Informatica — 2017-06-27

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

Esercizio 1. *Si forniscano, senza commentarle, tutte le regole della semantica big-step di IMP. In tali regole, σ rappresenta un elemento arbitrario di un certo insieme. Si definisca tale insieme, e si descriva molto brevemente (∼2 righe) cosa rappresenta σ nella definizione della semantica.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi binari di numeri naturali (regole $[T0], [T1]$), una relazione tra alberi $R \in \mathcal{P}(T \times T)$ (regole $[R0], [R1]$), una relazione tra alberi e naturali $S \in \mathcal{P}(T \times \mathbb{N})$ (regole $[S0], [S1]$), Sotto, n, m indicano naturali mentre $l, \hat{l}, r, t, u$ indicano alberi.*

$$\frac{}{n}(n \in \mathbb{N})[T0] \qquad \frac{l \quad r}{(l,r)}[T1] \qquad \frac{}{R(n, n+1)}[R0] \qquad \frac{R(l,\hat{l})}{R((l,r),(\hat{l},r))}[R1]$$

$$\frac{}{S(n,n)}[S0] \qquad \frac{S(l,n) \qquad S(r,m)}{S((l,r), n+m)}[S1]$$

1. *[20%] Si trovi $t \in T$ tale che $R(((1,2),(3,4)), t)$, mostrando una derivazione.*

2. *[20%] Si trovi $n \in \mathbb{N}$ tale che $S((1,((2,3),4)), n)$, mostrando una derivazione.*

3. *[20%] Si enunci il principio di induzione su R.*

4. *[40%] Si dimostri che*

$$\forall t, u \in T.\ \forall n \in \mathbb{N}.\ R(t,u) \land S(t,n) \implies S(u, n+1)$$

(Suggerimento: si proceda per induzione su $R(t,u)$.)

Soluzione (bozza). Parte 1.

$$\dfrac{\dfrac{\dfrac{}{R(1,2)}}{R((1,2),(2,2))}}{R(((1,2),(3,4)),((2,2),(3,4)))}$$

Parte 2.

$$\dfrac{\dfrac{}{S(1,1)} \quad \dfrac{\dfrac{\dfrac{}{S(2,2)} \quad \dfrac{}{S(3,3)}}{S((2,3),2+3=5)} \quad \dfrac{}{S(4,4)}}{S(((2,3),4),5+4=9)}}{S((1,((2,3),4)),1+9=10)}$$

Parte 3. Per dimostrare

$$\forall t, u \in T.\ R(t,u) \implies p(t,u)$$

è sufficiente verificare che

$$\begin{array}{ll} R0) & \forall n \in \mathbb{N}. p(n, n+1) \\ R1) & \forall l, \hat{l} \in T.\ p(l,\hat{l}) \implies p((l,r),(\hat{l},r)) \end{array}$$

Parte 4.

Definiamo

$$p(t,u): \qquad \forall n \in \mathbb{N}.\ S(t,n) \implies S(u, n+1)$$

L'enunciato desiderato è equivalente a

$$\forall t, u \in T.\ R(t,u) \implies p(t,u)$$

Procediamo quindi per induzione su $R(t,u)$, seguendo il principio enunciato prima.

(Caso $R0$) Dobbiamo dimostrare $p(n, n+1)$, ovvero che

$$\forall m.\ S(n,m) \implies S(n+1, m+1)$$

(Si noti come abbiamo rinominato $\forall n$ in $\forall m$ per evitare di confonderci con la variabile n in $p(n, n+1)$.)

Assumiamo $IP1 : S(n,m)$. Per inversione, questo si può solo ricavare tramite $[S0]$, da cui si ricava $n = m$.

La tesi diventa quindi $S(n+1, n+1)$, che segue da $[S0]$.

(Caso $R1$) Assumiamo l'ipotesi induttiva $IP1 : p(l,\hat{l})$, ovvero

$$IP1:\ \forall \bar{n} \in \mathbb{N}.\ S(l,\bar{n}) \implies S(\hat{l}, \bar{n}+1)$$

La tesi da dimostrare è invece

$$\forall n \in \mathbb{N}.\ S((l,r),n) \implies S((\hat{l},r), n+1)$$

Preso un n arbitrario, assumiamo l'antecedente $IP2 : S((l,r),n)$, e andiamo a dimostrare che $S((\hat{l},r), n+1)$.

Invertendo $IP2$, notiamo che può essere ricavata solo da $[S1]$, da cui ricaviamo che, per qualche $k, m \in \mathbb{N}$ si ha $IP3 : S(l,k)$, $IP4 : S(r,m)$ dove $IP5 : k + m = n$.

Da $IP1$, scegliendo $\bar{n} = k$, si ha

$$S(l,k) \implies S(\hat{l}, k+1)$$

Siccome l'antecedente vale per $IP3$, ricaviamo $IP6 : S(\hat{l}, k+1)$.

Da $IP6, IP4$, tramite la regola $[S1]$, otteniamo

$$S((\hat{l},r), k+1+m)$$

Da questo, usando $IP5$, otteniamo la tesi desiderata. $S((\hat{l},r), n+1)$

□

Esercizio 3. *Si considerino le seguenti proprietà sulla validità ($\models$) delle triple di Hoare.*

$$\begin{array}{lll} 1) & \models \{P_1\}\ c\ \{Q_1\} \wedge \models \{P_2\}\ c\ \{Q_2\} & \implies \models \{P_1 \wedge P_2\}\ c\ \{Q_1 \wedge Q_2\} \\ 2) & \models \{P_1\}\ c\ \{Q_1\} \vee \models \{P_2\}\ c\ \{Q_2\} & \implies \models \{P_1 \vee P_2\}\ c\ \{Q_1 \vee Q_2\} \end{array}$$

Si stabilisca quali delle proprietà sopra sono vere per ogni comando (c) e pre-/post-condizione (P_1, P_2, Q_1, Q_2). Si dimostrino quelle vere, e si fornisca un controesempio per le altre.
(Suggerimento: si sfrutti il fatto che $\sigma \models (P \wedge Q)$ è equivalente a $(\sigma \models P) \wedge (\sigma \models Q)$, mentre $\sigma \models (P \vee Q)$ è equivalente a $(\sigma \models P) \vee (\sigma \models Q)$.)

Soluzione (bozza).
(Parte 1) (Vera) Per ipotesi si ha, per ogni σ, σ',

$$\begin{array}{l} IP1: \ \sigma \models P_1 \wedge \langle c, \sigma\rangle \to_b \sigma' \implies \sigma \models Q_1 \\ IP2: \ \sigma \models P_2 \wedge \langle c, \sigma\rangle \to_b \sigma' \implies \sigma \models Q_2 \end{array}$$

Per dimostrare la tesi, assumiamo

$$\begin{array}{l} IP3: \ \sigma \models P_1 \wedge P_2 \\ IP4: \ \langle c, \sigma\rangle \to_b \sigma' \end{array}$$

e facciamo vedere che vale $\sigma' \models Q_1 \wedge Q_2$.

Da $IP3$ si ricava $\sigma \models P_1$, da cui usando $IP4, IP1$ otteniamo $IP5 : \sigma' \models Q_1$.

Analogamente, da $IP3$ si ricava $\sigma \models P_2$, da cui usando $IP4, IP2$ otteniamo $IP6 : \sigma' \models Q_2$.

Da $IP5, IP6$ otteniamo la tesi desiderata.

(Parte 2) (Falsa) Un possibile controesempio è dato da

$$\begin{array}{l} P_1 : x = 0 \\ c = (x := x + 1) \\ Q_1 : x = 1 \\ P_2 : \mathsf{vero} \\ Q_2 : \mathsf{falso} \end{array}$$

La tripla $\{x = 0\}\ x := x + 1\ \{x = 1\}$ è valida: per dimostrarlo possiamo sfruttare il teorema di correttezza e usare il sistema deduttivo per le triple. (La PrePost sotto è banale)

$$\begin{array}{l} \{x = 0\} \\ \{x + 1 = 1\} \\ x := x + 1 \\ \{x = 1\} \end{array}$$

Di conseguenza, l'antecedente

$$\models \{P_1\}\ c\ \{Q_1\} \vee \models \{P_2\}\ c\ \{Q_2\}$$

vale, siccome la parte sinistra è vera. Tuttavia, la conseguente

$$\models \{P_1 \vee P_2\}\ c\ \{Q_1 \vee Q_2\}$$

non vale. Essa è equivalente a

$$\models \{x = 0 \vee \mathsf{vero}\}\ \mathsf{x} := \mathsf{x} + 1\ \{\mathsf{x} = 1 \vee \mathsf{falso}\}$$

e quindi a

$$\models \{\mathsf{vero}\}\ \mathsf{x} := \mathsf{x} + 1\ \{\mathsf{x} = 1\}$$

che afferma che, da qualunque stato iniziale σ, dopo $x := x + 1$, lo stato finale σ' deve attribuire a x il valore 1. Questo è falso, come si vede prendendo, per esempio, lo stato iniziale σ dove tutte le variabili (tra cui x) valgono 2, in modo che $\sigma'(x) = 3 \neq 1$.

□

Nome _____ Matricola _____

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

$\{a = A \geq 0\}$

_____

$x := a;$

_____

$y := 0;$

_____

while $x > 0$ do

_____

_____

$x := x - 1;$

_____

$y := y + 1$

_____

$\{y = A\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Soluzione (bozza).

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

Per le PrePost:

1) Banale aritmetica.

2) L'ipotesi $x > 0$, siccome lavoriamo sugli interi, implica $x \geq 1$, da cui la tesi $x - 1 \geq 0$. La tesi $(x - 1) + (y + 1) = A$ deriva direttamente dall'equazione in INV.

3) Per ipotesi, abbiamo $x \geq 0$ e $\neg(x > 0)$, da cui $x = 0$. Siccome per INV si ha che $x + y = A$, allora $0 + y = A$ da cui la tesi $y = A$.

□