ENS DE LYON

TD – Semantics and Verification

IX– Bisimulations and HML

Friday 25th March 2022

TA: Ralph Sarkis
ralph.sarkis@ens-lyon.fr

Bisimulations

Recall that for two TS_0 and TS_1 such that $TS_i = (S_i, \mathrm{Act}, \to_i, I_i, \mathrm{AP}, L_i)$, the relation $\mathcal{R} \subseteq S_0 \times S_1$ is said to be a bisimulation iff for all $(s_0, s_1) \in \mathcal{R}$, we have:

- $L_0(s_0) = L_1(s_1)$, and
- for each $i \in \{0, 1\}$ and each $\alpha \in \mathrm{Act}$ if $s_i \xrightarrow{\alpha} s'_i$, then there is $s'_{1-i} \in S_{1-i}$ such that $s_{1-i} \xrightarrow{\alpha} s'_{1-i}$ and $(s'_0, s'_1) \in \mathcal{R}$.

We write $TS_0 \approx TS_1$ if there is bisimulation $\mathcal{R}$ such that for all $s_i \in S_i$, there is $s_{1-i} \in S_{1-i}$ satisfying $(s_0, s_1) \in \mathcal{R}$. The bisimilarity relation $\sim$ between two systems is defined by $s_0 \sim s_1$ iff there is a bisimulation $\mathcal{R}$ such that $(s_0, s_1) \in \mathcal{R}$.

Exercise 1.

Given two transition systems TS_0 and TS_1, show that:

1. for all $s \in S_0$, $s \sim s$.
2. if $\mathcal{R}$ is a bisimulation, then $\mathcal{R}^{-1} = \{(s_1, s_0) \in S_1 \times S_0 \mid (s_0, s_1) \in \mathcal{R}\}$ is also a bisimulation.
3. Given a third transition system TS_2, if $\mathcal{R}$ is a bisimulation between TS_0 and TS_1 and $\mathcal{T}$ is a bisimulation between TS_1 and TS_2 then
$$\mathcal{T} \circ \mathcal{R} = \{(s_0, s_2) \in S_0 \times S_2 \mid \exists s_1 \in S_1, (s_0, s_1) \in \mathcal{R} \text{ and } (s_1, s_2) \in \mathcal{T}\}$$
is also a bisimulation.
4. The bisimilarity relation between TS_0 and TS_1 is a bisimulation.
5. If $\mathcal{R}$ is a bisimulation between TS_0 and TS_1, then $\mathcal{R} \subseteq \sim$.
6. The bisimilarity between TS_0 and itself is an equivalence relation.

Exercise 2.

Given a transition system $TS = (S, \mathrm{Act}, \to, I, \mathrm{AP}, L)$ and $\sim$ its bisimilarity relation with itself, we define $TS_\sim = (S_\sim, \mathrm{Act}, \to_\sim, I_\sim, \mathrm{AP}, L_\sim)$ as follows:

- the states $S_\sim$ of $TS_\sim$ are the equivalence classes of $\sim$, i.e. $S_\sim = \{[s]_\sim \mid [s]_\sim = \{a \in S \mid s \sim a\}\}$
- $I_\sim = \{[i]_\sim \mid i \in I\}$
- $[s]_\sim \xrightarrow{\alpha}_\sim [s']_\sim$ if $s \xrightarrow{\alpha} s'$
- $L_\sim([s_\sim]) = L(s)$

Show that $TS \approx TS_\sim$.

HML

We recall that for two sets AP and Act,

- A Kripke frame over Act is given by a set of states S together with a relation $\to \subseteq S \times \mathrm{Act} \times S$.

- A Kripke model over Act and AP is given by a Kripke frame $(S, \mathrm{Act}, \to)$ together with a state labelling $L : S \to 2^{\mathrm{AP}}$.
- The formulae of HML are defined by $\varphi, \psi := \top \mid \bot \mid a \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \ \neg\varphi \mid [\alpha]\varphi \mid \langle\alpha\rangle\varphi$ with $\alpha \in \mathrm{Act}$ and $a \in \mathrm{AP}$.

Moreoever, given a Kripke model $M = (S, \mathrm{Act}, \to, \mathrm{AP}, L)$, we define the interpretation of an HML-formula inductively (note that M is not explicit in the notation of the interpretation, but the interpretation depends on M):

- $[\![a]\!] = \{s \in S \mid a \in L(s)\}$
- $[\![\top]\!] = S$
- $[\![\bot]\!] = \emptyset$
- $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$
- $[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$
- $[\![\neg\varphi]\!] = S \backslash [\![\varphi]\!]$
- $[\![[\alpha]\varphi]\!] = \{s \in S \mid \forall s', \text{if } s \xrightarrow{\alpha} s' \text{ then } s' \in [\![\varphi]\!]\}$
- $[\![\langle\alpha\rangle\varphi]\!] = \{s \in S \mid \exists s', s \xrightarrow{\alpha} s' \text{ and } s' \in [\![\varphi]\!]\}$

We say that a state s of M satisfies φ, and denote it $s \Vdash \varphi$, iff $s \in [\![\varphi]\!]$. We say that M satisfies φ, and denote it $M \models \varphi$, if $s \Vdash \varphi$ for all $s \in S$. We say that φ is valid, and denote it $\models \varphi$ if $M \models \varphi$ for every Kripke model M (over Act and AP). Finally we say that φ and ψ are logically equivalent, and denote it $\varphi \equiv \psi$, if $\models \varphi \leftrightarrow \psi$ (with the usual definition of $\leftrightarrow$). Equivalently, $\varphi \equiv \psi$ if and only if $[\![\phi]\!] = [\![\psi]\!]$ for every Kripke model.

Exercise 3.

Let AP be a set. We fix $\mathrm{Act} = \{\bullet\}$. We define the Kripke model $M((2^{\mathrm{AP}})^\omega) = ((2^{\mathrm{AP}})^\omega, \mathrm{Act}, \to, \mathrm{AP}, L)$ on streams where

- $\alpha \xrightarrow{\bullet} \beta$ iff $\beta = \alpha{\upharpoonright}1$
- $L(\alpha) = \alpha(0)$

1. Show that $[\![\langle\bullet\rangle\varphi]\!] = [\![[\bullet]\varphi]\!] = \{\sigma \mid \sigma{\upharpoonright}1 \in [\![\varphi]\!]\}$
2. Show that for all $P \subseteq (2^{\mathrm{AP}})^\omega$, the following are equivalent:
   - There is a HML–formula φ such that $P = [\![\varphi]\!]$
   - There is a LML–formula φ such that $P = [\![\varphi]\!]$
3. Show that for all $\alpha, \beta \in (2^{\mathrm{AP}})^\omega$, $\alpha = \beta$ iff $\alpha \sim \beta$.

Exercise 4.

Show the following equivalences:

1. $\langle\alpha\rangle\varphi \equiv \neg[\alpha]\neg\varphi$
2. $[\alpha]\varphi \equiv \neg\langle\alpha\rangle\neg\varphi$
3. $\langle\alpha\rangle(\varphi \vee \psi) \equiv (\langle\alpha\rangle\varphi) \vee (\langle\alpha\rangle\psi)$
4. $[\alpha](\varphi \wedge \psi) \equiv ([\alpha]\varphi) \wedge ([\alpha]\psi)$
5. $\langle\alpha\rangle\bot \equiv \bot$
6. $[\alpha]\top \equiv \top$

Characterization of DBAs

Exercise 5.

1. Let $\mathrm{AP} = \{a, b\}$. Show that $\{\sigma \mid \exists^\infty t, a \in \sigma(t)\} \subseteq (2^{\mathrm{AP}})^\omega$ is not closed.
2. Show that there is a DBA $\mathcal{A}$ such that $\mathcal{L}_\omega(\mathcal{A})$ is not a safety property.
3. Show that for every regular safety property P, there is a DBA $\mathcal{A}$ such that $P = \mathcal{L}_\omega(\mathcal{A})$.