Informatica — 2024-06-24

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

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

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi binari di interi (regole $[T0], [T1]$), una relazione $R \in \mathcal{P}(T \times T)$ (regole $[R0], [R1], [R2]$), e una relazione $Q \in \mathcal{P}(T \times \mathbb{Z})$ (regole $[Q0], [Q1]$), Sotto, x, y, z indicano interi, mentre s, d, t, u, v indicano alberi in T.*

$$\frac{}{z}(z \in \mathbb{Z})[T0] \qquad \frac{s \quad d}{(s,d)}[T1] \qquad \frac{}{Q(z,z)}[Q0] \qquad \frac{Q(t_1,z_1) \quad Q(t_2,z_2)}{Q((t_1,t_2),z_1+z_2)}[Q1]$$

$$\frac{}{R(t,t)}[R0] \qquad \frac{R(t,u) \quad R(u,v)}{R(t,v)}[R1] \qquad \frac{R(t_1,u_1) \quad R(t_2,u_2) \quad R(t_3,u_3)}{R(((t_1,t_2),t_3)\ ,\ (u_1,(u_2,u_3)))}[R2]$$

1. *[20%] Si trovino $t \in T$ e $z \in \mathbb{Z}$ per cui valga $R\Big(((1,2),3),4),\ (1,t)\Big) \wedge Q((1,t),z)$. Si giustifichi la risposta esibendo due derivazioni.*

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

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

$$\forall t, u \in T, z \in \mathbb{Z}.\ Q(t,z) \wedge R(t,u) \implies Q(u,z)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t, u \in T.\ R(t,u) \implies p(t,u)$$

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 è:

$$\dfrac{\dfrac{\dfrac{}{R((1,2),(1,2))}\ \dfrac{}{R(3,3)}\ \dfrac{}{R(4,4)}}{R((((1,2),3),4),\ ((1,2),(3,4)))}[R2] \quad \dfrac{\dfrac{}{R(1,1)}\ \dfrac{}{R(2,2)}\ \dfrac{}{R((3,4),(3,4))}}{R(((1,2),(3,4)),\ (1,(2,(3,4))))}[R2]}{R((((1,2),3),4),\ (1,(2,(3,4))))}[R1]$$

dove nella prima riga si è usato $[R0]$ ripetutamente.

$$\dfrac{\dfrac{}{Q(1,1)} \quad \dfrac{\dfrac{}{Q(2,2)} \quad \dfrac{\dfrac{}{Q(3,3)}\ \dfrac{}{Q(4,4)}}{Q((3,4),7)}}{Q((2,(3,4)),9)}}{Q((1,(2,(3,4))),10)}$$

Parte 2.
Affinché valga $\forall t, u.\ R(t,u) \implies p(t,u)$ è sufficiente che:

$$\begin{aligned}
&R0)\ \forall t.\ p(t,t)\\
&R1)\ \forall t, u, v.\ p(t,u) \wedge p(u,v) \implies p(t,v)\\
&R2)\ \forall t_1, t_2, t_3, u_1, u_2, u_3.\ p(t_1,u_1) \wedge p(t_2,u_2) \wedge p(t_3,u_3)\\
&\qquad\qquad \implies p(((t_1,t_2),t_3),(u_1,(u_2,u_3)))
\end{aligned}$$

Parte 3.
Basta prendere

$$p(t,u): \quad \forall z \in \mathbb{Z}.\ Q(t,z) \implies Q(u,z)$$

Parte 4. Andiamo quindi per induzione su R.
Caso [**R0**]. Dobbiamo dimostrare $p(t,t)$, ovvero

$$\forall z \in \mathbb{Z}.\ Q(t,z) \implies Q(t,z)$$

Questo è immediato perché l'antecedente è uguale alla conseguente.
Caso [**R1**]. Assumiamo le ipotesi induttive

$$IP1 : p(t,u) \qquad IP2 : p(u,v)$$

e dimostriamo $p(t,v)$. Riscriviamo le ipotesi come

$$\begin{array}{l} IP1: \ \forall z \in \mathbb{Z}.\ Q(t,z) \implies Q(u,z) \\ IP2: \ \forall z \in \mathbb{Z}.\ Q(u,z) \implies Q(v,z) \end{array}$$

e la tesi come $\forall z \in \mathbb{Z}.\ Q(t,z) \implies Q(v,z)$. Assumiamo quindi $IP3 : Q(t,z)$ e dimostriamo la nuova tesi $Q(v,z)$.
Da $IP3$ e $IP1$ otteniamo $Q(u,z)$, che con $IP2$ implica $Q(v,z)$ da cui la tesi.
Caso [**R2**]. Assumiamo le ipotesi induttive

$$IP1 : p(t_1,u_1) \qquad IP2 : p(t_2,u_2) \qquad IP3 : p(t_3,u_3)$$

e dimostriamo la tesi $p(((t_1,t_2),t_3),\ (u_1,(u_2,u_3)))$. Riscriviamo le ipotesi come

$$\begin{array}{l} IP1: \ \forall z \in \mathbb{Z}.\ Q(t_1,z) \implies Q(u_1,z) \\ IP2: \ \forall z \in \mathbb{Z}.\ Q(t_2,z) \implies Q(u_2,z) \\ IP3: \ \forall z \in \mathbb{Z}.\ Q(t_3,z) \implies Q(u_3,z) \end{array}$$

e la tesi come $\forall z \in \mathbb{Z}.\ Q(((t_1,t_2),t_3),z) \implies Q((u_1,(u_2,u_3)),z)$.
Assumiamo quindi $IP4 : Q(((t_1,t_2),t_3),z)$ e dimostriamo la nuova tesi $Q((u_1,(u_2,u_3)),z)$.
Invertendo $IP4$, notiamo che può essere ricavata solo in questo modo:

$$\dfrac{\dfrac{Q(t_1,z_1) \qquad Q(t_2,z_2)}{Q((t_1,t_2),z_1+z_2)}[Q1] \qquad Q(t_3,z_3)}{Q(((t_1,t_2),t_3),z=z_1+z_2+z_3)}[Q1]$$

per qualche z_1, z_2, z_3 che sommano a z. Assumiamo quindi $IP5 : Q(t_1,z_1)$, $IP6 : Q(t_2,z_2)$, $IP7 : Q(t_3,z_3)$.
Usando $IP5$ e $IP1$ (con $z = z_1$) otteniamo $IP8 : Q(u_1,z_1)$. Usando $IP6$ e $IP2$ (con $z = z_2$) otteniamo $IP9 : Q(u_2,z_2)$. Usando $IP7$ e $IP3$ (con $z = z_3$) otteniamo $IP10 : Q(u_3,z_3)$.
Possiamo quindi ottenere la tesi da $IP8, IP9, IP10$ tramite la derivazione seguente:

$$\dfrac{Q(u_1,z_1) \qquad \dfrac{Q(u_2,z_2) \qquad Q(u_3,z_3)}{Q((u_2,u_3),z_2+z_3)}[Q1]}{Q((u_1,(u_2,u_3)),z=z_1+z_2+z_3)}[Q1]$$

□

Esercizio 3. *Si consideri un'estensione di IMP ottenuta aggiungendo il nuovo comando* bif $e \neq 0$ then c_1 else c_2. *La semantica informale di questo comando è quella di verificare se la guardia $e \neq 0$ è vera, nel qual caso vengono eseguiti i comandi c_1 e c_2, in tale ordine; nel caso opposto invece vengono eseguiti i comandi c_2 e c_1, in tale ordine.*

1. *[35%] Si adatti la semantica big step di IMP in modo da includere il nuovo comando* bif. *Si aggiunga una o più regole di inferenza, commentandole brevemente.*

2. *[35%] Si adatti il sistema deduttivo delle triple di Hoare in modo da considerare il comando* bif. *Si aggiunga una o più regole di inferenza, commentandole brevemente.*

3. *[30%] Siano e_1, e_2, e_3 espressioni senza occorrenze della variabile x. Sia c il comando*

$$(\textsf{if } e_1 \neq 0 \textsf{ then } y := e_2 \textsf{ else } z := e_3) \ ; \ x := 0$$

Si costruisca un comando c' in IMP esteso che sia equivalente a c ($c' \equiv c$) e senza che c' abbia comandi if *o* while *all'interno. Si giustifichi la risposta in modo informale.*

Soluzione (bozza).
Nota: il comando bif $e \neq 0$ then c_1 else c_2 è equivalente a if $e \neq 0$ then $c_1; c_2$ else $c_2; c_1$, quindi basta adattare le regole dell'if opportunamente.

Parte 1.
Basta aggiungere

$$\frac{\langle e, \sigma\rangle \to_e v \neq 0 \qquad \langle c_1; c_2, \sigma\rangle \to_b \sigma'}{\langle \textsf{bif } e \neq 0 \textsf{ then } c_1 \textsf{ else } c_2, \sigma\rangle \to_b \sigma'}[Bif - True]$$

$$\frac{\langle e, \sigma\rangle \to_e 0 \qquad \langle c_2; c_1, \sigma\rangle \to_b \sigma'}{\langle \textsf{bif } e \neq 0 \textsf{ then } c_1 \textsf{ else } c_2, \sigma\rangle \to_b \sigma'}[Bif - False]$$

Parte 2.
Basta aggiungere

$$\frac{\{P \wedge e \neq 0\}\ c_1; c_2\ \{Q\} \qquad \{P \wedge \neg(e \neq 0)\}\ c_2; c_1\ \{Q\}}{\{P\}\ \textsf{bif } e \neq 0 \textsf{ then } c_1 \textsf{ else } c_2\ \{Q\}}[Bif]$$

Parte 3.
Basta prendere c' uguale a

$$\begin{array}{l} x := 0; \\ \textsf{bif } e_1 \neq 0 \textsf{ then} \\ \quad y := x * y + (1 - x) * e_2 \ ; \ x := 1 - x \\ \textsf{else} \\ \quad z := x * z + (1 - x) * e_3 \ ; \ x := 1 - x \end{array}$$

La valutazione di e_1, e_2, e_3 non viene influenzata dal valore di x, per ipotesi. Quindi, se nello stato iniziale $e_1 \neq 0$ il comando c' si comporterà come

$$\begin{array}{l} x := 0; \\ y := x * y + (1 - x) * e_2; \\ x := 1 - x; \\ z := x * z + (1 - x) * e_3; \\ x := 1 - x \end{array}$$

e quindi come

$$\begin{array}{l} x := 0; \\ y := 0 * y + 1 * e_2; \\ x := 1; \\ z := 1 * z + 0 * e_3; \\ x := 0; \end{array}$$

e quindi come

$$
\begin{aligned}
&x := 0;\\
&y := e_2;\\
&x := 1;\\
&z := z;\\
&x := 0;
\end{aligned}
$$

e quindi come (siccome e_2 non usa x)

$$
\begin{aligned}
&y := e_2;\\
&x := 0;
\end{aligned}
$$

e questo è proprio quanto avverrebbe eseguendo c nello stesso stato iniziale.

Il caso in cui la guardia $e_1 \neq 0$ è falsa è analogo.

□

Nome _____ Matricola _____

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

$\{n = 3N \geq 0\}$

$x := 0;$

---

while $n > 0$ do

---

if $x = 0$ then

$x := 2$

else

$x := x - 1;$

$n := n - 1$

$\{x = n\}$

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

Soluzione (bozza).

$\{n = 3N \geq 0\}$ (1)
$\{INV : n \geq 0 \wedge 0 = n \bmod 3\}$
$x := 0;$
$\{INV : n \geq 0 \wedge x = n \bmod 3\}$
while $n > 0$ do
    $\{INV \wedge n > 0\}$
    if $x = 0$ then
        $\{INV \wedge n > 0 \wedge x = 0\}$ (2)
        $\{n - 1 \geq 0 \wedge 2 = (n - 1) \bmod 3\}$
        $x := 2;$
    else
        $\{INV \wedge n > 0 \wedge \neg(x = 0)\}$ (3)
        $\{n - 1 \geq 0 \wedge x - 1 = (n - 1) \bmod 3\}$
        $x := x - 1;$
    $\{n - 1 \geq 0 \wedge x = (n - 1) \bmod 3\}$
    $n := n - 1$
$\{INV \wedge \neg(n > 0)\}$ (4)
$\{x = n\}$

Per le PrePost:

1) La tesi $n \geq 0$ è parte dell'ipotesi. La tesi $0 = n \bmod 3$ deriva da $n \bmod 3 = 3N \bmod 3 = 0$.

2) La tesi $n - 1 \geq 0$ deriva da $n > 0$. Per la tesi $2 = (n - 1) \bmod 3$ osserviamo che dalle ipotesi si ha $0 = x = n \bmod 3$, quindi n è multiplo di 3, e quindi $n - 1$ diviso 3 ha resto 2.

3) La tesi $n - 1 \geq 0$ deriva da $n > 0$. Per la tesi $x - 1 = (n - 1) \bmod 3$ osserviamo che dalle ipotesi si ha $0 \neq x = n \bmod 3$, quindi n non è multiplo di 3, e quindi n diviso 3 ha resto $x > 0$. Da questo otteniamo che $n - 1$ diviso 3 ha resto $x - 1$.

4) Dalle ipotesi $n \geq 0$ e n $leq0$, quindi $n = 0$ e $x = n \bmod 3 = 0$, quindi $x = 0 = n$ che è la tesi.

□