Informatica — 2022-07-18

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

Esercizio 1. Dato un insieme di regole $\mathcal{R}$ su un universo U , si definisca l'associato operatore delle conseguenze immediate $\hat{\mathcal{R}} : \mathcal{P}(U) \rightarrow \mathcal{P}(U)$. Si dimostri che è monotono.

Esercizio 2. Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di naturali (regole $[S0], [S1]$), una relazione $R \in \mathcal{P}(S \times S)$ (regole $[R0], [R1], [R2]$), e una relazione $Q \in \mathcal{P}(S \times \mathbb{N})$ (regole $[Q0], [Q1]$). Sotto, n, k indicano naturali, mentre s, s' indicano sequenze in S .

$$\begin{array}{c} \frac{}{\epsilon} [S0] \quad \frac{s}{n : s} (n \in \mathbb{N}) [S1] \quad \frac{}{Q(\epsilon, 0)} [Q0] \quad \frac{Q(s, k)}{Q(n : s, n + k)} [Q1] \\ \frac{}{R(\epsilon, \epsilon)} [R0] \quad \frac{R(s, s')}{R(n : s, 6 \cdot n : s')} [R1] \quad \frac{R(s, s')}{R(n : s, (n + 3) \cdot n : s')} [R2] \end{array}$$

1. [20%] Si forniscano due sequenze s_1, s_2 e un naturale k per cui s_1 contenga tre naturali e inoltre valga $R(s_1, s_2) \wedge Q(s_2, k)$. Si giustifichi la risposta esibendo due derivazioni.
2. [20%] Si enunci il principio di induzione associato all'insieme S .
3. [10%] Si consideri l'enunciato seguente:

$$\forall s_1, s_2 \in S, k \in \mathbb{N}. Q(s_2, k) \wedge R(s_1, s_2) \implies k \text{ pari}$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall s_1 \in S. p(s_1)$$

per un qualche predicato p .

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

Soluzione (bozza).

Parte 1

Parte 2

Per dimostrare $\forall s \in S. p(s)$ è sufficiente dimostrare che:

$$\begin{array}{l} S0) \quad p(\epsilon) \\ S1) \quad \forall s, n. p(s) \implies p(n : s) \end{array}$$

Parte 3

Basta prendere $p(s_1) : \forall s_2 \in S, k \in \mathbb{N}. Q(s_2, k) \wedge R(s_1, s_2) \implies k$ pari.

Parte 4

Caso S0

Bisogna dimostrare $p(\epsilon)$ e quindi

$$\forall s_2 \in S, k \in \mathbb{N}. Q(s_2, k) \wedge R(\epsilon, s_2) \implies k \text{ pari}$$

Assumiamo quindi $IP1 : Q(s_2, k)$ e $IP2 : R(\epsilon, s_2)$ e dimostriamo la tesi k pari.

Invertendo $IP2$ notiamo che può essere derivata solo da $R0$ e quindi otteniamo $s_2 = \epsilon$.

L'ipotesi $IP1$ diventa $Q(\epsilon, k)$ e invertendo notiamo che può essere derivata solo da $Q0$ per cui $k = 0$ che è pari, da cui la tesi.

Caso S1

Assumiamo come ipotesi induttiva $IP1 : p(s)$ e cioè:

$$IP1 : \forall \bar{s}_2 \in S, \bar{k} \in \mathbb{N}. Q(\bar{s}_2, \bar{k}) \wedge R(s, \bar{s}_2) \implies \bar{k} \text{ pari}$$

Dobbiamo dimostrare la tesi $p(n : s)$ ovvero:

$$\forall s_2 \in S, k \in \mathbb{N}. Q(s_2, k) \wedge R(n : s, s_2) \implies k \text{ pari}$$

Assumiamo quindi le ipotesi $IP2 : Q(s_2, k)$, $IP3 : R(n : s, s_2)$ e dimostriamo la nuova tesi k pari.

Invertendo $IP3$, notiamo che può essere derivata solo da $R1$ o da $R2$. Esaminiamo quindi i sottocasi:

Sottocaso R1

Qui abbiamo $s_2 = 6 \cdot n : s'$ dove $IP4 : R(s, s')$.

Possiamo riscrivere $IP2 : Q(6n : s', k)$ e invertendola notiamo che può derivare solo da $Q1$ e quindi otteniamo $k = 6n + k'$ dove $IP5 : Q(s', k')$.

Usando $IP1$ scegliendo $\bar{s}_2 = s', \bar{k} = k'$ assieme a $IP5$ e $IP4$ ricaviamo k' pari. Da questo otteniamo che $k = 6n + k'$ è somma di pari e quindi pari, che è la tesi.

Sottocaso R2

Qui abbiamo $s_2 = (n + 3) \cdot n : s'$ dove $IP4 : R(s, s')$.

Possiamo riscrivere $IP2 : Q((n + 3)n : s', k)$ e invertendola notiamo che può derivare solo da $Q1$ e quindi otteniamo $k = (n + 3)n + k'$ dove $IP5 : Q(s', k')$.

Usando $IP1$ scegliendo $\bar{s}_2 = s', \bar{k} = k'$ assieme a $IP5$ e $IP4$ ricaviamo k' pari. Notiamo anche che $(n + 3)n$ deve essere pari, in quanto i fattori $n + 3$ e n non possono essere entrambi dispari. Da questo otteniamo che $k = (n + 3)n + k'$ è somma di pari e quindi pari, che è la tesi. $\square$

Esercizio 3.

1. [40%] Sia $x \in Var$ una variabile di IMP. Si definisca un comando $\bar{c}$ tale che la sua esecuzione termini sempre e tale che quando

$$\langle \bar{c}; \bar{c}; \dots; \bar{c}, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma'$$

si ha che $\sigma'(x) = 1$ se e solo se nella scrittura $\bar{c}; \bar{c}; \dots; \bar{c}$ il comando $\bar{c}$ compare un numero pari di volte. Si giustifichi informalmente la risposta.

2. [40%] Sia c un comando di IMP e x una variabile non usata dentro c . Si definisca un comando $\bar{c}$ tale che, per ogni σ, σ'

$$\langle c, \sigma \rangle \rightarrow_b \sigma' \iff \langle \bar{c}; \bar{c}, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma'[x \mapsto 1]$$

Si giustifichi informalmente la risposta.

3. [20%] In relazione al punto precedente, si giustifichi l'implicazione ($\implies$) assumendo una derivazione per $\langle c, \sigma \rangle \rightarrow_b \sigma'$ e costruendo una derivazione per $\langle \bar{c}; \bar{c}, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma'[x \mapsto 1]$.

Soluzione (bozza).

Parte 1. Basta prendere $\bar{c} = (x := 1 - x)$. Dopo un numero dispari di $\bar{c}$ si avrà uno stato finale dove $\sigma'(x) = 1 - 1 = 0$, mentre dopo un numero pari si avrà invece $\sigma'(x) = 1 - 0 = 1$.

Parte 2. Basta prendere

$$\bar{c} = \left(x := 1 - x; \text{if } x \neq 0 \text{ then } c \text{ else skip} \right)$$

Supponiamo infatti $\langle c, \sigma \rangle \rightarrow_b \sigma'$. Quando si esegue $\bar{c}; \bar{c}$ a partire da $\sigma[x \mapsto 1]$, x viene modificata come segue. Inizialmente l'assegnamento porta x a 0, e poi eseguendo l'if entriamo nell'else e eseguiamo **skip** terminando in $\sigma'[x \mapsto 0]$. A questo punto si esegue la seconda copia di $\bar{c}$, e l'assegnamento porta x a 1, e poi eseguendo l'if entriamo nel **then** e eseguiamo c terminando in $\sigma'[x \mapsto 1]$ (perché c non usa x) come desiderato.

L'altra implicazione segue da un ragionamento analogo.

Parte 3. Sia D una derivazione per $\langle c, \sigma \rangle \rightarrow_b \sigma'$. Costruiamo una derivazione per $\langle \bar{c}; \bar{c}, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma'[x \mapsto 1]$ come segue:

$$\begin{array}{c}
\frac{A \quad B}{\langle \bar{c}; \bar{c}, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma'[x \mapsto 1]} \\
A = \frac{\frac{\langle 1 - x, \sigma[x \mapsto 1] \rangle \rightarrow_e 0}{\langle x := 1 - x, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma[x \mapsto 0]} \quad \frac{\frac{\langle x, \sigma[x \mapsto 0] \rangle \rightarrow_e 0 \quad \langle \text{skip}, \sigma[x \mapsto 0] \rangle \rightarrow_b \sigma[x \mapsto 0]}{\langle \text{if } \dots, \sigma[x \mapsto 0] \rangle \rightarrow_b \sigma[x \mapsto 0]}}{\langle \bar{c}, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma[x \mapsto 0]} \\
B = \frac{\frac{\langle 1 - x, \sigma[x \mapsto 0] \rangle \rightarrow_e 1}{\langle x := 1 - x, \sigma[x \mapsto 0] \rangle \rightarrow_b \sigma[x \mapsto 1]} \quad \frac{\frac{\langle x, \sigma[x \mapsto 1] \rangle \rightarrow_e 1 \quad \langle c, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma'[x \mapsto 1]}{\langle \text{if } \dots, \sigma[x \mapsto 1] \rangle \rightarrow_b \sigma'[x \mapsto 1]}}{\langle \bar{c}, \sigma[x \mapsto 0] \rangle \rightarrow_b \sigma'[x \mapsto 1]}
\end{array}$$

□

Nome _____ Matricola _____

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

{vero}

$n := 0;$

$x := 0;$

while $n < 10$ do

$n := n + 1;$

if $x < 5$ then

$x := x + 1$

else

skip

{ $x = 5$ }

Si giustifichino qui sotto gli eventuali usi della regola *PrePost*.

Soluzione (bozza).

```
{vero} (1)
{0 = min(0, 5)}
n := 0;
{0 = min(n, 5)}
x := 0;
{INV : x = min(n, 5)}
while n < 10 do
  {INV ∧ n < 10} (2)
  {x = min(n + 1 - 1, 5)}
  n := n + 1;
  {x = min(n - 1, 5)}
  if x < 5 then
    {x = min(n - 1, 5) ∧ x < 5} (3)
    {x + 1 = min(n, 5)}
    x := x + 1
  else
    {x = min(n - 1, 5) ∧ ¬(x < 5)} (4)
    {x = min(n, 5)}
  skip
{INV ∧ ¬(n < 10)} (5)
{x = 5}
```

Per le PrePost:

- 1) Banale aritmetica.
- 2) La tesi, dopo averla semplificata, è l'ipotesi *INV*.
- 3) Siccome $x < 5$ per ipotesi, il minimo $x = \min(n - 1, 5)$ deve essere $n - 1$. Abbiamo quindi $x = n - 1 < 5$. Di conseguenza, siccome siamo sugli interi, $x + 1 = n \leq 5$ e quindi $x + 1$ è uguale a $\min(n, 5)$.
- 4) Siccome per ipotesi $x \geq 5$, si ha $x = \min(n - 1, 5) = 5$ e $n \geq 6$. Quindi $\min(n, 5) = 5 = x$ da cui la tesi.
- 5) Per ipotesi, $n \geq 10$ e quindi $x = \min(n, 5) = 5$ che è la tesi.

□