HennessyMilner Logic and Bisimulation

Notes for the Course "Service Integration"

Giuseppe De Giacomo

Consider two transition systems $T = (A, S, s_0, \delta, F)$ and $T' = (A, S', t_0, \delta, F')$ whose states we denote by s, s' and t, t' respectively.
Let L be the language formed by all the HennessyMilner Logic formulas. We define:

$$\sim_L = \{(s,t) \mid \forall \Phi \in L. T, s \models \Phi \text{ iff } T', t \models \Phi\}$$

and

$$\sim = \{(s,t) \mid \exists \text{ bisimulation } R \text{ s.t. } R(s,t)\}$$

Next we show that notably these two equivalence relations coincide!

Theorem: *$s \sim t$ implies $s \sim_L t$, i.e., if there exists a bisimulation between s and t then s, t satisfy (make true) the same formulas of HenessyMilner Logic.*

Proof: By induction on the structure of the formulas. It sufficies to consider only formulas formed as follows:

$$\Phi \leftarrow Final \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid \langle a \rangle \Phi$$

Indeed, it is easy to see that $\Phi_1 \vee \Phi_2 \equiv \neg(\neg\Phi_1 \wedge \neg\Phi_2)$ and $[a]\Phi \equiv \neg\langle a \rangle \neg\Phi$.

- **Atomic formulas** ($Final$) *[base case]*

  $s \sim t$ implies $s \in F$ iff $t \in F'$ i.e., $T, s \models Final$ iff $T', t \models Final$.

- **Booleans** *[inductive cases]*

  By induction hypothesis, we assume that for every $s \sim t$ we have $T, s \models \Phi_i$ iff $T', t \models \Phi_i$, for $i = 1, 2$. Then by $T, s \models \Phi_1$ and $T, s \models \Phi_2$ iff $T', t \models \Phi_1$ and $T', t \models \Phi_2$ hence, by definition we have $T, s \models \Phi_1 \wedge \Phi_2$ iff $T', t \models \Phi_1 \wedge \Phi_2$.

  Similarly for $\neg\Phi$ (left as an exercise to the student).

- **Modal operators** *[another –the most interesting– inductive case]*

  By induction hypothesis, we assume that for every $ss \sim tt$ we have $T, ss \models \Phi$ iff $T', tt \models \Phi$. Now consider that $T, s \models \langle a \rangle \Phi$ iff there exists a transition $s \rightarrow_a s'$ in T such that $T, s' \models \Phi$.

  On the other hand since $s \sim t$ there exists a transition $t \rightarrow_a t'$ in T' such that $s' \sim t'$.

  But then by induction hypotesis $T, s' \models \Phi$ iff $T', t' \models \Phi$, and hence by definition $T', t \models \langle a \rangle \Phi$. □

Theorem: *$s \sim_L t$ implies $s \sim t$, i.e., if s, t satisfy (make true) the same formulas of HenessyMilner Logic, then there exists a bisimulation between s and t.*

Proof: By coinduction. We show that $\sim_L$ is a bisimulation, i.e., satisfies the following rules:

$$\begin{array}{l} s \sim_L t \text{ implies} \\ \quad s \in F \text{ iff } t \in F' \\ \quad \text{if } s \rightarrow_a s' \text{ then } \exists t \rightarrow_a t' \text{ s.t. } s' \sim_L t' \\ \quad \text{if } t \rightarrow_a t' \text{ then } \exists s \rightarrow_a s' \text{ s.t. } s' \sim_L t' \end{array}$$

- **Closure wrt the bisimulation rule**
  - *[local condition]*
    First, since $s \sim_L t$ we have $T, s \models Final$ iff $T', s \models Final$, but then we have $s \in F$ iff $t \in F'$.
  - *[nonlocal condition]*
    We prove the rest by contradiction. Suppose that for some s, t, we have that $s \sim_L t$, and $s \rightarrow_a s'$ but for all $t \rightarrow_a t'$ we have $s \not\sim_L t$. Then let $\{t'_1, \ldots, t'_n\} = \{t' \mid t \rightarrow_a t'\}$[1]. Notice since $T, s \models \langle a \rangle True$ we have also $T', t \models \langle a \rangle True$, so $n \geq 0$ above.
    On the other hand, since $s' \not\sim_L t'_i$, for each t'_i there is a formula $\Phi_{t'_i}$ such that $T', t'_i \models \Phi_{t'_i}$ but $T, s' \not\models \Phi_{t'_i}$. That is: $T, s' \models \bigwedge_{i=1,\ldots,n} \neg\Phi_{t'_i}$.
    Now consider the formula

    $$[a](\bigvee_{i=1,\ldots,n} \Phi_{t'_i})$$

    Clearly $T', t \models [a](\bigvee_{i=1,\ldots,n} \Phi_{t'_i})$ but, since $s \sim_L t$, then also $T, s \models [a](\bigvee_{i=1,\ldots,n} \Phi_{t'_i})$, which means that for all transitions $s \rightarrow_a s''$ we must have $T, s'' \models (\bigvee_{i=1,\ldots,n} \Phi_{t'_i})$, which is indeed false for $s'' = s'$. Contradiction.

Hence $\sim_L$ itself is a bisimulation, so $s \sim_L t$, implies that s, t are bisimilar and hence $s \sim_L t$. □

[1]Here we assume that the transition systems are finite branching.