Algebraic Algorithms for Probabilistic Automata

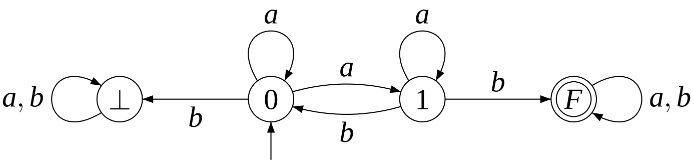
ONERA, Toulouse

Nathanaël Fijalkow

LIAFA, Université Denis Diderot - Paris 7, France
Institute of Informatics, Warsaw University, Poland

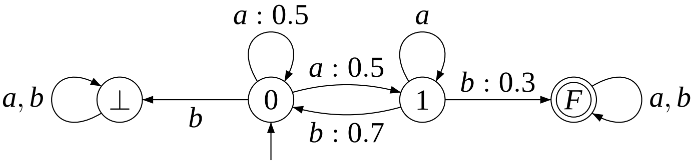
January 26th, 2015

Non-deterministic Automata



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

Probabilistic Automata



$$\langle a \rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \langle b \rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0.7 & 0 & 0.3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Let $u = abaaba$.

$$\mathbb{P}_{\mathcal{A}}(u) = I \cdot \underbrace{\langle a \rangle \cdot \langle b \rangle \cdot \langle a \rangle \cdot \langle a \rangle \cdot \langle b \rangle \cdot \langle a \rangle}_{\langle u \rangle} \cdot F$$

Everything boils down to matrix multiplications!

Algorithmic Properties of Probabilistic Automata

$$L^{>\frac{1}{2}}(\mathcal{A}) = \{w \in A^* \mid \mathbb{P}_{\mathcal{A}}(w) > \frac{1}{2}\}$$

1. *Emptiness*: $L^{>\frac{1}{2}}(\mathcal{A}) = \emptyset$?
2. *Universality*: $L^{>\frac{1}{2}}(\mathcal{A}) = A^*$?
3. *Equivalence*: is it true that for all words $w \in A^*$, we have $\mathbb{P}_{\mathcal{A}}(w) = \mathbb{P}_{\mathcal{B}}(w)$?
4. *Regularity*: is the language $L^{>\frac{1}{2}}(\mathcal{A}) =$ regular?
5. *Value*: is the value $\mathrm{val}(\mathcal{A}) = \sup_{w \in A^*} \mathbb{P}_{\mathcal{A}}(w)$ computable? Approximable?
6. *Value 1*: is it true that $\mathrm{val}(\mathcal{A}) = 1$?

Algorithmic Properties of Probabilistic Automata

$$L^{>\frac{1}{2}}(\mathcal{A}) = \{w \in A^* \mid \mathbb{P}_{\mathcal{A}}(w) > \frac{1}{2}\}$$

1. *Emptiness*: $L^{>\frac{1}{2}}(\mathcal{A}) = \emptyset$?
2. *Universality*: $L^{>\frac{1}{2}}(\mathcal{A}) = A^*$?
3. *Equivalence*: is it true that for all words $w \in A^*$, we have $\mathbb{P}_{\mathcal{A}}(w) = \mathbb{P}_{\mathcal{B}}(w)$?
4. *Regularity*: is the language $L^{>\frac{1}{2}}(\mathcal{A}) =$ regular?
5. *Value*: is the value $\mathrm{val}(\mathcal{A}) = \sup_{w \in A^*} \mathbb{P}_{\mathcal{A}}(w)$ computable? Approximable?
6. *Value 1*: is it true that $\mathrm{val}(\mathcal{A}) = 1$?

We would like to finitely represent

$$\{\langle w \rangle \mid w \in A^*\}$$

Negative Results

Theorem (Results from 1963 to 2010)

- *The Emptiness, Universality, Regularity and Value* 1 *problems are undecidable.*
- *The Value cannot be computed, nor approximated, even up to the constant* $\frac{1}{6}$.

Theorem (Results from 1963 to 2010)

- *The Emptiness, Universality, Regularity and Value* 1 *problems are undecidable.*
- *The Value cannot be computed, nor approximated, even up to the constant* $\frac{1}{6}$.

It is hard to accurately represent

$$\{\langle w \rangle \mid w \in A^*\}$$

Positive Results

Theorem (Schützenberg 61)

The Equivalence problem is decidable in polynomial time.

Indeed:

$$\forall w \in A^*, \quad \mathbb{P}_{\mathcal{A}}(w) = \mathbb{P}_{\mathcal{B}}(w)$$

$$\Longleftrightarrow$$

$$\forall w \in A^{\leq |\mathcal{A}|+|\mathcal{B}|}, \quad \mathbb{P}_{\mathcal{A}}(w) = \mathbb{P}_{\mathcal{B}}(w)$$

Positive Results

Theorem (Schützenberg 61)

The Equivalence problem is decidable in polynomial time.

Indeed:

$$\forall w \in A^*, \quad \mathbb{P}_{\mathcal{A}}(w) = \mathbb{P}_{\mathcal{B}}(w)$$

$$\Longleftrightarrow$$

$$\forall w \in A^{\leq |\mathcal{A}|+|\mathcal{B}|}, \quad \mathbb{P}_{\mathcal{A}}(w) = \mathbb{P}_{\mathcal{B}}(w)$$

$\looparrowright$ The best (randomized) algorithm is to pick small words at random and to check the equality.

The Value 1 Problem

Is the value $\mathrm{val}(\mathcal{A}) = \sup_{w \in A^*} \mathbb{P}_{\mathcal{A}}(w)$ equal to 1?

Equivalently:

Is it true that for all $\varepsilon > 0$,
there exists $w \in A^*$ such that $\mathbb{P}_{\mathcal{A}}(w) \geq 1 - \varepsilon$?

The Value 1 Problem

Is the value $\mathrm{val}(\mathcal{A}) = \sup_{w \in A^*} \mathbb{P}_{\mathcal{A}}(w)$ equal to 1?

Equivalently:

Is it true that for all $\varepsilon > 0$,
there exists $w \in A^*$ such that $\mathbb{P}_{\mathcal{A}}(w) \geq 1 - \varepsilon$?

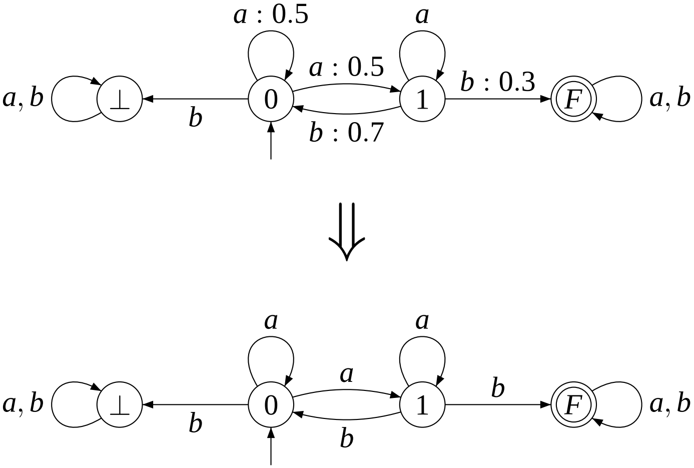
This is undecidable,

but we can construct an algorithm

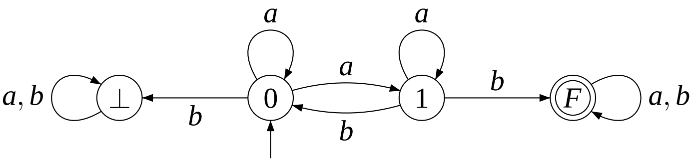
which is *often* correct!

The virtues of the Markov Monoid algorithm

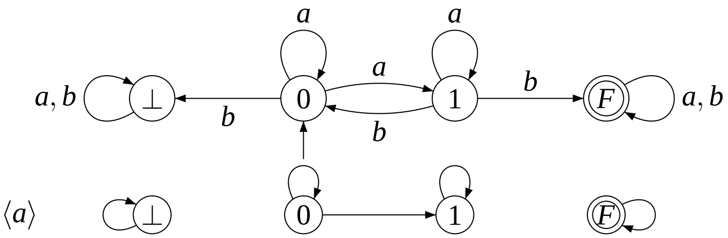
No numerical values



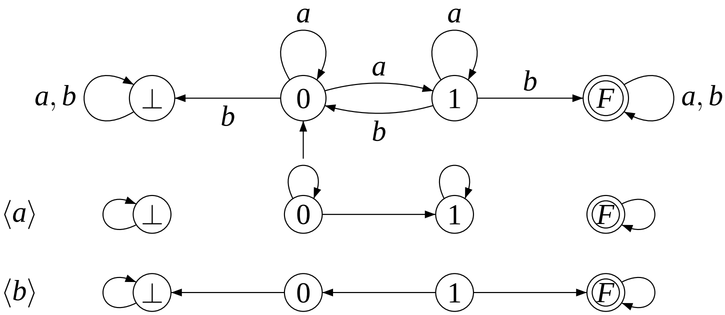
An example



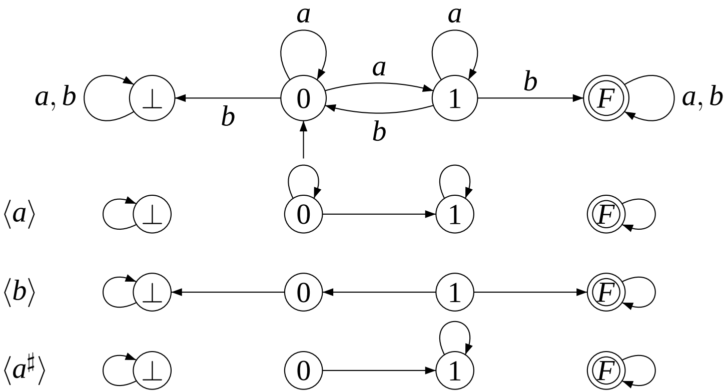
An example



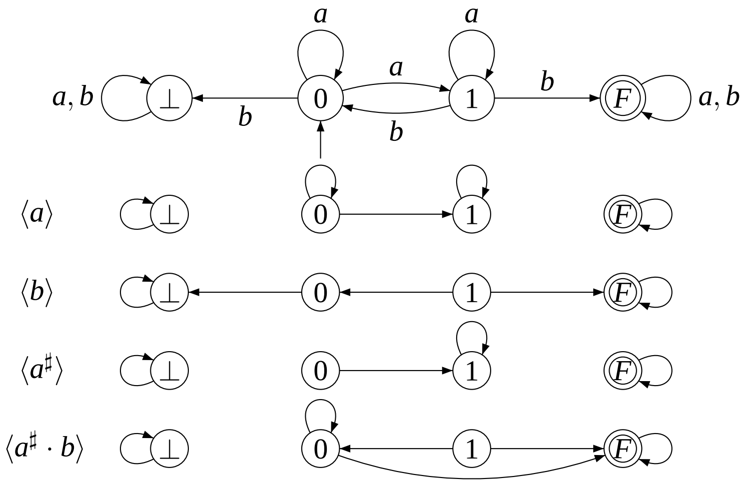
An example



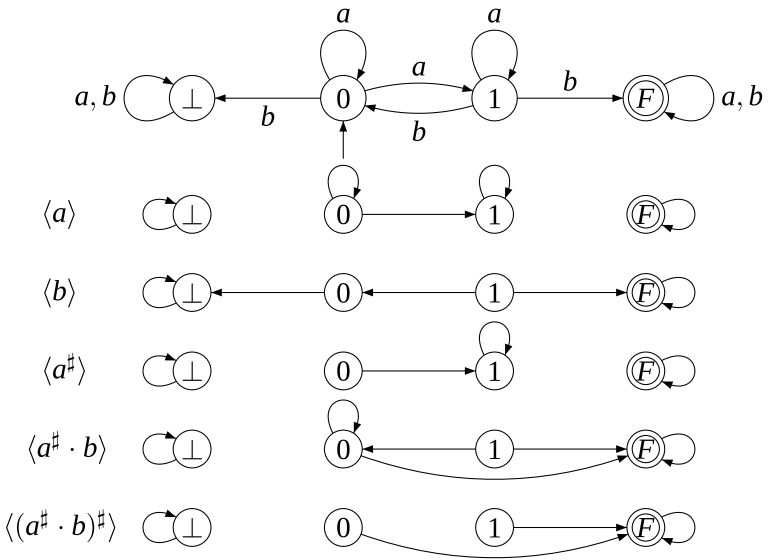
An example



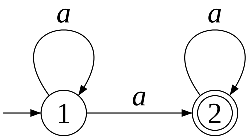
An example



An example



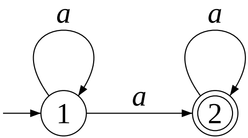
Defining stabilization



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

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

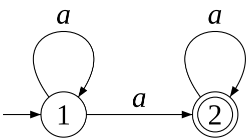
Defining stabilization



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

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.

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

Markov Monoid of an Automaton

Matrix multiplication $\longleftrightarrow$ concatenation

Markov Monoid of an Automaton

Matrix multiplication $\longleftrightarrow$ concatenation

Stabilization $\longleftrightarrow$ limit of the powers

$\langle u \rangle^\sharp$ represents $\lim_n \langle u^n \rangle$

Markov Monoid of an Automaton

Matrix multiplication $\longleftrightarrow$ concatenation

Stabilization $\longleftrightarrow$ limit of the powers

$\langle u \rangle^\sharp$ represents $\lim_n \langle u^n \rangle$

Definition

The Markov Monoid of $\mathcal{A}$ is the closure of $\{\langle a \rangle \mid a \in A\}$ under multiplication and stabilization.

The Markov Monoid of $\mathcal{A}$ contains a lot of information about $\mathcal{A}$!

Value 1 Witnesses

Definition

M is a value 1 witness if

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

If there exists a value 1 witness,
then the algorithm answers "$\mathcal{A}$ has value 1",
otherwise "$\mathcal{A}$ does not have value 1".

Correctness

Theorem

If there exists a value 1 *witness, then* $\mathcal{A}$ *has value* 1.

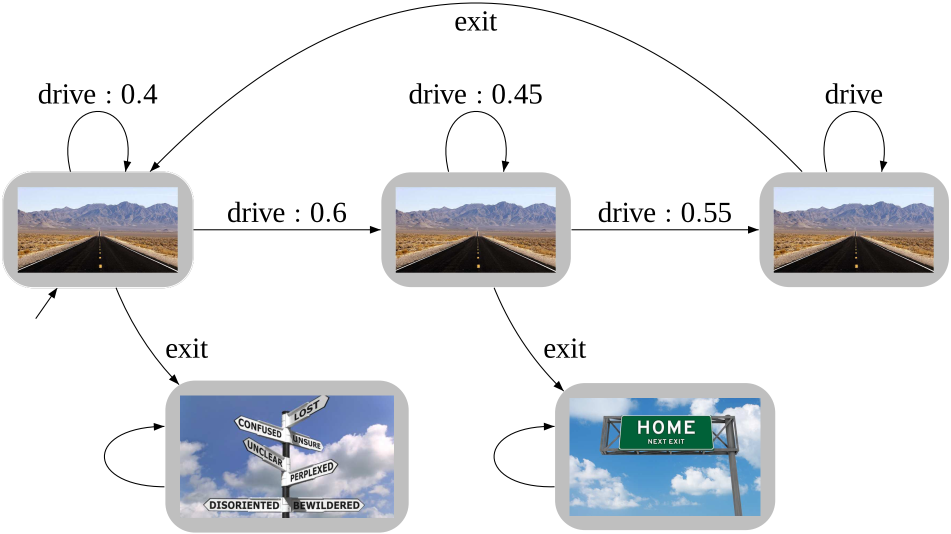
Correctness

Theorem

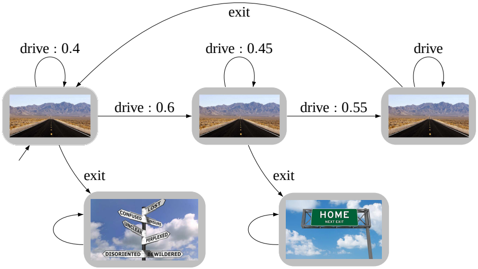
If there exists a value 1 *witness, then* $\mathcal{A}$ *has value* 1.

But the value 1 problem is undecidable, so…

No completeness

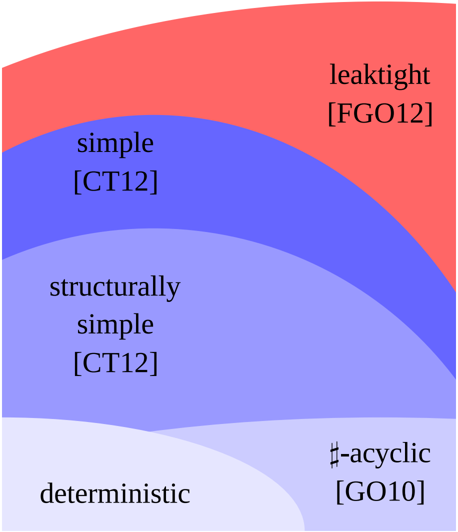


No completeness

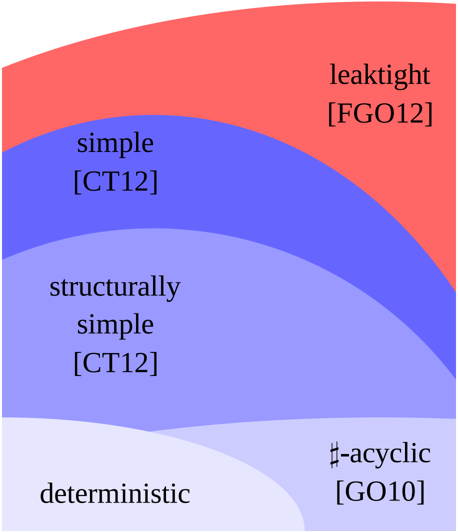


- No word ensures to reach home *almost surely*.
- For every $\varepsilon > 0$, there exists a word ensuring to reach home with probability at least $1 - \varepsilon$!
- This is not true anymore if the probabilities change, but the Markov Monoid algorithm cannot detect this!

Theoretical Results



Theoretical Results



In [FGO12], we introduced the Markov Monoid, generalizing the transition monoid.

Theorem ([FGO12])

The value 1 problem is decidable for leaktight automata.

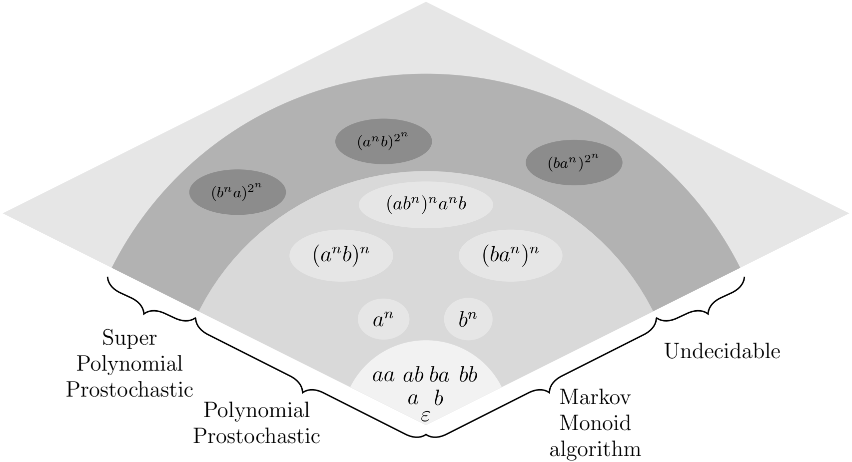
Theorem ([FGKO14])

Leaktight automata strictly contain the simple automata.

Theorem ([Fij15])

The Markov Monoid algorithm is optimal.

Optimality Argument



MMA in Practice!

Two implementations:

- ACMÉ: a naïve one, written in OCaML with Denis Kuperberg,
- ACMÉ++: an optimized one, written in C++ with Hugo Gimbert, Edon Kelmendis and Denis Kuperberg.

The end.

Thank you for your attention!

Krishnendu Chatterjee and Mathieu Tracol.
Decidable problems for probabilistic automata on infinite words.
In Logics in Computer Science, 2012.

Nathanaël Fijalkow, Hugo Gimbert, Edon Kelmendi, and Youssouf Oualhadj.
Deciding the value 1 problem for probabilistic leaktight automata.
Unpublished, 2014.

Nathanaël Fijalkow, Hugo Gimbert, and Youssouf Oualhadj.
Deciding the value 1 problem for probabilistic leaktight automata.
In Logics in Computer Science, pages 295–304, 2012.

Nathanaël Fijalkow.
Profinite techniques for probabilistic automata, and the optimality of the markov monoid algorithm.
Unpublished, 2015.

Hugo Gimbert and Youssouf Oualhadj.
Probabilistic automata on finite words: Decidable and undecidable problems.
In International Colloquium on Automata, Languages and Programming, pages 527–538, 2010.