Informatica — 2024-02-19

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

Esercizio 1. *Si forniscano le sei regole di inferenza che definiscono il sistema deduttivo (la relazione $\vdash \{P\}\ c\ \{Q\}$) delle triple di Hoare.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi con interi sui nodi interni (regole $[T0], [T1]$), e una relazione $R \in \mathcal{P}(T \times T)$ (regole $[R0], [R1], [R2]$). Sotto, a, b, c, x, y indicano interi, mentre s, d, t indicano alberi in T.*

$$\frac{}{\epsilon}[T0] \quad \frac{s \quad d}{(s, a, d)}(a \in \mathbb{Z})[T1] \quad \frac{}{R(\epsilon, \epsilon)}[R0] \quad \frac{}{R((\epsilon, a, \epsilon), (\epsilon, a, \epsilon))}[R1]$$

$$\frac{R(t_1, t_2) \quad R(t_3, t_4)}{R((t_1, a_5, t_3), (t_2, a_2 + a_4, t_4))}[R2] \text{ dove } t_i = (s_i, a_i, d_i) \text{ per } i = 1..4$$

1. *[20%] Si trovi un albero t tale per cui valga la seguente, Si giustifichi la risposta esibendo una derivazione.*

$$R\Big(\big(((\epsilon, 1, \epsilon), 100, (\epsilon, 2, \epsilon)),\ 200,\ (\epsilon, 3, \epsilon)\big),\ t\Big)$$

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

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

$$\forall u_1, u_2, u_3 \in T.\ R(u_1, u_2) \land R(u_2, u_3) \implies u_2 = u_3$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall u_1, u_2 \in T.\ R(u_1, u_2) \implies p(u_1, u_2)$$

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 è:

$$\dfrac{\dfrac{\dfrac{}{R((\epsilon,1,\epsilon),\ (\epsilon,1,\epsilon))}[R1] \quad \dfrac{}{R((\epsilon,2,\epsilon),\ (\epsilon,2,\epsilon))}[R1]}{R(((\epsilon,1,\epsilon),100,(\epsilon,2,\epsilon)),\ ((\epsilon,1,\epsilon),3,(\epsilon,2,\epsilon)))}[R2] \quad \dfrac{}{R((\epsilon,3,\epsilon),\ (\epsilon,3,\epsilon))}[R1]}{R((((\epsilon,1,\epsilon),100,(\epsilon,2,\epsilon)),\ 200,\ (\epsilon,3,\epsilon)),\ (((\epsilon,1,\epsilon),3,(\epsilon,2,\epsilon)),\ 6,\ (\epsilon,3,\epsilon)))}[R2]$$

Parte 2.

Affinché valga $\forall u_1, u_2 \in T.\ R(u_1, u_2) \implies p(u_1, u_2)$ basta che:

$$\begin{array}{ll} R0) & p(\epsilon, \epsilon) \\ R1) & \forall a.\ p((\epsilon, a, \epsilon), (\epsilon, a, \epsilon)) \\ R2) & \forall s_1, s_2, s_3, s_4, d_1, d_2, d_3, d_4, a_1, a_2, a_3, a_4, a_5. \\ & p(t_1, t_2) \land p(t_3, t_4) \implies p((t_1, a_5, t_3), (t_2, a_2 + a_4, t_4)) \end{array}$$

dove $t_i = (s_i, a_i, d_i)$ per $i = 1..4$.

Parte 3.

Basta prendere $p(u_1, u_2) : \forall u \in T.\ R(u_2, u) \implies u_2 = u$

Parte 4.

Caso $[R0]$. Dobbiamo dimostrare $p(\epsilon, \epsilon)$, ovvero $\forall u \in T.\ R(\epsilon, u) \implies \epsilon = u$.

Assumiamo $IP1 : R(\epsilon, u)$ e dimostriamo la tesi $\epsilon = u$.

Invertendo $IP1$ notiamo che può essere ricavata solo da $[R0]$ ($[R1]$ e $[R2]$ vogliono una tripla come primo argomento) e quindi otteniamo $u = \epsilon$.

Caso $[R1]$. Dobbiamo dimostrare $\forall a.\ p((\epsilon, a, \epsilon), (\epsilon, a, \epsilon))$, ovvero

$$\forall a, u \in T.\ R((\epsilon, a, \epsilon), u) \implies (\epsilon, a, \epsilon) = u$$

Assumiamo $IP1 : R((\epsilon, a, \epsilon), u)$ e dimostriamo la tesi $(\epsilon, a, \epsilon) = u$.

Invertendo $IP1$ notiamo che può essere ricavata solo da $[R1]$ (come primo argomento $[R0]$ vuole ϵ, mentre $[R2]$ vuole una tripla con dentro altre triple) e quindi otteniamo $u = (\epsilon, a, \epsilon)$.

Caso $[R2]$. Qui sotto scriviamo t_i al posto di (s_i, a_i, d_i) per $i = 1..4$.

Assumiamo le ipotesi induttive $IP1 : p(t_1, t_2), IP2 : p(t_3, t_4)$ e dimostriamo la tesi $p((t_1, a_5, t_3), (t_2, a_2 + a_4, t_4))$.

$$\begin{array}{l} IP1 : \forall \bar{u}.R(t_2, \bar{u}) \implies t_2 = \bar{u} \\ IP2 : \forall \hat{u}.R(t_4, \hat{u}) \implies t_4 = \hat{u} \\ tesi : \forall u.R((t_2, a_2 + a_4, t_4), u) \implies (t_2, a_2 + a_4, t_4) = u \end{array}$$

Assumiamo quindi $IP3 : R((t_2, a_2 + a_4, t_4), u)$ e dimostriamo la nuova tesi $(t_2, a_2 + a_4, t_4) = u$.

Invertendo $IP3$ notiamo che può essere ricavata solo da $[R2]$ in questo modo (come primo argomento $[R0]$ vuole ϵ, mentre $[R1]$ vuole una tripla con dentro $\epsilon \neq t_2$) e quindi otteniamo:

$$\frac{R(t_2, t_2') \quad R(t_4, t_4')}{R((t_2, a_2 + a_4, t_4), (t_2', a_2' + a_4', t_4'))}[R2] \text{ dove } t_i = (s_i, a_i, d_i), t_i' = (s_i', a_i', d_i')$$

Otteniamo quindi le nuove ipotesi $IP4 : R(t_2, t_2'), IP5 : R(t_4, t_4'), IP6 : u = (t_2', a_2' + a_4', t_4')$.

Usiamo $IP1$ scegliendo $\bar{u} = t_2'$ assieme a $IP4$, e ricaviamo quindi $t_2 = t_2'$ (da cui anche $a_2 = a_2'$).

Usiamo $IP2$ scegliendo $\hat{u} = t_4'$ assieme a $IP5$, e ricaviamo quindi $t_4 = t_4'$ (da cui anche $a_4 = a_4'$).

Mettendo assieme le uguaglianze ottenute, otteniamo la tesi: $u = (t_2', a_2' + a_4', t_4') = (t_2, a_2 + a_4, t_4)$.

□

Esercizio 3. *Si consideri un'estensione delle espressioni di IMP ottenuta aggiungendo $e_1 \rhd e_2$ come nuova espressione. Il valore di $e_1 \rhd e_2$, quando valutata, è lo stesso di e_2.*

Siano n ("normale") e p ("prioritario") due valori distinti arbitrari. La nuova semantica $(\rightarrow_e) \in \mathcal{P}(Exp \times State \times \mathbb{Z} \times \{n, p\})$, con notazione $\langle e, \sigma\rangle \rightarrow_e \langle v, \alpha\rangle$ indica che e in σ ha un valore $v \in \mathbb{Z}$ e una priorità $\alpha \in \{n, p\}$. Il risultato di un'espressione è intuitivamente calcolato come in IMP, con priorità normale, tranne nel caso in cui in all'interno dell'espressione venga valutata $e_1 \rhd e_2$ con e_1 avente valore non zero. In tal caso il risultato (che è il valore di e_2) è "prioritario" e diventa il valore di <u>tutta</u> l'espressione circostante. Nel caso in cui ci siano più valori prioritari in gioco, si considera solo quello "più a sinistra" o "più interno", come mostrato nei seguenti esempi.

$\langle 1 + 2, \sigma\rangle \rightarrow_e \langle 3, n\rangle$ $\quad \langle 10 + (0 \rhd 2), \sigma\rangle \rightarrow_e \langle 12, n\rangle$ $\quad \langle 10 + (1 \rhd 2), \sigma\rangle \rightarrow_e \langle 2, p\rangle$

$\langle 10 + ((1 \rhd 2) + (1 \rhd 3)), \sigma\rangle \rightarrow_e \langle 2, p\rangle$ $\quad \langle 1 \rhd (2 + (1 \rhd 3)), \sigma\rangle \rightarrow_e \langle 3, p\rangle$ $\quad \langle (1 \rhd 2) \rhd (1 \rhd 3), \sigma\rangle \rightarrow_e \langle 2, p\rangle$

1. *[50%] Si formalizzi la semantica delle espressioni con regole di inferenza.*

2. *[50%] Si forniscano le derivazioni per gli ultimi tre esempi sopra.*

Soluzione (bozza).
Parte 1.

$$\frac{}{\langle z, \sigma\rangle \to_e \langle z, n\rangle}[Lit]$$

$$\frac{}{\langle x, \sigma\rangle \to_e \langle \sigma(x), n\rangle}[Var]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \langle z_1, p\rangle}{\langle e_1 + e_2, \sigma\rangle \to_e \langle z_1, p\rangle}[Plus1]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \langle z_1, n\rangle \qquad \langle e_2, \sigma\rangle \to_e \langle z_2, p\rangle}{\langle e_1 + e_2, \sigma\rangle \to_e \langle z_2, p\rangle}[Plus2]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \langle z_1, n\rangle \qquad \langle e_2, \sigma\rangle \to_e \langle z_2, n\rangle}{\langle e_1 + e_2, \sigma\rangle \to_e \langle z_1 + z_2, n\rangle}[Plus3]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \langle z_1, p\rangle}{\langle e_1 \rhd e_2, \sigma\rangle \to_e \langle z_1, p\rangle}[Tri1]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \langle z_1, n\rangle \qquad \langle e_2, \sigma\rangle \to_e \langle z_2, p\rangle}{\langle e_1 \rhd e_2, \sigma\rangle \to_e \langle z_2, p\rangle}[Tri2]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \langle 0, n\rangle \qquad \langle e_2, \sigma\rangle \to_e \langle z_2, n\rangle}{\langle e_1 \rhd e_2, \sigma\rangle \to_e \langle z_2, n\rangle}[Tri3]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \langle z_1, n\rangle \qquad z_1 \neq 0 \qquad \langle e_2, \sigma\rangle \to_e \langle z_2, n\rangle}{\langle e_1 \rhd e_2, \sigma\rangle \to_e \langle z_2, p\rangle}[Tri4]$$

Parte 2.

$$\frac{\dfrac{}{\langle 10, \sigma\rangle \to_e \langle 10, n\rangle}[Lit] \qquad \dfrac{\dfrac{\dfrac{}{\langle 1, \sigma\rangle \to_e \langle 1, n\rangle}[Lit] \qquad \dfrac{}{\langle 2, \sigma\rangle \to_e \langle 2, n\rangle}[Lit]}{\langle 1 \rhd 2, \sigma\rangle \to_e \langle 2, p\rangle}[Tri4]}{\langle (1 \rhd 2) + (1 \rhd 3), \sigma\rangle \to_e \langle 2, p\rangle}[Plus1]}{\langle 10 + ((1 \rhd 2) + (1 \rhd 3)), \sigma\rangle \to_e \langle 2, p\rangle}[Plus2]$$

$$\frac{\dfrac{}{\langle 1, \sigma\rangle \to_e \langle 1, n\rangle}[Lit] \qquad \dfrac{\dfrac{}{\langle 2, \sigma\rangle \to_e \langle 2, n\rangle}[Lit] \qquad \dfrac{\dfrac{}{\langle 1, \sigma\rangle \to_e \langle 1, n\rangle}[Lit] \qquad \dfrac{}{\langle 3, \sigma\rangle \to_e \langle 3, n\rangle}[Lit]}{\langle 1 \rhd 3, \sigma\rangle \to_e \langle 3, p\rangle}[Tri4]}{\langle 2 + (1 \rhd 3), \sigma\rangle \to_e \langle 3, p\rangle}[Plus2]}{\langle 1 \rhd (2 + (1 \rhd 3)), \sigma\rangle \to_e \langle 3, p\rangle}[Tri2]$$

$$\frac{\dfrac{\dfrac{}{\langle 1, \sigma\rangle \to_e \langle 1, n\rangle}[Lit] \qquad \dfrac{}{\langle 2, \sigma\rangle \to_e \langle 2, n\rangle}[Lit]}{\langle 1 \rhd 2, \sigma\rangle \to_e \langle 2, p\rangle}[Tri4]}{\langle (1 \rhd 2) \rhd (1 \rhd 3), \sigma\rangle \to_e \langle 2, p\rangle}[Tri1]$$

□

Nome _____ Matricola _____

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

$\{n = N \wedge y \geq 2\}$

$x := 2;$

$z := 1;$

---

while $x < n$ do

---

if $x * y = n$ then

$z := 0;$

else

---

skip;

$x := x + 1$

$\{N \ primo \implies z = 1\}$

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

Soluzione (bozza).

$\{n = N \wedge y \geq 2\}$ (1)
$\{n = N \wedge 2 \geq 2 \wedge y \geq 2 \wedge (N \text{ primo } \implies 1 = 1)\}$
$x := 2;$
$\{n = N \wedge x \geq 2 \wedge y \geq 2 \wedge (N \text{ primo } \implies 1 = 1)\}$
$z := 1;$
$\{INV : n = N \wedge x \geq 2 \wedge y \geq 2 \wedge (N \text{ primo } \implies z = 1)\}$
while $x < n$ do
    $\{INV \wedge x < n\}$
    if $x * y = n$ then
        $\{INV \wedge x < n \wedge xy = n\}$ (2)
        $\{n = N \wedge x + 1 \geq 2 \wedge y \geq 2 \wedge (N \text{ primo } \implies 0 = 1)\}$
        $z := 0;$
    else
        $\{INV \wedge x < n \wedge xy \neq n\}$ (3)
        $\{n = N \wedge x + 1 \geq 2 \wedge y \geq 2 \wedge (N \text{ primo } \implies z = 1)\}$
        skip;
    $\{n = N \wedge x + 1 \geq 2 \wedge y \geq 2 \wedge (N \text{ primo } \implies z = 1)\}$
    $x := x + 1$
$\{INV \wedge \neg(x < n)\}$ (4)
$\{N \text{ primo } \implies z = 1\}$

Per le PrePost:

1) Parte della tesi è nell'ipotesi. Il resto è banalmente vero (in particolare $1 = 1$ è vero e quindi implicato da qualunque cosa).

2) Le tesi $n = N$ e $y \geq 2$ sono parte dell'ipotesi. La tesi $x + 1 \geq 2$ deriva dall'ipotesi $x \geq 2$. La tesi N primo $\implies 0 = 1$ afferma che N non è primo, e questo deriva dalle ipotesi $N = n = xy$, $x \geq 2$ e $y \geq 2$, visto che sono tutti interi.

3) La tesi è inclusa nell'ipotesi, tranne per $x+1 \geq 2$ che però deriva dall'ipotesi $x \geq 2$.

4) La tesi è parte dell'ipotesi INV.

□