Informatica — 2019-06-24

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

Esercizio 1. *Si forniscano le regole della semantica delle espressioni di IMP, e si enunci il risultato di determinismo per tale semantica.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi binari di numeri naturali (regole $[T0], [T1]$), una relazione $R \in \mathcal{P}(T \times \mathbb{N})$ (regole $[R0], [R1]$) e una relazione $Q \in \mathcal{P}(T \times T)$ (regole $[Q0], [Q1]$). Sotto, n, m indicano naturali mentre l, r, t e analoghi indicano alberi in T.*

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

$$\frac{}{Q(n, n+1)}[Q0] \qquad \frac{Q(t_1, t_1') \qquad Q(t_2, t_2') \qquad Q(t_3, t_3')}{Q((t_1, (t_2, t_3)), ((t_1', t_2'), t_3'))}[Q1]$$

1. *[20%] Si fornisca un albero $t \in T$ per cui valga $Q((1, ((2, (3, 4)), 5))\ ,\ t)$ e si giustifichi la risposta esibendo una derivazione.*

2. *[20%] Si enunci il principio di induzione associato alla relazione Q.*

3. *[10%] Si consideri l'enunciato seguente:*

$$\forall t, t' \in T, k \in \mathbb{N}.\ R(t,k) \land Q(t,t') \implies R(t',k)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t, t' \in T.\ Q(t,t') \implies p(t,t')$$

   per un qualche predicato p.

4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a Q.*

Soluzione (bozza).
Parte 1.

$$\frac{\dfrac{}{Q(1,2)} \qquad \dfrac{\dfrac{}{Q(2,3)} \qquad \dfrac{}{Q(3,4)} \qquad \dfrac{}{Q(4,5)}}{Q((2,(3,4)),((3,4),5))} \qquad \dfrac{}{Q(5,6)}}{Q(\ (1,((2,(3,4)),5))\ ,\ ((2,((3,4),5)),6)\ )}$$

Parte 2. Sia $p(-,-)$ una proprietà su due alberi. Per dimostrare che, per ogni t, t' alberi che soddisfano $Q(t,t')$ vale che $p(t,t')$ è sufficiente verificare che:

$Q0)$ $\forall n \in \mathbb{N}.\ p(n, n+1)$
$Q1)$ $\forall t_1, t_2, t_3, t_1', t_2', t_3'.\ p(t_1,t_1') \land p(t_2,t_2') \land p(t_3,t_3') \implies p((t_1,(t_2,t_3)),((t_1',t_2'),t_3')))$

Parte 3. L'enunciato

$$\forall t, t' \in S, k \in \mathbb{N}.\ R(t,k) \land Q(t,t') \implies R(t',k)$$

si riscrive equivalentemente come

$$\forall t, t' \in S, k \in \mathbb{N}.\ Q(t,t') \land R(t,k) \implies R(t',k)$$

che si riscrive equivalentemente come

$$\forall t, t' \in S.\ Q(t,t') \implies (\forall k \in \mathbb{N}.\ R(t,k) \implies R(t',k))$$

Quindi basta definire $p(t, t')$ come

$$\forall k \in \mathbb{N}.\ R(t, k) \implies R(t', k)$$

Parte 4.

Procediamo quindi per induzione.

Caso Q0.

Non ci sono ipotesi induttive. Dobbiamo dimostrare $p(n, n+1)$ ovvero $\forall k.\ R(n, k) \implies R(n+1, k)$.

Assumiamo $IP1 : R(n, k)$ e dimostriamo la nuova tesi $R(n+1, k)$.

Invertendo $IP1$, siccome può essere derivata solo da $R0$, abbiamo $k = 1$. La tesi diventa quindi $R(n+1, 1)$ che deriva da $R0$.

Caso Q1.

Per ipotesi induttive assumiamo $p(t_1, t'_1)$, $p(t_2, t'_2)$ e $p(t_3, t'_3)$, ovvero:

$$\begin{array}{ll} IP1: & \forall k_1. R(t_1, k_1) \implies R(t'_1, k_1) \\ IP2: & \forall k_2. R(t_2, k_2) \implies R(t'_2, k_2) \\ IP3: & \forall k_3. R(t_3, k_3) \implies R(t'_3, k_3) \end{array}$$

Dobbiamo dimostrare $p((t_1, (t_2, t_3)), ((t'_1, t'_2), t'_3)))$, cioè:

$$\forall k. R((t_1, (t_2, t_3)), k) \implies R(((t'_1, t'_2), t'_3)), k)$$

Assumiamo quindi

$$IP4: \ R((t_1, (t_2, t_3)), k)$$

e dimostriamo la tesi $R(((t'_1, t'_2), t'_3)), k)$.

Invertendo $IP4$, siccome può essere ricavata solo da $R1$, otteniamo che, per qualche $k_1, \bar{k}$ si ha:

$$\begin{array}{ll} IP5: & R(t_1, k_1) \\ IP6: & R((t_2, t_3), \bar{k}) \end{array}$$

dove $k_1 + \bar{k} = k$.

Analogamente, invertendo $IP6$, siccome può essere ricavata solo da $R1$, otteniamo che, per qualche k_2, k_3 si ha:

$$\begin{array}{ll} IP7: & R(t_2, k_2) \\ IP8: & R(t_3, k_3) \end{array}$$

dove $k_2 + k_3 = \bar{k}$. Di conseguenza, $k = k_1 + k_2 + k_3$.

Usiamo ora le ipotesi induttive:

Da $IP1$ (con $k_1 = k_1$) e $IP5$ si ha $IP9 : R(t'_1, k_1)$.

Da $IP2$ (con $k_2 = k_2$) e $IP7$ si ha $IP10 : R(t'_2, k_2)$.

Da $IP3$ (con $k_3 = k_3$) e $IP8$ si ha $IP11 : R(t'_3, k_3)$.

Sfruttando $IP9, IP10, IP11$, ricaviamo la tesi come segue:

$$\dfrac{\dfrac{R(t'_1, k_1) \qquad R(t'_2, k_2)}{R((t'_1, t'_2), k_1 + k_2)} \qquad R(t'_3, k_3)}{R(((t'_1, t'_2), t'_3), k_1 + k_2 + k_3 = k)}$$

□

Esercizio 3.

1. *[10%] Si consideri la proprietà $P(x, y, c)$ descritta informalmente da: "Supponiamo che, partendo da un certo stato, il comando c termini, e che alla fine la variabile y abbia un certo valore. Allora, anche partendo da un altro stato che differisce solo per il valore della variabile x, si otterrebbe comunque la terminazione e il valore di y alla*

fine sarebbe lo stesso.". Per esempio $P(x, y, y := 7)$ è vera, mentre $P(x, y, y := 7{+}x)$ è falsa.

Si forniscano tre insiemi A, B, C in modo che P, vista come relazione, soddisfi $P \in \mathcal{P}(A \times B \times C)$.

2. *[20%] Si definisca $P(x, y, c)$ rigorosamente tramite un'opportuna formula logica.*

3. *[70%] Si considerino gli asserti sottostanti. Per gli asserti veri, si fornisca una giustificazione informale per la loro validità. Per quelli falsi, si fornisca un controesempio.*

$$
\begin{array}{l}
A)\ \forall x, y.\ x \neq y \implies P(x, y, \mathsf{skip}) \\
B)\ \forall x, y, c_1, c_2.\ x \neq y \implies P(x, y, \mathsf{if}\ x \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c2) \\
C)\ \forall x, y, e.\ x \neq y \implies \neg P(x, y, \mathsf{while}\ e \neq 0\ \mathsf{do}\ y := x * x - 16)
\end{array}
$$

Soluzione (bozza).

Parte 1. $P \in \mathcal{P}(Var \times Var \times Com)$

Parte 2. $P(x, y, c)$ può essere definita come

$$\forall \sigma, \sigma'.\ \langle c, \sigma \rangle \to_b \sigma' \implies \forall v.\ \exists \sigma''.\ \langle c, \sigma[x \mapsto v] \rangle \to_b \sigma'' \wedge \sigma'(y) = \sigma''(y)$$

Parte 3. A) è vera, in quanto skip termina sempre e lascia il valore di y inalterato, qualunque sia il valore di x all'inizio.

B) è falsa, in quanto se eseguiamo

$$\mathsf{if}\ x \neq 0\ \mathsf{then}\ y := 1\ \mathsf{else}\ y := 2$$

il comando termina sempre, ma il valore finale di y è 2 se x all'inizio vale 0, altrimenti è 1.

Anche C) è falsa, in quanto se prendiamo $e = 0$, il comando

$$\mathsf{while}\ 0 \neq 0\ \mathsf{do}\ y := x * x - 16$$

diventa equivalente a skip e quindi soddisfa P.

(Alternativamente, prendere $e = 1$ non fa terminare mai il ciclo, e quindi P diventa vacuamente vera.)

$\square$

Nome ______________________________________ Matricola ______________

Esercizio 4. *Si dimostri formalmente la validità della tripla di Hoare seguente riempiendo le linee sottostanti con opportune asserzioni. Sotto, N è un naturale.*

$\{n = 2^N\}$

____

$x := 1;$

____

while $n > 1$ do

    ____

    ____

    $n := \lfloor n/2 \rfloor;$

    ____

    $x := x * 2$

____

$\{x = 2^N\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$$
\begin{array}{l}
\{n = 2^N\}\ (1) \\
\{n \cdot 1 = 2^N \wedge n \geq 1\} \\
x := 1; \\
\{INV : n \cdot x = 2^N \wedge n \geq 1\} \\
\textsf{while } n > 1 \textsf{ do} \\
\qquad \{INV \wedge n > 1\}\ (2) \\
\qquad \{\lfloor n/2 \rfloor \cdot (2x) = 2^N \wedge n \geq 1\} \\
\qquad n := \lfloor n/2 \rfloor; \\
\qquad \{n \cdot (2x) = 2^N \wedge n \geq 1\} \\
\qquad x := 2 * x \\
\{INV \wedge \neg(n > 1)\}\ (3) \\
\{x = 2^N\}
\end{array}
$$

Per le PrePost:

1) $n \cdot 1 = 2^N$ segue banalmente dall'ipotesi. Inoltre, siccome N è un naturale, si ha $n = 2^N \geq 1$.

2) Dalle ipotesi si ha $nx = 2^N$ e $n > 1$. Di qui, siccome x è un intero, segue che n deve essere potenza di 2. Inoltre non può essere 1 perché $n > 1$, quindi n è pari e $\lfloor n/2 \rfloor = n/2$. Possiamo quindi ottenere $\lfloor n/2 \rfloor \cdot (2x) = n/2 \cdot (2x) = nx = 2^N$. La tesi $n \geq 1$ segue banalmente da $n > 1$.

3) Per ipotesi $n \geq 1$ ma $\neg(n > 1)$, quindi $n = 1$. Da INV si ha quindi $x = nx = 2^N$ che è la tesi.

$\square$