Concurrency 6 = CCS (4/4)

Unique solutions ; Hennessy-Milner logic

Pierre-Louis Curien (CNRS – Université Paris 7)

MPRI concurrency course 2004/2005 with :

Jean-Jacques Lévy (INRIA-Rocquencourt)
Eric Goubault (CEA)
James Leifer (INRIA - Rocq)
Catuscia Palamidessi (INRIA - Futurs)

(`http://pauillac.inria.fr/~leifer/teaching/mpri-concurrency-2004`)

Unique solutions (1 / 13)

Definition : A process variable K is weakly guarded in P (notation $wg(K,P)$) if each occurrence of K is within some subterm of the form $\mu\cdot P'$ of P. Formally :

$$\frac{}{wg(K,\Sigma_{i\in I}\mu_i\cdot P_i)} \qquad \frac{(K\neq L)}{wg(K,L)}$$

$$\frac{wg(K,P_1)\quad wg(K,P_2)}{wg(K,P_1|P_2)} \qquad \frac{wg(K,P)}{wg(K,(\nu a)P} \qquad \frac{wg(K,P_1)\ \ldots\ wg(K;P_n)\ \ (K\notin\vec{L})}{wg(K,(let\ \vec{L}=\vec{P}\ in\ L_i))}$$

Unique solution theorem (strong case) : If $\vec{K}=\vec{P}$ is a system of equations where all K's are weakly guarded in all P's, and if $\vec{Q}$ and $\vec{R}$ are solutions of the system in the sense that $\vec{Q}\sim\vec{P}[\vec{K}\leftarrow\vec{Q}]$ and $\vec{R}\sim\vec{P}[\vec{K}\leftarrow\vec{R}]$, then $\vec{Q}\sim\vec{R}$.

Unique solutions (2 / 13)

Lemma : If $K_1,\ldots,K_n$ are weakly guarded in some process P, and if $P[\vec{K}\leftarrow\vec{Q}]\xrightarrow{\mu}T$ for some Q and T, then T has the form $P'[\vec{K}\leftarrow\vec{Q}]$ for some P' such that $P\xrightarrow{\mu}P'$ (and hence $P[\vec{K}\leftarrow\vec{Q'}]\xrightarrow{\mu}P'[\vec{K}\leftarrow\vec{Q'}]$ for any other Q').

By induction on the size of the proof of $P[K\leftarrow Q]\xrightarrow{\mu}T$, and by cases on the structure of P. We pick three cases :

$P=K$: This case cannot happen by the weak gardedness assumption.

Case $P=P_1|P_2$ and

$$\frac{P_1[\vec{K}\leftarrow\vec{Q}]\xrightarrow{\mu}T_1}{(P_1|P_2)[\vec{K}\leftarrow\vec{Q}]\xrightarrow{\mu}T_1|(S_2[\vec{K}\leftarrow\vec{Q}])=T}$$

Then by induction (K is weakly guarded in P_1) we know that

$$\exists\,P_1'\ \ (P_1\xrightarrow{\mu}P_1'\text{ and }T_1=P_1'[\vec{K}\leftarrow\vec{Q}])$$

Then, setting $P'=P_1'|P_2$, we have $P\xrightarrow{\mu}P'$ and $T=P'[\vec{K}\leftarrow\vec{Q}]$.

Unique solutions (3 / 13)

Case $P=(let\ \vec{L}=\vec{S}\ in\ L_i)$ and

$$\frac{S_i[\vec{K}\leftarrow\vec{Q}][\vec{L}\leftarrow(let\ \vec{L}=\vec{S}[\vec{K}\leftarrow\vec{Q}]\ in\ \vec{L})]\xrightarrow{\mu}T}{(let\ \vec{L}=\vec{S}\ in\ L_i)\xrightarrow{\mu}T}$$

(By definition, $(let\ \vec{L}=\vec{S}\ in\ L_i)[\vec{K}\leftarrow\vec{Q}]=(let\ \vec{L}=\vec{S}[\vec{K}\leftarrow\vec{Q}]\ in\ L_i)$.)

We have (commuting substitutions) :

$$S_i[\vec{K}\leftarrow\vec{Q}][\vec{L}\leftarrow(let\ \vec{L}=\vec{S}[\vec{K}\leftarrow\vec{Q}]\ in\ \vec{L})]=S_i[\vec{L}\leftarrow(let\ \vec{L}=\vec{S_i}\ in\ \vec{L})][\vec{K}\leftarrow\vec{Q}]$$

We apply induction to $S_i'=S_i[\vec{L}\leftarrow(let\ \vec{L}=\vec{S_i}\ in\ \vec{L})]$ (the proof of $S_i'[\vec{K}\leftarrow\vec{Q}]\xrightarrow{\mu}T$ is shorter, and K is weakly guarded in S_i, hence a fortiori in S_i'). Hence $\exists\,P'\ \ (S_i'\xrightarrow{\mu}P'\text{ and }T=P'[\vec{K}\leftarrow\vec{Q}])$. Finally, by folding :

$$\frac{S_i[\vec{L}\leftarrow(let\ \vec{L}=\vec{S_i}\ in\ \vec{L})]\xrightarrow{\mu}P'}{P\xrightarrow{\mu}P'}$$

Unique solutions (4 / 13)

Proof of the theorem : the set of all pairs

$$(S[\vec{K} \leftarrow \vec{Q}], S[\vec{K} \leftarrow \vec{R}])$$

where S is arbitrary, is a bisimulation up to $\sim$.

(And hence, in particular, taking $S = K_i$: $Q_i \sim R_i$.)

Let $S' = S[\vec{K} \leftarrow \vec{P}]$. The key remark is that K is weakly guarded in S'. We have

$$S[\vec{K} \leftarrow \vec{Q}] \sim S[\vec{K} \leftarrow \vec{P}[\vec{K} \leftarrow \vec{Q}]] = S'[\vec{K} \leftarrow \vec{Q}]$$

Hence if $S[\vec{K} \leftarrow \vec{Q}] \xrightarrow{\mu} Q'$, then $S'[\vec{K} \leftarrow \vec{Q}] \xrightarrow{\mu} Q''$ for some Q'' such that $Q' \sim Q''$. By the lemma, there exists P' such that

$$S' \xrightarrow{\mu} P' \quad \text{and} \quad Q'' = P'[\vec{K} \leftarrow \vec{Q}] \quad \text{and} \quad S'[\vec{K} \leftarrow \vec{R}] \xrightarrow{\mu} P'[\vec{K} \leftarrow \vec{R}]$$

Finally, since $S'[\vec{K} \leftarrow \vec{R}] \sim S[\vec{K} \leftarrow \vec{R}]$, there exists R' such that $S[\vec{K} \leftarrow \vec{R}] \xrightarrow{\mu} R'$ and $P'[\vec{K} \leftarrow \vec{R}] \sim R'$. Putting everything together, we have :

$$Q' \sim P'[\vec{K} \leftarrow \vec{Q}] \mathrel{\mathcal{R}} P'[\vec{K} \leftarrow \vec{R}] \sim R'$$

Unique solutions (5 / 13)

For weak bisimulation, we need strengthened hypotheses.

Definition : A process variable K is guarded in P if each occurrence of K is within some subterm of the form $\alpha \cdot P'$ of P.

A process variable K is sequential in P if no occurrence of K is within a subterm of P which is a parallel composition.

Example : K is weakly guarded, but neither guarded nor sequential in $(\tau \cdot K | a \cdot 0)$.

Unique solution theorem (weak case) : If $\vec{K} = \vec{P}$ is a system of equations where all K's are guarded and sequential in all P's, and if $\vec{Q}$ and $\vec{R}$ are solutions of the system in the sense that $\vec{Q} \approx \vec{P}[\vec{K} \leftarrow \vec{Q}]$ and $\vec{R} \approx \vec{P}[\vec{K} \leftarrow \vec{R}]$, then $\vec{Q} \approx \vec{R}$.

Unique solutions (6 / 13)

We need to be able to apply the lemma repeatedly (for τ-actions). Hence we need to have that when $P \xrightarrow{\mu} P'$ then P' is again guarded. This is true under the additional sequential assumption :

1. If P is sequential and if $P \xrightarrow{\mu} P'$, then P' is sequential ;
2. If P is sequential and guarded and if $P \xrightarrow{\tau} P'$, then P' is guarded.

Exercice 1 Prove it.

Counterexamples supporting these assumptions :

- $P = a \cdot K | \overline{a} \cdot 0 \xrightarrow{\tau} K | 0 = P'$: K is guarded but not sequential in P, and is not guarded in P'
- $P = \tau \cdot K \xrightarrow{\tau} K = P'$: K is weakly guarded in P, but (not even weakly) guarded in P'.

Unique solutions (7 / 13)

Proof of the theorem. One shows that the set of all pairs

$$(S[\vec{K} \leftarrow \vec{Q}], (S[\vec{K} \leftarrow \vec{R}])$$

where S is any process in which all the K's are sequential, is a bisimulation up to $\approx$.

Case 1 : $S[\vec{K} \leftarrow \vec{Q}] \xrightarrow{\mu} Q'$. We proceed exactly as in the strong case, replacing

- $\sim$ by $\approx$,
- $S'[\vec{K} \leftarrow \vec{Q}] \xrightarrow{\mu} Q''$ by $S'[\vec{K} \leftarrow \vec{Q}] \xRightarrow{\mu} Q''$, and the same for all subsequent uses of $\xrightarrow{\mu}$,
- and a single use of the lemma by repeated uses of the lemma. It is possible because the K's are guarded and sequential in $S' = S[\vec{K} \leftarrow \vec{Q}]$ (here we use the assumption on S !).

Unique solutions (8 / 13)

Case 2 : $S[\vec{K} \leftarrow \vec{Q}] \xrightarrow{\alpha} Q'$. Then we begin in the same way, and we get that $S'[\vec{K} \leftarrow \vec{Q}] \overset{\tau}{\Rightarrow}\xrightarrow{\alpha} Q''' \overset{\tau}{\Rightarrow} Q''$, with $Q' \approx Q''$.

By repeated use of the lemma, there exists P' such that the K's are sequential in P',

$$P \overset{\mu}{\Rightarrow}\xrightarrow{\alpha} P \quad \text{and} \quad Q''' = P'[\vec{K} \leftarrow \vec{Q}] \quad \text{and} \quad S'[\vec{K} \leftarrow \vec{Q}] \overset{\tau}{\Rightarrow}\xrightarrow{\alpha} P'[\vec{K} \leftarrow \vec{R}]$$

From there, we proceed exactly as in Case 1, with the only change that the initial assumption is now $P'[\vec{K} \leftarrow \vec{Q}] \overset{\tau}{\Rightarrow} Q''$ (instead of a $\xrightarrow{\mu}$ – this does not affect the rest of the argument, why ?). Thus we get R'' such that $Q''\ (\approx \mathcal{R} \approx)\ R''$ and $P'[\vec{K} \leftarrow \vec{R}] \overset{\tau}{\Rightarrow} R''$, and hence : $S'[\vec{K} \leftarrow \vec{Q}] \overset{\alpha}{\Rightarrow} R''$.

Finally, since $S'[\vec{K} \leftarrow \vec{R}] \approx S[\vec{K} \leftarrow \vec{R}]$, there exists R' such that $R'' \approx R'$ and $S[\vec{K} \leftarrow \vec{R}] \overset{\alpha}{\Rightarrow} R'$. We are done, as $Q' \approx Q''(\approx \mathcal{R} \approx)\ R'' \approx R'$.

Unique solutions (9 / 13)

We illustrate the theorem with the example of a slot machine :

Specification :

$$SPEC\langle x\rangle = s \cdot (\tau \cdot \bar{l} \cdot SPEC\langle x+1\rangle + \Sigma_{1 \leq y \leq x+1} \tau \cdot \overline{w} \cdot SPEC\langle x+1-y\rangle)\ .$$

Implementation : Let IO, B, D be given as follows :

(user) $IO = s \cdot \bar{b} \cdot (L \cdot \bar{l} \cdot IO + R(y) \cdot \overline{w}\langle y\rangle \cdot IO)$

(bank) $B\langle x\rangle = b \cdot \overline{\mu}\langle x+1\rangle \cdot \lambda(y) \cdot B\langle y\rangle$

(oracle) $D = \mu(z) \cdot (\overline{L} \cdot \overline{\lambda}\langle z\rangle \cdot D + \Sigma_{1 \leq y \leq z} \overline{R}\langle y\rangle \cdot \overline{\lambda}\langle z-y\rangle \cdot D)$

Our objective is to prove $SPEC\langle n\rangle \approx SM\langle n\rangle$,, where

$$SM\langle n\rangle = (\nu\, b, \mu, \lambda, L, R)(IO \mid B\langle n\rangle \mid D)$$

We write $(\vec{\nu})$ as shorthand for $(\nu\, b, \mu, \lambda, L, R)$.

Unique solutions (10 / 13)

By algebraic laws, we have :

$$\begin{aligned}
\vdash SM\langle n\rangle &= s \cdot ((\vec{\nu})((\bar{b} \cdot (L \cdot \bar{l} \cdot IO + R(y) \cdot \overline{w}\langle y\rangle \cdot IO)) \mid B\langle n\rangle \mid D)) \\
&= s \cdot \tau \cdot ((\vec{\nu})((L \cdot \bar{l} \cdot IO + R(y) \cdot \overline{w}\langle y\rangle \cdot IO) \mid \overline{\mu}\langle n+1\rangle \cdot \lambda(y) \cdot B\langle y\rangle \mid D)) \\
&= s \cdot \tau \cdot \tau \cdot P' \\
&= s \cdot P' \quad = \quad s \cdot (\tau.P'_0 + \Sigma_{1 \leq y \leq n+1} \tau \cdot P'_y)
\end{aligned}$$

where

$$P' = (\vec{\nu}) \begin{cases} (L \cdot \bar{l} \cdot IO + R(y) \cdot \overline{w}\langle y\rangle \cdot IO \\ \mid \lambda(y) \cdot B\langle y\rangle \\ \mid \overline{L} \cdot \overline{\lambda}\langle n+1\rangle \cdot D + \Sigma_{1 \leq y \leq n+1} \overline{R}\langle y\rangle \cdot \overline{\lambda}\langle n+1-y\rangle \cdot D) \end{cases}$$

$$P'_0 = (\nu b, \mu, \lambda, L, R) \begin{cases} (\bar{l} \cdot IO \\ \mid \lambda(y) \cdot B\langle y\rangle \\ \mid \overline{\lambda}\langle n+1\rangle \cdot D) \end{cases} \qquad P'_y = (\nu b, \mu, \lambda, L, R) \begin{cases} (\overline{w}\langle y\rangle \cdot IO \\ \mid \lambda(y) \cdot B\langle y\rangle \\ \mid \overline{\lambda}\langle n+1-y\rangle \cdot D) \end{cases}$$

Unique solutions (11 / 13)

So far, we have $\vdash SM\langle n\rangle = \tau.P'_0 + \Sigma_{1 \leq y \leq n+1} \tau \cdot P'_y$, where

$$P'_0 = (\nu b, \mu, \lambda, L, R) \begin{cases} (\bar{l} \cdot IO \\ \mid \lambda(y) \cdot B\langle y\rangle \\ \mid \overline{\lambda}\langle n+1\rangle \cdot D) \end{cases} \qquad P'_y = (\nu b, \mu, \lambda, L, R) \begin{cases} (\overline{w}\langle y\rangle \cdot IO \\ \mid \lambda(y) \cdot B\langle y\rangle \\ \mid \overline{\lambda}\langle n+1-y\rangle \cdot D) \end{cases}$$

We shall prove $\vdash P'_0 = \bar{l} \cdot SM\langle n+1\rangle$ and $\vdash P'_y = \overline{w} \cdot SM\langle n+1-y\rangle$, from which it follows that

$$\vdash SM\langle n\rangle = s \cdot (\tau.\bar{l} \cdot SM\langle n+1\rangle + \Sigma_{1 \leq y \leq n+1} \tau \cdot \overline{w} \cdot SM\langle n+1-y\rangle)$$

and we conclude by the unique solution theorem.

Unique solutions (12/13)

We just check $\vdash P'_0 = \bar{l} \cdot SM\langle n+1 \rangle$. We have :

$$\vdash P'_0 = \bar{l} \cdot (\tau \cdot SM\langle n+1 \rangle + s \cdot \tau \cdot P'') + \tau \cdot \bar{l} \cdot SM\langle n+1 \rangle$$

where P'' is such that $\vdash SM\langle n+1 \rangle = s \cdot P''$ So we have :

$$\begin{aligned}
\vdash P'_0 &= \bar{l} \cdot (\tau \cdot s \cdot P'' + s \cdot \tau \cdot P'') + \tau \cdot \bar{l} \cdot s \cdot P'' \\
&= \bar{l} \cdot (\tau \cdot s \cdot P'' + s \cdot P'') + \tau \cdot \bar{l} \cdot s \cdot P'' \\
&= \bar{l} \cdot \tau \cdot s \cdot P'' + \tau \cdot \bar{l} \cdot s \cdot P'' \\
&= \bar{l} \cdot s \cdot P'' + \tau \cdot \bar{l} \cdot s \cdot P'' \\
&= \bar{l} \cdot s \cdot P'' \\
&\approx \bar{l} \cdot SM\langle n+1 \rangle
\end{aligned}$$

Unique solutions (13/13)

Hindsight : We did not treat the constructs of CCS uniformly :

- recursion → unique solution
- the other constructions : → congruence

Note the following :

1. Formulating congruence for the recursive definitions would force us to define bisimulation for processes with free variables K.
2. We can avoid reasoning inside recursive definitions by unfolding them prior to the reasoning. This is exactly what happens in the example that we just unrolled.

The definition of equational reasoning (previous lecture) was left implicit and should be completed with reflexivity, symmetry, transitivity and :

$$\frac{\vdash P_i = Q_i \text{ (for all } i}{\vdash \Sigma_{i \in I} \mu_i \cdot P_i = \Sigma_{i \in I} \mu_i Q_i} \qquad \frac{\vdash P_1 = Q_1 \quad \vdash P_2 = Q_2}{\vdash (P_1 \mid P_2) = (Q_1 \mid Q_2)} \qquad \frac{\vdash P = Q}{\vdash (\nu a)P = (\nu a)Q}$$

Hennessy-Milner logic (1/14)

We revert to an arbitrary LTS, with its set of actions Act. We make the assumption that the LTS is image finite :

$$\forall P, \mu \ \ (\{(P' \mid P \xrightarrow{\mu} P'\} \text{ is finite})$$

We write Proc for the set of all states / processes.

Hennessy-Milner logic (2/14)

The set of formulas of Hennessy-Milner logic is defined by :

$$A := T \mid A \wedge A \mid \neg A \mid \langle \mu \rangle A$$

A formula A is interpreted by the the set of processes which satisfy it, whence two notations : $\llbracket A \rrbracket = \{P \mid P \models A\}$:

$$\begin{aligned}
&\llbracket T \rrbracket = Proc \\
&\llbracket A \wedge B \rrbracket = \llbracket A \rrbracket \cap \llbracket B \rrbracket \\
&\llbracket \neg A \llbracket = Proc \setminus \llbracket A \rrbracket \\
&\langle \mu \rangle A = \{P \mid (\exists P' \ \ P \xrightarrow{\mu} P' \text{ and } P' \models A)\}
\end{aligned}$$

Derived operators : $A \vee B = \neg((\neg A) \wedge (\neg B))$, $[\mu]A = \neg(\langle \mu \rangle (\neg A))$

Hennessy-Milner logic (3/14)

Theorem : Under the image finiteness assumption,

$$P \sim Q \quad \Leftrightarrow \quad \{A \mid P \models A\} = \{A \mid Q \models A\}$$

The theorem can be applied to finitary CCS (both strong and weak bisimulation). When weak bisimulation is meant, we write $\langle\!\langle \mu \rangle\!\rangle A$ and $[\![\mu]\!]A$.

It works also for the larger fragment of CCS with finite sums and recursive definitions where each recursively defined K is guarded and sequential in its definition.

More generally, it works for all pair of P, Q which are both hereditarily image finite, i.e., say, whenever $P \xrightarrow{s} Q$ ($s \in Act^\star$), then Q is image finite.

Remark : The interpretation $P \models A$ is compostional / congruential in A, not in P, hence the result does not help to establish that bisimilarity is a congruence

---

Hennessy-Milner logic (4/14)

Let L_n the subset of formulas with depth of at most n, where depth is defined by :

$$depth(T) = 0 \qquad depth(A \wedge B) = \max(depth(A), depth(B))$$
$$depth(\neg A) = depth(A) \qquad depth(\langle \mu \rangle A) = depth(A) + 1$$

Remember (lecture CCS (1/4) that $\sim$ is the greatest fixed point of some operator G_K, which is anti-continuous (image-finiteness !). Hence (ω stands for the set of natural numbers) :

$$\sim \; = \bigcap_{n \in \omega} \sim_n \quad \text{where} \quad \sim_0 = Proc \times Proc \quad \text{and} \quad \sim_{n+1} = G_K(\sim_n)$$

Unfolding the definition of G_K :

$P \sim_{n+1} Q \Leftrightarrow \forall \mu, P' \; (P \xrightarrow{\mu} P' \Rightarrow \exists Q' \; (Q \xrightarrow{\mu} Q'$ and $P' \sim_n Q'))$ and conversely

---

Hennessy-Milner logic (5/14)

We set $L_n(P) = \{A \in L_n \mid P \models A\}$. We prove by induction on n :

$$P \sim_n Q \quad \Leftrightarrow \quad L_n(P) = L_n(Q)$$

Case $n = 0$. Notice that for every $A \in L_0$ we have either $[\![A]\!] = \emptyset$ or $[\![A]\!] = Proc$ (by induction on A, which is $\langle \_ \rangle$ free). It follows that $P \in [\![A]\!]$ if and only if $Q \in [\![A]\!]$, for arbitrary P, Q.

Hennessy-Milner logic (6/14)

$P \not\sim_{n+1} Q \Rightarrow L_{n+1}(P) \neq L_{n+1}(Q)$.

Since $P \not\sim_{n+1} Q$, there exists a, P' such that for all $Q'_1, \ldots Q'_n$ (we are using image-finiteness) such that $Q \xrightarrow{a} Q'$ we have $P' \not\sim_n Q'_i$ for all i.

Now $L_n(P') \neq L_n(Q'_i)$ by induction. Hence there exists A_i in $L_n(P')$ not in $L_n(Q'_i)$ or there exists B in $L_n(Q'_i)$ not in $L_n(P')$. But in the latter case, we can take $\neg B$, hence we may assume that there exists A_i in $L_n(P')$ not in $L_n(Q'_i)$. Let $A = A_1 \wedge \ldots \wedge A_n$.

Then $P' \models A$, and since $Q'_i \not\models A_i$ we have a fortiori $Q'_i \not\models A$ for all i. From there it follows that $P \models \langle a \rangle A$ and $Q \not\models \langle i \rangle A$.

Hennessy-Milner logic (7/14)

$P \sim_{n+1} Q \Rightarrow L_{n+1}(P) = L_{n+1}(Q)$.

Let $A \in L_{n+1}(P)$. We proceed by structural induction on A. The only non-trivial case is $A = \langle a \rangle B$.

Since $P \models A$, there exist a, P' such that $P \xrightarrow{a} P'$ and $P' \models B$.

Since $P \sim_{n+1} Q$, there exists Q' such that $Q \xrightarrow{a} Q'$ and $P' \sim_n Q'$.

By induction, since $B \in L_n$, we get $Q' \models B$ and hence $A \in L_{n+1}(Q)$.

Hennessy-Milner logic (8/14)

How should we adapt this to overcome the image finiteness limitation ? We have to go to infinite conjunctions.

Ordinals are needed on both sides of the equivalence

$$P \sim_\kappa Q \quad \Leftrightarrow \quad L_\kappa(P) = L_\kappa(Q)$$

- On the left side, this is because the non image-finiteness entails non-anti-continuity of the operator of which $\sim$ is a fixpoint. And it is always true that $\sim$ is the intersection of the $\sim_\kappa$, but we then have to go beyond ordinal ω.

- on the right side, this is because of infinite branching, as the depth of a sum is the sup of the depths. In this way we may reach, say, depth $\omega = \sup\{1, \ldots, n, \ldots\}$.

Exercice 2 Show that $a^\omega + \Sigma_{n \in \omega} a^i$ (with infinite sum) and $\Sigma_{n \in \omega} a^i$ satisfy the same formulas (without infinite conjunction) but are not bisimilar (where $a^0 = 0$, $a^{i+1} = a \cdot a^i$, $a^\omega = (\mathit{let}\ K = a \cdot K\ \mathit{in}\ K)$). (Hint : prove that if $a^\omega \models A$, then $a^i \models A$ for all sufficiently large i, and for this use the alternative syntax $A := T \mid F \mid A \wedge A \mid A \vee A \mid \langle \mu \rangle A$)

Hennessy-Milner logic (9/14)

Recall from lecture 4 that $P = a \cdot (b + c)$ and $Q = a \cdot b + a \cdot c$ are not bisimilar.

Here is a formula that separates them :

$$P \models \langle a \rangle (\langle b \rangle T \wedge \langle c \rangle T) \qquad Q \not\models \langle a \rangle (\langle b \rangle T \wedge \langle c \rangle T)$$

Hennessy-Milner logic (10/14)

As a more sophisticated example, we show the correctness of the unbounded counter (cf. lecture 4) :

$$C = \mathsf{inc} \cdot (C \frown C) + \mathsf{dec} \cdot D \quad D = \overline{d} \cdot C + \overline{z} \cdot B \quad B = \mathsf{inc} \cdot (C \frown B) + \mathsf{zero} \cdot B$$

Notation : $\langle\langle \epsilon \rangle\rangle A = A$ and $\langle\langle as \rangle\rangle A = \langle\langle a \rangle\rangle (\langle\langle s \rangle\rangle A)$ (similarly for $\langle s \rangle A$, $[\![s]\!]A$, $[s]A$). $F = \neg T$. $\#_{\mathsf{inc}}(s)$ is the number of occurrences of inc in s. $\leq$ is the prefix ordering. We define :

$$\begin{array}{rcl}
(s \succeq 0) & = & (\forall s' \leq s\ (\#_{\mathsf{inc}}(s') \geq \#_{\mathsf{dec}}(s')) \wedge \\
& & \forall s'\ \ (s'0 \leq s \Rightarrow (\#_{\mathsf{inc}}(s') = \#_{\mathsf{dec}}(s')))) \\
(s \succ 0) & = & (s \succeq 0)\ \wedge\ (\#_{\mathsf{inc}}(s) > \#_{\mathsf{dec}}(s)) \\
(s = 0) & = & (s \succeq 0)\ \wedge\ (\#_{\mathsf{inc}}(s) = \#_{\mathsf{dec}}(s))
\end{array}$$

We shall show $C \models A_C$ where :

$$A_C = \left\{ \begin{array}{l}
(\bigwedge_{s \succeq 0} \langle\langle s \rangle\rangle T)\ \wedge\ (\bigwedge_{s \succ 0} [\![s]\!] (\langle\langle \mathsf{inc} \rangle\rangle T) \wedge \langle\langle \mathsf{dec} \rangle\rangle T \wedge [\![\mathsf{zero}]\!] F)) \wedge \\
(\bigwedge_{s = 0} [\![s]\!] (\langle\langle \mathsf{inc} \rangle\rangle T \wedge \langle\langle \mathsf{zero} \rangle\rangle T \wedge [\![\mathsf{dec}]\!] F))\ \wedge\ (\bigwedge_{s \not\succeq 0} [\![s]\!] F)
\end{array} \right.$$

Hennessy-Milner logic (11/14)

It can be shown, using algebraic laws and unique solution (as for the slot machine), that $C \approx Cnt_0$, where (specification) :

$$\begin{aligned} Cnt_0 &= \mathsf{inc} \cdot Cnt_1 + \mathsf{zero} \cdot Cnt_0 \\ Cnt_n &= \mathsf{inc} \cdot Cnt_{n+1} + \mathsf{dec} \cdot Cnt_{n-1} \end{aligned}$$

Then, by the logical characterization of bisimilarity, our goal can be reformulated as $Cnt_0 \models A_C$. Since the execution of Cnt_0 involves no τ actions, satisfaction of A_C is equivalent to satisfaction of the same formula where all $\langle\langle s \rangle\rangle\_$ and $[\![s]\!]\_$ are replaced by $\langle s \rangle\_$ and $[s]\_$, respectively.

Hennessy-Milner logic (12/14)

We are thus left to show :

$$Cnt_0 \models \begin{cases} (\bigwedge_{s \succeq 0} \langle s \rangle T) \;\wedge\; (\bigwedge_{s \succ 0} [s](\langle \mathsf{inc} \rangle T) \wedge \langle \mathsf{dec} \rangle T \wedge [\mathsf{zero}] F)) \;\wedge \\ (\bigwedge_{s = 0} [s](\langle \mathsf{inc} \rangle T \wedge \langle \mathsf{zero} \rangle T \wedge [\mathsf{dec}] F)) \;\wedge\; (\bigwedge_{s \not\succeq 0} [s] F) \end{cases}$$

This is an easy consequence of the following equivalence, which is proved by induction on the length of s :

$$Cnt_0 \xrightarrow{s} P \quad \Leftrightarrow (s \succeq 0 \text{ and } P = C_{\#_{\mathsf{inc}}(s) - \#_{\mathsf{dec}}(s)})$$

It can be shown that the formula A_C is a characteristic formula for C, i.e. that $Q \models A$ if and only if $Q \approx C$.

Hennessy-Milner logic (13/14)

Some perspective. It looks like :

- (weak) bisimilation or equational techniques used to show $P \approx Q$ where P is an "implementation" and Q is a "specification" is a tool for total correctness
- Hennessy-Milner logic or its extensions used to show $P \models A$ where P is a process and A is a property is a tool for partial correctness.

Hennessy-Milner logic (14/14)

But the picture is more mixed :

1. One can express a property of a process P in the form of another process Q and prove that P satisifes Q in the sense that for a suitable context C one has $C[P] \approx Q$. See Milner's "Communication and concurrency" [chapter 5] for an example where P is a scheduler of n tasks initiated in cycle by an action a_i, C implements hiding of all the other actions of the tasks, and $Q = a_1 \cdot \ldots \cdot a_n \cdot Q$.
2. For finite state LTS's, there is a characteristic formula (cf. previous slide) for each process / state, in an extension of the logic with a greatest fixed point operator (see, e.g. the course notes at `http://www.cs.aau.dk/~luca/SV/intro2ccs.pdf`)

Beyond Hennessy-Milner

Given a formula A, consider the following property, or set of processes ('no matter what transitions are made, A always holds") :

$$\mathsf{Inv}(A) = \{P \mid \forall s\ (P \xrightarrow{s} P' \Rightarrow P' \models A)\} = \bigwedge_{s \in \mathsf{Act}^*} [s]A$$

Proposition : $\mathsf{Inv}(F)$ is the greatest fixed point of the equation $X = A \wedge (\bigwedge_{a \in \mathsf{Act}} [a]X)$ in $\mathcal{P}(Proc)$.

Exercice 3 Prove it

More generally, safety and liveness properties ("whathever state is reached, it is possible to continue in such way") can be expressed by means of greatest and least fixed points, respectively (much more on this in the notes at `http://www.cs.aau.dk/~luca/SV/intro2ccs.pdf`)

Exercice 4 Find a formula that distinguishes the two processes of exercice 2.