Probabilistic Timed Automata: Current Challenges and Future Directions

Jeremy Sproston

Dipartimento di Informatica
University of Turin
Italy

OPCT 2023
29th June 2023

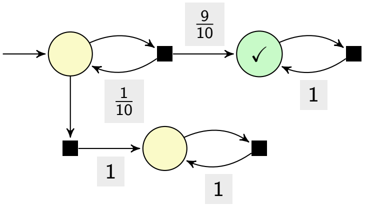
Reachability in probabilistic timed systems

- Reachability problems in systems exhibiting probabilistic and timed (and nondeterministic) behaviour.
- Modelling formalism: balance between expressivity of formalism and decidability of reachability properties.

Reachability in probabilistic timed systems

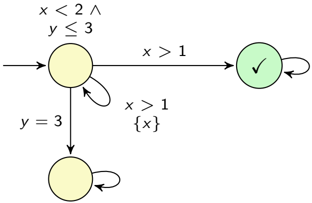
- Modelling formalism: classical starting points

Markov decision processes (MDPs)



Reachability: given $\lambda \in (0, 1]$, does there exist a way to resolve nondeterministic choice such that  is reached with probability at least λ? (maximum reachability)

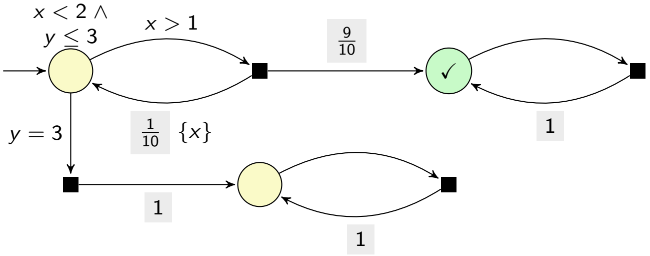
Timed automata



Reachability: does there exist a way to resolve nondeterministic choice such that  is reached?

Probabilistic timed automata

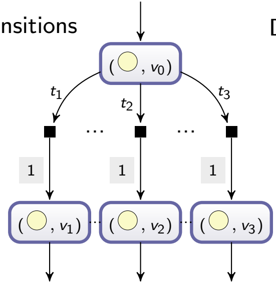
- Probabilistic timed automata (PTAs) [Gregersen & Jensen 1995; Kwiatkowska et al. 2002]: timed automata with (discrete) probabilistic choice over edges.
- PTA extend conservatively:
  - MDPs (presence of *nondeterministic* and *probabilistic* choice over transitions);
  - timed automata (clock variables, constraints and resets).
- Example:



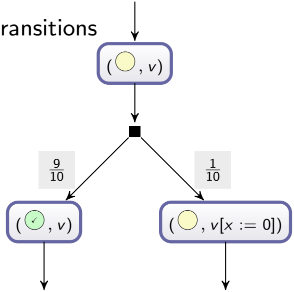
Probabilistic timed automata

- Semantics of a PTA: an infinite-state MDP.
  - State: pair (*location*, *valuation*), where *location* is the current node (circle) and *valuation* assigns to the clocks their current value.
  - Time elapses: choose *nondeterministically* a time delay, then the value of all clocks increase by that amount (must satisfy the invariant of the current location).
  - Discrete transition: choose enabled ■ *nondeterministically*, then make a *probabilistic* choice according to chosen ■ (e.g., with probability $\frac{9}{10}$ go to ✓, with probability $\frac{1}{10}$ go to ○ and reset x to 0 (reset annotation $\{x\}$).

Time elapse transitions



Discrete transitions



Reachability for probabilistic timed automata

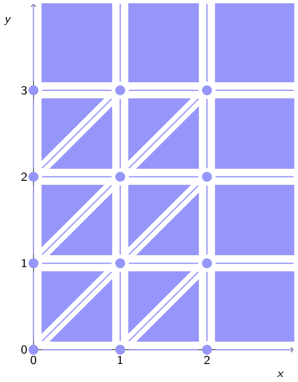
Maximum reachability for PTAs

Given an initial state and a threshold $\lambda \in (0, 1]$, does there exists a way to resolve nondeterminism such that the probability that the PTA reaches a set of final locations equal to or greater than λ?

Complexity results on maximum reachability for MDPs and PTAs:

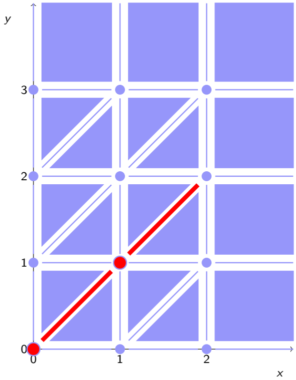
MDPs (PTAs with no clocks)	PTIME-c	[Courcoubetis & Yannakakis 1990, 1998] [Papadimitriou & Tsitsiklis 1987]
PTAs with one clock	PTIME-c	[Jurdzinski et al. 2008]
PTAs with at least two clocks	EXPTIME-c	[Kwiatkowska et al. 2002] [Jurdzinski et al. 2008]

Region equivalence applied to PTAs

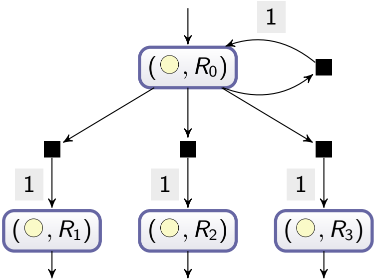


- Region equivalence [Alur & Dill 1994]: partition the clock valuation space into a finite number of classes.
- Induces a finite (probabilistic) bisimulation on the PTA's state space.
- Solve reachability problem on the finite-state MDP resulting from region equivalence.

Region equivalence applied to PTAs

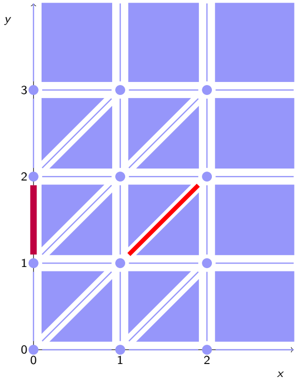


Time transitions
(from (○, R_0), where R_0 is defined by
$x = y = 0$, with invariant $x < 2 \land y \leq 3$)

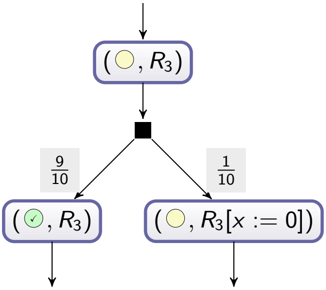


R_1 is defined by $0 < x = y < 1$,
R_2 is defined by $x = y = 1$,
R_3 is defined by $1 < x = y < 2$

Region equivalence applied to PTAs



Example of discrete transition (from (, R_3), where R_3 is defined by $1 < x = y < 2$)



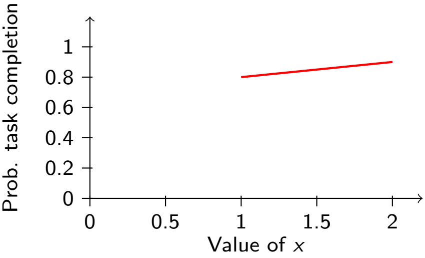
$R_3[x := 0]$ is defined by $x = 0, 1 < y < 2$

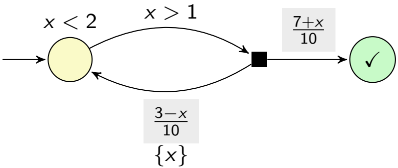
Beyond region-graph-based reachability

- Beyond the region graph:
  - Digital clocks [Kwiatkowska et al. 2006] (no strict constraints).
  - Zones [Kwiatkowska et al. 2007, 2009].
  - Statistical model checking [D'Argenio et al. 2016; Hartmanns at al. 2017].
  - ... future challenge (generic!): making analysis for PTAs applicable to larger models.
- Beyond reachability:
  - Model checking for probabilistic temporal logics [Kwiatkowska et al. 2002].
  - Reachability properties with prices/costs [Kwiatkowska et al. 2006, 2017].
  - Timed probabilistic bisimulation [Troina & S 2010] and timed bisimilarity metrics [Lanotte & Tini 2019].
  - ... future challenge: linear temporal logics, ...
- Beyond PTAs:
  - Parametric (over probabilities) PTA [Hartmanns et al. 2021].
  - ... future challenge: extend PTAs while maintaining decidability ...

Clock-dependent probabilistic timed automata

- Probabilities may depend on time: e.g., success of task completion may increase with the amount of time dedicated to the task attempt.
- *Clock-dependent probabilistic timed automata (cdPTAs)* [S 2021a]: label edges with affine expressions over clock values, defining distributions for each valuation of the clocks.





Reachability problems for cdPTA

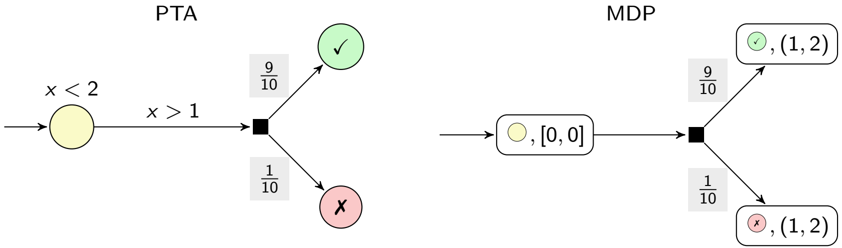
Undecidability of reachability for cdPTAs [S 2021a]

The maximum reachability problem is undecidable for cdPTAs with ≥ 3 clocks.

- Inspired by the undecidability result for stochastic timed automata of [Akshay et al. 2016].
- Can approximate the maximum probability to reach target locations by:
    - using an adaptation of the region-equivalence MDP construction (based on the "corner-point abstraction" [Bouyer et al. 2008]);
    - refining the granularity of timing constants of region equivalence to obtain an improved (no worse) approximation of the maximum reachability probability.
- Question: is the maximum reachability problem decidable for cdPTAs with *one* clock?

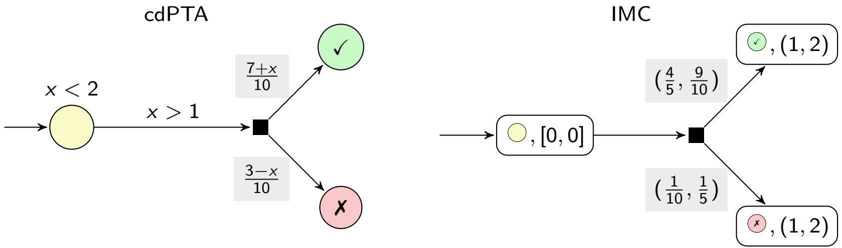
Results for PTAs with one clock

- Construct an equivalent *finite-state* MDP [Jurdzinski et al. 2008] (use concepts from non-probabilistic case [Laroussine et al. 2004]), analyse the MDP (in polynomial time).
- Principle: obtain a finite partition of the set of possible clock values (i.e., $\mathbb{R}_{\geq 0}$), endpoints of intervals are constants from the PTA (and 0).
- Example: partition $[0,0], (0,1), [1,1], (1,2), [2,2], (2,\infty)$.



- Intuition: in the MDP, take the transition from (, $[0,0]$) when x is in $(1,2)$.

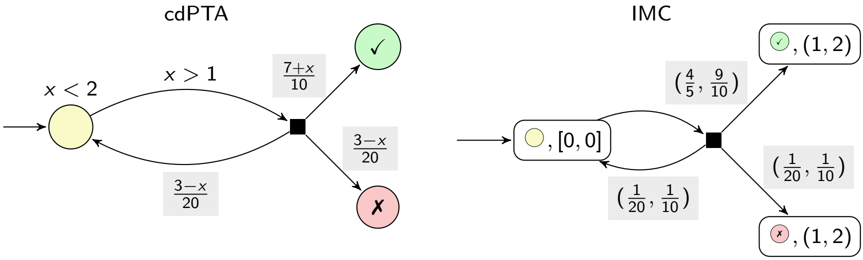
IMC construction for cdPTAs with one clock



- Use (open) interval Markov chains (IMCs) [Jonsson & Larsen 1991; Chakraborty & Katoen 2015]:
  - Label edges with intervals on probabilities; make *nondeterministic* choice between distributions allowed by the intervals.
- E.g., for transition from (, [0, 0]): choose *nondeterministically* a pair (λ, λ') of probabilities, where $\lambda \in (\frac{4}{5}, \frac{9}{10})$, $\lambda' \in (\frac{1}{10}, \frac{1}{5})$ and $\lambda + \lambda' = 1$.
  - This nondeterministic choice of (λ, λ') mimics the nondeterministic choice of time delay in $(1, 2)$ in .

IMC construction for cdPTAs with one clock

- General case (if squares have ≥ 3 outgoing edges):

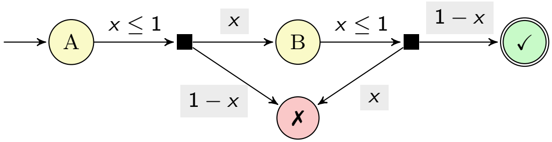


- ✗: incorrect! The IMC allows the distribution assigning:

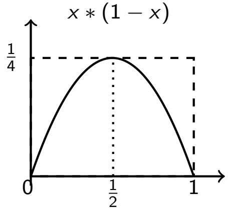
$\frac{17}{20}$ to (✓, (1, 2)), $\frac{7}{80}$ to (✗, (1, 2)), and $\frac{1}{16}$ to (○, [0, 0]).

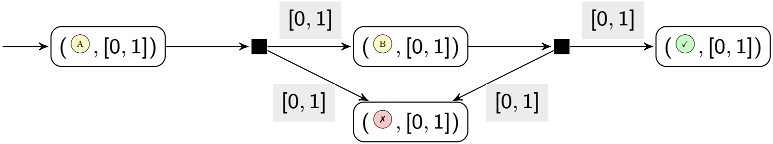
- Probabilities of going to (✗, (1, 2)) and (○, [0, 0]) *must be equal*.
- Solution: split a single cdPTA transition into a sequence of *two* transitions in the IMC (first simulates the choice of value of x in the interval $(1, 2)$, second is a purely probabilistic choice).

IMC construction for cdPTAs with one clock



- Maximum probability strategy to reach ✓:
  - Leave location A when x is equal to $\frac{1}{2}$, then leave location B instantly.
  - Probability of reaching location ✓ for this strategy is $\frac{1}{4}$.





- ✗: incorrect! In the IMC, ✓ can be reached with probability 1.

Results for cdPTAs with one clock

- Problem: optimal choices in different cdPTA locations may not be independent, yet dependencies between choices in different states of IMCs cannot be represented.
- *Initialisation*: between any probabilistic choices depending on the clock x (i.e., that are not constant functions), the clock must pass through a closed interval of the partition (either by letting time elapse or by resetting the clock).

Reachability for initialised cdPTAs with one clock [S 2021b]

Maximum reachability problems are PTIME-complete for initialised cdPTAs with one clock.

- Also minimum reachability problems and *qualitative* reachability problems can be decided in polynomial time for initialised cdPTAs with one clock.
- Results rely on polynomial-time algorithms for (open) IMCs (for max./min. problems [Chen et al. 2013; Pugelli et al. 2013; Chakraborty & Katoen 2015], for qualitative problems [S 2018]).

Beyond initialised one-clock cdPTAs

- Lifting "one clock" restriction: multiple clocks, only one of which is used to determine probabilities *and* which is initialised.
  - ✗: maximum reachability problem is undecidable.
- Lifting initialisation in one-clock cdPTAs: connection with parametric MDPs?
- Qualitative ($\lambda = 1$) maximum reachability for cdPTAs?
  - Beyond affine clock dependencies: ✗, maximum reachability problem is undecidable for cdPTAs with the dependencies of probabilities on clock described by quartic functions even when $\lambda = 1$.