MPRI Concurrency (Cours 2-3)
Final exam, 2005-2006
22 Feb 2006, 16.15–19.15
James.Leifer@inria.fr

Question annotations: [$*$] = easy; [$**$] = medium; [$***$] = hard

1. Consider the term $P = \boldsymbol{\nu} y.(x(x).x(x).\overline{x}y) \mid \boldsymbol{\nu} y.(\overline{x}y.\boldsymbol{\nu} x.(\overline{y}x.x(x)))$ with $x \neq y$.

   (a) [$*$] What is the set of free names of P?

   Solution: $\{x\}$.

   (b) [$*$] Define a process P' that is α-equivalent to P and has all bound names distinct from each other and from all free names.

   Solution: $P' = \boldsymbol{\nu} y_1.(x(x_1).x_1(x_2).\overline{x_2}y_1) \mid \boldsymbol{\nu} y_2.(\overline{x}y_2.\boldsymbol{\nu} x_3.(\overline{y_2}x_3.x_3(x_4)))$.

   (c) [$*$] What is the set of free names of P'?

   Solution: $\{x\}$, since α-conversion doesn't change the free names.

   (d) [$**$] Show the sequence of three reduction steps ($\longrightarrow$) starting at P', taking care to make explicit any scope extrusions you need (i.e. use of (str-ex) in $\equiv$).

   Solution:

	P'	
$\equiv$	$\boldsymbol{\nu} y_1, y_2.(x(x_1).x_1(x_2).\overline{x_2}y_1 \mid \overline{x}y_2.\boldsymbol{\nu} x_3.(\overline{y_2}x_3.x_3(x_4)))$	extrusion of y_2
$\longrightarrow$	$\boldsymbol{\nu} y_1, y_2.(y_2(x_2).\overline{x_2}y_1 \mid \boldsymbol{\nu} x_3.(\overline{y_2}x_3.x_3(x_4)))$	communication on x
$\equiv$	$\boldsymbol{\nu} y_1, y_2, x_3.(y_2(x_2).\overline{x_2}y_1 \mid \overline{y_2}x_3.x_3(x_4))$	extrusion of x_3
$\longrightarrow$	$\boldsymbol{\nu} y_1, y_2, x_3.(\overline{x_3}y_1 \mid x_3(x_4))$	communication on y_2
$\longrightarrow$	$\boldsymbol{\nu} y_1, y_2, x_3.(\mathbf{0} \mid \mathbf{0})$	communication on x_3

2. This question explores the relationship between name hiding and bisimulation in the core π-calculus (i.e. the calculus on slide 3 with no extra features).

   (a) [$***$] Prove that strong bisimilarity is closed by new binding, i.e. $P \sim Q$ implies $\boldsymbol{\nu} x.P \sim \boldsymbol{\nu} x.Q$. You may only use the basic definitions of bisimulation and labelled transition (no "up to" techniques).
   Hint: start with a relation $\mathcal{R} = \{(\boldsymbol{\nu} x.P, \boldsymbol{\nu} x.Q) \ / \ P \sim Q\}$ and try to show that $\mathcal{R}$ is a strong bisimulation. You may have to add some more pairs to $\mathcal{R}$.

   Solution: Take $\mathcal{R}' = \mathcal{R} \cup (\sim)$. We aim to show that $\mathcal{R}'$ is a bisimulation. To do that we need to consider $(P_0, Q_0) \in \mathcal{R}'$ and $P_0 \xrightarrow{\alpha} P'_0$ with $\mathsf{bn}(\alpha) \cap \mathsf{fn}(Q_0) = \varnothing$. We distinguish two cases.

   Case $P_0 \sim Q_0$: By definition of $\sim$, there exists Q'_0 such that $Q_0 \xrightarrow{\alpha} Q'_0$ and $P'_0 \sim Q'_0$, hence $(P'_0, Q'_0) \in \mathcal{R}'$, as desired.

   Case $(P_0, Q_0) \in \mathcal{R}$: Then there exists P and Q such that $P \sim Q$ and $P_0 = \boldsymbol{\nu} x.P$ and $Q_0 = \boldsymbol{\nu} x.Q$. We consider the two possible ways that the labelled transition $P_0 \xrightarrow{\alpha} P'_0$ could have been derived.

   Case (lab-new): Then there exists P' such that $P \xrightarrow{\alpha} P'$ and $P'_0 = \boldsymbol{\nu} x.P'$ and $x \notin \mathsf{bn}(\alpha)$. By hypothesis, we also have $\mathsf{bn}(\alpha) \cap \mathsf{fn}(Q_0) = \varnothing$, hence $\mathsf{bn}(\alpha) \cap \mathsf{fn}(Q) = \varnothing$, thus it is safe to apply the definition of bisimulation to the hypothesis $P \sim Q$; hence there exists Q' such that $Q \xrightarrow{\alpha} Q'$ and $P' \sim Q'$. Let $Q'_0 = \boldsymbol{\nu} x.Q'$. Then by (lab-new), $Q_0 \xrightarrow{\alpha} Q'_0$. Finally, $(P'_0, Q'_0) \in \mathcal{R} \subseteq \mathcal{R}'$, as desired.

Case (lab-open): Then there exists P' and w such that $P \xrightarrow{\overline{w}x} P'$ and $w \neq x$ and $P'_0 = P'$ and $\alpha = \overline{w}(x)$. By hypothesis, $P \sim Q$, so there exists Q' such that $Q \xrightarrow{\overline{w}x} Q'$ and $P' \sim Q'$. Let $Q'_0 = Q'$. By (lab-open), $Q_0 \xrightarrow{\alpha} Q'_0$. Finally, $(P'_0, Q'_0) \in (\sim) \subseteq \mathcal{R}'$, as desired.

Since $\mathcal{R}'$ is a symmetric relation, we conclude that it is a bisimulation. Hence for any $P \sim Q$, we have $(\boldsymbol{\nu}x.P, \boldsymbol{\nu}x.Q) \in \mathcal{R}' \subseteq (\sim)$, which completes the proof.

(b) [*] Give a counterexample to show that the converse is false, i.e. $\boldsymbol{\nu}x.P \sim \boldsymbol{\nu}x.Q$ does not imply $P \sim Q$.

Solution: Take $P = \overline{x}y$ and $Q = \mathbf{0}$ with x, y distinct. Then $\boldsymbol{\nu}x.P \sim \boldsymbol{\nu}x.Q$ since both sides are deadlocked. However $P \not\sim Q$ since P has the labelled transition $P \xrightarrow{\overline{x}y}$ but Q does not.

(c) [**] However if we hide *and then reveal* a name, then it is as if we never hid it! Prove that $\boldsymbol{\nu}x.(\overline{k}x \mid P) \sim \boldsymbol{\nu}x.(\overline{k}x \mid Q)$ implies $P \sim Q$ for $k \notin \mathsf{fn}(P) \cup \mathsf{fn}(Q) \cup \{x\}$.

Hint: There is no need to explicitly construct a bisimulation relation containing (P, Q). Instead consider the $\overline{k}(x)$ labelled transitions of $\boldsymbol{\nu}x.(\overline{k}x \mid P)$ and $\boldsymbol{\nu}x.(\overline{k}x \mid Q)$. Take care to clearly write out any proof trees you use when deriving labelled transitions.

Solution: We can infer a bound output for $\boldsymbol{\nu}x.(\overline{k}x \mid P)$ by the following derivation:

$$\cfrac{\cfrac{\cfrac{}{\overline{k}x \xrightarrow{\overline{k}x} \mathbf{0}}\,(\textsf{lab-out})}{\overline{k}x \mid P \xrightarrow{\overline{k}x} \mathbf{0} \mid P}\,(\textsf{lab-par-l})}{\boldsymbol{\nu}x.(\overline{k}x \mid P) \xrightarrow{\overline{k}(x)} \mathbf{0} \mid P}\,k \neq x, (\textsf{lab-open})$$

Since we have two bisimilar processes, $\boldsymbol{\nu}x.(\overline{k}x \mid P) \sim \boldsymbol{\nu}x.(\overline{k}x \mid Q)$, and $x \notin \mathsf{fn}(\boldsymbol{\nu}x.(\overline{k}x \mid Q))$, we know that the right-hand process must be able to match the transition we just derived, i.e. there exits Q'' such that $\mathbf{0} \mid P \sim Q''$ and $\boldsymbol{\nu}x.(\overline{k}x \mid Q) \xrightarrow{\overline{k}(x)} Q''$. There are only two possible rules that the this last labelled transition can be derived from, the first of which turns out to be impossible.

Case (lab-new): By the side condition for the rule, the only way it can be applied is if we do α-conversion on x, i.e. we have a derivation of the form:

$$\cfrac{\overline{k}x' \mid \{x'/x\}Q \xrightarrow{\overline{k}(x)}}{\boldsymbol{\nu}x'.(\overline{k}x' \mid \{x'/x\}Q) \xrightarrow{\overline{k}(x)}}\,(\textsf{lab-new})$$

where x' is fresh. Suppose, for contradition, that the premiss were derivable. By hypothesis, $k \notin \mathsf{fn}(Q)$, hence $k \notin \mathsf{fn}(\{x'/x\}Q)$, therefore we cannot have $\{x'/x\}Q \xrightarrow{\overline{k}(x)}$. Nor can $\overline{k}x' \xrightarrow{\overline{k}(x)}$ since x' is free here, disallowing any bound output. Thus this case is impossible.

Case (lab-open): Then the premiss is $\overline{k}x \mid Q \xrightarrow{\overline{k}x} Q''$. Since $k \notin \mathsf{fn}(Q)$, the output is due to $\overline{k}x \xrightarrow{\overline{k}x} \mathbf{0}$, thus $Q'' = \mathbf{0} \mid Q$. Finally, $P \sim \mathbf{0} \mid P \sim \mathbf{0} \mid Q \sim Q$, as desired.

3. This question addresses relationships between labelled transitions and barbs in the core π-calculus.

(a) [***] Prove that $P \xrightarrow{\overline{x}y} P'$ implies $P{\downarrow}x$. Hint: induct on the derivation of $P \xrightarrow{\overline{x}y} P'$.

Solution: According to the definition of $P{\downarrow}x$, we have to show that there exists $\vec{z}$, w, P_0, and P_1 such that $P \equiv \boldsymbol{\nu}\vec{z}.(\overline{x}w.P_0 \mid P_1)$. In fact we can always use $w = y$, as we show in the following induction on the derivation of $P \xrightarrow{\overline{x}y} P'$.

Case (lab-out): Then there exists P_0 such that $P = \overline{x}y.P_0$. Take $P_1 = \mathbf{0}$ and $\vec{z}$ to be the empty list of names. Then $P \equiv \boldsymbol{\nu}\vec{z}.(\overline{x}y.P_0 \mid P_1)$, as required.

Case (lab-par-l): Then there exists P_2 and Q such that $P = P_2 \mid Q$ with the premiss $P_2 \xrightarrow{\overline{x}y}$. Applying the inductive hypothesis to the premiss, there exist $\vec{z}$, P_0, and P_1 such that $P_2 \equiv \boldsymbol{\nu}\vec{z}.(\overline{x}y.P_0 \mid P_1)$. Without loss of generality, we may assume that $\vec{z} \cap \mathsf{fn}(Q) = \varnothing$, hence $P = P_2 \mid Q \equiv \boldsymbol{\nu}\vec{z}.(\overline{x}y.P_0 \mid P_1) \mid Q \equiv \boldsymbol{\nu}\vec{z}.(\overline{x}y.P_0 \mid (P_1 \mid Q))$ by scope extrusion, as required.

Case (lab-par-r): Symmetric to the previous case.

Case (lab-new): There exists P_2 and u such that $P = \boldsymbol{\nu}u.P_2$ and $u \notin \{x, y\}$, with the premiss $P_2 \xrightarrow{\overline{x}y}$. Applying the inductive hypothesis to the premiss, there exist $\vec{z}$, P_0, and P_1 such that $P_2 \equiv \boldsymbol{\nu}\vec{z}.(\overline{x}y.P_0 \mid P_1)$. Hence $P = \boldsymbol{\nu}u.P_2 \equiv \boldsymbol{\nu}u.(\boldsymbol{\nu}\vec{z}.(\overline{x}y.P_0 \mid P_1))$, as required.

(b) [*] Give an example to show that the converse is not true, i.e. find a P such that $P{\downarrow}x$ but not $P \xrightarrow{\overline{x}y}$.

Solution: Take $P = \boldsymbol{\nu}y.\overline{x}y$. Then $P{\downarrow}x$ but P can only do a *bound output* on x, i.e. $P \xrightarrow{\overline{x}(y)} \mathbf{0}$.