Informatica — 2019-02-07

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

Esercizio 1. *Si enunci e dimostri il lemma del minimo punto fisso.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di numeri naturali (regole $[S0], [S1]$), una relazione $R \in \mathcal{P}(S \times S)$ (regole $[R0], [R1]$) e una relazione $Q \in \mathcal{P}(S \times S)$ (regole $[Q0], [Q1]$). Sotto, n, m indicano naturali mentre s, z indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \qquad \frac{s}{n : s}(n \in \mathbb{N})[S1] \qquad \frac{}{R(\epsilon, \epsilon)}[R0] \qquad \frac{R(s, z)}{R(n : m : s, m : n : z)}[R1]$$

$$\frac{}{Q(\epsilon, \epsilon)}[Q0] \qquad \frac{Q(s, z)}{Q(n : s, n : z)}[Q1]$$

1. *[20%] Si fornisca una sequenza $s \in S$ per cui valga $R(1 : 6 : 5 : 2 : \epsilon\ ,\ s)$ e si giustifichi la risposta esibendo una derivazione.*

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

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

   $$\forall s, z, w \in S.\ R(s, z) \land Q(z, w) \implies R(w, s)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall s, z \in S.\ R(s, z) \implies p(s, z)$$

   per un qualche predicato p.

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

Soluzione (bozza).
Parte 1.

$$\dfrac{\dfrac{\dfrac{}{R(\epsilon, \epsilon)}[R0]}{R(5 : 2 : \epsilon, 2 : 5 : \epsilon)}[R1]}{R(1 : 6 : 5 : 2 : \epsilon, 6 : 1 : 2 : 5 : \epsilon)}[R1]$$

Parte 2.
Per dimostrare che, per ogni s, z sequenze tali che $R(s, z)$ vale $p(s, z)$ è sufficiente verificare che:

$R0)$ $p(\epsilon, \epsilon)$
$R1)$ $\forall s, z \in S, n, m \in \mathbb{N}.\ p(s, z) \implies p(n : m : s, m : n : z)$

Parte 3.
L'enunciato si riscrive come

$$\forall s, z \in S.\ R(s, z) \implies (\forall w \in S.\ Q(z, w) \implies R(w, s))$$

quindi basta scegliere

$$p(s, z) :\ \forall w \in S.\ Q(z, w) \implies R(w, s)$$

Parte 4.
Procediamo per induzione su R.

Caso $[R0]$**.** Dobbiamo dimostrare $p(\epsilon, \epsilon)$, ovvero

$$\forall w.\ Q(\epsilon, w) \implies R(w, \epsilon)$$

Assumiamo $IP1 : Q(\epsilon, w)$ e dimostriamo la tesi $R(w, \epsilon)$.

Invertendo $IP1$, siccome solo $[Q0]$ può generarla, ricaviamo $w = \epsilon$. La tesi diventa quindi $R(\epsilon, \epsilon)$, che segue usando la regola $[R0]$.

Caso $[R1]$**.** Per ipotesi induttiva assumiamo $IP1 : p(s, z)$, ovvero

$$\forall \bar{w}.\ Q(s, \bar{w}) \implies R(\bar{w}, z)$$

Dobbiamo dimostrare $p(n : m : s, m : n : z)$, ovvero

$$\forall w.\ Q(n : m : s, w) \implies R(w, m : n : z)$$

Assumiamo quindi $IP2 : Q(n : m : s, w)$ e dimostriamo come nuova tesi $R(w, m : n : z)$.

Invertendo $IP2$, osserviamo che può essere generata solo da $[Q1]$ e quindi $w = n : w'$ e $IP3 : Q(m : s, w')$ per qualche w'.

Di nuovo, invertendo $IP3$, osserviamo che può essere generata solo da $[Q1]$ e quindi $w' = m : w''$ e $IP4 : Q(s, w'')$ per qualche w''.

Usiamo ora $IP1$ scegliendo $\bar{w} = w''$, e anche $IP4$: da questo si ricava $IP5 : R(w'', z)$. Di qui, possiamo usare la regola $[R1]$ per ottenere $R(n : m : w'', m : n : z)$ che è proprio la tesi $R(w, m : n : z)$.

□

Esercizio 3. *La semantica big step di IMP è una relazione* $(\to_b) \in \mathcal{P}(Com \times State \times State)$*, che associa ad un comando da eseguire* c *e a uno stato iniziale* σ *uno stato finale* σ'*.*

1. *[70%] Si definisca, adattando le regole di inferenza di* $(\to_b)$*, una variante di tale semantica* $(\Rightarrow_b) \in \mathcal{P}(Com \times State \times State \times \mathbb{N})$*, che associ a* c *e* σ *non solo* σ' *ma anche un naturale* $n \in \mathbb{N}$*, pari al numero degli assegnamenti che sono stati eseguiti durante l'esecuzione di* c *a partire da* σ*. Per esempio, se* σ *è lo stato dove tutte le variabili valgono* 0*, la semantica deve soddisfare le seguenti proprietà:*

   $A)$ $\langle x := x; (\mathsf{skip}; y := x), \sigma\rangle \Rightarrow_b \langle \sigma, 2\rangle$
   $B)$ $\langle \mathsf{if}\ x \neq 0\ \mathsf{then}\ x := 1\ \mathsf{else}\ (x := 3; y := 5), \sigma\rangle \Rightarrow_b \langle \sigma[x \mapsto 3, y \mapsto 5], 2\rangle$
   $C)$ $\langle \mathsf{while}\ x - 5 \neq 0\ \mathsf{do}\ x := x + 1, \sigma\rangle \Rightarrow_b \langle \sigma[x \mapsto 5], 5\rangle$

   (Si possono omettere le regole per il comando if*)*

2. *[30%] Si fornisca una derivazione per l'esempio* A*) mostrato sopra.*

Soluzione (bozza).
Parte 1.

$$\frac{}{\langle \mathsf{skip}, \sigma\rangle \Rightarrow_b \langle \sigma, 0\rangle}[Skip]$$

$$\frac{\langle e, \sigma\rangle \to_e v}{\langle x := e, \sigma\rangle \Rightarrow_b \langle \sigma[x \mapsto v], 1\rangle}[Let]$$

$$\frac{\langle c_1, \sigma\rangle \Rightarrow_b \langle \sigma', n\rangle \qquad \langle c_2, \sigma'\rangle \Rightarrow_b \langle \sigma'', m\rangle}{\langle c_1; c_2, \sigma\rangle \Rightarrow_b \langle \sigma'', n + m\rangle}[Comp]$$

$$\frac{\langle e, \sigma\rangle \to_e v \neq 0 \qquad \langle c; \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma\rangle \Rightarrow_b \langle \sigma', n\rangle}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma\rangle \Rightarrow_b \langle \sigma', n\rangle}[While - True]$$

$$\frac{\langle e, \sigma\rangle \to_e 0}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma\rangle \Rightarrow_b \langle \sigma, 0\rangle}[While - False]$$

Parte 2.

$$\dfrac{\dfrac{\langle x,\sigma\rangle \to_e \sigma(x) = 0}{\langle x := x,\sigma\rangle \Rightarrow_b \langle \sigma[x \mapsto 0] = \sigma, 1\rangle}[Let] \qquad \dfrac{\dfrac{}{\langle \mathsf{skip},\sigma\rangle \Rightarrow_b \langle \sigma, 0\rangle} \qquad \dfrac{\langle x,\sigma\rangle \to_e \sigma(x) = 0}{\langle y := x,\sigma\rangle \Rightarrow_b \langle \sigma[y \mapsto 0] = \sigma, 1\rangle}}{\langle \mathsf{skip}; y := x,\sigma\rangle \Rightarrow_b \langle \sigma, 0 + 1 = 1\rangle}}{\langle x := x; (\mathsf{skip}; y := x),\sigma\rangle \Rightarrow_b \langle \sigma, 1 + 1 = 2\rangle}$$

□

Nome _____ Matricola _____

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

$\{n = N \geq 0\}$

$x := 0;$

$y := 0;$

---

while $x < n$ do

$x := x + 1;$

$y := 3 * y + 1$

$\{2 \cdot y = 3^N - 1\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

$\{n = N \geq 0\}$
$\{2 \cdot 0 = 3^0 - 1 \wedge 0 \leq n \wedge n = N\}$ (1)
$x := 0;$
$\{2 \cdot 0 = 3^x - 1 \wedge x \leq n \wedge n = N\}$
$y := 0;$
$\{INV : 2 \cdot y = 3^x - 1 \wedge x \leq n \wedge n = N\}$
while $x < n$ do
    $\{INV \wedge x < n\}$
    $\{2 \cdot (3y + 1) = 3^{x+1} - 1 \wedge x + 1 \leq n \wedge n = N\}$ (2)
    $x := x + 1;$
    $\{2 \cdot (3y + 1) = 3^x - 1 \wedge x \leq n \wedge n = N\}$
    $y := 3 * y + 1$
$\{INV \wedge \neg(x < n)\}$
$\{2 \cdot y = 3^N - 1\}$ (3)

Per le PrePost:
1) Banale aritmetica e conseguenze dirette dell'ipotesi.
2) La prima parte della tesi di ricava dall'INV come segue:

$$2 \cdot (3y + 1) = 3 \cdot 2y + 2 = 3 \cdot (3^x - 1) + 2 = 3^{x+1} - 1$$

Per il resto, $x + 1 \leq n$ deriva da $x < n$ e dal fatto che le variabili sono interi, mentre $n = N$ è un'ipotesi.

3) Per l'invariante, $x \leq n$ ma per ipotesi $\neg(x < n)$, quindi $x = n$. Usando l'invariante $n = N$, si ha quindi $x = N$. Dall'invariante infine si ha $2y = 3^x - 1 = 3^N - 1$.

□