Tecniche di Specifica e Dimostrazione

Prova scritta del 21 luglio 2005

(Recupero 1^o compitino: Esercizi 1 e 2 | Recupero 2^o compitino: Esercizi 3 e 4)

Esercizio 1 (8 punti)

Si consideri il comando:

$$w \;=\; \textbf{while } n \neq m \textbf{ do if } n < m \textbf{ then } m := m - n \textbf{ else } n := n - m.$$

Si dimostri che, per ogni $\sigma, \sigma' \in \Sigma$ con $\langle w, \sigma \rangle \rightarrow \sigma', \sigma(n), \sigma(m) > 0$ e per ogni $d > 0$:

$$d|\sigma(n),\;\; d|\sigma(m) \qquad \text{se e solo se} \qquad \sigma'(n) = \sigma'(m) > 0,\;\; d|\sigma'(n)$$

dove $i|j$ significa che i è un divisore di j, cioè $\exists k. j = ki$.
Si dimostri infine che $\sigma'(n) = MCD(\sigma(n), \sigma(m))$ dove $k = MCD(i, j)$, con k, i, j naturali, è il massimo comun divisore di i e j, cioè $k|i$ e $k|j$ se e solo se $k|MCD(i, j)$.

Esercizio 2 (7 punti)

Si dimostri che la relazione $R_S = (\mathcal{P}(\omega)\backslash S, \subseteq)$ è un ordinamento parziale per ogni classe S di insiemi di naturali. Si individui quindi un insieme $\overline{S}$ tale che $R_{\overline{S}}$ non sia completo e non abbia minimo. Si dimostri infine che R_S è completo se S contiene solo insiemi finiti.

Esercizio 3 (10 punti)

Si consideri il termine HOFL lazy $\mathit{uncurry} = \lambda f.\, \lambda x\; ((f\;\, \mathit{fst}(x))\;\, \mathit{snd}(x)).$ e se ne calcoli il tipo più generale.
Si dimostri inoltre che se $f : \sigma \rightarrow \tau \rightarrow \rho$ e $x : \sigma * \tau$ allora $((f\;\, \mathit{fst}(x))\;\, \mathit{snd}(x))$ e $((\mathit{uncurry}\;\, f)\;\, x)$ hanno lo stesso tipo e infine che per tutti gli f e gli x $((f\;\, \mathit{fst}(x))\;\, \mathit{snd}(x))$ e $((\mathit{uncurry}\;\, f)\;\, x)$ hanno la stessa semantica operazionale.

Esercizio 4 (5 punti)

Si dimostri che la bisimilarità strong del CCS è una congruenza rispetto alla restrizione e alla somma, cioè che:

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

(Cenno: data una bisimulazione R tale che pRq, si costruisca partendo da R una relazione R' che si dimostri essere una bisimulazione e tale che $p\backslash\alpha\; R\; q\backslash\alpha$. Similmente per il caso del $+$.)