Weighted Automata

— Version of February 7, 2011 —

Benedikt Bollig and Marc Zeitoun

LSV, ENS Cachan, CNRS
E-mail address: {bollig,mz}@lsv.ens-cachan.fr

Abstract. These notes present results from two series of MPRI lectures on weighted automata. The content presented in 2010–11 is covered by Chapters 1 to 5. Chapters 6 and 7 were presented in 2009–10. Most of the exercises are either direct applications, or have already been developed during the lectures.

References listed in these notes go in general beyond the scope of the lectures. Many of them are specialized research papers highlighting particular details. Reading them is of course not mandatory. General useful references are some chapters of textbooks: [BR11; Sak09; KS85; SS78; DKV09; BK08].

[BK08] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking (Representation and Mind Series)*. The MIT Press, 2008. ISBN: 026202649X, 9780262026499.

[BR11] J. Berstel and Ch. Reutenauer. *Noncommutative rational series with applications*. Vol. 137. Encyclopedia of Mathematics and Its Applications. Preliminary version at http://tagh.de/tom/wp-content/uploads/berstelreutenauer2008.pdf. Cambridge University Press, 2011.

[DKV09] M. Droste, W. Kuich, and W. Vogler. *Handbook of Weighted Automata*. Springer, 2009.

[KS85] W. Kuich and A. Salomaa. *Semirings, Automata and Languages*. Springer, 1985.

[Sak09] J. Sakarovitch. *Elements of Automata Theory*. New York, NY, USA: Cambridge University Press, 2009. ISBN: 0521844258, 9780521844253.

[SS78] A. Salomaa and M. Soittola. *Automata-theoretic aspects of formal power series*. Springer, 1978.

Contents

CHAPTER 1

Motivation and Preliminaries

1. Three examples

Weighted graphs and automata offer a unifying framework for treating problems or modeling systems with the same structural properties. Consider the following problems, which all share a common structure:

1. computing the language of/a regular expression for a given NFA,
2. finding shortest paths between all pairs of vertices in a graph,
3. computing the transitive closure of the edge relation of a graph,

We first recall for each of these problems a standard solution. In Section 1.3, we will see that one can carry the computation in a unified framework in order to answer all of them.

1.1. Semantics of an NFA. Suppose we are given a finite automaton $\mathcal{A} = (Q, A, \Delta, q_0, F)$ with $Q = \{1, \dots, n\}$ for some $n \geqslant 1$, alphabet A, and transition relation $\Delta \subseteq Q \times A \times Q$. Usually, we define the semantics of $\mathcal{A}$ to be its *language*, denoted by $L(\mathcal{A}) \subseteq A^*$. When we ignore q_0 and F, we obtain a triple $\mathcal{B} = (Q, A, \Delta)$. As a semantics of $\mathcal{B}$, we could think of a mapping

$$\|\mathcal{B}\| : \begin{cases} Q \times Q \to 2^{A^*} \\ (i, j) \mapsto L(\mathcal{A}_{i,j}) \end{cases}$$

where $\mathcal{A}_{i,j} = (Q, A, \Delta, i, \{j\})$.
To compute $\|\mathcal{B}\|$, we let, for $i, j \in \{1, \dots, n\}$ and $k \in \{0, \dots, n\}$,

$$W_{i,j}^{(k)} \stackrel{\text{def}}{=} \{w \in A^* \mid w \text{ leads from } i \text{ to } j \text{ without using } k+1, \dots, n \text{ as intermediate states}\}.$$

We have

$$W_{i,j}^{(n)} = \|\mathcal{B}\|(i, j)$$
$$W_{i,j}^{(k)} = \begin{cases} \{a \in A \mid (i, a, j) \in \Delta\} \cup \{\varepsilon \mid i = j\} & \text{if } k = 0, \\ W_{i,j}^{(k-1)} \cup W_{i,k}^{(k-1)} \left(W_{k,k}^{(k-1)}\right)^* W_{k,j}^{(k-1)} & \text{if } k \geqslant 1. \end{cases}$$

This characterization, which is illustrated in Fig. 1.1, suggests an algorithm to infer a regular expression for a given NFA.

1.2. Finding shortest paths. Consider a (directed) graph $G = (V, E, c)$. Here, $V = \{1, \dots, n\}$ is a nonempty finite set of *vertices*, $E \subseteq V \times V$ is a set of *edges*, and $c : E \to \mathbb{N}$ is a *cost function*. If we are interested in shortest paths, a semantics of G could be given as

$$\|G\| : \begin{cases} V \times V \to \mathbb{N} \\ (i, j) \mapsto \text{ minimal cost of a path from } i \text{ to } j \end{cases}$$

For $i, j \in \{1, \dots, n\}$ and $k \in \{0, \dots, n\}$, let

$$c_{i,j}^{(k)} \stackrel{\text{def}}{=} \text{ minimal cost of a path from } i \text{ to } j \text{ without using } k+1, \dots, n$$

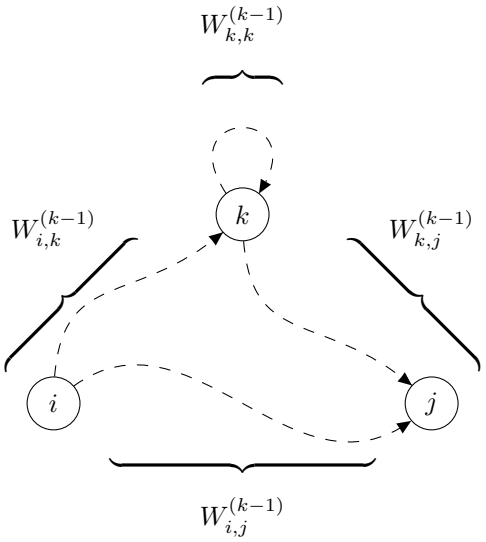


FIG. 1.1. Computation of the language $W_{i,j}^{(k)}$

We then have

$$c_{i,j}^{(n)} = \|G\|(i,j)$$

$$c_{i,j}^{(k)} = \begin{cases} 0 & \text{if } i = j \text{ and } k = 0 \\ c((i,j)) & \text{if } i \neq j \text{ and } (i,j) \in E \text{ and } k = 0 \\ \infty & \text{if } i \neq j \text{ and } (i,j) \notin E \text{ and } k = 0 \\ \min(c_{i,j}^{(k-1)}\,,\, c_{i,k}^{(k-1)} + c_{k,j}^{(k-1)}) & \text{if } k \geqslant 1 \end{cases}$$

This characterization suggests an algorithm to determine the minimal cost of a path between two vertices of a graph.

1.3. Computing transitive closure. Suppose we are interested in (V, E^*), *i.e.*, the reflexive and transitive closure of G. Then, a semantics of G could be given as

$$\|G\| : \begin{cases} V \times V \to \{\mathsf{true}, \mathsf{false}\} \\ (u,v) \mapsto \text{ “there is a path from } u \text{ to } v\text{”} \end{cases}$$

Let

$$e_{i,j}^{(k)} \stackrel{\text{def}}{=} \text{ “there is a path from } i \text{ to } j \text{ that does not use } k+1, \ldots, n\text{”}$$

We have

$$e_{i,j}^{(n)} = \|G\|(i,j)$$

$$e_{i,j}^{(k)} = \begin{cases} \mathsf{true} & \text{if } (i = j \text{ or } (i,j) \in E) \text{ and } k = 0 \\ \mathsf{false} & \text{if } i \neq j \text{ and } (i,j) \notin E \text{ and } k = 0 \\ e_{i,j}^{(k-1)} \vee (e_{i,k}^{(k-1)} \wedge e_{k,j}^{(k-1)}) & \text{if } k \geqslant 1 \end{cases}$$

This characterization suggests an algorithm to compute the reflexive transitive closure of a binary relation.

2. Semirings and Closed Weighted Systems

The semantics that we considered in the previous section rely on a specific interpretation of an edge (or an edge labeling), a path, and the subsumption of a set of paths. In general, these interpretations correspond to operations of a (closed) semiring.

DEFINITION 1.1. A *monoid* is a structure $\mathbb{S} = (S, \otimes, \mathbb{1})$ where

– S is a set,
– $\otimes : S \times S \to S$ is a binary operation that is *associative*, *i.e.*, for all $r, s, t \in S$:

$$r \otimes (s \otimes t) = (r \otimes s) \otimes t,$$

– $\mathbb{1} \otimes s = s \otimes \mathbb{1} = s$ for every $s \in S$.

We say that $\mathbb{S}$ is *commutative* if $\otimes$ is commutative, *i.e.*, $s \otimes t = t \otimes s$ for all $s, t \in S$. ■

Definition 1.2. A *semiring* is a structure $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ where

– $(S, +, \mathbb{0})$ is a commutative monoid,
– $(S, \cdot, \mathbb{1})$ is a monoid,
– $\cdot$ *distributes over* $+$, *i.e.*, for all $r, s, t \in S$,

$$(r + s) \cdot t = (r \cdot t) + (s \cdot t)$$
$$t \cdot (r + s) = (t \cdot r) + (t \cdot s)$$

– $\mathbb{0}$ is an *annihilator* wrt. $\cdot$, *i.e.*, $\mathbb{0} \cdot s = s \cdot \mathbb{0} = \mathbb{0}$ for every $s \in S$.

We call $\mathbb{S}$ *commutative* if $\cdot$ is commutative.
We call $\mathbb{S}$ *closed* if

– $+$ is *idempotent*, *i.e.*, $s + s = s$ for all $s \in S$,
– for every countable sequence $(s_i)_{i \in \mathbb{N}}$ of elements of S, the sum $\sum_{n \in \mathbb{N}} s_n$ is well-defined,
– associativity, commutativity, and idempotency apply to infinite sums, and
– for every two countable sequences $s_0, s_1, \ldots$ and $t_0, t_1, \ldots$ of elements of S, we have $\left(\sum_{n \in \mathbb{N}} s_n\right) \cdot \left(\sum_{n \in \mathbb{N}} t_n\right) = \sum_{i,j \in \mathbb{N}} (s_i \cdot t_j)$. ■

Example 1.3. Prominent semirings are:

– $\mathbb{L}\mathrm{ang}_A = (2^{A^*}, \cup, \cdot, \varnothing, \{\varepsilon\})$, the semiring of languages over alphabet A.
– $\mathbb{R}\mathrm{eg}_A = (\mathrm{Rat}(A), \cup, \cdot, \varnothing, \{\varepsilon\})$, the semiring of regular languages over A.
– $\mathbb{T}\mathrm{rop} = (\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$, called the tropical semiring.
– $\mathbb{B}\mathrm{ool} = (\{\mathsf{false}, \mathsf{true}\}, \vee, \wedge, \mathsf{false}, \mathsf{true})$, the boolean algebra.
– $\mathbb{N}\mathrm{at} = (\mathbb{N}, +, \cdot, 0, 1)$ the semiring of natural numbers.
– $\mathbb{P}\mathrm{rob} = (\mathbb{R}_{\geqslant 0}, +, \cdot, 0, 1)$, the probabilistic semiring.[1]
– Given a semiring $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ and a finite set Q, the the semiring of $(Q \times Q)$-*matrices* with coefficients in $\mathbb{S}$ is $(S^{Q \times Q}, \underline{+}, \underline{\cdot}, \underline{\mathbb{0}}, \underline{\mathbb{1}})$. For all $p, q \in Q$, $\underline{\mathbb{0}}_{p,q} = \mathbb{0}$, $\underline{\mathbb{1}}_{p,p} = \mathbb{1}$, and $\underline{\mathbb{1}}_{p,q} = \mathbb{0}$ if $p \neq q$. The operations $\underline{+}$ and $\underline{\cdot}$ are the usual matrix operations. That is, given $s, t \in S^{Q \times Q}$: $(s \mathbin{\underline{+}} t)_{p,q} = s_{p,q} + t_{p,q}$ and $(s \mathbin{\underline{\cdot}} t)_{p,q} = \sum_{r \in Q} s_{p,r} \cdot t_{r,q}$. To shorten the notation in the rest of these notes, we will write $+, \cdot, \mathbb{0}$ and $\mathbb{1}$ instead of $\underline{+}, \underline{\cdot}, \underline{\mathbb{0}}, \underline{\mathbb{1}}$.

For a closed semiring, we can define a closure operator:

Definition 1.4. Let $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ be a closed semiring and $s \in S$. The *closure* of s is the infinite sum

$$s^* \stackrel{\text{def}}{=} s^0 + s^1 + s^2 + \ldots$$

where $s^0 = \mathbb{1}$. ■

Revisiting our initial models, we realize that we actually deal with one and the same semantics. Every instance, however, is solved by a computation in a specific closed semiring:

Semantics of NFA	$\mathbb{L}\mathrm{ang}_A$
Shortest path	$\mathbb{T}\mathrm{rop}$
Transitive closure	$\mathbb{B}\mathrm{ool}$

Let us give a general formalization of our problem.

[1] Note that $([0, 1], \max, \cdot, 0, 1)$ is sometimes considered as the probabilistic semiring as its universe restricts to probabilities. It is, however, not suitable for our purposes, as it neglects addition and, thus, does not allow one to model non-determinism.

DEFINITION 1.5. Let $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ be a semiring. A *weighted system* over $\mathbb{S}$ is a pair $\mathcal{A} = (Q, \mu)$ where Q is a nonempty finite set of *states* and μ is the *weight function* $Q \times Q \to S$. We call $\mathcal{A}$ *closed* if $\mathbb{S}$ is closed. ■

Let $\mathcal{A} = (Q, \mu)$ be a **closed** weighted system over a (closed) semiring $\mathbb{S}$.

A *path* of $\mathcal{A}$ is a nonempty finite sequence $\rho = (q_0, \dots, q_m)$ of states. Hereby, m is the *length* of ρ. We extend μ to paths as follows:

$$\mu(\rho) \stackrel{\text{def}}{=} \begin{cases} \mathbb{1} & \text{if } m = 0 \\ \mu(q_0, q_1) \cdot \mu(q_1, q_2) \cdot \ldots \cdot \mu(q_{m-1}, q_m) & \text{if } m \geqslant 1 \end{cases}$$

Furthermore, we extend μ to sets P of paths:

$$\mu(P) \stackrel{\text{def}}{=} \begin{cases} \mathbb{0} & \text{if } P = \varnothing \\ \sum_{\rho \in P} \mu(\rho) & \text{if } P \neq \varnothing \end{cases}$$

For $p, q \in Q$, we denote by $P_{p,q}$ the set of paths $(q_0, \dots, q_m)$ with $q_0 = p$ and $q_m = q$. Thus, we are interested in computing $\mu(P_{p,q})$ for any $p, q \in Q$. So, we let

$$\|\mathcal{A}\| : \begin{cases} Q \times Q \to S \\ (p, q) \mapsto \mu(P_{p,q}) \end{cases}$$

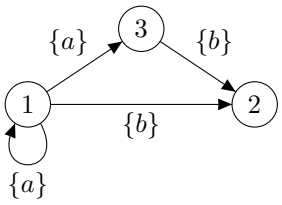


FIG. 1.2. Weighted system over $\mathbb{L}\text{ang}_A$

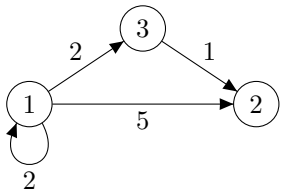


FIG. 1.3. Weighted system over $\mathbb{T}\text{rop}$

EXAMPLE 1.6. Let $A = \{a, b\}$ and consider Fig. 1.2, depicting a closed weighted system $\mathcal{A} = (Q, \mu)$ over $\mathbb{L}\text{ang}_A$. A labeled edge $(p, s, q) \in Q \times S \times Q$ indicates that $\mu(p, q) = s \neq \mathbb{0}$. Edges (p, s, q) with $\mu(p, q) = s = \mathbb{0}$ are omitted. The weight function μ and its semantics $\|\mathcal{A}\|$ are given as follows:

μ	1	2	3
1	$\{a\}$	$\{b\}$	$\{a\}$
2	$\varnothing$	$\varnothing$	$\varnothing$
3	$\varnothing$	$\{b\}$	$\varnothing$

$\|\mathcal{A}\|$	1	2	3
1	a^*	a^*b	a^*a
2	$\varnothing$	$\varnothing$	$\varnothing$
3	$\varnothing$	b	$\varnothing$

EXAMPLE 1.7. Consider Fig. 1.3, depicting a closed weighted system $\mathcal{A} = (Q, \mu)$ over $\mathbb{T}\text{rop}$ (*i.e.*, a weighted directed graph). We have:

μ	1	2	3
1	2	5	2
2	∞	∞	∞
3	∞	1	∞

$\|\mathcal{A}\|$	1	2	3
1	0	3	2
2	∞	0	∞
3	∞	1	0

Roy-Floyd-Warshall algorithm. The algorithms of sections 1.1, 1.2 and 1.3 can be presented as a single algorithm, called Roy-Floyd-Warshall algorithm [Cor+09], on an adequate semiring. Only the semiring differs from one problem to another.

Let $\mathcal{A} = (Q, \mu)$ be a closed weighted system over a closed semiring $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$.

To compute $\|\mathcal{A}\|$, we follow our above scheme and assume $Q = \{1, \dots, n\}$. For $i, j \in Q$ and $k \in \{1, \dots, n\}$, let

$P_{i,j}^{(k)}$ contain the paths $(i_0, \dots, i_m) \in P_{i,j}$ with $1 \leqslant i_1, \dots, i_{m-1} \leqslant k$

$P_{i,j}^{(0)}$ contain the paths from $P_{i,j}$ of the form (i_0) or (i_0, i_1)

In particular, $P_{ij}^{(n)} = P_{ij}$. We would like to compute $\|\mathcal{A}\|(i,j) = \mu(P_{i,j})$, for all $i, j \in Q$. In the following, we use $h_{i,j}^{(k)} = \mu(P_{i,j}^{(k)})$ as an abbreviation.

From the definitions, we directly deduce

$$h_{i,j}^{(0)} = \begin{cases} \mu(i,j) + \mathbb{1} & \text{if } i = j \\ \mu(i,j) & \text{if } i \neq j \end{cases}$$

For $k \geqslant 1$, we have:

$$h_{i,j}^{(k)} = \mu(P_{i,j}^{(k)}) = \sum_{\rho \in P_{i,j}^{(k)}} \mu(\rho) = \underbrace{\sum_{\rho \in P_{i,j}^{(k-1)}} \mu(\rho)}_{= h_{i,j}^{(k-1)}} + \underbrace{\sum_{\rho \in P_{i,j}^{(k)} \setminus P_{i,j}^{(k-1)}} \mu(\rho)}_{U}$$

where

$$U = \sum_{\substack{\rho_1 \in P_{i,k}^{(k-1)} \\ \rho_2 \in P_{k,k}^{(k)} \\ \rho_3 \in P_{k,j}^{(k-1)}}} \mu(\rho_1) \cdot \mu(\rho_2) \cdot \mu(\rho_3) = \underbrace{\sum_{\rho_1 \in P_{i,k}^{(k-1)}} \mu(\rho_1)}_{= h_{i,k}^{(k-1)}} \cdot \underbrace{\sum_{\rho_2 \in P_{k,k}^{(k)}} \mu(\rho_2)}_{V} \cdot \underbrace{\sum_{\rho_2 \in P_{k,j}^{(k-1)}} \mu(\rho_3)}_{= h_{k,j}^{(k-1)}}$$

Now we have

$$V = \mathbb{1} + \sum_{\ell \geqslant 1} \sum_{\substack{\rho_1, \dots, \rho_\ell \\ \in P_{k,k}^{(k-1)}}} \mu(\rho_1) \cdot \ldots \cdot \mu(\rho_\ell) = \mathbb{1} + \sum_{\ell \geqslant 1} \Big(\underbrace{\sum_{\rho \in P_{k,k}^{(k-1)}} \mu(\rho)}_{} \Big)^{\ell} h_{k,k}^{(k-1)} = \big(h_{k,k}^{(k-1)}\big)^*$$

Altogether, we obtain, for $k \in \mathbb{N}$:

$$h_{i,j}^{(k)} = \begin{cases} \mu(i,j) + \mathbb{1} & \text{if } i = j \text{ and } k = 0 \\ \mu(i,j) & \text{if } i \neq j \text{ and } k = 0 \\ h_{i,j}^{(k-1)} + \big(h_{i,k}^{(k-1)} \cdot \big(h_{k,k}^{(k-1)}\big)^* \cdot h_{k,j}^{(k-1)}\big) & \text{if } k \geqslant 1 \end{cases}$$

The procedure is suggested by these equations to compute $\|\mathcal{A}\|$ is called Roy-Floyd-Warshall algorithm.

The matrix approach. Again, let $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ be a **closed** semiring and $\mathcal{A} = (Q, \mu)$ be a closed weighted system over $\mathbb{S}$. To determine $\|\mathcal{A}\|$, we can work with matrix operations in the semiring $(S^{Q \times Q}, +, \cdot, \mathbb{0}, \mathbb{1})$ of $(Q \times Q)$-matrices with coefficients in $\mathbb{S}$. One can verify that this semiring is closed. Note that both $\|A\|$ and μ can be considered as $(Q \times Q)$-matrices with entries $\|A\|_{p,q} = \|A\|(p,q)$ and $\mu_{p,q} = \mu(p,q)$, respectively.

THEOREM 1.8. *Let $\mathcal{A} = (Q, \mu)$ be a closed weighted system. We have that*

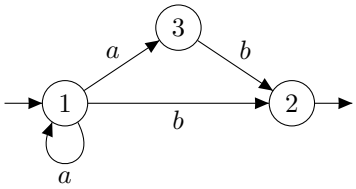
$$\|\mathcal{A}\| = \mu^* .$$

PROOF. Exercise. ∎

Markov chains. A weighted system that is not closed does not always have this natural semantics. Consider the following classical definition:

DEFINITION 1.9. A *discrete-time Markov chain* is a weighted system (Q, μ) over $\mathbb{P}\mathrm{rob}$ such that, for all $p \in Q$, $\sum_{q \in Q} \mu(p,q) \in \{0, 1\}$. ∎

In the case of a discrete-time Markov chain, however, the matrix $(\mu)^n$ contains the probabilities of going from p to q in exactly n steps.



Exercises for Chapter 1

EXERCISE 1.1. Let the NFA $\mathcal{A}$ with alphabet $A = \{a, b\}$ be given as follows:
Using the Floyd-Warshall method, specify a regular expression equivalent to $\mathcal{A}$.

EXERCISE 1.2. Which of the semirings from Example 1.3 is commutative, which of them is closed?

EXERCISE 1.3. Apply the matrix approach to the automaton of Fig. 1.2.

EXERCISE 1.4. Apply the matrix approach to the automaton of Fig. 1.3.

EXERCISE 1.5. Prove Theorem 1.8.

Further reading and references

[Cor+09] Th. H. Cormen et al. *Introduction to Algorithms*. 3rd. McGraw-Hill Higher Education, 2009 (cit. on p. 4).

CHAPTER 2

Weighted Automata: Definitions and Problems

In this section, $\mathbb{S}$ denotes a semiring $(S, +, \cdot, \mathbb{0}, \mathbb{1})$ and A a finite alphabet. A *formal power series*, or, for short, a *series* over A and $\mathbb{S}$ is a mapping $A^* \to S$ (we might also write $A^* \to \mathbb{S}$). The set of those formal power series is denoted by $\mathbb{S}\langle\langle A^* \rangle\rangle$. We are interested in automata whose semantics is a series.

We shall only present basic definitions here. The interested reader can find much more material in [Sak09], [KS85] or [DKV09], for instance.

1. Definitions and Examples

DEFINITION 2.1. A *weighted automaton* over the semiring $\mathbb{S}$ is a structure $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ where

- Q is the nonempty finite set of *states*,
- A is the *input alphabet*,
- $\mu : Q \times A \times Q \to S$ is the *transition-weight function*,
- $\lambda : Q \to S$ is the *initial-weight function*, and
- $\gamma : Q \to S$ is the *final-weight function*. ■

We represent weighted automata as usual automata, indicating the weights on each transition. When $\mu(p, a, q) = \mathbb{0}$, we do not put any edge between state p and state q. When $\mu(p, a, q) = k \neq \mathbb{0}$, we represent this transition graphically, using one of the conventions in Fig. 2.1. If in addition $\mu(b) = \ell$, with the

FIG. 2.1. Two graphical representations of transitions in weighted automata

representation (ii) we would label the edge by $k.a + \ell.b$.

Let $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be a weighted automaton over $\mathbb{S}$. To define the semantics $\|\mathcal{A}\|$ of $\mathcal{A}$, we extend μ to paths and, afterwards, to sets of paths. The weight of a word $w \in A^*$ is then the sum of all weights of paths that are labeled with w.

A *path* of $\mathcal{A}$ is an alternating sequence $\rho = (q_0, a_1, q_1, \ldots, a_n, q_n)$, $n \in \mathbb{N}$, of states $q_i \in Q$ and letters $a_i \in A$. We call $w = a_1 \cdots a_n$ the *label* of ρ. The weight of ρ is

$$\mu(\rho) \stackrel{\text{def}}{=} \lambda(q_0) \cdot \mu(q_0, a_1, q_1) \cdot \cdots \cdot \mu(q_{n-1}, a_n, q_n) \cdot \gamma(q_n)\,.$$

For a set P of paths, we let

$$\mu(P) \stackrel{\text{def}}{=} \begin{cases} \mathbb{0} & \text{if } P = \varnothing \\ \sum\limits_{\rho \in P} \mu(\rho) & \text{if } P \neq \varnothing \end{cases}$$

For $w = a_1 \ldots a_n \in A^*$, let P_w denote the set of all paths with label w. Then, we set

$$\|\mathcal{A}\|(w) \stackrel{\text{def}}{=} \mu(P_w).$$

One can easily verify the following statement.

PROPOSITION 2.2. Let $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be a weighted automaton over $\mathbb{S}$. For each letter $a \in A$, define the $(Q \times Q)$-matrix $\mu(a) \in \mathbb{S}^{Q \times Q}$ given by $\mu(a)_{p,q} = \mu(p, a, q)$. Similarly, consider λ as a row-vector in $\mathbb{S}^{1 \times n}$, and γ as a column vector in $\mathbb{S}^{n \times 1}$. Then

$$\|\mathcal{A}\|(a_1 \cdots a_n) = \lambda \cdot \mu(a_1) \cdot \ldots \cdot \mu(a_n) \cdot \gamma$$ ■

In the following, we will demonstrate that weighted automata are a generic model that subsumes many important automata classes.

1.1. Finite automata. A (non-deterministic) finite automaton is simply a weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over $\mathbb{B}\mathrm{ool}$ such that $\lambda^{-1}(\mathsf{true})$ is a singleton set (containing the unique initial state). The semantics of $\mathcal{A}$ is a mapping $\|\mathcal{A}\| : A^* \to \{\mathsf{true}, \mathsf{false}\}$ where true signals "accepted" and false "rejected". Usually, finite automata come with a set of final states $F \subseteq Q$ and a transition relation $\Delta \subseteq Q \times A \times Q$, which can be recovered from $\mathcal{A}$ by letting $F = \gamma^{-1}(\mathsf{true})$ and $\Delta = \mu^{-1}(\mathsf{true})$.

1.2. Probabilistic automata. A *probabilistic automaton* is a weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over $\mathbb{P}\mathrm{rob} = (\mathbb{R}_{\geqslant 0}, +, \cdot, 0, 1)$ such that

(1) there is a single state $p \in Q$ such that $\lambda(p) = 1$ and, for all $q \in Q \setminus \{p\}$, $\lambda(q) = 0$,
(2) for all $p \in Q$, $\gamma(p) \in \{0, 1\}$, and
(3) for all $p \in Q$ and $a \in A$, we have $\sum_{q \in Q} \mu(p, a, q) = 1$.

In that model, $\|\mathcal{A}\|(w)$ can be interpreted as the probability of reaching a final state when w is used as a *scheduling policy*.

1.3. Generative probabilistic automata. A *generative probabilistic automaton* is defined like a probabilistic automaton, apart from condition (3), which is replaced with

(3') for every $p \in Q$, we have $\sum_{(a,q) \in A \times Q} \mu(p, a, q) = 1$.

In that model, $\|\mathcal{A}\|(w)$ can be considered as the probability of executing w *and* ending in a final state, under the precondition that we perform $|w|$ steps.

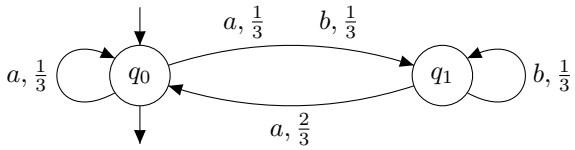


FIG. 2.2. A generative probabilistic automaton

EXAMPLE 2.3. Fig. 2.2 depicts a generative probabilistic automaton $\mathcal{A}$ over $\{a, b\}$. We have $\|\mathcal{A}\|(a) = \|\mathcal{A}\|(aa) = \frac{1}{3}$ and $\|\mathcal{A}\|(aaa) = \frac{5}{27}$ Moreover, $\|\mathcal{A}\|(w) = 0$ whenever w ends with the letter b. ■

1.4. Word transducers. A word transducer over an alphabet B is a weighted automaton over $\mathbb{R}\mathrm{eg}_B = (\mathrm{Rat}(B), \cup, \cdot, \varnothing, \{\varepsilon\})$. That is, transitions are labeled by letters of A, and weights are regular languages over B, and the semantics associates to a word in A^* a regular language in B^*.

2. Decision Problems for Weighted Automata

In classical automata theory, one often raises the question if a given automaton exhibits *some* behavior. Regarding a weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over a semiring $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$, this corresponds to asking if there is some word $w \in A^*$ such that $\|\mathcal{A}\|(w) \neq \mathbb{0}$.

Let $\mathscr{C}$ be a class of weighted automata over $\mathbb{S}$. The *emptiness problem* for $\mathscr{C}$ is given as follows:

INPUT	Weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma) \in \mathscr{C}$.
EMPTINESS PROBLEM	Do we have $\|\mathcal{A}\|(w) \neq \mathbb{0}$ for some word $w \in A^*$?

Under suitable assumptions (*e.g.*, for computable fields) this problem is decidable [Sch61; BR11], as we shall see for probabilistic automata in Chapter 3. The emptiness problem can be refined when the semiring comes with an ordering, which, given a formal power series, allows us to classify words according to a threshold. When we have a (possibly generative) probabilistic automaton, for example, we might be interested in the set of words that are accepted with a probability greater than some $\theta \in [0, 1]$. Or, given a word transducer, we might want to compute the set of words that generate sets that subsume a given regular language. In the subsequent chapters, we will see that both questions are undecidable. Let us give a general formal definition of this problem.

DEFINITION 2.4. Let $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ be a semiring, $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be a weighted automaton over $\mathbb{S}$, let $\bowtie \subseteq S \times S$ be a binary relation, and let $\theta \in S$. The *threshold language* of $\mathcal{A}$ wrt. $\bowtie$ and θ is given as follows:

$$L_{\bowtie\theta}(\mathcal{A}) \stackrel{\text{def}}{=} \{w \in A^* \mid \|\mathcal{A}\|(w) \bowtie \theta\}. \qquad \blacksquare$$

For instance, for probabilistic automata, $L_{=\frac{1}{2}}(\mathcal{A})$ represents the language of words accepted with probability exactly $\frac{1}{2}$, while $L_{\geqslant\frac{1}{4}}(\mathcal{A})$ is the set of words accepted with probability at least $\frac{1}{4}$.

It is easy to see, for instance in the probabilistic semiring, that threshold languages already capture regular languages. It is therefore natural, for a semiring $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$, a relation $\bowtie \subseteq S \times S$, and a class $\mathscr{C}$ of weighted automata over $\mathbb{S}$, to consider the following problem:

INPUT	Weighted automaton $\mathcal{A} \in \mathscr{C}$ and $\theta \in S$.
THRESHOLD REGULARITY FOR $\mathscr{C}$ WRT. $\bowtie$	Is $L_{\bowtie\theta}(\mathcal{A})$ (effectively) regular?

If this is not the case, we may want to decide whether a threshold language is empty or universal.

INPUT	Weighted automaton $\mathcal{A} \in \mathscr{C}$ and $\theta \in S$.
THRESHOLD EMPTINESS FOR $\mathscr{C}$ WRT. $\bowtie$	Do we have $L_{\bowtie\theta}(\mathcal{A}) \neq \varnothing$?
THRESHOLD UNIVERSALITY FOR $\mathscr{C}$ WRT. $\bowtie$	Do we have $L_{\bowtie\theta}(\mathcal{A}) = A^*$?

These questions will be studied in Chapters 3 and 6 for probabilistic automata and word transducers. Another direction to refine the emptiness problem, once we have a binary relation $\bowtie$ on $\mathbb{S}$, is to compare universally or existentially the semantics of two given automata.

INPUT	Weighted automata $\mathcal{A}, \mathcal{B} \in \mathscr{C}$.
(IN)EQUALITY FOR $\mathscr{C}$ WRT. $\bowtie$	Do we have $\|\mathcal{A}\|(w) \bowtie \|\mathcal{B}\|(w)$ for all $w \in A^*$?
EXISTENTIAL (IN)EQUALITY FOR $\mathscr{C}$ WRT. $\bowtie$	Is there $w \in A^*$ such that $\|\mathcal{A}\|(w) \bowtie \|\mathcal{B}\|(w)$?

When the semiring is endowed with a distance, one can define the notion of isolated cut point.

DEFINITION 2.5. Let $\mathbb{S}$ be a semiring endowed with a distance d. Let $\mathcal{A}$ be a weighted automaton and let $\theta \in S$. We say that θ is an *isolated cut point* of $\mathcal{A}$ if there is $\delta > 0$ such that, for all $w \in A^*$, we have

$$d(\|\mathcal{A}\|(w) - \theta) \geqslant \delta. \qquad \blacksquare$$

For probabilistic automata, we will show that the THRESHOLD REGULARITY problem stated above has a positive answer if θ is an isolated cut point. In fact, the associated threshold language is always regular in this case. It is therefore natural to consider the following problem.

INPUT	A weighted automaton $\mathcal{A} \in \mathscr{C}$ and $\theta \in S$.
ISOLATED CUT POINT PROBLEM FOR $\mathscr{C}$ WRT. $\bowtie$	Is θ an isolated cut point for $\mathcal{A}$?

These questions will be studied for some particular semirings in the next chapters.

Further reading and references

[BR11] J. Berstel and Ch. Reutenauer. *Noncommutative rational series with applications*. Vol. 137. Encyclopedia of Mathematics and Its Applications. Preliminary version at http://tagh.de/tom/wp-content/uploads/berstelreutenauer2008.pdf. Cambridge University Press, 2011 (cit. on p. 8).

[Cor+09] Th. H. Cormen et al. *Introduction to Algorithms*. 3rd. McGraw-Hill Higher Education, 2009.

[DKV09] M. Droste, W. Kuich, and W. Vogler. *Handbook of Weighted Automata*. Springer, 2009 (cit. on p. 7).

[KS85] W. Kuich and A. Salomaa. *Semirings, Automata and Languages*. Springer, 1985 (cit. on p. 7).

[Moh02] M. Mohri. "Semiring frameworks and algorithms for shortest-distance problems". In: *Journal of Automata, Languages, and Combinatorics* 7.3 (2002), pp. 321–350. ISSN: 1430-189X.

[Sak09] J. Sakarovitch. *Elements of Automata Theory*. New York, NY, USA: Cambridge University Press, 2009. ISBN: 0521844258, 9780521844253 (cit. on p. 7).

[Sch61] M.-P Schützenberger. "On the definition of a family of automata". In: *Information and Control* 4 (1961), pp. 245–270 (cit. on p. 8).

CHAPTER 3

Probabilistic Automata and Stochastic Languages

In Chapter 2, we have seen the definition of weighted automata, whose semantics is a mapping from A^* into a semiring. This chapter studies a particular kind of weighted automata: probabilistic automata. For probabilistic automata, the underlying semiring is $\mathbb{P}\mathrm{rob} = (\mathbb{R}_{\geqslant 0}, +, \cdot, 0, 1)$. A probabilistic automaton associates to each word a value in $\mathbb{R}_{\geqslant 0}$, which can be interpreted as the probability that this word is accepted by the automaton.

1. Definitions

Remember that $\mathbb{P}\mathrm{rob}$ denotes the probabilistic semiring $(\mathbb{R}_{\geqslant 0}, +, \cdot, 0, 1)$. We recall the definition given in Chapter 2 of a probabilistic automaton, which goes back to Rabin [Rab63].

DEFINITION 3.1. A *probabilistic automaton* is a weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over $\mathbb{P}\mathrm{rob} = (\mathbb{R}_{\geqslant 0}, +, \cdot, 0, 1)$ such that

(1) there is a single state $p \in Q$ such that $\lambda(p) = 1$ and, for all $q \in Q \setminus \{p\}$, $\lambda(q) = 0$,
(2) for all $p \in Q$, $\gamma(p) \in \{0, 1\}$, and
(3) for all $p \in Q$ and $a \in A$, we have $\sum_{q \in Q} \mu(p, a, q) = 1$.

Other common terms for this model are *probabilistic finite automaton (PFA)* or *reactive probabilistic automata* [Seg06]. When we neglect final states and consider the unfolding semantics rather than formal power series, then they also correspond to the classical model of a *Markov decision process* (MDP) [Put94].

The unique state p with $\lambda(p) = 1$ can be considered to be the initial state, and those states q with $\gamma(q) = 1$ are the final states.

A matrix of $\mathbb{R}_{\geqslant 0}^{Q \times Q}$ is *stochastic* if each of its rows sums to 1. Recall that we can view μ as the mapping from A into $\mathbb{R}_{\geqslant 0}^{Q \times Q}$ defined by $\mu(a)_{p,q} = \mu(p, a, q)$. Condition (3) states that the matrix $\mu(a)$ is stochastic for every letter $a \in A$. The value $\mu(p, a, q)$ can be interpreted as the probability to reach state q from state p upon reading letter a.

We still denote by μ the monoid homomorphism from A^* to $\mathbb{R}_{\geqslant 0}^{Q \times Q}$ induced by μ. It is easy to verify that the product of two stochastic matrices is again a stochastic matrix (that is, the set of stochastic matrices is actually a submonoid of $(\mathbb{R}_{\geqslant 0}^{n \times n}, ., \mathbb{1}_n)$. Consequently, (3) is equivalent to:

(3′) for every $p \in Q$ and every word $w \in A^*$, we have $\sum_{q \in Q} \mu(p, w, q) = 1$.

Recall that the semantics $\|\mathcal{A}\|$ of $\mathcal{A}$ is the mapping $\|\mathcal{A}\| : A^* \to \mathbb{P}\mathrm{rob}$ defined by $\|\mathcal{A}\|(w) = \lambda \cdot \mu(w) \cdot \gamma$. The weight $\|\mathcal{A}\|(w)$ of a word $w \in A^*$ can be seen as its probability of acceptance. More precisely, $\|\mathcal{A}\|(w)$ can be interpreted as the probability of reaching a final state when w is used as a scheduling policy. Observe that $\|\mathcal{A}\|(\varepsilon) \in \{0, 1\}$ by condition (1). Also recall that $\|\mathcal{A}\|(w)$ can be computed by adding the weights of all runs on w, where the weight of a run $(p_0, a_1, p_1), \ldots, (p_{k-1}, a_k, p_k)$ is the product $\lambda(p_0) \cdot \mu(p_0, a_1, p_1) \cdots \mu(p_{k-1}, a_k, p_k)\gamma(p_k)$.

Note that replacing (3) in Definition 3.1 with

(4) for every $p \in Q$ and $a \in A$, we have $\sum_{q \in Q} \mu(p, a, q) \in \{0, 1\}$.

is not more general, as one can always introduce a non-accepting sink state.

EXAMPLE 3.2. A probabilistic automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ with $Q = \{1, 2\}$ and $A = \{a, b\}$ is depicted in Fig. 3.1.

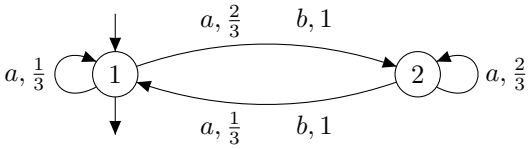


FIG. 3.1. A probabilistic automaton

Hereby,

$$\lambda = \begin{pmatrix} 1 & 0 \end{pmatrix} \qquad \mu(a) = \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix} \qquad \mu(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

For $n \in \mathbb{N}$, we have

$$\|\mathcal{A}\|(ab^n) = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{cases} \frac{1}{3} & \text{if } n \text{ is even} \\ \\ \frac{2}{3} & \text{if } n \text{ is odd} \end{cases}$$

Moreover, the image of $\|\mathcal{A}\|$ is finite, *i.e.*, $\|\mathcal{A}\|(A^*) = \{0, \frac{1}{3}, \frac{2}{3}, 1\}$. ■

EXAMPLE 3.3. For the probabilistic automaton given in Example 3.2, we have

$$L_{>0}(\mathcal{A}) = \{a, b\}^* \setminus \{b^n \mid n \text{ is odd}\}\,.$$

This threshold language is regular, which is not always the case as we shall see in the next section.

LEMMA 3.4. *Given two probabilistic automata $\mathcal{A}_1$ and $\mathcal{A}_2$, one can build automata $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$ such that*

(1) $\|\mathcal{B}_1\| = 1 - \|\mathcal{A}_1\|$,
(2) $\|\mathcal{B}_2\| = \|\mathcal{A}_1\| \cdot \|\mathcal{A}_2\|$,
(3) $\|\mathcal{B}_3\|(w) = \begin{cases} 0 & \text{if } w = \varepsilon \\ \alpha\|\mathcal{A}_1\|(w) + \beta\|\mathcal{A}_2\|(w) & \text{otherwise.} \end{cases}$, *where* $\alpha, \beta \in [0,1]$ *and* $\alpha + \beta \leqslant 1$.

PROOF. Exercise. ■

2. Stochastic Languages

In this section, we consider the THRESHOLD REGULARITY problem. We will consider threshold languages. This study can be motivated by problems that we encounter in the context of verification. Suppose that, for some alphabet A^*, we are given a set $Bad \subseteq A^*$ of bad behaviors, which our system $\mathcal{A}$ should accept with a very low probability 0.001. Then, we would like to have

$$Bad \cap L_{>0.001}(\mathcal{A}) = \varnothing\,.$$

If we are given a liveness property in terms of a set $Good \subseteq A^*$, then we would need a statement such as

$$Good \subseteq L_{>0.999}(\mathcal{A})\,.$$

So let us study the expressiveness of probabilistic automata in terms of threshold languages.

DEFINITION 3.5. We say that a language $L \subseteq A^*$ is <u>*stochastic*</u> if there are a probabilistic automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ and $\theta \in [0,1]$ such that $L = L_{>\theta}(\mathcal{A})$. ■

In this section, we will show the following fundamental results:

(1) Every regular language is stochastic.
(2) There is a stochastic language that is not recursively enumerable.
(3) For isolated cut point, the associated threshold language is regular. In other words, the THRESHOLD REGULARITY problem where we know in advance that θ is an isolated cut point is decidable (and its answer is positive).

THEOREM 3.6. *For every regular language L, there is a probabilistic automaton $\mathcal{A}$ such that $L = L_{>0}(\mathcal{A})$.*

PROOF. Exercise. ∎

THEOREM 3.7 (Rabin [Rab63]). *There is a stochastic language over the alphabet* $\{\mathbf{0},\mathbf{1}\}$ *that is not recursively enumerable.*

PROOF. We first build a probabilistic automaton $\mathcal{A}$ such that

$$\forall \theta_1,\theta_2 \in [0,1], \quad \theta_1 \neq \theta_2 \Longrightarrow L_{>\theta_1}(\mathcal{A}) \neq L_{>\theta_2}(\mathcal{A}). \tag{3.1}$$

This will show the result, since this shows that there are uncountably many stochastic languages, whereas there are only finitely many recursively enumerable languages.

Let $A = \{\mathbf{0},\mathbf{1}\}$ (we use boldface to distinguish the letters from the weights) and let $w = a_1 \dots a_n \in A^*$, with each $a_i \in \{\mathbf{0},\mathbf{1}\}$. We define $\overline{w}$ as the real number $\mathbf{0}.a_n \cdots a_1$ in binary expansion, *i.e.*, $\overline{\varepsilon} = 0$ and, if $n \geqslant 1$,

$$\overline{w} = \frac{a_n}{2^1} + \frac{a_{n-1}}{2^2} + \cdots + \frac{a_1}{2^n}$$

The probabilistic automaton $\mathcal{A}$ we exhibit computes $\overline{w}$, *i.e.*, $\|\mathcal{A}\|(w) = \overline{w}$. This actually shows (3.1). Indeed, $\overline{A^*}$, the set of rational of the form $\frac{a_n}{2^1} + \frac{a_{n-1}}{2^2} + \cdots + \frac{a_1}{2^n}$, is dense in $[0,1]$. Therefore, if $\theta_1 < \theta_2$, then there exist $\theta,\theta' \in \overline{A^*}$ such that $\theta_1 < \theta < \theta' < \theta_2$, so that $L_{>\theta_1}(\mathcal{A}) \supseteq L_{>\theta}(\mathcal{A}) \supsetneq L_{>\theta'}(\mathcal{A}) \supseteq L_{>\theta_2}(\mathcal{A})$.

The probabilistic automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ is pictured on Fig. 3.1. Recall that an edge from state p to state q is labeled $\mu(p,\mathbf{0},q)\mathbf{0} + \mu(p,\mathbf{1},q)\mathbf{1}$. For instance, the transition from state 2 to itself indicates that $\mu(2,\mathbf{0},2) = \frac{1}{2}$ and $\mu(2,\mathbf{1},2) = 1$.

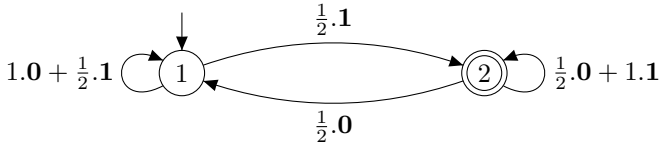


FIG. 3.2. A probabilistic automaton computing the value $\overline{w}$

Formally, $\mathcal{A}$ is given by $Q = \{1,2\}$, $A = \{\mathbf{0},\mathbf{1}\}$, and

$$\lambda = \begin{pmatrix} 1 & 0 \end{pmatrix} \qquad \mu(\mathbf{0}) = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \qquad \mu(\mathbf{1}) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{pmatrix} \qquad \gamma = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

We check that, for all $w \in A^*$,

$$\|\mathcal{A}\|(w) = \overline{w}\,. \tag{$*$}$$

We show ($*$) by induction on $n = |w|$. The claim clearly holds for $n = 0$. Moreover, in the case $n = 1$,

$$\begin{aligned} \|\mathcal{A}\|(\mathbf{0}) &= \mu(\mathbf{0})_{1,2} = \mathbf{0.0} = \overline{\mathbf{0}} \\ \text{and} \quad \|\mathcal{A}\|(\mathbf{1}) &= \mu(\mathbf{1})_{\mathbf{1},2} = \mathbf{0.1} = \overline{\mathbf{1}}\ . \end{aligned}$$

Now suppose, for $w = a_1 \dots a_n$ with $n \geqslant 1$, that $\|\mathcal{A}\|(w) = \overline{w}$ holds. Moreover, let

$$\mu(w) = \begin{pmatrix} 1-p & p \\ 1-q & q \end{pmatrix}$$

for suitable $p,q \in [0,1]$. In particular,

$$p = \|\mathcal{A}\|(w) = \overline{w}\,. \tag{$+$}$$

Let $a \in \{\mathbf{0}, \mathbf{1}\}$. We have

$$\|\mathcal{A}\|(a_1 \dots a_n a) \;=\; \mu(a_1 \dots a_n a)_{1,2} = \left(\begin{pmatrix} 1-p & p \\ 1-q & q \end{pmatrix} \cdot \mu(a) \right)_{1,2} = \begin{cases} \dfrac{p}{2} & \text{if } a = \mathbf{0} \\ \dfrac{1+p}{2} & \text{if } a = \mathbf{1} \end{cases}$$

$$= \frac{a}{2} + \frac{p}{2} \overset{(+)}{=} \mathbf{0}.a \;+\; \mathbf{0}.\mathbf{0}a_n \dots a_1 = \mathbf{0}.aa_n \dots a_1 \;=\; \overline{a_1 \dots a_n a}$$

This concludes the proof of Theorem 3.7. ∎

Remark 3.8. The proof of Theorem 3.7 is a pure existence proof. However, one can come up with a concrete counterexample. Let $w_0, w_1, \dots$ be any enumeration of A^*. For $\theta = \overline{w_0 w_1 \dots}$ (with a suitable extension of the encoding to infinite sequences), $L_{>\theta}(\mathcal{A})$ is not recursively enumerable (without proof).

In the following, we will show that, in some cases, the threshold language is regular. This is obviously the case if the threshold is 0:

Theorem 3.9. *Let $\mathcal{A}$ be a probabilistic automaton. Then, $L_{>0}(\mathcal{A})$ is regular.*

Proof. Let $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be a probabilistic automaton. Consider the NFA $\mathcal{B} = (Q, A, \Delta, Q_0, F)$ given by

- $Q_0 = \{q \in Q \mid \lambda(q) = 1\}$,
- $F = \{q \in Q \mid \gamma(q) = 1\}$, and
- $\Delta = \{(p, a, q) \in Q \times A \times Q \mid \mu(p, a, q) > 0\}$.

We have $L(\mathcal{B}) = L_{>0}(\mathcal{A})$. ∎

Note that Theorem 3.9 does no longer hold when one considers automata over infinite words [BBG08].

Next, we show that threshold languages are regular if the threshold is a certain *isolated cut point*. Intuitively, the formal power series of an automaton does not converge against an isolated cut point. We use the usual distance $d(\alpha, \beta) = |\alpha - \beta|$ on $\mathbb{R}_{\geqslant 0}$. Let us reformulate the definition of isolated cut point.

Definition 3.10. Let $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be a probabilistic automaton and let $\theta \in [0, 1]$. We say that θ is an *isolated cut point* of $\mathcal{A}$ if there is $\delta > 0$ such that, for all $w \in A^*$, we have

$$|\|\mathcal{A}\|(w) - \theta| \geqslant \delta\,.$$ ∎

Theorem 3.11 (Rabin [Rab63]). *Let $\mathcal{A}$ be a probabilistic automaton and $\theta \in [0, 1]$ be an isolated cut point of $\mathcal{A}$. Then, $L_{>\theta}(\mathcal{A})$ is regular.*

Proof. Let $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be a probabilistic automaton. We assume $Q = \{1, \dots, n\}$ and $\lambda(1) = 1$ (hence, 1 is the initial state). Let θ be an isolated cut point of $\mathcal{A}$ and let $\delta > 0$ such that $|\|\mathcal{A}\|(w) - \theta| \geqslant \delta$ for all $w \in A^*$. We set $L = L_{>\theta}(\mathcal{A})$.

Consider the Myhill-Nerode congruence $\equiv_L \subseteq A^* \times A^*$ given as follows: for $u, v \in A^*$,

$$u \equiv_L v \quad \text{iff} \quad \forall w \in A^* :\; (uw \in L \iff vw \in L)$$

It is well-known that $\equiv_L$ has finite index iff L is regular. So let us show that $\equiv_L$ has indeed finitely many equivalence classes.

Let $u, v \in A^*$ and set

$$\xi^u = (\mu(u)_{1,1}, \dots, \mu(u)_{1,n})$$
$$\text{and} \quad \xi^v = (\mu(v)_{1,1}, \dots, \mu(v)_{1,n})\,.$$

These vectors contain the probabilities to go, via u and v, respectively, from the initial state 1 into states $1, \dots, n$.

We will show that

$$(*) \qquad u \not\equiv_L v \implies |\xi^u - \xi^v| \geqslant 4\delta$$

where, for an n-dimensional vector ξ, we let $|\xi| = \sum_{i=n}^{n} |\xi_i|$. Indeed, $(*)$ implies the theorem: consider the n-dimensional space $[0,1]^n$, covered by "cubes" of side length $\frac{2\delta}{n}$, starting with $[0, \frac{2\delta}{n}]^n$. If ξ^u and ξ^v are in the same cube, then $|\xi_i^u - \xi_i^v| \leqslant \frac{2\delta}{n} < \frac{4\delta}{n}$ for every i, so $|\xi^u - \xi^v| < 4\delta$, hence by $(*)$, $u \equiv_L v$. Thus, "being in the same cube" is a refinement of $\equiv_L$. As only finitely many cubes are necessary to cover $[0,1]^n$, $\equiv_L$ has only finitely many equivalence classes.

So let us show $(*)$. Suppose $u \not\equiv_L v$. There is $w \in A^*$ such that $uw \in L$ and $vw \notin L$ (or vice versa, which is analogous). As θ is an isolated cut point with bound δ, we have

$$\begin{aligned} \lambda \cdot \mu(uw) \cdot \gamma &\geqslant \theta + \delta \\ \text{and} \quad \lambda \cdot \mu(vw) \cdot \gamma &\leqslant \theta - \delta \,. \end{aligned}$$

Therefore,

$$\begin{aligned} (\lambda \cdot \mu(uw) \cdot \gamma) - (\lambda \cdot \mu(vw) \cdot \gamma) \geqslant 2\delta \iff & \lambda \cdot (\mu(uw) - \mu(vw)) \cdot \gamma \geqslant 2\delta \\ \iff & \lambda \cdot (\mu(u) \cdot \mu(w) - \mu(v) \cdot \mu(w)) \cdot \gamma \geqslant 2\delta \\ \iff & \lambda \cdot (\mu(u) - \mu(v)) \cdot \mu(w) \cdot \gamma \geqslant 2\delta \\ \iff & \textstyle\sum_{i=1}^{n} (\xi_i^u - \xi_i^v) \cdot (\mu(w) \cdot \gamma)_i \geqslant 2\delta \end{aligned}$$

Let

$$\begin{aligned} \mathrm{P} &= \sum \{\xi_i^u - \xi_i^v \mid i \in \{1, \dots, n\} and \xi_i^u - \xi_i^v > 0\} \\ \text{and } \mathrm{N} &= \sum \{|\xi_i^u - \xi_i^v| \mid i \in \{1, \dots, n\} and \xi_i^u - \xi_i^v < 0\} \,. \end{aligned}$$

With this, $\mathrm{P} \geqslant 2\delta$. As $\sum_{i=1}^{n} \xi_i^u = \sum_{i=1}^{n} \xi_i^v = 1$, it holds $\mathrm{P} = \mathrm{N}$. Therefore,

$$\textstyle\sum_{i=1}^{n} |\xi_i^u - \xi_i^v| \;=\; 2\mathrm{P} \;\geqslant\; 4\delta \,.$$

We conclude $|\xi^u - \xi^v| \geqslant 4\delta$. ∎

3. Threshold emptiness and Isolated cut points

We first show that the Threshold emptiness problem is undecidable, first for equality as $\bowtie$, and $\theta = \frac{1}{2}$. The proof can then be adapted for other threshold values. This result is due to Paz [Paz71]. We present here another proof, which can be found *e.g.* in [BC08; Gim10]. See also [MHC03] for an alternative, but more technical proof.

Theorem 3.12 (Paz [Paz71]). *The following problem is undecidable:*

Input: *A probabilistic automaton $\mathcal{A}$.*
Problem: *Do we have $L_{=\frac{1}{2}}(\mathcal{A}) \neq \varnothing$?*

Proof. The proof is a reduction from the following undecidable variant of the Post's correspondence problem (PCP):

Input: Alphabet A and morphisms $f_i : A^* \to \{0,1\}^*$ $(i = 1, 2)$ such that $f_i(A) \subseteq 1\{0,1\}^*$.
Problem: Is there $w \in A^+$ such that $f_1(w) = f_2(w)$?

The idea is that, under the condition $f_i(A) \subseteq 1\{0,1\}^*$, we have $f_1(w) = f_2(w)$ if and only if $\overline{f_1(w)} = \overline{f_2(w)}$. Just as we can compute $\overline{w}$ with a probabilistic automaton, we can as well compute $\overline{f_i(w)}$ for $i = 1, 2$. Combining the automata computing $\overline{f_i(w)}$, one can build, using Lemma 3.4, an automaton computing 0 on the empty word and $\frac{1}{2}(\overline{f_1(w)} + 1 - \overline{f_2(w)})$ on $w \neq \varepsilon$. This function yields $\frac{1}{2}$ exactly on the words $w \in A^+$ such that $\overline{f_1(w)} = \overline{f_2(w)}$, *i.e.*, $f_1(w) = f_2(w)$.

The original PCP does not have the restriction $f_i(A) \subseteq 1\{0,1\}^*$ on morphisms. It is however easy to enforce this starting from two arbitrary morphisms g_1, g_2: it suffices to replace g_i by $f_i = f \circ g_i$ where $f : \{0,1\}^* \to \{0,1\}^*$ is the morphism defined by $f(0) = 10$ and $f(1) = 11$. Then clearly $f_i(A) \subseteq 1\{0,1\}^*$, and $f_1(w) = f_2(w)$ if and only if $g_1(w) = g_2(w)$, which shows that the variant of PCP remains undecidable.

Let now an instance of the modified PCP be given by an alphabet A and morphisms $f_1, f_2 : A^* \to \{0,1\}^*$. Consider the mappings $\varphi_1, \varphi_2 : A^* \to \mathbb{P}\mathrm{rob}$ defined by $\varphi_i(w) = \overline{f_i(w)}$, and define the probabilistic automaton $\mathcal{A}$ as follows. For $i = 1, 2$, first let $\mathcal{A}_i = (Q, A, \lambda, \mu_i, \gamma_i)$ be the probabilistic automaton given by $Q = \{1, 2\}$,

$$\lambda = \begin{pmatrix} 1 & 0 \end{pmatrix} \quad \gamma_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \gamma_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and, for $i \in \{1, 2\}$ and $a \in A$,

$$\mu_i(a) = \begin{pmatrix} 1 - \varphi_i(a) & \varphi_i(a) \\ 1 - \varphi_i(a) - \dfrac{1}{2^{|f_i(a)|}} & \varphi_i(a) + \dfrac{1}{2^{|f_i(a)|}} \end{pmatrix}$$

One can readily verify that, for all $w \in A^*$,

$$\|\mathcal{A}_1\|(w) = \varphi_1(w)$$
$$\text{and} \quad \|\mathcal{A}_2\|(w) = 1 - \varphi_2(w)\,.$$

We combine $\mathcal{A}_1$ and $\mathcal{A}_2$ towards a probabilistic automaton $\mathcal{A}$ such that $\|\mathcal{A}\|(\varepsilon) = 0$ and, for all $w \in A^+$,

$$\begin{aligned} \|\mathcal{A}\|(w) &= \frac{1}{2}\|\mathcal{A}_1\|(w) + \frac{1}{2}\|\mathcal{A}_2\|(w) \\ &= \frac{1}{2}\varphi_1(w) + \frac{1}{2}(1 - \varphi_2(w)) \\ &= \frac{1}{2} + \frac{1}{2}(\varphi_1(w) - \varphi_2(w)) \end{aligned}$$

Then, for all $w \in A^*$, $\|\mathcal{A}\|(w) = \frac{1}{2}$ iff $w \in A^+$ and $\varphi_1(w) = \varphi_2(w)$ iff $w \in A^+$ and $f_1(w) = f_2(w)$. Note that the last step requires the fact that $f_1(w)$ and $f_2(w)$ both start with 1. This concludes the proof. ■

This result can then be used to show undecidability of the threshold emptiness problem when $\bowtie$ is $>$ or $\geqslant$.

Theorem 3.13 (Madani et al. [MHC03]). *The following problem is undecidable:*

Input: *Probabilistic automaton $\mathcal{A}$ and $\theta \in [0,1]$.*
Problem: *Do we have $L_{>\theta}(\mathcal{A}) \neq \varnothing$?*

An elegant proof of Theorem 3.13, even for fixed thresholds, uses Theorem 3.12 [Gim10].

Corollary 3.14 (of Thm. 3.12). *Let $0 < \theta < 1$. The following problems are undecidable:*

Input: *Probabilistic automaton $\mathcal{A}$.*
Problem 1: *Do we have $L_{\geqslant \frac{1}{4}}(\mathcal{A}) \neq \varnothing$?*
Problem 2: *Do we have $L_{> \frac{1}{8}}(\mathcal{A}) > \varnothing$?*

Proof. For Problem 1, using Lemma 3.4, we build $\mathcal{B}$ such that $\|\mathcal{B}\| = \|\mathcal{A}\|(1 - \|\mathcal{A}\|)$. Now, $\|\mathcal{B}\|(w) = \|\mathcal{A}\|(w)(1 - \|\mathcal{A}\|(w)) \geqslant 1/4$ if and only if $\|\mathcal{A}\|(w) = 1/2$, since $1/4$ is the maximum of the function from $[0,1]$ to $\mathbb{R}_{\geqslant 0}$ given by $t \mapsto t(1-t)$, reached only for $t = 1/2$.

We reduce Problem 1 to Problem 2. Note first that the weights occurring in the construction of $\mathcal{A}$ in the proof of Theorem 3.12 are sums of powers of 2. Adding new states, one can easily check that an automaton having only weights 0, 1/2 and 1 can be used instead. Then, the automaton $\mathcal{B}$ built from $\mathcal{A}$ can be chosen with weights only in $\{0, 1/4, 1/2, 1\}$. Hence, $\|\mathcal{B}\|(w) \geqslant 1/4$ if and only if $\|\mathcal{B}\|(w) > 1/4 - 1/4^{|w|}$. Using Lemma 3.4, one builds a probabilistic automaton $\mathcal{C}$ such that $\|\mathcal{C}\|(\varepsilon) = 0$

and $\|\mathcal{C}\|(aw) = \frac{1}{2}(\mathcal{B}(w) + 1/4^{|w|})$, so that there exists u such that $\|\mathcal{C}\|(u) > 1/8$ if and only if $u = aw$ and $\|\mathcal{C}\|(aw) > 1/8$, that is $\|\mathcal{B}\|(w) + 1/4^{|w|} > 1/4$, *i.e.*, if and only if $\|\mathcal{B}\|(w) \geqslant 1/4$. ■

One can slightly extend Corollary 3.14.

COROLLARY 3.15. *Let $\theta \in \mathbb{Q}$, $0 < \theta < 1$. Then, the* THRESHOLD EMPTINESS *problem for probabilistic automata is undecidable for θ wrt. to all relations $\bowtie \in \{<, =, >\}$.*

We have shown previously that the threshold language at an isolated cut point is regular. Unfortunately, the ISOLATED CUT POINT problem is undecidable:

THEOREM 3.16 (Bertoni et al. [BMT09]). *The following problem is undecidable:*

INPUT: *A probabilistic automaton $\mathcal{A}$ and $\theta \in [0, 1]$.*
PROBLEM: *Is θ an isolated cut point of $\mathcal{A}$?*

PROOF. We show that the problem is already undecidable for fixed $\theta = \frac{1}{2}$. For $u, v \in \{0, 1\}^*$, let $u \wedge v$ denote the longest common suffix of u and v.

The proof is by reduction from the following undecidable variant of the PCP, see [BC08] for a proof and application to probabilistic automata:

INPUT: Alphabet A and morphisms $f_i : A^* \to \{0, 1\}^*$ $(i = 1, 2)$ such that $f_i(A) \subseteq 1\{0, 1\}^*$.
PROBLEM: Is $\{f_1(w) \wedge f_2(w) \mid w \in A^*\}$ finite?

So let f_1, f_2 constitute an instance of that problem. As in the proof of Theorem 3.7, we define $\overline{\varepsilon} = 0$ and, for $w = a_1 \dots a_n \in \{0, 1\}^+$,

$$\overline{w} = \frac{a_n}{2^1} + \frac{a_{n-1}}{2^2} + \dots + \frac{a_1}{2^n}.$$

Moreover, we set, for $i = 1, 2$ and $w \in A^*$, $\phi_i(w) = \overline{f_i(w)}$.

CLAIM 3.17. The following statements are equivalent:

(1) There is $\delta > 0$ such that, for all $w \in A^+$, $|\phi_1(w) - \phi_2(w)| \geqslant \delta$.
(2) The set $\{f_1(w) \wedge f_2(w) \mid w \in A^*\}$ is finite.

PROOF of Claim 3.17.

(1) $\Longrightarrow$ (2): Assume that (2) does not hold. Pick any $n \in \mathbb{N}$. There is $w \in A^*$ such that $|f_1(w) \wedge f_2(w)| \geqslant n$. The latter implies that $|\phi_1(w) - \phi_2(w)| < \dfrac{1}{2^n}$. We conclude that (1) does not hold.

(1) $\Longleftarrow$ (2): Assume that (1) does not hold.

Case 1: Suppose there is $w \in A^+$ such that $|\phi_1(w) - \phi_2(w)| = 0$. Then, $f_1(w) = f_2(w)$. Thus, $\{f_1(w^i) \wedge f_2(w^i) \mid i = 1, 2, \dots\}$ is infinite, and so is $\{f_1(u) \wedge f_2(u) \mid u \in A^*\}$.

Case 2: Suppose that Case 1 does not apply. Then, for all $n \in \mathbb{N}$, there is $w \in A^+$ such that $0 < |\phi_1(w) - \phi_2(w)| < \dfrac{1}{2^n}$. The latter implies $|f_1(w) \wedge f_2(w)| \geqslant n$. We conclude that $\{f_1(w) \wedge f_2(w) \mid w \in A^*\}$ is infinite. ■

Consider the probabilistic automaton $\mathcal{A}$ from the proof of Theorem 3.12. Recall that $\|\mathcal{A}\|(\varepsilon) = 0$ and, for all $w \in A^+$,

$$\|\mathcal{A}\|(w) = \frac{1}{2} + \frac{1}{2}(\phi_1(w) - \phi_2(w))$$

The following statements are equivalent due to Claim 3.17:

(1) There is $\delta > 0$ such that, for all $w \in A^*$, $|\, \|\mathcal{A}\|(w) - \frac{1}{2}\,| \geqslant \delta$.
(2) There is $\delta > 0$ such that, for all $w \in A^+$, $|\phi_1(w) - \phi_2(w)| \geqslant \delta$.
(3) The set $\{f_1(w) \wedge f_2(w) \mid w \in A^*\}$ is finite.

Thus, $\frac{1}{2}$ is an isolated cut point of $\mathcal{A}$ iff $\{f_1(w) \wedge f_2(w) \mid w \in A^*\}$ is finite. Since this problem is undecidable [BC08], we have shown Theorem 3.16. ■

As before, one can extend Theorem 3.16 to other values than 1/2.

COROLLARY 3.18. *Let $\theta \cap \mathbb{Q}$, $0 < \theta < 1$. It is undecidable, given a probabilistic automaton $\mathcal{A}$, whether θ is an isolated cut point of $\mathcal{A}$.*

Bertoni et al. [BMT09] leave open the value 1 problem, which is to decide whether 1 is an isolated cut point. We now show that the ISOLATED CUT POINT problem is undecidable, even for $\theta = 1$.

THEOREM 3.19. *The value 1 problem is undecidable for probabilistic automata. That is, given an automaton $\mathcal{A}$, it is undecidable whether 1 is an isolated cut point of $\mathcal{A}$.*

PROOF. The following proof comes from [Gim10]. It uses a different technique as the one of [BMT09]: it consists in a reduction of the emptiness problem for stochastic languages to the value 1 problem. The first technical step is to construct an automaton $\mathcal{C}_\alpha$, whose weights depend on some $\alpha \in [0,1]$, such that

$$\alpha > \frac{1}{2} \iff \mathcal{C}_\alpha \text{ has value 1.} \tag{3.2}$$

The key idea is then to replace α with an arbitrary probabilistic automaton $\mathcal{A}$, *i.e.* to build from $\mathcal{A}$ a probabilistic automaton $\mathcal{C}_\mathcal{A}$ such that

$$L_{>\frac{1}{2}}(\mathcal{A}) \neq \varnothing \iff \mathcal{C}_\mathcal{A} \text{ has value 1.} \tag{3.3}$$

This provides the desired reduction from the emptiness problem.

To build $\mathcal{C}_\alpha$, first consider the probabilistic automaton $\mathcal{A}_\alpha = (\{1,2,3\}, \{a,b\}, (1,0,0), \mu_\alpha, (0,0,1))$ whose matrices $\mu_\alpha(a)$ and $\mu_\alpha(b)$ are given below, and which is pictured in Fig. 3.3.

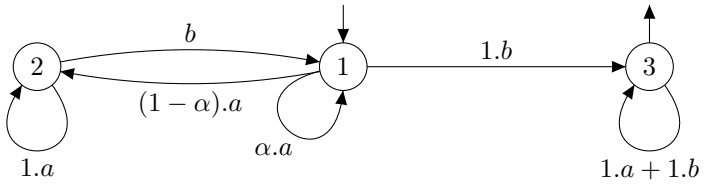


FIG. 3.3. Probabilistic automaton $\mathcal{A}_\alpha$

$$\mu(a) = \begin{pmatrix} \alpha & 1-\alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \mu(b) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ so that } \mu(a^n b) = \begin{pmatrix} 1-\alpha^n & 0 & \alpha^n \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Observe that $\mathcal{A}_\alpha(wa^k) = \mathcal{A}_\alpha(w)$ for all $w \in \{a,b\}^*$ and $k \geqslant 0$, and that $\mathcal{A}_\alpha(\varepsilon) = 0$. Therefore, if we are interested in words whose value is arbitrarily close to 1, it suffices to consider words with at least one b and no suffix in a^+, that is, of the form $w = a^{n_1} b a^{n_2} b \cdots a^{n_k} b$. By the above, applying $a^n b$ from the distribution $(0, \beta, 1-\beta)$ yields the distribution $(0, (1-\alpha^n)\beta, 1-(1-\alpha^n)\beta)$. Therefore,

$$\|\mathcal{A}_\alpha\|(w) = 1 - \prod_{i=1}^{k} (1 - \alpha^{n_i}).$$

Exchanging initial and final states, and replacing α by $1-\alpha$, we obtain a probabilistic automaton $\mathcal{B}_\alpha$ such that

$$\|\mathcal{B}_\alpha\|(w) = \prod_{i=1}^{k} (1 - (1-\alpha)^{n_i}).$$

Combining $\mathcal{A}_\alpha$ and $\mathcal{B}_\alpha$ as in Lemma 3.4, we obtain a probabilistic automaton $\mathcal{C}_\alpha$ such that

$$\|\mathcal{C}_\alpha\|(w) = \frac{1}{2}\Big[1 - \prod_{i=1}^{k} (1 - \alpha^{n_i}) + \prod_{i=1}^{k} (1 - (1-\alpha)^{n_i})\Big]. \tag{3.4}$$

If $\alpha \leqslant \frac{1}{2}$, then $\alpha \leqslant 1-\alpha$ so $\prod_{i=1}^{k}(1-\alpha^{n_i}) \geqslant \prod_{i=1}^{k}(1-(1-\alpha)^{n_i})$, hence $\|\mathcal{C}_\alpha\|(w) \leqslant \frac{1}{2}$.

Conversely, assume that $\alpha > \frac{1}{2}$. Let us show that one can choose w, that is, the integers k and n_i ($i = 1, \dots, k$), so that $\|\mathcal{C}_\alpha\|(w)$ is arbitrarily close to 1. If $\alpha = 1$ this is clear, so assume $\alpha \neq 1$. Since $\ln(1-\beta) \leqslant -\beta$ when $0 \leqslant \beta < 1$, we get $\ln \prod_{i=1}^k (1-\alpha^{n_i}) \leqslant \sum_{i=1}^k -\alpha^{n_i}$, that is:

$$\prod_{i=1}^k (1-\alpha^{n_i}) \leqslant \exp\Big(-\sum_{i=1}^k \alpha^{n_i}\Big). \tag{3.5}$$

Moreover, a straighforward induction on k shows that

$$\prod_{i=1}^k (1-(1-\alpha)^{n_i}) \geqslant 1 - \sum_{i=1}^k (1-\alpha)^{n_i}. \tag{3.6}$$

Let $\varepsilon > 0$. We first choose $n_i = K + \lfloor \log_\alpha(1/i) \rfloor$ for some integer K to be determined later. Then $\alpha^{n_i} \geqslant \alpha^{K+\log_\alpha(1/i)+1} = \alpha^{K+1}/i$, and since $\sum 1/i$ diverges to ∞, so does $\sum \alpha^{n_i}$. Therefore, there exists k such that $\sum_{i=1}^k \alpha^{n_i} \geqslant \ln(1/\varepsilon)$, hence by (3.5), we obtain

$$\prod_{i=1}^k (1-\alpha^{n_i}) \leqslant \varepsilon. \tag{3.7}$$

On the other hand, since $\alpha > 1/2$, there exists some $r > 1$ such that $1-\alpha = \alpha^r$ (namely $r = \ln(1-\alpha)/\ln\alpha$), and therefore $(1-\alpha)^{n_i} = \alpha^{rn_i} \leqslant \alpha^{r(K-1)}/i^r$. Hence $\sum_{i=1}^k (1-\alpha)^{n_i} < M\alpha^{r(K-1)}$ where $M = \sum_{i=1}^\infty 1/i^r$ (this series converges since $r > 1$). Now, for $K > 1 + \frac{1}{r}\log_\alpha(\varepsilon/M)$, we have $M\alpha^{r(K-1)} < \varepsilon$ so that by (3.6)

$$\prod_{i=1}^k (1-(1-\alpha)^{n_i}) \geqslant 1 - \varepsilon \tag{3.8}$$

Combining (3.4), (3.7) and (3.8), we obtain $\|\mathcal{C}_\alpha\|(w) \geqslant 1-\varepsilon$, which proves (3.2) as required.

We now explain the construction for (3.3). The idea is to replace the probabilistic a transitions labeled α and $1-\alpha$ by sub-automata $\mathcal{A}$ and its complement. Let $\mathcal{A}$ be a probabilistic automaton on alphabet A, with $a, b \notin A$. We transform $\mathcal{A}_\alpha$ as follows (same transformation on $\mathcal{B}_\alpha$ and $\mathcal{C}_\alpha$). We delete the a-transitions from $\mathcal{A}_\alpha$, and add the following transitions:

- a weight 1 transition from state 1 of $\mathcal{A}_\alpha$ labeled a, going in the initial state of $\mathcal{A}$,
- from final states of $\mathcal{A}$ we go back in state 1 of $\mathcal{A}_\alpha$ upon reading a a (weight 1),
- from non final states of $\mathcal{A}$ we go in state 2 of $\mathcal{A}_\alpha$ upon reading a a (weight 1),
- we add 1-weighted self-loops around state 3 of $\mathcal{A}_\alpha$ labeled by $A \cup \{a, b\}$.

Denote by $\mathcal{C}_\mathcal{A}$ the resulting automaton. Then, one can check that (3.3) holds. For instance, if there exists y such that $\alpha = \|\mathcal{A}\|(y) > 1/2$, then we consider the word $u = (aya)^{n_1} b \cdots (aya)^{n_k} b$, and we observe that $\|\mathcal{C}_\mathcal{A}\|(u) = \|\mathcal{C}_\alpha\|(a^{n_1} b \cdots a^{n_k} b)$, so by (3.2) $\mathcal{C}_\mathcal{A}$ has value 1. If on the contrary $\|\mathcal{A}\| \leqslant 1/2$, it is easy to check that $\|\mathcal{C}_\mathcal{A}\| \leqslant 1/2$, as in the case of $\mathcal{C}_\alpha$. This proves (3.3) and concludes the proof. ∎

4. Decidability of the Equality Problem

The equality problem is the (In)Equality problem when $\bowtie$ is the equality. We have already seen that the Threshold emptiness problem is undecidable (does there exists w accepted with probability at least 1/2? exactly 1/2?), and it follows that the Existential (In)Equality problem is also undecidable. We will show the following result:

Theorem 3.20 (Schützenberger [Sch61], Tzeng[Tze92]). *Given two probabilistic automata with rational coefficients $\mathcal{A}_i = (Q_i, A, \lambda_i, \mu_i, \gamma_i)$, one can decide in time $O(|A|(|Q_1|+|Q_2|)^4)$ whether $\|\mathcal{A}_1\| = \|\mathcal{A}_2\|$.*

Proof. The decidability follows from a more general result from Schützenberger [Sch61], who proved that on a field (be it commutative or skew), one can decide whether a given recognizable series is null. This result in turn relies on a notion of rank, which can be thought as the minimal number of states necessary to implement the series, and which is computable in cubic time wrt. the automaton representation. Only for the null series, the rank is zero, and deciding Equality between $\mathcal{A}$ and $\mathcal{B}$ is reduced to checking if $\|\mathcal{A}\| - \|\mathcal{B}\|$ is null. The result has been rediscovered by Tzeng [Tze92] which presents a simple procedure.

First, the question reduces to $\|\mathcal{A}\| = 0$, for the weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ on $(\mathbb{Q}, +, \cdot, 0, 1)$ given by $Q = Q_1 \uplus Q_2$,

$$\lambda = (\lambda_1, \lambda_2), \quad \mu(a) = \begin{pmatrix} \mu_1(a) & 0 \\ 0 & \mu_2(a) \end{pmatrix}, \quad \text{and} \gamma = \begin{pmatrix} \gamma_1 \\ -\gamma_2 \end{pmatrix}.$$

Note that $\mathcal{A}$ is not a probabilistic automaton: γ may have negative coefficients, so we work on $\mathbb{Q}$ rather than on $\mathbb{Q}_{\geqslant 0}$.

So let $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be such a weighted automaton on the field $\mathbb{Q}$. Let $n = |Q|$. Then $\|\mathcal{A}\| = 0$ if and only if $\lambda\mu(w)\gamma = 0$ for all $w \in A^*$. Since the set of line vectors $V = \{\eta \in \mathbb{Q}^n \mid \eta\gamma = 0\}$ is subspace of the vector space $\mathbb{Q}^n$ over $\mathbb{Q}$, it suffices to show that one can compute a basis B of the vector space on $\mathbb{Q}$ generated by $\{\lambda\mu(w) \mid w \in A^*\}$: indeed, $\|\mathcal{A}\| = 0$ if and only if $B \subseteq V$.

To compute such a basis B, we compute $\{\lambda\mu(w) \mid w \in A^*\}$ for w in increasing hierarchical ordering $\preccurlyeq$. Assume $\lambda\mu(w)$ is a linear combination of vectors of the basis computed so far, say $\lambda\mu(w) = \sum \alpha_i.\lambda\mu(w_i)$ ($\alpha_i \in \mathbb{Q}$) for words $w_i \prec w$. Then for all $u \in A^*$, the vector $\lambda\mu(wu) = \sum \alpha_i.\lambda\mu(w_i u)$ is also a linear combination of vectors obtained for smaller words $w_i u \prec wu$. Therefore, one can safely ignore the contribution to B of all words of wA^*.

This justifies the algorithm computing B, where we mark a word w if $\lambda\mu(w)$ is a linear combination of vectors currently in B:

- Start with $B = \varnothing$, and all words of A^* initially unmarked.
- While $W = \{w \in A^* \mid \text{no prefix of } w \text{ is marked}\}$ is nonempty
  - Pick $w = \min_{\preccurlyeq} W$.
  - If w is a linear combination of vectors of B, then mark w. Otherwise, add w to B.
- Return B.

Since we work in a vector space of dimension n, the algorithm can add at most n vectors to the basis, so it terminates. The $O(|A|n^4)$ complexity comes from the fact that testing if a vector is a linear combination of vectors in B can be done in $O(n^3)$, see [Cor+09, Chap. 31]. ∎

Exercises for Chapter 3

Exercise 3.1. Prove Lemma 3.4.

Exercise 3.2. Consider the probabilistic automaton $\mathcal{A}$ from Example 3.2. Determine the (finite) class $\mathscr{L} = \{L_{>\theta}(\mathcal{A}) \mid \theta \in [0, 1]\}$.

Exercise 3.3. Prove Theorem 3.6. (Hint: probabilistic automata with one positive entry in every row of a transition matrix are deterministic finite automata.)

Exercise 3.4. Let $\mathcal{A}$ be a probabilistic automaton and $\theta \in [0, 1]$ be an isolated cut point of $\mathcal{A}$. Recall that $L_{>\theta}(\mathcal{A})$ is regular (Theorem 3.11). Determine an upper bound on the number of states of a finite automaton recognizing $L_{>\theta}(\mathcal{A})$.

Exercise 3.5. Prove Corollaries 3.15 and 3.18.

Exercise 3.6. Is the value 0 problem decidable?

Exercise 3.7. Show that the two following problems are undecidable:

- Input: A nondeterministic finite automaton.
- Problem 1: Does there exist a word having more accepting runs than rejecting runs?
- Problem 2: Does there exist a word whose ratio accepting runs/rejecting runs is arbitrarily close to 1?

Exercise 3.8. Is the Inequality problem decidable for probabilistic automata when $\bowtie = >$?

Further reading and references

[BBG08] Ch. Baier, N. Bertrand, and M. Größer. "On Decision Problems for Probabilistic Büchi Automata". In: *Proc. of FoSSaCS'08*. Vol. 4962. Lect. Notes Comp. Sci. Springer, 2008, pp. 287–301 (cit. on p. 14).

[BC08] V.D. Blondel and V. Canterini. "Undecidable problems for probabilistic automata of fixed dimension". In: *Theory of Computing systems* 36.3 (2008), pp. 231–245 (cit. on pp. 15, 17).

[BMT09] A. Bertoni, G. Mauri, and M. Torelli. "Some Recursively Unsolvable Problems Relating to Isolated Cutpoints in Probabilistic Automata." In: *Proc. of ICALP'77*. Vol. 52. Lect. Notes Comp. Sci. Springer, Sept. 19, 2009, pp. 87–94. ISBN: 3-540-08342-1. URL: http://dblp.uni-trier.de/db/conf/icalp/icalp77.html#BertoniMT77 (cit. on pp. 17–18).

[Cor+09] Th. H. Cormen et al. *Introduction to Algorithms*. 3rd. McGraw-Hill Higher Education, 2009 (cit. on p. 20).

[Gim10] Y. Gimbert H.and Oualhadj. "Probabilistic Automata on Finite Words: Decidable and Undecidable Problems". In: *Proc. of ICALP'10*. Vol. 6199. Lect. Notes Comp. Sci. Springer, 2010, pp. 527–538. URL: http://hal.archives-ouvertes.fr/hal-00456538/en/ (cit. on pp. 15–16, 18).

[MHC03] O. Madani, S. Hanks, and A. Condon. "On the undecidability of probabilistic planning and related stochastic optimization problems". In: *Artificial Intelligence* 147.1-2 (2003), pp. 5–34 (cit. on pp. 15–16).

[Paz71] A. Paz. *Introduction to probabilistic automata*. Academic Press, 1971 (cit. on p. 15).

[Put94] M. L. Puterman. *Markov Decision Processes*. New York, NY: John Wiley & Sons, Inc., 1994 (cit. on p. 11).

[Rab63] M. O. Rabin. "Probabilistic automata". In: *Information and Control* 6 (3 1963), pp. 230–245 (cit. on pp. 11, 13–14).

[Sch61] M.-P Schützenberger. "On the definition of a family of automata". In: *Information and Control* 4 (1961), pp. 245–270 (cit. on p. 19).

[Seg06] R. Segala. "Probability and Nondeterminism in Operational Models of Concurrency". In: *Proceedings of CONCUR'06*. Vol. 4137. Lect. Notes Comp. Sci. Springer, 2006, pp. 64–78 (cit. on p. 11).

[Tze92] W.G. Tzeng. "A polynomial-time algorithm for the equivalence of probabilistic automata". In: *SIAM J. Comput.* 21 (1992), pp. 216–227 (cit. on p. 19).

CHAPTER 4

Weighted Automata and Recognizable Series: General Results

The aim of this chapter is to present the Kleene-Schützenberger's theorem for formal power series. It states that recognizable series (*i.e.*, series which are the semantics of a weighted automaton) are exactly the rational series (series built from letters and scalars using finitely many times basic operations, like sum, product or star). As in the Boolean case, the proof is effective. We just give an outline here. For additional details, the reader is referred to [BR11] (which we follow here, adopting the same notation), or to [Sak09; DKV09].

1. Rational Series

Recall that a (formal power) series over a semiring $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ is a mapping from A^* into S. The set of formal power series over $\mathbb{S}$ is denoted $\mathbb{S}\langle\langle A^* \rangle\rangle$. For $f \in \mathbb{S}\langle\langle A^* \rangle\rangle$ and $w \in A^*$, we frequently write $\langle f, w\rangle$ instead of $f(w)$. We call $\langle f, w\rangle$ the *coefficient* of f on w.

We first define rational series. The *rational operations* are the sum, the product and the star. The sum is just defined pointwise: for $f, g \in \mathbb{S}\langle\langle A^* \rangle\rangle$,

$$\langle f + g, w\rangle = \langle f, w\rangle + \langle g, w\rangle.$$

The product is the *Cauchy product*, defined by

$$\langle fg, w\rangle = \sum_{w=uv} \langle f, u\rangle\langle g, v\rangle.$$

Note that the sum is finite since there is a finite number of factorizations of a word w, in the free monoid.

We also consider left and right multiplication by scalars: if $s \in S$ and $f \in \mathbb{S}\langle\langle A^* \rangle\rangle$, then $s.f$ (resp. $f.s$) is the series defined by $\langle s.f, w\rangle = s.\langle f, w\rangle$ (resp. $\langle f.s, w\rangle = \langle f, w\rangle.s$).

To define the star operation, we need to be able to sum infinitely many series, with the intention to define f^* as $\sum_{n \geqslant 0} f^n$. For this, we endow $\mathbb{S}\langle\langle A^* \rangle\rangle$ with a topology. The *distance* $d(f, g)$ of two series f, g is defined by

$$\begin{cases} d(f,g) & = 2^{-r(f,g)}, \text{ where } 2^{-\infty} = 0, \text{ and} \\ r(f,g) & = \inf\{|w| \mid w \in A^* \text{ and } \langle f, w\rangle \neq \langle g, w\rangle\} \in \mathbb{N} \cup \{\infty\}. \end{cases}$$

That is, two series are close if they cannot be distinguished by small words. It is easy to see that d is a distance on $\mathbb{S}\langle\langle A^* \rangle\rangle$ (actually, an ultrametric distance).

Definition 4.1 (Support, polynomial). The *support* of a formal power series f is

$$\mathrm{Supp}(f) = \big\{w \in A^* \mid \langle f, w\rangle \neq \mathbb{0}\big\}.$$

A *polynomial* is a series having finite support. The set of polynomials is denoted $\mathbb{S}\langle A^* \rangle$. ■

Let $f \in \mathbb{S}\langle\langle A^* \rangle\rangle$ and let $P_n = \sum_{|w| \leqslant n} \langle f, w\rangle.w$. Clearly, P_n is a polynomial which coincides with f on all words of length n or less. Therefore, the sequence $(P_n)_n$ converges to f, which shows that $\mathbb{S}\langle A^* \rangle$ is dense in $\mathbb{S}\langle\langle A^* \rangle\rangle$.

We say that a family $(f_k)_{k \in K}$ is *summable* if there is a series f such that, for every $\varepsilon > 0$, there exists a *finite* set of indices $I \subseteq K$ such that, whenever $J \supseteq I$, we have $d(\sum_{j \in J} f_j, f) < \varepsilon$. The series f is then obviously unique, and we write $f = \sum_{k \in K} f_k$. A family $(f_k)_{k \in K}$ is *locally finite* if for each $w \in A^*$, there is only a finite number of indices k such that $\langle f_k, w\rangle \neq \mathbb{0}$. In this case, the family is also clearly summable, and $\langle f, w\rangle$ is actually the finite sum of all non-null values $\langle f_k, w\rangle$.

An example of a locally finite family is the following. Denote by w the series which maps w to $\mathbb{1}$ and all other words to $\mathbb{0}$. Let $(f_w)_{w\in A^*}$ be a sequence of elements of $\mathbb{S}$. Then the family $f_w.w$ is locally finite (since all the series $f_v.v$ for $v \neq w$ have a zero value on w). Let $f = \sum_{w\in A^*} f_w.w$. Then $\langle f, w\rangle = f_w$. In other words, $f = \sum_{w\in A^*} \langle f, w\rangle.w$.

There is another important example of a summable family. A series f is said *proper* if $\langle f, \varepsilon\rangle = \mathbb{0}$. In this case, by definition of the Cauchy product, $\langle f^n, w\rangle = 0$ if $|w| < n$, and therefore $(f^n)_{n\in\mathbb{N}}$ is locally finite, hence summable. For a proper series f, one denotes by f^* the following series:

$$f^* = \sum_{n\geqslant 0} f^n.$$

where $\mathbb{1}$ denotes the series mapping $\varepsilon \in A^*$ to $\mathbb{1} \in \mathbb{S}$ and nonempty words to $\mathbb{0}$ (*i.e.*, $\mathbb{1} = \varepsilon$ with the above notation, that is, $\mathbb{1}$ is the neutral element for the multiplication of $\mathbb{S}\langle\langle A^*\rangle\rangle$). We check that

$$f^* = ff^* + \mathbb{1} = f^*f + \mathbb{1}. \tag{4.1}$$

We then define the set of rational series $\mathbb{S}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle$ as the smaller subset of $\mathbb{S}\langle\langle A^*\rangle\rangle$ containing polynomials, and closed under addition, Cauchy product, left and right scalar multiplication, and star (applied to *proper* series only).

2. Recognizable Series

Recognizable series are simply series realized by a weighted automaton. That is, a series is recognizable if there exist $n \geqslant 0$ and a representation (λ, μ, γ), with $\lambda \in S^{1\times n}$, $\mu \in S^{n\times n}$ and $\gamma \in S^{n\times 1}$ such that for all word $w \in A^*$, we have $f(w) = \lambda\mu(w)\gamma$. The set of all recognizable series over alphabet A and semiring $\mathbb{S}$ is denoted by $\mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$.

The main result of this chapter is that recognizable and rational series coincide. A first step in this direction is to show stability of $\mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$ by rational operations. A first observation is the following.

Lemma 4.2. *$\mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$ is stable under taking linear combinations (*i.e.*, under the operations $f \mapsto s.f$, $f \mapsto f.s$, $(f, g) \mapsto f + g$).*

Proof. Exercise. ∎

We shall now state a result analogous to the fact that, in the Boolean semiring, a recognizable language only has a finite number of residuals. We first need to define residuals. For $f \in \mathbb{S}\langle\langle A^*\rangle\rangle$ and $w \in A^*$, we let $w^{-1}f$ be the formal power series defined by

$$\forall v \in A^* \quad \langle w^{-1}f, v\rangle = \langle f, wv\rangle.$$

It is easy to see that a recognizable series has in general an infinite number of residuals.

Lemma 4.3. *Let $f \in \mathbb{S}\langle\langle A^*\rangle\rangle$ and $w \in A^*$. We have:*

1. *If $f \in \mathbb{S}\langle A^*\rangle$, then $w^{-1}f \in \mathbb{S}\langle A^*\rangle$*
2. *If $f \in \mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$, then $w^{-1}f \in \mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$.*

Proof. Exercise. ∎

We need the notion of left $\mathbb{S}$-module, analogous to that of vector spaces when $\mathbb{S}$ is a field. We say that M is a *left $\mathbb{S}$-module* if it is endowed with an internal law $+$ making it a commutative monoid (neutral element denoted by 0), and if we have a left action from $S \times M$ into M, denoted $(s, w) \mapsto sw$, satisfying

$$\begin{aligned} s(m_1 + m_2) &= sm_1 + sm_2 & \mathbb{1}m &= m \\ (s_1 + s_2)m &= s_1m + s_2m & \mathbb{0}m &= 0 \\ s_1(s_2m) &= (s_1s_2)m & s0 &= 0 \end{aligned}$$

for all $s, s_1, s_2 \in S$ and $m, m_1, m_2 \in M$. A *submodule* of M is a subset of M containing 0 and stable by addition and left action. For instance, $\mathbb{S}\langle\langle A^*\rangle\rangle$ is a left $\mathbb{S}$-module (with the addition of series as addition, and the left scalar product as left action), and $\mathbb{S}\langle A^*\rangle$ is a submodule of $\mathbb{S}\langle\langle A^*\rangle\rangle$.

A submodule M of $\mathbb{S}\langle\langle A^*\rangle\rangle$ is *finitely generated* if there exist series $f_1, \ldots, f_n$ such that $M = \{\alpha_1 f_1 + \cdots + \alpha_n f_n \mid \alpha_i \in S\}$. It is called *stable* if, whenever f belongs to M, then so do all its residuals $w^{-1}f$.

For instance, the set $\mathbb{S}\langle A^*\rangle$ of polynomials is stable (by Lemma 4.3), but clearly not finitely generated. The same holds for $\mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$ by Lemma 4.3.

The characterization of recognizable series is then the following:

PROPOSITION 4.4. A series $f \in \mathbb{S}\langle\langle A^*\rangle\rangle$ is recognizable if and only if it belongs to some stable finitely generated submodule of $\mathbb{S}\langle\langle A^*\rangle\rangle$.

PROOF SKETCH. If f is recognizable, say with a representation (λ, μ, γ), then $f = \sum_{i=1}^n \lambda_i f_i$ where $f_i = (\mu\gamma)_i$. The submodule $\left\{\sum_{i=1}^n s_i f_i \mid s_i \in S\right\}$ is obviously finitely generated and contains f. It just remains to check that it is stable (left as an exercise).

Conversely, if $f = \sum_{i=1}^n \lambda_i f_i$ where $\left\{\sum_{i=1}^n s_i f_i \mid s_i \in S\right\}$ is stable, then by definition of stability, there are coefficients $\mu_{a,i,j}$ such that for every $a \in A$, we have $a^{-1}f_i = \sum_{j=1}^n \mu_{a,i,j} f_j$. Set $\mu(a)_{i,j} = \mu_{a,i,j}$ and $\gamma_i = \langle f_i, \varepsilon\rangle$, and check that (λ, μ, γ) is indeed a representation of f.

See [BR11] for details. ∎

The *Hadamard product* of two formal power series f and g is the pointwise multiplication of series, that is, the series $f \odot g$ defined by $f \odot g(w) = f(w)g(w)$ for all $w \in A^*$.

COROLLARY 4.5. *If $\mathbb{S}$ is commutative and if f and g are recognizable, then so is $f \odot g$.*

PROOF. Exercise. ∎

We now prove that $\mathbb{S}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle \subseteq \mathbb{S}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle$.

LEMMA 4.6. *For all $f, g \in \mathbb{S}\langle\langle A^*\rangle\rangle$ and $a \in A$, we have*

$$a^{-1}(fg) = \langle f, \varepsilon\rangle(a^{-1}g) + (a^{-1}f)g.$$

Moreover, if f is proper, then

$$a^{-1}(f^*) = (a^{-1}f)f^*.$$

PROOF. We have for $w \in A^*$

$$\langle a^{-1}(fg), w\rangle = \langle fg, aw\rangle = \sum_{uv=aw} \langle f, u\rangle.\langle g, v\rangle = \langle f, \varepsilon\rangle\langle a^{-1}g, w\rangle + \langle a^{-1}f, w\rangle\langle g, w\rangle$$

(last equality by isolating the first term of the sum.)

For the other equality, we use $f^* = ff^* + \mathbb{1}$. We have $a^{-1}f^* = a^{-1}(ff^*) + a^{-1}\mathbb{1} = a^{-1}f.f^*$, using the first statement, and since $\langle f, \varepsilon\rangle = \mathbb{0}$ by hypothesis. ∎

COROLLARY 4.7. *We have $\mathbb{S}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle \subseteq \mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$.*

PROOF. Clearly, the series $\mathbb{1}$ and a, for $a \in A$, are recognizable. Therefore, by Lemma 4.2, $\mathbb{S}\langle A^*\rangle \subseteq \mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$. It remains to show that $\mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$ is closed under rational operations. The cases of addition and scalar multiplication are given by Lemma 4.2. Assume that f, g are recognizable. We show that so are fg and f^* using the characterization of Proposition 4.4 and Lemma 4.6.

Let $M = \left\{\sum_{i=1}^n s_i f_i \mid s_i \in S\right\}$ and $N = \left\{\sum_{i=1}^m t_i g_i \mid t_i \in S\right\}$ be stable submodules of $\mathbb{S}\langle\langle A^*\rangle\rangle$ containing f and g, respectively. Then, $Mg + N$ is generated by $\{f_1 g, \ldots, f_n g, g_1, \ldots, g_n\}$, so it is finitely generated. It obviously contains fg. It remains to show that it is stable. We have $a^{-1}(f_i g) = a^{-1}f_i.g + \langle f_i, \varepsilon\rangle.a^{-1}g \in Mg + N$ by stability of M and N. By linearity of $h \mapsto a^{-1}h$ we conclude that $Mg + N$ is stable, as required.

Similarly, one shows that, if f is proper, we check that $Mf^* + S$ is a finitely generated stable submodule containing f^*. ∎

We now show that $\mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle \subseteq \mathbb{S}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle$. We consider elements of $\mathbb{S}\langle\langle A^*\rangle\rangle^{n\times n}$, that is, matrices whose elements are series over $\mathbb{S}$. We say that such a matrix is *proper* if so are all its coefficients. In this case one can consider $\bar{\mu}^* = \sum_{k\geqslant 0} \bar{\mu}^k$.

LEMMA 4.8. *Let $\bar{\mu}$ be a proper matrix of $\mathbb{S}\langle\langle A^*\rangle\rangle^{n\times n}$. The coefficients of $\bar{\mu}^*$ are in the rational closure of the coefficients of $\bar{\mu}$. In particular, if $\bar{\mu}$ has rational series as coefficients, so has $\bar{\mu}^*$.*

PROOF SKETCH. By induction on the dimension n of $\bar{\mu}$. For $n > 1$, one uses a block decomposition of $\bar{\mu}$ and $\bar{\mu}^*$ in 4 blocks, and the identity $\mu^* = \mathbb{1} + \mu\mu^*$ yields relations between the blocks of $\bar{\mu}$ and those of $\bar{\mu}^*$. These relations are linear, *i.e.*, of the form $\phi = \alpha\phi + \beta$ for α proper. A simple topological argument shows that this equation in ϕ has a unique solution $\alpha^*\beta$. This makes it possible to solve the linear relations obtained considering the blocks of $\bar{\mu}^*$ as unknowns, and to show that they are in the rational closure of the blocks of $\bar{\mu}$. ∎

PROPOSITION 4.9. We have $\mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle \subseteq \mathbb{S}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle$.

PROOF. Let $f \in \mathbb{S}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$ and let (λ, μ, γ), be a representation of f.

Let $\bar{\mu} = \sum_{a\in A} \mu(a).a \in \mathbb{S}^{n\times n}\langle\langle A^*\rangle\rangle$, The series $\bar{\mu}$ maps $A^*\setminus A$ on the zero element of $\mathbb{S}^{n\times n}$. In particular it is proper. Applying the definition of the star operation, we obtain $\bar{\mu}^* = \sum_{w\in A^*} \mu w.w$. Viewing matrices of $\mathbb{S}^{n\times n}\langle\langle A^*\rangle\rangle$ as elements of $\mathbb{S}\langle\langle A^*\rangle\rangle^{n\times n}$, we have $\bar{\mu}^*_{i,j} = \sum_{w\in A^*}(\mu w)_{i,j}.w$, and therefore, $f = \sum \lambda_i \mu^*_{i,j} \gamma_j$. Moreover, $\bar{\mu}^*_{i,j}$ is rational by Lemma 4.8, hence so is f. ∎

From Corollary 4.7 and Proposition 4.9, one deduces the Kleene-Schützenberger's theorem.

THEOREM 4.10. *A formal power series is recognizable if and only if it is rational.*

Given a language $L \subseteq A$, its *characteristic series*, denoted $\underline{L}$, is defined by

$$\langle \underline{L}, w\rangle = \begin{cases} \mathbb{1} & \text{if } w \in L \\ \mathbb{0} & \text{otherwise.} \end{cases}$$

As an application of Theorem 4.10, let us show the following useful statement.

PROPOSITION 4.11. The characteristic series of a regular language is effectively recognizable.

PROOF. Since $L \subseteq A^*$ is regular, there is a finite monoid M and a morphism $\varphi : A^* \to M$ such that $L = \varphi^{-1}(P)$ for $P = \varphi(L)$ (by Kleene's theorem). Consider the right representation of M, that is, the mapping $\rho : M \to S^{M\times M}$ defined by $\rho(m)_{s.t} = \begin{cases} \mathbb{1} & \text{if } sm = t \\ \mathbb{0} & \text{otherwise.} \end{cases}$ It is easy to check that ρ is a morphism: $\big(\rho(m_1)\rho(m_2)\big)_{s,t} = \sum_{r\in M} \rho(m_1)_{s,r}\rho(m_2)_{r,t}$, and $\rho(m_1)_{s,r}\rho(m_2)_{r,t} = \mathbb{1}$ only if $sm_1 = r$ and $rm_2 = t$, which gives $\big(\rho(m_1)\rho(m_2)\big)_{s,t} = \mathbb{1}$ if $t = sm_1m_2$ and $\mathbb{0}$ otherwise.

Therefore, $\mu : A^* \to S^{M\times M}$ defined by $\mu(w) = \rho(\varphi(w))$ is a morphism. Let $\lambda \in S^M$ be the row vector defined by $\lambda_m = \mathbb{1}$ if $m = 1$ and $\lambda_m = \mathbb{0}$ otherwise, and let $\gamma \in S^M$ be the column vector defined by $\gamma_m = \mathbb{1}$ if $m \in P$ and $\gamma_m = \mathbb{0}$ otherwise. Then (λ, μ, γ) is a representation of $\underline{L}$. ∎

Exercises for Chapter 4

EXERCISE 4.1. Show that $\mathbb{S}\langle\langle A^*\rangle\rangle$ is the topological completion of $\mathbb{S}\langle A^*\rangle$.

EXERCISE 4.2. Prove Lemma 4.3.

EXERCISE 4.3. Let $\mathbb{S}$ be a ring.

1. Show that a series $f \in \mathbb{S}\langle\langle A^*\rangle\rangle$ is invertible iff. $\langle f, \varepsilon\rangle$ is invertible in $\mathbb{S}$. What is then its inverse?
2. On the semiring $\mathbb{N}\mathrm{at}$ with $A = \{a\}$, compute $\langle f, a^n\rangle$, $n \geqslant 0$, for the series $f = (a + aa)^*$.
3. Show that if $|A| = 1$ and $\mathbb{S}$ is a commutative, rational series are exactly the series expansion of fractions P/Q, where $P, Q \in \mathbb{S}\langle\langle\{a\}^*\rangle\rangle$ are polynomials in one variable, and $Q(0)$ is invertible.
4. What are the polynomials corresponding to the series f of question 2 (considering $f \in \mathbb{Z}\langle\langle\{a\}^*\rangle\rangle$)?

EXERCISE 4.4. Prove Corollary 4.5. Is it still true when $\mathbb{S}$ is not commutative?

EXERCISE 4.5. For $n \in \mathbb{N}$, we still write n the element $\underbrace{\mathbb{1} + \mathbb{1} + \cdots + \mathbb{1}}_{n \text{ times}}$ of S.

1. Show that the series f defined by $\langle f, w\rangle = |w|_a$ is rational (where $|w|_a$ denotes the number of a's in the word w) by providing a rational expression.
2. Let $A = \sum_{a\in A} a$. Show that the series A^* is the constant series mapping every word to $\mathbb{1}$.

EXERCISE 4.6. Give a matrix representation of the series $\langle f, w\rangle = |w|_a$ defined in Exercise 4.5.

EXERCISE 4.7. 1. We know from Chapter 3 that the formal power series $\{0,1\}^* \to \mathbb{R}_{\geqslant 0}$ which associates to the word w the value $\overline{w}$ (defined page 13) is recognizable on $\mathbb{R}_{\geqslant 0}$. Reprove this result using Proposition 4.4.

2. Show that the series in $\mathbb{N}\mathrm{at}\langle\langle\{0,1\}^*\rangle\rangle$ which maps ε to 0 and $w \in \{0,1\}^+$ to the integer whose binary representation is w is recognizable.

EXERCISE 4.8. Show that for $\mathbb{S}$ commutative, every mapping $\varphi : A \to S\langle\langle B^*\rangle\rangle$ such that $\varphi(a)$ is a proper rational series uniquely extends to a continuous semiring morphism $\varphi : S\langle\langle A^*\rangle\rangle \to S\langle\langle B^*\rangle\rangle$ inducing the identity on S. Show that the image of a rational series by this morphism is rational.

Further reading and references

[BR11] J. Berstel and Ch. Reutenauer. *Noncommutative rational series with applications*. Vol. 137. Encyclopedia of Mathematics and Its Applications. Preliminary version at http://tagh.de/tom/wp-content/uploads/berstelreutenauer2008.pdf. Cambridge University Press, 2011 (cit. on pp. 23, 25).

[DKV09] M. Droste, W. Kuich, and W. Vogler. *Handbook of Weighted Automata*. Springer, 2009 (cit. on p. 23).

[KS85] W. Kuich and A. Salomaa. *Semirings, Automata and Languages*. Springer, 1985.

[Sak09] J. Sakarovitch. *Elements of Automata Theory*. New York, NY, USA: Cambridge University Press, 2009. ISBN: 0521844258, 9780521844253 (cit. on p. 23).

[SS78] A. Salomaa and M. Soittola. *Automata-theoretic aspects of formal power series*. Springer, 1978.

CHAPTER 5

Series over Semirings of Integers

In this chapter, we review some decidability and undecidability results for series over the following semirings:

- $\mathbb{N}\mathrm{at} = (\mathbb{N}, +, \cdot, 0, 1)$ the semiring of natural numbers,
- $\mathbb{Z} = (\mathbb{Z}, +, \cdot, 0, 1)$, the semiring of integers,
- $\mathbb{T}\mathrm{rop} = (\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$, called the tropical semiring,
- $\mathbb{T}\mathrm{rop}_{\mathbb{Z}} = (\mathbb{Z} \cup \{\infty\}, \min, +, \infty, 0)$.

In particular, we look at the (In)equality problems.

1. Semirings $\mathbb{Z}$ and $\mathbb{N}$at

We begin by a decidability result, which actually has already been proved.

Theorem 5.1. *The* Equality *problem over* $\mathbb{N}$at *and* $\mathbb{Z}$ *is decidable. That is, it is decidable whether two rational formal power series are equal.*

The proof is the same as for probabilistic automata (Theorem 3.20), embedding $\mathbb{N}$at or $\mathbb{Z}$ into the field $\mathbb{Q}$.

For other problems over $\mathbb{Z}$, the situation is often undecidability. The first easy observation is that over the semiring $\mathbb{Z}$, one can encode usual polynomials (*i.e.*, in commutative variables) with coefficients in $\mathbb{Z}$.

Lemma 5.2. *Let* $P \in \mathbb{Z}[X_1, \ldots, X_n]$ *be a polynomial over* $\mathbb{Z}$. *Then there exists a recognizable series* f *over* $\mathbb{Z}$ *and over* $A = \{a_1, \ldots, a_n\}$ *such that* $f(w) = P(|w|_{a_1}, \ldots, |w|_{a_n})$.

Proof. Exercise. ∎

Due to Lemma 5.2, it is natural to encode Hilbert's 10th problem, which we recall:

Input	A polynomial $P \in \mathbb{Z}[X_1, \ldots, X_n]$.
Problem	Does there exist positive integers $k_1, \ldots, k_n$ such that $P(k_1, \ldots, k_n) = 0$?

This problem is undecidable [Mat93; DMR76]. Using Lemma 5.2, one can reduce Hilbert's 10th problem reduces to several problems for rational formal power series in $\mathbb{Z}$, listed in Theorem 5.3. See for instance [SS78; KS85] (or go to Exercise 5.1!). Note that the PCP is also adapted and provides simple proofs, too (see Exercise 5.1). The advantage in reducing from the PCP is not to depend on the very difficult result of [Mat93; DMR76].

Theorem 5.3. *Assume that* $|A| \geqslant 2$. *Given a rational series* $f \in \mathbb{Z}^{\mathrm{Rat}}\langle\langle A^* \rangle\rangle$, *it is undecidable whether* f

(a) *has a zero coefficient,*
(b) *has infinitely many zero coefficients,*
(c) *has a positive coefficient,*
(d) *has infinitely many positive coefficients,*
(e) *is one-to-one,*
(f) *has only a finite number of nonnegative values.*

Proof. Exercise. Hint: by reduction from Hilbert's 10th problem, or from the Post correspondence problem, which is also well-suited. Note that if the alphabet is fixed (not part of the input), then one cannot directly apply Lemma 5.2, which uses an unbounded alphabet. However, given $P \in \mathbb{Z}[X_1, \ldots, X_n]$, one can use instead of $P(|w|_{a_1}, \ldots, |w|_{a_n})$ the series mapping the word $a^{n_1}b \cdots a^{n_k}b$ to $P(n_1, \ldots, n_k)$, and words outside of $a^*b \cdots a^*b$ to some constant $k \in \mathbb{Z}$. This series is indeed recognizable over $\mathbb{Z}$. ∎

On the other hand, it is decidable whether a rational series has infinitely many *nonzero* coefficients.

THEOREM 5.4. *Given a series $f \in \mathbb{Z}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle$, it is decidable whether $f \in \mathbb{Z}\langle A^*\rangle$.*

PROOF. Exercise. Hint: first prove the result for $|A| = 1$ using Exercise 4.3. ∎

2. The Tropical Semiring

Weighted automata over $\mathbb{T}\mathrm{rop} = (\mathbb{N} \cup \{\infty\}, \min, +, \infty, 0)$ have a nice interpretation: weights can be viewed as costs that we have to pay on a path, when traveling along the transitions of the automaton. Thanks to the min operation, the semantics on a word w computes the cheapest cost for w.

An easy application of this semiring in the theory of formal languages is the finite power property: given a regular language L, is there some integer $n \geqslant 0$ such that $L^* = L^n$? This question easily reduces to the so-called *limitedness problem*, which asks whether a rational series over $\mathbb{T}\mathrm{rop}$ is bounded. It turns out that this problem is decidable (PSPACE-complete, see [LP04]). The tropical semiring has actually been considered by I. Simon to solve the star-height problem [Sim94]. The simplest solution to this nontrivial problem requires additional algebraic tools. Many extensions have also been considered, see for instance [Kir05].

However, in contrast to the limitedness problem, several variants of the (IN)EQUALITY or EXISTENTIAL (IN)EQUALITY problems are undecidable [Kro94]. We consider for technical reasons the semiring $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$, and we show the following results. The reduction presented in [Kro94] is from Hilbert's 10^{th} problem. We present a proof reducing the HALTING problem of 2-counter machines to these problems, first in $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$, then in $\mathbb{T}\mathrm{rop}$. This proof is due to Th. Colcombet (unpublished).

THEOREM 5.5. *Let A be an alphabet with at least two letters. Then the* (IN)EQUALITY *problems, as well as the* EXISTENTIAL (IN)EQUALITY *problems are all undecidable for rational formal power series in $\mathbb{T}\mathrm{rop}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle$ or $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}^{\mathrm{Rat}}\langle\langle A^*\rangle\rangle$.*

PROOF. The proof is in two steps.

(*i*) We reduce the HALTING problem of 2-counter machines to the INEQUALITY problem over $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$.
(*ii*) We reduce the INEQUALITY problem over $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$ to all other problems.

When working in $\mathbb{T}\mathrm{rop}$ or $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$, we use min and $+$ with their usual meaning, and we write $\oplus$ and $\otimes$, respectively, to emphasize the semiring operations. That is, $\oplus$ stands for min and $\otimes$ stands for $+$. Recall that the Hadamard product $\odot$ is the pointwise multiplication of series, that is, $f \odot g = f + g$. We freely use Kleene-Schützenberger's theorem (Theorem 4.10) and the fact that rational power series are stable under taking Hadamard product (Corollary 4.5), since we work on commutative semirings.

Let us first explain (*ii*). In the INEQUALITY problem, we consider the relation $\bowtie = \leqslant$. All choices in $\{<, \leqslant, >, \geqslant\}$ are in fact equivalent wrt. decidability on $\mathbb{T}\mathrm{rop}$ or $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$. To see this, note that for $f \in \mathbb{T}\mathrm{rop}^{\mathrm{Rec}}\langle\langle A^*\rangle\rangle$, the support

$$\mathrm{Supp}(f) = \{w \in A^* \mid \langle f, w\rangle = \infty\}$$

is effectively recognizable, since the function from $\mathbb{T}\mathrm{rop}$ to $\mathbb{B}\mathrm{ool}$ mapping ∞ to 0 and all other values to 1 is a morphism (so, starting from a weighted automaton for f over $\mathbb{T}\mathrm{rop}$, an automaton recognizing $\mathrm{Supp}(f)$ is obtained by replacing ∞ weights by 0, and other weights by 1). Then we have, for instance, $f < g$ if and only if $\mathrm{Supp}(f) = \varnothing$ and $f + 1 \leqslant g$, that is, $f \odot 1 \leqslant g$, where 1 is the constant (rational) series on $\mathbb{T}\mathrm{rop}$ or $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$. We deduce that the INEQUALITY problem for $<$ is decidable if and only if so is the INEQUALITY problem for $\leqslant$.

For $L \subseteq A^*$ and $f \in \mathbb{T}\mathrm{rop}_{(\mathbb{Z})}\langle\langle A^*\rangle\rangle$, let $f^L(w) = 0$ if $w \in L$ and $f^L(w) = f(w)$ if $w \notin L$. We have $f^L = \min(\underline{L}, f) = \underline{L} \oplus f$, so by Proposition 4.11, if L is regular and f recognizable, so is f^L.

For power series f, g over $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$ or $\mathbb{T}\mathrm{rop}$, we then have:

- $f \leqslant g$ if and only if $\min(f, g) = f$, that is, $f \oplus g = f$. This shows that INEQUALITY $\leqslant$ EQUALITY.
- $f \leqslant g$ if and only if $\mathrm{Supp}(f) \subseteq \mathrm{Supp}(g)$, and it not the case that for some w, $\langle g^L, w\rangle < \langle f^L, w\rangle$ with $L = \mathrm{Supp}(g)$. In case $\mathrm{Supp}(f) \subseteq \mathrm{Supp}(g)$, note that neither f^L nor g^L take ∞ values. Therefore, $\langle g^L, w\rangle < \langle f^L, w\rangle$ is equivalent to $\langle g^L \odot 1, w\rangle \leqslant \langle f^L, w\rangle$. This shows that INEQUALITY $\leqslant$ EXISTENTIAL INEQUALITY.

– $\langle f, w\rangle \leqslant \langle g, w\rangle$ holds for some w if and only if $\langle f \oplus g, w\rangle = \langle f, w\rangle$ holds for some w. This shows that Existential Inequality $\leqslant$ Existential Equality, and therefore Inequality $\leqslant$ Existential Equality by the above.

To conclude the proof of *(ii)*, it remains to prove that Inequality($\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$) $\leqslant$ Inequality($\mathbb{T}\mathrm{rop}$) — with an obvious notation. So let $f, g \in \mathbb{T}\mathrm{rop}_{\mathbb{Z}}\langle\langle A^*\rangle\rangle$ be given by their representations (λ, μ, γ) and (η, ν, δ), that one can assume to be of the same dimension n (adding unnecessary states to the smallest representation). We uniformly lift all entries of both matrices, in order to obtain series with nonnegative entries: let k be the smallest value appearing in these representations, and consider the series f_k, g_k having as representations $\big((\lambda_i + |k|)_i, (\mu_{i,j} + |k|)_{i,j}, (\gamma_j + |k|)_j\big)$ and $\big((\eta_i + |k|)_i, (\nu_{i,j} + |k|)_{i,j}, (\delta_j + |k|)_j\big)$. By construction, f_k and g_k are rational series over $\mathbb{T}\mathrm{rop}$ (all of their entries are in $\mathbb{N}$). Moreover, we compute $\langle f_k, w\rangle = \langle f, w\rangle + k(|w| + 2)$ and similarly $\langle g_k, w\rangle = \langle g, w\rangle + k(|w| + 2)$, whence $f \leqslant g$ if and only if $f_k \leqslant g_k$. This shows that Inequality($\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$) $\leqslant$ Inequality($\mathbb{T}\mathrm{rop}$).

It remains to prove *(i)*. We consider a 2-counter Minsky machine, consisting in a finite automaton (Q, q_0, q_f, Δ) where Q is a finite set of states, $q_0, q_f \in Q$ ($q_0 \neq q_f$), and $\Delta \subseteq Q \times \text{Guards} \times \text{Actions} \times Q$ is a finite set of transitions that handle two counters c_1 and c_2, each storing a natural integer. Intuitively, the machine has two kinds of instructions, *increment* and *test for decrement*, pictured in Fig. 5.1:

(*a*) Increment
$p : \{c_i{+}{+}\};$ goto q.

(*b*) Test for decrement
$p :$ if $c_i = 0$ goto q_2 else $(\{c_i{-}{-}\};$ goto $q_1)$.

Fig. 5.1. Transitions of a Minsky machine

Transitions are of the form $(p, [guard], \{action\}, q)$, where *guard* is a condition on counters that has to be fulfilled for the transition to be enabled, and *action* possibly modifies the counter values. A *configuration* of such a machine is a tuple $(q, n_1, n_2) \in Q \times \mathbb{N} \times \mathbb{N}$. Possible guards are

– $[true]$: transition is always enabled,
– $[c_i = 0]$: transition is enabled only if the value n_i of c_i in the current configuration is 0, and
– $[\neg(c_i = 0)]$: transition is enabled only if the value n_i of c_i in the current configuration is not 0.

Actions are either

– $\{c_i{+}{+}\}$: increment c_i, always guarded by $[true]$,
– $\{c_i{-}{-}\}$: decrement c_i, always guarded by $[\neg(c_i = 0)]$, or
– $\{\}$ no change in the counter values, always guarded by $[c_1 = 0]$ or $[c_2 = 0]$.

A computation of a 2-counter Minsky machine (Q, q_0, q_f, Δ) is a sequence of configurations $C_0, C_1, \ldots, C_n$ with $C_0 = (q_0, 0, 0)$, and such that the semantics of transitions in Δ is respected:

(1) $C_j = (p, n_1, n_2)$ and $C_{j+1} = (q, n_1 + 1, n_2)$ and $(p, [true], \{c_1{+}{+}\}, q) \in \Delta$. Idem for c_2.
(2) $C_j = (p, n_1 + 1, n_2)$, $C_{j+1} = (q, n_1, n_2)$ and $(p, [\neg(c_1 = 0)], \{c_1{-}{-}\}, q) \in \Delta$. Idem for c_2.
(3) $C_j = (p, n_1, n_2)$, $C_{j+1} = (q, n_1, n_2)$ and for some $i = 1, 2$, $n_i = 0$ and $(p, [c_i = 0], \{\}, q) \in \Delta$.

The following Halting problem for 2-counters Minsky machines is undecidable [Min67]:

Input	A 2-counter Minsky machine $\mathcal{M} = (Q, q_0, q_f, \Delta)$.
Problem	Is there a computation of $\mathcal{M}$ ending in $\{q_f\} \times \mathbb{N} \times \mathbb{N}$?

For *(i)*, we build from a 2-counter Minsky machine $\mathcal{M}$ a weighted automaton $\mathcal{A}_{\mathcal{M}}$ over $\mathbb{T}\mathrm{rop}_{\mathbb{Z}}$ such that

$$\mathcal{M} \text{ has no computation reaching } \{q_f\} \times \mathbb{N} \times \mathbb{N} \iff -1 \geqslant \|\mathcal{A}\|_{\mathcal{M}}.$$

The semantics of $\mathcal{A}_{\mathcal{M}}$ will be nonpositive. More precisely, it shall assign zero to words encoding computations of $\mathcal{M}$ that reach $\{q_f\} \times \mathbb{N} \times$, and negative values for all other words, which we call *incorrect*.

We encode computations of $\mathcal{M}$ as follows. Let $a, b \in \Delta$. For a configuration $C = (q,k,\ell)$, let $\tilde{C} = a^k b^\ell \in a^*b^*$. A computation $C_0, C_1, \ldots, C_n$ taking transitions $\delta_1, \delta_2, \ldots, \delta_{n-1}$ is encoded by the word $\tilde{C_0}\delta_0\tilde{C_1}\delta_1 \cdots \delta_{n-1}\tilde{C_n} \in (\Delta \cup \{a,b\})^*$. $\mathcal{A}_\mathcal{M}$ shall assign 0 to the words encoding a computation ending in q_f, and negative values to incorrect words. A word is incorrect if one of the following conditions holds:

Wrong shape: It is not in $a^*b^*(\Delta a^*b^*)^*$,
Not starting in $(q_0,0,0)$**:** Its first letter is not in $\bigcup_{g,a,q}(q_0,[g],\{a\},q)$,
Not ending in q_f**:** It does not have a suffix in $\bigcup_{g,a,q}(q_f,[g],\{a\},q)a^*b^*$,
Wrong consecutive transitions: It contains a factor in $\bigcup_{q_1\neq p_2}(p_1,[g_1],\{a_1\},q_1)a^*b^*(p_2,[g_2],\{a_2\},q_2)$,
Illegal zero test: It contains a factor in $\bigcup_{p,q}\big[a^+b^*(p,[c_1=0],\{\},q) \cup a^*b^+(p,[c_2=0],\{\},q)\big]$,
Wrong increment on c_1**:** It contains a factor in $\bigcup_{\ell\neq k+1}\bigcup_{p,q}\Delta a^k b^*(p,[true],\{c_1{+}{+}\},q)a^\ell b^*\Delta$.
Wrong decrement on c_1**:** It contains a factor in $\bigcup_{\ell\neq k-1}\bigcup_{p,q}\Delta a^k b^*(p,[true],\{c_1{-}{-}\},q)a^\ell b^*\Delta$.
Wrong increment or decrement on c_2**:** Similar to the corresponding property on c_1.

The first 5 conditions are described by a regular language L. By Proposition 4.11, the characteristic function $\underline{L}$ is effectively recognizable: there is a computable recognizable series f such that $f(w) = \mathbb{0} = \infty$ if $w \notin L$ and $f(w) = \mathbb{1} = 0$ if $w \in L$. Therefore, $g = \min(0, f-1) = 0 \oplus (f \odot (-1))$ is also effectively recognizable and

$$g(w) = \begin{cases} -1 & \text{if } w \in L, \text{ and,} \\ 0 & \text{if } w \notin L. \end{cases}$$

It remains to treat the last conditions: wrong increment or decrement on c_1 or c_2. Let us explain how to handle a wrong increment on c_1, *i.e.*, the encoding contains a factor $\Delta a^k b^*(p,[true],\{c_1{+}{+}\},q)a^\ell b^*\Delta$ with $\ell \neq k+1$. Therefore, either $\ell > k+1$ or $\ell < k+1$. Let us treat only the case $\ell > k+1$. To assign a negative value to such words, we design a weighted automaton which

- scan the word with weight 0, until nondeterministically guessing the beginning of a factor $\Delta a^k b^*(p,[true],\{c_1{+}{+}\},q)a^\ell b^*\Delta$ to be checked.
- then count
  - weight 0 for the first letter of this factor in Δ,
  - weight 1 for each a and 0 for each b in the block $a^k b^*$,
  - weight 1 for the intermediate transition, checking that it is if the form $(p,[true],\{c_1{+}{+}\},q)$,
  - weight -1 for each a and 0 for each b in the block $a^\ell b^*$,
- finally scan the rest of the word with weight 0.

Therefore on a run, the computed weight is $k+1-\ell$, which is negative if and only if $k+1 < \ell$. Call $f_{1,+,>}$ the corresponding recognizable series. Since the semantics of a weighted automaton on a word w is the minimum of the weights of all runs on w, we have $f_{1,+,>}(w) < 0$ if and only if w has a factor of the form $\Delta a^k b^*(p,[true],\{c_1{+}{+}\},q)a^\ell b^*\Delta$ with $\ell > k+1$. If w has no wrong increment, then $f_{1,+,>}(w) = 0$.

Similarly, one builds $f_{1,+,<}$ which computes a negative value if and only if there is a factor of the form $\Delta a^k b^*(p,[true],\{c_1{+}{+}\},q)a^\ell b^*\Delta$ with $\ell < k+1$. Therefore, $f_{1,+} = \min(f_{1,+,<}, f_{1,+,>}) = f_{1,+,<} \oplus f_{1,+,>}$ computes a negative value if and only if w contains some wrong increment on c_1, and 0 otherwise. Similarly we build $f_{2,+}$ for checking a wrong increment on c_2, and $f_{1,-}, f_{2,-}$ for checking wrong decrements. Then, $h = \min(g, f_{1,-}, f_{2,-}, f_{1,+}, f_{2,+})$ is such that $h(w) < 0$ if and only if w is incorrect, and $h(w) = 0$ otherwise, that is, if w is a correct encoding of a computation of $\mathcal{M}$ ending in $\{q_f\} \times \mathbb{N} \times \mathbb{N}$.

This shows (*i*) and concludes the proof. ∎

Exercises for Chapter 5

Exercise 5.1. Show theorem 5.3

1. by a reduction from Hilbert's 10^{th} problem,
2. by a reduction from PCP.

Exercise 5.2. Prove Theorem 5.4.

Exercise 5.3. Show that the function mapping $(a^k b)^\ell$ to $k\ell$, and words not in $(a^*b)^*$ to 0 is recognizable on $\mathbb{T}\text{rop}$.

Further reading and references

[DMR76] M. Davis, Y. V. Matijasevič, and J. Robinson. "Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution". In: *Mathematical Developments Arising from Hilbert Problems*. Vol. 28. Proc. of Symposia in Pure Mathematics. Providence, Rhode Island: American Mathematical Society, 1976, pp. 323–378 (cit. on p. 29).

[Kir05] Daniel Kirsten. "Distance desert automata and the star height problem". In: *RAIRO Inform. Théor. Appl.* 39.3 (2005), pp. 455–509. ISSN: 0988-3754 (cit. on p. 30).

[Kro94] D. Krob. "The equality problem for rational series with multiplicities in the tropical semiring is undecidable". In: *Int. J. of Algebra and Comput.* 4.3 (1994), pp. 405–425 (cit. on p. 30).

[KS85] W. Kuich and A. Salomaa. *Semirings, Automata and Languages*. Springer, 1985 (cit. on p. 29).

[LP04] Hing Leung and Viktor Podolskiy. "The limitedness problem on distance automata: Hashiguchi's method revisited". In: *Theor. Comp. Sci.* 310.1-3 (2004), pp. 147–158 (cit. on p. 30).

[Mat93] Y. V. Matijasevič. *Hilbert's Tenth Problem*. Cambridge, Massachusetts: MIT Press, 1993. ISBN: 0-262-13295-8 (cit. on p. 29).

[Min67] Marvin L. Minsky. *Computation: finite and infinite machines*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1967. ISBN: 0-13-165563-9 (cit. on p. 31).

[Sim94] Imre Simon. "On Semigroups of Matrices over the Tropical Semiring". In: *ITA* 28.3-4 (1994), pp. 277–294 (cit. on p. 30).

[SS78] A. Salomaa and M. Soittola. *Automata-theoretic aspects of formal power series*. Springer, 1978 (cit. on p. 29).

CHAPTER 6

Word Transducers

1. Definition

Word transducers have manifold applications in computer science, e.g., in regular model checking [Abd+04], speech recognition, natural language processing [Moh97], etc. A general reference for word transducers is [Ber79].

DEFINITION 6.1. Let B be an alphabet. A word transducer over B is a weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over $\mathbb{R}\mathrm{eg}_B = (\mathrm{Rat}(B), \cup, \cdot, \varnothing, \{\varepsilon\})$. ■

Thus, $\|\mathcal{A}\|$ assigns to a word $w \in A^*$ a language $\|\mathcal{A}\|(w) \subseteq B^*$. Usually, $\|\mathcal{A}\|$ is represented by the binary relation

$$R(\mathcal{A}) \stackrel{\text{def}}{=} \{(u, v) \in A^* \times B^* \mid v \in \|\mathcal{A}\|(u)\}\,.$$

From that point of view, word transducers describe precisely the *rational relations* (cf. [Cho04; Cho09]).

EXAMPLE 6.2. Let $A = \{a, b\}$. A word transducer $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over A is depicted in Fig. 6.1, where $\lambda(q_0) = \gamma(q_0) = A^* \in \mathcal{R}_A$. For all $u \in A^*$, $\|\mathcal{A}\|(u)$ is the set of words $v \in A^*$ such that u is an infix of v.

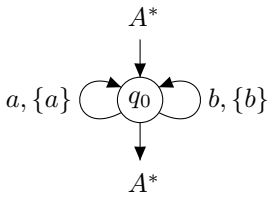


FIG. 6.1. A word transducer

2. Threshold Problems for Word Transducers

Word transducers can be used to model systems that communicate with an environment. Suppose a system can execute actions from an alphabet A that are triggered by input streams from B^* where B is a set of signals (cf. Fig. 6.2). This can be modeled by a word transducer $\mathcal{A}$ over B with input alphabet A. For a sequence $w \in A^*$ of actions, $\|\mathcal{A}\|(w)$ contains the sequences that trigger the behavior w. Often, the input stream cannot be predicted in advance but only isolated by a, say, regular set $E \subseteq B^*$. Thus, it can be useful to know the set of words $w \in A^*$ such that $E \cap \|\mathcal{A}\|(w) \neq \varnothing$. This corresponds to the set $L_{\cap_{\neq\varnothing}\, E}(\mathcal{A})$ where $\cap_{\neq\varnothing}$ is the set of pairs (M_1, M_2) with nonempty intersection.

Suppose we are given a set $\mathit{Bad} \subseteq A^*$ of bad behaviors that our system must avoid. Then, we would like to have

$$\mathit{Bad} \cap L_{\cap_{\neq\varnothing}\, E}(\mathcal{A}) = \varnothing\,.$$

If, on the other hand, we are given a set $\mathit{Good} \subseteq A^*$ of behaviors that the system should exhibit, then we need a statement such as

$$\mathit{Good} \subseteq L_{\subseteq E}(\mathcal{A})\,.$$

The first problem, where $\mathcal{A}$, E, and Bad act as the input, is the *model checking problem wrt. safety properties*. The second one, where in the input Bad is replaced with Good, is the *model checking problem wrt. liveness properties*. These considerations motivate us to study the threshold emptiness and universality problems for word transducers.

$$\text{stream from } B^* \Longrightarrow \mathcal{A} \Longrightarrow \text{behavior from } A^*$$

FIG. 6.2. A system communicating with its environment

The following result follows from a standard automaton construction.

THEOREM 6.3. *Let B be an alphabet and let $\mathcal{A}$ be a word transducer over B. For every regular language $E \subseteq B^*$, the threshold language $L_{\cap_{\neq\varnothing} E}(\mathcal{A})$ is effectively regular.*

PROOF. Suppose $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ and let E be represented by the finite automaton $\mathcal{B} = (P, B, \Delta, p_0, F)$. We construct the finite automaton $\mathcal{B}' = (P', A, \Delta', P'_0, F')$ (here, $P'_0 \subseteq P'$ is a set of initial states) with $L(\mathcal{B}') = L_{\cap_{\neq\varnothing} E}(\mathcal{A})$ as follows:

- $P' = Q \times P$
- $P'_0 = \{(q, p) \in P' \mid p \in \delta(p_0, \lambda(q))\}$
- $F' = \{(q, p) \in Q \times P \mid \delta(p, \gamma(q)) \cap F \neq \varnothing\}$
- $((q, p), a, (q', p')) \in \Delta'$ if $p' \in \delta(p, \mu(q, a, q'))$

Hereby, for $p \in P$ and a regular set $L \subseteq B^*$, $\delta(p, L)$ denotes the (computable) set of states of $\mathcal{B}$ that are reachable from p by reading some word from L. ∎

COROLLARY 6.4. *For word transducers, both the threshold emptiness problem and the threshold universality problem wrt. $\cap_{\neq\varnothing}$ are decidable.*

We also conclude that, for word transducers over B, the model checking problem wrt. safety properties is decidable.

Unfortunately, both the threshold emptiness and the threshold universality problem become undecidable when we consider the binary relation $\subseteq$. We will first show the result for the universality problem.

THEOREM 6.5. *Let B be an alphabet with at least two letters. Then, the threshold universality problem for word transducers over B wrt. $\subseteq$ is undecidable.*

We will actually show undecidability of a concrete instance of that problem:

THEOREM 6.6. *Let B be an alphabet with at least two letters. The following problem is undecidable:*

INPUT: *Word transducer $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over B.*
PROBLEM: *Do we have $\|\mathcal{A}\|(w) = B^*$ for every $w \in A^*$?*

PROOF. The proof is by reduction from Post's correspondence problem (PCP), which is given as follow:

INPUT: Alphabet A and morphisms $f, g : A^* \to \{0,1\}^*$.
PROBLEM: Is there $w \in A^+$ such that $f(w) = g(w)$?

Let an instance of the PCP be given by A and f, g. Suppose $B = \{0, 1\}$. Our reduction is based on two binary relations $R_f, R_g \subseteq A^+ \times B^*$:

$$R_f = \{(w, f(w)) \mid w \in A^+\}$$
$$R_g = \{(w, g(w)) \mid w \in A^+\}$$

We can construct a word transducer $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over B such that

$$R(\mathcal{A}) = \overline{R_f} \cup \overline{R_g}$$

where, for a relation $R \subseteq A^* \times B^*$, we let $\overline{R} = (A^* \times B^*) \setminus R$. We have

$$\begin{aligned} & \|\mathcal{A}\|(w) = B^* \text{ for every } w \in A^* \\ \text{iff} \quad & R(\mathcal{A}) = A^* \times B^* \\ \text{iff} \quad & \text{there is no } w \in A^+ \text{ such that } f(w) = g(w) \end{aligned}$$

The construction of $\mathcal{A}$ is left as an exercise (Exercise 6.1). This concludes the proof of Theorem 6.6. ∎

From that result, we deduce that, for word transducers over B, the model checking problem wrt. liveness properties is undecidable.

THEOREM 6.7. *Let B be an alphabet with at least two letters. Then, the threshold emptiness problem for word transducers over B wrt. $\subseteq$ is undecidable.*

Again, we will show undecidability of a more specific problem:

THEOREM 6.8. *Let B be an alphabet with at least two letters. The following problem is undecidable:*

INPUT: *Word transducer $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over B.*
PROBLEM: *Do we have $\|\mathcal{A}\|(w) = B^*$ for some $w \in A^*$?*

PROOF. Again, the proof is by reduction from the PCP. It is inspired by a result from a timed setting [Aks+08].

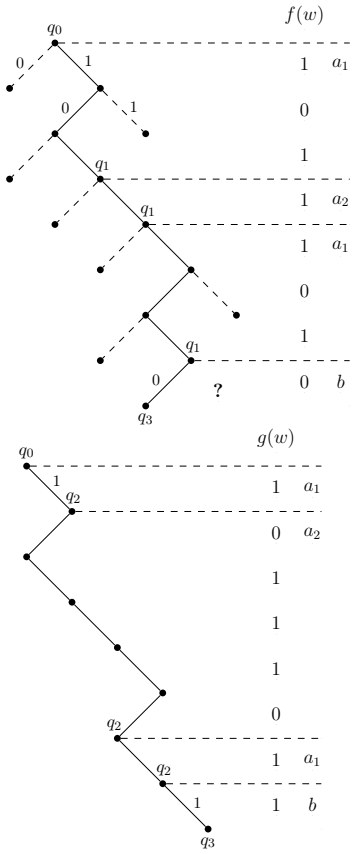


FIG. 6.3. The trees generated by $w = a_1a_2a_1b$

From a PCP instance A, f, g, we will construct a word transducer $\mathcal{A}$ over $B = \{0, 1\}$ such that $L_{\subseteq B^*}(\mathcal{A}) = \{u.b \mid u \in A^+ \text{ and } f(u) = g(u)\}$. The idea of our construction is illustrated in Fig. 6.3. Consider the PCP instance given by $A = \{a_1, a_2\}$ and

$$\begin{aligned} f(a_1) &= 101 & f(a_2) &= 1 \\ g(a_1) &= 1 & g(a_2) &= 01110 \end{aligned}$$

with the obvious solution $u = a_1a_2a_1$. Our transducer will be split into two parts. One part is concerned with f (cf. the left hand side of the figure). Intuitively, it reads a sequence $u.b$ with $u \in A^+$ and generates a tree whose nodes correspond to words over B. A node (or, the path to reach the node from the root) will be accepted unless it corresponds to $f(u)$. In the latter case, the transducer remains in a state q_1. When reading b in q_1, our transducer will produce 0, and will accept. However, the sequence $u.b$ is in $L_{\subseteq B^*}(\mathcal{A})$ only if a path labeled $f(u).1$ is accepted, too. Such a path can be provided by the second part of the automaton, simulating g (cf. the right hand side of the figure). The missing path needs to follow

$f(u)$ and produce the letter 1 on that node where the f-part had produced 0. For this, $f(u)$ and $g(u)$ have to coincide, which implies that the PCP instance has a solution.

Let an instance of the PCP be given by the alphabet $A = \{a_1, \ldots, a_k\}$ with $k \geqslant 1$ and two corresponding morphisms f and g. We will construct a word transducer $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over $B = \{0, 1\}$, with $A = \{a_1, \ldots, a_k, b\}$, such that

$$L_{\subseteq B^*}(\mathcal{A}) = \{u.b \mid u \in A^+ \text{ and } f(u) = g(u)\}\,.$$

The automaton $\mathcal{A}$ is given by Fig. 6.4. Hereby, for $i \in \{1, \ldots, k\}$, we let

$$\begin{aligned} \mathrm{F}_i &= \{f(a_i)\} \qquad & \overline{\mathrm{F}}_i &= \{v \in B^* \mid f(a_i) \notin \mathit{Pref}(v)\} \\ \mathrm{G}_i &= \{g(a_i)\} \end{aligned}$$

where $\mathit{Pref}(v) = \{v_1 \in B^* \mid v = v_1.v_2 \text{ for some } v_2 \in B^*\}$ is the set of *prefixes* of v.

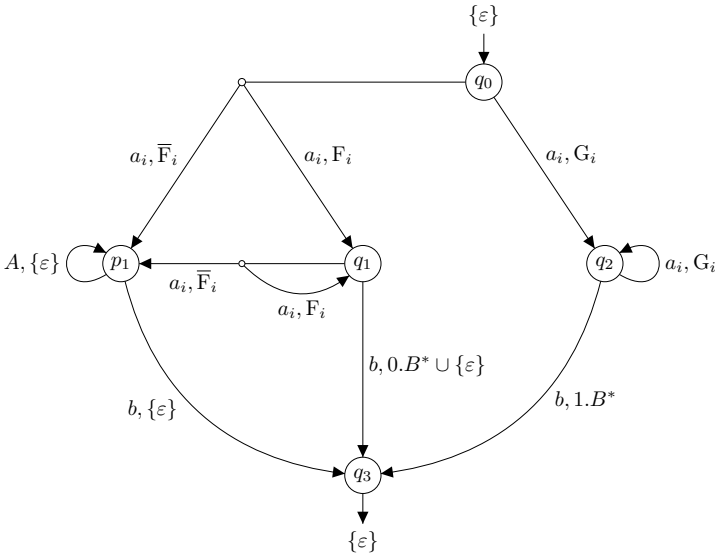


FIG. 6.4. Encoding of PCP in terms of a word transducer

For a state $q \in Q$, let in the following $\mathcal{A}_q$ refer to the word transducer $(Q, A, \lambda, \mu, \gamma')$ where, for $p \in Q$,

$$\gamma'(p) = \begin{cases} \{\varepsilon\} & \text{if } p = q \\ \varnothing & \text{if } p \neq q \end{cases}$$

CLAIM 6.9. For every $u \in A^+$, the following hold:

(1) $\|\mathcal{A}_{q_1}\|(u) = \{f(u)\}$
(2) $\|\mathcal{A}_{q_2}\|(u) = \{g(u)\}$
(3) $\|\mathcal{A}_{p_1}\|(u) = \{v \in B^* \mid f(u) \notin \mathit{Pref}(v)\}$

We can now show that $L_{\subseteq B^*}(\mathcal{A}) = \{u.b \mid u \in A^+ \text{ and } f(u) = g(u)\}$.

Let $u \in A^+$ with $f(u) = g(u)$ and let $v \in B^*$. To prove that $v \in \|\mathcal{A}\|(u.b)$, we distinguish three cases:

(1) If $v = f(u)$ or $v \in f(u).0.B^*$, then $v \in \|\mathcal{A}\|(u.b)$ by Claim 6.9 (1).
(2) If $v \in f(u).1.B^*$, then $v \in \|\mathcal{A}\|(u.b)$ by Claim 6.9 (2).
(3) If $v \notin f(u).B^*$, then $v \in \|\mathcal{A}\|(u.b)$ by Claim 6.9 (3).

Thus, we have $v \in \|\mathcal{A}\|(u.b)$.

Conversely, let $u \in A^+$ and suppose $\|\mathcal{A}\|(u.b) = B^*$. We have $f(u) \in \|\mathcal{A}_{q_1}\|(u)$ and $f(u) \notin \|\mathcal{A}_{p_1}\|(u)$ (Claims 6.9 (1) and (3)). As $f(u).1 \in \|\mathcal{A}\|(u.b)$, we must have $f(u) \in \|\mathcal{A}_{q_2}\|(u)$. By Claim 6.9 (2), we deduce $f(u) = g(u)$. ∎

Exercises for Chapter 6

EXERCISE 6.1. Construct the word transducer $\mathcal{A}$ over $B = \{0, 1\}$ from the proof of Theorem 6.6. Recall that $\mathcal{A}$ should satisfy $R(\mathcal{A}) = \overline{R_f} \cup \overline{R_g}$. Note that $\overline{R_f}$ (similarly for $\overline{R_g}$) is the union of the following relations:

$$R_0 = \{(u, v) \in A^* \times B^* \mid u = \varepsilon\}$$
$$R_1 = \{(u, v) \in A^+ \times B^* \mid |v| < |f(u)|\}$$
$$R_2 = \{(u, v) \in A^+ \times B^* \mid |v| > |f(u)|\}$$
$$R_3 = \{(u, v) \in A^+ \times B^* \mid |v| = |f(u)| \text{ and } v \neq f(u)\}$$

The respective word transducers can then be combined towards $\mathcal{A}$.

EXERCISE 6.2. Show Theorem 6.6 by means of a variant of the proof of Theorem 6.8.

EXERCISE 6.3. Show Claim 6.9 (3).

Further reading and references

[Abd+04] P. Aziz Abdulla et al. "A Survey of Regular Model Checking." In: *Proc. of CONCUR'04*. Vol. 3170. Lect. Notes Comp. Sci. Springer, 2004, pp. 35–48 (cit. on p. 35).

[Aks+08] S. Akshay et al. "Distributed Timed Automata with Independently Evolving Clocks". In: *Proc. of CONCUR'08*. Vol. 5201. Lect. Notes Comp. Sci. Springer, 2008, pp. 82–97. DOI: 10.1007/978-3-540-85361-9_10 (cit. on p. 37).

[Ber79] J. Berstel. *Transductions and context-free languages*. Teubner Stuttgart, 1979 (cit. on p. 35).

[Cho04] Ch. Choffrut. "Rational Relations as Rational Series". In: *Theory Is Forever, Essays Dedicated to Arto Salomaa on the Occasion of His 70th Birthday*. Vol. 3113. Lect. Notes Comp. Sci. Springer, 2004, pp. 29–34 (cit. on p. 35).

[Cho09] Ch. Choffrut. *A short introductory course to rational relations*. 2009 (cit. on p. 35).

[Moh97] M. Mohri. "Finite-state transducers in language and speech processing". In: *Computational Linguistics* 23.2 (1997), pp. 269–311 (cit. on p. 35).

CHAPTER 7

Weighted Logic

In this section, we present a logical characterization of weighted automata in terms of a monadic second-order logic [DG07; DG09]. This characterization extends one of the fundamental theorems in computer science, which goes back to Büchi and Elgot: the precise correspondence between finite automata and monadic second-order formulas [Büc60; Elg61]. A detailed exposition of weighted logics and their connection with weighted automata can be found in [DG07; DG09].

1. MSO Logic over Words

We fix infinite supplies $Var = \{x, y, x_1, x_2, \ldots\}$ of *first-order* and $VAR = \{X, Y, X_1, X_2, \ldots\}$ of *second-order variables*.

Let us recall monadic second-order logic in the traditional boolean setting. Fix an alphabet A.

Definition 7.1. The set of *monadic second-order formulas* (MSO formulas) over A is given by the grammar

$$\phi ::= P_a(x) \mid x \leqslant y \mid x \in X \mid \phi_1 \vee \phi_2 \mid \neg\phi \mid \exists x.\phi \mid \exists X.\phi$$

where $a \in A$, $x, y \in Var$, and $X \in VAR$. The set of all those formulas is denoted by $\mathrm{MSO}(A)$. ∎

Furthermore, we may usual abbreviations such as $\phi_1 \wedge \phi_2$, $x = y$, $succ(x, y)$, $\phi_1 \to \phi_2$, $\phi_1 \leftrightarrow \phi_2$, $\forall x.\phi$, and $\forall x.\phi$.

For $\phi \in \mathrm{MSO}(A)$, let $Free(\phi)$ denote the set of variables that are free in ϕ. If $Free(\phi) = \varnothing$, then ϕ is called a *sentence*.

For a finite set $\mathcal{V} \subseteq Var \cup VAR$ and a word $w = a_1 \ldots a_n \in A^*$, a $(\mathcal{V}, w)$-*assignment* is a function σ that maps a first-order variable in $\mathcal{V}$ to an element of $\{1, \ldots, n\}$ and a second-order variable in $\mathcal{V}$ to a subset of $\{1, \ldots, n\}$. For $x \in Var$, $i \in \{1, \ldots, n\}$, and $I \subseteq \{1, \ldots, n\}$, $\sigma[x \to i]$ will denote the $(\mathcal{V} \cup \{x\}, w)$-assignment that maps x to i and, otherwise, coincides with σ. The $(\mathcal{V} \cup \{X\}, w)$-assignment $\sigma[X \to I]$ is defined accordingly.

A word $w = a_1 \ldots a_n \in A^*$ can be considered as the mathematical structure

$$\underline{w} \stackrel{\text{def}}{=} (\{1, \ldots, n\}, \leqslant, (R_a)_{a \in A})$$

where, for $a \in A$, $R_a = \{i \in \{1, \ldots, n\} \mid a_i = a\}$.

For a formula $\phi \in \mathrm{MSO}(A)$, a finite set $\mathcal{V} \subseteq Var \cup VAR$ with $Free(\phi) \subseteq \mathcal{V}$, a word $w \in A^*$, and a $(\mathcal{V}, w)$-assignment σ, the satisfaction relation $(w, \sigma) \models \phi$ is defined as usual, by induction on the basis of the structure $\underline{w}$.

Example 7.2. Let $A = \{a, b, c\}$. Here are some formulas from $\mathrm{MSO}(A)$:

- $\phi_1 = \forall x.(P_a(x) \to \exists y.(x \leqslant y \wedge P_b(y)))$
  "every a is eventually followed by a b"
- $\phi_2 = \exists x.\forall y.(x \leqslant y \to \neg P_a(y))$
  "from some time on, there are only b's or c's"
- $\phi_3 = \exists X.\exists x.\exists y.(\quad \neg\exists z.(z < x \vee y < z)$
  $\wedge \quad x \in X \wedge y \in X$
  $\wedge \quad \forall z.(z \in X \leftrightarrow \forall z'.(succ(z, z') \to \neg(z' \in X))))$
  "the word has odd length"

In the following, it will be convenient to encode a pair (w, σ) where σ is a $(\mathcal{V}, w)$-assignment as a word over the extended alphabet $A_{\mathcal{V}} \stackrel{\text{def}}{=} A \times \{0,1\}^{\mathcal{V}}$ (setting $A_{\varnothing} = A$). We write a word $(a_1, \sigma_1) \dots (a_n, \sigma_n) \in A_{\mathcal{V}}^*$ as (w, σ) where $w = a_1 \dots a_n \in A^*$ and $\sigma = \sigma_1 \dots \sigma_n \in \{0,1\}^{\mathcal{V}}$. We call (w, σ) *valid* if, for each first-order variable $x \in \mathcal{V}$, the x-row of σ contains exactly one 1. If (w, σ) is valid, then σ can be considered as the $(\mathcal{V}, w)$-assignment that maps a first-order variable $x \in \mathcal{V}$ to the unique position carrying 1 in the x-row and a second-order variable $X \in \mathcal{V}$ to the set of positions carrying 1 in the X-row.

EXAMPLE 7.3. Let $A = \{a, b, c\}$ and $\mathcal{V} = \{x, y, X\}$. Consider the pair $(w, \sigma) \in A_{\mathcal{V}}^*$ given as follows:

$$\begin{array}{cc} w & \left\{\begin{array}{cccc} a & b & a & c \end{array}\right. \\ \sigma & \left\{\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{array}\right. \end{array} \qquad \begin{array}{c} x \\ y \\ X \end{array}$$

Then, (w, σ) is valid, *i.e.*, σ can be considered as a $(\mathcal{V}, w)$-assignment.

Let $\phi \in \mathrm{MSO}(A)$ and $\mathcal{V}$ be a finite set of variables such that $\mathit{Free}(\phi) \subseteq \mathcal{V}$. It is easy to see that $N_{\mathcal{V}} \stackrel{\text{def}}{=} \{(w, \sigma) \in A_{\mathcal{V}}^* \mid (w, \sigma) \text{ is valid}\}$ is recognizable in terms of a finite automaton. Moreover, the set $L_{\mathcal{V}}(\phi) \stackrel{\text{def}}{=} \{(w, \sigma) \in N_{\mathcal{V}} \mid (w, \sigma) \models \phi\} \subseteq A_{\mathcal{V}}^*$ of valid pairs satisfying ϕ form a recognizable language. Let $L(\phi)$ abbreviate $L_{\mathit{Free}(\phi)}(\phi)$.

THEOREM 7.4 (Büchi and Elgot [Büc60; Elg61]). *Let $L \subseteq A^*$. The following statements are equivalent:*

(1) There is a finite automaton $\mathcal{A}$ such that $L(\mathcal{A}) = L$.
(2) There is a sentence $\phi \in \mathrm{MSO}(A)$ such that $L(\phi) = L$.

2. Weighted MSO Logic over Words

For the rest of this section, we fix a *commutative* semiring $\mathbb{S} = (S, +, \cdot, \mathbb{0}, \mathbb{1})$ and an alphabet A.

DEFINITION 7.5. The set of <u>*weighted monadic second-order formulas*</u> (or, simply, wMSO formulas) over $\mathbb{S}$ and A is given by the grammar

$$\begin{aligned} \phi ::= {} & s \mid P_a(x) \mid \neg(P_a(x)) \mid x \leqslant y \mid \neg(x \leqslant y) \mid \\ & x \in X \mid \neg(x \in X) \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2 \mid \\ & \exists x.\phi \mid \exists X.\phi \mid \forall x.\phi \mid \forall X.\phi \end{aligned}$$

where $s \in \mathbb{S}$, $a \in A$, $x, y \in \mathit{Var}$, and $X \in \mathit{VAR}$. The set of those formulas is denoted by $\mathrm{wMSO}(\mathbb{S}, A)$. ■

Negated formulas and formulas of the form s, $P_a(x)$, $x \leqslant y$, and $x \in X$ as well as are called *atomic*.

DEFINITION 7.6. Let $\phi \in \mathrm{wMSO}(\mathbb{S}, A)$ and $\mathcal{V}$ be a finite set of first-order and second-order variables such that $\mathit{Free}(\phi) \subseteq \mathcal{V}$. The semantics of ϕ wrt. $\mathcal{V}$ is a formal power series $[\![\phi]\!]_{\mathcal{V}} \in \mathbb{S}\langle\langle A_{\mathcal{V}}^* \rangle\rangle$, which is given as follows: If (w, σ) is not valid, we set $[\![\phi]\!]_{\mathcal{V}}(w, s) = \mathbb{0}$. Otherwise, $[\![\phi]\!]_{\mathcal{V}}(w, \sigma)$, where $w = a_1 \dots a_n$, is determined inductively as shown in Table 1. ■

We will simply write $[\![\phi]\!]$ for $[\![\phi]\!]_{\mathit{Free}(\phi)}$.

Let us consider some examples.

EXAMPLE 7.7. Recall that $\mathbb{B}\mathrm{ool} = (\{\mathsf{false}, \mathsf{true}\}, \vee, \wedge, \mathsf{false}, \mathsf{true})$ is the boolean algebra. The logic $\mathrm{wMSO}(\mathbb{B}\mathrm{ool}, A)$ actually reduces to $\mathrm{MSO}(A)$.

EXAMPLE 7.8. Let $A = \{a, b, c\}$ and consider the semiring of natural numbers $\mathbb{N}\mathrm{at} = (\mathbb{N}, +, \cdot, 0, 1)$. Let $\phi = \exists x.P_a(x) \in \mathrm{wMSO}(\mathbb{N}\mathrm{at}, A)$. For all $w \in A^*$, we have $[\![\phi]\!](w) = |w|_a$, *i.e.*, ϕ "counts" the number of occurrences of a in w.

EXAMPLE 7.9. Consider the alphabet $A = \{a_1, \dots, a_k\}$ and the *reliability* semiring $([0,1], \max, \cdot, 0, 1)$. Assume that every letter a_i comes with a reliability $p_i \in [0,1]$. Let $\phi = \forall x. \bigvee_{i=1}^{k} (P_{a_i}(x) \wedge p_j)$. Then, $[\![\phi]\!](w)$ can be interpreted as the reliability of the word $w \in A^*$.

$$
\begin{aligned}
[\![s]\!]_{\mathcal{V}}(w,\sigma) &= s \\
[\![P_a(x)]\!]_{\mathcal{V}}(w,\sigma) &= \begin{cases} \mathbb{1} & \text{if } a_{\sigma(x)} = a \\ \mathbb{0} & \text{otherwise} \end{cases} \\
[\![x \leqslant y]\!]_{\mathcal{V}}(w,\sigma) &= \begin{cases} \mathbb{1} & \text{if } \sigma(x) \leqslant \sigma(y) \\ \mathbb{0} & \text{otherwise} \end{cases} \\
[\![x \in X]\!]_{\mathcal{V}}(w,\sigma) &= \begin{cases} \mathbb{1} & \text{if } \sigma(x) \in \sigma(X) \\ \mathbb{0} & \text{otherwise} \end{cases} \\
[\![\neg\phi]\!]_{\mathcal{V}}(w,\sigma) &= \begin{cases} \mathbb{1} & \text{if } [\![\phi]\!]_{\mathcal{V}}(w,\sigma) = \mathbb{0} \\ \mathbb{0} & \text{if } [\![\phi]\!]_{\mathcal{V}}(w,\sigma) = \mathbb{1} \end{cases}
\end{aligned}
$$

$$
\begin{aligned}
[\![\phi_1 \vee \phi_2]\!]_{\mathcal{V}}(w,\sigma) &= [\![\phi_1]\!]_{\mathcal{V}}(w,\sigma) + [\![\phi_2]\!]_{\mathcal{V}}(w,\sigma) \\
[\![\phi_1 \wedge \phi_2]\!]_{\mathcal{V}}(w,\sigma) &= [\![\phi_1]\!]_{\mathcal{V}}(w,\sigma) \cdot [\![\phi_2]\!]_{\mathcal{V}}(w,\sigma)
\end{aligned}
$$

$$
\begin{aligned}
[\![\exists x.\phi]\!]_{\mathcal{V}}(w,\sigma) &= \sum_{i \in \{1,\dots,n\}} [\![\phi]\!]_{\mathcal{V}\cup\{x\}}(w, \sigma[x \to i]) \\
[\![\forall x.\phi]\!]_{\mathcal{V}}(w,\sigma) &= \prod_{i \in \{1,\dots,n\}} [\![\phi]\!]_{\mathcal{V}\cup\{X\}}(w, \sigma[x \to i]) \\
[\![\exists X.\phi]\!]_{\mathcal{V}}(w,\sigma) &= \sum_{I \subseteq \{1,\dots,n\}} [\![\phi]\!]_{\mathcal{V}\cup\{x\}}(w, \sigma[X \to I]) \\
[\![\forall X.\phi]\!]_{\mathcal{V}}(w,\sigma) &= \prod_{I \subseteq \{1,\dots,n\}} [\![\phi]\!]_{\mathcal{V}\cup\{X\}}(w, \sigma[X \to I])
\end{aligned}
$$

TABLE 1. The semantics of wMSO$(\mathbb{S}, A)$-formulas

EXAMPLE 7.10. Consider the sentences $\phi_1 = \forall x.2$ and $\phi_2 = \forall y.\forall x.2$ from wMSO$(\mathbb{N}\mathrm{at}, A)$. For all $w \in A^*$, we have $[\![\phi_1]\!](w) = 2^{|w|}$ and $[\![\phi_2]\!](w) = (2^{|w|})^{|w|} = 2^{|w|^2}$. While $[\![\phi_1]\!]$ is recognizable (*i.e.*, there is a weighted automaton whose semantics is $[\![\phi_1]\!]$), $[\![\phi_2]\!]$ is not: Suppose there is a weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over $\mathbb{N}\mathrm{at}$ such that $\|\mathcal{A}\| = [\![\phi_2]\!]$. Let $m = \max\{\lambda(p), \gamma(p), \mu(p,a,q) \mid p,q \in Q \text{ and } a \in A\}$. Then, for all $w \in A^*$, $\|\mathcal{A}\|(w) \leqslant |Q|^{|w|+1} \cdot m^{|w|+2}$, which is a contradiction to $\|\mathcal{A}\|(w) = 2^{|w|^2}$. Now let $\phi_3 = \forall X.2 \in \mathrm{MSO}(\mathbb{N}\mathrm{at}, A)$. Then, for all $w \in A^*$, $[\![\phi_3]\!](w) = 2^{2^{|w|}}$. Thus, $[\![\phi_3]\!]$ is not recognizable either.

The last examples show that we need to restrict universal quantification in formulas to obtain a logical characterization of weighted automata. So let us introduce the notion of a restricted formula:

DEFINITION 7.11. A formula $\phi \in \mathrm{wMSO}(\mathbb{S}, A)$ is called *restricted* if

- it does not contain universal set quantification, and
- for every subformula of ϕ of the form $\forall x.\psi$, the series $[\![\psi]\!]$ is a recognizable step function.

The set of restricted MSO formulas is denoted by $\mathrm{wRMSO}(\mathbb{S}, A)$. ■

Here, a series $f \in \mathbb{S}\langle\langle A^*_{\mathcal{V}} \rangle\rangle$ (for a finite set $\mathcal{V}$) is a *recognizable step function* if there are $k \in \mathbb{N}$, $s_1, \dots, s_k \in S$, and regular languages $L_1, \dots, L_k \subseteq A^*_{\mathcal{V}}$ such that

$$f = \sum_{j=1}^{k} s_j \cdot \mathbb{1}_{L_j}$$

where $\mathbb{1}_{L_i}$ is the characteristic function of L_i.

Let $f \in \mathbb{S}\langle\langle A^* \rangle\rangle$. We say that f is *recognizable* if there is a weighted automaton $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ over $\mathbb{S}$ such that $\|\mathcal{A}\| = f$. For a formula class $\mathcal{C} \subseteq \mathrm{MSO}(\mathbb{S}, A)$, we say that f is $\mathcal{C}$-definable if there exists a sentence $\phi \in \mathcal{C}$ such that $[\![\phi]\!] = f$.

The rest of this section will be devoted to the proof of the following theorem, which is a proper generalization of Theorem 7.4 to weighted automata and logic.

THEOREM 7.12 (Droste & Gastin [DG07; DG09]). *Let $f \in \mathbb{S}\langle\langle A^* \rangle\rangle$. The following statements are equivalent:*

(1) f is wRMSO$(\mathbb{S}, A)$*-definable.*
(2) f is recognizable.

3. From Logic to Automata

For proving the direction (1) $\Longrightarrow$ (2) of Theorem 7.12, we proceed inductively. Two lemmas will provide us with the required translations.

LEMMA 7.13. *Let $\phi, \psi \in$ wMSO$(\mathbb{S}, A)$.*

(a) If ϕ is atomic, then $[\![\phi]\!]$ is recognizable.
(b) If $[\![\phi]\!]$ and $[\![\psi]\!]$ are recognizable, then so are $[\![\phi \vee \psi]\!]$ and $[\![\phi \wedge \psi]\!]$.
(c) If $[\![\phi]\!]$ is recognizable, then $[\![\exists x.\phi]\!]$ and $[\![\exists X.\phi]\!]$ are recognizable.

The most difficult case, however, arises when we are facing universal quantification.

LEMMA 7.14. *Let $\phi \in$ wMSO$(\mathbb{S}, A)$ such that $[\![\phi]\!]$ is a recognizable step function. Then, $[\![\forall x.\phi]\!]$ is recognizable.*

PROOF. Let $\phi \in$ wMSO$(\mathbb{S}, A)$ such that $[\![\phi]\!]$ is a recognizable step function. Let $\mathcal{W} = \mathit{Free}(\phi)$ and $\mathcal{V} = \mathit{Free}(\forall x.\phi) = \mathcal{W} \setminus \{x\}$. There are $k \in \mathbb{N}$, $s_1, \ldots, s_k \in S$, and regular languages $L_1, \ldots, L_k \subseteq A_{\mathcal{W}}^*$ such that, for all $(w, \sigma) \in A_{\mathcal{W}}^*$, we have $[\![\phi]\!](w, \sigma) = \sum_{j=1}^{k} s_j \cdot \mathbb{1}_{L_j}$. Without loss of generality, we assume that the sets L_j form a partition of $A_{\mathcal{W}}^*$.

Case 1: Suppose $x \in \mathcal{W}$. Consider the alphabet $\widetilde{A} = A \times \{1, \ldots, k\}$. A word from $(\widetilde{A}_{\mathcal{V}})^*$ will be written as the triple (w, ν, σ) where (w, σ) is its projection onto $A_{\mathcal{V}}$ and $\nu \in \{1, \ldots, k\}^{|w|}$. In the obvious manner, we can consider ν to be a mapping $\nu : \{1, \ldots, |w|\} \to \{1, \ldots, k\}$. Let $\widetilde{L}$ be the set of words (w, ν, σ) over $\widetilde{A}_{\mathcal{V}}$ such that, for all $i \in \{1, \ldots, |w|\}$ and $j \in \{1, \ldots, k\}$,

$$\nu(i) = j \text{ implies } (w, \sigma[x \to i]) \in L_j \,.$$

We will show that

(*) $$\widetilde{L} \text{ is regular.}$$

Thus, there is a deterministic finite automaton $\widetilde{\mathcal{A}}$ over $\widetilde{A}_{\mathcal{V}}$ such that $L(\widetilde{\mathcal{A}}) = \widetilde{L}$. In turn, $\widetilde{\mathcal{A}}$ can be transformed into a weighted automaton $\mathcal{A}$ with input alphabet $\widetilde{A}_{\mathcal{V}}$ as follows:

- A transition of the form $(p, (a, j, \tau), q)$ is replaced with a transition $(p, (a, j, \tau), q)$ of weight s_j (*i.e.*, $\mu(p, (a, j, \tau), q) = s_j$). All other transitions have weight $\mathbb{0}$.
- The initial state of $\widetilde{\mathcal{A}}$ gets the initial weight $\mathbb{1}$, the other states get the initial weight $\mathbb{0}$.
- Each final state of $\widetilde{\mathcal{A}}$ gets the final weight $\mathbb{1}$, the other states get the final weight $\mathbb{0}$.

Then, for all $(w, \nu, \sigma) \in (\widetilde{A}_{\mathcal{V}})^*$, we have

$$\|\mathcal{A}\|(w, \nu, \sigma) = \begin{cases} \prod_{j=1}^{k} s_j^{|\nu^{-1}(j)|} & \text{if } (w, \nu, \tau) \in \widetilde{L} \\ \mathbb{0} & \text{if } (w, \nu, \tau) \notin \widetilde{L} \end{cases}$$

Note that, for each $(w, \sigma) \in A_{\mathcal{V}}^*$, there is a unique extension ν such that $(w, \nu, \sigma) \in \widetilde{L}$. If $\mathcal{A}'$ is the canonical projection of $\mathcal{A}$ onto the alphabet $A_{\mathcal{V}}$, we therefore have $\|\mathcal{A}'\|(w, \sigma) = \prod_{j=1}^{k} s_j^{|\nu^{-1}(j)|}$. As

$$[\![\forall x.\phi]\!](w, \sigma) = \prod_{i=1}^{|w|} [\![\phi]\!](w, \sigma[x \to i]) = \prod_{j=1}^{k} s_j^{|\nu^{-1}(j)|} \,,$$

we are done.

Let us show (*). Actually, it is sufficient, to construct, for every $j \in \{1, \dots, k\}$, a finite automaton $\widetilde{\mathcal{A}}_j$ over $\widetilde{A}_{\mathcal{V}}$ recognizing the set $\widetilde{L}_j$ of words (w, ν, σ) over $\widetilde{A}_{\mathcal{V}}$ such that, for all $i \in \{1, \dots, |w|\}$,

$$\nu(i) = j \text{ implies } (w, \sigma[x \to i]) \in L_j \,.$$

The reason is that $\widetilde{L} = \bigcap_{j \in \{1,\dots,k\}} \widetilde{L}_j$.

So let us fix $j \in \{1, \dots, k\}$ and let $\mathcal{A}_j = (Q, A_{\mathcal{W}}, \delta, q_0, F)$ be a deterministic finite automaton such that $L(\mathcal{A}_j) = L_j$. We specify $\widetilde{\mathcal{A}}_j = (\widetilde{Q}, \widetilde{A}_{\mathcal{V}}, \widetilde{\delta}, \widetilde{q_0}, \widetilde{F})$ with $L(\widetilde{\mathcal{A}}_j) = \widetilde{L}_j$ as follows:

- $\widetilde{Q} = Q \times 2^Q$
- $\widetilde{q_0} = (q_0, \varnothing)$
- $\widetilde{F} = Q \times 2^F$
- $\widetilde{\delta}((p, P), (a, \ell, \tau)) = (\delta(p, (a, \tau[x \to 0])), P')$

where

$$P' = \begin{cases} \{\delta(q, (a, \tau[x \to 0])) \mid q \in P\} & \text{if } \ell \neq j \\ \{\delta(q, (a, \tau[x \to 0])) \mid q \in P\} \cup \{\delta(p, (a, \tau[x \to 1]))\} & \text{if } \ell = j \end{cases}$$

Case 2: Suppose $x \notin \mathcal{W}$, which implies $\mathcal{W} = \mathcal{V}$. Consider the formula $\phi' = \phi \wedge (x \leqslant x)$. Then, $[\![\phi']\!]$ is recognizable due to Lemma 7.13(a) and (b). Moreover, it is a recognizable step function. Clearly, $[\![\phi']\!]_{\mathcal{V} \cup \{x\}} = [\![\phi]\!]_{\mathcal{V} \cup \{x\}}$ and $[\![\forall x.\phi']\!]_{\mathcal{V}} = [\![\forall x.\phi]\!]_{\mathcal{V}}$, which is recognizable due to Case 1. ∎

From Lemmas 7.13 and 7.14, we can indeed deduce the direction (1) $\Longrightarrow$ (2) of Theorem 7.12. If $\mathbb{S}$ is a computable field, then that direction is effective and one can decide if a formula is rstricted. Thus, decidable decision problems for weighted automata such as emptiness and equivalence can be extended to wRMSO-formulas [DG07; DG09].

4. From Automata to Logic

Let us prove the direction (2) $\Longrightarrow$ (1) of Theorem 7.12.

Let $\phi \in \mathrm{MSO}(A)$ be an unweighted MSO formula without set quantifier. We define formulas $\phi^+, \phi^- \in \mathrm{wMSO}(\mathbb{S}, A)$ such that $[\![\phi^+]\!] = \mathbb{1}_{L(\phi)}$ and $[\![\phi^-]\!] = \mathbb{1}_{L(\neg\phi)}$ inductively as follows: We assume that, in ϕ, negation is pushed inwards so that it is applied to (positive) atomic formulas only (*i.e.*, our syntax makes use of universal quantification and conjunction). If ϕ is atomic, then we set $\phi^+ = \phi$ and $\phi^- = \neg\phi$ (where $\neg\neg\psi$ is reduced to ψ). Moreover,

$$\begin{aligned}
(\phi \vee \psi)^+ &= \phi^+ \vee (\phi^- \wedge \psi^+) \\
(\phi \vee \psi)^- &= \phi^- \wedge \psi^- \\
(\phi \wedge \psi)^- &= \phi^- \vee (\phi^+ \wedge \psi^-) \\
(\phi \wedge \psi)^+ &= \phi^+ \wedge \psi^+ \\
(\exists x.\phi)^+ &= \exists x.(\phi^+(x) \wedge \forall y.((x \leqslant y) \vee (\neg(x \leqslant y) \wedge \phi^-(y)))) \\
(\exists x.\phi)^- &= \forall x.\phi^- \\
(\forall x.\phi)^- &= \exists x.(\phi^-(x) \wedge \forall y.((x \leqslant y) \vee (\neg(x \leqslant y) \wedge \phi^+(y)))) \\
(\forall x.\phi)^+ &= \forall x.\phi^+
\end{aligned}$$

Now let $\mathcal{A} = (Q, A, \lambda, \mu, \gamma)$ be a weighted automaton over $\mathbb{S}$. We show that there is a sentence $\phi \in \mathrm{wRMSO}(\mathbb{S}, A)$ such that $[\![\phi]\!] = \|\mathcal{A}\|$.

In the following, t and t' will range over $Q \times A \times Q$. Let $\overline{X}$ be the collection $(X_t)_t$ of second-order variables. The construction of a wMSO sentence from a weighted automaton follows the standard procedure of transforming a finite automaton into an MSO sentence: an interpretation of second-order variables reflects an assignment of positions in a word to transitions. We first provide some building blocks of the desired wRMSO formula.

The formula

$$\mathrm{partition}(\overline{X}) := \forall x. \bigvee_t ((x \in X_t) \wedge \bigwedge_{t' \neq t} \neg(x \in X_{t'}))$$

claims that $\overline{X}$ actually represents a run, *i.e.*, an assignment of vertices to transitions. Now let

$$\begin{aligned}\psi(\overline{X}) \stackrel{\text{def}}{=} \mathrm{partition}(\overline{X}) &\wedge \bigwedge_{p,a,q} \forall x.((x \in X_{p,a,q}) \to P_a(x))^+ \\ &\wedge \forall x. \forall y. \big(succ(x,y) \to \bigvee_{\substack{p,q,r \in Q \\ a,b \in A}} (x \in X_{p,a,q}) \wedge (y \in X_{q,b,r})\big)^+\end{aligned}$$

where

$$succ(x,y) \stackrel{\text{def}}{=} (x \leqslant y) \wedge \neg(y \leqslant x) \wedge \forall z.(z \leqslant x \vee y \leqslant z)$$

and the implications are considered to be unweighted (*i.e.*, boolean) formula. vWe set

$$\begin{aligned}\phi(\overline{X}) \stackrel{\text{def}}{=} \psi(\overline{X}) &\wedge \bigwedge_{p,a,q} \forall x.((x \in X_{p,a,q}) \to \mu(p,a,q)) \\ &\wedge \exists y. \big(\min(y) \wedge \bigvee_{p,a,q} (y \in X_{p,a,q}) \wedge \lambda(p)\big) \\ &\wedge \exists z. \big(\max(z) \wedge \bigvee_{p,a,q} (z \in X_{p,a,q}) \wedge \gamma(q)\big)\end{aligned}$$

where $(x \in X) \to s \stackrel{\text{def}}{=} \neg(x \in X) \vee ((x \in X) \wedge s)$, $\min(y) \stackrel{\text{def}}{=} \forall x. y \leqslant x$, and $\max(z) \stackrel{\text{def}}{=} \forall x. x \leqslant z$. For

$$\begin{aligned}\xi &\stackrel{\text{def}}{=} \exists \overline{X}. \phi(\overline{X}) \\ \zeta &\stackrel{\text{def}}{=} (\lambda \cdot \gamma) \wedge \forall x. \mathbb{0}\end{aligned}$$

we have

$$\|\mathcal{A}\| = [\![\zeta \vee \xi]\!] .$$

As $\zeta \vee \xi \in \mathrm{wRMSO}(\mathbb{S}, A)$, this concludes the proof of (2) $\Longrightarrow$ (1) in Theorem 7.12.

Exercises for Chapter 7

Exercise 7.1. Let $A = \{a, b\}$. Determine semirings $\mathbb{S}_i$ and sentences $\phi_i \in \mathrm{wMSO}(\mathbb{S}_i, A)$, $i = 1, 2$, such that, for all $w = a_1 \dots a_n \in A^*$,

- $[\![\phi_1]\!](w) = |\{i \in \{1, \dots, n-1\} \mid a_i a_{i+1} = ab\}|$.
- $[\![\phi_2]\!](w) = \{u \in A^* \mid u \text{ is an infix of } w\}$.

Hint: Note that $\mathbb{S}_2$ is not commutative. For the universal quantification, the product over the positions $\{1, \dots, n\}$ of w should follow the natural ordering $1 \leqslant \dots \leqslant n$.

Exercise 7.2. Let $A = \{a, b\}$. Determine a sentence $\phi \in \mathrm{wRMSO}(\mathbb{N}\mathrm{at}, A)$ such that $[\![\phi]\!]$ is not definable by a sentence without existential set quantification.

Further reading and references

[Büc60] J. R. Büchi. "Weak second-order arithmetic and finite automata". In: *Z. Math. Logik Grundlagen Math.* 6 (1960), pp. 66–92 (cit. on pp. 41–42).

[DG07] M. Droste and P. Gastin. "Weighted automata and weighted logics". In: *Theor. Comp. Sci.* 380.1-2 (2007). Special issue of ICALP'05., pp. 69–86 (cit. on pp. 41, 44–45).

[DG09] M. Droste and P. Gastin. "Weighted automata and weighted logics". In: *Handbook of Weighted Automata*. Ed. by W. Kuich, H. Vogler, and M. Droste. EATCS Monographs in Theoretical Computer Science. Springer, 2009 (cit. on pp. 41, 44–45).

[Elg61] C. C. Elgot. "Decision problems of finite automata design and related arithmetics". In: *Trans. Amer. Math. Soc.* 98 (1961), pp. 21–52 (cit. on pp. 41–42).

List of references

[Abd+04] P. Aziz Abdulla et al. "A Survey of Regular Model Checking." In: *Proc. of CONCUR'04*. Vol. 3170. Lect. Notes Comp. Sci. Springer, 2004, pp. 35–48.

[AD94] R. Alur and D. L. Dill. "A Theory of Timed Automata." In: *Theor. Comp. Sci.* 126.2 (1994), pp. 183–235.

[AHK03] S. Andova, H. Hermanns, and J. P. Katoen. "Discrete-time rewards model-checked". In: *Proc. of FORMATS'03*. Vol. 2791. Lect. Notes Comp. Sci. Springer, 2003, pp. 88–104.

[Aks+08] S. Akshay et al. "Distributed Timed Automata with Independently Evolving Clocks". In: *Proc. of CONCUR'08*. Vol. 5201. Lect. Notes Comp. Sci. Springer, 2008, pp. 82–97. DOI: 10.1007/978-3-540-85361-9_10.

[Alf+05] L. de Alfaro et al. "Model checking discounted temporal properties". In: *Theor. Comp. Sci.* 345.1 (2005), pp. 139–170.

[Alf98] L. de Alfaro. *Formal Verification of Probabilistic Systems*. Tech. rep. PhD thesis. Stanford University, 1998.

[BBG08] Ch. Baier, N. Bertrand, and M. Größer. "On Decision Problems for Probabilistic Büchi Automata". In: *Proc. of FoSSaCS'08*. Vol. 4962. Lect. Notes Comp. Sci. Springer, 2008, pp. 287–301.

[BC08] V.D. Blondel and V. Canterini. "Undecidable problems for probabilistic automata of fixed dimension". In: *Theory of Computing systems* 36.3 (2008), pp. 231–245.

[Ber79] J. Berstel. *Transductions and context-free languages*. Teubner Stuttgart, 1979.

[BG05] C. Baier and M. Größer. "Recognizing ω-regular Languages with Probabilistic Automata". In: *Proc. of LICS'05*. IEEE Computer Society Press, 2005, pp. 137–146.

[BK08] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking (Representation and Mind Series)*. The MIT Press, 2008. ISBN: 026202649X, 9780262026499.

[BK09] P. Buchholz and P. Kemper. "Model Checking for a Class of Weighted Automata". In: *Discrete Event Dynamic Systems* (2009). to appear. DOI: 10.1007/s10626-008-0057-0.

[BL04] B. Bollig and M. Leucker. "Verifying Qualitative Properties of Probabilistic Programs". In: *Validation of Stochastic Systems*. Vol. 2925. Lect. Notes Comp. Sci. Springer, 2004, pp. 124–146.

[BMT09] A. Bertoni, G. Mauri, and M. Torelli. "Some Recursively Unsolvable Problems Relating to Isolated Cutpoints in Probabilistic Automata." In: *Proc. of ICALP'77*. Vol. 52. Lect. Notes Comp. Sci. Springer, Sept. 19, 2009, pp. 87–94. ISBN: 3-540-08342-1. URL: http://dblp.uni-trier.de/db/conf/icalp/icalp77.html#BertoniMT77.

[Bou+08] P. Bouyer et al. "Infinite Runs in Weighted Timed Automata with Energy Constraints". In: *Proceedings of FORMATS'08*. Vol. 5215. Lect. Notes Comp. Sci. Springer, 2008, pp. 33–47.

[BR11] J. Berstel and Ch. Reutenauer. *Noncommutative rational series with applications*. Vol. 137. Encyclopedia of Mathematics and Its Applications. Preliminary version at http://tagh.de/tom/wp-content/uploads/berstelreutenauer2008.pdf. Cambridge University Press, 2011.

[BR88] J. Berstel and Ch. Reutenauer. *Rational series and their languages*. Springer, 1988.

[Büc60] J. R. Büchi. "Weak second-order arithmetic and finite automata". In: *Z. Math. Logik Grundlagen Math.* 6 (1960), pp. 66–92.

[Büc62] J. R. Büchi. "On a decision method in restricted second order arithmetic". In: *Proc. of the International Congress on Logic, Methodology and Philosophy*. Standford University Press, 1962, pp. 1–11.

[CDH08] K. Chatterjee, L. Doyen, and T. A. Henzinger. "Quantitative Languages". In: *Proc. of CSL'08*. Vol. 5213. Lect. Notes Comp. Sci. Springer, 2008, pp. 385–400.

[CE81] E. M. Clarke and E. A. Emerson. "Design and Synthesis of Synchronization Skeletons using Branching Time Temporal Logic". In: *Proc. of the Workshop on Logics of Programs*. Vol. 131. Lect. Notes Comp. Sci. Springer, 1981, pp. 52–71.

[CG04] F. Ciesinski and M. Größer. "On Probabilistic Computation Tree Logic". In: *Validation of Stochastic Systems*. Vol. 2925. Lect. Notes Comp. Sci. Springer, 2004, pp. 147–188.

[CGP99] E. M. Clarke, O. Grumberg, and D. Peled. *Model Checking*. Cambridge, Massachusetts: The MIT Press, 1999.

[Cho04] Ch. Choffrut. "Rational Relations as Rational Series". In: *Theory Is Forever, Essays Dedicated to Arto Salomaa on the Occasion of His 70th Birthday*. Vol. 3113. Lect. Notes Comp. Sci. Springer, 2004, pp. 29–34.

[Cho09] Ch. Choffrut. *A short introductory course to rational relations*. 2009.

[CK93] K. Culik and J. Kari. "Image compression using weighted finite automata". In: *Computer and Graphics* 17.3 (1993), pp. 305–313.

[Cor+09] Th. H. Cormen et al. *Introduction to Algorithms*. 3rd. McGraw-Hill Higher Education, 2009.

[CY95] C. Courcoubetis and M. Yannakakis. "The Complexity of Probabilistic Verification". In: *Journal of the ACM* 42.4 (1995), pp. 857–907.

[DG07] M. Droste and P. Gastin. "Weighted automata and weighted logics". In: *Theor. Comp. Sci.* 380.1-2 (2007). Special issue of ICALP'05., pp. 69–86.

[DG09] M. Droste and P. Gastin. "Weighted automata and weighted logics". In: *Handbook of Weighted Automata*. Ed. by W. Kuich, H. Vogler, and M. Droste. EATCS Monographs in Theoretical Computer Science. Springer, 2009.

[DKV09] M. Droste, W. Kuich, and W. Vogler. *Handbook of Weighted Automata*. Springer, 2009.

[DMR76] M. Davis, Y. V. Matijasevič, and J. Robinson. "Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution". In: *Mathematical Developments Arising from Hilbert Problems*. Vol. 28. Proc. of Symposia in Pure Mathematics. Providence, Rhode Island: American Mathematical Society, 1976, pp. 323–378.

[DR07] M. Droste and G. Rahonis. "Weighted Automata and Weighted Logics with Discounting". In: *Proc. of CIAA'07*. Vol. 4783. Lect. Notes Comp. Sci. Springer, 2007, pp. 73–84.

[DV06] M. Droste and H. Vogler. "Weighted tree automata and weighted logics". In: *Theor. Comp. Sci.* 366.3 (2006), pp. 228–247.

[Eis01] J. Eisner. "Expectation Semirings: Flexible EM for Learning Finite-State Transducers". In: *Proc. of the ESSLLI workshop on finite-state methods in NLP*. 2001.

[Elg61] C. C. Elgot. "Decision problems of finite automata design and related arithmetics". In: *Trans. Amer. Math. Soc.* 98 (1961), pp. 21–52.

[FGK09] D. Fischer, E. Grädel, and L. Kaiser. "Model Checking Games for the Quantitative μ-Calculus". In: *Theory of Computing Systems* (2009). Special Issue of STACS'08.

[Gim10] Y. Gimbert H.and Oualhadj. "Probabilistic Automata on Finite Words: Decidable and Undecidable Problems". In: *Proc. of ICALP'10*. Vol. 6199. Lect. Notes Comp. Sci. Springer, 2010, pp. 527–538. URL: http://hal.archives-ouvertes.fr/hal-00456538/en/.

[Gr06] M. Größer et al. "On reduction criteria for probabilistic reward models". In: *Proc. of FSTTCS'06*. Vol. 4337. Lect. Notes Comp. Sci. Springer, 2006, pp. 309–320.

[GSS95] R. J. van Glabbeek, S. A. Smolka, and B. Steffen. "Reactive, Generative and Stratified Models of Probabilistic Processes". In: *Information and Computation* 121.1 (1995), pp. 59–80.

[HJ94] H. Hansson and B. Jonsson. "A Logic for Reasoning about Time and Reliability". In: *Formal Aspects of Computing* 6.5 (1994), pp. 512–535.

[Kar+04] J. Karhumäki et al., eds. *Theory Is Forever, Essays Dedicated to Arto Salomaa on the Occasion of His 70th Birthday*. Vol. 3113. Lect. Notes Comp. Sci. Springer, 2004. ISBN: 3-540-22393-2.

[Kir05] Daniel Kirsten. "Distance desert automata and the star height problem". In: *RAIRO Inform. Théor. Appl.* 39.3 (2005), pp. 455–509. ISSN: 0988-3754.

[Kno90] K. Knopp. *Theory and Application of Infinite Series*. Republication of the second English edition, 1951. New York: Dover Publications, 1990.

[Koz83] D. Kozen. "Results on the Propositional μ-calculus". In: *Theor. Comp. Sci.* 27 (1983), pp. 333–354.

[Kro94] D. Krob. "The equality problem for rational series with multiplicities in the tropical semiring is undecidable". In: *Int. J. of Algebra and Comput.* 4.3 (1994), pp. 405–425.

[KS60] J. G. Kemeny and J. L. Snell. *Finite Markov Chains*. New York: Van Nostrand Reinhold, 1960.

[KS85] W. Kuich and A. Salomaa. *Semirings, Automata and Languages*. Springer, 1985.

[LP04] Hing Leung and Viktor Podolskiy. "The limitedness problem on distance automata: Hashiguchi's method revisited". In: *Theor. Comp. Sci.* 310.1-3 (2004), pp. 147–158.

[Mat93] Y. V. Matijasevič. *Hilbert's Tenth Problem*. Cambridge, Massachusetts: MIT Press, 1993. ISBN: 0-262-13295-8.

[Mei09] I. Meinecke. "A weighted μ-calculus on words". In: *Proceedings of DLT'09*. Vol. 5583. Lect. Notes Comp. Sci. Springer, 2009.

[MHC03] O. Madani, S. Hanks, and A. Condon. "On the undecidability of probabilistic planning and related stochastic optimization problems". In: *Artificial Intelligence* 147.1-2 (2003), pp. 5–34.

[Min67] Marvin L. Minsky. *Computation: finite and infinite machines*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1967. ISBN: 0-13-165563-9.

[Moh02] M. Mohri. "Semiring frameworks and algorithms for shortest-distance problems". In: *Journal of Automata, Languages, and Combinatorics* 7.3 (2002), pp. 321–350. ISSN: 1430-189X.

[Moh97] M. Mohri. "Finite-state transducers in language and speech processing". In: *Computational Linguistics* 23.2 (1997), pp. 269–311.

[Paz71] A. Paz. *Introduction to probabilistic automata*. Academic Press, 1971.

[Pnu77] A. Pnueli. "The temporal logic of programs". In: *Proc. of FOCS'77*. IEEE Computer Society Press, 1977, pp. 46–57.

[Put94] M. L. Puterman. *Markov Decision Processes*. New York, NY: John Wiley & Sons, Inc., 1994.

[PZ93] A. Pnueli and L. D. Zuck. "Probabilistic Verification". In: *Information and Computation* 103.1 (1993), pp. 1–29.

[Rab63] M. O. Rabin. "Probabilistic automata". In: *Information and Control* 6 (3 1963), pp. 230–245.

[Sak09] J. Sakarovitch. *Elements of Automata Theory*. New York, NY, USA: Cambridge University Press, 2009. ISBN: 0521844258, 9780521844253.

[Sch61] M.-P Schützenberger. "On the definition of a family of automata". In: *Information and Control* 4 (1961), pp. 245–270.

[Seg06] R. Segala. "Probability and Nondeterminism in Operational Models of Concurrency". In: *Proceedings of CONCUR'06*. Vol. 4137. Lect. Notes Comp. Sci. Springer, 2006, pp. 64–78.

[Sim94] Imre Simon. "On Semigroups of Matrices over the Tropical Semiring". In: *ITA* 28.3-4 (1994), pp. 277–294.

[SS78] A. Salomaa and M. Soittola. *Automata-theoretic aspects of formal power series*. Springer, 1978.

[Tho97] W. Thomas. "Languages, Automata and Logic". In: *Handbook of Formal Languages*. Ed. by A. Salomaa and G. Rozenberg. Vol. 3, Beyond Words. Springer, 1997, pp. 389–455.

[Tze92] W.G. Tzeng. "A polynomial-time algorithm for the equivalence of probabilistic automata". In: *SIAM J. Comput.* 21 (1992), pp. 216–227.

[Var85] M. Y. Vardi. "Automatic Verification of Probabilistic Concurrent Finite-State Programs". In: *Proc. of FOCS'85*. IEEE, 1985, pp. 327–338.

[Var99] M. Y. Vardi. "Probabilistic Linear-Time Model Checking: An Overview of the Automata-Theoretic Approach". In: *Formal Methods for Real-Time and Probabilistic Systems, 5th International AMAST Workshop, ARTS'99*. Vol. 1601. Lect. Notes Comp. Sci. Springer, 1999, pp. 265–276.