Concurrency theory

Weak equivalences, axiomatizations, Hennessy-Milner logic

James Leifer Francesco Zappa Nardelli

INRIA Rocquencourt, MOSCOVA research team

james.leifer@inria.fr francesco.zappa_nardelli@inria.fr

together with

Frank Valencia (INRIA Futurs) Catuscia Palamidessi (INRIA Futurs) Roberto Amadio (PPS)

Today's plan

- Weak bisimulation and "up-to" techniques
- Equational axiomatisation
- Hennessy-Milner logic

A couple of useful pointers

- Aceto, Inglfsdttir, Larsen, Srba: *Reactive systems: modelling, specification and verification*.

  `http://www.cs.auc.dk/~luca/SV/intro2ccs.pdf`

- Winskel: Chapter 4 of *Set theory for computer science*.

  `http://www.cl.cam.ac.uk/~gw104/DiscMath.pdf`

Weak bisimulation

Definition: a weak bisimulation is a binary relation $\mathcal{R}$ on the set of processes such that for all P, Q, if $P \mathrel{\mathcal{R}} Q$ then

$$- \ \forall \mu, P', \ P \xrightarrow{\mu} P' \ \Rightarrow \ \exists Q', \ Q \stackrel{\hat{\mu}}{\Longrightarrow} Q' \text{ and } P' \mathrel{\mathcal{R}} Q' \ ;$$

$$- \ \forall \mu, Q', \ Q \xrightarrow{\mu} Q' \ \Rightarrow \ \exists P', \ P \stackrel{\hat{\mu}}{\Longrightarrow} P' \text{ and } P' \mathrel{\mathcal{R}} Q' \ ;$$

where $\stackrel{\hat{\mu}}{\Longrightarrow}$ is $\xrightarrow{\tau}^{*}$ if $\mu = \tau$ and $\xrightarrow{\tau}^{*}\xrightarrow{\mu}\xrightarrow{\tau}^{*}$ otherwise.

We say that P and Q are weakly bisimilar, denoted $P \approx Q$, if there exists a bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

Exercise: Prove that weak bisimilarity is an equivalence relation.

Some interesting examples

Some inequivalences:

$$P = a + b \qquad Q = a + \tau.b \qquad R = \tau.a + \tau.b$$

Some equivalences (for P, Q, R arbitrary):

$$\tau.a \approx a \qquad a + \tau.a \approx \tau.a \qquad a.c + a.(b + \tau.c) \approx a.(b + \tau.c)$$

$$\tau.P + R \approx P + \tau.P + R \qquad a.(\tau.P + Q) + R \approx a.(\tau.P + Q) + a.P + R$$

Up-to techniques for weak bisimulation

Definition: a weak bisimulation up-to $\sim$ is a binary relation $\mathcal{R}$ on the set of processes such that for all P, Q, if $P \mathrel{\mathcal{R}} Q$ then

$$\forall \mu, P',\ P \xrightarrow{\mu} P' \ \Rightarrow\ \exists Q',\ Q \stackrel{\hat{\mu}}{\Longrightarrow} Q' \text{ and } P' \sim\!\mathcal{R}\!\sim Q' \quad \text{and conversely.}$$

Theorem If $\mathcal{R}$ is a weak bisimulation up-to $\sim$, then $\mathcal{R} \subseteq \approx$.

Exercise: Is *weak bisimulation up-to* $\approx$ a sound proof technique? Consider the processes $P = \tau.a.0$ and $Q = \tau.0$.

See *Techniques of weak bisimulation up to* by Milner and Sangiorgi.

Specification and weak bisimulation

Consider the processes:

Hammer	Jobber	Strong jobber
$H = g.H' \quad H' = p.H$	$J = in.S \quad S = \overline{g}.U$ $U = \overline{p}.F \quad F = \overline{out}.J$	$K = in.D \quad D = \overline{out}.K$

Exercise: show that $(\boldsymbol{\nu} g, p)(J \parallel J \parallel H) \approx K \parallel K$ using the up-to $\equiv$ proof technique.

Weak bisimulation is not a congruence for unguarded sums

Consider CCS with prefix and sums instead of guarded sums, i.e. replace $\Sigma_{i \in I} \mu_i.P_i$ by $\Sigma_{i \in I} P_i$ and $\mu.P$, with rules

$$\frac{P_i \xrightarrow{\mu} P_i'}{\Sigma_{i \in I} P_i \xrightarrow{\mu} P_i'} \qquad \mu.P \xrightarrow{\mu} P$$

Strong bisimilarity is a congruence, and weak bisimilarity *is not* a congruence.

Exercise: find a counter example to congruence of weak bisimulation in CCS + sums.

Weak bisimulation is not a congruence for unguarded sums, ctd.

If you attempt to prove congruence, you will fail when dealing with the sum rule:

Suppose $P \approx Q$ and our goal is to show $P + S \approx Q + S$. If $P + S \xrightarrow{\tau} P'$ because $P \xrightarrow{\tau} P'$ then there exists Q' such that $Q \xrightarrow{\tau}^{*} Q'$, which may involve zero τ steps! In this case, there is no weak transition of $Q + S$ to reach a state matching P'.

Strong axiomatization

For finitary CCS (no recursion, finite guarded sums),

$$P \sim Q \text{ iff } \mathcal{A}_1 \vdash P = Q$$

where $\mathcal{A}_1$ is:

1. $\Sigma_{i\in I}\mu_i.P_i = \Sigma_{i\in I}\mu_{f(i)}.P_{f(i)}$ (f permutation)
2. $\Sigma_{i\in I}\mu_i.P_i + \mu_j.P_j = \Sigma_{i\in I}\mu_i.P_i$ for $j \in I$ (idempotency)
3. $P \parallel Q = \Sigma\{\mu.(P' \parallel Q) : P \xrightarrow{\mu} P'\} + \Sigma\{\mu.(P \parallel Q') : Q \xrightarrow{\mu} Q'\}$
   $+\Sigma\{\tau.(P' \parallel Q') : P \xrightarrow{\alpha} P' \text{ and } Q \xrightarrow{\overline{\alpha}} Q'\}$ (expansion)
4. $(\boldsymbol{\nu}a)(\Sigma_{i\in I}\mu_i.P_i) = \Sigma_{\{j\in I:\mu_j\neq a,\overline{a}\}}\mu_j.(\boldsymbol{\nu}a)P_j$

plus the rules for *equational reasoning* (reflexivity, symmetry, transitivity) and *congruence wrt sum, parallel and restriction*.

Exercise on axiomatization

Show that

$$\mathcal{A}_1 \vdash (\boldsymbol{\nu} b)(a.(b \; || \; c) + \tau.(b \; || \; \bar{b}.c)) \; = \; \tau.\tau.c + a.c$$

Proof of strong axiomatization

First step: each process is provably equal to a synchronization tree (guarded sums only), using only

3. $P \parallel Q = \Sigma\{\mu.(P' \parallel Q) : P \xrightarrow{\mu} P'\} + \Sigma\{\mu.(P \parallel Q') : Q \xrightarrow{\mu} Q'\}$
   $+\Sigma\{\tau.(P' \parallel Q') : P \xrightarrow{\alpha} P'$ and $Q \xrightarrow{\overline{\alpha}} Q'\}$ (expansion)
4. $(\boldsymbol{\nu} a)(\Sigma_{i \in I} \mu_i.P_i) = \Sigma_{\{j \in I : \mu_j \neq a, \overline{a}\}} \mu_j.(\boldsymbol{\nu} a) P_j$

The following *weight* function on processes decreases with each application of rules (3)-(4).

$$w(\Sigma_{i \in I} \mu_i.P_i) = 1 + \max_{i \in I} w(P_i)$$

$$w(P \parallel Q) = 2 \cdot (w(P) + w(Q))$$

$$w((\boldsymbol{\nu} a)P) = 1 + 2 \cdot w(P)$$

Strong axiomatization, ctd.

Second step: if $P = \Sigma_{i \in 1..m} \mu_i . P_i$ and $Q = \Sigma_{j \in m+1..n} \mu_j . P_j$, and if $P \sim Q$, then P and Q are provably equal, using only

1. $\Sigma_{i \in I} \mu_i . P_i = \Sigma_{i \in I} \mu_{f(i)} . P_{f(i)}$ (f permutation)
2. $\Sigma_{i \in I} \mu_i . P_i + \mu_j . P_j = \Sigma_{i \in I} \mu_i . P_i$ for $j \in I$ (idempotency)

Induct on $\mathrm{size}(P) + \mathrm{size}(Q)$: let $\rightleftharpoons$ be the equivalence relation on $\{1..n\}$ defined by $i \rightleftharpoons j$ iff $\mu_i = \mu_j$ and $P_i \sim P_j$. By induction $i \rightleftharpoons j$ implies $\vdash P_i = P_j$. By strong bisimilarity each $\rightleftharpoons$ equivalence class contains at least one element of $[1, m]$ and at least one element of $[m+1, n]$. Now for each of the equivalence classes we pick one representative in $[1, m]$ and one in $[m+1, n]$. Call them $p_1, \ldots, p_k$ and $q_1, \ldots . q_k$ respectively. Then using (1)-(2) and congruence we have:

$$\vdash \Sigma_{i=1..m} \mu_i . P_i = \Sigma_{l=1..k} \mu_{p_l} . P_{p_l} = \Sigma_{l=1..k} \mu_{q_l} . P_{q_l} = \Sigma_{j=m+1..n} \mu_j . P_j$$

Weak axiomatization

For finitary CCS,

$$P \approx Q \text{ iff } \mathcal{A}_1 + \mathcal{A}_2 \vdash P = Q$$

where $\mathcal{A}_2$ is:

1. $P = \tau.P$

2. $\tau.P + R = P + \tau.P + R$

3. $\mu.(\tau.P + Q) + R = \mu.(\tau.P + Q) + \mu.P + R$

(In general, we do not have $\vdash P + Q = \tau.P + Q$).

(We postpone the proof of the completness of this axiomatization to a later lecture).

Image finite LTS

We revert to an arbitrary LTS, with its set of actions $\mathbf{A}$. We make the assumption that the LTS is *image finite*:

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

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

Hennessy-Milner logic

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 set of processes that satisfy it, whence two notations: $[\![A]\!] = \{P : P \Vdash A\}$.

$$\begin{aligned}
[\![T]\!] &= \texttt{Proc} \\
[\![A \wedge B]\!] &= [\![A]\!] \cap [\![B]\!] \\
[\![\neg A]\!] &= \texttt{Proc} \setminus [\![A]\!] \\
[\![\langle \mu \rangle A]\!] &= \{P : \exists P' \ P \xrightarrow{\mu} P' \text{ and } P' \Vdash A\}
\end{aligned}$$

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

Hennessy-Milner logic, ctd.

Theorem: Under the image finitness assumption,

$$P \sim Q \text{ iff } \{A : P \Vdash A\} = \{A : Q \Vdash Q\}$$

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 that are both hereditarily image finite, i.e. say, whenever $P \xrightarrow{\tilde{\mu}} Q$ ($\tilde{\mu} \in \mathbf{A}^*$), then Q is image finite.

Hennessy-Milner logic, ctd.

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

$$\begin{array}{ll} \mathrm{depth}(T) = 0 & \mathrm{depth}(A \wedge B) = \max(\mathrm{depth}(A), \mathrm{depth}(B)) \\ \mathrm{depth}(\neg A) = \mathrm{depth}(A) & \mathrm{depth}(\langle \mu \rangle A) = \mathrm{depth}(A) + 1 \end{array}$$

Remember that $\sim$ is the greatest fixed point of some operator G_K. Since we suppose image finiteness, G_K is anti-continuous and

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

Hennessy-Milner logic, ctd.

Remark: unfolding the definition of G_K, we have:

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

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

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

Case $n = 0$. Notice that for every $A \in L_0$ we have either $[\![A]\!] = \emptyset$ or $[\![A]\!] = \texttt{Proc}$. It follows that $P \in [\![A]\!]$ iff $Q \in [\![A]\!]$ for arbitrary P, Q.

Hennessy-Milner logic, ctd.

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

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

Now $L_n(P') \neq L_n(Q'_i)$ by induction. Hence there exists $A_i \in L_n(P') \backslash L_n(Q'_i)$ or there exists $B_i \in L_n(Q'_i) \backslash L_n(P')$. But in the latter case we can take $A_i = \neg B_i$, hence we may assume that there exists $A_i \in L_n(P') \backslash L_n(Q'_i)$. Let $A = A_1 \wedge \cdots \wedge A_k$.

Then $P' \Vdash A$, and since $Q'_i \nVdash A_i$ we have $Q'_i \nVdash A$ for all i. It follows that $P \Vdash \langle \mu \rangle A$ and $Q \nVdash \langle \mu \rangle A$.

Hennessy-Milner logic, ctd.

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

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

Since $P \Vdash A$ there exists μ, P' such that $P \xrightarrow{\mu} P'$ and $P' \Vdash B$. By the hypothesis that $P \sim_{n+1} Q$, there exists Q' such that $Q \xrightarrow{\mu} Q'$ and $P' \sim_n Q'$.

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