Informatica — 2015-01-16

Nota: Scrivete su **tutti** i fogli nome e matricola.

Esercizio 1. *Si definisca l'operatore* $\hat{\mathcal{R}}$ *e se ne dimostri la monotonia.*

Esercizio 2. *Il principio di induzione afferma che, sotto opportune ipotesi,* $f(X) \subseteq X \implies A \subseteq X$.

1. *Si elenchino tali ipotesi. In particolare, si dica cosa è* A.
2. *Sotto le stesse ipotesi, si dimostri che* $f(X \cap A) \subseteq X \implies A \subseteq X$.

Soluzione (bozza).
1) A è il minimo punto fisso di f, che deve essere una funzione monotona $f : \mathcal{P}(U) \to \mathcal{P}(U)$.

2) Per monotonia, da $X \cap A \subseteq A$ si ricava $f(X \cap A) \subseteq f(A) = A$ visto che A è punto fisso. Quindi, con l'ipotesi abbiamo che:

$$f(X \cap A) \subseteq A \qquad f(X \cap A) \subseteq X$$

da cui $f(X \cap A) \subseteq X \cap A$. Da questo, per il principio di induzione si ha che $A \subseteq X \cap A$, e quindi la tesi $A \subseteq X$. □

Esercizio 3. *Si consideri l'estensione di IMP ottenuta aggiungendo il comando* return*. La sua semantica intuitiva è quella di fermare il programma non appena viene eseguito. Per esempio, eseguendo a partire dallo stato* σ *il comando*

$$x := 1;\ \mathsf{while}\ 1 \neq 0\ \mathsf{do}\ (x := x + 4;\ \mathsf{return};\ x := x + 6)$$

questo termina nello stato $\sigma[x \mapsto 5]$.
La semantica big-step di questa estensione di IMP è una relazione

$$(\to_b) \in \mathcal{P}(Com \times Store \times Store \times \{\mathsf{norm}, \mathsf{ret}\})$$
$$\textit{Notazione: } \langle c, \sigma\rangle \to_b \langle \sigma', r\rangle$$

dove $r = \mathsf{norm}$ *indica che il comando è terminato normalmente, mentre* $r = \mathsf{ret}$ *indica che è terminato a causa di un* return.

1. *Si formalizzi la semantica* $\to_b$ *del* return *con una regola di inferenza.*
2. *Si formalizzi la nuova semantica* $\to_b$ *della composizione* $c_1; c_2$ *con regole di inferenza (ne potrebbero servire più di una).*

Si estenda ulteriormente IMP con il nuovo comando block c*, dove* c *è un comando. La sua semantica intuitiva è quella di fare in modo che dopo un* return *in* c *si prosegua il programma da dopo il* block*. Per esempio,*

$$c_{\mathsf{a}} = \quad (c_1; \mathsf{block}\ (c_2;\ \mathsf{return};\ c_3);\ c_4)$$

è equivalente a $c_{\mathsf{b}} = (c_1; c_2; c_4)$ *se* c_2 *non termina con un* return.

3. *Si formalizzi la semantica* $\to_b$ *di* $\mathsf{block}\ c$ *con regole di inferenza.*

4. *Si dimostri che se* $\langle c_{\mathsf{b}}, \sigma\rangle \to_b \langle \sigma', r\rangle$ *allora* $\langle c_{\mathsf{a}}, \sigma\rangle \to_b \langle \sigma', r\rangle$*, dove* c_{a} *e* c_{b} *sono i comandi visti sopra. Nel farlo, assumete che* c_2 *termina solo normalmente, ovvero che quando* $\langle c_2, \bar\sigma\rangle \to_b \langle \bar\sigma', \bar r\rangle$ *allora* $\bar r = \mathsf{norm}$*, per ogni* $\bar\sigma, \bar\sigma', \bar r$*.*

Soluzione (bozza).

1)

$$\frac{}{\langle \mathsf{return}\ ,\ \sigma\rangle \to_b \langle \sigma\ ,\ \mathsf{ret}\rangle}[\mathit{Return}]$$

2)

$$\frac{\langle c_1\ ,\ \sigma\rangle \to_b \langle \sigma'\ ,\ \mathsf{ret}\rangle}{\langle c_1; c_2\ ,\ \sigma\rangle \to_b \langle \sigma'\ ,\ \mathsf{ret}\rangle}[\mathit{CompRet}]$$

$$\frac{\langle c_1\ ,\ \sigma\rangle \to_b \langle \sigma'\ ,\ \mathsf{norm}\rangle \qquad \langle c_2\ ,\ \sigma'\rangle \to_b \langle \sigma''\ ,\ r\rangle}{\langle c_1; c_2\ ,\ \sigma\rangle \to_b \langle \sigma''\ ,\ r\rangle}[\mathit{CompNorm}]$$

3)

$$\frac{\langle c, \sigma\rangle \to_b \langle \sigma', r\rangle}{\langle \mathsf{block}\ c\ ,\ \sigma\rangle \to_b \langle \sigma'\ ,\ \mathsf{norm}\rangle}[\mathit{Block}]$$

4) Per ipotesi abbiamo che $\langle c_{\mathsf{b}}, \sigma\rangle \to_b \langle \sigma', r\rangle$. dove $c_{\mathsf{b}} = c_1; c_2; c_4$. Una derivazione può essere della forma (caso 1)

$$\frac{\dfrac{D}{\langle c_1, \sigma\rangle \to_b \langle \sigma', \mathsf{ret}\rangle}}{\langle c_{\mathsf{b}}, \sigma\rangle \to_b \langle \sigma', r = \mathsf{ret}\rangle}[\mathit{CompRet}]$$

oppure della forma (caso 2)

$$\frac{\dfrac{D_1}{\langle c_1, \sigma\rangle \to_b \langle \sigma'', \mathsf{norm}\rangle} \qquad \dfrac{\dfrac{D_2}{\langle c_2, \sigma''\rangle \to_b \langle \sigma''', \mathsf{norm}\rangle} \quad \dfrac{D_3}{\langle c_4, \sigma'''\rangle \to_b \langle \sigma', r\rangle}}{\langle c_2; c_4, \sigma''\rangle \to_b \langle \sigma', r\rangle}[\mathit{CompNorm}]}{\langle c_{\mathsf{b}}, \sigma\rangle \to_b \langle \sigma', r\rangle}[\mathit{CompNorm}]$$

Non ci sono altri casi perché c_2 può solo terminare con norm, per ipotesi. In ogni caso sopra, costruiamo una derivazione per c_{a}.

Caso 1.

$$\frac{\dfrac{D}{\langle c_1, \sigma\rangle \to_b \langle \sigma', \mathsf{ret}\rangle}}{\langle c_{\mathsf{a}}, \sigma\rangle \to_b \langle \sigma', r = \mathsf{ret}\rangle}[\mathit{CompRet}]$$

dove D è quella ricavata sopra. (Qui la parte $\mathsf{block}\ (c_2;\ \mathsf{return};\ c_3);\ c_4$ non viene proprio raggiunta.)

Caso 2. Sia $c = (c_2;\ \mathsf{return};\ c_3)$ e $c' = \mathsf{block}\ c;\ c_4$. Si ha $c_{\mathsf{a}} = (c_1; c')$.

$$\frac{\dfrac{D_1}{\langle c_1, \sigma\rangle \to_b \langle \sigma'', \mathsf{norm}\rangle} \qquad \dfrac{\dfrac{D'}{\langle \mathsf{block}\ c\ , \sigma''\rangle \to_b \langle \sigma''', \mathsf{norm}\rangle} \quad \dfrac{D_3}{\langle c_4, \sigma'''\rangle \to_b \langle \sigma', r\rangle}}{\langle c', \sigma''\rangle \to_b \langle \sigma', r\rangle}[\mathit{CompNorm}]}{\langle c_{\mathsf{a}}, \sigma\rangle \to_b \langle \sigma', r\rangle}[\mathit{CompNorm}]$$

dove D_1, D_3 sono quelle ricavate sopra, mentre D' è

$$\cfrac{\cfrac{D_2}{\langle c_2\ , \sigma''\rangle \to_b \langle \sigma''', \mathsf{norm}\rangle} \qquad \cfrac{\cfrac{}{\langle \mathsf{return}\ , \sigma'''\rangle \to_b \langle \sigma''', \mathsf{ret}\rangle}[Return]}{\langle \mathsf{return}; c_3\ , \sigma'''\rangle \to_b \langle \sigma''', \mathsf{ret}\rangle}[CompRet]}{\cfrac{\langle c\ , \sigma''\rangle \to_b \langle \sigma''', \mathsf{ret}\rangle}{\langle \mathsf{block}\ c\ , \sigma''\rangle \to_b \langle \sigma''', \mathsf{norm}\rangle}[Block]}[CompNorm]$$

dove D_2 è quella ricavata sopra.

$\square$

Nome ______________________________ Matricola ____________

Esercizio 4. *Si dimostri formalmente la validità della tripla di Hoare seguente riempiendo le linee sottostanti con opportune asserzioni.*

$\{n \ \mathit{dispari} \ \leq -10\}$

____

while $n < 0$ do

____

____

if $n = -4$ then

____

____

$n := n + 1$

else

____

____

$n := n + 2$

____

____

$\{n \geq 1\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

Soluzione (bozza).

$$
\begin{array}{l}
\{n \text{ dispari } \ \leq -10\} \\
\{INV : n \text{ dispari}\} \qquad (1) \\
\textsf{while } n < 0 \textsf{ do} \\
\quad \{INV \wedge n < 0\} \\
\quad \{n \text{ dispari}\} \qquad (2) \\
\quad \textsf{if } n = -4 \textsf{ then} \\
\quad\quad \{n \text{ dispari} \wedge n = -4\} \\
\quad\quad \{n + 1 \text{ dispari}\} \qquad (3) \\
\quad\quad n := n + 1 \\
\quad \textsf{else} \\
\quad\quad \{n \text{ dispari} \wedge \neg(n = -4)\} \\
\quad\quad \{n + 2 \text{ dispari}\} \qquad (4) \\
\quad\quad n := n + 2 \\
\quad \{INV\} \\
\{INV \wedge \neg(n < 0)\} \\
\{n \geq 1\} \qquad (5)
\end{array}
$$

Per le PrePost:

1) Banale.

2) Banale.

3) Dall'ipotesi si ricava un assurdo, visto che -4 non è dispari, quindi la tesi è implicata.

4) Se n è dispari, chiaramente anche $n + 2$ lo è.

5) Sappiamo che $n \geq 0$ e che n è dispari, quindi non è 0, da cui $n \geq 1$.

□