DD2552 - Seminars on Theoretical Computer Science, Programming Languages and Formal Methods, Seminar 3

Karl Palmskog (palmskog@kth.se)

2021-09-06

Last Seminar and Today

Last seminar:

- formal semantics of PCTL fragment
- reasoning manually on DTMCs with PCTL

Today:

- more PCTL operators
- deciding PCTL formulas on DTMCs
- intuitions behind CTMCs and CSL

Basic PCTL

$$\phi ::= \top \mid a \mid \neg\phi \mid \phi \wedge \phi \mid P_{\geq\theta}(\psi)$$
$$\psi ::= \phi \, U^{\leq t} \, \phi$$
$$t \in Z^{\geq 0}, \quad \theta \in [0, 1]$$

extensions:

- disjunction, implication
- next operator
- unbounded until operator
- weak until
- steady state operator
- probability equals operator
- all and globally operators
- exists and finally operators

Disjunction and Implication

$$\phi ::= \ldots \mid \phi \vee \phi \mid \phi \rightarrow \phi$$

Approach to avoid growing language for tools:

- define semantics of $\phi \vee \phi'$ and $\phi \rightarrow \phi'$
- define translation from $\phi \vee \phi'$ to $\phi_{\vee}$ in basic PCTL
- define translation from $\phi \rightarrow \phi'$ to $\phi_{\rightarrow}$ in basic PCTL

Next operator

$$\psi ::= \ldots \mid X(\phi)$$

- all paths have a current and next state (since infinite)
- "in the next state in the path"

Unbounded until

$$\psi ::= \ldots \mid \phi \, U \, \phi$$

- another possibility: extend t with ∞
- can deal with this in finite-state models
- how do we check this for a prefix?

Weak until operator

$$\psi ::= \ldots \mid \phi \, W \, \phi$$

- right-hand side does not have to become true

Steady state operator

$$\phi ::= \ldots \mid S_{<\theta}(\phi)$$

- "in the long run"
- "in the equilibrium state"
- see: ergodic analysis of Markov chains

$$S_{<0.01}(\texttt{num\_sensors} < \texttt{min\_sensors})$$

Probability equals operator

$$\gamma ::= P_{=?}(\psi)$$

- logics usually deal with propositions ("less than 0.5")
- convenient to be able to get actual probability
- more expensive as required precision increases

$$P_{=?}(\texttt{proc2\_terminate}\, U\, \texttt{proc1\_terminate})$$

All and globally operators

$$\phi ::= \ldots \mid A(\psi)$$
$$\psi ::= \ldots \mid G(\phi)$$

- "Along all paths starting in this state"
- "Globally for states in this path"

$$A(G(\texttt{x\_lt\_10}))$$

Exists and finally operators

$$\phi ::= \ldots \mid E(\psi)$$
$$\psi ::= \ldots \mid F(\phi)$$

- "There exists a path starting in this state"
- "Finally for some state in this path"
- F can be extended with time bound

$$P_{<=0.1}(F(\texttt{num\_errors\_gt}_5))$$

Deciding PCTL formulas on DTMCs

- assume we reduce formulas ϕ, ψ to ones in minimal set
- how do we model check against some DTMC $\mathcal{M}$?
- how does decision time vary with formula and model size?

Key idea of initial model checking algorithm

- Hansson and Jonsson, following Clarke et al. for CTL
- idea: unwind the formula and label each state s with subformulas true in s
- start by labeling each state with its atomic true formulas
- $\neg$ and $\vee$ have straightforward recursive definitions

Complexity

- model checking CTL grows with size of formula times size of state space
- PCTL model checking is similar (better for restricted cases)

Continuous Time Markov Chains (CTMCs)

- changing models of formulas changes the game!
- continuous time Markov chains stay for a real-timed duration in each state
- replace transition matrix with **transition rate matrix**

$\mathcal{M} = (S, s_i, Q, L)$ where

- S is a (finite) set of states
- $s_i \in S$ is the initial state
- Q is a matrix where
  - $Q(s_j, s_k)$ is the rate of transition from s_j to s_k
  - $Q(s_j, s_j)$ is constrained to be $-(\sum_{j \neq k} Q(s_k, s_j))$
- $L : S \mapsto 2^{\mathrm{AP}}$

Paths for CTMCs

- paths π must now track the (real-valued) time that was spent in states
- define CTMC path as function from positive reals to states