Strict Divergence for Probabilistic Timed Automata

Angelo Troina

Dipartimento di Informatica, University of Turin, Italy

Work by J. Sproston

2nd PaCo meeting, 25th June 2009
Timed automata

- Timed automata [AlurDill94]:
  - Finite-state graph
  - 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

- **Probabilistic timed automata** [Jen96, KNSS02]:
  - **Finite-state Markov decision process** (probabilistic and nondeterministic choice)
  - 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

- Nondeterminism is resolved by strategies:
  - Strategy: function from the finite behaviour (history of the system) to the next nondeterministic choice to take.
  - A strategy induces a probability space over behaviours.
  - Have pessimistic and optimistic reasoning about correctness properties:
    - Pessimistic: corresponds to a strategy with the minimum probability of satisfying the property.
    - E.g., is the probability of reaching a goal state within 6000ns at least 0.8, no matter how unfavourable the nondeterministic choices are?
    - Optimistic: corresponds to a strategy with the maximum probability of satisfying the property.
    - E.g., can nondeterminism be resolved (in a favourable way) so that the probability of reaching a goal state within 6000ns is greater than 0.99?
Typical verification method:
- Transform to a finite-state Markov decision process (e.g., using region equivalence).
- Use a probabilistic model checking tool (e.g., PRISM).
What is (time) divergence?

- Models of timed systems can (erroneously) contain unrealistic behaviour.
- E.g., loop in $l_0$ forever: elapsed time in the system is 1.
- Timed automata: exist techniques to include only divergent behaviours (time exceeds any bound).
What is probabilistic divergence?

- E.g., take rightmost distribution from $l_0$: with probability $\frac{1}{2}$ elapsed time in the system is $\infty$ (good), but with probability $\frac{1}{2}$ elapsed time in the system is $1$ (bad).

- A solution: only consider those strategies that let time diverge with probability $1$ [KNSS02].
What is probabilistic divergence?

- **Probabilistically divergent strategies**: let time diverge with probability 1.
- Model checking algorithms under probabilistically divergent strategies:
  - EXPTIME algorithm if we know *a priori* (e.g., syntactically) that all strategies are probabilistic time divergent [KNSS02].
  - General case subsequently considered, but algorithm not optimal (2EXPTIME) [KNSW07].
  - Therefore provided an optimal EXPTIME algorithm in the general case.
What is the maximum probability of reaching $l_2$ from $(l_0, x = 0)$ under probabilistically divergent strategies?
The maximum probability of reaching $l_2$ from $(l_0, x = 0)$ under probabilistically divergent strategies is 1.
But what does a strategy have to do to achieve probability 1 of reaching $l_2$ from $(l_0, x = 0)$? Consider the following probabilistically divergent strategy:

- Let $\frac{1}{2}$ time units elapse in $l_0$, then take rightmost transition.
- If return to $l_0$, let $\frac{1}{4}$ time units elapse, then take rightmost transition.
- If return to $l_0$, let $\frac{1}{8}$ time units elapse, then take rightmost transition.
- ...
Strict divergence

- To achieve probability 1 of reaching $l_2$ from $(l_0, x = 0)$, a strategy must take the rightmost transition an infinite number of times before 1 time units elapse.
- Realistic? Not if the rightmost transition corresponds to a physical action.
- **Strictly divergent strategy**: time must diverge on *all* of the strategy’s paths.
Strict divergence

- What is the maximum probability of reaching $l_2$ from $(l_0, x = 0)$ under strictly divergent strategies?
- A strictly divergent strategy tries to reach $l_2$ via the rightmost transition, but cannot take this transition an infinite number of times.
- Intuitively, a strictly divergent strategy must ”give up” after a finite but arbitrary number of attempts to reach $l_2$. 
Strict divergence

There does not exist any strictly divergent strategy reaching \( l_2 \) from \( l_0 \) when \( x = 0 \) with probability 1.

But, for any \( \epsilon > 0 \), we can find strictly divergent strategy such that the probability of \( l_2 \) from \( l_0 \) when \( x = 0 \) is greater than \( 1 - \epsilon \).

In general: strictly divergent strategies can approximate arbitrarily closely the maximum reachability probability attained by probabilistically divergent strategies.
Strict divergence

- What is the **minimum** probability of reaching $l_2$ from $(l_1, x = 0)$?
  - The path that loops forever in $l_0$ is not time divergent, but has probability 0.
  - Probabilistically divergent strategies: min. prob. is 0.
  - Strictly divergent strategies: min. prob. is 1.

- Minimum reachability probabilities may differ arbitrarily much between probabilistically and strictly divergent strategies.
Present a model-checking algorithm which considers only strictly divergent strategies.

Consider maximum reachability properties.

Non-strict bounds in properties (e.g., maximum probability of reaching $l_2$ is $\leq \frac{99}{100}$): similar to the algorithm for probabilistically divergent strategies.
Model-checking algorithms: strict divergence

• Strict bounds in properties (e.g., maximum probability of reaching \( l_2 \) is < 1):
  
  • For each state, distinguish between the following two cases:
    
    1. The supremum probability can be attained by a strictly divergent strategy.
    2. Strictly divergent strategies can only approximate the supremum probability.

• Compute the set of states in Case 1.
• E.g., from \((l_0, x = 0)\), the maximum probability of reaching \( l_2 \) is < 1?
  
  • Compute the supremum probability of reaching \( l_2 \) from \((l_0, x = 0)\); say this is 1.
  • If \((l_0, x = 0)\) is in the set of Case 1 states, answer No, otherwise Yes.
Model-checking algorithms: strict divergence

- Minimum reachability properties: relies on:
  1. Reasoning about non-strict/strict bounds similar to that for maximum reachability properties.
  2. Reasoning about infinite sojourns in *end components* (MDP analogue of bottom strongly connected components).

- Not limited to reachability properties: can apply all results to *Ptctl* (probabilistic, timed temporal logic).

- Algorithms are EXPTIME-complete.