Model checking Continuous Stochastic Logic

against

labelled Continuous Time Markov Chains

screencast by Anne Remke, University of Twente
A Labelled CTMC is a tuple \((S, R, L)\)

- \(S\) is a countable set of states
- *rate matrix*: \(R : S \times S \rightarrow \mathbb{R}_{\geq 0}\) \(R = (R(i, j))\)
- \(R(s, s')\): “speed” to leave \(s\) for \(s'\)
- \(E(s) = R(s, S) = \sum_{s' \in S \setminus \{s\}} R(s, s')\) is the *exit rate* from state \(s\)
- \(L : S \rightarrow 2^{AP}\) is a labelling function that assigns to each state zero or more *atomic properties* taken from set \(AP\)
Continuous stochastic logic (CSL)

**State-formulas**

\[ \Phi ::= a \mid \neg \Phi \mid \Phi \lor \Phi \mid S_{\leq p}(\Phi) \mid P_{\leq p}(\varphi) \]

- \( S_{\leq p}(\Phi) \): probability that \( \Phi \) holds in steady state is \( \leq p \)
- \( P_{\leq p}(\varphi) \): probability that paths fulfill \( \varphi \) is \( \leq p \)

**Path-formulas**

\[ \varphi ::= X^t \Phi \mid \Phi U^t \Phi \]

- \( X^t \Phi \): next state is reached at time \( t \in l \) and fulfills \( \Phi \)
- \( \Phi U^t \Psi \): \( \Phi \) holds along the path until \( \Psi \) holds at time \( t \in l \)
Example CSL state formulae

- transient probability of state $s$ at time 3 is at most 20%

- steady-state probability of being in state $s$ is at most 0.00001

- in the long run, for at least 99% of time at least 2 processors are up
Example CSL path formulae

- the probability of the system going down between 10 and 30 time units is at most 0.01

- the probability of the system going down in 10 time units after continuously operating with at least 2 processors is at most 0.01
Model-checking CSL

- checking whether a state \( s \) in a CTMC satisfies a CSL formula is performed in the same way as for CTL:
  - compute recursively the set \( \text{Sat}(\Phi) \) of states that satisfy \( \Phi \)
  - check whether state \( s \) belongs to \( \text{Sat}(\Phi) \)
- for the non-stochastic part: as for CTL
- how to compute \( \text{Sat}(\Phi) \) for the stochastic operators?
Model-checking the steady-state operator (I)

For an ergodic (strongly-connected) CTMC:

\[ s \in Sat(S_{\leq}p(\Phi)) \iff \sum_{s' \in Sat(\Phi)} \pi_{s'} \leq p \]

\[ \implies \] this boils down to a standard steady-state analysis
Model-checking the steady-state operator (II)

For an arbitrary CTMC:

- determine the *bottom* strongly-connected components
- for BSCC $B$ determine the steady-state probability of a $\Phi$-state
- compute the probability to reach BSCC $B$ from state $s$
- check whether

$$\sum_{B} \left( \Pr\{ \text{reach } B \text{ from } s \} \cdot \sum_{s' \in B \cap \text{Sat}(\Phi)} \pi^B_{s'} \right) \preceq p$$
Verifying steady-state properties: an example (I)

first determine the bottom strongly-connected components
Verifying steady-state properties: an example (II)

$s \models S_{>75\%}(\text{green ?})$ iff
Check out how to check the next and the until operator in my next screencast!