K}$ is a *field*, not necessarily commutative, hence a *skew field*, or *division ring*. The preceding considerations about quotients of series will take on, we might say, a new dimension since the ring of series $\mathbb{K}\langle\langle A^* \rangle\rangle$ is not only a $\mathbb{K}$-algebra, but a (left) $\mathbb{K}$-*vector space*, and the *dimension* of subspaces will give us a new invariant.

We use the notion of dimension essentially via two results:

- Every submodule V (called *subspace*) of a vector space is given a dimension $\dim V$ and if $V \subseteq V'$, and $\dim V = \dim V'$ finite, then $V = V'$.
- From every generating set G of a subspace V of finite dimension one can effectively extract a *basis*, that is a free generating set of V.

For the rest of this section, $\mathbb{K}$ is a division ring.

4.1 Rank of a series

Definition 26. The *rank* $\mathsf{r}(s)$ of a series s of $\mathbb{K}\langle\langle A^* \rangle\rangle$ is the dimension of the subspace of $\mathbb{K}\langle\langle A^* \rangle\rangle$ generated by $\mathbf{R}_s$ the set of (left) quotients of s:

$$\mathsf{r}(s) = \dim \langle \mathbf{R}_s \rangle \ .$$

In this setting, and with no further ado, Theorem 23 becomes:

Theorem 27. *A series s of $\mathbb{K}\langle\langle A^* \rangle\rangle$ is recognisable if and only if $\mathsf{r}(s)$ is finite.* ∎

Let $\mathcal{A}$ be a $\mathbb{K}$-representation of dimension n that realises s.[4] From Property 19 follows that $\mathsf{r}(s)$ is smaller than, or equal to, $\dim(\mathrm{Im}\, \Phi_{\mathcal{A}})$ which is smaller than, or equal to, n. Hence the minimal dimension of a representation for s is $\mathsf{r}(s)$.

[4] In this context where we compare dimensions, it is more convenient they be integers rather than sets.

Definition 28. A representation of a recognisable series s is *reduced* if its dimension is equal to the rank of s.

From Proposition 25 follows that reduced representations do exist since we have:

Property 29. *With every basis of* $\langle \mathbf{R}_s \rangle$ *is associated a reduced representation of* s.

Conversely, reduced representations are characterised by the following statement.

Theorem 30. *A* $\mathbb{K}$*-representation* $\mathcal{A}$ *is reduced if and only if it is both* controllable *and* observable*, that is, if and only if* $\Psi_{\mathcal{A}}$ *is surjective, and* $\Phi_{\mathcal{A}}$ *injective.*

Proof. Let s be the series realised by $\mathcal{A}$. The morphism

$$\Phi_{\mathcal{A}} \circ \Psi_{\mathcal{A}} \colon \mathbb{K}\langle A^* \rangle \longrightarrow \mathbb{K}\langle\langle A^* \rangle\rangle \qquad \text{is such that} \qquad [\Phi_{\mathcal{A}} \circ \Psi_{\mathcal{A}}](w) = w^{-1}s$$

for every w in A^* and $\mathsf{Im}\,[\Phi_{\mathcal{A}} \circ \Psi_{\mathcal{A}}]$ is the subspace $\langle \mathbf{R}_s \rangle$. For the dimension of $\mathsf{Im}\,[\Phi_{\mathcal{A}} \circ \Psi_{\mathcal{A}}]$ be equal to n, the dimension of $\mathcal{A}$, it is necessary, and sufficient, that the dimension of both $\mathsf{Im}\,\Psi_{\mathcal{A}}$ and $\mathsf{Im}\,\Phi_{\mathcal{A}}$ be equal to n. The second equality holds if and only if the dimension of $\mathsf{Ker}\,\Phi_{\mathcal{A}}$ is zero. ∎

4.2 Reduction of a representation

It is not enough to know that reduced representations exist and to characterise them. We want to effectively compute them and, for that purpose, we establish the following.

Theorem 31. *A reduced representation of a recognisable series* s *is effectively computable from any representation that realises* s *with a procedure whose complexity is cubic in the dimension of the representation.*

For the rest of this section, let $\mathcal{A}$ be a $\mathbb{K}$-representation of A^* of dimension n, that realises the series $s = |\mathcal{A}|$. Let us first assume that, given $\mathcal{A}$, one can effectively compute a *basis* of the subspace $\mathsf{Im}\,\Psi_{\mathcal{A}}$ (this will be proved in the next subsection, where the complexity of the whole procedure will be established as well).

Proposition 32. *Let* G *be a basis of the state-space* $\mathsf{Im}\,\Psi_{\mathcal{A}}$*, of cardinal* m*. This basis determines a* $\mathbb{K}$*-representation* $\mathcal{A}'$ *of dimension* m*, conjugate to* $\mathcal{A}$*, and with the properties:*

(i) $\Psi_{\mathcal{A}'}$ *is surjective (*$\mathcal{A}'$ *is controllable);*

(ii) *if* $\Phi_{\mathcal{A}}$ *is injective, so is* $\Phi_{\mathcal{A}'}$ *(if* $\mathcal{A}$ *is observable, so is* $\mathcal{A}'$*).*

Proof. By Proposition 6 and with the notation set there, the existence of G, generating set of $\mathsf{Im}\,\Psi_{\mathcal{A}}$ of cardinal m, implies the one of a $\mathbb{K}$-representation $\mathcal{A}' = \langle J, \kappa_G, U \rangle$ of dimension m which is conjugate to $\mathcal{A} = \langle I, \mu, T \rangle$ by M_G, that is, such that:

$$I = \alpha_G(J) = J \cdot M_G\,, \quad \forall a \in A \quad \kappa_G(a) \cdot M_G = M_G \cdot \mu(a)\,, \quad U = M_G \cdot T\ .$$

Since G is a *basis*, $\mathsf{dim}(\mathsf{Im}\,\Psi_{\mathcal{A}}) = \mathsf{dim}(\mathbb{K}^G) = m$ and α_G is *injective*. The diagram of Figure 5, that will be shown to commute, helps in following the next sequences of equalities.

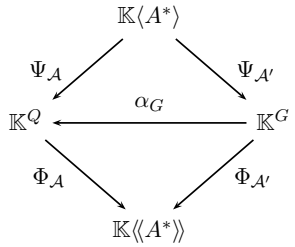


Figure 5: A diagram for Proposition 32

For every w in A^*, it then comes:

$$\begin{aligned}\Psi_{\mathcal{A}}(w) = I \cdot \mu(w) = \alpha_G(J) \cdot \mu(w) = J \cdot M_G \cdot \mu(w) \\ = J \cdot \kappa_G(a) \cdot M_G = \alpha_G(J \cdot \kappa_G(a)) = \alpha_G(\Psi_{\mathcal{A}'}(w)) \quad .\end{aligned}$$

Hence $\Psi_{\mathcal{A}} = \alpha_G \circ \Psi_{\mathcal{A}'}$. Since $\mathsf{dim}(\mathsf{Im}\,\Psi_{\mathcal{A}}) = m$ and α_G is injective, $\mathsf{dim}(\mathsf{Im}\,\Psi_{\mathcal{A}'}) = m$ and $\Psi_{\mathcal{A}'}$ is surjective.

Let x in $\Psi_{\mathcal{A}'}(A^*)$, that is, there exists w in A^* such that $x = \Psi_{\mathcal{A}'}(w)$.
Then $\Phi_{\mathcal{A}'}(x) = \Phi_{\mathcal{A}'}(\Psi_{\mathcal{A}'}(w)) = w^{-1}s$.

On the other hand, $\Phi_{\mathcal{A}}(\alpha_G(\Psi_{\mathcal{A}'}(w))) = \Phi_{\mathcal{A}}(\Psi_{\mathcal{A}}(w))\, w^{-1}s$, and then

$$\Phi_{\mathcal{A}'}(x) = \Phi_{\mathcal{A}}(\alpha_G(x)) \quad . \tag{4.1}$$

Since $\Psi_{\mathcal{A}'}(A^*)$ generates $\mathbb{K}^G$, (4.1) holds on the whole space $\mathbb{K}^G$ and $\Phi_{\mathcal{A}'} = \Phi_{\mathcal{A}} \circ \alpha_G$. Since α_G is injective, if $\Phi_{\mathcal{A}}$ is injective, so is $\Phi_{\mathcal{A}}$. ∎

We now introduce the *transpose* of the representation $\mathcal{A}$, $\mathcal{A}^{\mathsf{t}} = (T^{\mathsf{t}}, \mu^{\mathsf{t}}, I^{\mathsf{t}})$ where $\mu^{\mathsf{t}}(a) = (\mu(a))^{\mathsf{t}}$ for every a in A and it comes $\mu^{\mathsf{t}}(w) = (\mu(w^{\mathsf{t}}))^{\mathsf{t}}$ for every w in A^*. We then have the following connection between $\mathcal{A}$ and $\mathcal{A}^{\mathsf{t}}$.

Remark 33. The use of the transpose of a $\mathbb{K}$-representation is not satisfactory as it is not well-defined when $\mathbb{K}$ is *not commutative*, a case that we want to cover. On the other hand , it is an easy shortcut, as it save the definition the dual of every notion we have defined so far (state-space, control morphism, *etc.*). It is enough to say that it is legitimate for the case where $\mathbb{K}$ is commutative, which holds in all the forthcoming examples and exercices and that there exists a method to overcome the problem when needed (as in the case of Corollary 43 for instance).

Lemma 34. *If $\Psi_{\mathcal{A}^{\mathsf{t}}}$ is surjective, then $\Phi_{\mathcal{A}}$ is injective.*

Proof. If $\Phi_{\mathcal{A}}(x) = 0$ then $x \cdot \mu(w) \cdot T = 0$ for every w in A^* and x belongs to the orthogonal of the subspace generated by the vectors $\{\mu(w) \cdot T \mid w \in A^*\}$ which is of dimension n by hypothesis: thus $x = 0$. ∎

Proof of Theorem 31. Starting from a representation $\mathcal{A}$, we first compute a basis for the state-space of $\mathcal{A}^{\mathsf{t}}$ which determines a representation $\mathcal{A}'^{\mathsf{t}}$ such that $\Psi_{\mathcal{A}'^{\mathsf{t}}}$ is surjective, and thus by Lemma 34, $\Phi_{\mathcal{A}'}$ is injective. We then compute a basis for the state-space of $\mathcal{A}'$ which determines a representation $\mathcal{A}''$ such that $\Psi_{\mathcal{A}''}$ is surjective and $\Phi_{\mathcal{A}''}$ is injective: $\mathcal{A}''$ is reduced. ∎

The proof of Theorem 31 will be complete when we have proved that basis for the state-spaces are effectively computable (with the ascribed complexity).

4.3 Effective computations

Word basis

Definition 35. We call *word basis* for $\mathcal{A}$ a prefix-closed subset P of A^* such that the set $\Psi_{\mathcal{A}}(P) = \{I \cdot \mu(p) \mid p \in P\}$ is a basis of $\mathsf{Im}\,\Psi_{\mathcal{A}}$.

Proposition 36. *Word basis for $\mathcal{A}$ do exist.*

Proof. If $I = 0$, $\mathsf{Im}\,\Psi_{\mathcal{A}}$ is the null vector space, of dimension 0 and the empty set (which is prefix-closed!) is a word basis. Assuming that I is non-zero, the family of prefix-closed subsets P of A^* such that $\{I \cdot \mu(p) \mid p \in P\}$ is a free subset of $\mathbb{K}^n$ is not empty since it contains at least the singleton $\{1_{A^*}\}$. Every such subset contains at most $k = \dim(\mathsf{Im}\,\Psi_{\mathcal{A}})$ elements and there exist thus maximal elements (for the inclusion order) in that family.

It remains to show that such a maximal element P is a word basis, that is, $\Psi_{\mathcal{A}}(P)$ generates $\mathsf{Im}\,\Psi_{\mathcal{A}}$. By way of contradiction, let w in A^* such that $I \cdot \mu(w)$ does not belong to $\langle \Psi_{\mathcal{A}}(P) \rangle$; the word w factorises in $w = pg$, with p in P, and we choose w in such a way that g is of minimal length. The word g is not empty: $g = ah$, with a in A, and $I \cdot \mu(w) = I \cdot \mu(pa) \cdot \mu(h)$. As P is maximal, $I \cdot \mu(pa)$ belongs to $\langle \Psi_{\mathcal{A}}(P) \rangle$ that is, $I \cdot (pa)\mu = \sum_{p_i \in P} x_i \, (I \cdot \mu(p_i))$. It then follows

$$I \cdot \mu(w) = \left(\sum_{p_i \in P} x_i \, (I \cdot \mu(p_i)) \right) \cdot \mu(h) = \sum_{p_i \in P} x_i \, (I \cdot \mu(p_i h)) \quad .$$

By the minimality of g, every $I \cdot \mu(p_i h)$ belongs to $\langle \Psi_{\mathcal{A}}(P) \rangle$: contradiction. ∎

In the sequel, we do not consider the trivial case $I = 0$ anymore.

If P is a non-empty prefix-closed subset of A^*, the *border of P* is the set:

$$C = PA \setminus P \quad .$$

As an example, the prefix-closed subset $\{1_{A^*}, b, ba\}$ and its border $\{a, bb, baa, bab\}$ are shown in Figure 6.

The following proposition and its proof exhibit the computation underlying Proposition 32.

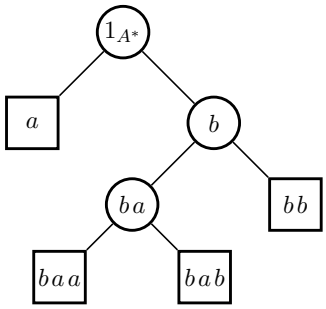


Figure 6: A prefix-closed subset and its border

Proposition 37. *Word basis for $\mathcal{A}$ are effectively computable, with complexity $O(dn^3)$, where d is the cardinal of A.*

Proof. We set $P_0 = \{1_{A^*}\}$ and $C_0 = \emptyset$. The algorithm to compute a word basis P can be written in the following manner.

If $E_k = (P_k A \setminus P_k) \setminus C_k$ is non-empty, choose an arbitrary w in E_k and decide whether $I \cdot \mu(w)$ belongs to $\langle I \cdot P_k \mu \rangle$.

(i) If not, then $P_{k+1} = P_k \cup \{w\}$ and $C_{k+1} = C_k$.

(ii) If so, then $P_{k+1} = P_k$ and $C_{k+1} = C_k \cup \{w\}$.

Set $k = k + 1$ and start again.

The algorithm terminates when E_k is empty and at that moment $C_k = P_k A \setminus P_k$ is the border of P_k. The algorithm must terminate since P_k has at most n elements, so $P_k \cup C_k$ has at most $\|A\| n + 1$ elements and this set grows by 1 at each step of the algorithm.

By construction, P_k is prefix-closed, and each element w of C_k is such that $I \cdot \mu(w)$ belongs to $\langle I \cdot \mu(P_k) \rangle$: when E_k is empty, P_k is maximal. ∎

Gaussian elimination The foregoing proofs all correspond to effective computations, assuming of course that the operations in $\mathbb{K}$ (addition, multiplication, taking the inverse) are effective. All the complexities that follow are calculated assuming that each operation in $\mathbb{K}$ has a fixed constant cost, independent of its operands.[5] Computations in $\mathbb{K}^n$ are based on the *Gaussian elimination* procedure.

Definition 38. A sequence of k vectors $(x^1, x^2, \ldots, x^k)$ of $\mathbb{K}^n$ is an *echelon system* if, for all i in $[k]$:

(i) $x^i{}_i = 1_{\mathbb{K}}$; (ii) $\forall j < i \quad x^i{}_j = 0_{\mathbb{K}}$.

An echelon system is free and hence $k \leqslant n$. The following proposition is classic, at least for commutative fields, and its proof is not really different for division rings.

[5] It is to be acknowledged that this is a completely unrealistic assumption.

Proposition 39 (Gaussian elimination)**.** *Let $\mathbb{K}$ be a skew field and let us view $\mathbb{K}^n$ as a left vector space over $\mathbb{K}$. Let $S = (x^1, x^2, \ldots, x^k)$ be an echelon system and let y be a vector in $\mathbb{K}^n$.*

(i) *We can decide whether y is in $\langle S \rangle$, the subspace generated by S, and, in this case, compute effectively the coordinates of y in S.*

(ii) *If y is not in $\langle S \rangle$, we can compute effectively y' such that $S' = S \cup \{y'\}$ is echelon and generates the same subspace as $S \cup \{y\}$.*

The complexity of these operations (deciding whether y is in $\langle S \rangle$ and computing the coordinates of either y or y') is $O(kn)$.

From this proposition we deduce the effective nature of the assertions, constructions, and specifications used in the proofs of this section. More precisely:

Corollary 40. *Let S be a finite set of vectors of $\mathbb{K}^n$ and let y be in $\mathbb{K}^n$. We can:*

(i) *decide whether y belongs to $\langle S \rangle$;*

(ii) *extract effectively from S a basis T of $\langle S \rangle$;*

(iii) *compute effectively the coordinates in T of an (explicitly given) vector of $\langle S \rangle$.*

5 Applications of the reduction of recognisable series

5.1 Decidability of the equivalence

Even if a series has not a unique reduced representation (they are all *similar*), the existence of reduced representations implies the decidability of equivalence for automata with weights in a field.

Theorem 41. *The equivalence of recognisable series over A^* with coefficients in a (sub-semiring of a) skew field — and thus of rational series — is decidable, with a procedure which is cubic in the dimension of the representation of the series.*

Proof. Let $\mathbb{K}$ be a sub-semiring of a skew field $\mathbb{F}$. Two series s_1 and s_2 of $\mathbb{K}\mathrm{Rec}\, A^*$ are also in $\mathbb{F}\mathrm{Rec}\, A^*$ and $s_1 = s_2$ holds if and only if $(s_1 - s_2)$ is a series of $\mathbb{F}\mathrm{Rec}\, A^*$ of rank 0, and the rank of $(s_1 - s_2)$ can be computed effectively. ∎

This result, together with the well-known decidability of equivalence of classical Boolean automata, should not let us think that this is the universal status. For instance, the following holds.

Theorem 42 (Krob)**.** *The equivalence of recognisable series over A^* with coefficients in the semiring $\mathbb{M} = \langle \mathbb{N}, \mathsf{min}, + \rangle$ is undecidable.*

Theorem 41 has however far reaching and to some extent 'unexpected' consequences, as the following one, discovered by T. Harju and J. Karhumäki.

Corollary 43. *The equivalence of rational series over $A_1^* \times A_2^* \times \cdots \times A_k^*$ with coefficients in $\mathbb{N}$ is decidable.*

Proof. A series in $\mathbb{N}\mathrm{Rat}\,(A_1^* \times A_2^* \times \cdots \times A_k^*)$ is a series in $[\mathbb{N}\mathrm{Rat}\,(A_2^* \times \cdots \times A_k^*)]\mathrm{Rat}\,A_1^*$. By Theorem 46, the latter family is isomorphic to $[\mathbb{N}\mathrm{Rat}\,(A_2^* \times \cdots \times A_k^*)]\mathrm{Rec}\,A_1^*$ and the decidability of equivalence follows from Theorem 44. ∎

Theorem 44. *$\mathbb{N}\mathrm{Rat}\,(A_2^* \times \cdots \times A_k^*)$ is a sub-semiring of a skew field.*

This result is the direct consequence of a series of classical results in mathematics which we shall not present here.

cf.EAT, Sec. IV.7, p. 616

5.2 From the series to the representation

Another way to exploit Proposition 32, is by 'computing' the coefficients of a *reduced representation* of a recognisable series as a function of the coefficients of the series itself. Going from the series back to the representation does not so much correspond to an effective procedure as it expresses a fundamental property of recognisable series on a field (see an application with Theorem 46).

Proposition 45. *Let $\mathbb{K}$ be a skew field, s a $\mathbb{K}$-recognisable series of rank n, and $\langle I, \mu, T \rangle$ a reduced representation of s. There exist two sets of n words: $P = \{p_1, p_2, \ldots, p_n\}$ and $Q = \{q_1, q_2, \ldots, q_n\}$ (which we can choose to be respectively prefix-closed and suffix-closed) and two $n \times n$ matrices α_P and β_Q such that*

$$\forall w \in A^* \qquad \mu(w) = \alpha_P \cdot (\langle s, p_i\, w\, q_j \rangle) \cdot \beta_Q \ ,$$

where $(\langle s, p_i\, w\, q_j \rangle)$ denote the $n \times n$ matrix whose entry (i, j) is $\langle s, p_i\, w\, q_j \rangle$.

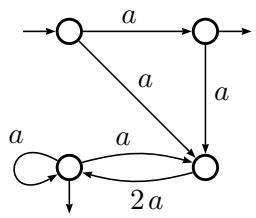
A remarkable application of this result is the following.

Theorem 46. *Let $\mathbb{K}$ be a (skew) field. If s is a $\mathbb{K}$-rational series with a finite image, then $k\, s^{-1}$ is rational for all k in $\mathbb{K}$.*

Proof. Let $\langle I, \mu, T \rangle$ be a reduced representation that recognises s. By Proposition 45, the image $\mu(A^*)$ is a *finite submonoid* of $\mathbb{K}^{Q \times Q}$ if s has a finite image and the conclusion follows. ∎

6 Exercises

1. Compute the reduced representation of the following $\mathbb{N}$-automaton.



2. Let $\mathcal{A}_1$ be the $\mathbb{Q}$-automaton on $\{a\}^*$ shown at Figure 7 (the unique letter a of the alphabet is not shown on the transitions of the figure). Compute a reduced automaton, equivalent to $\mathcal{A}_1$.

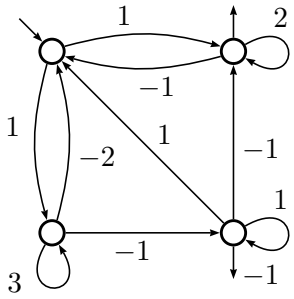


Figure 7: The $\mathbb{Q}$-automaton $\mathcal{A}_1$

3. Consider the minimal (Boolean) automaton of $\{a^n \mid n \equiv 0, 1, 2, 4 \pmod 7\}$ as an automaton with multiplicity in $\mathbb{Z}/2\mathbb{Z}$ and reduce it. Comment.

4. Let $\mathbb{F}$ be a field. Show that two $\mathbb{F}$-recognisable series over A^* are equal if and only if they coincide on all the words of length less than the sum of the dimensions of the representations which realise them.

Show the bound is sharp. [*Hint: consider the following two automata.*]

5. **Discriminating length.** We call the *discriminating length* between two non-equivalent (Boolean) automata $\mathcal{A}$ and $\mathcal{B}$ the length of a shortest word which is accepted by one and not the other. We write $L_{\mathsf{d}}(n, m)$ (resp. $L_{\mathsf{nd}}(n, m)$) for the maximum of the discriminating lengths when $\mathcal{A}$ and $\mathcal{B}$ have respectively n and m states and are deterministic (resp. and are non-deterministic).

(a) With methods relevant to Boolean automata, show that $L_{\mathsf{d}}(n, m) \leqslant n\, m$.

(b) Compute $L_{\mathsf{d}}(n, m)$.

(c) Give an upper bound for $L_{\mathsf{nd}}(n, m)$.

Notation Index

General Index