Tecniche di Specifica e Dimostrazione

Prova scritta del 4 settembre 2009

Esercizio 1 (7 punti)

Si calcoli la semantica denotazionale del comando IMP:

$$c \;=\; \textbf{if } b \textbf{ then while } \mathit{true} \textbf{ do } c' \textbf{ else while } \mathit{false} \textbf{ do } c'.$$

Si diano quindi condizioni sufficienti su c' affinche' c e **while** b *do* c' abbiano la stessa semantica denotazionale per ogni b e si fornisca un comando c' per cui cio' accade. Infine si diano condizioni necessarie e sufficienti.

Esercizio 2 (8 punti)

Si consideri l'ordinamento parziale completo $\langle D, \sqsubseteq \rangle$ con $D = \omega \cup \{\infty\}$ e

$$n \leq m \Rightarrow n \sqsubseteq m \quad x \sqsubseteq \infty \quad n, m \in \omega \;\; x \in D.$$

Si dimostri che la relazione $\langle D', \sqsubseteq' \rangle$ con $D' = D \to D$ e

$$f \sqsubseteq' g \quad \text{se e solo se} \quad \forall x.\; f(x) \sqsubseteq g(x)$$

(i) e' un ordinamento parziale; (ii) e' completo; (iii) possiede il minimo elemento $\bot'$; (iv) possiede il massimo elemento $\top'$; (v) possiede il minimo maggiorante (lub) non solo di ogni catena, ma di ogni insieme di elementi.

Esercizio 3 (11 punti)

Si assuma che il termine HOFL t_2 abbia forma canonica c_2. Si dimostri utilizzando il lemma di sostituzione *(i)* che per ogni termine t_1' vale

$$[\![t_1'[t_2/x]]\!]\rho \;= [\![t_1'[c_2/x]]\!]\rho.$$

Si dimostri quindi, utilizzando un teorema enunciato a lezione, nell'ipotesi che t_1' sia un termine di tipo *int* con variabili libere al piu' x, *(ii)* che $t_1'[t_2/x]$ e $t_1'[c_2/x]$ o non hanno forma canonica o hanno la stessa forma canonica.

Si concluda *(iii)* che sostitendo in HOFL la regola *lazy*

$$\frac{t_1 \to \lambda x.\; t_1' \;\; t_1'[t_2/x] \to c}{(t_1 \;\; t_2) \to c} \quad \text{con la regola } \textit{eager} \quad \frac{t_1 \to \lambda x.\; t_1' \;\; t_2 \to c_2 \;\; t_1'[c_2/x] \to c}{(t_1 \;\; t_2) \to c}$$

se vale $(t_1 \;\; t_2) \to c$ nel caso eager, allora questo vale anche nel caso lazy.

Si faccia infine vedere *(iv)* un semplice controesempio in cui valga $(t_1 \;\; t_2) \to c$ nel caso lazy ma non nel caso eager, e *(v)* un altro controesempio in cui, essendo t_1' non di tipo *int*, le proprieta' *(ii)* e *(iii)* non valgono.

Esercizio 4 (4 punti)

Si considerino gli agenti CCS

$$A \;=\; (\textbf{rec } x.\alpha.x) + (\textbf{rec } x.\beta.x) \qquad \text{e} \qquad B \;=\; \textbf{rec } x.(\alpha.x + \beta.x).$$

Si calcoli l'insieme S di tutti gli agenti raggiungibili da essi (anche con molti passi) e le relative transizioni. Si applichi iterativamente a SxS l'operatore di bisimulazione Φ visto a lezione fino a raggiungere il punto fisso. Si concluda dal risultato che A e B non sono bisimilari. Si determini infine una formula della logica Hennessy - Milner in grado di distinguere tra A e B.