Consistency in Parametric Interval Probabilistic Timed Automata

Étienne André[1,2] *Benoît Delahaye*[3]

[1]Université Paris 13, LIPN

[2]École Centrale de Nantes, IRCCyN

[3]Université de Nantes, LINA

TIME'16

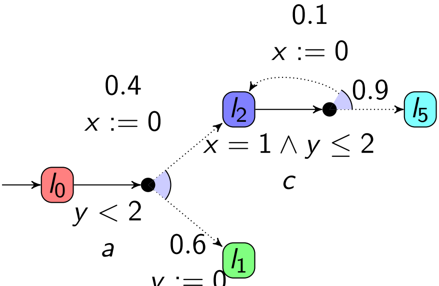
Motivation

- Allow uncertainty in probabilistic timed models
  - On probabilities $\Rightarrow$ Intervals
  - On timing constants $\Rightarrow$ Parameters
  - Is it possible to concretize an abstract model containing uncertainties? $\Rightarrow$ **Consistency**
- We want to compute the **whole** set of parameter values ensuring the desired properties.

Outline

Outline

Probabilistic Timed Automata ($\mathbb{P}$TA)



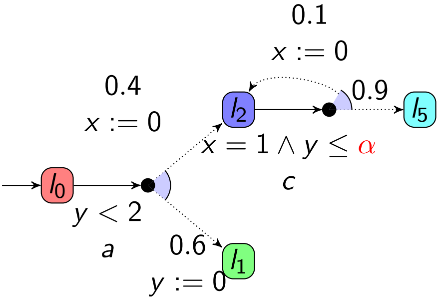
$\mathbb{P}$TA

- Clocks
- Discrete Probabilities

Restriction

- No invariants

Parametric Probabilistic Timed Automata (P$\mathbb{P}$TA)



P$\mathbb{P}$TA

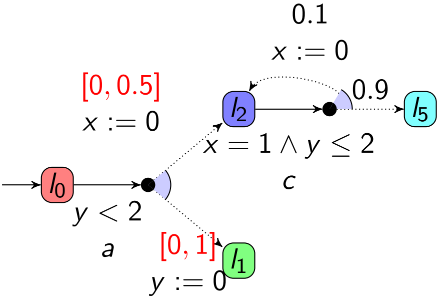
- Clocks compared to parameters

? Parameter Synthesis

Results

- Reachability emptyness is *undecidable* [AHV93]
- Halting Problem of a 2-counter machine

Interval Probabilistic Timed Automata (I$\mathbb{P}$TA)



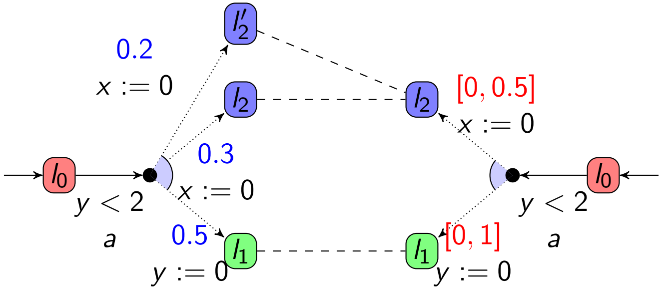
I$\mathbb{P}$TA

- Probabilities replaced with intervals
- Implementations = $\mathbb{P}$TA

Symbolic Semantics: Classical LTS Semantics + probabilities

$\Rightarrow$ Interval Markov Decision Process (IMDP)

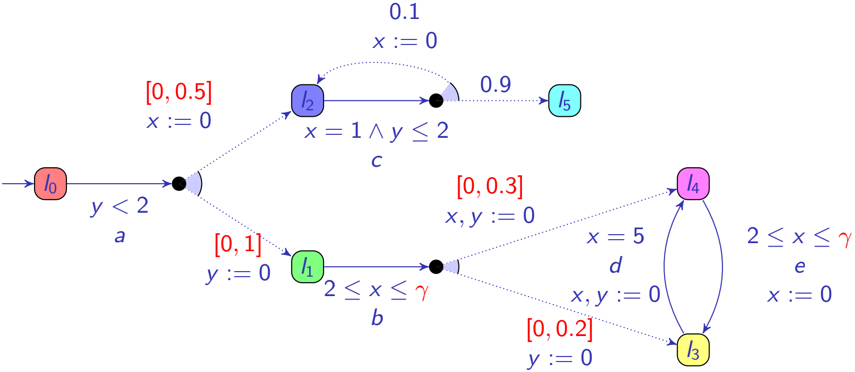
Implementation of I$\mathbb{P}$TA



Satisfaction Relation

- Simulation-like relation
- **Structure not necessarilly preserved**
- Clocks, Guards and Resets must be the same

Parametric Interval Probabilistic Timed Automata (PI$\mathbb{P}$TA)



Implementation: $\mathbb{P}$TA

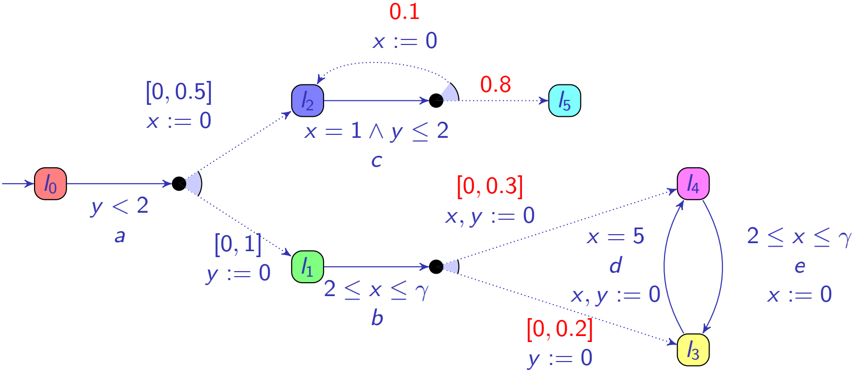
Same as for I$\mathbb{P}$TA:

+ Parameter Valuation fixed

- Simulation-like: Structure not preserved
- Same Clocks, Guards and Resets

Outline

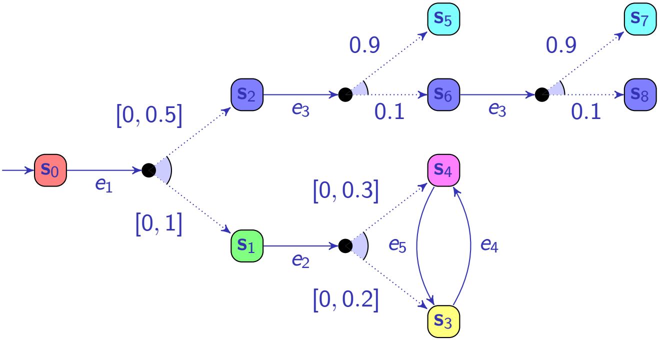
Consistency



Consistency

Does there exist a parameter valuation such that a given PI$\mathbb{P}$TA admits at least one implementation?

Consistency in IMC/IMDP

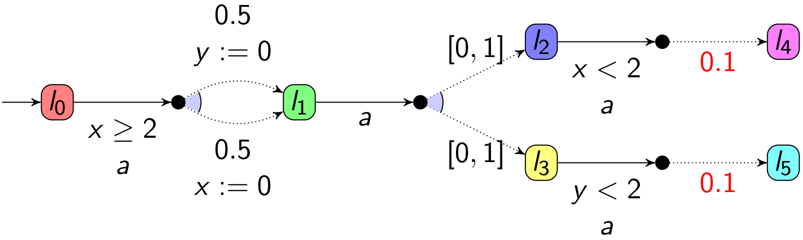


IMC/IMDP Consistency

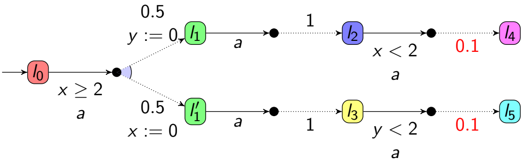
- Decidable [DLLPW11]
- Polynomial Algorithm [D15]

Theorem[D15]:
Structure can be conserved

Theorem from [D15] does not hold for IℙTA



- **Consistent**
- No implementation with same structure



Solution: Zone Graph

Theorem (Zone Graph Consistency)

An $\mathbb{IP}$TA *is consistent iff its* IMDP *zone graph is consistent*

Theorem

An IMDP is consistent iff it admits an implementation with the same structure

Algorithm: Consistency of $\mathbb{IP}$TA

- Build IMDP Zone Graph $\mathcal{IM}$
- Check Consistency of $\mathcal{IM}$

Constructive algorithm

$\Rightarrow$ Build $\mathbb{P}$TA implementation from IMDP implementation

Outline

Introduction

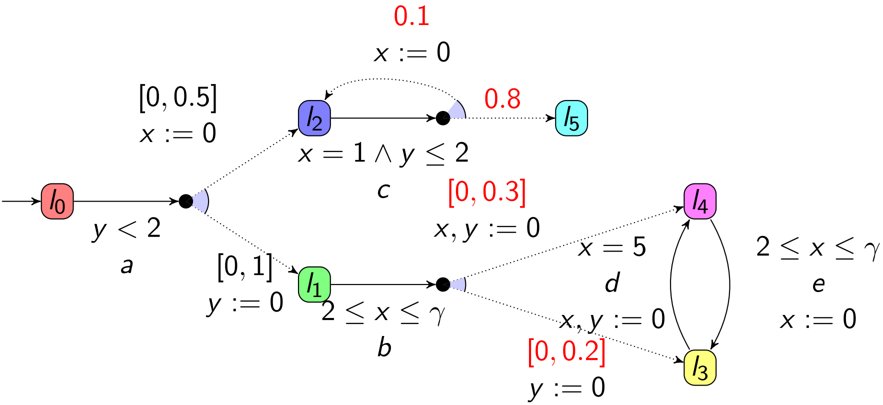
Probabilistic and Timed Specifications
- Timing Uncertainties
- Probabilistic Uncertainties
- Combining both approaches

The Consistency Problem
- Consitency in IMC/IMDP
- Consistency in Interval Probabilistic TA

Parameter Synthesis for PI$\mathbb{P}$TA Consistency
- Undecidability of Consistency for PI$\mathbb{P}$TA
- Semi-Algorithm

Conclusion

More leverage than I$\mathbb{P}$TA



⇒ We can use **parameter values** *and* **probabilities** to make inconsistent states unreachable

Undecidability of Consistency for PI$\mathbb{P}$TA

Theorem

The consistency-emptyness for PI$\mathbb{P}$TA *is undecidable*

- Reduction from the halting problem of a 2-counter machine
- Halting-state is made inconsistent by adding an inconsistent transition
- 2-counter machine halts iff PI$\mathbb{P}$TA is inconsistent for all parameter valuations

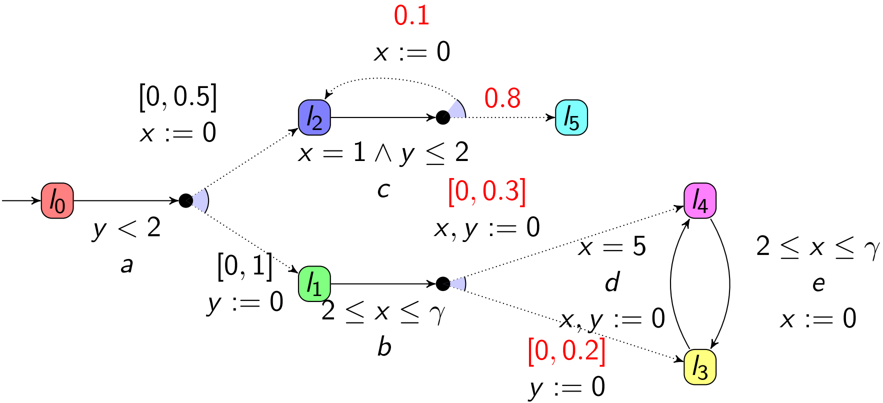
Consistency Synthesis 1/2

Algorithm (Sketch)

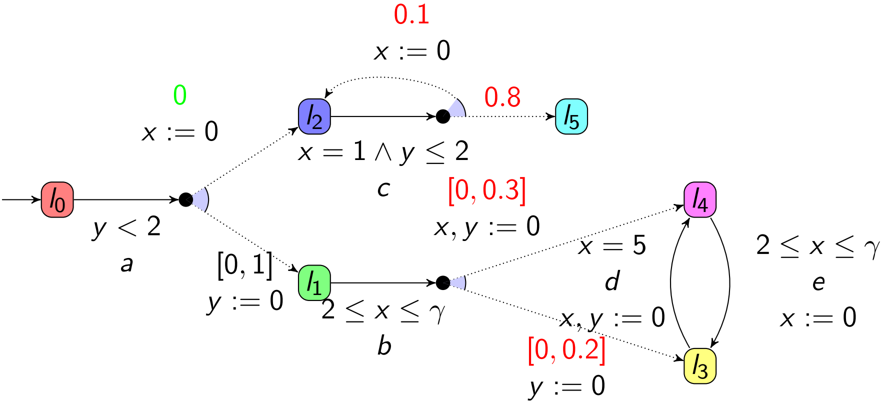
Input: Labeled IMDP semantics (zone graph) of PI$\mathbb{P}$TA
Output: Constraint K on parameters ensuring consistency

- Identify locally inconsistent states Inc
- While Inc $\neq \emptyset$
  - Pick $s \in$ Inc
  - Remove s from Inc and **mark**^{1} s
  - If **possible**, use probabilities to make s unreachable
  - Else **mark**^{2} predecessor states as inconsistent
- If s_0 is not **marked**^{2} then **return** $\top$
- Remove unreachable states
- For all **marked**^{2} states s
  - $K \leftarrow K \setminus C_s$
- Remove all states s s.t. $C_s \cap K = \emptyset$

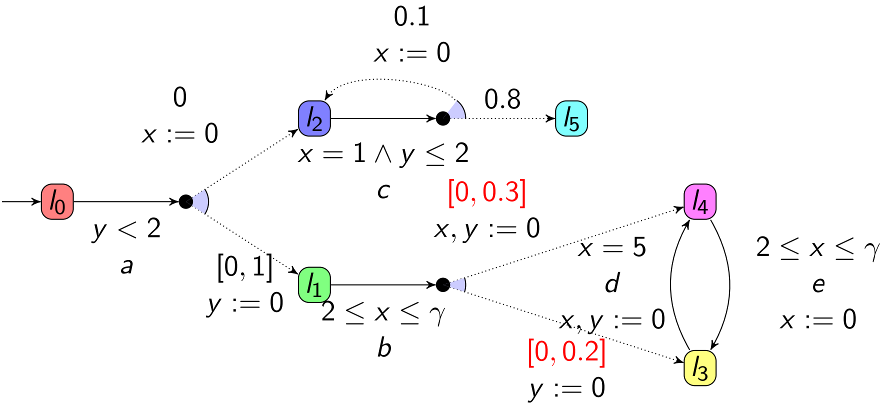
Consistency Synthesis Example



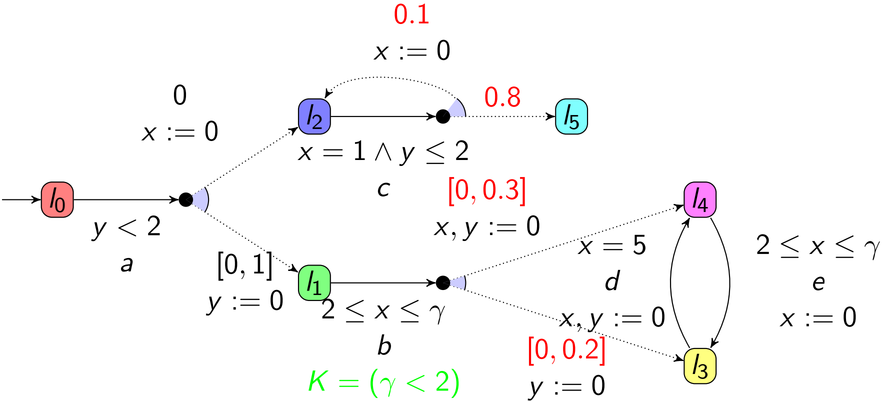
Consistency Synthesis Example



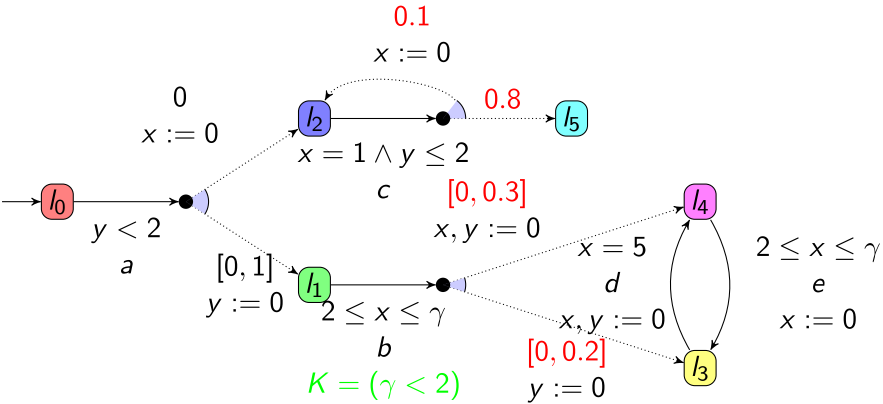
Consistency Synthesis Example



Consistency Synthesis Example



Consistency Synthesis Example



Result

$\gamma < 2$

Consistency Synthesis 2/2

Theorem

A parameter valuation v satisfies K iff v ensures that PI$\mathbb{P}$TA *is consistent*

But...

- Semi Algorithm because IMDP semantics might be infinite

Outline

Conclusion – Future work

- New formalism taking into account uncertainty on probabilities and timing constants
- Decidability of Consistency for I$\mathbb{P}$TA
- Undecidability of Consistency for PI$\mathbb{P}$TA
- Semi-Algorithm

- Under-approximation that always terminates
- Subclasses for which exact synthesis can be achieved
- Parameters on probabilities