Informatica — 2019-01-18

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* ($\rightarrow_e$) *e della semantica dei comandi big step di IMP* ($\rightarrow_b$).

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi di numeri naturali (regole* $[T0], [T1]$*) e una relazione* $Q \in \mathcal{P}(T \times \mathbb{N})$ *(regole* $[Q0], [Q1], [Q2]$*). Sotto, n, m indicano naturali mentre s, d indicano alberi in T.*

$$\frac{}{n}(n \in \mathbb{N})[T0] \qquad \frac{s \quad d}{(s,d)}[T1]$$

$$\frac{}{Q(n,n)}[Q0] \qquad \frac{Q(s,n) \quad Q(d,m) \quad n \geq m}{Q((s,d),n)}[Q1] \qquad \frac{Q(s,n) \quad Q(d,m) \quad m > n}{Q((s,d),m)}[Q2]$$

1. *[20%] Si fornisca un albero t contenente almeno 3 naturali per cui valga $Q(t,7)$ e si giustifichi la risposta esibendo una derivazione.*
2. *[20%] Si enunci il principio di induzione associato alla relazione Q.*
3. *[10%] Si consideri l'enunciato seguente:*

$$\forall t \in T.\ \forall n, m \in \mathbb{N}.\ Q(t,n) \land Q(t,m) \implies n = m$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t \in T.\ \forall n \in \mathbb{N}.\ Q(t,n) \implies p(t,n)$$

per un qualche predicato p.

4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a Q. Nel farlo, potete tralasciare il caso del principio di induzione relativo a $[Q2]$.*

Soluzione (bozza).
Parte 1. Per esempio,

$$\frac{\dfrac{\dfrac{}{Q(1,1)}[Q0] \quad \dfrac{}{Q(2,2)}Q0] \quad 2 > 1}{Q((1,2),2)}[Q2] \quad \dfrac{}{Q(7,7)}[Q0] \quad 7 > 2}{Q(((1,2),7),7)}[Q2]$$

Parte 2. Per potere dimostrare che, per ogni t, n tali che $Q(t,n)$ vale che $p(t,n)$, è sufficiente dimostrare che:

$Q0)$ $\forall n \in \mathbb{N}.\ p(n,n)$
$Q1)$ $\forall n, m \in \mathbb{N}, s, d \in T.\ p(s,n) \land p(d,m) \land n \geq m \implies p((s,d),n)$
$Q2)$ $\forall n, m \in \mathbb{N}, s, d \in T.\ p(s,n) \land p(d,m) \land m > n \implies p((s,d),m)$

Parte 3. Basta scegliere

$$p(t,n):\ \forall m \in \mathbb{N}.\ Q(t,m) \implies n = m$$

Parte 4. Applichiamo quindi il principio di induzione su Q. Abbiamo tre casi da dimostrare.

Caso $[Q0]$**.** Senza ipotesi induttive, dobbiamo dimostrare $p(n,n)$. Quindi, assumendo $IP1 : Q(n,m)$, dobbiamo dimostrare che $n = m$.

Invertendo $IP1$, si osserva che può essere derivata solo dalla regola $[Q0]$, e quindi $n = m$.

Caso $[Q1]$**.** Come ipotesi induttive assumiamo $IP1 : p(s, n)$, $IP2 : p(d, m)$. Riscritte, diventano:

$$IP1 : \ \forall m_1 \in \mathbb{N}.\ Q(s, m_1) \implies n = m_1$$
$$IP2 : \ \forall m_2 \in \mathbb{N}.\ Q(d, m_2) \implies m = m_2$$

Assumiamo anche la condizione a lato $IP3 : n \geq m$. Dobbiamo dimostrare la tesi $p((s, d), n)$, ovvero

$$\forall \bar{m} \in \mathbb{N}.\ Q((s, d), \bar{m}) \implies n = \bar{m}$$

Assumiamo quindi $IP4 : Q((s, d), \bar{m})$, e dimostriamo la nuova tesi $n = \bar{m}$.

Invertendo $IP4$, osserviamo che non può essere derivata dalla regola $[Q0]$, in quanto (s, d) non è un albero costituito da un solo naturale. È invece possibile che sia derivata usando le regole $[Q1]$ e $[Q2]$, quindi consideriamo i sottocasi.

Inversione, sottocaso $[Q1]$. Dall'inversione, ricaviamo $IP5 : Q(s, \bar{m})$, $IP6 : Q(d, m')$ e $IP7 : \bar{m} \geq m'$.

Usando $IP1$ (scegliendo $m_1 = \bar{m}$), ricaviamo

$$Q(s, \bar{m}) \implies n = \bar{m}$$

L'antecedente è $IP5$, quindi otteniamo $n = \bar{m}$ che è la tesi.

Inversione, sottocaso $[Q2]$. Dall'inversione, ricaviamo $IP5 : Q(s, n')$, $IP6 : Q(d, \bar{m})$ e $IP7 : \bar{m} > n'$.

Usando $IP1$ (scegliendo $m_1 = n'$), ricaviamo

$$Q(s, n') \implies n = n'$$

L'antecedente è $IP5$, quindi otteniamo $n = n'$.

Usando $IP2$ (scegliendo $m_2 = \bar{m}$), ricaviamo

$$Q(d, \bar{m}) \implies m = \bar{m}$$

L'antecedente è $IP6$, quindi otteniamo $m = \bar{m}$.

Alla luce di quanto detto possiamo riscrivere $IP7$ come $m > n$, ma questo contraddice $IP3 : n \geq m$. Avendo trovato un assurdo, la tesi segue (qualunque essa sia).

Caso $[Q2]$**.** Analogo al caso $[Q1]$. (Inoltre, non richiesto dal testo dell'esercizio.)

□

Esercizio 3. *Si consideri una variante del linguaggio delle* espressioni *di IMP, definito come segue. Le costanti numeriche sono numeri razionali $a \in \mathbb{Q}$. Analogamente, il valore delle variabili $x \in Var$ è un numero razionale, dato dallo stato $\sigma \in State$, con $State = (Var \to \mathbb{Q})$. Il linguaggio include le operazioni aritmetiche usuali* $e_1 + e_2$, $e_1 - e_2$, $e_1 * e_2$ *ed* e_1/e_2.

La valutazione delle espressioni viene fatta secondo il normale significato degli operatori aritmetici, tranne nel caso in cui si divide per zero, in cui il risultato è invece posto convenzionalmente ad un valore speciale di errore $\mathsf{err} \notin \mathbb{Q}$. *La semantica delle espressioni, soddisfa quindi le seguenti proprietà.*

$$(\to_e) \in \mathcal{P}(Exp \times State \times (\mathbb{Q} \cup \{\mathsf{err}\}))$$

$A)$ $\langle 5/(7-3), \sigma\rangle \to_e 5/4$	$B)$ $\langle (x + (1/3)) * 2, \sigma\rangle \to_e 4/3$ *se* $\sigma(x) = 1/3$
$C)$ $\langle 3/(5-5), \sigma\rangle \to_e \mathsf{err}$	$D)$ $\langle 100 + (1/(x-2)), \sigma\rangle \to_e \mathsf{err}$ *se* $\sigma(x) = 2$

1. *[70%] Si definisca tale semantica formalmente, fornendo opportune regole di inferenza. Per brevità, se alcune regole sono perfettamente analoghe ad altre, potete fare notare l'analogia ed evitare di scriverle.*

2. [30%] Si esibisca una derivazione per l'esempio D di sopra.

Soluzione (bozza).
Parte 1.

$$\frac{}{\langle a, \sigma\rangle \to_e a}[Lit] \qquad \frac{}{\langle x, \sigma\rangle \to_e \sigma(x)}[Var]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \textsf{err}}{\langle e_1 + e_2, \sigma\rangle \to_e \textsf{err}}[Plus - Err1] \qquad \frac{\langle e_2, \sigma\rangle \to_e \textsf{err}}{\langle e_1 + e_2, \sigma\rangle \to_e \textsf{err}}[Plus - Err2]$$

$$\frac{\langle e_1, \sigma\rangle \to_e a_1 \neq \textsf{err} \quad \langle e_2, \sigma\rangle \to_e a_2 \neq \textsf{err}}{\langle e_1 + e_2, \sigma\rangle \to_e a_1 + a_2}[Plus - OK]$$

$$\frac{\langle e_1, \sigma\rangle \to_e \textsf{err}}{\langle e_1 / e_2, \sigma\rangle \to_e \textsf{err}}[Div - Err1] \qquad \frac{\langle e_2, \sigma\rangle \to_e \textsf{err}}{\langle e_1 / e_2, \sigma\rangle \to_e \textsf{err}}[Div - Err2]$$

$$\frac{\langle e_2, \sigma\rangle \to_e 0}{\langle e_1 / e_2, \sigma\rangle \to_e \textsf{err}}[Div - Err3]$$

$$\frac{\langle e_1, \sigma\rangle \to_e a_1 \neq \textsf{err} \quad \langle e_2, \sigma\rangle \to_e a_2 \neq \textsf{err} \quad a_2 \neq 0}{\langle e_1 / e_2, \sigma\rangle \to_e a_1 / a_2}[Div - OK]$$

Le regole per $*$ e $-$ sono analoghe a quelle per il $+$.
Parte 2.

$$\frac{\dfrac{\dfrac{\dfrac{}{\langle x, \sigma\rangle \to_e \sigma(x) = 2}[Var] \qquad \dfrac{}{\langle 2, \sigma\rangle \to_e 2}[Lit]}{\langle x - 2, \sigma\rangle \to_e 2 - 2 = 0}[Sub - OK]}{\langle 1/(x-2), \sigma\rangle \to_e \textsf{err}}[Div - Err3]}{\langle 100 + (1/(x-2)), \sigma\rangle \to_e \textsf{err}}[Plus - Err2]$$

$\square$

Nome ______________________________________ Matricola ______________

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

$\{n = N \geq 0\}$

____

$x := 1;$

____

$y := 0;$

____

while $x \neq 0$ do

    ____

    ____

    if $y = n$ then

        ____

        ____

        $x := 0$

    else

        ____

        ____

        $y := y + 1$

____

$\{y = N\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

Soluzione (bozza).

$\{n = N \geq 0\}$
$\{n = N \wedge (1 = 0 \implies 0 = N)\}$ (1)
$x := 1;$
$\{n = N \wedge (x = 0 \implies 0 = N)\}$
$y := 0;$
$\{INV : n = N \wedge (x = 0 \implies y = N)\}$
while $x \neq 0$ do
  $\{INV \wedge x \neq 0\}$
  if $y = n$ then
    $\{INV \wedge x \neq 0 \wedge y = n\}$
    $\{n = N \wedge (0 = 0 \implies y = N)\}$ (2)
    $x := 0$
  else
    $\{INV \wedge x \neq 0 \wedge \neg(y = n)\}$
    $\{n = N \wedge (x = 0 \implies y + 1 = N)\}$ (3)
    $y := y + 1$
$\{INV \wedge \neg(x \neq 0)\}$
$\{y = N\}$ (4)

Per le PrePost:

1) La tesi $n = N$ fa parte delle ipotesi, mentre $1 = 0$ è falso e quindi implica qualunque cosa.

2) La tesi $n = N$ fa parte dell'ipotesi INV. Assumendo il banale $0 = 0$, dobbiamo dimostrare che $y = N$, ma questo segue immediatamente dalle ipotesi $y = n$ e $n = N$.

3) La tesi $n = N$ fa parte dell'ipotesi INV. Per l'altra tesi, assumendo $x = 0$ dobbiamo fare vedere $y + 1 = N$. Per far questo, basta osservare che $x = 0$ è falsa in quanto $x \neq 0$ per ipotesi, e quindi implica qualunque cosa.

4) Per ipotesi si ha $\neg(n \neq 0)$ e quindi $x = 0$. Da questo e da INV $(x = 0 \implies y = N)$, si ha $y = N$ che è la tesi.

□