Informatica — 2016-09-09

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

Esercizio 1. *Si forniscano le regole della semantica "big step" di IMP, senza commentarle.*

Esercizio 2. *Si considerino le regole di inferenza:*

$$\frac{}{\epsilon}[S0] \qquad \frac{s}{x : s}(x \in \mathbb{Z})[S1] \qquad \frac{}{\epsilon\ R\ \epsilon}[R0] \qquad \frac{s\ R\ s'}{(x : s)\ R\ (5 - x : s')}[R1]$$

Sopra, con x indichiamo un intero. Con s, s' indichiamo sequenze di interi, il cui insieme S è definito (induttivamente) da $[S0, S1]$. La relazione $R \in \mathcal{P}(S \times S)$ è definita ricorsivamente da $[R0, R1]$.

1. *[20%] Si enunci il principio di induzione su S.*
2. *[80%] Data la seguente proprietà p sulle sequenze $s \in S$*

$$p(s) : \qquad \forall s_1, s_2.\ s\ R\ s_1\ \wedge\ s_1\ R\ s_2\ \Longrightarrow\ s = s_2$$

si dimostri $\forall s \in S.\ p(s)$ per induzione su s.

Soluzione (bozza).

Parte 1. Se valgono
1) $p(\epsilon)$
2) $\forall s, x \in \mathbb{Z}.p(s)\ \Longrightarrow\ p(x : s)$
allora vale $\forall s \in S.\ p(s)$.

Parte 2. Caso $[S0]$**.**

Bisogna dimostrare $p(\epsilon)$, ovvero

$$\forall s_1, s_2.\ \epsilon\ R\ s_1\ \wedge\ s_1\ R\ s_2\ \Longrightarrow\ \epsilon = s_2$$

Assumiamo $IP1 : \epsilon\ R\ s_1$ e $IP2 : s_1\ R\ s_2$, e dimostriamo $\epsilon = s_2$.

Invertendo $IP1$, osserviamo che può essere ricavato solo da $[R0]$, e quindi $s_1 = \epsilon$.

Invertendo $IP2 : s_1 = \epsilon\ R\ s_2$, come sopra, otteniamo $s_2 = \epsilon$ da cui la tesi.

Caso $[S1]$**.**

Per ipotesi induttiva assumiamo $p(s)$, ovvero:

$$IP1 : \qquad \forall s_1, s_2.\ s\ R\ s_1\ \wedge\ s_1\ R\ s_2\ \Longrightarrow\ s = s_2$$

e dimostriamo $p(x : s)$, ovvero:

$$\forall z_1, z_2.\ x : s\ R\ z_1\ \wedge\ z_1\ R\ z_2\ \Longrightarrow\ n : s = z_2$$

Assumiamo quindi $IP2 : (x : s)\ R\ z_1$ e $IP3 : z_1\ R\ z_2$, e dimostriamo la tesi $(x : s) = z_2$.

Invertendo $IP2$, osserviamo che può essere ricavato solo da $[R1]$, da cui otteniamo $IP4 : sRs'$, $IP5 : z_1 = (5 - x : s')$.

Invertendo $IP3 : z_1 = (5 - x : s')\ R\ z_2$, osserviamo che può essere ricavato solo da $[R1]$, da cui otteniamo $IP6 : s'Rs''$, $IP7 : z_2 = (5-(5-x) : s'') = (x : s'')$.

Da $IP1$, scegliendo $s_1 = s'$ e $s_2 = s''$ si ha

$$s\ R\ s'\ \wedge\ s'\ R\ s''\implies s = s''$$

L'antecedente segue da $IP4$ e da $IP6$, quindi otteniamo $s = s''$. Da questo segue la tesi in quanto $(x : s) = (x : s'') = z_2$ per $IP7$.

□

Esercizio 3. *Sia σ_0 lo stato che associa ad ogni variabile il valore 0, e sia c il comando seguente:*

$$c = \quad (\mathsf{while}\ x + 1 \neq 0\ \mathsf{do}\ x := x + 1)$$

Si dimostri formalmente che vale la proprietà

$$P : \qquad \nexists \sigma'.\ \langle c, \sigma_0\rangle \to_b \sigma'$$

seguendo la traccia seguente:

1. *[25%] Si definiscano due asserzioni Q, R in modo che la validità della tripla di Hoare $\{Q\}\ c\ \{R\}$ implichi la proprietà P di sopra.*
2. *[45%] Si dimostri che se $\{Q\}\ c\ \{R\}$ è valida, allora P vale.*
3. *[30%] Si dimostri la validità di $\{Q\}\ c\ \{R\}$.*

Soluzione (bozza).
Parte 1. Scegliamo $Q : x \geq 0$ e $R : \mathsf{false}$.
Parte 2. Supponiamo che sia valida $\{x \geq 0\}\ c\ \{\mathsf{false}\}$ e che quindi

$$\forall \sigma, \sigma'.\ \sigma \models (x \geq 0) \wedge \langle c, \sigma\rangle \to \sigma' \implies \sigma' \models \mathsf{false}$$

Si nota che $\sigma \models (x \geq 0)$ è equivalente a $\sigma(x) \geq 0$, mentre $\sigma' \models \mathsf{false}$ è equivalente a false (infatti nessuno stato σ' può rendere vera l'asserzione false). Riscriviamo il tutto come:

$$IP1 : \qquad \forall \bar\sigma, \bar\sigma'.\ \bar\sigma(x) \geq 0 \wedge \langle c, \bar\sigma\rangle \to_b \bar\sigma' \implies \mathsf{false}$$

Per dimostrare P, assumiamo per assurdo che esista un σ' tale che $IP2 : \langle c, \sigma_0\rangle \to_b \sigma'$, e ricaviamo un assurdo. Infatti, da $IP1$, scegliendo $\bar\sigma = \sigma_0$ e $\bar\sigma' = \sigma'$, si ha

$$\sigma_0(x) \geq 0 \wedge \langle c, \sigma_0\rangle \to_b \sigma' \implies \mathsf{false}$$

L'antecedente segue da $\sigma_0(y) = 0$ (per ogni $y \in Var$) e da $IP2$, per cui otteniamo il conseguente false, l'assurdo cercato.

Parte 3.

$$
\begin{array}{l}
\{Q : x \geq 0\} \\
\{INV : x \geq 0\}\ (1) \\
\mathsf{while}\ x + 1 \neq 0\ \mathsf{do} \\
\qquad \{INV\ \wedge\ x + 1 \neq 0\} \\
\qquad \{x + 1 \geq 0\}\ (2) \\
\qquad x := x + 1 \\
\{INV\ \wedge\ \neg(x + 1 \neq 0)\} \\
\{R : \mathsf{false}\}\ (3)
\end{array}
$$

La PrePost (1) è banale. Per la (2), dall'invariante $x \geq 0$ si ha $x+1 \geq 0$. Per la (3), da $x+1 = 0$ si ricava $x = -1$ che contraddice l'invariante $x \geq 0$, da cui la tesi false.

□

Nome _____ Matricola _____

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

$\{x = 2^K\}$

_____

$n := 1;$

_____

$y := 0;$

_____

while $n \neq x$ do

_____

_____

$n := n * 2;$

_____

$y := y + 1;$

_____

$\{y = K\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Soluzione (bozza).

$\{x = 2^K\}$
$\{1 = 2^0 \wedge x = 2^K\}$ (1)
$n := 1;$
$\{n = 2^0 \wedge x = 2^K\}$
$y := 0;$
$\{INV : \ n = 2^y \wedge x = 2^K\}$
while $n \neq x$ do
    $\{INV \wedge n \neq y\}$
    $\{n * 2 = 2^{(y+1)} \wedge x = 2^K\}$ (2)
    $n := n * 2;$
    $\{n = 2^{(y+1)} \wedge x = 2^K\}$
    $y := y + 1;$
$\{INV \wedge \neg(n \neq x)\}$
$\{y = K\}$ (3)

Per le PrePost:
La (1) è banale aritmetica.
Per la (2), da $n = 2^y$ segue $n * 2 = 2^{(y+1)}$, mentre $x = 2^K$ è in INV.
Per la (3), abbiamo $n = x$ e quindi da INV $2^y = 2^K$ da cui $y = K$.

□