Focus on model checking labeled transition systems against computational tree logic (CTL) properties

creencast by Anne Remke, University of Twente
Transition systems
- Model to describe the behavior of systems
- Nodes represent states
- Edges model transitions
A labelled transition system (LTS) is a triple \((S, T, L)\) with:

- A finite set of states \(S\)
- A transition relation \(T \subseteq S \times S\)
- A labelling function \(L : S \rightarrow AP\)
Triple modular redundant system
Branching notion of time

**Computational Tree Logic** based on a branching notion of time

- Evolution is represented by an infinite tree of states
- One state might have several possible successor states
State and path properties

**State vs path properties**

- **a path** is a (finite or infinite) sequence of states $s_0, s_1, s_2, s_3, \cdots$ such that $(s_i, s_{i+1}) \in T$, for all $i \geq 0$

- **state properties**: validity of properties in states

- **path properties**: validity of properties for some (or all) paths starting from a state
Statements about states and, all or some, paths starting in a state

State-formulas

\[ \Phi ::= a \mid \neg \Phi \mid \Phi \lor \Phi \mid \exists \varphi \mid \forall \varphi \]

- \( a \) atomic proposition
- \( \exists \varphi \) there Exists a path that fulfills \( \varphi \)
- \( \forall \varphi \) All paths fulfill \( \varphi \)
Path-formulas \( \varphi ::= X\,\Phi \mid \Phi U \Phi \)

- \(X\,\Phi\) the next state fulfills \(\Phi\)
- \(\Phi U \Psi\) \(\Phi\) holds along the path Until \(\Psi\) holds
- \(\Diamond\,\Phi\) true U \(\Phi\), i.e., eventually \(\Phi\)
- \(\Box\,\Phi\) \(\neg\Diamond\neg\Phi\), i.e., always \(\Phi\)
Illustration of the semantics

\[ \exists \Diamond red \]

\[ \exists \square red \]

\[ \exists (yellow \cup red) \]

\[ \forall \Diamond red \]

\[ \forall \square red \]

\[ \forall (yellow \cup red) \]
Example properties in CTL

Reachability
- Simple reachability $\exists \diamond \psi$
- Conditional reachability $\exists (\Phi U \Psi)$
- Reachability from any state $\forall \Box (\exists \diamond \Phi)$

safety
- Simple safety $\forall \Box \Phi$
- Conditional safety $\forall (\Phi U \Psi) \lor \forall \Box \Phi$

liveness
$\forall \Box (\Phi \Rightarrow \forall \diamond \Psi)$

fairness
$\forall \Box (\forall \diamond \Phi)$
Check out:

Next screencast on

Model checking algorithms for CTL