Directed Model Checking

Sebastian Kupferschmid

Transition System

A Timed Automata System

Directed Model Checking
Sebastian Kupferschmid
Temporal Formulas

Computation Tree Logic

- $E\Box \varphi$
- $A\Box \varphi$
- $E\Diamond \varphi$
- $A\Diamond \varphi$
## Problems

<table>
<thead>
<tr>
<th>Model Checking</th>
<th>Planning</th>
</tr>
</thead>
</table>
| • Transition system $T$, initial state $s_0$, **temporal** formula $\varphi$  
  $T, s_0 \models \varphi$ | • Set of vars, operators, initial state $s_0$, **goal** formula $G$
  • Seq. of operators $o_1, \ldots, o_n$
  s.t. $s_0 \xrightarrow{o_1} s_1, \ldots, s_{n-1} \xrightarrow{o_n} s_g$
  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. $T, s_0 \models A\Box \varphi$ or $T, s_0 \not\models E\Diamond \neg \varphi$
Problem

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