Informatica — 2021-06-28

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

Esercizio 1. *Si enuncino, senza dimostrarli, i risultati relativi al determinismo e alla totalità della semantica delle espressioni di IMP ($\to_e$) e della semantica dei comandi big step di IMP ($\to_b$).*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi di interi (regole $[T0], [T1]$), una proprietà $S \in \mathcal{P}(T)$ (regole $[S0], [S1], [S2]$), e una relazione $R \in \mathcal{P}(T \times \mathbb{Z})$ (regole $[R0], [R1]$). Sotto, a, b indicano interi mentre t, t_1, t_2, s, d indicano alvberi in T.*

$$\frac{}{a}(a \in \mathbb{Z})[T0] \qquad \frac{s \quad d}{(s,d)}(a \in \mathbb{Z})[T1] \qquad \frac{a > 0}{S(a)}[S0] \qquad \frac{S(s)}{S((s,d))}[S1] \qquad \frac{S(d)}{S((s,d))}[S2]$$

$$\frac{}{R(a,a)}[R0] \qquad \frac{R(s,a)\ R(d,b)}{R((s,d), \max(a,b))}[R1]$$

1. *[20%] Si fornisca un albero t con 5 interi per cui valga $S(t) \wedge R(t, 10)$ e si giustifichi la risposta esibendo due derivazioni.*
2. *[20%] Si enunci il principio di induzione associato alla relazione R.*
3. *[10%] Si consideri l'enunciato seguente:*

   $$\forall t \in T, a \in \mathbb{Z}.\ S(t) \wedge R(t,a) \implies a > 0$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall t \in T, a \in \mathbb{Z}.\ R(t,a) \implies p(t,a)$$

   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

Un possibile albero è $t = ((-4, 10), (-5, (7, -1)))$.

$$\dfrac{\dfrac{\dfrac{}{S(10)}[S0]}{S((-4,10))[S2]}}{S(((-4,10),(-5,(7,-1))))}[S1]$$

$$\dfrac{\dfrac{\dfrac{}{R(-4,-4)} \quad \dfrac{}{R(10,10)}}{R((-4,10),10)} \quad \dfrac{\dfrac{}{R(-5,-5)} \quad \dfrac{\dfrac{}{R(7,7)} \quad \dfrac{}{R(-1,-1)}}{R((7,-1),7)}}{R((-5,(7,-1)),7)}}{R(((-4,10),(-5,(7,-1))),10)}$$

Parte 2

Per dimostrare che vale $p(t,a)$ per ogni t, a tali che $R(t,a)$ è sufficiente dimostrare che:

$R0)$ $\forall a \in \mathbb{Z}.\ p(a,a)$
$R1)$ $\forall s, d \in T, a \in \mathbb{Z}.\ p(s,a) \wedge p(d,b) \implies p((s,d), \max(a,b))$

Parte 3

Basta prendere

$$p(t,a) :\ S(t) \implies a > 0$$

Parte 4

Procediamo per induzione su R:

Caso $R0$

Dobbiamo dimostrare $p(a, a)$ per ogni $a \in \mathbb{Z}$, cioè:

$$S(a) \implies a > 0$$

Assumiamo $IP1 : S(a)$ e dimostriamo la nuova tesi $a > 0$.

Invertendo $IP1$, notiamo che può essere derivata solo dalla regola $[S0]$, e quindi ricaviamo $a > 0$ che è la tesi.

Caso $R1$

Assumiamo le ipotesi induttive $p(s, a)$ e $p(d, b)$, cioè:

$$\begin{array}{ll} IP1: & S(s) \implies a > 0 \\ IP2: & S(d) \implies b > 0 \end{array}$$

e dimostriamo la tesi $p((s, d), \max(a, b))$. Per farlo, assumiamo

$$IP3 : S((s, d))$$

e dimostriamo la nuova tesi $\max(a, b) > 0$.

Invertendo $IP3$, notiamo che può essere derivata solo da $[S1]$ o $[S2]$, quindi facciamo ambo i sottocasi.

Sottocaso [S1]

In questo caso otteniamo la premessa $S(s)$. Da questo e da $IP1$ ricaviamo $a > 0$. La tesi quindi segue da $\max(a, b) \geq a > 0$.

Sottocaso [S2]

In questo caso otteniamo la premessa $S(d)$. Da questo e da $IP2$ ricaviamo $b > 0$. La tesi quindi segue da $\max(a, b) \geq b > 0$.

□

Esercizio 3. *Si consideri la seguente relazione* $Q \in \mathcal{P}(Var \times Com)$*:*

$$Q = \{(x, c) \mid \forall \sigma, \sigma'.\ \langle c, \sigma\rangle \to_b \sigma' \implies \sigma(x) < \sigma'(x)\}$$

1. *[50%] Si dimostri la seguente proprietà:*

$$\forall x, c_1, c_2.\ xQc_1 \wedge xQc_2 \implies xQ(c_1; c_2)$$

2. *[50%] Si fornisca un comando* c *tale che* $\forall x \in Var.\ xQc$*. Si giustifichi la risposta.*

Soluzione (bozza). Parte 1

Assumiamo $IP1 : xQc_1$, $IP2 : xQc_2$, ovvero

$$\begin{array}{ll} IP1: & \forall \sigma_1, \sigma_1'.\ \langle c_1, \sigma_1\rangle \to_b \sigma_1' \implies \sigma_1(x) < \sigma_1'(x) \\ IP2: & \forall \sigma_2, \sigma_2'.\ \langle c_2, \sigma_2\rangle \to_b \sigma_2' \implies \sigma_2(x) < \sigma_2'(x) \end{array}$$

e dimostriamo la tesi $xQ(c_1; c_2)$. Per farlo, prendiamo σ, σ' arbitrari, assumiamo $IP3 : \langle c_1; c_2, \sigma\rangle \to_b \sigma'$ e dimostriamo la nuova tesi $\sigma(x) < \sigma'(x)$.

Invertendo $IP3$, notiamo che può solo essere ricavata con la regola $[Comp]$, e quindi otteniamo che per qualche σ'' si ha:

$$\begin{array}{ll} IP4: & \langle c_1, \sigma\rangle \to_b \sigma'' \\ IP5: & \langle c_2, \sigma''\rangle \to_b \sigma' \end{array}$$

Usiamo quindi $IP1$ scegliendo $\sigma_1 = \sigma, \sigma_1' = \sigma''$ assieme a $IP4$, e otteniamo $\sigma(x) < \sigma''(x)$.

Analogamente, usiamo $IP2$ scegliendo $\sigma_2 = \sigma'', \sigma_2' = \sigma'$ assieme a $IP5$, e otteniamo $\sigma(x)'' < \sigma'(x)$.

Dalle due disequazioni precedente otteniamo la tesi: $\sigma(x) < \sigma(x)'' < \sigma'(x)$.

Parte 2

Per ottenere la proprietà desiderata è sufficiente (e pure necessario) prendere un comando c che non termina mai, come per esempio $c = (\mathsf{while}\ 1 \neq 0\ \mathsf{do\ skip})$. In questo caso, qualunque sia $x \in Var$, vale l'implicazione

$$\langle c, \sigma \rangle \to_b \sigma' \implies \sigma(x) < \sigma'(x)$$

perché l'antecedente è falsa.

□

Nome _____ Matricola _____

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

$\{\mathsf{vero}\}$

$x := 1;$

$n := 1;$

$\mathsf{while}\ n \leq N\ \mathsf{do}$

$x := n * x;$

$n := n + 2$

$\{x\ \textit{dispari}\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

Soluzione (bozza).

$\{\mathsf{vero}\}$ (1)
$\{1 \text{ dispari} \wedge 1 \text{ dispari}\}$
$x := 1;$
$\{x \text{ dispari} \wedge 1 \text{ dispari}\}$
$n := 1;$
$\{INV : \ x \text{ dispari} \wedge n \text{ dispari}\}$
$\mathsf{while}\ n \leq N\ \mathsf{do}$
    $\{INV \wedge n \leq N\}$ (2)
    $\{nx \text{ dispari} \wedge n + 2 \text{ dispari}\}$
    $x := n * x;$
    $\{x \text{ dispari} \wedge n + 2 \text{ dispari}\}$
    $n := n + 2$
$\{INV \wedge \neg(n \leq N)\}$ (3)
$\{x \text{ dispari}\}$

PrePost:
1) Banale aritmetica.
2) Per INV, sia n che x sono dispari, quindi $n * x$ e $n + 2$ sono dispari.
3) La tesi è parte dell'ipotesi INV.

□