Introduction to Model Checking

René Thiemann

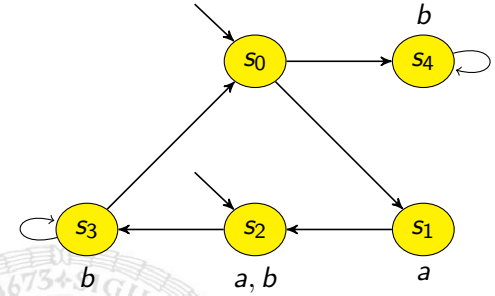
Institute of Computer Science
University of Innsbruck

WS 2007/2008

Outline

Last Exercises

$\Phi = \mathsf{A}\,(a\,\mathsf{U}\,b) \vee \mathsf{E}\,\mathsf{X}\,(\mathsf{A}\,\mathsf{G}\,b)$

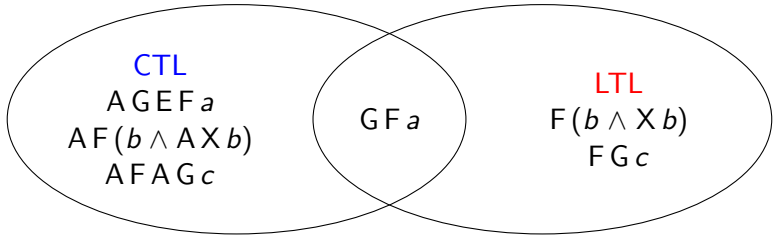


Last Exercises

Provide a direct fixpoint characterization of $Sat(\mathsf{E}\,\mathsf{G}\,\Phi)$ without using the following equivalence.

$$\mathsf{E}\,\mathsf{G}\,\Phi \equiv \neg\mathsf{A}\,\mathsf{F}\,\neg\Phi \equiv \neg\mathsf{A}\,\mathsf{true}\,\mathsf{U}\,\neg\Phi$$

Expressiveness of CTL and LTL



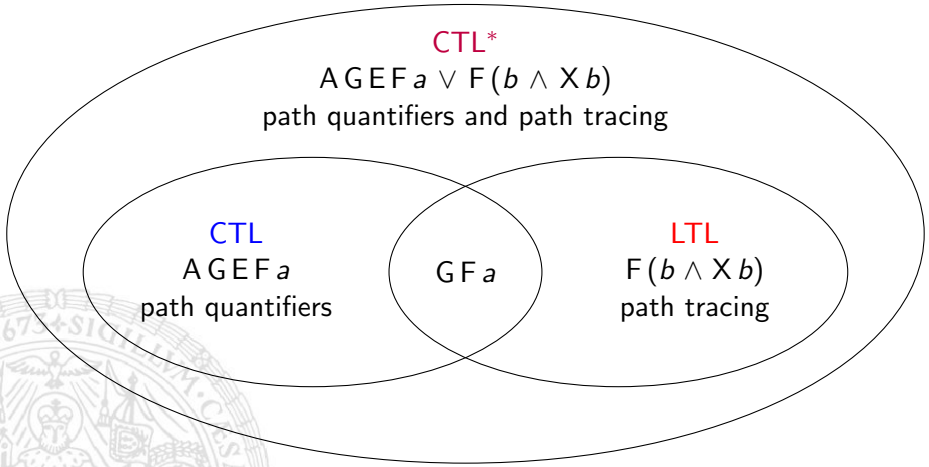
Theorem (Clarke, Draghicescu)

Let Φ be a CTL-state-formula and φ the LTL-formula that is obtained by eliminating all path quantifiers in Φ. Then:

$\Phi \equiv \varphi$ *or there does not exist any LTL-formula that is equivalent to* Φ.

Hence, to prove that A F A G c is not LTL-expressible it suffices to show that A F A G a and F G c are not equivalent.

Expressiveness of CTL and LTL



CTL*

- Formulas over states (capital greek letters)
  - true
  - $a \in AP$ — atomic proposition
  - $\neg\Phi$ and $\Phi \wedge \Psi$ — negation and conjunction
  - $\mathsf{E}\,\varphi$ — there exists a path fulfilling φ
  - $\mathsf{A}\,\varphi$ — all paths fulfill φ
- Formulas over paths (lower case greek letters)
  - $\mathsf{X}\,\varphi$ — in the next moment φ holds
  - $\varphi\,\mathsf{U}\,\psi$ — φ holds until ψ
  - $\neg\varphi$ and $\varphi \wedge \psi$ — negation and conjunction
  - Φ — the current state satisfies Φ

Semantics of CTL*

A state-formula Φ holds in state s (written $s \models \Phi$) iff

$s \models \text{true}$

$s \models a$ iff $a \in L(s)$

$s \models \neg\Phi$ iff $s \not\models \Phi$

$s \models \Phi \wedge \Psi$ iff $s \models \Phi$ and $s \models \Psi$

$s \models \mathsf{E}\,\varphi$ iff $\pi \models \varphi$ for some path π that starts in s

$s \models \mathsf{A}\,\varphi$ iff $\pi \models \varphi$ for all paths π that start in s

A path-formula φ holds for path π (written $\pi \models \varphi$) iff

$\pi \models \mathsf{X}\,\varphi$ iff $\pi[1..] \models \varphi$

$\pi \models \varphi\,\mathsf{U}\,\psi$ iff $(\exists\, j \geqslant 0.\, \pi[j..] \models \psi$ and $(\forall\, 0 \leqslant k < j.\, \pi[k..] \models \varphi))$

$\pi \models \varphi \wedge \psi$ iff $\pi \models \varphi$ and $\pi \models \psi$

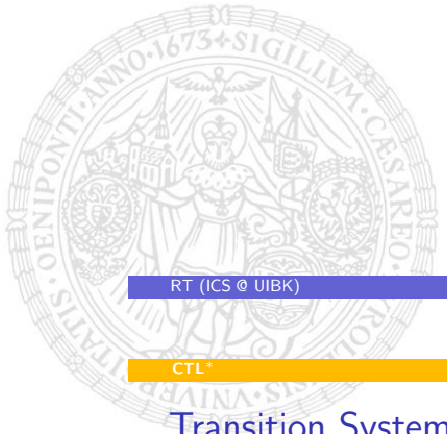
$\pi \models \neg\varphi$ iff $\pi \not\models \varphi$

$\pi \models \Phi$ iff $\pi[0] \models \Phi$

Derived Operators

As usual one can use the following shortcuts:

$$\begin{aligned} \mathsf{F}\,\varphi &\equiv \mathsf{true}\,\mathsf{U}\,\varphi \\ \mathsf{G}\,\varphi &\equiv \neg\mathsf{F}\,\neg\varphi \end{aligned}$$



Transition System Semantics for CTL*

- For state-formula Φ, the satisfaction set $\mathit{Sat}(\Phi)$ is defined by:

$$\mathit{Sat}(\Phi) \;=\; \{\, s \in S \mid s \models \Phi \,\}$$

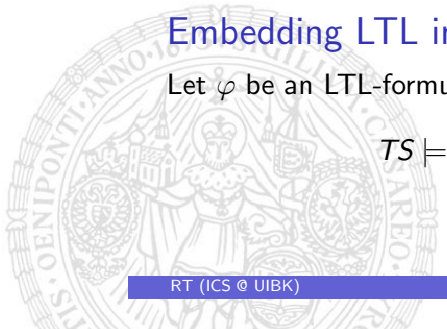
- TS satisfies state-formula Φ iff Φ holds in all its initial states:

$$I \subseteq \mathit{Sat}(\Phi)$$

Embedding LTL in CTL*

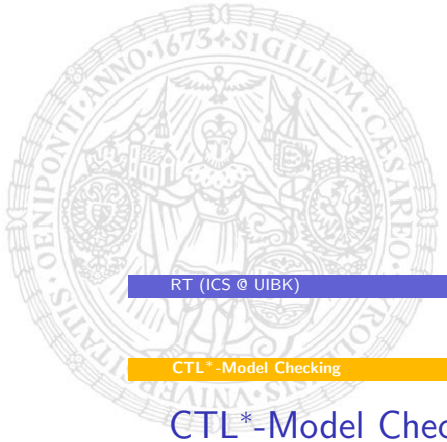
Let φ be an LTL-formula. Then

$$\mathit{TS} \models \varphi \text{ (LTL)} \quad \text{iff} \quad \mathit{TS} \models \mathsf{A}\,\varphi \text{ (CTL}^*\text{)}$$



Example

On all paths it is infinitely often served and there always is a possibility to get back to the main menu



CTL*-Model Checking Algorithm [Emerson, Lei]

Eliminating Existential Path Quantifiers

Lemma

For every path-formula φ the following equivalence is valid:

$$\mathsf{E}\,\varphi \equiv \neg\mathsf{A}\,\neg\varphi$$

Proof.

$s \models \mathsf{E}\,\varphi$

iff there is a path π starting in s such that $\pi \models \varphi$

iff it is not the case that there is no path π starting in s with $\pi \models \varphi$

iff it is not the case that all paths π starting in s violate $\pi \models \varphi$

iff it is not the case that all paths π starting in s satisfy $\pi \models \neg\varphi$

iff it is not the case that $s \models \mathsf{A}\,\neg\varphi$

iff $s \models \neg\mathsf{A}\,\neg\varphi$

Use Bottom-Up CTL-Model Checking Procedure

Let $TS = (S, \rightarrow, I, AP, L)$

Compute sets $Sat(.)$ for state-formulas in a bottom-up way:

- $Sat(\text{true}) = S$
- $Sat(a) = \{s \mid a \in L(s)\}$
- $Sat(\neg\,\Phi) = S \setminus Sat(\Phi)$
- $Sat(\Phi \wedge \Psi) = Sat(\Phi) \cap Sat(\Psi)$

Use LTL-Model Checker for Universal Formulas

- $s \in \mathit{Sat}(\mathrm{A}\,\varphi)$ iff all paths π starting in s satisfy $\pi \models \varphi$
- Essentially, φ is LTL-formula but may contain CTL*-state-formulas

$\Rightarrow$ LTL-model checker not directly applicable

Solution

- States which satisfy contained CTL*-state formulas are known

$\Rightarrow$
- Replace every maximal state-formula Ψ in φ which is not an atomic proposition by a new atomic proposition a_Ψ, result: LTL-formula φ'
- Extend labeling of states: Whenever $s \in \mathit{Sat}(\Psi)$ then add a_Ψ to the set of labels of s.

- Afterwards apply LTL-model checker to determine $\mathit{Sat}(\mathrm{A}\,\varphi)$:

$$s \in \mathit{Sat}(\mathrm{A}\,\varphi) \text{ iff } s \models \varphi'$$

Example

Comparison

Formalism	LTL	CTL	CTL*
MC-algorithm	NBAs	*Sat*-computation (set operations)	*Sat*-computation (set ops. + NBAs)
MC-complexity (fixed formula)	PSPACE-comp. linear	linear linear	PSPACE-comp. linear

Exercises

- Prove that there is no LTL-formula which is equivalent to $\mathsf{A}\,\mathsf{F}\,(b \wedge \mathsf{A}\,\mathsf{X}\,b)$
- Consider the formula $\Phi = \mathsf{A}\,\mathsf{G}\,((\neg \mathsf{E}\,\mathsf{F}\,\mathit{serve}) \vee (\mathsf{E}\,\mathsf{G}\,\mathsf{F}\,\mathit{main}))$
  - Try to formulate the meaning in words
  - Apply the CTL*-model checking algorithm on the following example. Do not construct the NBAs for the LTL-model checking, but do LTL-model checking intuitively.