Bisimulation and CTL*

Lecture #24 of Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

E-mail: `katoen@cs.rwth-aachen.de`

January 28, 2009

Overview Lecture #24

$\Rightarrow$ Repetition: Bisimulation equivalence

- CTL* equivalence

Bisimulation on states

$\mathcal{R} \subseteq S \times S$ is a *bisimulation* on *TS* if for any $(s_1, s_2) \in \mathcal{R}$:

- $L(s_1) = L(s_2)$
- if $s_1' \in \mathit{Post}(s_1)$ then there exists an $s_2' \in \mathit{Post}(s_2)$ with $(s_1', s_2') \in \mathcal{R}$
- if $s_2' \in \mathit{Post}(s_2)$ then there exists an $s_1' \in \mathit{Post}(s_1)$ with $(s_1', s_2') \in \mathcal{R}$

s_1 and s_2 are *bisimilar*, $s_1 \sim_{TS} s_2$, if $(s_1, s_2) \in \mathcal{R}$ for some bisimulation $\mathcal{R}$ for *TS*

$$s_1 \sim_{TS} s_2 \quad \text{if and only if} \quad TS_{s_1} \sim TS_{s_2}$$

Bisimulation equivalence

$$\begin{array}{ccc} s_1 & \longrightarrow & s_1' \\ \mathcal{R} & & \\ s_2 & & \end{array} \quad \text{can be completed to} \quad \begin{array}{ccc} s_1 & \longrightarrow & s_1' \\ \mathcal{R} & & \mathcal{R} \\ s_2 & \longrightarrow & s_2' \end{array}$$

and

$$\begin{array}{ccc} s_1 & & \\ \mathcal{R} & & \\ s_2 & \longrightarrow & s_2' \end{array} \quad \text{can be completed to} \quad \begin{array}{ccc} s_1 & \longrightarrow & s_1' \\ \mathcal{R} & & \mathcal{R} \\ s_2 & \longrightarrow & s_2' \end{array}$$

Coarsest bisimulation

$\sim_{TS}$ is an equivalence and the coarsest bisimulation for TS

Quotient transition system

For $TS = (S, Act, \rightarrow, I, AP, L)$ and bisimulation $\sim_{TS} \subseteq S \times S$ on TS let

$$TS/\sim_{TS} = (S', \{ \tau \}, \rightarrow', I', AP, L'), \qquad \text{the } \textit{quotient} \text{ of } TS \text{ under } \sim_{TS}$$

where

- $S' = S/\sim_{TS} = \{ [s]_\sim \mid s \in S \}$ with $[s]_\sim = \{ s' \in S \mid s \sim s' \}$
- $\rightarrow'$ is defined by: $$\frac{s \xrightarrow{\alpha} s'}{[s]_\sim \xrightarrow{\tau}{}' [s']_\sim}$$
- $I' = \{ [s]_\sim \mid s \in I \}$
- $L'([s]_\sim) = L(s)$

Overview Lecture #24

- Repetition: Bisimulation equivalence

$\Rightarrow$ CTL* equivalence

Syntax of CTL*

CTL* *state-formulas* are formed according to:

$$\Phi ::= \text{true} \;\Big|\; a \;\Big|\; \Phi_1 \wedge \Phi_2 \;\Big|\; \neg\Phi \;\Big|\; \exists\varphi$$

where $a \in$ *AP* and φ is a path-formula

CTL* *path-formulas* are formed according to the grammar:

$$\varphi ::= \Phi \;\Big|\; \varphi_1 \wedge \varphi_2 \;\Big|\; \neg\varphi \;\Big|\; \bigcirc\varphi \;\Big|\; \varphi_1 \,\mathsf{U}\, \varphi_2$$

where Φ is a state-formula, and φ, φ_1 and φ_2 are path-formulas

in CTL*: $\forall\varphi \;=\; \neg\exists\neg\varphi$. This does not hold in CTL!

CTL* equivalence

States s_1 and s_2 in *TS* (over *AP*) are CTL*-equivalent:

$$s_1 \equiv_{CTL^*} s_2 \quad \text{if and only if} \quad (s_1 \models \Phi \text{ iff } s_2 \models \Phi)$$

for all CTL* state formulas over *AP*

$$TS_1 \equiv_{CTL^*} TS_2 \quad \text{if and only if} \quad (TS_1 \models \Phi \text{ iff } TS_2 \models \Phi)$$

for any sublogic of CTL*, logical equivalence is defined analogously

Trace equivalence and LTL equivalence

Let *TS* be a *finite* transition system and s, s' states in *TS*

The following statements are equivalent:

(1) $\mathit{Traces}(s) = \mathit{Traces}(s')$

(2) s and s' are LTL-equivalent, i.e., $s \equiv_{\mathit{LTL}} s'$

Bisimulation vs. CTL* and CTL equivalence

Let *TS* be a *finite* transition system and s, s' states in *TS*

The following statements are equivalent:

(1) $s \sim_{TS} s'$

(2) s and s' are CTL-equivalent, i.e., $s \equiv_{CTL} s'$

(3) s and s' are CTL*-equivalent, i.e., $s \equiv_{CTL^*} s'$

this is proven in three steps: $\equiv_{CTL} \subseteq \sim \subseteq \equiv_{CTL^*} \subseteq \equiv_{CTL}$

Proof: $\equiv_{CTL} \quad \subseteq \quad \sim_{TS}$

Example master formula

Proof: $\sim_{TS} \quad \subseteq \quad \equiv_{CTL^*}$

Important remarks

- Consider the following CTL fragment, say CTL$^-$:

$$\Phi ::= \text{true} \;\Big|\; a \;\Big|\; \Phi_1 \wedge \Phi_2 \;\Big|\; \neg\Phi \;\Big|\; \exists\bigcirc\Phi$$

- Then: $\equiv_{CTL^-}$ coincides with $\equiv_{CTL^*}$

$\Rightarrow$ CTL$^-$ thus also characterizes bisimulation

- The relations $\sim$, $\equiv_{CTL^*}$, and $\equiv_{CTL}$ coincide
  - for finite transition systems
  - for finitely-branching transition systems; Why?
  - but not for arbitrary infinite transition systems' Why?

Bisimulation vs. CTL*-equivalence

For any transition systems *TS* and *TS*$'$ (over *AP*):

$$TS \sim TS' \quad \text{iff} \quad TS \equiv_{CTL} TS' \quad \text{iff} \quad TS \equiv_{CTL^*} TS'$$

$\Rightarrow$ prior to model-check Φ, it is safe to first minimize *TS* wrt. $\sim$

this can be done with time complexity $\mathcal{O}(K \cdot \log N)$

The importance of this result

- CTL and CTL* equivalence coincide
  - despite the fact that CTL* is more expressive than CTL
- Bisimilar transition systems preserve the same CTL* formulas
  - and thus the same LTL formulas (and LT properties)
- Non-bisimilarity can be shown by a single CTL (or CTL*) formula
  - $TS_1 \models \Phi$ and $TS_2 \not\models \Phi$ implies $TS_1 \not\sim TS_2$
- You even do not need to use an until-operator!
- To check $TS \models \Phi$, it suffices to check $TS/\sim \models \Phi$

Example