The Value 1 Problem for Probabilistic Automata

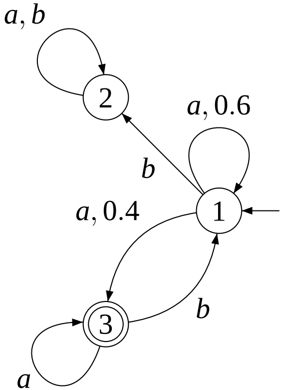
FREC Final Conference

Nathanaël Fijalkow

LIAFA, Université Denis Diderot - Paris 7, France
Institute of Informatics, Warsaw University, Poland
nath@liafa.univ-paris-diderot.fr

April 28th, 2014

Probabilistic automata (Rabin, 1963)



$$\mathbb{P}_{\mathcal{A}} : A^* \to [0, 1]$$

$\mathbb{P}_{\mathcal{A}}(w)$ is the probability that a run for w ends up in F

The value 1 problem

This talk is about the value 1 problem:

INPUT: $\mathcal{A}$ a probabilistic automaton
OUTPUT: for all $\varepsilon > 0$, there exists $w \in A^*$, $\mathbb{P}_{\mathcal{A}}(w) \geq 1 - \varepsilon$.

The value 1 problem

This talk is about the value 1 problem:

INPUT: $\mathcal{A}$ a probabilistic automaton
OUTPUT: for all $\varepsilon > 0$, there exists $w \in A^*$, $\mathbb{P}_{\mathcal{A}}(w) \geq 1 - \varepsilon$.

It is undecidable (Gimbert and Oualhadj, 2010).

But *to what extent*?

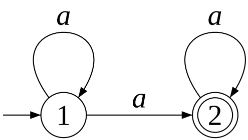
Objective

Construct an algorithm to decide the value 1 problem,
which is *often* correct.

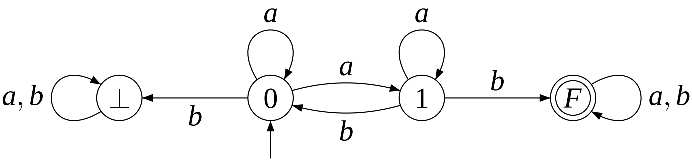
Objective

Construct an algorithm to decide the value 1 problem,
which is *often* correct.

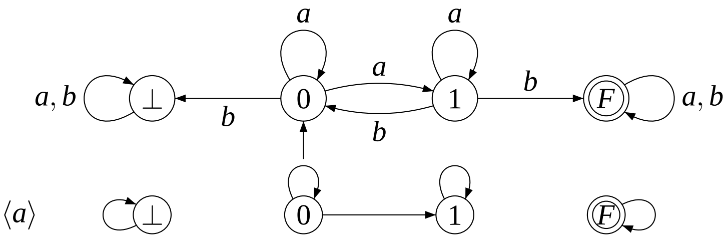
We project $(\mathbb{R}, +, \cdot)$ into the boolean semiring $(\{0, 1\}, \vee, \wedge)$.



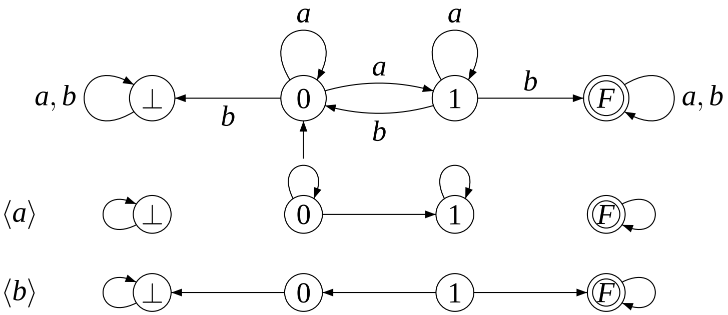
An example



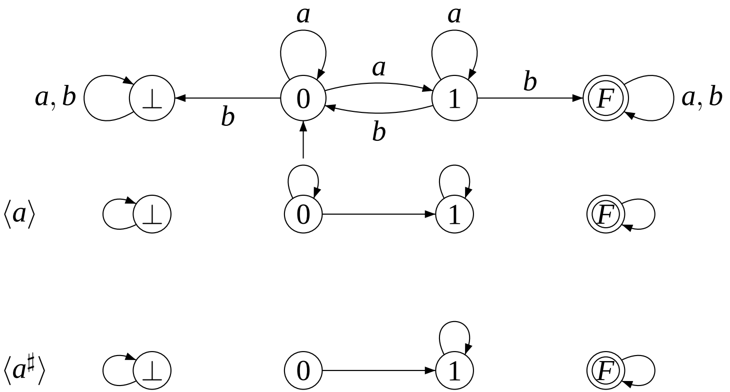
An example



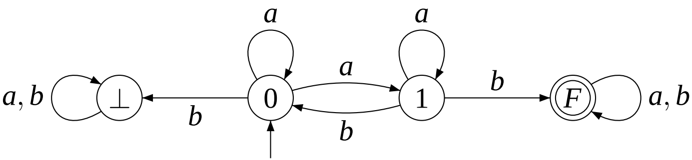
An example



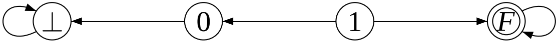
An example



An example



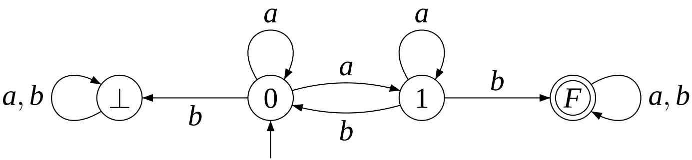
$\langle b \rangle$



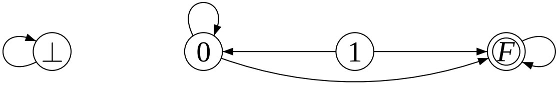
$\langle a^{\sharp} \rangle$

$\langle a^{\sharp} \cdot b \rangle$

An example

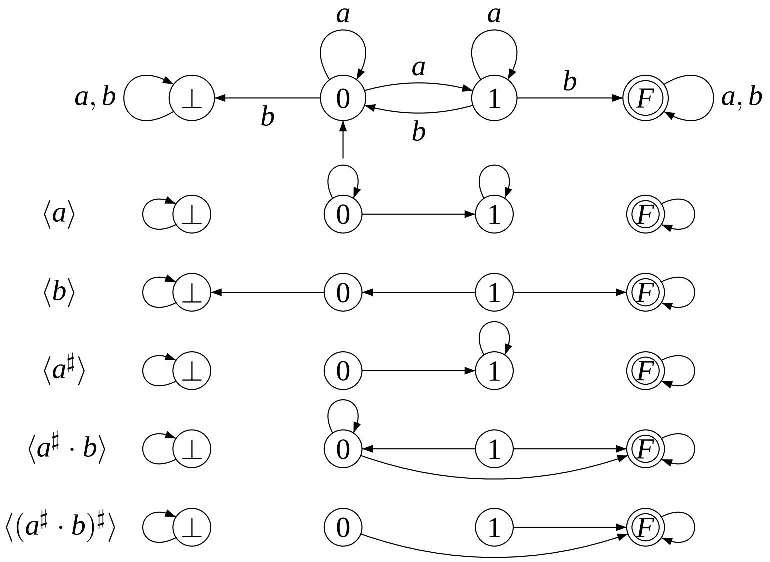


$\langle a^\sharp \cdot b \rangle$



$\langle (a^\sharp \cdot b)^\sharp \rangle$

An example



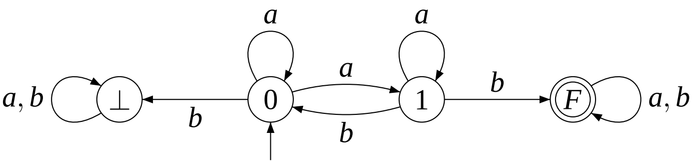
a
a
a
b
a, b
$\perp$
b
0
1
F
a, b
b
$\langle a \rangle$
$\langle b \rangle$
$\langle a^\sharp \rangle$
$\langle a^\sharp \cdot b \rangle$
$\langle (a^\sharp \cdot b)^\sharp \rangle$

Stabilization monoids (Colcombet)

This is an algebraic structure with two operations:

- binary composition
- stabilization, denoted $\sharp$.

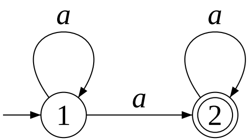
Boolean matrices representations



$$\langle a \rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \langle b \rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$I \cdot \langle u \rangle \cdot F = 1 \quad \text{if and only if} \quad \mathbb{P}_{\mathcal{A}}(u) > 0$$

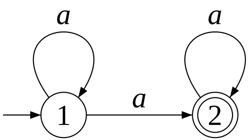
Defining stabilization



$$\langle a \rangle = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

In $\langle a \rangle$, the state 1 is transient and the state 2 is recurrent.

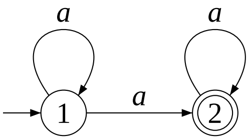
Defining stabilization



$$\langle a \rangle = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \langle a^\sharp \rangle = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

In $\langle a \rangle$, the state 1 is transient and the state 2 is recurrent.

Defining stabilization



$$\langle a \rangle = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \langle a^\sharp \rangle = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

In $\langle a \rangle$, the state 1 is transient and the state 2 is recurrent.

$$M^\sharp(s,t) = \begin{cases} 1 & \text{if } M(s,t) = 1 \text{ and } t \text{ recurrent in } M, \\ 0 & \text{otherwise.} \end{cases}$$

The Markov Monoid Algorithm

Compute a monoid inside the **finite** monoid $\mathcal{M}_{Q\times Q}(\{0,1\},\vee,\wedge)$.

- Compute $\langle a\rangle$ for $a \in A$:

$$\langle a\rangle(s,t) = \begin{cases} 1 & \text{if } \mathbb{P}_{\mathcal{A}}(s \xrightarrow{a} t) > 0, \\ 0 & \text{otherwise.} \end{cases}$$

- Close under product and stabilization.

The Markov Monoid Algorithm

Compute a monoid inside the **finite** monoid $\mathcal{M}_{Q\times Q}(\{0,1\},\vee,\wedge)$.

- Compute $\langle a\rangle$ for $a \in A$:

$$\langle a\rangle(s,t) = \begin{cases} 1 & \text{if } \mathbb{P}_{\mathcal{A}}(s \xrightarrow{a} t) > 0, \\ 0 & \text{otherwise.} \end{cases}$$

- Close under product and stabilization.
- If there exists a matrix M such that

$$\forall t \in Q, \quad M(s_0,t) = 1 \Rightarrow t \in F$$

then "$\mathcal{A}$ has value 1", otherwise "$\mathcal{A}$ does not have value 1".

Correctness

Theorem

If there exists a matrix M such that

$$\forall t \in Q, \quad M(s_0, t) = 1 \Rightarrow t \in F$$

then $\mathcal{A}$ *has value* 1.

Correctness

Theorem

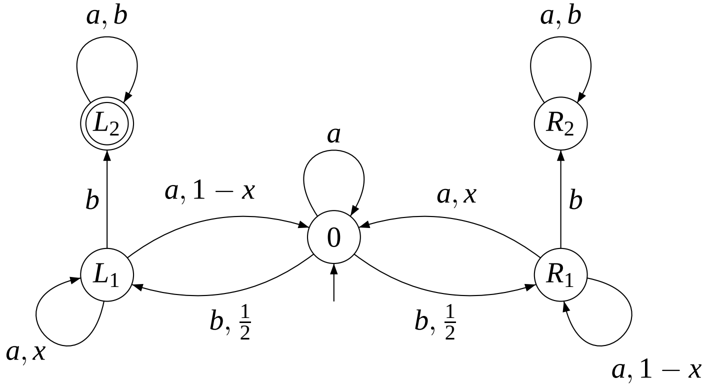
If there exists a matrix M such that

$$\forall t \in Q, \quad M(s_0, t) = 1 \Rightarrow t \in F$$

then $\mathcal{A}$ has value 1.

But the value 1 problem is undecidable, so…

No completeness

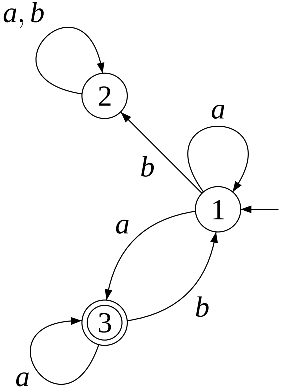


Left and right parts are symmetric, so for all M:

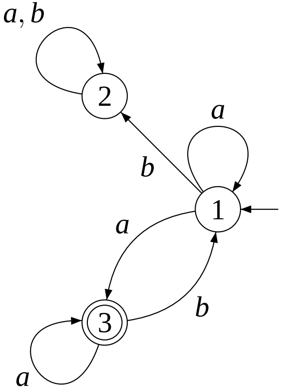
$$M(0, L_2) = 1 \iff M(0, R_2) = 1.$$

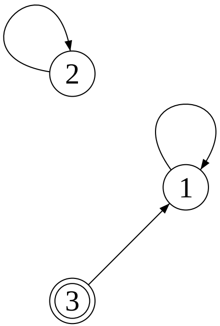
Yet: it has value 1 if and only if $x > \frac{1}{2}$.

A leak



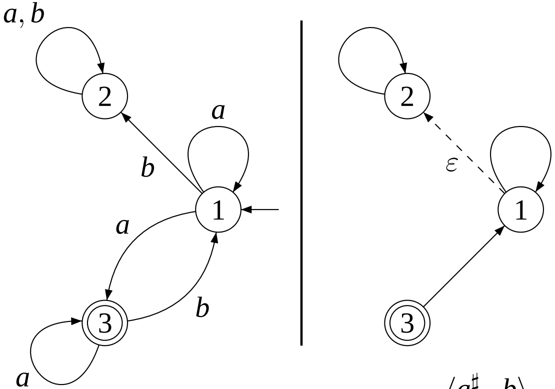
A leak





$\langle a^\sharp \cdot b \rangle$

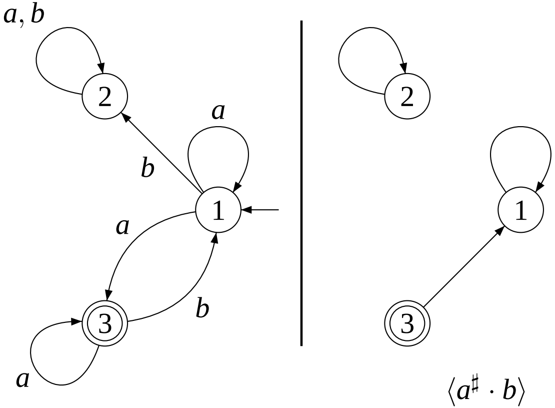
A leak



$\langle a^{\sharp} \cdot b \rangle$

There is a leak from 1 to 2.

A leak



There is a leak from 1 to 2.

Definition

An automaton $\mathcal{A}$ is leaktight if it has no leak.

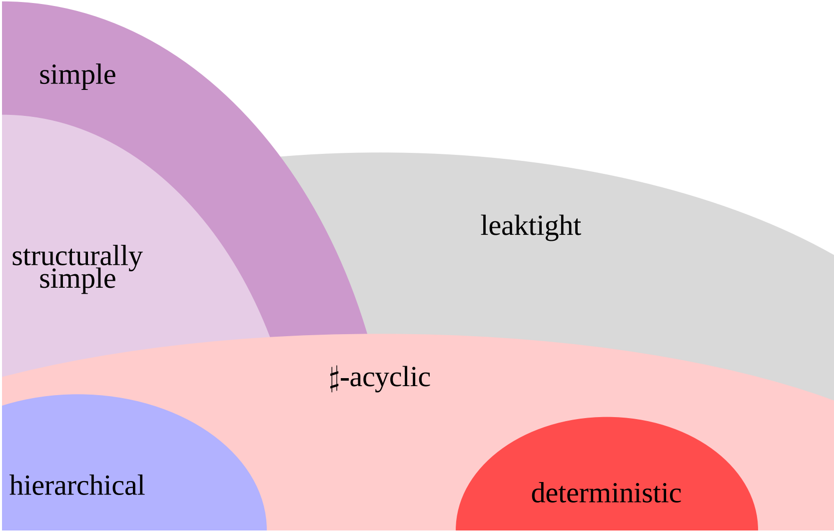
Leaktight automata

Theorem (F.,Gimbert and Oualhadj 2012)

The algorithm is complete for leaktight automata.
Hence, the value 1 *problem is decidable for leaktight automata.*

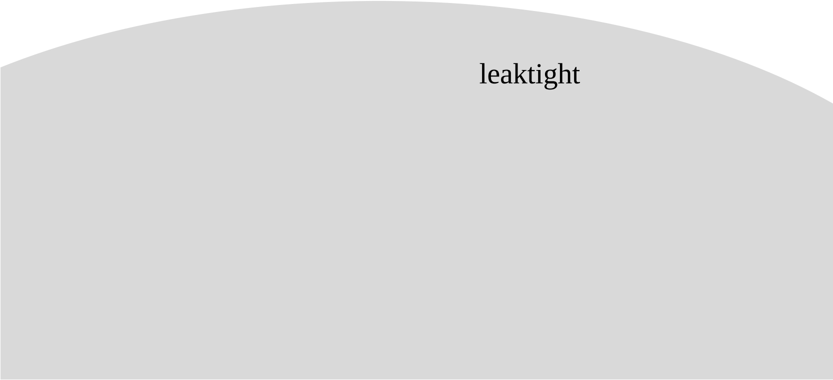
The proof relies on Simon's factorization forest theorem.

Other decidable subclasses: in 2012



Other decidable subclasses: today

(F.,Gimbert,Kelmendi and Oualhadj 2013)

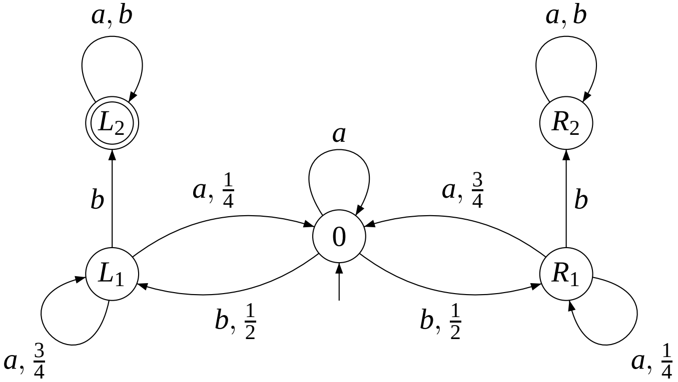


So far,
the Markov Monoid Algorithm is
the *most correct* algorithm known
to solve the value 1 problem.

So far,
the Markov Monoid Algorithm is
the *most correct* algorithm known
to solve the value 1 problem.

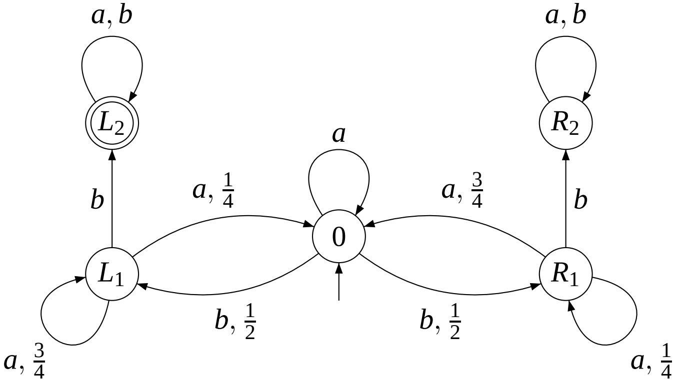
But for *how long*?

What it misses: different convergence speeds



$$\lim_n \mathbb{P}_{\mathcal{A}}\left(b(a^n b)^{f(n)}\right) = 1 \text{ if and only if } \lim_n f(n) \cdot \left(\frac{3}{4}\right)^n = \infty\ ,$$

What it misses: different convergence speeds



$$\lim_n \mathbb{P}_{\mathcal{A}}\left(b(a^n b)^{f(n)}\right) = 1 \text{ if and only if } \lim_n f(n) \cdot \left(\frac{3}{4}\right)^n = \infty ,$$

so $f(n) = 2^n$ works but $f(n) = n$ does not.

An answer through profinite techniques

$\widetilde{A^*}$ is the space of profinite probabilistic words.

$$A^* = \widetilde{A^*}[0] \subsetneq \widetilde{A^*}[1] \subsetneq \widetilde{A^*}[2] \subsetneq \cdots \subsetneq \widetilde{A^*} .$$

Lemma

The following are equivalent:

- *The value* 1 *problem over finite words,*
- *The emptiness problem over profinite probabilistic words.*

An answer through profinite techniques

$\widetilde{A^*}$ is the space of profinite probabilistic words.

$$A^* = \widetilde{A^*}[0] \subsetneq \widetilde{A^*}[1] \subsetneq \widetilde{A^*}[2] \subsetneq \cdots \subsetneq \widetilde{A^*} .$$

Lemma

The following are equivalent:

- *The value* 1 *problem over finite words,*
- *The emptiness problem over profinite probabilistic words.*

Theorem

1. *The Markov Monoid Algorithm answers "YES" if and only if there exists $x \in \widetilde{A^*}[1]$ accepted by $\mathcal{A}$,*
2. *The following problem is undecidable: determine whether there exists $x \in \widetilde{A^*}[2]$ accepted by $\mathcal{A}$.*

An equivalent characterization

Theorem

The Markov Monoid Algorithm answers "YES" if and only if there exists $(u_n)_{n \in \mathbb{N}}$ *a sequence of finite words such that:*

1. $(u_n)_{n \in \mathbb{N}}$ *is of polynomial growth, i.e.* $|u_n| \leq P(n)$ *for some polynomial* P*,*
2. $(\mathbb{P}_{\mathcal{A}}(u_n))_{n \in \mathbb{N}}$ *converges exponentially fast to* 1*, i.e.*

$$\mathbb{P}_{\mathcal{A}}(u_n) \geq 1 - P(n) \cdot C^{-n} \ ,$$

for some polynomial P *and constant* $C > 1$*.*

In *some* sense,

the Markov Monoid Algorithm is
the *most correct* algorithm
to solve the value 1 problem.

In *some* sense,

the Markov Monoid Algorithm is
the *most correct* algorithm
to solve the value 1 problem.

Thanks for your attention!