Embedded Systems Specification and Design
Model-based Design and Verification

David Kendall
Going further

- Stopwatch automata
- Costs (Priced Timed Automata)
- Statistical model checking
- Hybrid and stochastic systems
Stopwatch automata

- Can use clocks with a rate of 0 in one or more locations.
- Clock \( ax \) in Task has a rate of 0 in location Blocked.
- The rate is specified using the notation for the derivative, e.g. \( ax' == 0 \).
- Reachability is undecidable for stopwatch automata but ...
- UPPAAL uses an over-approximation algorithm to allow a ’classical’ model-checking approach.
- See demo (also Gantt chart in concrete simulator)

Task

Scheduler
A more general expression can be used to determine the rate of a clock, e.g. \( C' = 4 \).

The rate need not be a constant expression and may depend on the values of discrete state variables.

Clocks with this kind of rate are often used to measure the costs associated with the use of resources.

’Classical’ model-checking is not available for clocks with this kind of rate but . . .

Statistical model-checking can be used to simulate behaviour and to estimate the probability that properties will be satisfied.
Statistical model checking

Monitor simulations of a system model and use statistical techniques to determine, with some degree of confidence, whether or not properties are satisfied

Queries supported by UPPAAL-SMC

- **Simulation** — simulate \( N [\leq \text{bound}] \{E_1, \ldots, E_k\} \)
  
  e.g. simulate 1 \([A.x \leq 2]\) \{A.x, C\}

- **Probability estimation** — \(\Pr[\text{bound}](\psi)\)

- **Hypothesis testing** — \(\Pr[\text{bound}](\psi) \geq p\)

- **Probability comparison** —
  
  \(\Pr[\text{bound1}](\psi_1) \geq \Pr[\text{bound2}](\psi_2)\)

Bounds can be given

- Implicitly by time, e.g. \([\leq 600]\)
- Explicitly by cost, e.g. \([C \leq 6]\)
- By number of discrete steps, e.g. \([\# \leq 1000]\)
Hybrid and Stochastic Systems

*Hybrid* — mixed continuous and discrete dynamics

*Stochastic* — having a random probability distribution

- Clock rates can depend not only on the values of discrete variables but also on other clocks (effectively supports representation of ODE’s)
- Time elapsed chosen from uniform distribution over bounded time delays and exponential distribution (with given rate) over unbounded time delays
- Probabilistic choices represented by *branch points*
  - Each branch has a probability of being chosen of its weight over the sum of the weights of all branches at the branch point
Summary

- UPPAAL-SMC conducts simulations of hybrid, stochastic systems, monitors them, and uses statistical methods to decide, with some degree of confidence, whether or not properties are satisfied.
- SMC is a compromise between testing and classical model-checking.
- Requires much less memory and time than classical model checking to produce a result.
- Becoming more widely used in industrial applications of:
  - software engineering
  - embedded systems
  - systems biology