Informatica — 2018-02-12

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. *Sia $A = \{-1, 1\}$. Le seguenti regole definiscono induttivamente l'insieme T degli alberi binari di numeri interi (regole $[T0], [T1]$) e una proprietà $R \in \mathcal{P}(T \times A \times T)$ (regole $[R0], [R1], [R2]$). Sotto, si usa $s, d \in T$, $x \in \mathbb{Z}$ e $a \in A$.*

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

$$\frac{R(s, 1, s')}{R((s,d), -1, (s', d))}[R1] \quad \frac{R(d, -1, d')}{R((s,d), 1, (s, d'))}[R2]$$

1. *[20%] Si forniscano $d \in T, a \in A$, tali per cui $R(((1,2),(3,4)), a, d)$ valga. Si giustifichi la risposta con una derivazione.*

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

3. *[1%] Si consideri l'enunciato seguente:*

$$\forall t_1, t_2, t_3 \in T.\ \forall a \in A.\ R(t_1, a, t_2) \land R(t_2, a, t_3) \implies t_1 = t_3$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma $\forall t_1 \in T.\ p(t_1)$ per un qualche predicato p.

4. *[59%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato ad T.*

Soluzione (bozza).
Parte 1.

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

Parte 2.
Per dimostrare $\forall t \in T.\ p(t)$ è sufficiente verificare che

$$\begin{array}{l} 1)\forall x \in \mathbb{Z}.\ p(x) \\ 2)\forall s, d.\ p(s) \land p(d) \implies p((s,d)) \end{array}$$

Parte 3.

Basta prendere

$$p(t_1) : \forall t_2, t_3 \in T.\ \forall a \in A.\ R(t_1, a, t_2) \wedge R(t_2, a, t_3) \implies t_1 = t_3$$

Parte 4. Procediamo per induzione su t_1.
(Caso $[T0]$**)**
Dato $x \in \mathbb{Z}$, bisogna dimostrare $p(x)$, ovvero che

$$\forall t_2, t_3 \in T.\ \forall a \in A.\ R(x, a, t_2) \wedge R(t_2, a, t_3) \implies x = t_3$$

Per farlo assumiamo $IP1 : R(x, a, t_2)$ e $IP2 : R(t_2, a, t_3)$ e dimostriamo $x = t_3$.

Invertendo $IP1$, siccome solo $[R0]$ può derivarlo, otteniamo $t_2 = ax$. Invertendo $IP2 : R(ax, a, t_3)$, siccome solo $[R0]$ può derivarlo, otteniamo $t_3 = a^2x$. Ora, siccome $a \in A$, si ha $a^2 = 1$ e quindi $t_3 = x$, da cui la tesi.
(Caso $[T1]$**)**
Come ipotesi induttive si hanno $p(s), p(d)$, ovvero:

$$\begin{aligned} IP1 &: \forall t_2, t_3 \in T.\ \forall a \in A.\ R(s, a, t_2) \wedge R(t_2, a, t_3) \implies s = t_3 \\ IP2 &: \forall t_2, t_3 \in T.\ \forall a \in A.\ R(d, a, t_2) \wedge R(t_2, a, t_3) \implies d = t_3 \end{aligned}$$

Dobbiamo quindi dimostrare $p((s, d))$, ovvero

$$\forall t_2, t_3 \in T.\ \forall a \in A.\ R((s, d), a, t_2) \wedge R(t_2, a, t_3) \implies (s, d) = t_3$$

Per farlo assumiamo

$$\begin{aligned} &IP3 : R((s, d), a, t_2) \\ &IP4 : R(t_2, a, t_3) \end{aligned}$$

e dimostriamo $(s, d) = t_3$.

Invertiamo $IP3$: può essere ricavata da $[R1]$ o da $[R2]$, quindi abbiamo due sottocasi.
(Sottocaso $[R1]$**)**
Qui si ha $a = -1$, $t_2 = (s', d)$ con $IP5 : R(s, 1, s')$. Invertendo $IP4 : R((s', d), -1, t_3)$, siccome solo $[R1]$ può ricavarlo, otteniamo $t_3 = (s'', d)$ e $IP6 : R(s', 1, s'')$.

Da $IP1$ (scegliendo $t_2 = s', t_3 = s'', a = 1$) si ha

$$R(s, 1, s') \wedge R(s', 1, s'') \implies s = s''$$

dove l'antecedente segue da $IP5, IP6$, quindi otteniamo $s = s''$.

La tesi segue perché $(s, d) = (s'', d) = t_3$.
(Sottocaso $[R2]$**)**
Questo caso è analogo a $[R1]$.

Qui si ha $a = 1$, $t_2 = (s, d')$ con $IP5 : R(d, -1, d')$. Invertendo $IP4 : R((s, d'), 1, t_3)$, siccome solo $[R2]$ può ricavarlo, otteniamo $t_3 = (s, d'')$ e $IP6 : R(d', -1, d'')$.

Da $IP2$ (scegliendo $t_2 = d', t_3 = d'', a = -1$) si ha

$$R(d, -1, d') \wedge R(d', -1, d'') \implies d = d''$$

dove l'antecedente segue da $IP5, IP6$, quindi otteniamo $d = d''$.

La tesi segue perché $(s, d) = (s, d'') = t_3$.

□

Esercizio 3. *Si consideri un'estensione di IMP fatta aggiungendo il comando* unless $e \neq 0$ do c *avente la seguente semantica intuitiva. Per iniziare, viene valutata la guardia $e \neq 0$. Se è vera, non si fa nulla. Se invece è falsa, viene eseguito il comando c.*

1. *[40%] Si formalizzi la semantica di* unless*, fornendo opportune regole di inferenza da aggiungere a quelle di IMP.*

2. *[60%] Usando le regole fornite sopra, si dimostri formalmente una delle due implicazioni che, insieme, esprimono l'equivalenza tra il comando* unless $e \neq 0$ do c *e il comando* if $e \neq 0$ then skip else c.

Soluzione (bozza).

Parte 1.

$$\frac{\langle e, \sigma \rangle \to_e v \neq 0}{\langle \mathsf{unless}\ e \neq 0\ \mathsf{do}\ c, \sigma \rangle \to_b \sigma}[Unless - True]$$

$$\frac{\langle e, \sigma \rangle \to_e 0 \qquad \langle c, \sigma \rangle \to_b \sigma'}{\langle \mathsf{unless}\ e \neq 0\ \mathsf{do}\ c,\ \sigma \rangle \to_b \sigma'}[Unless - False]$$

Parte 2.

Dimostriamo che

$$\langle \mathsf{unless}\ e \neq 0\ \mathsf{do}\ c,\ \sigma \rangle \to_b \sigma' \implies \langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ \mathsf{skip}\ \mathsf{else}\ c,\ \sigma \rangle \to_b \sigma'$$

Assumiamo $IP1 : \langle \mathsf{unless}\ e \neq 0\ \mathsf{do}\ c,\ \sigma \rangle \to_b \sigma'$. Invertendo $IP1$, notiamo che può essere generata da $[Unless - True]$ o $[Unless - False]$. Vediamo i due casi.

Caso $[Unless - True]$**.**

In questo caso $\sigma' = \sigma$ e $IP2 : \langle e, \sigma \rangle \to_e v \neq 0$. La tesi si ottiene da:

$$\frac{(IP2)\langle e, \sigma \rangle \to_e v \neq 0 \qquad \dfrac{}{\langle \mathsf{skip}, \sigma \rangle \to_b \sigma}[Skip]}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ \mathsf{skip}\ \mathsf{else}\ c,\ \sigma \rangle \to_b \sigma = \sigma'}[If - False]$$

Caso $[Unless - False]$**.**

In questo caso $IP2 : \langle e, \sigma \rangle \to_e 0$ e $IP3 : \langle c, \sigma \rangle \to_b \sigma'$ e La tesi si ottiene da:

$$\frac{(IP2)\langle e, \sigma \rangle \to_e 0 \qquad (IP3)\langle c, \sigma \rangle \to_b \sigma'}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ \mathsf{skip}\ \mathsf{else}\ c,\ \sigma \rangle \to_b \sigma'}[If - True]$$

□

Nome ________________________________ Matricola ____________

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

$\{a = 2A\}$

____

$b := 0;$

____

while $a \neq 0$ do

____

____

$a := a - 2;$

____

$b := b + 2$

____

$\{b = 2A\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$$
\begin{array}{l}
\{a = 2A\} \\
\{a + 0 = 2A\} \\
b := 0; \\
\{INV : a + b = 2A\} \\
\textsf{while } a \neq 0 \textsf{ do} \\
\qquad \{INV \wedge a \neq 0\} \\
\qquad \{(a-2) + (b+2) = 2A\} \\
\qquad a := a - 2; \\
\qquad \{a + (b+2) = 2A\} \\
\qquad b := b + 2 \\
\{INV \wedge \neg(a \neq 0)\} \\
\{b = 2A\}
\end{array}
$$

Per le PrePost:

1) banale aritmetica

2) banale aritmetica: basta semplificare $a - 2 + b + 2 = a + b$

3) Per ipotesi, $a = 0$, quindi l'invariante diventa $a + b = b = 2A$ che è la tesi.

□