Introduction to Model Checking

René Thiemann

Institute of Computer Science

University of Innsbruck

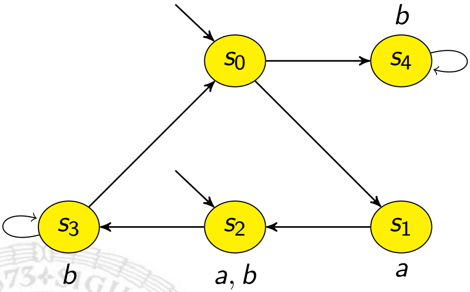
WS 2007/2008

Outline

- Last Exercises
- Expressiveness of CTL and LTL
- CTL*
- CTL*-Model Checking

Last Exercises

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

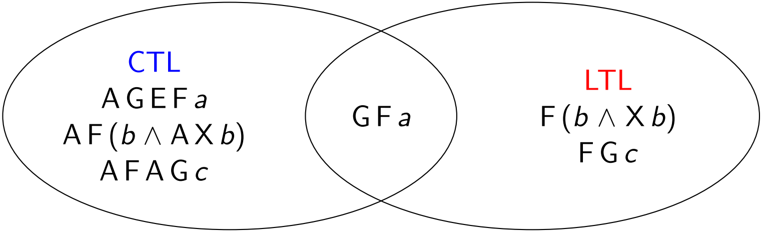


Last Exercises

Provide a direct fixpoint characterization of $\mathit{Sat}(\mathsf{E}\,\mathsf{G}\,\Phi)$ 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



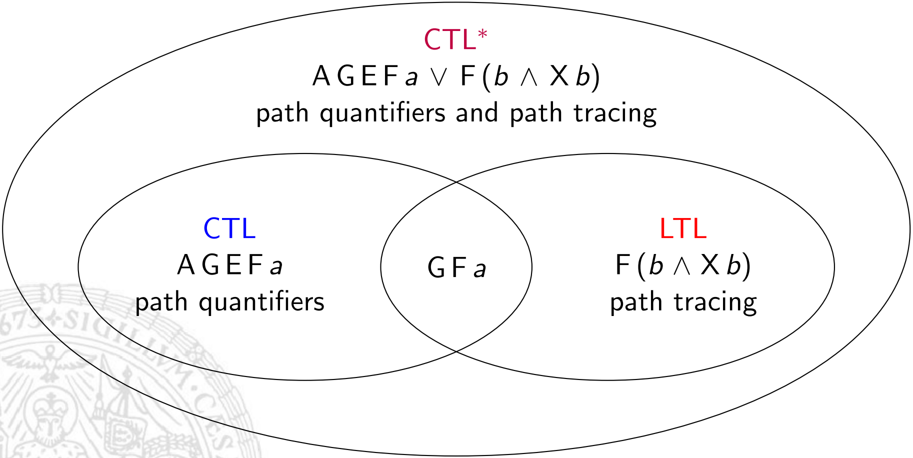
Theorem (Clarke, Draghicescu)

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

$$\Phi \equiv \varphi \text{ or there does not exist any LTL-formula that is equivalent to } \Phi.$$

Hence, to prove that $\mathsf{A\,F\,A\,G}\,c$ is not LTL-expressible it suffices to show that $\mathsf{A\,F\,A\,G}\,a$ and $\mathsf{F\,G}\,c$ 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

$$
\begin{array}{lll}
s \models \mathsf{true} & & \\
s \models a & \text{iff} & a \in L(s) \\
s \models \neg\,\Phi & \text{iff} & s \not\models \Phi \\
s \models \Phi \wedge \Psi & \text{iff} & s \models \Phi \text{ and } s \models \Psi \\
s \models \mathsf{E}\,\varphi & \text{iff} & \pi \models \varphi \text{ for some path } \pi \text{ that starts in } s \\
s \models \mathsf{A}\,\varphi & \text{iff} & \pi \models \varphi \text{ for all paths } \pi \text{ that start in } s
\end{array}
$$

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

$$
\begin{array}{ll}
\pi \models \mathsf{X}\,\varphi & \text{iff } \pi[1..] \models \varphi \\
\pi \models \varphi\,\mathsf{U}\,\psi & \text{iff } (\exists\, j \geqslant 0.\, \pi[j..] \models \psi \text{ and } (\forall\, 0 \leqslant k < j.\, \pi[k..] \models \varphi)) \\
\pi \models \varphi \wedge \psi & \text{iff } \pi \models \varphi \text{ and } \pi \models \psi \\
\pi \models \neg\varphi & \text{iff } \pi \not\models \varphi \\
\pi \models \Phi & \text{iff } \pi[0] \models \Phi
\end{array}
$$

Derived Operators

As usual one can use the following shortcuts:

$$\mathsf{F}\,\varphi \equiv \mathsf{true}\,\mathsf{U}\,\varphi$$
$$\mathsf{G}\,\varphi \equiv \neg\mathsf{F}\,\neg\varphi$$

Transition System Semantics for CTL*

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

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

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

$$I \subseteq Sat(\Phi)$$

Embedding LTL in CTL*

Let φ be an LTL-formula. Then

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

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

- $s \in Sat(\mathsf{A}\,\varphi)$ 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 $s \in Sat(\Psi)$ then add a_Ψ to the set of labels of s.

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

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

Example

Comparison

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

Exercises

- Prove that there is no LTL-formula which is equivalent to $\mathsf{A\,F}\,(b \wedge \mathsf{A\,X}\,b)$
- Consider the formula $\Phi = \mathsf{A\,G}\,((\neg \mathsf{E\,F}\,\mathit{serve}) \vee (\mathsf{E\,G\,F}\,\mathit{main}))$
  - 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.