Simulation and Bisimulation Relations for Probabilistic Timed Automata (ongoing work)

Jeremy Sproston and Angelo Troina

Dipartimento di Informatica
University of Turin
Italy

L'Aquila, 2nd March 2010

Motivation

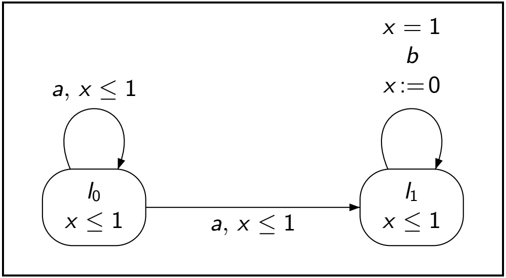
- Aim: construction of abstractions (or refinements) of probabilistic timed automata.
- Extensive work on abstraction for Markov chains, Markov decision processes, and timed automata, often based (in part) on simulation or bisimulation relations.
- Method: combine techniques from Markov decision processes and timed automata to use (bi)simulation for probabilistic timed automata.
- In particular, study algorithms and logical characterization.

(Bi)simulation

- Labelled transition system $(S, Act, \rightarrow)$, where $\rightarrow \subseteq S \times Act \times S$ (write $s \xrightarrow{a} s'$ to denote $(s, a, s') \in \rightarrow$).
- Relation $R \subseteq S \times S$ is a simulation relation if R satisfies the following condition:
  $(s_1, s_2) \in R$ implies that, for each $s_1 \xrightarrow{a} s_1'$, there exists $s_2 \xrightarrow{a} s_2'$ such that $(s_1', s_2') \in R$.
- s_2 simulates s_1 if there exists a simulation relation R such that $(s_1, s_2) \in R$.
- Relation $R \subseteq S \times S$ is a bisimulation relation if both R and R^{-1} are simulation relations.
- s_1 and s_1 are bisimilar if there exists a bisimulation relation R such that $(s_1, s_2) \in R$.

Timed automata

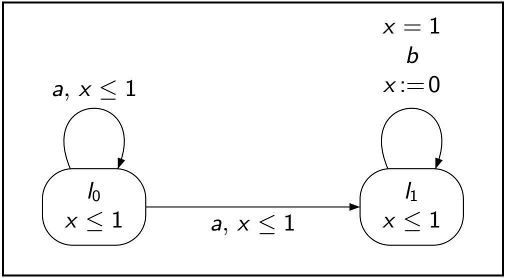
- Timed automata [AlurDill94]:
  - Finite-state graph (where the nodes are called *locations*).
  - Finite set of *clocks*: real-valued variables increasing at the same rate as real-time.
  - Clock constraints (*invariants* in locations, *guards* on edges).
  - Clock resets (set some clocks to 0 when an edge is traversed).



Timed automata

- Semantics of timed automata (in brief):
  - Represented by a timed transition system $(S, Act, \rightarrow)$, where $\rightarrow \subseteq S \times \mathbb{R}_{\geq 0} \times Act \times S$.
  - States: of the form (l, v), where l is a location and $v : \mathcal{X} \rightarrow \mathbb{R}_{\geq 0}$ is a *clock valuation* (must satisfy the invariant condition of l).
  - Transitions: for example (only a selection...),

$$((l_0, v(x) = 0.2), a, 0.1, (l_0, v(x) = 0.3)),\ ((l_0, v(x) = 0.3), a, 0.7, (l_1, v(x) = 1))$$
$$((l_1, v(x) = 1), b, 0, (l_1, v(x) = 0)),\ ((l_1, v(x) = 0), b, 1, (l_1, v(x) = 0))$$



Timed (bi)simulation

- Timed transition system $(S, Act, \rightarrow)$, where $\rightarrow \subseteq S \times \mathbb{R}_{\geq 0} \times Act \times S$.
- Relation $R \subseteq S \times S$ is a timed simulation relation if R satisfies the following condition:
  $(s_1, s_2) \in R$ implies that, for each $s_1 \xrightarrow{t,a} s_1'$, there exists $s_2 \xrightarrow{t,a} s_2'$ such that $(s_1', s_2') \in R$.
- s_2 timed simulates s_1 if there exists a timed simulation relation R such that $(s_1, s_2) \in R$.
- Relation $R \subseteq S \times S$ is a timed bisimulation relation if both R and R^{-1} are timed simulation relations.
- s_1 and s_1 are timed bisimilar if there exists a timed bisimulation relation R such that $(s_1, s_2) \in R$.

Timed vs. time-abstract (bi)simulation

- Timed transition system $(S, Act, \rightarrow)$, where $\rightarrow \subseteq S \times \mathbb{R}_{\geq 0} \times Act \times S$.
- Relation $R \subseteq S \times S$ is a time-abstract simulation relation if R satisfies the following condition:
  $(s_1, s_2) \in R$ implies that, for each $s_1 \xrightarrow{t,a} s_1'$ there exists $s_2 \xrightarrow{t',a} s_2'$ such that $(s_1', s_2') \in R$.
- s_2 time-abstract simulates s_1 if there exists a time-abstract simulation relation R such that $(s_1, s_2) \in R$.
- Relation $R \subseteq S \times S$ is a time-abstract bisimulation relation if both R and R^{-1} are time-abstract simulation relations.
- s_1 and s_1 are time-abstract bisimilar if there exists a time-abstract bisimulation relation R such that $(s_1, s_2) \in R$.

Timed vs. time-abstract (bi)simulation

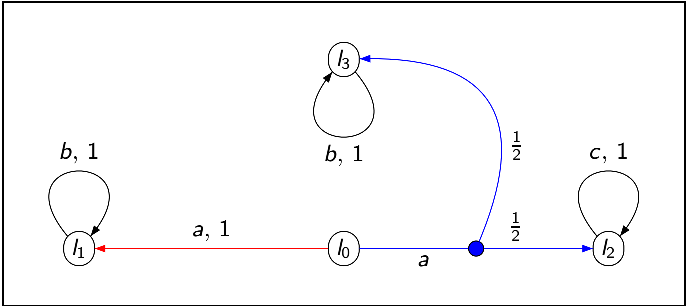
- Time-abstract bisimulation can be used to construct finite-state abstractions of timed automata.
- Region equivalence [AlurDill94]: a finitary time-abstract bisimulation equivalence relation over states of a timed automaton.
- The number of regions equivalence classes corresponding to a timed automaton is exponential in the number of clocks and the maximal constant used in the model (in guards or invariants).
- Intuitively, states $(l, v), (l', v')$ are region equivalent if $l = l'$, and v and v' are "clock equivalent".

Timed vs. time-abstract (bi)simulation

- For each clock $x \in \mathcal{X}$, let c_x be the maximal constant to which x is compared in any of the guards or invariants.
- Two clock valuations $v, v' \in \mathbb{R}_{\geq 0}^{\mathcal{X}}$ are *clock equivalent* if if the following conditions are satisfied:
  1. for all clocks $x \in \mathcal{X}$, we have $v(x) \leq c_x$ if and only if $v'(x) \leq c_x$;
  2. for all clocks $x \in \mathcal{X}$ with $v(x) \leq c_x$, we have $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$;
  3. for all clocks $x, y \in \mathcal{X}$ with $v(x) \leq c_x$ and $v(y) \leq c_y$, we have $\mathrm{frac}(v(x)) \leq \mathrm{frac}(v(y))$ if and only if $\mathrm{frac}(v'(x)) \leq \mathrm{frac}(v'(y))$;
  4. for all clocks $x \in \mathcal{X}$ with $v(x) \leq c_x$, we have $\mathrm{frac}(v(x)) = 0$ if and only if $\mathrm{frac}(v'(x)) = 0$.
- Two states $(l, v), (l', v')$ of a timed automata are *region equivalent*, if:
  1. $l = l'$;
  2. v and v' are clock equivalent.
- A *region* is an equivalence class of region equivalence.

Non-deterministic probabilistic systems

- (Simple) probabilistic automata [SegalaLynch95] (similar to Markov decision processes):
  - Graph with nondeterministic and probabilistic choice.
  - E.g., from l_0 have a nondeterministic choice whether to take the left or right transition.
  - Right transition: make a probabilistic choice (l_2 with probability $\frac{1}{2}$, and l_3 with probability $\frac{1}{2}$).
  - Left transition: go to l_1 with probability 1.



Probabilistic simulation

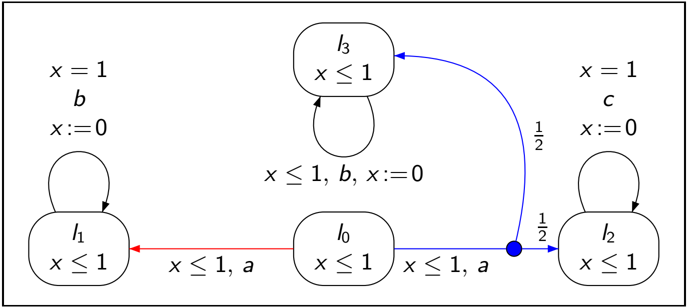
- Dist(S) is the set of probability distributions over S.
- Weight function [JonssonLarsen91]: for $\mu_1, \mu_2 \in \text{Dist}(S)$ with respect to relation $R \subseteq S \times S$ is a function $\Delta : S \times S \rightarrow [0, 1]$ such that:
  1. $\Delta(s_1, s_2)$ implies $(s_1, s_2) \in R$;
  2. $\sum_{s_2 \in S} \Delta(s_1, s_2) = \mu_1(s_1)$;
  3. $\sum_{s_1 \in S} \Delta(s_1, s_2) = \mu_2(s_2)$.
- Example:
  - $\mu_1(s_1) = 0.5, \mu_1(s_1') = 0.5$.
  - $\mu_2(s_2) = 0.3, \mu_2(s_2') = 0.4, \mu_2(s_2'') = 0.3$.
  - $R = ((s_1, s_2), (s_1, s_2'), (s_1', s_2'), (s_1', s_2''))$.
  - Then an example of a weight function for μ_1, μ_2 w.r.t. R is: $\Delta(s_1, s_2) = 0.3, \Delta(s_1, s_2') = \Delta(s_1', s_2') = 0.2, \Delta(s_1', s_2'')) = 0.3$.

Probabilistic simulation

- Probabilistic automaton $(S, Act, \rightarrow)$, where $\rightarrow \subseteq S \times Act \times$ Dist(S).
- Relation $R \subseteq S \times S$ is a probabilistic simulation relation [SegalaLynch95] if R satisfies the following condition: $(s_1, s_2) \in R$ implies that, for each $s_1 \xrightarrow{a} \mu_1$, there exists $s_2 \xrightarrow{a} \mu_2$ such that there is a weight function for μ_1, μ_2 w.r.t. R.
- s_2 probabilistically simulates s_1 if there exists a probabilistic simulation relation R such that $(s_1, s_2) \in R$.
- Relation $R \subseteq S \times S$ is a probabilistic bisimulation relation if both R and R^{-1} are probabilistic simulation relations.
- s_1 and s_1 are probabilistically bisimilar if there exists a probabilistic bisimulation relation R such that $(s_1, s_2) \in R$.

Probabilistic timed automata

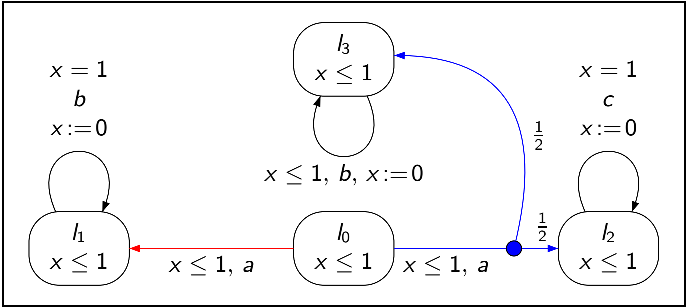
- Probabilistic timed automata (PTA) [Jensen96,KNSS02]:
  - Finite-state probabilistic automaton.
  - Finite set of *clocks*: real-valued variables increasing at the same rate as real-time.
  - Clock constraints (*invariants* in nodes, *guards* on edges).
  - Clock resets (set some clocks to 0 when an edge is traversed).



Probabilistic timed automata

- Semantics of probabilistic timed automata (in brief):
  - Represented by a "probabilistic automata with timing" $(S, Act, \rightarrow)$, where $\rightarrow \subseteq S \times \mathbb{R}_{\geq 0} \times Act \times \mathrm{Dist}(S)$.
  - States: of the form (l, v), as for timed automata.
  - Transitions: for example (only a selection...),

$$((l_0, v(x) = 0.2), a, 0.1, \mu((l_3, v(x) = 0.3) \mapsto \tfrac{1}{2}, (l_2, v(x) = 0.3) \mapsto \tfrac{1}{2}),$$
$$((l_0, v(x) = 0.2), a, 0.7, \mu((l_1, v(x) = 0.9) \mapsto 1)$$



Probabilistic timed simulation

- "Probabilistic automaton with timing" $(S, Act, \rightarrow)$, where $\rightarrow \subseteq S \times \mathbb{R}_{\geq 0} \times Act \times \mathrm{Dist}(S)$.
- Relation $R \subseteq S \times S$ is a probabilistic timed simulation relation if R satisfies the following condition:
  $(s_1, s_2) \in R$ implies that, for each $s_1 \xrightarrow{t,a} \mu_1$, there exists $s_2 \xrightarrow{t,a} \mu_2$ such that there is a weight function for μ_1, μ_2 w.r.t. R.
- s_2 probabilistically timed simulates s_1 if there exists a probabilistic timed simulation relation R such that $(s_1, s_2) \in R$.
- Relation $R \subseteq S \times S$ is a probabilistic timed bisimulation relation if both R and R^{-1} are probabilistic timed simulation relations.
- s_1 and s_1 are probabilistically timed bisimilar if there exists a probabilistic timed bisimulation relation R such that $(s_1, s_2) \in R$.
- (Probabilistic time-abstract (bi)simulation can be defined as for time-abstract (bi)simulation.)

Probabilistic timed (bi)simulation: algorithm

- Aim: to decide whether, given two PTA P_1, P_2, whether P_1 is probabilistically timed simulated by P_2.
  - More precisely: to decide whether the initial state of P_1 is probabilistically timed simulated by the initial state of P_2 on the "disjoint union" of P_1 and P_2.
- Combination of techniques for timed automata and for probabilistic automata:
  - Timed automata: [Čerāns91] for timed bisimulation, [TașiranAKB96] for timed simulation.
  - Probabilistic automata: [BEM00, ZHEJ08].

Probabilistic timed (bi)simulation: algorithm

- [Čerāns91,TaşiranAKB96]:
  - Construct region equivalence over *both* timed automata ("simulator" and "simulatee").
  - Theorem 1: if two states (l_1, v_1) and (l_2, v_2) in the same region r are such that (l_2, v_2) timed simulates (l_1, v_1), then *all* states (l_1', v_1') and (l_2', v_2') in r are such that (l_2', v_2') timed simulates (l_1', v_1').
  - Theorem 2: can consider only a finite number of time durations when deciding timed simulation.
- Proposal: apply region equivalence over PTA, adapt Theorems 1 and 2 to the probabilistic case.
- Adapt for probabilistic timed bisimulation.
- EXPTIME algorithm (optimal, same complexity as for timed automata).

Probabilistic timed bisimulation: logical characterization

- Probabilistic timed bisimilar states satisfy the same probabilistic timed temporal logic properties.
- ... but little work on using probabilistic timed Hennessy-Milner logic to characterize probabilistic timed bisimilarity.
- Related work:
  - [GregersenJensen95]: on "reactive probabilistic timed automata" (no nondeterminism between actions).
  - [ParmaSegala07]: logical characterization of probabilistic bisimilarity for probabilistic automata.
  - [BozelliLegayPinchinat09]: logical characterization of timed similarity for timed automata (actually, timed automata games).
- Proposal: combine [ParmaSegala07] and [BozelliLegayPinchinat09] to give a logical characterization of probabilistic timed bisimilarity for PTA.

Further work

- Probabilistic timed (bi)simulation can potentially provide the basis for further abstraction methods for PTA.
- Weak relations.
- Metrics and/or approximate equivalences.