Informatica — 2015-07-13

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

Esercizio 1. *Si enuncino, senza dimostrarli o commentarli, i quattro risultati relativi alla (non-)totalità e al (non-)determinismo della semantica delle espressioni ($\to_e$) e dei comandi ($\to_b$).*

Esercizio 2. *Sia U un insieme e $\mathcal{R} \subseteq \mathcal{P}^{fin}(U) \times U$ un insieme di regole di inferenza su U. Sia inoltre $\mathcal{R}' = \mathcal{R} \cup \left\{ \dfrac{x}{x} \;\middle|\; x \in U \right\}$.*

1. *[90%] Si dimostrino le seguenti, giustificando tutti i passaggi:*

a) $\forall X \subseteq U.\ \hat{\mathcal{R}}'(X) = \hat{\mathcal{R}}(X) \cup X$ *b)* $\forall i \in \mathbb{N}.\ \hat{\mathcal{R}}^i(\emptyset) = \hat{\mathcal{R}}'^{\,i}(\emptyset)$

2. *[10%] Si dimostri quindi che $fix(\hat{\mathcal{R}}) = fix(\hat{\mathcal{R}}')$, dove fix indica il minimo punto fisso.*

Soluzione (bozza).

Parte 1a Per l'inclusione $\supseteq$, sia $y \in \hat{\mathcal{R}}(X) \cup X$. Se $y \in \hat{\mathcal{R}}(X)$ deve esistere una regola in $\mathcal{R}$ con premesse in X e conseguenza y. La stessa regola è anche in $\mathcal{R}'$, quindi $y \in \hat{\mathcal{R}}'(X)$. Se invece $y \in X$, in $\mathcal{R}'$ troviamo la regola y/y e quindi possiamo comunque concludere $y \in \hat{\mathcal{R}}'(X)$.

Per l'inclusione $\subseteq$, sia $y \in \hat{\mathcal{R}}'(X)$. Deve quindi esistere una regola in $\mathcal{R}'$ con premesse in X e conseguenza y. Tale regola è in $\mathcal{R}$ oppure della forma y/y. Nel primo caso abbiamo che $y \in \hat{\mathcal{R}}(X)$, nel secondo che $y \in X$. In ogni caso, $y \in \hat{\mathcal{R}}(X) \cup X$.

Parte 1b Per induzione su i. Se $i = 0$ abbiamo banalmente $\hat{\mathcal{R}}^0(\emptyset) = \emptyset = \hat{\mathcal{R}}'^0(\emptyset)$. Supponendo l'equazione vera per i, la verifichiamo per $i+1$:

$$
\begin{array}{lll}
 & \hat{\mathcal{R}}'^{i+1}(\emptyset) & \\
= & \hat{\mathcal{R}}'(\hat{\mathcal{R}}'^{i}(\emptyset)) & \\
= & \hat{\mathcal{R}}'(\hat{\mathcal{R}}^{i}(\emptyset)) & \text{ip. induttiva} \\
= & \hat{\mathcal{R}}(\hat{\mathcal{R}}^{i}(\emptyset)) \cup \hat{\mathcal{R}}^{i}(\emptyset) & \text{proprietà (a)} \\
= & \hat{\mathcal{R}}^{i+1}(\emptyset) \cup \hat{\mathcal{R}}^{i}(\emptyset) & \\
= & \hat{\mathcal{R}}^{i+1}(\emptyset) & \hat{\mathcal{R}}^{i}(\emptyset) \text{ è una sequenza crescente}
\end{array}
$$

Parte 2 Per il teorema del punto fisso di Kleene, basta dimostare che

$$\bigcup_i \hat{\mathcal{R}}^i(\emptyset) = \bigcup_i \hat{\mathcal{R}}'^i(\emptyset)$$

ma per la parte (1b) abbiamo $\hat{\mathcal{R}}^i(\emptyset) = \hat{\mathcal{R}}'^i(\emptyset)$ da cui la tesi segue immediatamente.

□

Esercizio 3. *Si dimostri la validità della tripla di Hoare seguente*

$$\{n \geq 0\}\ w\ \{n = 0\} \qquad \textit{dove } w = (\mathsf{while}\ n \cdot (n+7) \neq 0\ \mathsf{do}\ n := n - 1)$$

<u>senza</u> usare il teorema di correttezza, ma seguendo la traccia sottostante.

1. *[10%] Si fornisca la definizione di validità per una tripla di Hoare, senza commentarla.*

2. *[10%] Assumendo $(\to_b) \subseteq p$, si dimostri la validità della tripla, dove p è la proprietà/relazione*

$$p(c,\sigma,\sigma'): \begin{array}{lll} (c = w \ \wedge\ \sigma(n) \geq 0 & \implies & \sigma'(n) = 0) \ \wedge \\ (c = (n := n-1; w) \ \wedge\ \sigma(n) > 0 & \implies & \sigma'(n) = 0) \ \wedge \\ (c = n := n-1 \ \wedge\ \sigma(n) > 0 & \implies & \sigma'(n) \geq 0) \end{array}$$

3. *[60%] Si dimostri che $(\to_b) \subseteq p$ per induzione. Esaminare solo i casi $[While - True]$ e $[Comp]$, evidenziando bene dove si usano le varie ipotesi. Suggerimento: in ogni caso, al massimo una delle tre clausole di p è non banale.*

4. *[20%] Esaminare tutti gli altri casi. Identificare i tre casi banali come tali, e svolgere i rimanenti due. (Non dimenticatevi il suggerimento di sopra)*

Soluzione (bozza).

Parte 1 e 2 Per la definizione di validità, la tripla $\{P\}\ c\ \{Q\}$ è valida sse per ogni σ, σ'

$$\sigma \models P \wedge \langle c, \sigma\rangle \to_b \sigma' \implies \sigma' \models Q$$

Assumiamo $(\to_b) \subseteq p$ e dimostriamo la formula di sopra nel caso proposto. Supponiamo quindi $\sigma \models n \geq 0$ (cioè che $\sigma(n) \geq 0$) e che $\langle w, \sigma\rangle \to_b \sigma'$, ed andiamo a dimostrare $\sigma' \models n = 0$ (cioè $\sigma'(n) = 0$).

Da $\langle w, \sigma\rangle \to_b \sigma'$, e da $(\to_b) \subseteq p$ si ricava $p(w, \sigma, \sigma')$, da cui prendiamo la prima clausola:

$$w = w \ \wedge\ \sigma(n) \geq 0 \implies \sigma'(n) = 0$$

Siccome $w = w$ vale banalmente, e $\sigma(n) \geq 0$ è un'ipotesi, otteniamo $\sigma'(n) = 0$ che è proprio la tesi.

Parti 3 e 4 I casi $[If-True], [If-False], [Skip]$ sono banali in quanto le condizioni $c = w, c = (n := n-1; w), c = n := n-1$ diventano false su if e skip, quindi p è banalmente vera. Esaminiamo gli altri casi.

Let Bisogna dimostrare $p(x := e, \sigma, \sigma[x \mapsto v])$ supponendo $\langle e, \sigma\rangle \to_e v$. Sia $c = x := e$, e $\sigma' = \sigma[x \mapsto v]$.

L'unica clausola rilevante di $p(x := e, \sigma, \sigma[x \mapsto v])$ è

$$x := e = n := n-1 \ \wedge \ \sigma(n) > 0 \implies \sigma[x \mapsto v](n) \geq 0$$

visto che le altre sono implicazioni con premesse false, e quindi banalmente vere. Sia $\sigma' = \sigma[x \mapsto v]$.

Assumiamo $x := e = n := n-1 \ \wedge \ \sigma(n) > 0$. Se ne deriva $x = n$ ed $e = n-1$, da cui $\sigma'(n) = v$. Invertendo $\langle n-1, \sigma\rangle \to_e v$ è immediato vedere che $v = \sigma(n) - 1$. Quindi resta da verificare che

$$\sigma(n) > 0 \implies \sigma(n) - 1 \geq 0$$

Siccome si lavora sui numeri interi, l'implicazione vale.

Comp Bisogna dimostrare $p(c_1; c_2, \sigma, \sigma')$ supponendo come ipotesi induttive $p(c_1, \sigma, \sigma'')$ e $p(c_2, \sigma'', \sigma')$.

L'unica clausola non banale di $p(c_1; c_2, \sigma, \sigma')$ è

$$c_1; c_2 = (n := n-1; w) \ \wedge \ \sigma(n) > 0 \implies \sigma'(n) = 0$$

Assumendo $(c_1; c_2) = (n := n-1; w) \ \wedge \ \sigma(n) \geq 0$, abbiamo che $c_1 = n := n-1$, e $c_2 = w$. Da $\sigma(n) > 0$ e $p(c_1 = n := n-1, \sigma, \sigma'')$ ricaviamo $\sigma''(n) \geq 0$. Da $\sigma''(n) \geq 0$ e $p(c_2 = w, \sigma'', \sigma')$ ricaviamo $\sigma'(n) = 0$, che è la tesi.

While-True Sia $w' =$ while $e \neq 0$ do c'. Bisogna dimostrare $p(w', \sigma, \sigma')$ supponendo come ipotesi induttiva $p(c'; w', \sigma, \sigma')$ e come condizione a lato $\langle e, \sigma\rangle \to_e v \neq 0$. Sia $c = w'$.

L'unica clausola non banale di $p(w', \sigma, \sigma')$ è

$$w' = w \ \wedge \ \sigma(n) \geq 0 \implies \sigma'(n) = 0$$

Assumiamo $w' = w$ e $\sigma(n) \geq 0$, da cui $e = n \cdot (n+7)$ e $c' = n := n-1$. Dalla condizione a lato $\langle n \cdot (n+7), \sigma\rangle \to_e v \neq 0$ è facile ricavare per inversione ed aritmetica che $\sigma(n) \neq 0$, e quindi con l'ipotesi $\sigma(n) \geq 0$ si conclude $\sigma(n) > 0$.

Siccome, $c'; w' = n := n-1; w$ e $\sigma(n) > 0$, possiamo usare la seconda clausola di $p(c'; w', \sigma, \sigma')$ per dedurre $\sigma'(n) = 0$, che è la tesi.

While-False Sia $w' = \mathsf{while}\ e \neq 0\ \mathsf{do}\ c'$. Bisogna dimostrare $p(w', \sigma, \sigma)$ supponendo che $\langle e, \sigma\rangle \to_e 0$. Sia $c = w'$ e $\sigma' = \sigma$.

L'unica clausola non banale di $p(w', \sigma, \sigma)$ è

$$w' = w \ \wedge\ \sigma(n) \geq 0 \implies \sigma(n) = 0$$

Assumiamo $w' = w$ e $\sigma(n) \geq 0$, da cui $e = n \cdot (n + 7)$ e $c' = n := n - 1$. Dall'ipotesi $\langle n \cdot (n + 7), \sigma\rangle \to_e 0$ è facile vedere che $\sigma(n) = 0 \vee \sigma(n) = -7$. Visto che $\sigma(n) \geq 0$, deve essere $\sigma(n) = 0$, che è la tesi.

□

Nome _____ Matricola _____

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

$\{n \geq 0\}$

_____

$x := n;$

_____

$y := 0;$

_____

while $x > 0$ do

_____

_____

$y := y + 2;$

_____

$x := x - 1$

_____

$\{y = 2n\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

_____

_____

_____

_____

_____

_____

Soluzione (bozza).

$\{n \geq 0\}$
$\{0 + 2n = 2n \wedge n \geq 0\}$ (1)
$x := n;$
$\{0 + 2x = 2n \wedge x \geq 0\}$
$y := 0;$
$\{INV : y + 2x = 2n \wedge x \geq 0\}$
while $x > 0$ do
    $\{INV \wedge x > 0\}$
    $\{(y + 2) + 2(x - 1) = 2n \wedge x - 1 \geq 0\}$ (2)
    $y := y + 2;$
    $\{y + 2(x - 1) = 2n \wedge x - 1 \geq 0\}$
    $x := x - 1$
$\{INV \wedge \neg(x > 0)\}$
$\{y = 2n\}$ (3)

Per le PrePost:
1) banale.
2) l'equazione segue da INV e un po' di aritmetica, mentre $x - 1 \geq 0$, ovvero $x \geq 1$, segue da $x > 0$ e dal fatto che si lavora su interi.
3) dalle ipotesi si ricava $x = 0$, da cui $y = 2n$.

□