Models of Computation

Written Exam on September 4, 2013

Exercise 1 (6)

Let us extend **IMP** with a new syntactic category *Prog* for *programs* defined by the clause

$$p \ ::= \ \mathbf{prog}\ c.$$

Define an operational and a denotational semantics with

$$< p, n > \longrightarrow m \qquad \text{e} \qquad \mathcal{P}:\ Prog \to N \to N_\perp.$$

Finally extend to the new construct the proofs of equivalence between operational and denotational semantics. (Hint: Consider two special locations **input** and **output**, where to write the initial datum n and where to read the result m respectively. Initially, every location different from **input** will contain 0. Thus the initial memory will be $\sigma_0[n/\mathbf{input}]$, with $\forall x.\ \sigma_0(x) = 0$.)

Exercise 2 (6)

Let

$$\mathcal{P} = \{(X,Y) \mid X, Y \subseteq \omega \wedge X \cap Y = \emptyset\} \quad \text{with} \quad (X,Y) \sqsubseteq (X',Y') \text{ iff } X \subseteq X' \wedge Y' \subseteq Y$$

Prove that: (i) $(\mathcal{P}, \sqsubseteq)$ is a partial ordering; (ii) $(\mathcal{P}, \sqsubseteq)$ is complete.

Exercise 3 (8)

Consider HOFL with the following additional inference rule:

$$\frac{t_1 \to 0}{t_1 * t_2 \to 0}$$

and prove that determinism still holds: $t \to c_1,\ t \to c_2 \Rightarrow c_1 = c_2$. On the contrary, prove with a counterexample that the property $t \to c \ \Rightarrow\ [\![t]\!] = [\![c]\!]$ does not hold. Thus modify the denotational semantics to make the above property true and prove it. Finally add also the rule

$$\frac{t_2 \to 0}{t_1 * t_2 \to 0}$$

and repeat the same steps: find another counterexample and fix the denotational semantics accordingly, if possible.

Exercise 4 (5)

Prove that CCS strong bisimilarity is a congruence for restriction and sum, namely

$$p \simeq q \ \Rightarrow\ p\backslash\alpha \simeq\ q\backslash\alpha \qquad p_1 \simeq q_1\ \ p_2 \simeq q_2 \ \Rightarrow\ p_1 + p_2 \simeq q_1 + q_2.$$

Exercise 5 (5)

Consider the PEPA program B with

$$A = (\alpha,\lambda).B + (\alpha,\lambda).C \quad B = (\alpha,\lambda).A + (\alpha,\lambda).C \quad C = (\alpha,\lambda).B$$

and derive the corresponding finite state CTMC. What is the probability distribution of staying in B? If $\lambda = 0.1\ sec^{-1}$, what it the probability that the system be still in B after 10 seconds? Are there bisimilar states?

Correzione della Prova Scritta del 4 settembre 2013

ES. 1

Semantica Operazionale

$$\frac{\langle c, \sigma_0[n/input]\rangle \to \sigma}{\langle prog\ c, n\rangle \to \sigma(output)} \qquad \text{dove } \forall x.\ \sigma_0(x) = 0$$

Semantica Denotazionale

$$\mathcal{P}[\![prog\ c]\!]\, n = (\lambda\sigma'.\ \sigma'(output))^{*}\ \mathcal{C}[\![c]\!]\,\sigma_0[n/input]$$

$$P(\langle p, n\rangle \to m) \overset{def}{=} \mathcal{P}[\![p]\!]\, n \overset{?}{=} m$$

$$P(\langle prog\ c, n\rangle \to \sigma(output)) \overset{def}{=} \mathcal{P}[\![prog\ c]\!]\, n \overset{?}{=} \sigma(output)$$

$$\mathcal{P}[\![prog\ c]\!]\, n = (\lambda\sigma'.\ \sigma'(output))^{*}\ \mathcal{C}[\![c]\!]\,\sigma_0[n/input]$$

ma per l'equivalenza sui comandi, abbiamo

$$P(\langle c, \sigma_0[n/input]\rangle \to \sigma) \overset{def}{=} \mathcal{C}[\![c]\!]\,\sigma_0[n/input] = \sigma$$

quindi si può sostituire ed eliminare la $*$:

$$\mathcal{P}[\![prog\ c]\!]\, n = (\lambda\sigma'.\ \sigma'(output))\,\sigma \overset{?}{=} \sigma(output) \qquad \text{CVD.}$$

2

$$\underline{P}(p) \stackrel{def}{=} \mathcal{P}[\![p]\!]n = m \Rightarrow \langle p, n\rangle \to m$$

$$\underline{P}(\text{prog } c) \stackrel{def}{=} \mathcal{P}[\![\text{prog } c]\!]n = m \stackrel{?}{\Rightarrow} \langle p, n\rangle \to m$$

Assumiamo la premessa

$(\lambda \sigma'. \sigma'(output))^* \mathcal{C}[\![c]\!] \sigma_0[n/input] = m$

Essendo $m \neq \bot_N$, anche $\mathcal{C}[\![c]\!]\sigma_0[n/input] = \sigma$

con $\langle c, \sigma_0[n/input]\rangle \to \sigma$ per le proprietà dei comandi.

inoltre eliminando la $*$ abbiamo

$(\lambda \sigma'. \sigma'(output))\ \sigma = m$ quindi $m = \sigma(output)$

Quindi possiamo applicare la semantica operazionale

$\langle \text{prog } c, n\rangle \to \sigma(output) = m$ CVD.

2 a) i) riflessività

$$(X,Y) \sqsubseteq (X,Y) \iff X \overset{?}{\subseteq} X \wedge Y \overset{?}{\subseteq} Y \quad \text{OK.}$$

ii) antisimmetria

$$(X,Y) \sqsubseteq (X',Y') \wedge (X',Y') \sqsubseteq (X,Y) \overset{?}{\Longrightarrow} X=X' \wedge Y=Y'$$

$$X \subseteq X' \wedge Y' \subseteq Y \wedge X' \subseteq X \wedge Y \subseteq Y' \overset{?}{\Longrightarrow} X=X' \wedge Y=Y' \quad \text{OK.}$$

iii) transitività

$$(X,Y) \sqsubseteq (X',Y') \sqsubseteq (X'',Y'') \overset{?}{\Longrightarrow} (X,Y) \sqsubseteq (X'',Y'')$$

$$X \subseteq X' \subseteq X'' \wedge Y'' \subseteq Y' \subseteq Y \overset{?}{\Longrightarrow} X \subseteq X'' \wedge Y'' \subseteq Y \quad \text{OK}$$

b) $\bigsqcup_{i \in \omega} (X_i, Y_i)$ esiste?

Dimostriamo che $\left(\bigcup_{i \in \omega} X_i , \bigcap_{i \in \omega} Y_i \right)$

i) è un maggiorante: ovvio che $\left(\bigcup_{i \in \omega} X_i , \bigcap_{i \in \omega} Y_i \right) \sqsupseteq (X_i, Y_i) \ \forall i.$

Bisogna però dimostrare che

$$\left(\bigcup_{i \in \omega} X_i \right) \cap \left(\bigcap_{i \in \omega} Y_i \right) = \emptyset$$

Per assurdo:

sia $n \in \bigcup_{i \in \omega} X_i$. Allora $\exists i.\ n \in X_i$.

Sia $n \in \bigcap_{i \in \omega} Y_i$. Allora $\forall j.\ n \in Y_i$

4

Quindi $X_i \cap Y_i \neq \emptyset$ assurdo. OK

iii) E' il minimo maggiorante. Per assurdo.

Se $(\overline{X}, \overline{Y}) \lneq \left(\left(\bigcup_{i \in \omega} X_i\right), \left(\bigcap_{i \in \omega} Y_i\right)\right)$

allora $\overline{X} \subsetneq \bigcup_{i \in \omega} X_i \quad \forall i.\ \overline{X} \subseteq X_i$ oppure

$\overline{Y} \supsetneq \bigcap_{i \in \omega} Y_i \quad \forall i.\ \overline{Y} \supseteq Y_i$ assurdo.

Esercizio 3

Per induzione sulle regole

$P(t \to c_1) \stackrel{def}{=} t \to c_2 \Rightarrow c_1 = c_2$

Ci sono due regole per $t_1 * t_2$:

$$\frac{t_1 \to n_1 \quad t_2 \to n_2}{t_1 * t_2 \to n_1 n_2}$$

Dobbiamo di mostrare

$P(t_1 * t_2 \to n_1 n_2) \stackrel{def}{=} t_1 * t_2 \to m \Rightarrow n_1 n_2 = m$

Assumiamo $t_1 * t_2 \to m$. Se procediamo goal oriented con la stesse regole abbiamo

$t_1 * t_2 \to m \xleftarrow[m = n_1' n_2']{} t_1 \to n_1' \quad t_2 \to n_2'$

con l'ipotesi induttiva $t_1 \to n_1$ e $t_1 \to n_1' \Rightarrow n_1 = n_1'$
$t_2 \to n_2$ e $t_2 \to n_2' \Rightarrow n_2 = n_2'$ $\Rightarrow m = n_1 n_2$

CVD

Possiamo anche usare la nuova regola:

$t_1 * t_2 \to m \xleftarrow[m = 0]{} t_1 \to 0$

Ma se $t_1 \to 0$ allora $n_1 = 0$ per l'ip. induttiva.

Quindi ancora $n_1 n_2 = m$.

Con la seconda regola $\frac{t_1 \to 0}{t_1 * t_2 \to 0}$ assumiamo $t_1 * t_2 \to 0$.

Con la 2ª regola è banale.

Con la 1ª regola $t_1 * t_2 \to 0 \xleftarrow[n_1 n_2 = 0]{} t_1 \to n_1 \quad t_2 \to n_2$

Anche qui $0 = 0$.

Il controesempio è

$$0 * \mathrm{rec}\, x.x \to n \xleftarrow[n=0]{} 0 \to 0 \longleftarrow \square$$

con $[\![0 * \mathrm{rec}\, x.x]\!]\rho = \lfloor 0 \rfloor \underline{*}_\perp \perp_{N_\perp} = \perp_{N_\perp}$

La nuova semantica è:

$$[\![t_1 * t_2]\!]\rho = Cond([\![t_1]\!]\rho, \lfloor 0 \rfloor, [\![t_1]\!]\rho \underline{*}_\perp [\![t_2]\!]\rho)$$

La prova è sulle regole:

$$\frac{t_1 \to 0}{t_1 * t_2 \to 0} \qquad t_1 \to 0 \text{ per ip. induttiva } [\![t_1]\!]\rho = \lfloor 0 \rfloor$$

$P(t_1 * t_2 \to 0) \stackrel{def}{=} [\![t_1 * t_2]\!]\rho = \lfloor 0 \rfloor$

$[\![t_1 * t_2]\!]\rho = Cond([\![t_1]\!]\rho, \lfloor 0 \rfloor, [\![t_1]\!]\rho \underline{*}_\perp [\![t_2]\!]\rho)$
$= \lfloor 0 \rfloor$ CVD

Va dimostrata anche l'altra regola!

$$\frac{t_1 \to n_1 \quad t_2 \to n_2}{t_1 * t_2 \to n_1 n_2}$$

$P(t_1 * t_2 \to n_1 n_2) \stackrel{def}{=} [\![t_1 * t_2]\!] = \lfloor n_1 n_2 \rfloor$

$Cond([\![t_1]\!]\rho, \lfloor 0 \rfloor, [\![t_1]\!]\rho \underline{*}_\perp [\![t_2]\!]\rho)$

Caso $[\![t_1]\!]\rho = \lfloor 0 \rfloor$. Anche $[\![n_1]\!]\rho = \lfloor 0 \rfloor$ $n_1 = 0$

$Cond(\lfloor 0 \rfloor, \lfloor 0 \rfloor, \ldots) = \lfloor 0 \rfloor = \lfloor n_1 n_2 \rfloor$

Caso $[\![t_1]\!]\rho = \lfloor n_1 \rfloor \neq \lfloor 0 \rfloor$

$Cond(\lfloor n_1 \rfloor, \lfloor 0 \rfloor, [\![t_1]\!]\rho \underline{*}_\perp [\![t_2]\!]\rho) = [\![t_1]\!]\rho \underline{*}_\perp [\![t_2]\!]\rho$
$= \lfloor n_1 n_2 \rfloor$ per ip. induttiva.

con l'aggiunta delle regole

$$\frac{t_2 \to 0}{t_1 * t_2 \to 0}$$

c'è un altro controesempio

$$rec\, x.\, x * 0 \to n \Leftarrow 0 \to 0 \Leftarrow \square$$

mentre $[\![rec\, x.\, x * 0]\!]\rho = Cond(\bot, \lfloor 0 \rfloor, m) = \bot$

Non c'è modo di dare una semantica denotazionale corrispondente. Servirebbe un prodotto non stretto!

$x_1 \backslash x_2$	$\bot$	0	$m \neq 0$
$\bot$	$\bot$	0	$\bot$
0	0	0	0
$n \neq 0$	$\bot$	0	nm

$x_1 \circledast x_2$

che è possibile essendo continuo (monotono).
ma non è esprimibile con le funzioni viste per HOFL. Se si introduce, allora

$$[\![t_1 * t_2]\!]\rho = [\![t_1]\!]\rho \circledast [\![t_2]\!]\rho.$$

Esercizio 4

(i) $p \simeq q \overset{?}{\Rightarrow} p\backslash\alpha \simeq q\backslash\alpha$

Se $p \simeq q$ esiste R bisimulazione (cioè $R = \phi(R)$) con pRq. Sia $R' = \{(p'\backslash\alpha, q'\backslash\alpha) \mid p'Rq'\}$

Dimostriamo che R' è una bisimulazione, evidentemente con $p\backslash\alpha\, R'\, q\backslash\alpha$.

Infatti se $p'Rq'$ allora $p' \xrightarrow{\mu} p''$ implica $q' \xrightarrow{\mu} q''$ con $p''Rq''$ e viceversa.

Quindi se $p'\backslash\alpha\, R'\, q'\backslash\alpha$ allora $p'\backslash\alpha \xrightarrow{\mu} p''\backslash\alpha$ implica $q'\backslash\alpha \xrightarrow{\mu} q''\backslash\alpha$ con $p''\backslash\alpha\, R'\, q''\backslash\alpha$.

Questo è possibile essendo le mosse di $p'\backslash\alpha$ le stesse di p', meno quelle etichettate α o $\bar{\alpha}$.

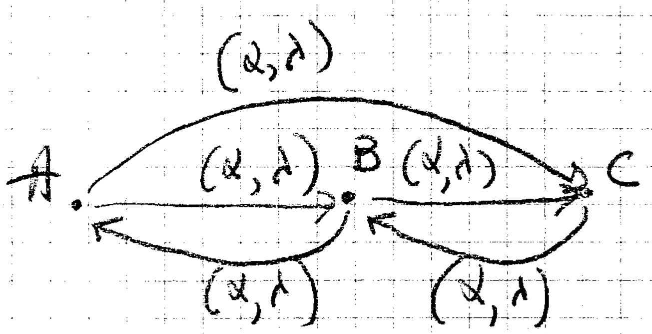
(ii) $p_1 \simeq q_1 \quad p_2 \simeq q_2 \overset{?}{\Rightarrow} p_1 + p_2 \simeq q_1 + q_2$

Sia R_1 una bisimulazione con $p_1 R_1 q_1$ e R_2 con $p_2 R_2 q_2$

Sia ora $R = R_1 \cup R_2 \cup \{p_1 + p_2 \simeq q_1 + q_2\}$
evidentemente con $p_1 + p_2 \; R \; q_1 + q_2$

R è una bisimulazione, in quanto se $p_1 \xrightarrow{\mu} p_1'$ allora $q_1 \xrightarrow{\mu} q_1'$ e $p_1 R_1 q_1$. Ma allora se $p_1 + p_2 \xrightarrow{\mu} p_1'$ abbiamo $q_1 \xrightarrow{\mu} q_1$ e $p_1' R\, q_1'$. Similmente se $p_1 + p_2 \xrightarrow{\mu} p_2'$.

Exercise 5



$\text{Prob}\{X_t = B \mid X_0 = B\} = e^{-\lambda_a t}$ λ_a: apparent rate

$\lambda = 0.1 \quad t = 10 \quad \lambda_a = 2\lambda = 0.2$

$\text{Prob} = e^{-2} = 0{,}3387$

$R_0 = \{\{A,B,C\}\}$

$\gamma\, A\, \alpha \{A,B,C\} = 2\lambda$

$\gamma\, B\, \alpha \{A,B,C\} = 2\lambda$ $\qquad R_1 = \{\{A,B\},\{C\}\}$

$\gamma\, C\, \alpha \{A,B,C\} = \lambda$

$\gamma\, A\, \alpha \{A,B\} = \lambda \qquad \gamma\, B\, \alpha \{A,B\} = \lambda$

$\gamma\, A\, \alpha \{C\} = \lambda \qquad \gamma\, B\, \alpha \{C\} = \lambda$

$R_2 = \{\{A,B\},\{C\}\} = R_1 = \text{fix}$