Tecniche di Specifica e Dimostrazione

Prova scritta del 7 aprile 2009

Esercizio 1 (10 punti)

Il comando $\mathbf{if^n}\ b\ \mathbf{then}\ c$ è un'abbreviazione del comando:

$$\begin{array}{rcl} \mathbf{if^1}\ b\ \mathbf{then}\ c & = & \mathbf{if}\ b\ \mathbf{then\ div\ else\ skip} \\ \mathbf{if^{n+1}}\ b\ \mathbf{then}\ c & = & \mathbf{if}\ b\ \mathbf{then}\ (c\ ;\mathbf{if^n}\ b\ \mathbf{then}\ c)\ \mathbf{else\ skip} \end{array}$$

dove $\mathbf{div}\ =\ \mathbf{while}\ true\ \mathbf{do\ skip}$. Ad esempio:

$$\mathbf{if^2}\ b\ \mathbf{then}\ c\ =\ \mathbf{if}\ b\ \mathbf{then}\ (c\ ;\mathbf{if}\ b\ \mathbf{then\ div\ else\ skip})\ \mathbf{else\ skip}.$$

Si dimostri che la semantica di $\mathbf{if^n}\ b\ \mathbf{then}\ c$ coincide con quella di $\mathbf{while}\ b\ \mathbf{do}\ c$ nel caso in cui quest'ultimo comando venga eseguito al più n volte. A tale scopo si dimostri, per la semantica operazionale, la proprietà

$$\begin{array}{rcll} P(n,i) \stackrel{def}{=} & < \mathbf{if^n}\ b\ \mathbf{then}\ c, \sigma > \rightarrow \sigma' & \underbrace{\stackrel{true}{\longleftarrow} \ldots \stackrel{true}{\longleftarrow}}_{i\ volte} \stackrel{false}{\longleftarrow} G & \text{and} \\ & < \mathbf{while}\ b\ \mathbf{do\ c}, \sigma > \rightarrow \sigma' & \underbrace{\stackrel{true}{\longleftarrow} \ldots \stackrel{true}{\longleftarrow}}_{i\ volte} \stackrel{false}{\longleftarrow} G' & \text{implies}\ \ G = G' \end{array}$$

che tutte le prove goal-oriented che utilizzano i volte ($0 \leq i < n$) la regola *true* e una volta la regola *false* riducono $\mathbf{if^n}\ b\ \mathbf{then}\ c$ e $\mathbf{while}\ b\ \mathbf{do}\ c$ agli stessi sottogoal. Come prima cosa si constati la proprietà per le prove per $n = 2$ e $i = 0, 1$. (Cenno. Per il caso generale si dimostri come caso base $P(n, 0)$ e assumendo $P(n, i)$ si dimostri $P(n + 1, i + 1), 0 \leq i < n$).

Per la semantica denotazionale si dimostri che $\mathcal{C}[\![\mathbf{if^n}\ b\ \mathbf{then}\ c]\!] = \Gamma^n \perp, n = 1, \ldots$, dove al solito $\Gamma = \lambda\varphi.\lambda\sigma.\mathcal{B}[\![b]\!]\sigma \rightarrow \varphi^*(\mathcal{C}[\![c]\!]\sigma), \sigma$.

Esercizio 2 (9 punti)

Si considerino le regole di inferenza R su formule ben formate che sono stringhe su $\{S, (,)\}$ corrispondenti alla grammatica $S ::= ()|(S)|SS$, se ne definisca il corrispondente operatore $\hat{R}$ delle conseguenze immediate e si costruisca l'insieme di stringhe $\hat{R}^3(\emptyset)$.

Si dimostri quindi che $\hat{R}^n(\emptyset)$ contiene almeno tutte le stringhe $\alpha \in fix(\hat{R}) = I_R$ con $|\alpha| \leq 2n$, e si concluda quindi che l'insieme I_R è un insieme decidibile.
(Cenno. Si ricordi che $\hat{R}^n(\emptyset)$ sono tutti i teoremi α dimostrabili con una qualche derivazione (d/α) profonda $|d| \leq n$ e si dimostri per induzione sulle derivazioni che $P(d/\alpha) \stackrel{def}{=} 2|d| \leq |\alpha|$. Pertanto se $\alpha \in I_R$ con $|\alpha| \leq 2n$, allora α ha una derivazione profonda al massimo n e quindi $\alpha \in \hat{R}^n(\emptyset)$.)

Esercizio 3 (11 punti)

Una *sostituzione* per la segnatura Σ che comprende un'operazione binaria f e una costante c, è una coppia di termini $\sigma =< t_1(x_1, x_2), t_2(x_1, x_2) >$ sulla segnatura Σ con variabili x_1 e x_2.

La *composizione sequenziale* $\sigma;\sigma'$ di $\sigma =< t_1(x_1, x_2), t_2(x_1, x_2) >$ e $\sigma' =< t'_1(x_1, x_2), t'_2(x_1, x_2) >$ è definita come $\sigma;\sigma' =< t'_1[t_1/x_1, t_2/x_2], t'_2[t_1/x_1, t_2/x_2] >$. Ad esempio se $\sigma =< f(c, x_2), c >$ e $\sigma' =< f(x_1, x_1), x_1 >$, allora $\sigma;\sigma' =< f(f(c, x_2), f(c, x_2)), f(c, x_2) >$.

Si osservi che $\_;\_$ è un *monoide*, cioè esiste una sostituzione id con $id;\sigma = \sigma;id = \sigma$ (lo si dimostri), e $\sigma_1;(\sigma_2;\sigma_3) = (\sigma_1;\sigma_2);\sigma_3$ (si assuma).

La relazione $\sqsubseteq$ sulle sostituzioni è definita come $\sigma' \sqsubseteq \sigma''$ se e solo se esiste una sostituzione σ con $\sigma;\sigma' = \sigma''$. Quindi nell'esempio $< f(x_1, x_1), x_1 > \sqsubseteq < f(f(c, x_2), f(c, x_2)), f(c, x_2) >$.

Si dimostri che $\sqsubseteq$ non è un ordinamento parziale, ma è un preordine (cioè valgono le proprietà riflessiva e transitiva ma non quella antisimmetrica). (Cenno: si consideri la sostituzione $\rho =< x_2, x_1 >$.)

Si definisca quindi la relazione di equivalenza $\equiv$ con $\sigma \equiv \sigma'$ se e solo se $\sigma \sqsubseteq \sigma'$ e $\sigma' \sqsubseteq \sigma$. Si dimostri che la risultante relazione $\sqsubseteq_{/\equiv}$ sulle classi di equivalenza di $\equiv$ è un ordinamento parziale con bottom. Si dimostri infine che $\sqsubseteq_{/\equiv}$ non è un ordinamento parziale completo fornendo una catena senza maggioranti.