Lecture I — Exercises with solution

Unless stated otherwise, the alphabet A is $A = \{a, b\}$.

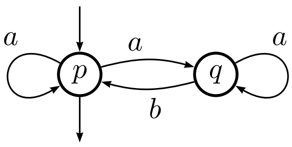
1. **Semiring structure.** *Is* $\mathbb{M} = \langle\, \mathbb{N}, \mathsf{max}, +, 0, 0\,\rangle$ *a semiring?*

No. It is true that 0 is an identity element for both the addition max and the multiplication $+$ of $\mathbb{M}$ but it is not a *zero* for the multiplication (since it is the identity element) and axiom 'SA4' is not satisfied.

2. **Positive semiring.** *Give an example of a semiring in which the sum of any two non-zero elements is non-zero but which is not positive.*

The subsemiring of $\mathbb{N}^{2\times 2}$ generated by $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ and $\begin{pmatrix}0&0\\0&1\end{pmatrix}$ answers the question.

3. **Example of $\mathbb{N}$-automaton.** (a) *Compute the coefficient of $a^3 b\, a^2 b\, a$ in the series realised by the $\mathbb{N}$-automaton:*



(b) *Give the general formula for the coefficient of every word of A^*.*

(a) A 'successful' computation whose label is $a^3 b\, a^2 b\, a$ is necessarily of the form

$$p \xrightarrow{a} r_1 \xrightarrow{a} r_2 \xrightarrow{a} q \xrightarrow{b} p \xrightarrow{a} s_1 \xrightarrow{a} q \xrightarrow{b} p \xrightarrow{a} p \quad .$$

There are 3 possible choices for the pair r_1, r_2 : p, p , p, q , and q, q , 2 choices for s_1 : p and q , hence 6 possible computations, each one with weight 1: the weight of $a^3 b\, a^2 b\, a$ is 6.

(b) More generally, every word w of $\{a, b\}^*$ with k occurrences of b may be writen as:

$$a^{n_1} b\, a^{n_2} b \cdots a^{n_k} b\, a^{n_{k+1}} \quad .$$

With the same reasonning as above, every factor a^{n_i}, $1 \leq i \leq k$, gives rise to n_i computations, the factor $a^{n_{k+1}}$ to 1 computation: the coefficient of w is $\prod_{i=1}^{i=k} n_i$.

4. **Examples of $\mathbb{N}\mathsf{min}$, $\mathbb{N}\mathsf{max}$-automata.** *Let $\mathcal{E}_1$ be the $\mathbb{N}\mathsf{min}$-automaton over $\{a\}^*$ shown in Fig. 1 (a) and $\mathcal{E}_2$ the $\mathbb{N}\mathsf{max}$-automaton shown in the same figure. Similarly, let $\mathcal{E}_3$ and $\mathcal{E}_4$ be the $\mathbb{N}\mathsf{min}$ and $\mathbb{N}\mathsf{max}$-automata shown in Fig. 1 (b).*

Give a formula for $\langle\!|\mathcal{E}_1|, a^n\rangle$, $\langle\!|\mathcal{E}_2|, a^n\rangle$, $\langle\!|\mathcal{E}_3|, a^n\rangle$, and $\langle\!|\mathcal{E}_4|, a^n\rangle$.

(a) The automata $\mathcal{E}_1$ and $\mathcal{E}_2$ (b) The automata $\mathcal{E}_3$ and $\mathcal{E}_4$

Figure 1: 'Four' 'tropical' automata

For every n, there are $n+1$ computations with label a^n in each of the four automata. In $\mathcal{E}_1$ and $\mathcal{E}_4$, the 'victorious' computation, that is, the one that gives a^n its weight in $\mathcal{E}_1$ or $\mathcal{E}_4$, is the one that stays in state p and, for every n in $\mathbb{N}$:

$$\langle\!| \mathcal{E}_1 |\!, a^n \rangle = n \qquad \text{and} \qquad \langle\!| \mathcal{E}_4 |\!, a^n \rangle = 2\,n \enspace .$$

In $\mathcal{E}_2$ and $\mathcal{E}_3$, the 'victorious' computation, is the one that goes to state q and then:[1]

$$\langle\!| \mathcal{E}_2 |\!, a^n \rangle = 2\,n-1 \quad \text{and} \quad \langle\!| \mathcal{E}_3 |\!, a^n \rangle = n+1 \quad \text{for } n \geq 1 \quad \text{and} \quad \langle\!| \mathcal{E}_2 |\!, 1_{a^*} \rangle, = \langle\!| \mathcal{E}_3 |\!, 1_{a^*} \rangle = 0 \enspace .$$

5. **A $\mathbb{Z}$-automaton.**
Build a $\mathbb{Z}$-automaton $\mathcal{D}_1$ such that $\langle\!| \mathcal{D}_1 |\!, w \rangle = |w|_a - |w|_b$, for every w in A^*.

The automaton shown at Figure 2 answers the question. It is derived from the automaton $\mathcal{B}_1$.

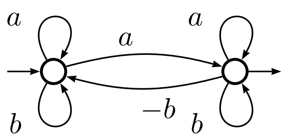


Figure 2: The $\mathbb{Z}$-automaton $\mathcal{D}_1$

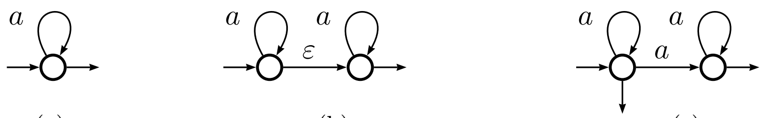
6. **Support of $\mathbb{Z}$-automata.**
Give an example of a $\mathbb{Z}$-automaton $\mathcal{A}$ such that the inclusion $\mathsf{supp}\, (\!|\mathcal{A}|\!) \subseteq |\mathsf{supp}\ \mathcal{A}|$ *is strict.*

The automaton $\mathcal{D}_1$ of the previous Exercise 5. answers the question.

7. **Automata construction.** *Let $\underline{a^*}$ be the characteristic $\mathbb{N}$-series of a^* : $\underline{a^*} = \sum_{n\in\mathbb{N}} a^n$. Give an 'automatic' proof (that is, by means of automata constructions) for:*

$$(\underline{a^*})^2 = \sum_{n\in\mathbb{N}} (n+1)\, a^n \enspace .$$

An automaton which realises the series $\underline{a^*}$ is shown at Fig. 3 (a). The Cauchy product $(\underline{a^*})^2 = \underline{a^*}\,\underline{a^*}$ is realised by the *concatenation* of automata, shown at Fig. 3 (b) with a spontaneous transition, and at Fig. 3 (c)after elimination of that spontaneous transition by (backward) closure. It is easily seen on this last automaton that there are $n+1$ distinct computations for the word a^n, each one with a weight 1.



(a) (b) (c)

Figure 3: Automatic construction of Cauchy product

[1] This exercise looks somewhat dumb. It gains some more interest when one looks at the decision of the *sequentiality* of the series realised by these automata. A subject that has not been treated this year.

8. **Shortest run and $\mathbb{N}\mathsf{min}$-automata.**
Build a $\mathbb{N}\mathsf{min}$-automaton $\mathcal{F}_1$ such that, for every w in A^*, $\langle\!|\mathcal{F}_1|, w\rangle$ is the minimal length of runs of 'a' 's in w, that is, if $w = a^{n_0}\,b\,a^{n_1}\,b\cdots a^{n_{k-1}}\,b\,a^{n_k}$, then $\langle\!|\mathcal{F}_1|, w\rangle = \mathsf{min}\{n_0, n_1, \ldots, n_k\}$.

The $\mathbb{N}\mathsf{min}$-automaton shown at Figure 4 answers the question. If the shortest run is found at the beginning of w, that is, if $n_0 = \mathsf{min}\{n_0, n_1, \ldots, n_k\}$, then a victorious computation is found between state i and state q; if it is found at the end of w, that is, if $n_k = \mathsf{min}\{n_0, n_1, \ldots, n_k\}$, then a victorious computation is found between state q and state t; in all other cases, a victorious computation is found between state i and state t.

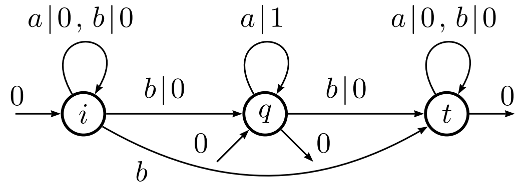


Figure 4: An automaton for computing the length of shortest run

9. **Identification of a $\mathbb{Q}$-automaton.** *Show that the final function of the $\mathbb{Q}$-automaton $\mathcal{Q}_2$ over $\{a\}^*$ depicted on the right in Figure 5 (where every transition is labelled by $a\,|\,1$) can be specified in such a way the result is equivalent to $\mathcal{Q}_1$ depicted on the left.*

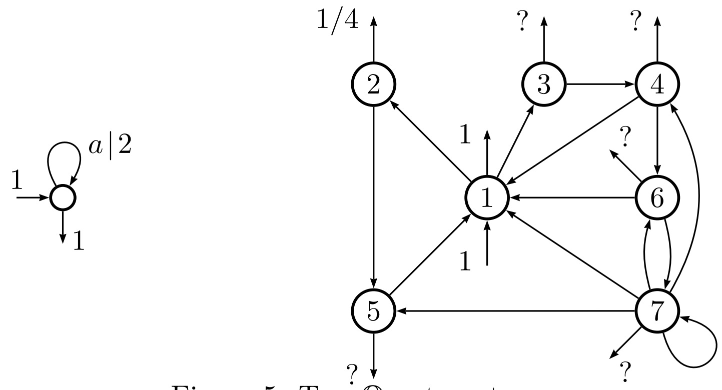


Figure 5: Two $\mathbb{Q}$-automata

The representation of $\mathcal{Q}_2$ is $(\,I, \mu, T\,)$ where

$$I = \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix}, \quad \mu(a) = \mu = \begin{pmatrix}0&1&1&0&0&0&0\\0&0&0&0&1&0&0\\0&0&0&1&0&0&0\\1&0&0&0&0&1&0\\1&0&0&0&0&0&0\\1&0&0&0&0&0&1\\1&0&0&1&1&1&1\end{pmatrix}, \quad T = \begin{pmatrix}1\\1/4\\x_3\\x_4\\x_5\\x_6\\x_7\end{pmatrix}$$

The equivalence between $\mathcal{Q}_2$ and $\mathcal{Q}_1$ implies then the sequence of equations:

$$
\begin{aligned}
I \cdot T &= 1 && \text{which holds}\\
I \cdot \mu \cdot T &= 1/4 + x_3 = 2 && \text{which implies } x_3 = 7/4\\
I \cdot \mu^2 \cdot T &= x_4 + x_5 = 4 &&\\
I \cdot \mu^3 \cdot T &= 2 + x_6 = 8 && \text{which implies } x_6 = 6\\
I \cdot \mu^4 \cdot T &= 5 + x_7 = 16 && \text{which implies } x_7 = 11
\end{aligned}
$$

It is verified that the computation of $I \cdot \mu^5 \cdot T$, $I \cdot \mu^6 \cdot T$, and $I \cdot \mu^7 \cdot T$ all lead to the condition $x_4 + x_5 = 4$. Further developments show then that if this condition is satisfied, then the two automata are equivalent (*cf.* Exercise **??**).

10. **Ambiguous automata.** *Show that it is decidable whether a Boolean automaton is unambiguous or not.*

11. **Representation with finite image.** *Let s be a $\mathbb{K}$-recognisable series of A^*, realised by a representation $\langle I, \mu, T \rangle$ of dimension Q. Show that if $\mu(A^*)$ is a finite submonoid of $\mathbb{K}^{Q \times Q}$, then, for every k in $\mathbb{K}$ the set $s^{-1}(k) = \{w \in A^* \mid \langle s, w \rangle = k\}$ is a recognisable language of A^*.*

Let $M = \mu(A^*)$ be the finite submonoid of $\mathbb{K}^{Q \times Q}$, image of A^* by μ: $\mu \colon A^* \to M$. For every k in $\mathbb{K}$, let P_k be the subset of M defined by $P_k = \{m \in M \mid I \cdot m \cdot T = k\}$. Then, $s^{-1}(k) = \mu^{-1}(P_k)$ is a recognisable language of A^*, by definition.

12. **Support of $\mathbb{Z}$-rational series.** (a) *Give an example of a $\mathbb{Z}$-rational series over A^* whose support is not a recognisable language of A^*.*

(b) *Give an example of a $\mathbb{Z}$-rational series over A^* which is an $\mathbb{N}$-series (that is, all coefficients are non-negative) and which is not an $\mathbb{N}$-rational series over A^*.*

Let $d_1 = |\mathcal{D}_1|$ be the series realised by the $\mathbb{Z}$-automaton $\mathcal{D}_1$ of Figure 2. Then, $\mathsf{supp}\ d_1 = \{w \in A^* \mid |w|_a \neq |w|_b\}$ is not a recognisable language of A^*. The series $d_2 = d_1 \odot d_1$ has the same support as d_1 and all its coefficients, which are squares, are non-negative.

13. **Support of $\mathbb{Z}$-rational series.** (a) *Prove that the support of an $\mathbb{N}$-rational series over A^* is a recognisable language of A^*.*

(b) *Let s be in $\mathbb{N}\mathrm{Rec}\, A^*$. Prove that for any k in $\mathbb{N}$, the sets*
$$s^{-1}(k) = \{w \in A^* \mid \langle s, w \rangle = k\} \quad \text{and} \quad s^{-1}(k + \mathbb{N}) = \{w \in A^* \mid \langle s, w \rangle \geqslant k\}$$
are recognisable languages of A^*.

(c) *Give an example of a $\mathbb{Z}$-rational series s over A^* such that there exists an integer z such that $s^{-1}(z)$ is not a recognisable language of A^*.*

(a) There are many ways to prove the statement. One in the line of the proofs to come is the following. Let $\sigma \colon \mathbb{N} \to \mathbb{B}$ be the support map, which is a morphism since $\mathbb{N}$ is positive. The image of a $\mathbb{N}$-rational, hence $\mathbb{N}$-recognisable, series s over A^* under σ is precisely $\mathsf{supp}\ s$ and is a $\mathbb{B}$-recognisable series over A^*, that is, a recognisable language.

(b) It is easy to verify that, for any integer $h \geq 1$, the structure $\mathbb{N}_h = \langle [0, 1, \ldots, h], \oplus, \otimes \rangle$ defined by:

$$\forall x, y \in [0, 1, \ldots, h] \qquad x \oplus y = \mathsf{min}(x + y, h) \qquad \text{and} \qquad x \otimes y = \mathsf{min}(x\,y, h) \ .$$

is a (finite) semiring. Somehow, h plays the role of an infinity element but 'at finite distance'.

The map $\sigma_h\colon \mathbb{N} \to \mathbb{N}_h$ defined by $\sigma_h(x) = \mathsf{min}(x,h)$ is a semiring morphism. (Note that $\mathbb{B} = \mathbb{N}_1$ and that the support map σ is σ_1.)

It then follows that if a $\mathbb{N}$-series s over A^* is realised by a representation $(\,I,\mu,T\,)$ then $\sigma_h(s)$ is a $\mathbb{N}_h$-series realised by the representation $(\,\sigma_h(I),\mu_h,\sigma_h(T)\,)$ where $\mu_h(a) = \sigma_h(\mu(a))$, for every a of A. Moreover, for every w in A^*, $\langle s,w\rangle = k$ if and only if $\langle \sigma_h(s),w\rangle = k$ for any $h > k$ and $\langle s,w\rangle \geq k$ if and only if $\langle \sigma_k(s),w\rangle = k$, that is, $s^{-1}(k) = (\sigma_h(s))^{-1}(k)$ and $s^{-1}(k+\mathbb{N}) = (\sigma_k(s))^{-1}(k)$.

Since $\mathbb{N}_h$ is finite, it follows that $\mu_h(A^*)$ is finite and the conclusion follows from Exercise 11..

(c) The series d_1 of Exercise 12. will serve again as an example:

$$d_1^{-1}(0) = \{w \in A^* \mid |w|_a = |w|_b\}$$

is not a recognisable language and the same indeed holds for $d_1^{-1}(z)$ for any z in $\mathbb{Z}$.

14. **Support of $\mathbb{Z}\mathsf{min}$-rational series.** (a) *Let s be a $\mathbb{N}\mathsf{min}$-rational series over A^*. Prove that for any k in $\mathbb{N}$, the sets*

$$s^{-1}(k) = \{w \in A^* \mid \langle s,w\rangle = k\} \qquad \text{and} \qquad s^{-1}(k+\mathbb{N}) = \{w \in A^* \mid \langle s,w\rangle \geqslant k\}$$

are recognisable languages of A^*.

(b) *Give an example of a $\mathbb{Z}\mathsf{min}$-rational series s over A^* such that there exists an integer z such that $s^{-1}(z)$ is not a recognisable language of A^*.*

(a) The proof follows the same pattern as the one of the preceding Exercise 13.. The structure $\mathbb{M}_h = \langle\, [0,1,\ldots,h] \cup \{+\infty\}, \mathsf{min}, \oplus \,\rangle$ defined by:

$$\forall x,y \in [0,1,\ldots,h] \cup \{+\infty\} \qquad x \oplus y = \mathsf{min}(x+y,h)$$

is a (finite) semiring and the map $\psi_h\colon \mathbb{N}\mathsf{min} \to \mathbb{M}_h$ defined by $\psi_h(x) = \mathsf{min}(x,h)$ is a semiring morphism.

If a $\mathbb{N}\mathsf{min}$-series s over A^* is realised by a representation $(\,I,\mu,T\,)$ then $\psi_h(s)$ is a $\mathbb{M}_h$-series realised by the representation $(\,\psi_h(I),\mu_h,\psi_h(T)\,)$ where $\mu_h(a) = \psi_h(\mu(a))$, for every a of A. Moreover, for every w in A^*, $\langle s,w\rangle = k$ if and only if $\langle \psi_h(s),w\rangle = k$ for any $h > k$ and $\langle s,w\rangle \geq k$ if and only if $\langle \psi_k(s),w\rangle = k$, that is, $s^{-1}(k) = (\psi_h(s))^{-1}(k)$ and $s^{-1}(k+\mathbb{N}) = (\psi_k(s))^{-1}(k)$.

Since $\mathbb{M}_h$ is finite, it follows that $\mu_h(A^*)$ is finite and the conclusion follows from Exercise 11..

(b) The $\mathbb{Z}\mathsf{min}$-series e_1 defined by $\langle e_1,w\rangle = \langle d_1,w\rangle = |w|_a - |w|_b$ is a $\mathbb{Z}\mathsf{min}$-recognisable series accepted by the following $\mathbb{Z}\mathsf{min}$-automaton.

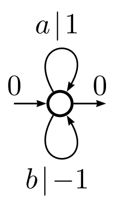


Figure 6: A $\mathbb{Z}\mathsf{min}$-automaton

15. **Recognisable series in direct product of free monoids.** *Let* $\mathbb{K}$ *be a commutative semiring. The two semirings* $\mathbb{K}\langle\langle A^*\rangle\rangle$ *and* $\mathbb{K}\langle\langle B^*\rangle\rangle$ *are canonically subalgebras of* $\mathbb{K}\langle\langle A^* \times B^*\rangle\rangle$*; the injection is induced by*

$$u \mapsto (u, 1_{B^*}) \qquad \text{and} \qquad v \mapsto (1_{A^*}, v) \ \ ,$$

for all u *in* A^* *and all* v *in* B^*. *Modulo this identification, a product* $(k\,u)\,(h\,v)$ *is written* $k\,h\,(u,v)$ *and the extension by linearity of this notation gives the following definition.*

Definition 1. Let s be in $\mathbb{K}\langle\langle A^*\rangle\rangle$ and t be in $\mathbb{K}\langle\langle B^*\rangle\rangle$. The *tensor product* of s and t, written $s \otimes t$, is the series of $\mathbb{K}\langle\langle A^* \times B^*\rangle\rangle$ defined by:

$$\forall (u,v) \in A^* \times B^* \qquad \langle s \otimes t, (u,v)\rangle = \langle s, u\rangle\,\langle t, v\rangle \ \ .$$

On the other hand, $\mathbb{K}$-recognisable series *over a non-free monoid* M *are defined, exactly as the* $\mathbb{K}$*-recognisable series over a free monoid, as the series realised by a* $\mathbb{K}$*-representation* $\langle\, I, \mu, T\,\rangle$, *where* μ *is a morphism from* M *into* $\mathbb{K}^{Q\times Q}$.

Establish:

Proposition 2. *A series* s *of* $\mathbb{K}\langle\langle A^* \times B^*\rangle\rangle$ *is recognisable if and only if there exists a finite family* $\{r_i\}_{i\in I}$ *of series of* $\mathbb{K}\mathrm{Rec}\,A^*$ *and a finite family* $\{t_i\}_{i\in I}$ *of series of* $\mathbb{K}\mathrm{Rec}\,B^*$ *such that*

$$s = \sum_{i\in I} r_i \otimes t_i \ \ .$$

16. **Distance on the semirings of series.**

A distance *on any set* S *is a map* $\mathbf{d}\colon S \times S \to \mathbb{R}_+$ *with the three properties: for all* x, y *and* z *in* S *it holds:*

(i) symmetry*:* $\mathbf{d}(x,y) = \mathbf{d}(y,x)$;

(ii) positivity*:* $\mathbf{d}(x,y) = 0 \Leftrightarrow x = y$;

(iii) triangular inequality*:* $\mathbf{d}(x,z) \leqslant \mathbf{d}(x,y) + \mathbf{d}(y,z)$.

If (iii) is replaced by the stronger property:

(iv) triangular inequality*:* $\mathbf{d}(x,z) \leqslant \mathsf{max}\,(\mathbf{d}(x,y), \mathbf{d}(y,z))$,

then $\mathbf{d}$ *is said to be an* ultrametric distance.

(a) *Show that the function defined on* S *by*

$$\forall x,y \in S \qquad \mathbf{d}(x,y) = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{otherwise} \end{cases}$$

is an ultrametric distance. We call it the discrete distance *on* S.

Classically, a sequence $\left(s_n\right)_{n\in\mathbb{N}}$ *of elements of* S converges *to* s *in* S *for the distance* $\mathbf{d}$ *if:*

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n > N \qquad \mathbf{d}(s_n, s) < \varepsilon \ \ .$$

In this way, a distance $\mathbf{d}$ *defines a* topology *on* S.

(b) Show that if S is equipped with the discrete distance, the only convergent sequences are the ultimately stationnary sequences.

Two distances on S are *equivalent* if the same sequences converge, that is, $\mathbf{d}$ and $\mathbf{d}'$ are equivalent if for any sequence $s = \left(s_n\right)_{n\in\mathbb{N}}$, s converges for $\mathbf{d}$ if and only if it converges for $\mathbf{d}'$.

(c) Show that one can always assume that *a distance is bounded by* 1, that is, if $\mathbf{d}$ is a distance on S, the function $\mathbf{f}$ defined by

$$\forall x, y \in S \qquad \mathbf{f}\,(x,y) = \mathsf{inf}\{\mathbf{d}\,(x,y)\,, 1\}$$

is a distance, equivalent to $\mathbf{d}$.

(d) Let $\mathbf{d}$ and $\mathbf{d}$' be two distances on S. Show that if there exist two constant C and D in $\mathbb{R}_+ \setminus \{0\}$ such that

$$\forall x, y \in S \qquad C\,\mathbf{d}\,(x,y) \leqslant \mathbf{d}\text{'}\,(x,y) \leqslant D\,\mathbf{d}\,(x,y)$$

then $\mathbf{d}$ and $\mathbf{d}$' are equivalent. Is this condition necessary for $\mathbf{d}$ and $\mathbf{d}$' be equivalent?

Let $\mathbb{K}$ be a semiring. For s and t in $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$, let $\mathbf{e}(s,t)$ be the *gap between s and t*, defined as the minimal length of words on which s and t are different:

$$\mathbf{e}(s,t) = \mathsf{min}\,\{n \in \mathbb{N} \mid \exists w \in A^*, \quad |w| = n \text{ and } \langle s, w\rangle \neq \langle t, w\rangle\} \quad .$$

The gap is a generalisation of the notion of *valuation* of a series. The valuation $\mathbf{v}(s)$ of s in $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$ is defined by:

$$\mathbf{v}(s) = \mathbf{e}(s,0) = \mathsf{min}\,\{|w| \mid \langle s, w\rangle \neq 0\} = \mathsf{min}\,\{|w| \mid w \in \mathsf{supp}\ s\} \quad .$$

Conversely, and if $\mathbb{K}$ is a *ring*, $\mathbf{e}(s,t) = \mathbf{v}(s-t)$.

(e) Show that the map defined by

$$\forall s, t \in \mathbb{K}\langle\!\langle A^*\rangle\!\rangle \qquad \mathbf{d}\text{'}\,(s,t) = 2^{-\,\mathsf{e}(s,t)} \tag{0.1}$$

is an ultrametric distance on $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$, bounded by 1.

(f) Let $\mathbf{c}$ be a distance on $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$, bounded by 1. Show that the map defined by

$$\forall s, t \in \mathbb{K}\langle\!\langle A^*\rangle\!\rangle \qquad \mathbf{d}\,(s,t) = \frac{1}{2}\sum_{n\in\mathbb{N}}\left(\frac{1}{2^n}\,\mathsf{max}\,\{\mathbf{c}\,(\langle s,w\rangle, \langle t,w\rangle) \mid |w| = n\}\right) \tag{0.2}$$

is a distance on $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$, bounded by 1.

(g) Show that, whatever the distance $\mathbf{c}$, $\mathbf{d}\,(s,t) \leqslant \mathbf{d}\text{'}\,(s,t)$ holds.

(h) Show that if $\mathbf{c}$ is the discrete distance, then $\mathbf{d}\text{'}\,(s,t) \leqslant 2\,\mathbf{d}\,(s,t)$ holds, hence that (0.1) and (0.2) define two equivalent distances on $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$ if $\mathbb{K}$ is equipped with the discrete distance.

(i) Show that the topology defined by $\mathbf{d}$ on $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$ is the topology of the simple convergence.

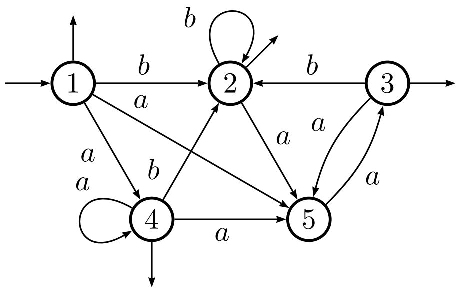
(j) Show that if $\mathbb{K}$ is a topological semiring, then so are $\mathbb{K}^{Q\times Q}$ (Q finite) and $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$.

(k) Let $\left(s_n\right)_{n\in\mathbb{N}}$ and $\left(t_n\right)_{n\in\mathbb{N}}$ be two sequences of series in the topological semiring $\mathbb{K}\langle\!\langle A^*\rangle\!\rangle$. Verify that $\left(s_n + t_n\right)_{n\in\mathbb{N}}$ or $\left(s_n\,t_n\right)_{n\in\mathbb{N}}$ may be convergent sequences, without $\left(s_n\right)_{n\in\mathbb{N}}$ or $\left(t_n\right)_{n\in\mathbb{N}}$ being convergent sequences.

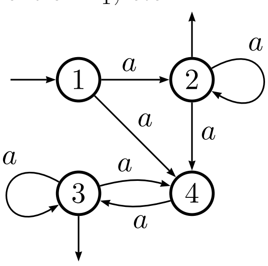
Lecture II — Exercises with solution

Unless stated otherwise, the alphabet A is $A = \{a, b\}$.

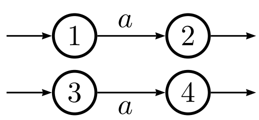
1. *Compute the (minimal) quotient of the following* $\mathbb{B}$*-automaton:*



2. *Let* $\mathcal{D}_1$ *be the* $\mathbb{B}$*-automaton below. Compute the (minimal) quotient of* $\mathcal{D}_1$*, the co-quotient of* $\mathcal{D}_1$*, the co-quotient of the quotient of* $\mathcal{D}_1$*, etc.*



3. *Calculate all the quotients and all the co-quotients of the* $\mathbb{N}$*-automaton:*



4. ***Coloured Transition Lemma.*** *Establish the following statement:*

Let $\mathcal{A}$ *be a (Boolean) automaton on a monoid* M *the transitions of which are coloured in red or in blue. Then, the set of labels of computations of* $\mathcal{A}$ *that contain at least one red transition is a rational set (of* M*).*

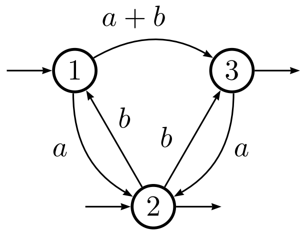
We construct a *covering* $\mathcal{B}'$ of $\mathcal{A}$: $\mathcal{B}' = \langle\, M, Q\times\{0,1\}, F, I\times\{0\}, T\times\{0,1\}\,\rangle$, in the following manner (the Out-morphism from $\mathcal{B}'$ to $\mathcal{A}$ is the projection on the first component):

$$F = \big\{\big((p,0),m,(q,0)\big) \bigm| (p,m,q)\in E \quad\text{and}\quad (p,m,q) \text{ is blue}\big\}$$
$$\cup \big\{\big((p,0),m,(q,1)\big) \bigm| (p,m,q)\in E \quad\text{and}\quad (p,m,q) \text{ is red}\big\}$$
$$\cup \big\{\big((p,1),m,(q,1)\big) \bigm| (p,m,q)\in E\big\} \quad .$$

A successful computation of $\mathcal{B}'$ which ends in a state $(t,0)$ contains only blue transitions, by construction. Hence the behaviour of $\mathcal{B} = \langle\, Q\times\{0,1\}, M, F, I\times\{0\}, T\times 1\,\rangle$ is the rational set we seek.

5. *Show that any* $\mathbb{Z}$*-rational series is the difference of two* $\mathbb{N}$*-rational series.*

6. *Construct the Schützenberger covering $\mathcal{S}$ of the following $\mathbb{B}$-automaton $\mathcal{A}$.*



How many S-immersions are there in this covering (that is, how many sub-automata $\mathcal{T}$ of $\mathcal{S}$ that are unambiguous and equivalent to $\mathcal{A}$)?

La Figure 1 montre $\mathcal{A}$, $\widehat{\mathcal{A}}$ et le revêtement de Schützenberger $\mathcal{S}$.

Les transitions de $\mathcal{S}$ qui arrivent dans un même état et se projettent sur une même transition de $\widehat{\mathcal{A}}$ sont marquées avec des lignes doubles. On notera qu'on a fait de même pour les flèches finales des états de $\mathcal{S}$ notés u et v (qu'on peut voir comme deux transitions qui arrivent sur l'état final subliminal de $\mathcal{S}$ et qui se projettent sur la même transition finale de $\widehat{\mathcal{A}}$.

Pour avoir une $\mathcal{S}$-immersion, il faut supprimer un élément de chacun de ces couples, ce qui donne $2^3 = 8$ possibilités distinctes.

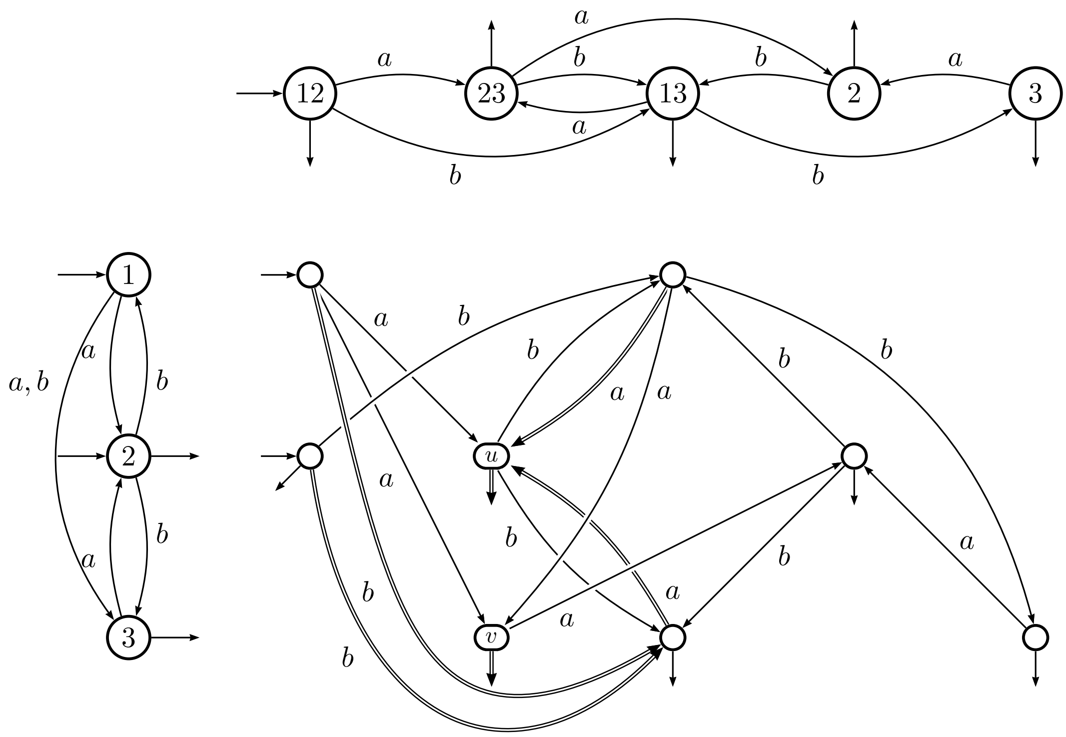


Figure 1: L'automate $\mathcal{A}$, son déterminisé, et son revêtement de Schützenberger

7. *Compute the Schützenberger covering of the $\mathbb{B}$-automaton $\mathcal{B}_1$ of the Figure 2.*

Le revêtement de Schützenberger de l'automate $\mathcal{B}_1$ est dessiné à la Figure 3. Les transitions concurrentes sont marquées par des lignes doubles.

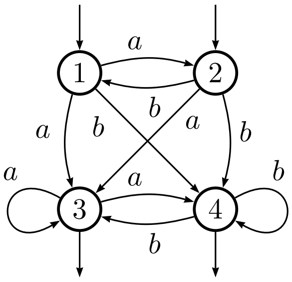


Figure 2: The automaton $\mathcal{B}_1$

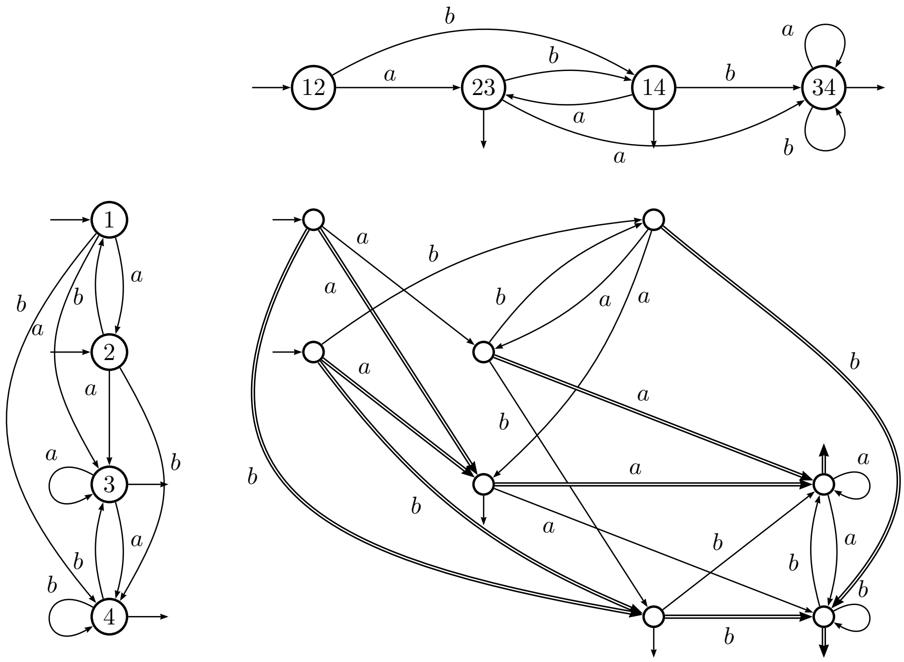


Figure 3: The Schützenberger covering of $\mathcal{B}_1$

8. **Quotients and product of automata.** *Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be three $\mathbb{K}$-automata on A^*. Show that if $\mathcal{B}$ is a quotient of $\mathcal{A}$, then $\mathcal{B}\otimes\mathcal{C}$ is a quotient of $\mathcal{A}\otimes\mathcal{C}$.*

9. **Quotients and co-quotients of the $\mathcal{C}_n$.**

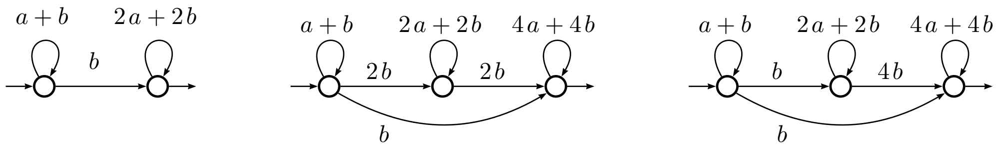
The $\mathbb{N}$-automaton $\mathcal{C}_1$ over $\{a,b\}^*$ shown at Figure 4(a) associates with every word w the integer $\overline{w}$ the binary representation of which is w when a is replaced by the digit 0 and b by 1.

Let $\mathcal{C}_2$ be the tensorial square of $\mathcal{C}_1$: $\mathcal{C}_2 = \mathcal{C}_1\otimes\mathcal{C}_1$; $\mathcal{V}_2$, shown at Figure 4(b), is the minimal quotient of $\mathcal{C}_2$ and $\mathcal{V}'_2$, shown at Figure 4(c), is the minimal co-quotient of $\mathcal{C}_2$.

(a) *Compute the minimal quotient $\mathcal{V}_3$ and the minimal co-quotient $\mathcal{V}'_3$ of $\mathcal{C}_3 = \mathcal{C}_2\otimes\mathcal{C}_1$.*

(b) *Compute the minimal co-quotient $\mathcal{V}'_4$ of $\mathcal{C}_4 = \mathcal{C}_3\otimes\mathcal{C}_1$. Compare with $\mathcal{V}'_3$.*

(c) *Generalising the above computation, compute the minimal co-quotient $\mathcal{V}'_{n+1}$ of $\mathcal{C}_{n+1} = \mathcal{C}_n\otimes\mathcal{C}_1$, for every n.*



(a) $\mathcal{C}_1$ (b) $\mathcal{V}_2$ (c) $\mathcal{V}_2'$

Figure 4: Three $\mathbb{N}$-automata

10. **Conjugacy of an automaton and its determinisation.**

(a) *Let* $\mathcal{A}_1$ *be the (Boolean) automaton of Figure 5 and* $\widehat{\mathcal{A}_1}$ *its determinisation. Verify that* $\widehat{\mathcal{A}_1} \stackrel{X_1}{\Longrightarrow} \mathcal{A}_1$ *holds, with*

$$X_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} .$$

(b) *Generalisation. Let* $\mathcal{A}$ *be a (Boolean) automaton and* $\widehat{\mathcal{A}}$ *its determinisation. Show that there exists an Boolean matrix* X *such that* $\widehat{\mathcal{A}} \stackrel{X}{\Longrightarrow} \mathcal{A}$ *.*

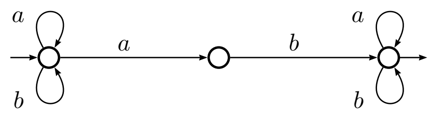


Figure 5: L'automate $\mathcal{A}_1$

Solution: (a) Le déterminisé $\widehat{\mathcal{A}_1}$ est représenté à la Figure 6. Les automates $\mathcal{A}_1$ et $\widehat{\mathcal{A}_1}$ s'écrivent:

$$\mathcal{A}_1 = \left\langle \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} a+b & a & 0 \\ 0 & 0 & b \\ 0 & 0 & a+b \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle \qquad \widehat{\mathcal{A}_1} = \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} b & a & 0 & 0 \\ 0 & a & b & 0 \\ 0 & 0 & b & a \\ 0 & 0 & b & a \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle .$$

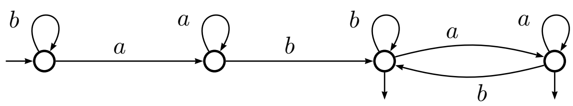


Figure 6: L'automate $\widehat{\mathcal{A}_1}$

On vérifie:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \qquad \text{et}$$

$$\begin{pmatrix} b & a & 0 & 0 \\ 0 & a & b & 0 \\ 0 & 0 & b & a \\ 0 & 0 & b & a \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & a & 0 \\ a+b & a & b \\ a+b & a & a+b \\ a+b & a & a+b \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a+b & a & 0 \\ 0 & 0 & b \\ 0 & 0 & a+b \end{pmatrix} ,$$

qui est bien l'identité voulue.

(b) Soient $\mathcal{A} = \langle I, \mu, T \rangle$ un automate booléen de dimension Q et $\widehat{\mathcal{A}} = \left\langle \widehat{I}, \widehat{\mu}, \widehat{T} \right\rangle$ son déterminisé, de dimension R, avec

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

[À l'imitation de la matrice X_1 de la question précédente,] soit X_R la $R{\times}Q$-matrice (booléenne) dont la J-ième ligne est J. Par définition du déterminisé, on a:

$$\widehat{I}_J = \begin{cases} 1 & \text{si} \quad J = I \\ 0 & \text{sinon} \end{cases} \quad , \qquad \widehat{\mu}(a)_{J,K} = \begin{cases} 1 & \text{si} \quad K = J \cdot \mu(a) \\ 0 & \text{sinon} \end{cases} \quad ,$$

$$\text{and} \qquad \widehat{T}_J = J \cdot T \quad .$$

Il s'ensuit alors que la J-ème ligne de $\widehat{\mu}(a) \cdot X_R$ est égale à K avec $K = J \cdot \mu(a)$ et que puisque la J-ième ligne de X_R est J, la J-ième ligne de $X_R \cdot \mu(a)$ est $J \cdot \mu(a) = K$. Les égalités évidentes $\widehat{I} \cdot X_R = I$ et $\widehat{T}_J = X_R \cdot T$ achèvent la preuve de ce que $\widehat{\mathcal{A}} \stackrel{X_R}{\Longrightarrow} \mathcal{A}$.

11. **Automata with bounded ambiguity and the Schützenberger covering.** *In the sequel, $\mathcal{A}$ is a Boolean automaton, $\widehat{\mathcal{A}}$ its determinisation, and $\mathcal{S}$ its Schützenberger covering.*

Definition 3. We call *concurrent transition set* of $\mathcal{S}$ a set of transitions which

(i) have the same destination (final extremity),

(ii) are mapped onto the same transition of $\widehat{\mathcal{A}}$.

Two transitions of $\mathcal{S}$ are called *concurrent* if they belong to the same concurrent transition set.

We also set the folllowing definition:

Definition 4. An automaton $\mathcal{A}$ over A^* is of *bounded ambiguity* if there exists an integer k such that every word w in $|\mathcal{A}|$ is the label of at most k distinct computations. The smallest such k is the *ambiguity degree* of $\mathcal{A}$.

(a) *What can be said of an automaton whose Schützenberger covering contains no concurrent transitions?*

(b) *Show that there exists a computation in $\mathcal{S}$ which contains two transitions of the same concurrent transition set if and only if there exists a concurrrent transition which belongs to a circuit.*

(c) *Let $p \xrightarrow{a} s$ and $q \xrightarrow{a} s$ be two concurrent transitions of $\mathcal{S}$ and*

$$c \;:=\; \xrightarrow[\mathcal{S}]{} i \xrightarrow[\mathcal{S}]{x} p \xrightarrow[\mathcal{S}]{a} s \xrightarrow[\mathcal{S}]{y} q \xrightarrow[\mathcal{S}]{a} s \xrightarrow[\mathcal{S}]{z} t \xrightarrow[\mathcal{S}]{}$$

a computation of $\mathcal{S}$ where i is an initial state and t a final state. Show that $w = x\,a\,y\,a\,z$ is the label of at least two computations of $\mathcal{A}$.

(d) *Prove that an automaton $\mathcal{A}$ is of bounded ambiguity if and only if no concurrent transition of its Schützenberger covering belongs to a circuit.*

(e) *Check that $\mathcal{B}_1$ of Figure 2 is of bounded ambiguity.*

(f) *Give a bound on the ambiguity degree of an automaton as a function of the cardinals of the concurrent transition sets of its Schützenberger covering.*
Compute that bound in the case of $\mathcal{B}_1$.

(g) *Infer from the above the complexity of an algorithm which decide if an automaton is of bounded ambiguity.*

(a) Si $\mathcal{S}$ ne contient pas de transitions concurrentes, la projection de $\mathcal{S}$ sur $\widehat{\mathcal{A}}$, qui est localement co-surjective par construction, est localement co-bijective. Elle fait de $\mathcal{S}$ un co-revêtement de $\widehat{\mathcal{A}}$, et il y a donc bijection entre les calculs de $\mathcal{S}$ et ceux de $\widehat{\mathcal{A}}$. Comme il y a, par construction, bijection entre les calculs de $\mathcal{S}$ et ceux de $\mathcal{A}$, chaque mot accepté par $\mathcal{A}$ est accepté par un seul calcul dans $\widehat{\mathcal{A}}$ donc dans $\mathcal{A}$: $\mathcal{A}$ est non ambigu.

(b) Soient $p \xrightarrow{a} s$ et $q \xrightarrow{a} s$ deux transitions concurrentes de $\mathcal{S}$. Si $i \xrightarrow{x} p \xrightarrow{a} s \xrightarrow{y} q \xrightarrow{a} s \xrightarrow{z} t$ est un calcul de $\mathcal{S}$ qui les contient toutes les deux, $s \xrightarrow{y} q \xrightarrow{a} s$ est un circuit qui contient l'une d'entre elles. Si réciproquement $s \xrightarrow{y} q \xrightarrow{a} s$ est un circuit qui contient l'une d'entre elles, alors $i \xrightarrow{x} p \xrightarrow{a} s \xrightarrow{y} q \xrightarrow{a} s \xrightarrow{z} t$ est un calcul de $\mathcal{S}$ qui les contient toutes les deux.

(c) Notons plus précisément les états de $\mathcal{S}$ sous la forme (I,i), (P,p), (P,q), (S,s), (T,t), et le calcul

$$c \;:=\; \xrightarrow[\mathcal{S}]{} (I,i) \xrightarrow[\mathcal{S}]{x} (P,p) \xrightarrow[\mathcal{S}]{a} (S,s) \xrightarrow[\mathcal{S}]{y} (P,q) \xrightarrow[\mathcal{S}]{a} (S,s) \xrightarrow[\mathcal{S}]{z} (T,t) \xrightarrow[\mathcal{S}]{} \;.$$

Ce calcul se projette dans $\widehat{\mathcal{A}}$ sur un calcul $e \;:=\; \xrightarrow[\widehat{\mathcal{A}}]{} I \xrightarrow[\widehat{\mathcal{A}}]{x\,a\,y} P \xrightarrow[\widehat{\mathcal{A}}]{a} S \xrightarrow[\widehat{\mathcal{A}}]{z} T \xrightarrow[\widehat{\mathcal{A}}]{}$.
Inversement, le calcul e de $\widehat{\mathcal{A}}$ se relève dans $\mathcal{S}$ en c, mais il peut également se relever en un calcul dont la dernière transition est $(P,p) \xrightarrow[\mathcal{S}]{a} (S,s)$: par induction sur la longueur de $x\,a\,y$, puisque $\pi_{\widehat{\mathcal{A}}} \colon \mathcal{S} \to \widehat{\mathcal{A}}$ est localement co-surjectif, et en procédant *de la droite vers la gauche*, on construit un calcul

$$c \;:=\; \xrightarrow[\mathcal{S}]{} (I,j) \xrightarrow[\mathcal{S}]{x\,a\,y} (P,p) \xrightarrow[\mathcal{S}]{a} (S,s) \xrightarrow[\mathcal{S}]{z} (T,t) \xrightarrow[\mathcal{S}]{}$$

dont le premier état est initial.
Par projection sur $\mathcal{A}$, on a alors deux calculs réussis

$$c' \;:=\; \xrightarrow[\mathcal{A}]{} i \xrightarrow[\mathcal{A}]{x\,a\,y} q \xrightarrow[\mathcal{A}]{a} s \xrightarrow[\mathcal{A}]{z} t \xrightarrow[\mathcal{A}]{} \quad \text{et} \quad c'' \;:=\; \xrightarrow[\mathcal{A}]{} j \xrightarrow[\mathcal{A}]{x\,a\,y} p \xrightarrow[\mathcal{A}]{a} s \xrightarrow[\mathcal{A}]{z} t \xrightarrow[\mathcal{A}]{}$$

qui acceptent w et qui sont distincts puisque p et q le sont.

(d) Montrons d'abord que la condition est nécessaire, c'est-à-dire, que si une transition concurrente de $\mathcal{S}$ appartient à un circuit, $\mathcal{A}$ n'est pas d'ambiguité bornée.
Pour cela on reprend les notations de la question précédente, et on va montrer que le mot $x\,a\,(y\,a)^n\,z$ est reconnu par (au moins) $n+1$ calculs dans $\mathcal{A}$. Avec le même raisonnement que précédemment, on observe que $x\,a\,(y\,a)^n\,z$ est accepté par le calcul

$$e \;:=\; \xrightarrow[\widehat{\mathcal{A}}]{} I \xrightarrow[\widehat{\mathcal{A}}]{x\,a} S \left(\xrightarrow[\widehat{\mathcal{A}}]{y} P \xrightarrow[\widehat{\mathcal{A}}]{a} S \right)^n \xrightarrow[\widehat{\mathcal{A}}]{z} T \xrightarrow[\widehat{\mathcal{A}}]{}$$

qui se relève dans $\mathcal{S}$ en $n+1$ calculs distincts (pour $j = 0$ à n):

$$\xrightarrow[\mathcal{S}]{} (I,j) \xrightarrow[\mathcal{S}]{x\,(a\,y)^{n-j}} (P,p) \xrightarrow[\mathcal{S}]{a} (S,s) \left(\xrightarrow[\mathcal{S}]{y} (P,q) \xrightarrow[\mathcal{S}]{a} (S,s) \right)^j \xrightarrow[\mathcal{S}]{z} (T,t) \xrightarrow[\mathcal{S}]{}$$

qui eux-mêmes se projettent en $n+1$ calcul distincts de $\mathcal{A}$ qui ont tous $x\,a\,(y\,a)^n\,z$ comme étiquette.

Inversement, si aucune transition concurrente de $\mathcal{S}$ n'appartient à un circuit, un calcul réussi de $\mathcal{S}$ ne contient jamais deux transitions d'un même ensemble de concurrence (question (c)). C'est donc un calcul d'au moins un des sous-automates de $\mathcal{S}$ dans lequel on n'a gardé qu'une seule transition par ensemble de concurrence. Chacun de ces automates est non ambigu par construction (co-revêtement d'un automate non ambigu), il n'y en a qu'un nombre fini, et leur réunion donne tous les calculs de $\mathcal{S}$ donc de $\mathcal{A}$.

(e) On observe aisément qu'aucune des transitions concurrentes du revêtement de la Figure 3 n'appartient à un circuit.

(f) S'il y a k ensembles de concurrence, et que chaque ensemble de concurrence contient c_j transitions, la construction décrite à la question (e) donne $\prod_{j=1} j = kc_j$ automates non ambigus dont la réunion recompose l'ensemble des calculs de $\mathcal{A}$.

Dans le cas de $\mathcal{B}_1$, il y a 5 ensembles de concurrence (NPO l'ensemble des deux transitions finales des états qui se projettent en 34), chaque ensemble a deux éléments, d'où une borne de 32.

(N.B. Le vrai degré d'ambiguïté de $\mathcal{B}_1$ est 6, ce que l'on peut découvrir par d'autres méthodes plus sophistiquées (cf. par exemple J.S. et R. de Souza, Theory of Computing Systems 47, (2010), 758–785, accessible depuis ma page web) — mais ceci est une autre histoire.)

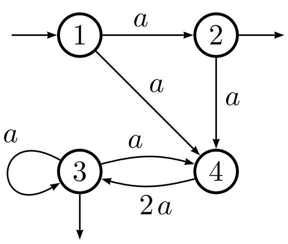
(g) Si $\mathcal{A}$ a n états et m transitions, $\mathcal{S}$ a (au plus) $n\,2^n$ états et $k = m\,2^n$ transitions. La détermination des transitions concurrentes se fait au cours de la construction de $\mathcal{S}$ et celle des circuits par un parcours en profondeur de $\mathcal{S}$, linéaire en k. Au total, une procédure dont la complexité (dans le cas le pire) est en $\mathrm{O}(m\,2^n)$.

(N.B. Cette méthode n'est pas la méthode optimale pour décider si un automate $\mathcal{A}$ est d'ambiguïté bornée. Cette propriété peut être observée sur le cube de $\mathcal{A}$, avec un algorithme de complexité $\mathrm{O}(m^3)$, ce qui est évidemment bien meilleur. Dans le cas de notre automate $\mathcal{B}_1$, c'est encore plus simple puisque son carré ne contient aucun circuit: il n'est pas difficile de se convaincre que c'est une condition suffisante mais pas nécessaire).

Lecture III — Exercises with solution

Unless stated otherwise, the alphabet A is $A = \{a, b\}$.

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



Solution: La représentation correspondant à cet automate est

$$I_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}, \quad \mu_1(a) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad T_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

On calcule:

$$\begin{aligned} I_1 \cdot \mu_1(1_{A^*}) &= \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}, \\ I_1 \cdot \mu_1(a) &= \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \\ \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix} \cdot \mu_1(a) &= \begin{pmatrix} 0 & 0 & 1 & 2 \end{pmatrix}, \\ \begin{pmatrix} 0 & 0 & 1 & 2 \end{pmatrix} \cdot \mu_1(a) &= \begin{pmatrix} 0 & 0 & 2 & 4 \end{pmatrix} = 2 \begin{pmatrix} 0 & 0 & 1 & 2 \end{pmatrix} \end{aligned}$$

Equations qui correspondent à la représentation ci-dessous:

$$I_2 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \quad \mu_2(a) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}.$$

La transposée de la représentation précédente est:

$$I_3 = \begin{pmatrix} 0 & 1 & 2 \end{pmatrix}, \quad \mu_3(a) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad T_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

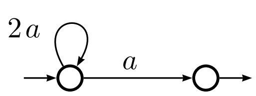
On calcule:

$$\begin{aligned} I_3 \cdot \mu_3(1_{A^*}) &= \begin{pmatrix} 0 & 1 & 2 \end{pmatrix}, \\ I_3 \cdot \mu_3(a) &= \begin{pmatrix} 1 & 2 & 4 \end{pmatrix}, \\ \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \cdot \mu_3(a) &= \begin{pmatrix} 2 & 4 & 8 \end{pmatrix} = 2 \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} \end{aligned}$$

Equations qui correspondent à la représentation ci-dessous,

$$I_4 = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \mu_4(a) = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}, \quad T_4 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

et dont la transposée correspond à l'automate ci-dessous.



2. *Let $\mathcal{A}_1$ be the $\mathbb{Q}$-automaton on $\{a\}^*$ shown at Figure 1 (the unique letter a of the alphabet is not shown on the transitions of the figure). Compute a reduced automaton, equivalent to $\mathcal{A}_1$.*

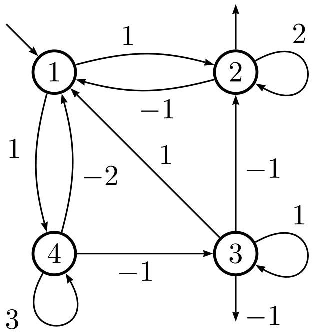


Figure 1: The $\mathbb{Q}$-automaton $\mathcal{A}_1$

Solution: La représentation correspondant à $\mathcal{A}_1$ est

$$I_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}, \quad \mu_1(a) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ -1 & 2 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ -2 & 0 & -1 & 3 \end{pmatrix}, \quad T_1 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} .$$

On calcule:[2]

$$\begin{aligned} I_1 \cdot \mu_1(1_{A^*}) &= \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}, \\ I_1 \cdot \mu_1(a) &= \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \\ \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix} \cdot \mu_1(a) &= \begin{pmatrix} -3 & 2 & -1 & 3 \end{pmatrix} = -3 \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} + 2 \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 1 & -1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 1 & -1 \end{pmatrix} \cdot \mu_1(a) &= \begin{pmatrix} 3 & -1 & 2 & -3 \end{pmatrix} = 3 \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix} + 2 \begin{pmatrix} 0 & 0 & 1 & -1 \end{pmatrix} \end{aligned}$$

Equations qui correspondent à la représentation ci-dessous, et donc à l'automate de la Figure 2 (a)

$$I_2 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \quad \mu_2(a) = \begin{pmatrix} 0 & 1 & 0 \\ -3 & 2 & -1 \\ 3 & -1 & 2 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} .$$

La transposée de la représentation précédente est:

$$I_3 = \begin{pmatrix} 0 & 1 & -1 \end{pmatrix}, \quad \mu_3(a) = \begin{pmatrix} 0 & -3 & 3 \\ 1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}, \quad T_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} .$$

On calcule:

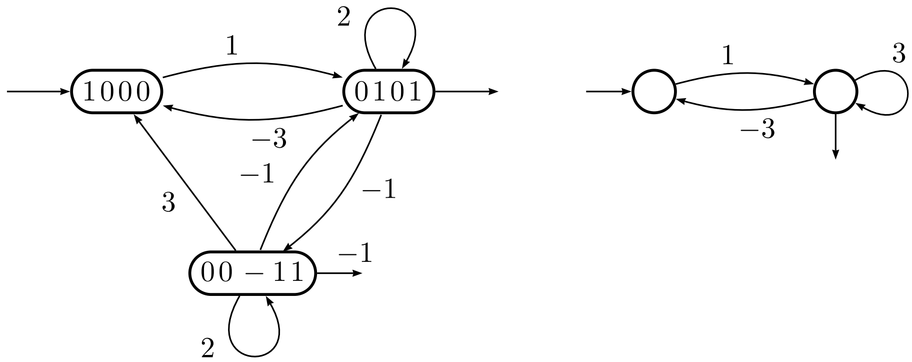
$$\begin{aligned} I_3 \cdot \mu_3(1_{A^*}) &= \begin{pmatrix} 0 & 1 & -1 \end{pmatrix}, \\ I_3 \cdot \mu_3(a) &= \begin{pmatrix} 1 & 3 & -3 \end{pmatrix} = 3 \begin{pmatrix} 0 & 1 & -1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \cdot \mu_3(a) &= \begin{pmatrix} 0 & -3 & 3 \end{pmatrix} = -3 \begin{pmatrix} 0 & 1 & -1 \end{pmatrix} \end{aligned}$$

[2] On choisit de mettre les pivots à 1 pour suivre les calculs de Awali (*cf.* `vaucanson-project.org/Awali`).

Equations qui correspondent à la représentation ci-dessous,

$$I_4 = \begin{pmatrix}1 & 0\end{pmatrix}, \quad \mu_4(a) = \begin{pmatrix}3 & 1\\ -3 & 0\end{pmatrix}, \quad T_4 = \begin{pmatrix}0\\ 1\end{pmatrix} ,$$

et dont la transposée correspond à l'automate de la Figure 2 (b).



(a) Semi-réduction gauche-droite (b) Semi-réduction droite-gauche

Figure 2: Réduction de $\mathcal{A}_1$

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.

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* $L_{\mathsf{nd}}(n,m)$ *.*

Lecture IV — Exercises with solution

Unless stated otherwise, the alphabet A is $A = \{a, b\}$.

1. **Orders.** The alphabet A is *totally ordered* and this order is denoted by $\leqslant$.

The *lexicographic order*, denoted by $\preccurlyeq$, extends the order on A to an order on A^* and is defined as follows. Let v and w be two words in A^* and u their *longest common prefix*. Then, $v \preccurlyeq w$ if $v = u$ or, if $v = u\,a\,s$, $w = u\,b\,t$ with a and b in A, then $a < b$.

(a) Give a finite transducer over $A^* \times A^*$ which realises $\preccurlyeq$, that is, which asssociates with every word u of A^* the set of words which are equal to or greater than u.

The *radix order* (also called the *genealogical order* or the *short-lex order*), denoted by $\sqsubseteq$, is defined as follows: $v \sqsubseteq w$ if $|v| < |w|$ or $|v| = |w|$ and $v \preccurlyeq w$.

(b) Give a finite transducer over $A^* \times A^*$ which realises $\sqsubseteq$,

For every language L of A^*, we denote by $\mathsf{minlg}\,(L)$ *(resp.* $\mathsf{Maxlg}\,(L)$*) the set of words of L which have no smaller (resp. no greater) words in L of* the same length *in the lexicographic order.*

(c) *Show that if L is a rational language, so are* $\mathsf{minlg}\,(L)$ *and* $\mathsf{Maxlg}\,(L)$.

2. **Number representation.**

Let $A_2 = \{0, 1\}$ and $A_3 = \{0, 1, 2\}$ be two alphabets of digits.

The alphabet A_3 can be first considered as a non-canonical alphabet for the representation of integers in base 2: $\overline{1\,2} = 4$, $\overline{2\,0\,1} = 9$, *etc.*

Let $\nu_2 \colon A_3^* \to A_2^*$ be the *normalisation* in base 2, that is, the relation which associates with a word of A_3^* the word of A_2^* which represents the same integer in base 2.

(a) *Give a transducer which realises ν_2. Comment.*

Let $\varphi \colon A_2^* \to A_3^*$ be the function which maps the binary representation of every integer onto its representation in base 3, *e.g.* $\varphi(1\,0\,0\,0) = 2\,2$.

(b) *Show that φ is not a rational relation.*

3. **Operation on numbers.**

(a) *Give a transducer which realises the multiplication by 9 on the integers written in binary representation, that is, the relation $\tau \colon A_2^* \to A_2^*$ such that $\overline{\tau(w)} = 9 \cdot \overline{w}$.*

(b) *Let $\mu \colon A_2^* \times A_2^* \to A_2^*$ be the relation which realises the multiplication, that is, such that $\mu(u, v) = w$ where $\overline{w} = \overline{u} \cdot \overline{v}$.*

Show that μ is not a rational relation.

4. **Map equivalence of a morphism.**

Let $\varphi_1 \colon \{a,b,c\}^* \to \{x,y\}^*$ *be the morphism defined by:*

$$\varphi_1(a) = x\,, \quad \varphi_1(b) = y\,x\,, \quad \varphi_1(c) = x\,y\,.$$

(a) Give a subnormalised transducer which realises φ_1.

(b) Give a subnormalised transducer which realises ${\varphi_1}^{-1}$.

(c) Compute a subnormalised transducer which realises ${\varphi_1}^{-1} \circ \varphi_1$.

5. **Iteration Lemma.** *Let* $\theta \colon A^* \to B^*$ *be a rational relation.*

(a) Show that there exists an integer N *such that for every pair* (u,v) *in* $\widehat{\theta}$ *whose length*[3] *is greater than* N*, there exists a factorisation:*

$$(u,v) = (s,t)\,(x,y)\,(w,z)$$

such that: (i) $1 \leqslant |x| + |y| \leqslant N$ *and* (ii) $(u,v) = (s,t)\,(x,y)^*(w,z) \subseteq \widehat{\theta}\,.$

(b) Show that the mirror *function* $\rho \colon A^* \to A^*$ *:*

$$\rho(a_1\,a_2 \cdots a_n) = a_n\,a_{n-1} \cdots a_1 \;\;,$$

is not a rational relation.

6. **Conjugacy.** *Let* $\mathsf{Conj} \colon A^* \to A^*$ *be the relation which associates with every word* w *the set of its* conjugates*:* $\mathsf{Conj}(w) = \{v\,u \mid u,v \in A^* \quad u\,v = w\}$.

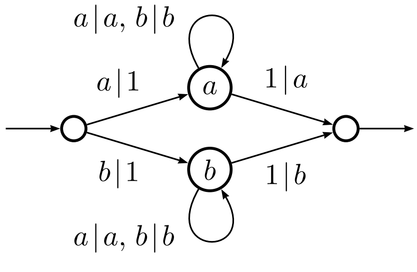
(a) Show that if L *is a rational language, then so is* $\mathsf{Conj}(L)$.

(b) Give a transducer which associates with every word w *of* $\{a,b\}^*$ *the word obtained by moving the first letter of* w *to its end.*

(c) Compose this transducer with itself.

(d) Show that Conj *is not a rational relation.*

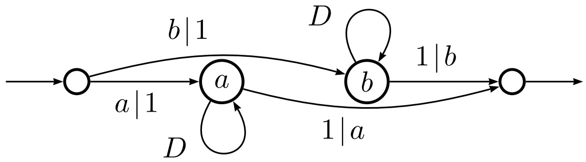
(b) Dans le transducteur suivant, la première lettre ne donne lieu à aucune sortie mais est mémorisée dans l'état d'arrivée. On a ensuite une recopie de la suite du mot. On quitte l'état en sortant la lettre mémorisée.

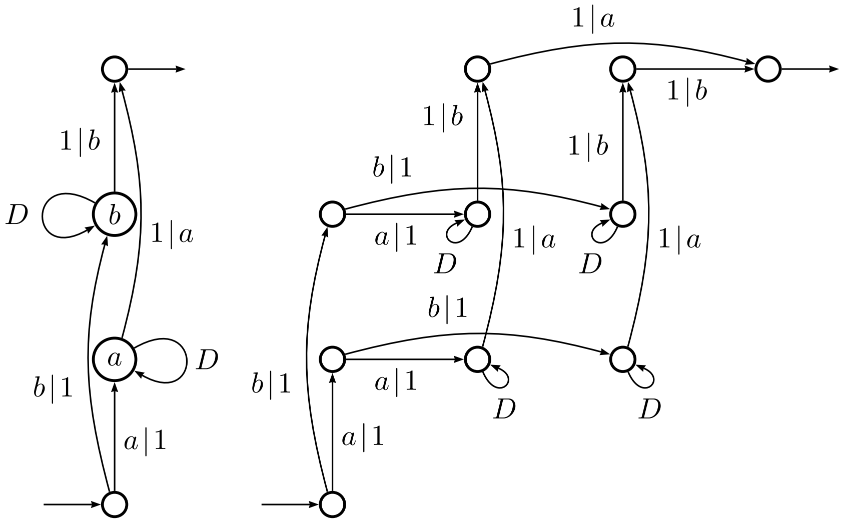


[3] The length of a pair is the sum of the lengths of its components.

(c) Si on applique la construction de la composition de ce transducteur avec lui-même, on obtient le transducteur suivant. (On a posé $D = a|a,\, b|b$.)

On observe que le transducteur composé consiste bien à mémoriser les deux premières lettres du mot lu, à recopier la suite, et à sortir enfin les lettres mémorisées.





Lecture V — Exercises with solution

1. *Apply the construction of the proof of Theorem 3 in order to build real-time transducers from the two transducers below which realise the universal relation on $\{a\}^* \times \{b\}^*$.*

(a) $\mathcal{U}_1$ (b) $\mathcal{U}_2$

2. *Give a realisation by representation of the following relations:*

(a) *the complement of the identity;* (b) *the lexicographic order;* (c) *the radix order.*

3. ***Finite and infinite components of a rational relation.*** *Let $\tau\colon A^* \to B^*$ be a relation. The* finite *and* infinite components *τ_{f} and τ_∞ of τ are defined by:*

$$\tau_{\mathsf{f}}(w) = \begin{cases} \tau(w) & \text{if } \|\tau(w)\| \text{ is finite} \\ \emptyset & \text{otherwise} \end{cases} \qquad \text{et} \qquad \tau_\infty(w) = \begin{cases} \emptyset & \text{if } \|\tau(w)\| \text{ is finite} \\ \tau(w) & \text{otherwise} \end{cases}$$

Show that if τ is rational, then τ_{f} and τ_∞ are rational and effectively computable from τ.

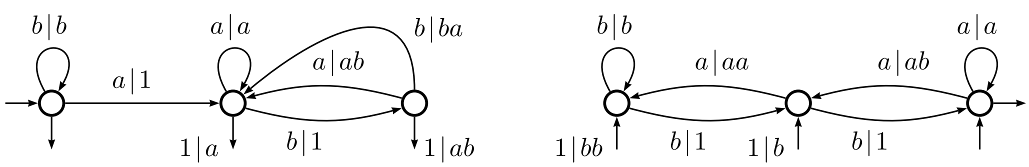
Let $\mathcal{T}$ be a real-time transducer which realises τ; it is an automaton over $M = A^* \times B^*$. The transitions the label of which have a second component which is an infinite subset of B^* are said to be 'red'.

A word of A^* is in the domain of τ_∞ if and only if it is the first component of a label of at least one successful computation of $\mathcal{T}$ which contains at least one red transition. (Remark: such a word may also be the first component of the label of a successful computation of $\mathcal{T}$ which contains no red transitions.)

Let $\alpha\colon A^* \to B^*$ be the relation realised by the computations of $\mathcal{T}$ which contain at least one red transition. By the Coloured Transition Lemma proved in Exercise II.4., α is a rational relation that iseffectively computable from $\mathcal{T}$.

It follows that $\widehat{\tau_\infty} = \widehat{\tau} \bigcap (\mathsf{Dom}\, \alpha \times B^*)$ and that $\widehat{\tau_{\mathsf{f}}} = \widehat{\tau} \bigcap [(\mathsf{Dom}\, \tau \setminus \mathsf{Dom}\, \tau_\infty) \times B^*]$, and both are rational subsets of $A^* \times B^*$.

4. ***Fibonacci reduction.*** *Give a transducer which realises the composition of the relations realised by the transducers below (the transducer on the left by the transducer on the right).*



5. ***Choosing the uniformisation.*** *Let $A = \{a, b, c\}$ be a totally ordered alphabet, where $a < b < c$, and let θ be the rational relation from A^* into itself whose graph is:*

$$\widehat{\theta} = (a, a)^* \, (b, 1)^* \, (1, b) \cup (a, 1)^* \, (b, a)^* \, (1, c) \quad .$$

Show that neither the radix uniformisation θ_{rad} nor the lexicographic selection θ_{lex} are rational functions.

Le domaine de θ est $a^* \, b^*$ et on a $\theta(a^n \, b^m) = \{a^n \, b, a^m \, c\}$, d'où l'on déduit

$$\theta_{\mathsf{rad}}(a^n \, b^m) = \begin{cases} a^n \, b & \text{si } n \leqslant m \,, \\ a^n \, c & \text{sinon,} \end{cases} \qquad \text{et} \qquad \theta_{\mathsf{lex}}(a^n \, b^m) = \begin{cases} a^n \, b & \text{si } n \geqslant m \,, \\ a^n \, c & \text{sinon.} \end{cases}$$

Il s'en ensuit que ni $(\theta_{\mathsf{rad}})^{-1}(a^* b)$ ni $(\theta_{\mathsf{lex}})^{-1}(a^* b)$ ne sont rationnels, ce qui établit la propriété.

6. ***Inherently ambiguous rational relation.*** *Let $\mathcal{V}_1$ and $\mathcal{W}_1$ be the transducers of Example IV.2:*

$$|\mathcal{V}_1| = \{(a^n b^m, c^n) \mid n, m \in \mathbb{N}\} \qquad \text{and} \qquad |\mathcal{W}_1| = \{(a^n b^m, c^m) \mid n, m \in \mathbb{N}\} \quad .$$

Show that the rational relation $|\mathcal{V}_1| \cup |\mathcal{W}_1|$ is inherently ambiguous.