Verification

Lecture 19

Bernd Finkbeiner

UNIVERSITÄT DES SAARLANDES

Plan for today

- Simulation equivalence

REVIEW: Bisimulation

Let $TS_i = (S_i, Act_i, \rightarrow_i, I_i, AP, L_i)$, i=1, 2, be transition systems
A bisimulation for (TS_1, TS_2) is a binary relation $\mathcal{R} \subseteq S_1 \times S_2$ such that:

1. $\forall s_1 \in I_1\, \exists s_2 \in I_2.\, (s_1, s_2) \in \mathcal{R}$ and $\forall s_2 \in I_2\, \exists s_1 \in I_1.\, (s_1, s_2) \in \mathcal{R}$
2. for all states $s_1 \in S_1$, $s_2 \in S_2$ with $(s_1, s_2) \in \mathcal{R}$ it holds:

   2.1 $L_1(s_1) = L_2(s_2)$

   2.2 if $s_1' \in Post(s_1)$ then there exists $s_2' \in Post(s_2)$ with $(s_1', s_2') \in \mathcal{R}$

   2.3 if $s_2' \in Post(s_2)$ then there exists $s_1' \in Post(s_1)$ with $(s_1', s_2') \in \mathcal{R}$

TS_1 and TS_2 are bisimilar, denoted $TS_1 \sim TS_2$, if there exists a bisimulation for (TS_1, TS_2)

REVIEW: Bisimulation on states

$\mathcal{R} \subseteq S \times S$ is a bisimulation on TS if for any $(q_1, q_2) \in \mathcal{R}$:

- $L(q_1) = L(q_2)$
- if $q_1' \in Post(q_1)$ then there exists an $q_2' \in Post(q_2)$ with $(q_1', q_2') \in \mathcal{R}$
- if $q_2' \in Post(q_2)$ then there exists an $q_1' \in Post(q_1)$ with $(q_1', q_2') \in \mathcal{R}$

q_1 and q_2 are bisimilar, $q_1 \sim_{TS} q_2$, if $(q_1, q_2) \in \mathcal{R}$ for some bisimulation $\mathcal{R}$ for TS

$\boxed{q_1 \sim_{TS} q_2 \quad \text{if and only if} \quad TS_{q_1} \sim TS_{q_2}}$

REVIEW: Bisimulation vs. CTL* and CTL equivalence

Let TS be a finite state graph 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: $\equiv_{CTL} \subseteq \sim \subseteq \equiv_{CTL^*} \subseteq \equiv_{CTL}$

important: equivalence is also obtained for any sub-logic containing $\neg$, $\wedge$ and X

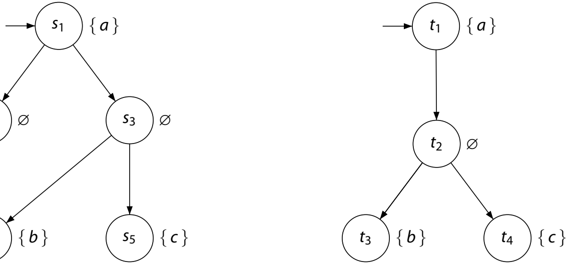
REVIEW: Simulation order

Let $TS_i = (S_i, Act_i, \rightarrow_i, I_i, AP, L_i)$, i=1, 2,
be two transition systems over AP.
A simulation for (TS_1, TS_2) is a binary relation $\mathcal{R} \subseteq S_1 \times S_2$ such that:

1. $\forall q_1 \in I_1 \; \exists q_2 \in I_2 . \, (q_1, q_2) \in \mathcal{R}$
2. for all $(q_1, q_2) \in \mathcal{R}$ it holds:
   - 2.1 $L_1(q_1) = L_2(q_2)$
   - 2.2 if $q_1' \in Post(q_1)$
     then there exists $q_2' \in Post(q_2)$ with $(q_1', q_2') \in \mathcal{R}$

$TS_1 \preceq TS_2$ iff there exists a simulation $\mathcal{R}$ for (TS_1, TS_2)

REVIEW: Similar but not bisimilar



$TS_{left} \simeq TS_{right}$ but $TS_{left} \not\sim TS_{right}$

Simulation quotient

For $TS = (S, Act, \rightarrow, I, AP, L)$ and simulation equivalence $\simeq \subseteq S \times S$ let

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

where

- $S' = S/\simeq = \{ [s]_\simeq \mid s \in S \}$ and $I' = \{ [s]_\simeq \mid s \in I \}$
- $\rightarrow'$ is defined by: $\dfrac{s \xrightarrow{\alpha} s'}{[s]_\simeq \xrightarrow{\tau}{}' [s']_\simeq}$
- $L'([s]_\simeq) = L(s)$

lemma: $TS \simeq TS/\simeq$; proof not straightforward!

Universal fragment of CTL*

$\forall$CTL* state-formulas are formed according to:

$$\Phi \ ::= \ \text{true} \ \Big| \ \text{false} \ \Big| \ a \ \Big| \ \neg a \ \Big| \ \Phi_1 \wedge \Phi_2 \ \Big| \ \Phi_1 \vee \Phi_2 \ \Big| \ \mathsf{A}\,\varphi$$

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

$\forall$CTL* path-formulas are formed according to:

$$\varphi \ ::= \ \Phi \ \Big| \ \mathsf{X}\,\varphi \ \Big| \ \varphi_1 \wedge \varphi_2 \ \Big| \ \varphi_1 \vee \varphi_2 \ \Big| \ \varphi_1 \,\mathsf{U}\, \varphi_2 \ \Big| \ \varphi_1 \,\mathsf{R}\, \varphi_2$$

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

Universal CTL* contains LTL

$\boxed{\text{For every LTL formula there exists an equivalent } \forall\text{CTL}^* \text{ formula}}$

Proof: Bring LTL formula into positive normal form (PNF).

Simulation order and $\forall\mathrm{CTL}^*$

Let TS be a finite transition system (without terminal states) and q, q' states in TS.

The following statements are equivalent:

(1) $q \preceq_{TS} q'$

(2) for all $\forall\mathrm{CTL}^*$-formulas Φ: $q' \models \Phi$ implies $q \models \Phi$

(3) for all $\forall\mathrm{CTL}$-formulas Φ: $q' \models \Phi$ implies $q \models \Phi$

proof is carried out in three steps: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1)

Existential fragment of CTL*

$\exists$CTL* state-formulas are formed according to:

$$\Phi \ ::= \ \text{true} \ \big| \ \text{false} \ \big| \ a \ \big| \ \neg a \ \big| \ \Phi_1 \wedge \Phi_2 \ \big| \ \Phi_1 \vee \Phi_2 \ \big| \ \exists \varphi$$

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

$\exists$CTL* path-formulas are formed according to:

$$\varphi \ ::= \ \Phi \ \big| \ \mathrm{X}\,\varphi \ \big| \ \varphi_1 \wedge \varphi_2 \ \big| \ \varphi_1 \vee \varphi_2 \ \big| \ \varphi_1 \,\mathrm{U}\, \varphi_2 \ \big| \ \varphi_1 \,\mathrm{R}\, \varphi_2$$

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

Simulation order and $\exists$CTL*

Let TS be a finite transition system (without terminal states) and q, q' states in TS.

The following statements are equivalent:

(1) $q \preceq_{TS} q'$

(2) for all $\exists$CTL*-formulas Φ: $q \models \Phi$ implies $q' \models \Phi$

(3) for all $\exists$CTL-formulas Φ: $q \models \Phi$ implies $q' \models \Phi$

$\simeq$, $\forall$CTL*, and $\exists$CTL* equivalence

For finite transition system *TS* without terminal states:

$$\simeq_{TS} \;=\; \equiv_{\forall CTL^*} \;=\; \equiv_{\forall CTL} \;=\; \equiv_{\exists CTL^*} \;=\; \equiv_{\exists CTL}$$

Simulation preorder checking

Require: finite transition system $TS = (S, Act, \rightarrow, I, AP, L)$ over AP
Ensure: simulation order $\preceq_{TS}$

$\mathcal{R} := \{ (q_1, q_2) \mid L(q_1) = L(q_2) \};$

while $\mathcal{R}$ is not a simulation **do**
  choose $(q_1, q_2) \in \mathcal{R}$
    such that $(q_1, q_1') \in E$, but for all q_2' with $(q_2, q_2') \in E$, $(q_1', q_2') \notin \mathcal{R}$;
  $\mathcal{R} := \mathcal{R} \setminus \{ (q_1, q_2) \}$
end while
return $\mathcal{R}$

The number of iterations is bounded from above by $|S|^2$, since:

$$S \times S \supseteq \mathcal{R}_0 \supsetneqq \mathcal{R}_1 \supsetneqq \mathcal{R}_2 \supsetneqq \ldots \supsetneqq \mathcal{R}_n = \preceq$$

Checking trace equivalence

Let TS_1 and TS_2 be finite transition systems over AP. Then:

1. The problem whether

$$Traces_{fin}(TS_1) = Traces_{fin}(TS_2) \quad \text{is PSPACE-complete}$$

2. The problem whether

$$Traces(TS_1) = Traces(TS_2) \quad \text{is PSPACE-complete}$$

Overview implementation relations

	bisimulation equivalence	simulation order	trace equivalence
preservation of temporal-logical properties	CTL^* CTL	$\forall CTL^* / \exists CTL^*$ $\forall CTL / \exists CTL$	LTL
checking equivalence	PTIME	PTIME	PSPACE-complete
graph minimization	PTIME	PTIME	---