Informatica — 2023-06-28

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

Esercizio 1. *Si fornisca la definizione di validità per una tripla di Hoare, commentandola sinteticamente. Dopo, si enunci il teorema di correttezza per il sistema deduttivo delle triple di Hoare, commentandolo sinteticamente.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di interi (regole $[S0], [S1]$) e una relazione $R \in \mathcal{P}(S \times S \times \mathbb{Z} \times \mathbb{Z})$ (regole $[R0], [R1]$). Sotto, a, b, p, q indicano interi, mentre s, z indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{a : s}(a \in \mathbb{Z})[S1] \quad \frac{}{R(\epsilon, \epsilon, 1, 1)}[R0] \quad \frac{R(s, z, p, q)}{R(a : s,\ (-a) : z,\ ap, -q)}[R1]$$

1. *[25%] Si trovino due sequenze s_1, s_2 con almeno tre interi tale per cui valga $R(s_1, s_2, 24, -1)$. Si giustifichi la risposta esibendo una derivazione.*
2. *[20%] Si enunci il principio di induzione associato all'insieme S.*
3. *[5%] Si consideri l'enunciato seguente:*

   $$\forall s, z \in S, p, q \in \mathbb{Z}.\ R(s, z, p, q) \implies R(z, s, pq, q)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

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

   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.
Una possibile soluzione è:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R(\epsilon, \epsilon, 1, 1)}}{R(4 : \epsilon, -4 : \epsilon, 4, -1)}}{R(3 : 4 : \epsilon, -3 : -4 : \epsilon, 12, 1)}}{R(2 : 3 : 4 : \epsilon, -2 : -3 : -4 : \epsilon, 24, -1)}$$

Parte 2.
Affinché valga $p(s)$ per tutte le sequenze $s \in S$ è sufficiente che:

$$\begin{array}{ll} S0) & p(\epsilon) \\ S1) & \forall a \in \mathbb{Z}, s.p(s) \implies p(a : s) \end{array}$$

Parte 3.
Ovviamente basta prendere $p(s) :\ \forall z \in S, p, q \in \mathbb{Z}.\ R(s, z, p, q) \implies R(z, s, pq, q)$
Parte 4. Procediamo quindi per induzione.
Caso $[S0]$. Dobbiamo dimostrare $p(\epsilon)$, ovvero

$$\forall z \in S, p, q \in \mathbb{Z}.\ R(\epsilon, z, p, q) \implies R(z, \epsilon, pq, q)$$

Assumiamo $IP1 : R(\epsilon, z, p, q)$ e dimostriamo la nuova tesi $R(z, \epsilon, pq, q)$.

Invertendo $IP1$, osserviamo che può derivare solo da $[R0]$ e quindi abbiamo $z = \epsilon, p = q = 1$. La tesi diventa quindi $R(\epsilon, \epsilon, 1, 1)$ che è vera per $[R0]$.

Caso $[S1]$. Assumiamo $IP1 : p(s)$ e dimostriamo $p(a : s)$.

$$\begin{array}{ll} IP1: & \forall \bar{z} \in S, \bar{p}, \bar{q} \in \mathbb{Z}.\ R(s, \bar{z}, \bar{p}, \bar{q}) \implies R(\bar{z}, s, \bar{p}\bar{q}, \bar{q}) \\ tesi: & \forall z \in S, p, q \in \mathbb{Z}.\ R(a : s, z, p, q) \implies R(z, a : s, pq, q) \end{array}$$

Assumiamo $IP2 : R(a : s, z, p, q)$ e dimostriamo la nuova tesi $R(z, a : s, pq, q)$.

Invertendo $IP2$, osserviamo che può derivare solo da $[R1]$ e quindi abbiamo $z = -a : z', p = ap', q = -q'$ per qualche z', p', q' tali che $IP3 : R(s, z', p', q')$.

Usiamo $IP1$ scegliendo $\bar{z} = z', \bar{p} = p', \bar{q} = q'$ assieme a $IP3$ e otteniamo $IP4 : R(z', s, p'q', q')$.

Applichiamo a $IP4$ la regola $[R1]$ scegliendo le sue variabili in questo modo:

$$\frac{R(z', s, p'q', q')}{R(-a : z',\ -(-a) : s,\ -ap'q', -q')}[R1]$$

Ricaviamo quindi $R(-a : z',\ -(-a) : s,\ -ap'q', -q')$ che usando le equazioni trovate sopra si riscrive come $R(z,\ a : s,\ pq, q)$ che è la tesi.

□

Esercizio 3. *Si consideri una variante del linguaggio IMP dove le variabili perdono metà del loro valore ogni volta che vengono lette. La semantica delle espressioni ora ha segnatura* $(\to_e) \in \mathcal{P}(Exp \times State \times \mathbb{Z} \times State)$ *dove* $\langle e, \sigma\rangle \to_e \langle z, \sigma'\rangle$ *include sia il risultato dell'espressione* (z) *che il nuovo stato con le variabili dimezzate* (σ')*. La semantica dei comandi è conseguentemente adeguata. Più precisamente, qui sotto trovate le regole per l'espressione* x *(variabile arbitraria) e per il comando assegnamento.*

$$\frac{}{\langle x, \sigma\rangle \to_e \langle \sigma(x), \sigma[x \mapsto \lfloor \sigma(x)/2 \rfloor]\rangle}[Var] \qquad \frac{\langle e, \sigma\rangle \to_e \langle v, \sigma'\rangle}{\langle x := e, \sigma\rangle \to_b \sigma'[x \mapsto v]}[Let]$$

1. *[30%] Si forniscano le regole per la semantica delle espressioni costante intera* (z) *e somma* $(e_1 + e_2)$ *dove in quest'ultima il secondo addendo vede le variabili dimezzate dalla valutazione del primo addendo.*

2. *[30%] Si forniscano le regole per la semantica dei comandi* if e while*. (Si ricorda che la valutazione delle guardie può modificare le variabili)*

3. *[40%] Si fornisca un comando* c *di questo linguaggio che calcoli il fattoriale, nel senso espresso dalla seguente proprietà. Nelle espressioni è consentito l'uso degli operatori aritmetici* $+, -, *, /$*. Si giustifichi la risposta informalmente.*

$$\forall \sigma.\ \sigma(n) \geq 0 \implies \exists \sigma'.\ \langle c, \sigma\rangle \to_b \sigma' \wedge \sigma'(x) = \sigma(n)!$$

Soluzione (bozza).
Parte 1.

$$\frac{}{\langle z, \sigma\rangle \to_e \langle z, \sigma\rangle} \qquad \frac{\langle e_1, \sigma\rangle \to_e \langle z_1, \sigma'\rangle \quad \langle e_2, \sigma'\rangle \to_e \langle z_2, \sigma''\rangle}{\langle e_1 + e_2, \sigma\rangle \to_e \langle z_1 + z_2, \sigma''\rangle}$$

Parte 2.

$$\frac{\langle e, \sigma\rangle \to_e \langle v, \sigma'\rangle \quad v \neq 0 \quad \langle c_1, \sigma'\rangle \to_b \sigma''}{\langle \text{if } e \neq 0 \text{ then } c_1 \text{ else } c_2, \sigma\rangle \to_b \sigma''} \qquad \frac{\langle e, \sigma\rangle \to_e \langle 0, \sigma'\rangle \quad \langle c_2, \sigma'\rangle \to_b \sigma''}{\langle \text{if } e \neq 0 \text{ then } c_1 \text{ else } c_2, \sigma\rangle \to_b \sigma''}$$

$$\frac{\langle e, \sigma\rangle \to_e \langle v, \sigma'\rangle \quad v \neq 0 \quad \langle c; \text{while } e \neq 0 \text{ do } c, \sigma'\rangle \to_b \sigma''}{\langle \text{while } e \neq 0 \text{ do } c, \sigma\rangle \to_b \sigma''} \qquad \frac{\langle e, \sigma\rangle \to_e \langle 0, \sigma'\rangle}{\langle \text{while } e \neq 0 \text{ do } c, \sigma\rangle \to_b \sigma'}$$

Parte 3. Un possibile comando c per il fattoriale è il seguente:

$$
\begin{array}{l}
x := 1; \\
n := 2 * n; \\
\mathsf{while}\ n \neq 0\ \mathsf{do} \\
\qquad n := 2 * n; \\
\qquad x := x * n/2; \\
\qquad n := 2 * (n - 1)
\end{array}
$$

Si noti che, per come sono definite le regole $[Var]$ e $[Let]$, il comando $n := 2 * n$ raddoppia il valore di n: nella semantica si crea brevemente uno stato σ' con n dimezzata, ma poi questo valore viene sovrascritto col doppio del valore originale.

Per lo stesso motivo, $x := x * n/2$ non dimezza il valore di x, ma solo quello di n.

Quindi, eseguendo il comando $n := 2 * n; x := x * n/2$ da uno stato iniziale con i valori non negativi $\sigma(x) = X,\ \sigma(n) = N$, si passa attraverso uno stato intermedio $\sigma'(x) = X,\ \sigma'(n) = 2N$, per poi finire in $\sigma''(x) = 2NX/2 = NX,\ \sigma''(n) = N$.

Prima del controllo della guardia $n \neq 0$ si raddoppia il valore di n in modo che il dimezzamento dovuto alla valutazione della guardia lo riporti al valore originale. Il raddoppio non influenza il valore di verità della guardia $n \neq 0$.

□

Nome _____ Matricola _____

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

$\{n = N \geq 10\}$

$x := 0;$

$y := 0;$

---

while $x < n$ do

$x := x + 1;$

---

if $y < 10$ then

$y := y + 1$

else

---

skip

$\{x = N \wedge y = 10\}$

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

Soluzione (bozza).

$\{n = N \geq 10\}$ (1)
$\{n = N \geq 10 \wedge 0 \leq n \wedge 0 = \min(10, 0)\}$
$x := 0;$
$\{n = N \geq 10 \wedge x \leq n \wedge 0 = \min(10, x)\}$
$y := 0;$
$\{INV : n = N \geq 10 \wedge x \leq n \wedge y = \min(10, x)\}$
while $x < n$ do
    $\{INV \wedge x < n\}$ (2)
    $\{n = N \geq 10 \wedge x + 1 \leq n \wedge y = \min(10, x + 1 - 1)\}$
    $x := x + 1;$
    $\{n = N \geq 10 \wedge x \leq n \wedge y = \min(10, x - 1)\}$
    if $y < 10$ then
        $\{n = N \geq 10 \wedge x \leq n \wedge y = \min(10, x - 1) \wedge y < 10\}$ (3)
        $\{n = N \geq 10 \wedge x \leq n \wedge y + 1 = \min(10, x)\}$
        $y := y + 1$
    else
        $\{n = N \geq 10 \wedge x \leq n \wedge y = \min(10, x - 1) \wedge \neg(y < 10)\}$ (4)
        $\{INV\}$
        skip
$\{INV \wedge \neg(x < n)\}$ (5)
$\{x = N \wedge y = 10\}$

Per le PrePost:

1) Banale aritmetica.

2) La tesi $n = N \geq 10$ è parte di INV. La tesi $x + 1 \leq n$ è equivalente a $x < n$ visto che sono valori interi, e quest'ultima è un'ipotesi. La tesi $y = \min(10, x + 1 - 1)$ è equivalente a $y = \min(10, x)$ che è un'ipotesi.

3) La tesi $n = N \geq 10 \wedge x \leq n$ è parte dell'ipotesi. Visto che $y = min(10, x - 1) < 10$ per ipotesi, deve essere $y = x - 1 < 10$, da cui la tesi $y + 1 = \min(10, x)$ visto che sono valori interi.

4) La tesi $n = N \geq 10 \wedge x \leq n$ è parte dell'ipotesi. Siccome per ipotesi $y = \min(10, x - 1) \geq 10$, deve essere $y = 10$ e $x - 1 \geq 10$. Questo implica la tesi $y = \min(10, x)$.

5) Per ipotesi $x \leq n$ e $\neg(x < n)$ da cui $x = n$ che con le altre ipotesi implica $x = N \geq 10$. Questo, assieme a $y = \min(10, x)$, implica anche che $y = 10$.

□