Informatica — 2019-09-05

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 di numeri naturali (regole $[T0], [T1]$), una relazione $F \in \mathcal{P}(T \times T)$ (regole $[F0], [F1]$) e una relazione $R \in \mathcal{P}(T \times \mathbb{N} \times \mathbb{N})$ (regole $[R0], [R1]$). Sotto, n, m indicano naturali mentre t, l, r indicano alberi in T.*

$$\frac{}{n}(n \in \mathbb{N})[T0] \qquad \frac{l \qquad r}{(l, r)}[T1] \qquad \frac{}{F(n, n)}[F0] \qquad \frac{F(l_1, l_2) \qquad F(r_1, r_2)}{F((l_1, r_1), (r_2, l_2))}[F1]$$

$$\frac{}{R(n, n, n)}[R0] \qquad \frac{R(l, n_1, n_2) \qquad R(r, n_3, n_4)}{R((l, r), n_1, n_4)}[R1]$$

1. *[20%] Si forniscano $n, m \in \mathbb{N}$ per cui valga $R(((1, 2), (3, (4, 5))), n, m)$. Si giustifichi la risposta esibendo un'opportuna derivazione.*

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

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

$$\forall t_1, t_2 \in T, n, m \in \mathbb{N}.\ R(t_1, n, m) \land F(t_1, t_2) \implies R(t_2, m, n)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

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

   per un qualche predicato p.

4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione <u>associato a T</u>.*

Soluzione (bozza).
Parte 1.

$$\cfrac{\cfrac{\cfrac{}{R(1,1,1)} \qquad \cfrac{}{R(2,2,2)}}{R((1,2),1,2)} \qquad \cfrac{\cfrac{}{R(3,3,3)} \qquad \cfrac{\cfrac{}{R(4,4,4)} \qquad \cfrac{}{R(5,5,5)}}{R((4,5),4,5)}}{R((3,(4,5)),3,5)}}{R(((1,2),(3,(4,5))),1,5)}$$

Parte 2.
Sia $p(t)$ una proprietà sugli alberi. Per dimostrare $\forall \in T.\ p(t)$ è sufficiente verificare che:

$$T0) \forall n \in \mathbb{N}.\ p(n)$$
$$T1) \forall l, r.\ p(l) \land p(r) \implies p((l, r))$$

Parte 3.
Basta definire

$$p(t_1) : \forall t_2 \in T, n, m \in \mathbb{N}.\ R(t_1, n, m) \land F(t_1, t_2) \implies R(t_2, m, n)$$

Parte 4.
Caso $T0$.

Preso, $n \in \mathbb{N}$, dobbiamo dimostrare $p(n)$, cioè:

$$\forall t_2 \in T, k, m \in \mathbb{N}.\ R(n,k,m) \wedge F(n,t_2) \implies R(t_2,m,k)$$

Assumiamo quindi $IP1 : R(n,k,m)$ e $IP2 : F(n,t_2)$ e dimostriamo la tesi $R(t_2,m,k)$.

Invertendo $IP1$, siccome può essere derivata solo da $R0$, otteniamo $n = k = m$. Invertendo $IP2$, siccome può essere derivata solo da $F0$, otteniamo $t_2 = n$.

La tesi diventa quindi $R(n,n,n)$ che si ottiene da $R0$.

Caso $T1$.

Assumiamo come ipotesi induttive $p(l)$ e $p(r)$, cioè:

$$\begin{aligned} IP1 :\ & \forall t_2' \in T, n', m' \in \mathbb{N}.\ R(l,n',m') \wedge F(l,t_2') \implies R(t_2',m',n') \\ IP2 :\ & \forall \bar{t}_2 \in T, \bar{n}, \bar{m} \in \mathbb{N}.\ R(r,\bar{n},\bar{m}) \wedge F(r,\bar{t}_2) \implies R(\bar{t}_2,\bar{m},\bar{n}) \end{aligned}$$

e dimostriamo la tesi $p((l,r))$, cioè:

$$\forall t_2 \in T, n, m \in \mathbb{N}.\ R((l,r),n,m) \wedge F((l,r),t_2) \implies R(t_2,m,n)$$

Assumiamo quindi $IP3 : R((l,r),n,m)$ e $IP4 : F((l,r),t_2)$ e dimostriamo la nuova tesi $R(t_2,m,n)$.

Invertendo $IP3$, siccome può essere derivata solo da $R1$, otteniamo che per qualche n_2, n_3 si ha $IP5 : R(l,n,n_2)$ e $IP6 : R(r,n_3,m)$.

Invertendo $IP4$, siccome può essere derivata solo da $F1$, otteniamo che per qualche l', r' si ha $t_2 = (r', l')$ con $IP7 : F(l,l')$ e $IP8 : F(r,r')$.

Usiamo ora $IP1$ scegliendo $t_2' = l', n' = n, m' = n_2$, che diventa:

$$R(l,n,n_2) \wedge F(l,l') \implies R(l',n_2,n)$$

Da questo e $IP5, IP7$ otteniamo $IP9 : R(l',n_2,n)$.

Usiamo ora $IP2$ scegliendo $\bar{t}_2 = r', \bar{n} = n_3, \bar{m} = m$, che diventa:

$$R(r,n_3,m) \wedge F(r,r') \implies R(r',m,n_3)$$

Da questo e $IP6, IP8$ otteniamo $IP10 : R(r',m,n_3)$.

Infine, usando $IP10, IP9$ nella regola $R1$, si ottiene $R((r',l'),m,n)$ che è la tesi.

□

Esercizio 3. *Si consideri l'estensione del linguaggio IMP ottenuta aggiungendo il comando* foo z *(con $z \in Var$), la cui semantica è data dalle regole seguenti:*

$$\frac{}{\langle \mathsf{foo}\ z, \sigma\rangle \to_b \sigma[z \mapsto 0]}[Foo-0] \qquad \frac{}{\langle \mathsf{foo}\ z, \sigma\rangle \to_b \sigma}[Foo-1]$$

Sia σ_0 lo stato che assegna ad ogni variabile il valore 0. Si fornisca un comando c di questo linguaggio che soddisfi la proprietà:

$$\begin{aligned} & \forall n \in \mathbb{N}.\ \exists \sigma', \sigma''. \\ & \quad \langle c, \sigma_0[x \mapsto n]\rangle \to_b \sigma' \wedge \sigma'(y) = n! \wedge \langle c, \sigma_0[x \mapsto n]\rangle \to_b \sigma'' \wedge \sigma''(y) = n^2 \end{aligned}$$

dove $n!$ è il fattoriale di n. Si giustifichi la risposta in modo informale ma dettagliato.

Soluzione (bozza).

```
z := 1;
foo z;
if z ≠ 0 then
    y := 1;
    while x > 0 do
        y := y * x;
        x := x - 1
else
    y := x * x
```

All'inizio la variabile z è impostata a 1. Dopo foo z, può essere sia 1 che 0, a seconda di quale regola tra $Foo-0$ e $Foo-1$ è stata usata. Qui il comportamento di foo z è non deterministico, e la semantica può raggiungere entrambi questi stati intermedi.

Di qui, l'if controlla in quale dei due stati ci troviamo. Nel caso in cui z è rimasto 1, calcoliamo in y il fattoriale di x (che vale n all'inizio) con un ciclo while, raggiungendo il desiderato stato σ'. Nel caso in cui z è diventato 0, calcoliamo in y il quadrato di x (che vale n), raggiungendo il desiderato stato σ''.

□

Nome ______________________________________ Matricola ______________

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

$\{y > 30\}$

____

$x := 4;$

____

$z := 2 * y + x$

____

while $y > 0$ do

____

____

$y := z - 2 * x - y;$

____

$z := 2 * y + x$

____

$\{y \geq -5)\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$\{y > 30\}$ (1)
$\{4 = 4 \wedge 2y + 4 = 2y + 4 \wedge y \geq -5\}$
$x := 4;$
$\{x = 4 \wedge 2y + x = 2y + 4 \wedge y \geq -5\}$
$z := 2 * y + x$
$\{INV : x = 4 \wedge z = 2y + 4 \wedge y \geq -5\}$
while $y > 0$ do
  $\{INV \wedge y > 0\}$ (2)
  $\{x = 4 \wedge 2(z - 2x - y) + x = 2(z - 2x - y) + 4 \wedge z - 2x - y \geq -5\}$
  $y := z - 2 * x - y;$
  $\{x = 4 \wedge 2y + x = 2y + 4 \wedge y \geq -5\}$
  $z := 2 * y + x$
$\{INV \wedge \neg(y > 0)\}$
$\{y \geq -5)\}$

Per le PrePost:

1) Banali. Se $y < 30$, sicuramente è ≥ -5.

2) La tesi $x = 4$ è parte di INV. Per la seconda tesi, basta sostituire $x = 4$ e si ha l'uguaglianza $2(z - 2x - y) + x = 2(z - 2x - y) + 4$. Per la terza tesi, usando INV si ha:

$$z - 2x - y = 2y + 4 - 8 - y = y - 4 \geq -5$$

dove all'ultimo si è sfruttato $y > 0$.

3) La tesi è parte di INV.

□