

Informatica — 2021-02-15

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 interi (regole $[S0], [S1]$) e una relazione $R \in \mathcal{P}(S \times S)$ (regole $[R0], [R1]$). Sotto, a, a' indicano interi mentre s, s' indicano sequenze in S .*

$$\frac{}{\epsilon} [S0] \quad \frac{s}{a : s} (a \in \mathbb{Z}) [S1] \quad \frac{}{R(\epsilon, s)} [R0] \quad \frac{R(s, s') \quad a > a'}{R(a : s, a' : s')} [R1]$$

1. [20%] *Si fornisca una sequenza s contenente esattamente 5 interi per cui valga $R(10 : 7 : 5 : \epsilon, s)$ 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:*

$$\forall s_1, s_2, s_3 \in S. R(s_1, s_2) \wedge R(s_2, s_3) \implies R(s_1, s_3)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall s_1, s_2 \in S. R(s_1, s_2) \implies p(s_1, s_2)$$

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

Una possibile soluzione:

$$\frac{\frac{\frac{R(\epsilon, 10 : 20 : \epsilon)}{R(5 : \epsilon, 2 : 10 : 20 : \epsilon)}}{R(7 : 5 : \epsilon, 6 : 2 : 10 : 20 : \epsilon)}}{R(10 : 7 : 5 : \epsilon, 4 : 6 : 2 : 10 : 20 : \epsilon)}$$

Parte 2

Per dimostrare che vale $p(s_1, s_2)$ per ogni s_1, s_2 tali che soddisfano $R(s_1, s_2)$ è sufficiente dimostrare che

$$\begin{array}{l} R0) \quad \forall s \in S. p(\epsilon, s) \\ R0) \quad \forall a, a' \in \mathbb{Z}, s, s' \in S. p(s, s') \wedge a > a' \implies p(a : s, a' : s') \end{array}$$

Parte 3

Basta prendere

$$p(s_1, s_2) : \forall s_3 \in S. R(s_2, s_3) \implies R(s_1, s_3)$$

Parte 4 Caso R0.

Dobbiamo dimostrare $p(\epsilon, s)$ e cioè:

$$\forall s_3 \in S. R(s, s_3) \implies R(\epsilon, s_3)$$

Assumiamo quindi l'ipotesi $IP1 : R(s, s_3)$ e dimostriamo la nuova tesi $R(\epsilon, s_3)$. La tesi si ricava immediatamente dalla regola $R0$ (scegliendo s nella regola come s_3).

Caso R1. Per ipotesi assumiamo $IP1 : a > a'$ e $IP2 : p(s, s')$, cioè:

$$IP2 : \forall \bar{s}_3 \in S. R(s', \bar{s}_3) \implies R(s, \bar{s}_3)$$

Dobbiamo dimostrare $p(a : s, a' : s')$ e cioè:

$$\forall s_3 \in S. R(a' : s', s_3) \implies R(a : s, s_3)$$

Assumiamo quindi $IP3 : R(a' : s', s_3)$ e dimostriamo la nuova tesi $R(a : s, s_3)$.

Invertiamo $IP3$, che può essere generata solo dalla regola $R1$. Otteniamo quindi $s_3 = a'' : s''$ con $IP4 : a' > a''$ e $IP5 : R(s', s'')$.

Usando $IP2$ (scegliendo $\bar{s}_3 = s''$) assieme a $IP5$, otteniamo $IP6 : R(s, s'')$.

Da $IP1$ e $IP4$ otteniamo $IP7 : a > a''$.

Usiamo la regola $R1$ (scegliendo $a = a, s = s, a' = a'', s' = s''$). Le premesse sono vere per $IP6$ e $IP7$. Otteniamo quindi $R(a : s, a'' : s'')$ che è la tesi siccome $s_3 = a'' : s''$. $\square$

Esercizio 3. Si consideri una semantica alternativa del linguaggio IMP $(\rightarrow_a) \in \mathcal{P}(Com \times State \times State)$ che esegua i comandi di IMP come di consueto, eccetto per gli assegnamenti. In tale semantica, il primo assegnamento eseguito ha il normale effetto, il secondo invece non ne ha alcuno, il terzo ha effetto, il quarto no, e così via, come se gli assegnamenti venissero eseguiti “uno sì, uno no”. Per esempio, eseguendo

$$z := 1; (\text{if } x \neq 0 \text{ then } z := 3; y := 7; w := 1 \text{ else skip}); a := 9; b := 2$$

in uno stato iniziale σ con $\sigma(x) = 0$, gli assegnamenti con effetto sono solo $z := 1, b := 2$. Se invece fosse $\sigma(x) \neq 0$, gli assegnamenti con effetto sarebbero solo $z := 1, y := 7, a := 9$.

1. [50%] Si definisca $(\rightarrow_a) \in \mathcal{P}(Com \times State \times State)$ nel seguente modo. Dato l'insieme $P = \{0, 1\}$, si definisca prima una (altra) semantica $(\rightarrow_p) \in \mathcal{P}(Com \times State \times P \times State \times P)$ tramite un insieme di regole di inferenza. Dopo, si definisca $\langle c, \sigma \rangle \rightarrow_a \sigma'$ con una semplice formula logica sfruttando $\langle c, \sigma, p \rangle \rightarrow_p \langle \sigma', p' \rangle$.
2. [50%] Si definisca tramite un insieme di regole una relazione $R \in \mathcal{P}(Com \times Com)$ in modo tale che sia una funzione e che per ogni $c_1, c_2 \in Com$ tali che $R(c_1, c_2)$ valga l'equivalenza

$$\forall \sigma, \sigma'. \quad \langle c_1, \sigma \rangle \rightarrow_b \sigma' \iff \langle c_2, \sigma \rangle \rightarrow_a \sigma'$$

Si giustifichi in modo informale la soluzione proposta.

Soluzione (bozza). Parte 1

Definiamo $\langle c, \sigma \rangle \rightarrow_a \sigma'$ come $\exists p'. \langle c, \sigma, 0 \rangle \rightarrow_p \langle \sigma', p' \rangle$, dove $\rightarrow_p$ è definita dalle regole seguenti:

$$\begin{array}{c}
\overline{\langle \text{skip}, \sigma, p \rangle \rightarrow \langle \sigma, p \rangle} \\
\frac{\langle e, \sigma \rangle \rightarrow_e v}{\overline{\langle x := e, \sigma, 0 \rangle \rightarrow \langle \sigma[x \mapsto v], 1 \rangle}} \\
\overline{\langle x := e, \sigma, 1 \rangle \rightarrow \langle \sigma, 0 \rangle} \\
\frac{\langle c_1, \sigma, p \rangle \rightarrow \langle \sigma', p' \rangle \quad \langle c_2, \sigma', p' \rangle \rightarrow \langle \sigma'', p'' \rangle}{\overline{\langle c_1; c_2, \sigma, p \rangle \rightarrow \langle \sigma'', p'' \rangle}} \\
\frac{\langle e, \sigma \rangle \rightarrow_e v \neq 0 \quad \langle c_1, \sigma, p \rangle \rightarrow \langle \sigma', p' \rangle}{\overline{\langle \text{if } e \neq 0 \text{ then } c_1 \text{ else } c_2, \sigma, p \rangle \rightarrow \langle \sigma', p' \rangle}} \\
\frac{\langle e, \sigma \rangle \rightarrow_e 0 \quad \langle c_2, \sigma, p \rangle \rightarrow \langle \sigma', p' \rangle}{\overline{\langle \text{if } e \neq 0 \text{ then } c_1 \text{ else } c_2, \sigma, p \rangle \rightarrow \langle \sigma', p' \rangle}} \\
\frac{\langle e, \sigma \rangle \rightarrow_e v \neq 0 \quad \langle c; \text{while } e \neq 0 \text{ do } c, \sigma, p \rangle \rightarrow \langle \sigma', p' \rangle}{\overline{\langle \text{while } e \neq 0 \text{ do } c, \sigma, p \rangle \rightarrow \langle \sigma', p' \rangle}} \\
\frac{\langle e, \sigma \rangle \rightarrow_e 0}{\overline{\langle \text{while } e \neq 0 \text{ do } c, \sigma, p \rangle \rightarrow \langle \sigma, p \rangle}}
\end{array}$$

Parte 2

Una possibile R è quella che “raddoppia” ogni assegnamento. In questo modo usando $\rightarrow_a$ il primo assegnamento ha effetto, e il secondo no, e quindi l’esecuzione di questo comando “raddoppiato” secondo $\rightarrow_a$ è equivalente a eseguire il comando non “raddoppiato” secondo $\rightarrow_b$.

$$\begin{array}{c}
\overline{R(\text{skip}, \text{skip})} \\
\overline{R(x := e, x := e; x := e)} \\
\frac{R(c_1, c'_1) \quad R(c_2, c'_2)}{\overline{R(c_1; c_2, c'_1; c'_2)}} \\
\frac{R(c_1, c'_1) \quad R(c_2, c'_2)}{\overline{R(\text{if } e \neq 0 \text{ then } c_1 \text{ else } c_2, \text{if } e \neq 0 \text{ then } c'_1 \text{ else } c'_2)}} \\
\frac{R(c, c')}{\overline{R(\text{while } e \neq 0 \text{ do } c, \text{while } e \neq 0 \text{ do } c')}}
\end{array}$$

□

Nome _____ Matricola _____

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

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

$x := 0;$

$r := 4;$

while $x < n$ do

$x := x + 1;$

$r := r + 2 * x + 3$

$\{r = (N + 2)^2\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

```
{n = N ≥ 0} (1)
{0 ≤ n = N ∧ 4 = (0 + 2)2}
x := 0;
{x ≤ n = N ∧ 4 = (x + 2)2}
r := 4;
{INV : x ≤ n = N ∧ r = (x + 2)2}
while x < n do
  {INV ∧ x < n} (2)
  {x + 1 ≤ n = N ∧ r + 2(x + 1) + 3 = ((x + 1) + 2)2}
  x := x + 1;
  {x ≤ n = N ∧ r + 2x + 3 = (x + 2)2}
  r := r + 2 * x + 3
{INV ∧ ¬(x < n)} (3)
{r = (N + 2)2}
```

PrePost:

1) Banale aritmetica.

2) Da $x < n$, siccome le variabili sono intere, si ricava $x + 1 \leq n$. La tesi $n = N$ fa parte delle ipotesi. La tesi $r + 2(x + 1) + 3 = ((x + 1) + 2)^2$ si semplifica in $r + 2x + 5 = x^2 + 6x + 9$. Sostituendo r come da INV , la riscriviamo come $(x + 2)^2 + 2x + 5 = x^2 + 6x + 9$ e cioè $x^2 + 4x + 4 + 2x + 5 = x^2 + 6x + 9$ che è vera.

3) Da $\neg(x < n)$ e l'ipotesi $x \leq n = N$ ricaviamo $x = n = N$, che consente di riscrivere l'ipotesi $r = (x + 2)^2$ come la tesi $r = (N + 2)^2$.

□