Controlling probabilistic systems under partial observation an automata and verification perspective

Nathalie Bertrand, Inria Rennes, France

Uncertainty in Computation Workshop
October 4th 2016, Simons Institute, Berkeley
Partially observable probabilistic systems

Why probabilities? randomized algorithms, unpredictable behaviours, abstraction of non-determinism

Why partial observation? abstraction of large systems, security concerns
Partially observable probabilistic systems

Why probabilities? randomized algorithms, unpredictable behaviours, abstraction of non-determinism

Why partial observation? abstraction of large systems, security concerns

this talk: known automaton-like model
Partially observable probabilistic systems

**Why probabilities?** randomized algorithms, unpredictable behaviours, abstraction of non-determinism

**Why partial observation?** abstraction of large systems, security concerns

**this talk**: known automaton-like model

- language-theoretic questions: languages defined by prob. automata
- monitoring issues: fault diagnosis, supervision, etc.
- control problems: optimization for a given objective
Outline

Probabilistic automata

Partially observable MDP

Discussion
Motivating example for probabilistic automata (PA)

Planning holidays *in advance*:

1. choose an airline type (lowcost/highcost);
2. book accommodation (internet/phone);
3. choose tour (seeall/missnothing).

each action fails with some probability

success probability of plan \textit{lowcost \cdot internet \cdot seeall} is \( \frac{27}{64} \).
Strategies are words
what is the probability to reach a final state after word $w$?

The acceptance probability of $w = a_1 \ldots a_n$ by $A$ is:

$$\Pr_A(w) = \sum_{q \in Q} \pi_0[q] \sum_{q' \in F} \left( \prod_{i=1}^{n} P_{a_i} \right)[q, q'] = \pi_0 P_w 1_F^T$$
Control strategies in PA

**Strategies are words**
what is the probability to reach a final state after word $w$?

The **acceptance probability** of $w = a_1 \ldots a_n$ by $\mathcal{A}$ is:

$$
\Pr_{\mathcal{A}}(w) = \sum_{q \in Q} \pi_0[q] \sum_{q' \in F} \left( \prod_{i=1}^{n} P_{a_i} \right)[q, q'] = \pi_0 P_w 1_F^T
$$

Optimal strategies may not exist

![Diagram](https://via.placeholder.com/150)

$$
\Pr_{\mathcal{A}}(a_1 \ldots a_n) = \sum_{i=1}^{n} 2^{i-n-1} \cdot 1_{a_i=b}
$$
Control strategies in PA

**Strategies are words**
what is the probability to reach a final state after word $w$?

The acceptance probability of $w = a_1 \ldots a_n$ by $\mathcal{A}$ is:

$$
\Pr_{\mathcal{A}}(w) = \sum_{q \in Q} \pi_0[q] \sum_{q' \in F} \left( \prod_{i=1}^{n} P_{a_i} \right) [q, q'] = \pi_0 P_w 1_F^T
$$

Optimal strategies may not exist

$$
\Pr_{\mathcal{A}}(a_1 \ldots a_n) = \sum_{i=1}^{n} 2^{i-n-1} \cdot 1_{a_i=b}
$$

$\rightarrow$ Find good enough strategies, i.e. that guarantee a given probability
Existence of good-enough strategies

\[ L_{\otimes \theta}(A) = \{ w \in A^* \mid \Pr_A(w) \otimes \theta \} \]

The problem, given a PA $A$ of telling whether $L_{[\frac{1}{2}]}(A) \neq \emptyset$ is undecidable.

Paz'71
Existence of good-enough strategies

\[ L_{\bowtie \theta}(\mathcal{A}) = \{ w \in A^* \mid \Pr_\mathcal{A}(w) \bowtie \theta \} \]

The problem, given a PA \( \mathcal{A} \) of telling whether \( L_{\geq \frac{1}{2}}(\mathcal{A}) \neq \emptyset \) is undecidable. \hspace{1cm} \text{Paz'71}

Undecidability is robust

refined emptiness \hspace{1cm} \text{assuming that for } \epsilon > 0 \text{ either } \exists w \Pr_\mathcal{A}(w) \geq 1 - \epsilon \text{ or } \forall w \Pr_\mathcal{A}(w) < \epsilon \text{, decide which is the case} \hspace{1cm} \text{Condon et al.'03}

value one problem \hspace{1cm} \text{does there exist } (w_n)_{n \in \mathbb{N}} \text{ such that } \limsup_n \Pr_\mathcal{A}(w_n) = 1? \hspace{1cm} \text{Gimbert and Oualhadj'10}

parametric probability values \hspace{1cm} \text{does there exist a valuation of probabilities such that } \mathcal{A} \text{ has value one?} \hspace{1cm} \text{Fijalkow et al.'14}
Anything decidable?

**Almost-sure language:** \( L_{\epsilon_1}(A) \)

- Emptiness of almost-sure language is PSPACE-complete.
- Equivalent to universality problem for NFA.

**Quantitative language equivalence**
- **Input:** \( A \) and \( A' \)
- **Output:** yes iff \( \forall w \in A^* \Pr_{A}(w) = \Pr_{A'}(w) \)

Quantitative language equivalence is decidable in PTIME.

- Schützenberger'61, Tzeng'92
- Linear algebra argument
- Polynomial bound on length of counterexample to equivalence.
Almost-sure language: $L_{=1}(A)$

Emptiness of almost-sure language is PSPACE-complete.

equivalent to universality problem for NFA

Quantitative language equivalence

Input: $A$ and $A'$ PA

Output: yes iff $\forall w \in A^* \Pr_A(w) = \Pr_{A'}(w)$

Quantitative language equivalence is decidable in PTIME.

Schützenberger'61, Tzeng'92

linear algebra argument

polynomial bound on length of counterexample to equivalence
Recap on Probabilistic Automata

Partial observation: the plan must be decided in advance!
Recap on Probabilistic Automata

Partial observation: the plan must be decided in advance!

- model of system is known
- the effect of a plan can be computed: after word $w$, probability distribution over states
- yet most optimization problems are undecidable
Recap on Probabilistic Automata

Partial observation: the plan must be decided in advance!

- model of system is known
- the effect of a plan can be computed: after word $w$, probability distribution over states
- yet most optimization problems are undecidable

What if we execute a plan, but have feedback, and can modify the plan?

partially observable Markov decision processes
Outline

Probabilistic automata

Partially observable MDP

Discussion
Example of partially observable MDP (POMDP)

McCallum maze: robot with limited sensor abilities, and imperfect moves

- Robot only sees walls surrounding it, not the precise cell
  \[ \Omega = \{ \{L, U \}, \{U, D \}, \{U, R \}, \{L, D, R \} \cdots \} \]
- Actions \( A = \{N, W, S, E\} \) are not implemented accurately
  - Action \( N \) leads to north with probability \( \frac{2}{3} \) and others with \( \frac{1}{3} \)

Reachability objective: move to target cell

Optimization: minimum expected time
McCallum maze: robot with limited sensor abilities, and imperfect moves

- robot only sees walls surrounding it, not the precise cell observations

- observations \( \Omega = \{ \{L, U\}, \{U, D\}, \{U, R\}, \{L, D, R\} \ldots \} \)

- actions \( A = \{N, W, S, E\} \) are not implemented accurately
  - action \( N \) leads to north with probability \( \frac{2}{3} \) and others with \( \frac{1}{3} \)
Example of partially observable MDP (POMDP)

McCallum maze: robot with limited sensor abilities, and imperfect moves

- robot only sees walls surrounding it, not the precise cell observations \( \Omega = \{ \{L, U\}, \{U, D\}, \{U, R\}, \{L, D, R\} \ldots \} \)
- actions \( A = \{N, W, S, E\} \) are not implemented accurately
  action \( N \) leads to north with probability \( \frac{2}{3} \) and others with \( \frac{1}{3} \)

Reachability objective: move to target cell •
Optimization: minimum expected time
Strategies

**Strategy**: maps *history* $\rho \in (A\Omega)^*$ with distribution over actions;

$$\nu : (A\Omega)^* \rightarrow \text{Dist}(A)$$

$\nu(\rho, a)$: probability that $a$ is chosen given history $\rho$

- **pure** strategy: all distributions are Dirac
- **belief-based** strategy: based on set of current possible states

word in PA $\iff$ pure strategy in POMDP with $|\Omega| = 1$

**Consequence**: all hardness results lift from PA to POMDP
Infinite horizon objectives

**Objectives**

**Reachability** $F$ visited at least once:

$$\Diamond F = \{ q_0 q_1 q_2 \cdots \in S^\omega \mid \exists n, q_n \in F \}$$

**Safety** always stay in $F$:

$$\Box F = \{ q_0 q_1 q_2 \cdots \in S^\omega \mid \forall n, q_n \in F \}$$

**Büchi** $F$ visited an infinite number of times:

$$\Box \Diamond F = \{ q_0 q_1 q_2 \cdots \in S^\omega \mid \forall m \exists n \geq m, q_n \in F \}$$

**Goal:** For $\varphi$ an objective, evaluate $\sup_\nu \mathbb{P}(\mathcal{M} = \varphi)$.
Infinite horizon objectives

Objectives

Reachability  $F$ visited at least once:

$$\Diamond F = \{q_0q_1q_2\cdots \in S^\omega \mid \exists n, \ q_n \in F\}$$

Safety  always stay in $F$:

$$\square F = \{q_0q_1q_2\cdots \in S^\omega \mid \forall n, \ q_n \in F\}$$

Büchi  $F$ visited an infinite number of times:

$$\square \Diamond F = \{q_0q_1q_2\cdots \in S^\omega \mid \forall m \exists n \geq m, \ q_n \in F\}$$

Goal: For $\varphi$ an objective, evaluate $\sup_\nu P^\nu(\mathcal{M} \models \varphi)$.

Pure strategies suffice!

For every strategy $\nu$, there exists a pure strategy $\nu'$ such that

$$P^\nu(\mathcal{M} \models \varphi) \leq P^{\nu'}(\mathcal{M} \models \varphi).$$

Chatterjee et al.'15
Undecidability results

Undecidability of qualitative objectives...

... beyond the ones already mentioned for PA
Undecidability results

Undecidability of qualitative objectives…

… beyond the ones already mentioned for PA

positive repeated reachability does there exist $\nu$ such that

$$\mathbb{P}^\nu(M \models \Box \Diamond F) > 0?$$

Baier et al.'08

combined objectives does there exist $\nu$ such that

$$\mathbb{P}^\nu(M \models \Box \Diamond F_1) = 1$$

and

$$\mathbb{P}^\nu(M \models \Box F_2) > 0?$$

Bertrand et al.'14
Undecidability results

Undecidability of qualitative objectives...
... beyond the ones already mentioned for PA

**positive repeated reachability** does there exist \( \nu \) such that
\[
\mathbb{P}^\nu(M \models \square \Diamond F) > 0?
\]

Baier et al.'08

**combined objectives** does there exist \( \nu \) such that
\[
\mathbb{P}^\nu(M \models \square \Diamond F_1) = 1
\]
and
\[
\mathbb{P}^\nu(M \models \square F_2) > 0?
\]

Bertrand et al.'14

Proof of first statement: reduction from the value one problem for PA

pure strategies in \( M \):
\[\nu_w = w_1\#w_2\#w_3 \cdots\]

\[\text{val}(A) = 1 \iff \exists (w_i)_{i \in \mathbb{N}} \prod_i \mathbb{P}(w_i) > 0\]

\[\iff \exists \nu_w \mathbb{P}^\nu_w(M \models \square \Diamond f_\#) > 0\]
Decidability results

Good news: decidable problems for PA remain decidable
Decidability results

Good news: decidable problems for PA remain decidable

- **almost-sure safety** existence of $\nu$ such that $\mathbb{P}^{\nu}(M \models \square F) = 1$
- **positive safety** existence of $\nu$ such that $\mathbb{P}^{\nu}(M \models \square F) > 0$
- **almost-sure repeated reachability** existence of $\nu$ such that $\mathbb{P}^{\nu}(M \models \square \Diamond F) = 1$

are all EXPTIME-complete.
Decidability results

Good news: decidable problems for PA remain decidable

almost-sure safety  existence of $\nu$ such that $\mathbb{P}^{\nu}(\mathcal{M} \models \Box F) = 1$

positive safety  existence of $\nu$ such that $\mathbb{P}^{\nu}(\mathcal{M} \models \Box F) > 0$

almost-sure repeated reachability  existence of $\nu$ such that $\mathbb{P}^{\nu}(\mathcal{M} \models \Box \Diamond F) = 1$

are all EXPTIME-complete.

fixpoint algorithms on a powerset construction

belief-based strategies suffice except for positive safety
Decidability results

Good news: decidable problems for PA remain decidable

Almost-sure safety existence of $\nu$ such that $\mathbb{P}^\nu(M \models \Box F) = 1$

Positive safety existence of $\nu$ such that $\mathbb{P}^\nu(M \models \Box F) > 0$

Almost-sure repeated reachability existence of $\nu$ such that
$$\mathbb{P}^\nu(M \models \Box \Diamond F) = 1$$

are all EXPTIME-complete.

Fixpoint algorithms on a powerset construction

Belief-based strategies suffice except for positive safety

No belief-based strategy can achieve
$$\mathbb{P}^\nu(M \models \Box \{q_0, q_1, q_2\}) > 0$$

Alternate $a$ and $b$ forever, guarantees a probability $\frac{1}{2}$.
Decidability results

Good news: decidable problems for PA remain decidable

almost-sure safety existence of $\nu$ such that $\mathbb{P}^\nu(M \models \square F) = 1$

positive safety existence of $\nu$ such that $\mathbb{P}^\nu(M \models \square F) > 0$

almost-sure repeated reachability existence of $\nu$ such that $\mathbb{P}^\nu(M \models \square \diamond F) = 1$

are all EXPTIME-complete.

fixpoint algorithms on a powerset construction belief-based strategies suffice except for positive safety

no belief-based strategy can achieve $\mathbb{P}^\nu(M \models \square \{q_0, q_1, q_2\}) > 0$

alternate $a$ and $b$ forever, guarantees a probability $\frac{1}{2}$

Open: decidability of non-null proportion with positive probability

$\exists \nu, \mathbb{P}^\nu(M \models \limsup_n \frac{\#\text{visits to } F \text{ in } n \text{ first steps}}{n} > 0) > 0$?
Outline

Probabilistic automata

Partially observable MDP

Discussion
Life is hard...
Life is hard...

most optimization problems are undecidable
  ▶ notably quantitative questions
  ▶ but also some qualitative questions
  ▶ and undecidability is robust
... but there is still hope

- usual way arounds
  - decidable subclasses
  - restricted classes of strategies
  - approximations, although with no termination guarantees

Fijalkow et al.'12
Yu'06
... but there is still hope

- usual way arounds
  - decidable subclasses
  - restricted classes of strategies
  - approximations, although with no termination guarantees

- promising alternative: discretization
  - continuous distributions approximated by large discrete population

Fijalkow et al.'12
Yu'06
... but there is still hope

- usual way arounds
  - decidable subclasses
  - restricted classes of strategies
  - approximations, although with no termination guarantees

- promising alternative: discretization
  - continuous distributions approximated by large discrete population

![Diagram](image-url)
... but there is still hope

- usual way arounds
  - decidable subclasses
  - restricted classes of strategies
  - approximations, although with no termination guarantees

- promising alternative: discretization
  - continuous distributions approximated by large discrete population

- limit for large populations differs from continuous semantics
- possible alternative semantics to PA/POMDP models, with more decidability results
... but there is still hope

- usual way arounds
  - decidable subclasses
  - restricted classes of strategies
  - approximations, although with no termination guarantees  
    \[ \text{Yu'06} \]

- promising alternative: discretization
  - continuous distributions approximated by large discrete population

\[ \text{Fijalkow et al.'12} \]

- limit for large populations differs from continuous semantics
- possible alternative semantics to PA/POMDP models, with more decidability results

Thank you!