Informatica — 2023-07-24

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

Esercizio 1. *Si enunci e dimostri il teorema di Knaster-Tarski.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi di naturali (regole $[T0], [T1]$), una relazione $R \in \mathcal{P}(T \times T)$ (regole $[R0], [R1], [R2]$), e un predicato $Q \in \mathcal{P}(T)$ (regole $[Q0], [Q1]$), Sotto, n, m, k indicano naturali, mentre s, d, t, u indicano alberi in T.*

$$\frac{}{n}(n \in \mathbb{N})[T0] \quad \frac{s \quad d}{(s,d)}[T1] \quad \frac{}{Q(n)}(n < 100)[Q0] \quad \frac{Q(t_1) \quad Q(t_2)}{Q((t_1,t_2))}[Q1]$$

$$\frac{}{R(n+m,(n,m))}[R0] \quad \frac{R(t_1,u_1) \quad R(t_2,u_2)}{R((t_1,t_2),(u_1,u_2))}[R1] \quad \frac{R(t_1,t_2) \quad R(t_2,t_3)}{R(t_1,t_3)}[R2]$$

1. *[20%] Si trovi un albero t con almeno tre naturali tale per cui valga $R(25, t)$. Si giustifichi la risposta esibendo una derivazione.*
2. *[20%] Si enunci il principio di induzione associato alla relazione R.*
3. *[10%] Si consideri l'enunciato seguente:*

$$\forall t, u \in T.\ Q(t) \land R(t,u) \implies Q(u)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t, u \in T.\ R(t,u) \implies p(t,u)$$

per un qualche predicato p.

4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione <u>associato a R</u>.*

Soluzione (bozza).
Parte 1.
Una possibile soluzione è:

$$\cfrac{\cfrac{}{R(25,(10,15))}[R0] \quad \cfrac{\cfrac{}{R(10,(3,7))}[R0] \quad \cfrac{}{R(15,(2,13))}[R0]}{R((10,15),((3,7),(2,13)))}[R1]}{R(25,((3,7),(2,13)))}[R2]$$

Parte 2. Affinché valga $\forall t, u. R(t,u) \implies p(t,u)$ è sufficiente che

$$\begin{array}{ll} R0) & \forall n, m \in \mathbb{N}.\ p(n+m,(n,m)) \\ R1) & \forall t_1, t_2, u_1, u_2 \in T.\ p(t_1,u_1) \land p(t_2,u_2) \implies p((t_1,t_2),(u_1,u_2)) \\ R2) & \forall t_1, t_2, t_3 \in T.\ p(t_1,t_2) \land p(t_2,t_3) \implies p(t_1,t_3) \end{array}$$

Parte 3. Basta prendere

$$p(t,u) :\ Q(t) \implies Q(u)$$

Parte 4.
Caso $[R0]$. Dobbiamo dimostrare $p(n+m,(n,m))$ e quindi $Q(n+m) \implies Q((n,m))$. Assumiamo $IP1 : Q(n+m)$ e dimostriamo la nuova tesi $Q((n,m))$.

Invertendo $IP1$, siccome si ricava solo dalla regola $[Q0]$, ricaviamo $n + m < 100$. Siccome n, m sono naturali, si ha pure $n < 100$ e $m < 100$. Applicando a questi ultimi la regola $[Q0]$ si ha $Q(n)$ e $Q(m)$, da cui applicando la regola $[Q1]$ si ottiene la tesi $Q((n,m))$.

Caso $[R1]$. Assumiamo come ipotesi induttive $p(t_1, u_1)$ e $p(t_2, u_2)$ e cioè

$$\begin{array}{ll} IP1: & Q(t_1) \implies Q(u_1) \\ IP2: & Q(t_2) \implies Q(u_2) \end{array}$$

Dobbiamo dimostrare $p((t_1, t_2), (u_1, u_2))$ e cioè

$$Q((t_1, t_2)) \implies Q((u_1, u_2))$$

Assumiamo quindi $IP3 : Q((t_1, t_2))$ e dimostriamo la nuova tesi $Q((u_1, u_2))$.

Invertendo $IP3$, siccome si ricava solo dalla regola $[Q1]$, ricaviamo $IP4 : Q(t_1)$ e $IP5 : Q(t_2)$.

Usando $IP1$ e $IP4$ si ricava $IP6 : Q(u_1)$. Usando $IP2$ e $IP5$ si ricava $IP7 : Q(u_2)$.

Applicando a $IP6, IP7$ la regola $[Q1]$ si ha $Q((u_1, u_2))$ che è la tesi.

Caso $[R2]$. Assumiamo come ipotesi induttive $p(t_1, t_2)$ e $p(t_2, t_3)$ e cioè

$$\begin{array}{ll} IP1: & Q(t_1) \implies Q(t_2) \\ IP2: & Q(t_2) \implies Q(t_3) \end{array}$$

Dobbiamo dimostrare $p(t_1, t_3)$ e cioè

$$Q(t_1) \implies Q(t_3)$$

La tesi deriva immediatamente da $IP1, IP2$ per la transitività dell'implicazione.

□

Esercizio 3. *Dato σ uno stato di IMP, indichiamo con $\sigma[+1]$ lo stato ottenuto da σ aumentando di uno il valore di tutte le variabili. Si ha quindi $\sigma[+1](x) = \sigma(x) + 1$ per ogni $x \in Var$. Si consideri una variante della semantica di IMP nella quale il ciclo* while $e \neq 0$ do c *ripete l'esecuzione di c come di consueto, ma lo fa incrementando il valore di tutte le variabili sia subito prima di ogni esecuzione di c, sia all'uscita del ciclo. In ogni caso la guardia viene controllata prima dell'incremento. Per esempio, se nello stato iniziale tutte le variabili valgono zero, eseguendo* while $x - 3 \neq 0$ do $y := y + z$ *si arriva in uno stato finale σ' dove $\sigma'(x) = 4$, $\sigma'(z) = 4$, $\sigma'(y) = (1 + 1) + (1 + 2) + (1 + 3) + 1 = 10$.*

1. *[50%] Si formalizzi tale semantica del* while *con opportune regole di inferenza.*
2. *[50%] Si fornisca un comando c che, con la semantica alternativa, calcoli il fattoriale di un naturale n nel senso seguente:*

   $$\forall \sigma.\ \sigma(n) \geq 0 \implies \exists \sigma'.\ \langle c, \sigma\rangle \to_b \sigma' \wedge \sigma'(x) = \sigma(n)!$$

   Si giustifichi informalmente la risposta.

Soluzione (bozza).
Parte 1.

$$\frac{\langle e,\ \sigma\rangle \to_e v \neq 0 \qquad \langle c; \mathsf{while}\ e \neq 0\ \mathsf{do}\ c,\ \sigma[+1]\rangle \to_b \sigma'}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c,\ \sigma\rangle \to_b \sigma'}[While - True]$$

$$\frac{\langle e,\ \sigma\rangle \to_e 0}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c,\ \sigma\rangle \to_b \sigma[+1]}[While - True]$$

Parte 2.

Basta decrementare tutte le variabili in uso all'inizio di ogni iterazione del ciclo, e subito dopo l'uscita del ciclo, per potere scrivere un programma simile a quello che si userebbe in IMP non modificato.

$x := 1;$
while $n \neq 0$ do
    $n := n - 1;$
    $x := x - 1;$
    $x := x * n;$
    $n := n - 1;$
$x := x - 1$

$\square$

Nome ______________________________________ Matricola ______________

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

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

____

$x := 0;$

____

$y := 1;$

____

while $x < n$ do

    ____

    ____

    $z := 6 * x;$

    ____

    $y := y + 2 * (z * x - 1);$

    ____

    $x := x + 1$

____

$\{y = 4N^3 - 6N^2 + 1\}$

Si giustifichino qui sotto gli eventuali usi della regola *PrePost*.

____

____

____

____

____

____

____

Soluzione (bozza).

$\{n = N \geq 0\}$ (1)
$\{0 \leq n = N \wedge 1 = 40^3 - 60^2 + 1\}$
$x := 0;$
$\{x \leq n = N \wedge 1 = 4x^3 - 6x^2 + 1\}$
$y := 1;$
$\{INV : x \leq n = N \wedge y = 4x^3 - 6x^2 + 1\}$
while $x < n$ do
$\{INV \wedge x < n\}$ (2)
$\{x + 1 \leq n = N \wedge y + 2((6x)x - 1) = 4(x + 1)^3 - 6(x + 1)^2 + 1\}$
$z := 6 * x;$
$\{x + 1 \leq n = N \wedge y + 2(zx - 1) = 4(x + 1)^3 - 6(x + 1)^2 + 1\}$
$y := y + 2 * (z * x - 1);$
$\{x + 1 \leq n = N \wedge y = 4(x + 1)^3 - 6(x + 1)^2 + 1\}$
$x := x + 1$
$\{INV \wedge \neg(x < n)\}$ (3)
$\{y = 4N^3 - 6N^2 + 1\}$

Per le PrePost:

1) Banale aritmetica.

2) Da $x < n$ segue $x + 1 \leq n$ visto che sono interi. La parte $n = N$ è una delle ipotesi. L'equazione $y+2((6x)x-1) = 4(x+1)^3-6(x+1)^2+1$ si semplifica in $y+12x^2-2 = 4(x^3+3x^2+3x+1)-6(x^2+2x+1)+1$ che si semplifica in $y = 4(x^3+1)-6(x^2+1)+3 = 4x^3-6x^2+1$ che è una delle ipotesi.

3) Da INV e $\neg(x < n)$ segue $x = n$ che con INV implica $x = N$. Sempre da INV si ricava quindi $y = 4N^3 - 6N^2 + 1$.

□