Informatica — 2021-01-27

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 $\hat{\mathcal{R}} : \mathcal{P}(U) \to \mathcal{P}(U)$. 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 $R \in \mathcal{P}(T \times \mathbb{Z} \times T)$ (regole $[R0], [R1]$), e un sottoinsieme di alberi $Q \in \mathcal{P}(T)$ (regole $[Q0], [Q1]$). Sotto, a, x indicano interi mentre s, d, t indicano alberi in T.*

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

$$\frac{}{Q(2 \cdot x)}[Q0] \qquad \frac{Q(s) \quad Q(d)}{Q((s,d))}[Q1]$$

1. *[20%] Si fornisca un albero t contenente esattamente 5 interi, tutti pari, e un albero t' per cui valga $R(t, 7, t')$ e si giustifichi la risposta esibendo una derivazione.*

2. *[20%] Si enunci il principio di induzione associato all'insieme T.*

3. *[5%] Si consideri l'enunciato seguente:*

   $$\forall t_1, t_2 \in T, x \in \mathbb{Z}.\ R(t_1, x, t_2) \land x \text{ pari} \implies Q(t_2)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall t_1 \in T.\ p(t_1)$$

   per un qualche predicato p.

4. *[55%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione <u>associato a T</u>.*

Soluzione (bozza).

Parte 1

Un possibile esempio è:

$$\dfrac{\dfrac{\dfrac{}{R(2,7,7)} \quad \dfrac{}{R(4,7,7)}}{R((2,4),7,(7,7))} \quad \dfrac{\dfrac{}{R(6,7,7)} \quad \dfrac{\dfrac{}{R(8,7,7)} \quad \dfrac{}{R(4,7,7)}}{R((8,4),7,(7,7))}}{R((6,(8,4)),7,(7,(7,7)))}}{R(((2,4),(6,(8,4))),7,((7,7),(7,(7,7))))}$$

Parte 2

Sia $p(t)$ un predicato su $t \in T$. Per dimostrare $p(t)$ per ogni $t \in T$ è sufficiente verificare che:

1) $\forall a \in \mathbb{Z}.\ p(a)$
2) $\forall s, d.\ p(s) \land p(d) \implies p((s,d))$

Parte 3

Basta prendere:

$$p(t) : \forall t_2 \in T, x \in \mathbb{Z}.\ R(t, x, t_2) \land x \text{ pari} \implies Q(t_2)$$

Parte 4 Procediamo per induzione su T:

Caso $[T0]$

Dobbiamo dimostrare $p(a)$. Per farlo, assumiamo come ipotesi

$$IP1 : R(a, x, t_2)$$
$$IP2 : x \text{ pari}$$

e dimostriamo la nuova tesi $Q(t_2)$.

Invertiamo $IP1$: siccome può essere ricavata solo da $[R0]$, otteniamo $t_2 = x$ quindi $t_2 = 2y$ per qualche y, visto che x è pari.

La tesi diventa $Q(2y)$ che deriva da $[Q0]$.

Caso $[T1]$

Assumendo come ipotesi induttive $IP1 : p(s)$ e $IP2 : p(d)$, ovvero

$$IP1 : \forall \bar{t}_2 \in T, \bar{x} \in \mathbb{Z}.\ R(s, \bar{x}, \bar{t}_2) \wedge \bar{x} \text{ pari} \implies Q(\bar{t}_2)$$
$$IP2 : \forall t'_2 \in T, x' \in \mathbb{Z}.\ R(d, x', t'_2) \wedge x' \text{ pari} \implies Q(t'_2)$$

dimostriamo la tesi $p((s, d))$. Per farlo, assumiamo come ipotesi

$$IP3 : R((s, d), x, t_2)$$
$$IP4 : x \text{ pari}$$

e dimostriamo la nuova tesi $Q(t_2)$.

Invertiamo $IP3$: siccome può essere ricavata solo da $[R1]$, otteniamo $t_2 = (t_s, t_d)$ per qualche t_s, t_d tali che

$$IP5 : R(s, x, t_s)$$
$$IP6 : R(d, x, t_d)$$

Da $IP1$ (con $\bar{t}_2 = t_s$ e $\bar{x} = x$) e da $IP5, IP4$ otteniamo $IP7 : Q(t_s)$.

Da $IP2$ (con $t'_2 = t_d$ e $x' = x$) e da $IP6, IP4$ otteniamo $IP8 : Q(t_d)$.

Da $IP7, IP8$, usando la regola $[Q1]$ si ricava la tesi $Q(t_2)$ ovvero $Q((t_s, t_d))$.

□

Esercizio 3.

1. *[25%] Si definisca induttivamente tramite un insieme di regole di inferenza una relazione $S \in \mathcal{P}(Com \times \mathbb{N})$ tale per cui $S(c, n)$ valga se e solo se dentro il comando c ci sono esattamente n occorrenze del comando* skip.

2. *[25%] Si definisca induttivamente tramite un insieme di regole di inferenza una variante della semantica big step $(\rightarrow) \in \mathcal{P}(Com \times State \times State \times \mathbb{N})$ tale per cui $\langle c, \sigma \rangle \rightarrow \langle \sigma', n \rangle$ valga se e solo se il comando c eseguito a partire dallo stato σ termina nello stato σ' e n è il numero di volte in cui durante tale esecuzione è stato eseguito un qualche* skip *presente all'interno di c.*

3. *[25%] Si forniscano c, σ, σ', n, m tali per cui valgano le seguenti, giustificando informalmente la risposta.*

$$n < m \qquad S(c, n) \qquad \langle c, \sigma \rangle \rightarrow \langle \sigma', m \rangle$$

4. *[25%] Si forniscano c, σ, σ', n, m tali per cui valgano le seguenti, giustificando informalmente la risposta.*

$$n > m \qquad S(c, n) \qquad \langle c, \sigma \rangle \rightarrow \langle \sigma', m \rangle$$

Soluzione (bozza). Parte 1

$$\frac{}{S(\mathsf{skip}, 1)}$$

$$\frac{}{S(x := e, 0)}$$

$$\frac{S(c_1, n_1) \qquad S(c_2, n_2)}{S(c_1; c_2, n_1 + n_2)}$$

$$\frac{S(c_1, n_1) \qquad S(c_2, n_2)}{S(\mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, n_1 + n_2)}$$

$$\frac{S(c, n)}{S(\mathsf{while}\ e \neq 0\ \mathsf{do}\ c, n)}$$

Parte 2

$$\frac{}{\langle \mathsf{skip}, \sigma \rangle \to \langle \sigma, 1 \rangle}$$

$$\frac{\langle e, \sigma \rangle \to_e v}{\langle x := e, \sigma \rangle \to \langle \sigma[x \mapsto v], 0 \rangle}$$

$$\frac{\langle c_1, \sigma \rangle \to \langle \sigma', n_1 \rangle \qquad \langle c_2, \sigma' \rangle \to \langle \sigma'', n_2 \rangle}{\langle c_1; c_2, \sigma \rangle \to \langle \sigma'', n_1 + n_2 \rangle}$$

$$\frac{\langle e, \sigma \rangle \to_e v \neq 0 \qquad \langle c_1, \sigma \rangle \to \langle \sigma', n \rangle}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma \rangle \to \langle \sigma', n \rangle}$$

$$\frac{\langle e, \sigma \rangle \to_e 0 \qquad \langle c_2, \sigma \rangle \to \langle \sigma', n \rangle}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma \rangle \to \langle \sigma', n \rangle}$$

$$\frac{\langle e, \sigma \rangle \to_e v \neq 0 \qquad \langle c; \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma \rangle \to \langle \sigma', n \rangle}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma \rangle \to \langle \sigma', n \rangle}$$

$$\frac{\langle e, \sigma \rangle \to_e 0}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma \rangle \to \langle \sigma, 0 \rangle}$$

Parte 3

Si prenda c come segue

$$c = \mathsf{while}\ x \neq 0\ \mathsf{do}\ (\mathsf{skip}; x := x - 1)$$

Inoltre, siano $n = 1$, $m = 10$ e σ lo stato in cui tutte le variabili valgono 10 e $\sigma' = \sigma[x \mapsto 0]$.

È immediato vedere che $S(c, 1)$ vale perché c'è solo uno skip nella definizione di c.

Inoltre, vale $\langle c, \sigma \rangle \to \langle \sigma', 10 \rangle$ perché il ciclo ripete il suo corpo 10 volte e quindi esegue lo skip 10 volte.

Parte 4

Si prenda c come segue

$$c = \mathsf{if}\ x \neq 0\ \mathsf{then\ skip\ else\ skip}$$

Inoltre, siano $n = 2$, $m = 1$ e $\sigma = \sigma'$ uno stato qualunque.

È immediato vedere che $S(c, 2)$ vale perché ci sono due skip nella definizione di c.

Inoltre, vale $\langle c, \sigma \rangle \to \langle \sigma', 1 \rangle$ perché viene eseguito solo un ramo dell'if, e quindi uno skip solo.

□

Nome _____ Matricola _____

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

$\{x = N\}$

$y := 20;$

---

while $x \neq 0$ do

$x := x - 1;$

$y := y - 5$

$\{y = 20 - 5N\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

Soluzione (bozza).

$\{x = N\}$ (1)
$\{20 = 20 - 5(N - x)\}$
$y := 20;$
$\{INV : y = 20 - 5(N - x)\}$
while $x \neq 0$ do
    $\{INV \wedge x \neq 0\}$ (2)
    $\{y - 5 = 20 - 5(N - (x - 1))\}$
    $x := x - 1;$
    $\{y - 5 = 20 - 5(N - x)\}$
    $y := y - 5$
$\{INV \wedge \neg(x \neq 0)\}$ (3)
$\{y = 20 - 5N\}$

PrePost:

1) Banale aritmetica, visto che $N - x = 0$ per ipotesi.

2) La tesi si semplifica in $y - 5 = 20 - 5(N - x) - 5$ il che deriva immediatamente da INV.

3) Da $\neg(x \neq 0)$ si ha $x = 0$. Di qui e INV, si ha $y = 20 - 5(N - 0) = 20 - 5N$ e quindi la tesi.

□