Directed Model Checking

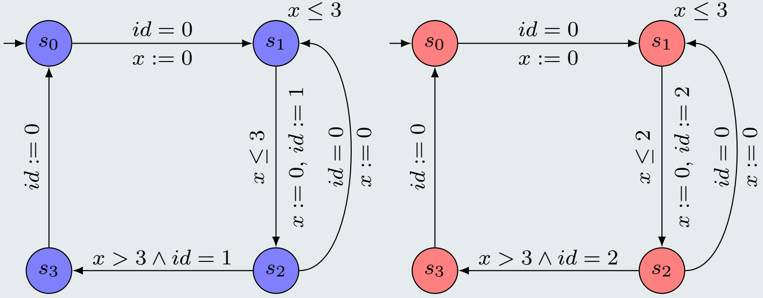
Sebastian Kupferschmid

Albert-Ludwigs-Universität Freiburg

February 14, 2007

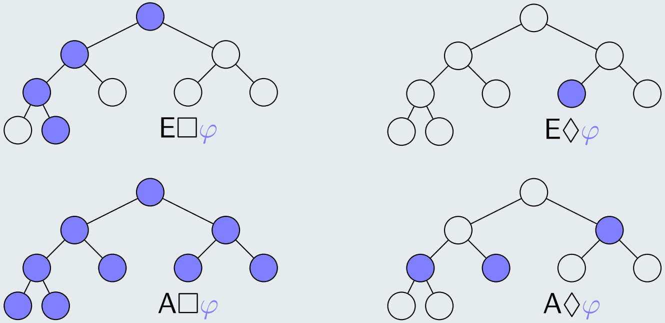
Transition System

A Timed Automata System



Temporal Formulas

Computation Tree Logic



Model Checking and Planning

Problems

Model Checking

- Transition system T, initial state s_0, **temporal** formula φ
- $T,\, s_0 \overset{?}{\models} \varphi$

Planning

- Set of vars, operators, initial state s_0, **goal** formula G
- Seq. of operators $o_1,\, \dots,\, o_n$ s.t. $s_0 \xrightarrow{o_1} s_1,\, \dots,\, s_{n-1} \xrightarrow{o_n} s_g$ with $s_g \models G$

Reachability Analysis

Liveness (progress) properties

- Something good should happen
- Failure can be demonstrated only by an infinite sequence

Model Checking Safety (invariant) properties

- Nothing bad should happen
- Failure can be demonstrated by a finite seq. of transitions
- E.g. $T, s_0 \models \mathsf{A}\Box\varphi$ or $T, s_0 \not\models \mathsf{E}\Diamond\neg\varphi$

Directed Model Checking

Problem

- Find states violating a given safety property
- State explosion problem
- Planning Techniques for falsification