Informatica — 2024-01-29

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

Esercizio 1. *Si enuncino tutti i risultati relativi al determinismo e alla totalità della semantica delle espressioni ($\to_e$) e dei comandi ($\to_b$) di IMP.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di interi (regole $[S0], [S1]$), una relazione $R \in \mathcal{P}(S \times \mathbb{Z})$ (regole $[R0], [R1]$), e una relazione $Q \in \mathcal{P}(S \times \mathbb{Z})$ (regole $[Q0], [Q1], [Q2]$). Sotto, a, b, c, x, y indicano interi, mentre s, z indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{a : s}(a \in \mathbb{Z})[S1] \quad \frac{}{R(\epsilon, 0)}[R0] \quad \frac{R(s, a)}{R(b : s, a + b)}[R1]$$

$$\frac{}{Q(\epsilon,\ 0)}[Q0] \quad \frac{}{Q(a : \epsilon,\ a)}[Q1] \quad \frac{Q((a + b) : z, c)}{Q(a : b : z,\ c)}[Q2]$$

1. *[20%] Si trovi una sequenza s con almeno tre interi, tale per cui valga $R(s, 12) \land Q(s, 12)$. Si giustifichi la risposta esibendo due derivazioni.*

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

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

   $$\forall s \in S, x, y \in \mathbb{Z}.\ R(s, x) \land Q(s, y) \implies x = y$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall s \in S, y \in \mathbb{Z}.\ Q(s, y) \implies p(s, y)$$

   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.
Una possibile soluzione è:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R(\epsilon, 0)}}{R(5 : \epsilon, 0 + 5 = 5)}}{R(4 : 5 : \epsilon, 5 + 4 = 9)}}{R(3 : 4 : 5 : \epsilon, 9 + 3 = 12)}$$

$$\dfrac{\dfrac{\dfrac{}{Q(12 : \epsilon, 12)}}{Q(7 : 5 : \epsilon, 12)}}{Q(3 : 4 : 5 : \epsilon, 12)}$$

Parte 2. Affinché valga $\forall s, y.\ Q(s, y) \implies p(s, a)$ basta che:

$Q0)$ $p(\epsilon,\ 0)$
$Q1)$ $\forall a \in \mathbb{Z}.\ p(a : \epsilon,\ a)$
$Q2)$ $\forall a, b, c \in \mathbb{Z}, z \in S.\ p((a + b) : z,\ c) \implies p(a : b : z,\ c)$

Parte 3.
Basta prendere $p(s, y) :\ \forall x \in \mathbb{Z}.\ R(s, x) \implies x = y$

Parte 4.

Caso $[Q0]$.

Dobbiamo dimostrare $p(\epsilon,\ 0)$ e cioè $\forall x \in \mathbb{Z}.\ R(\epsilon, x) \implies x = 0$.

Prendiamo per ipotesi $IP1 : R(\epsilon, x)$ e dimostriamo la tesi $x = 0$.

Invertendo $IP1$ notiamo che si può derivare solo da $[R0]$ e otteniamo quindi la tesi $x = 0$.

Caso $[Q1]$.

Dobbiamo dimostrare $p(a : \epsilon,\ a)$ e cioè $\forall x \in \mathbb{Z}.\ R(a : \epsilon, x) \implies x = a$.

Prendiamo per ipotesi $IP1 : R(a : \epsilon, x)$ e dimostriamo la tesi $x = a$.

Invertendo $IP1$ notiamo che si può derivare solo in questo modo:

$$\frac{\overline{R(\epsilon, 0)}[R0]}{R(a : \epsilon, x = 0 + a)}[R1]$$

Otteniamo quindi la tesi $x = 0 + a = a$.

Caso $[Q2]$. Assumiamo l'ipotesi induttiva $IP1 : p((a + b) : z,\ c)$, ovvero

$$IP1 : \forall \bar{x} \in \mathbb{Z}.\ R((a + b) : z, \bar{x}) \implies \bar{x} = c$$

e dimostriamo la tesi $p(a : b : z,\ c)$, ovvero

$$\forall x \in \mathbb{Z}.\ R(a : b : z, x) \implies x = c$$

Introducendo la tesi, assumiamo quindi $IP2 : R(a : b : z, x)$ e dimostriamo la nuova tesi $x = c$.

Invertendo $IP2$, notiamo che può essere ricavata solo in questo modo:

$$\frac{\dfrac{R(z, e)}{R(b : z, d = e + b)}[R1]}{R(a : b : z, x = d + a)}[R1]$$

Otteniamo quindi $IP3 : R(z, e)$ per qualche intero e per cui $x = e + b + a$.

Possiamo quindi applicare la regola $[R1]$ a $IP3$ e ottenere

$$\frac{R(z, e)}{R((a + b) : z, e + a + b)}[R1]$$

e quindi $IP4 : R((a + b) : z, x)$.

Usiamo ora $IP1$ scegliendo $\bar{x} = x$ assieme a $IP4$, e otteniamo così $x = c$ che è la tesi. □

Esercizio 3. *Siano Var e Exp le variabili e le espressioni di IMP. Si definisca una relazione $R \in \mathcal{P}(Var \times Exp \times Var \times Exp \times Exp)$ tramite regole di inferenza in modo da soddisfare entrambe le seguenti proprietà:*

- *Per ogni $x_1, x_2 \in Var, e_1, e_2 \in Exp$, esiste un'unica espressione f che soddisfa $R(x_1, e_1, x_2, e_2, f)$.*
- *Per ogni $x_1, x_2 \in Var, e_1, e_2, f \in Exp$, se (i) x_1 e x_2 sono variabili distinte, (ii) x_2 non compare all'interno di e_1, (iii) vale $R(x_1, e_1, x_2, e_2, f)$, allora vale l'equivalenza tra comandi*

$$x_1 := e_1;\ x_2 := e_2 \qquad \equiv \qquad x_2 := f;\ x_1 := e_1$$

1. *[30%] Si forniscano le regole di inferenza per R.*
2. *[30%] Si giustifichi informalmente perché esiste un'unica f.*

3. [40%] Si giustifichi informalmente perché vale l'equivalenza tra comandi richiesta.

Soluzione (bozza).
Parte 1.

$$\frac{}{R(x_1, e_1, x_2, z, z)}(z \in \mathbb{Z})[Lit]$$

$$\frac{y \neq x_1}{R(x_1, e_1, x_2, y, y)}(y \in Var)[Var1]$$

$$\frac{}{R(x_1, e_1, x_2, x_1, e_1)}[Var2]$$

$$\frac{R(x_1, e_1, x_2, e', f') \quad R(x_1, e_1, x_2, e'', f'')}{R(x_1, e_1, x_2, e' + e'', f' + f'')}[Plus]$$

Parte 2.

Basta considerare le forme che può avere l'espressione e_2: costante, variabile, addizione. Per costanti e addizioni esiste esattamente una regola che gestisce il caso. Per le variabili y ci sono due regole, una per il caso $y = x_1$ e l'altra per il caso $y \neq x_1$, quindi se ne applica sempre esattamente una.

Visto che in ogni caso si applica esattamente una regola (e tenendo conto delle ipotesi induttive in $[Plus]$), esiste esattamente una f.

Parte 3.

In pratica, le regole definiscono f come l'espressione e_2 modificata rimpiazzando tutte le occorrenze di x_1 con e_2. Resta quindi da convincersi che vale l'equivalenza

$$x_1 := e_1;\ x_2 := e_2 \qquad \equiv \qquad x_2 := e_2\{e_1/x_1\};\ x_1 := e_1$$

Nel primo comando $x_1 := e_1;\ x_2 := e_2$ l'espressione e_2 viene valutata nello stato dove x_1 è stato modificato al valore che aveva e_1 nello stato iniziale. Di conseguenza, l'espressione e_2 in tale stato ha come valore lo stesso che si avrebbe valutando $e_2\{e_1/x_1\}$ nello stato iniziale. Di conseguenza, a x_2 viene assegnato lo stesso valore in entrambi i comandi.

Inoltre, a x_1 viene assegnato il valore di e_1 in entrambi i comandi. Questi due valori sono uguali perché nel primo comando e_1 viene valuata nello stato iniziale, mentre nel secondo e_1 viene valuata nello stato con x_2 modificato, ma siccome per ipotesi e_1 non contiene x_2 la differenza negli stati è irrilevante. Di conseguenza, anche a x_1 viene assegnato lo stesso valore in entrambi i comandi.

□

Nome _____ Matricola _____

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

$\{x = X \wedge y = Y \geq 0\}$

$n := y * (y + 1);$

---

while $n > 0$ do

$z := x - y;$

$x := x - z;$

$y := y + z;$

$n := n - 1$

$\{x = X \wedge y = Y\}$

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

Soluzione (bozza).

$\{x = X \wedge y = Y \geq 0\}$ (1)
$\{y*(y+1) \geq 0 \wedge \begin{array}{ll}(y*(y+1) \text{ pari} & \implies x = X \wedge y = Y) \wedge \\ (y*(y+1) \text{ dispari} & \implies x = Y \wedge y = X)\end{array}\}$
$n := y*(y+1);$
$\{INV : n \geq 0 \wedge \begin{array}{ll}(n \text{ pari} & \implies x = X \wedge y = Y) \wedge \\ (n \text{ dispari} & \implies x = Y \wedge y = X)\}\end{array}$
while $n > 0$ do
  $\{INV \wedge n > 0\}$ (2)
  $\{n-1 \geq 0 \wedge \begin{array}{ll}(n-1 \text{ pari} & \implies x-(x-y) = X \wedge y+(x-y) = Y) \wedge \\ (n-1 \text{ dispari} & \implies x-(x-y) = Y \wedge y+(x-y) = X)\end{array}\}$
  $z := x - y;$
  $\{n-1 \geq 0 \wedge \begin{array}{ll}(n-1 \text{ pari} & \implies x-z = X \wedge y+z = Y) \wedge \\ (n-1 \text{ dispari} & \implies x-z = Y \wedge y+z = X)\end{array}\}$
  $x := x - z;$
  $\{n-1 \geq 0 \wedge \begin{array}{ll}(n-1 \text{ pari} & \implies x = X \wedge y+z = Y) \wedge \\ (n-1 \text{ dispari} & \implies x = Y \wedge y+z = X)\end{array}\}$
  $y := y + z;$
  $\{n-1 \geq 0 \wedge \begin{array}{ll}(n-1 \text{ pari} & \implies x = X \wedge y = Y) \wedge \\ (n-1 \text{ dispari} & \implies x = Y \wedge y = X)\end{array}\}$
  $n := n - 1$
$\{INV \wedge \neg(n > 0)\}$ (3)
$\{x = X \wedge y = Y\}$

Per le PrePost:

1) Siccome $y = Y \geq 0$ sicuramente $y(y+1) \geq 0$. Inoltre, la prima implicazione è vera perché la sua conseguente è vera per ipotesi. La seconda implicazione è vera perché la sua antecedente è falsa, essendo $y(y+1)$ sempre pari.

2) Dall'ipotesi $n > 0$, siccome n è intero, ricaviamo la tesi $n-1 \geq 0$. Il resto della tesi è

$$\begin{array}{ll}(n-1 \text{ pari} & \implies x-(x-y) = X \wedge y+(x-y) = Y) \wedge \\ (n-1 \text{ dispari} & \implies x-(x-y) = Y \wedge y+(x-y) = X)\end{array}$$

che si riscrive semplificando come

$$\begin{array}{ll}(n \text{ dispari} & \implies y = X \wedge x = Y) \wedge \\ (n \text{ pari} & \implies y = Y \wedge x = X)\end{array}$$

il che deriva immediatamente da INV.

3) Dalle ipotesi $n \geq 0$ e $\neg(n > 0)$ si ricava $n = 0$ che è pari. Dal resto di INV segue quindi la tesi $x = X \wedge y = Y$.

□