Informatica — 2016-07-12

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

Esercizio 1. *Si dia la definizione dell'operatore delle conseguenze immediate $\hat{\mathcal{R}}$ e se ne dimostri la monotonia.*

Esercizio 2. *Siano c_1, c_2 due comandi arbitrari di IMP. Si definiscano:*

$$\begin{aligned} c_A &= (x := 1;\ c_2) \\ c_B &= (x := 0;\ \mathsf{if}\ x \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ (x := x+1; c_2)) \end{aligned}$$

I comandi c_A e c_B sono equivalenti. Si svolga la parte della dimostrazione della loro equivalenza espressa dalla seguente proprietà:

$$\forall \sigma, \sigma'. \qquad \langle c_A, \sigma\rangle \to_b \sigma' \implies \langle c_B, \sigma\rangle \to_b \sigma'$$

Soluzione (bozza). Assumiamo $\langle c_A, \sigma\rangle \to_b \sigma'$. Invertendolo, scopriamo che la derivazione ha necessariamente la forma seguente:

$$\dfrac{\dfrac{\overline{\langle 1, \sigma\rangle \to_e 1}}{\langle x := 1, \sigma\rangle \to_b \sigma[x \mapsto 1]}[Let] \qquad \dfrac{A}{\langle c_2, \sigma[x \mapsto 1]\rangle \to_b \sigma'}}{\langle c_A, \sigma\rangle \to_b \sigma'}[Comp]$$

dove A è una qualche derivazione.

Costruiamo quindi una derivazione per $\langle c_B, \sigma\rangle \to_b \sigma'$ come segue. Scriviamo i per il comando $\mathsf{if}\ x \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ (x := x+1; c_2)$.

$$\dfrac{\dfrac{\overline{\langle 0, \sigma\rangle \to_e 1}}{\langle x := 0, \sigma\rangle \to_b \sigma[x \mapsto 0]}[Let] \qquad \dfrac{\overline{\langle x, \sigma[x \mapsto 0]\rangle \to_e \sigma[x \mapsto 0](x) = 0} \qquad B}{\langle i, \sigma[x \mapsto 0]\rangle \to_b \sigma'}[If-F]}{\langle c_B, \sigma\rangle \to_b \sigma'}[Comp]$$

dove B è come segue:

$$\dfrac{\dfrac{\dfrac{\overline{\langle x, \sigma[x \mapsto 0]\rangle \to_e 0} \qquad \overline{\langle 1, \sigma[x \mapsto 0]\rangle \to_e 1}}{\langle x+1, \sigma[x \mapsto 0]\rangle \to_e 0+1 = 1}}{\langle x := x+1, \sigma[x \mapsto 0]\rangle \to_b \sigma[x \mapsto 1]}[Let] \qquad \dfrac{A}{\langle c_2, \sigma[x \mapsto 1]\rangle \to_b \sigma'}}{\langle x := x+1; c_2, \sigma[x \mapsto 0]\rangle \to_b \sigma'}[Comp]$$

Sopra, abbiamo usato il fatto che $\sigma[x \mapsto 0][x \mapsto 1] = \sigma[x \mapsto 1]$.

$\square$

Esercizio 3. *Sia $f \in (\mathbb{N} \to \mathbb{N})$ una funzione fissata. Si considerino le regole di inferenza:*

$$\dfrac{}{n}(n \in \mathbb{N})[T0] \qquad \dfrac{l \quad r}{(l, r)}[T1] \qquad \dfrac{}{n\ S\ n}[S0] \qquad \dfrac{l\ S\ n \qquad r\ S\ m}{(l, r)\ S\ (n+m)}[S1]$$

$$\dfrac{}{n\ R\ f(n)}[R0] \qquad \dfrac{l_1\ R\ l_2 \qquad r_1\ R\ r_2}{(l_1, r_1)\ R\ (l_2, r_2)}[R1]$$

Sopra, n, m sono naturali. Con l, r, t, u si indicano alberi binari di naturali, il cui insieme T è definito (induttivamente) da $[T0, T1]$. La relazione $S \in \mathcal{P}(T \times \mathbb{N})$, definita da $[S0, S1]$ vale tra t e n quando sommando tutti i naturali in t si ottiene n. La relazione $R \in \mathcal{P}(T \times T)$ è definita da $[R0, R1]$.

1. *[20%] Si enunci il principio di induzione su T.*
2. *[80%] Sia p la seguente proprietà sugli alberi $t \in T$*

$$p(t) : \qquad \forall m, u.\ t\ S\ m\ \wedge\ t\ R\ u \implies u\ S\ f(m)$$

Assumendo che valga $\forall n, m.\ f(n+m) = f(n) + f(m)$, si dimostri $\forall t \in T.\ p(t)$ per induzione su t.

Soluzione (bozza). Parte 1. Per dimostrare $p(t)$ per induzione su $t \in T$, basta dimostrare che

1. $\forall n \in \mathbb{N}.\ p(n)$
2. $\forall l, r.\ p(l) \wedge p(r) \implies p((l, r))$

Parte 2.
Nota: in questa soluzione enumeriamo, in modo un po' pedante, tutte le ipotesi che emergono durante la dimostrazione. È perfettamente accettabile anche una soluzione più succinta e informale, a patto che renda chiaro quando vengono usate le varie ipotesi.

Caso [T0]. Dobbiamo dimostrare $p(n)$ per ogni $n \in \mathbb{N}$, cioè:

$$\forall m, u.\ n\ S\ m\ \wedge\ n\ R\ u \implies u\ S\ f(m)$$

Assumiamo quindi $IP1:\ nSm$ e $IP2: nRu$, e dimostriamo la tesi $uSf(m)$.

Invertendo IP1, notiamo che può essere derivata solo da $[S0]$, che obbliga $m = n$.

Invertendo IP2, notiamo che può essere derivata solo da $[R0]$, che obbliga $u = f(n)$.

Con queste uguaglianze, possiamo riscrivere la tesi come $f(n)\ S\ f(n)$, che segue dalla regola $[S0]$.

Caso [T1]. Per ipotesi induttiva abbiamo che $IP1 : p(l)$ e che $IP2 : p(r)$. Dobbiamo dimostrare $p((l, r))$, cioè:

$$\forall m, u.\ (l, r)\ S\ m\ \wedge\ (l, r)\ R\ u \implies u\ S\ f(m)$$

Assumiamo quindi $IP3 : (l, r)\ S\ m$ e $IP4 : (l, r)\ R\ u$, e dimostriamo la tesi $u\ S\ f(m)$.

Invertendo IP3, notiamo che può essere derivata solo da $[S1]$, in questo modo:

$$\frac{lSa \qquad rSb}{(l, r)\ S\ (a + b)}[S1]$$

con qualche a, b tali che $a + b = m$. Dalle premesse otteniamo $IP5 : lSa$ e $IP6 : rSb$.

Invertendo IP4, notiamo che può essere derivata solo da $[R1]$, in questo modo:

$$\frac{l\ R\ l_2 \qquad r\ R\ r_2}{(l, r)\ R\ (l_2, r_2)}[R1]$$

con qualche l_2, r_2 tali che $(l_2, r_2) = u$. Dalle premesse otteniamo $IP7 : l\ R\ l_2$ e $IP8 : r\ R\ r_2$.

Dall'ipotesi induttiva IP1, scegliendo $m = a$ e $u = l_2$, abbiamo che

$$l\ S\ a\ \wedge\ l\ R\ l_2 \implies l_2\ S\ f(a)$$

Visto che l'antecedente segue da $IP5$ e $IP7$, ricaviamo $IP9 : l_2Sf(a)$.

Dall'ipotesi induttiva IP2, scegliendo $m = b$ e $u = r_2$, abbiamo che

$$r\ S\ b\ \wedge\ r\ R\ r_2 \implies r_2\ S\ f(b)$$

Visto che l'antecedente segue da $IP6$ e $IP8$, ricaviamo $IP10 : r_2Sf(b)$.

Infine, usando $IP9, IP10$, otteniamo

$$\frac{l_2Sf(a) \qquad r_2Sf(b)}{(l_2, r_2)S(f(a) + f(b))}[S1]$$

La conclusione sopra è proprio la tesi $uSf(m)$. Infatti, sappiamo che $(l_2, r_2) = u$ e anche che $f(a) + f(b)$ per ipotesi è $f(a + b)$ da cui si conclude con $m = a + b$. $\square$

Nome ________________________________ Matricola ____________

Esercizio 4. *Si dimostri formalmente la validità della tripla di Hoare seguente riempiendo le linee sottostanti con opportune asserzioni. (Suggerimento: provate $INV : \ldots \ \vee \ \ldots$)*

$\{x < y\}$

____

$n := 1;$

____

while $x < y$ do

  ____

  ____

  $n := n * n + n;$

  ____

  $x := x + 1;$

____

$\{n \ pari\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$\{x < y\}$ (1)
$\{(x < y \wedge 1 = 1) \vee n \text{ pari}\}$
$n := 1;$
$\{INV: \ (x < y \wedge n = 1) \vee n \text{ pari}\}$
while $x < y$ do
  $\{INV \wedge x < y\}$ (2)
  $\{(x + 1 < y \wedge n^2 + n = 1) \vee n^2 + n \text{ pari}\}$
  $n := n * n + n;$
  $\{(x + 1 < y \wedge n = 1) \vee n \text{ pari}\}$
  $x := x + 1;$
$\{INV \wedge \neg(x < y)\}$ (3)
$\{n \text{ pari}\}$

Per le PrePost:

1) Siccome $1 = 1$ vale, dall'ipotesi $x < y$ segue la parte sinistra di $(x < y \wedge 1 = 1) \vee n$ pari

2) Assumiamo INV e $x < y$. Procediamo per casi su INV. Se vale la parte sinistra di INV, si ha anche $n = 1$, da cui $n^2 + n = 2$ che è pari, e quindi la tesi (parte destra). Se vale la parte sinistra di INV, si ha n pari, quindi n^2 è pari, come lo è $n^2 + n$, da cui la tesi (parte destra).

3) Assumiamo INV e $\neg(x < y)$. La parte sinistra di INV non puó valere visto che implica $x < y$ che non vale per ipotesi. Quindi, deve valere necessariamente la parte destra di INV, che afferma che n è pari.

$\square$