Informatica — 2018-07-23

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

Esercizio 1. *Si considerino le semantiche delle espressioni $\to_e$ e dei comandi $\to_b$ (big step) di IMP. Si forniscano i relativi enunciati dei risultati di totalità e non-totalità, descrivendoli brevemente.*

Esercizio 2. *Sia $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ una funzione tale per cui, per ogni $a, b, c \in \mathbb{N}$ si ha $g(a, g(b, c)) = g(g(a, b), c)$ e $g(a+1, b+1) = g(a, b)+1$. Le seguenti regole definiscono induttivamente l'insieme T degli alberi binari di numeri naturali (regole $[T0], [T1]$) e una proprietà $R \in \mathcal{P}(T \times \mathbb{N} \times T)$ (regole $[R0], [R1]$). Sotto, si usano le variabili $t, s, d, s', d' \in T$, $n, k \in \mathbb{N}$.*

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

$$\frac{}{R(n, k, g(n, k))}[R0] \qquad \frac{R(s, k, s') \qquad R(d, k, d')}{R((s, d), k + 1, (s', d'))}[R1]$$

1. *[20%] Si fornisca un $t \in T$, tale per cui $R(((1, 2), 3), 4, t)$ valga. Si giustifichi la risposta con una derivazione.*
2. *[20%] Si enunci il principio di induzione associato all'insieme degli alberi T.*
3. *[60%] Si dimostri l'enunciato seguente*

   $$\forall t_1, t_2, t_3 \in T.\, \forall k_1, k_2 \in \mathbb{N}.\, R(t_1, k_1, t_2) \wedge R(t_2, k_2, t_3) \implies R(t_1, g(k_1, k_2), t_3)$$

   per induzione su $t_1 \in T$ (quindi usando il principio di induzione associato ad T).

Soluzione (bozza).
Parte 1.

$$\dfrac{\dfrac{\dfrac{}{R(1,2,g(1,2))} \qquad \dfrac{}{R(2,2,g(2,2))}}{R((1,2),3,(g(1,2),g(2,2)))} \qquad \dfrac{}{R(3,3,g(3,3))}}{R(((1,2),3),4,((g(1,2),g(2,2)),g(3,3)))}$$

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

$$\begin{array}{ll} T0) & \forall n \in \mathbb{N}.\ p(n) \\ T1) & \forall s, d.\ p(s) \wedge p(d) \implies p((s, d)) \end{array}$$

Parte 3.
Dimostriamo quindi $\forall t_1 \in T.p(t_1)$ dove p è dato da

$$p(t_1) : \forall t_2, t_3 \in T.\, \forall k_1, k_2 \in \mathbb{N}.\, R(t_1, k_1, t_2) \wedge R(t_2, k_2, t_3) \implies R(t_1, g(k_1, k_2), t_3)$$

procedendo per induzione su $t_1 \in T$.

(Caso $[T0]$**)** Dato $n \in \mathbb{N}$, bisogna dimostrare $p(n)$, ovvero che

$$\forall t_2, t_3 \in T.\ \forall k_1, k_2 \in \mathbb{N}.\ R(n, k_1, t_2) \wedge R(t_2, k_2, t_3) \implies R(n, g(k_1, k_2), t_3)$$

Per farlo assumiamo $IP1 : R(n, k_1, t_2)$ e $IP2 : R(t_2, k_2, t_3)$ e dimostriamo $R(n, g(k_1, k_2), t_3)$.

Invertendo $IP1$, siccome solo $[R0]$ può derivarlo (n non è una coppia), otteniamo $t_2 = g(n, k_1)$.

Di qui, $IP2$ diventa $R(g(n, k_1), k_2, t_3)$. Invertendo questo, siccome solo $[R0]$ può derivarlo ($g(n, k_1)$ non è una coppia), otteniamo $t_3 = g(g(n, k_1), k_2)$. Sfruttando le ipotesi su g, abbiamo anche che $t_3 = g(n, g(k_1, k_2))$.

La tesi si può riscrivere quindi come $R(n, g(k_1, k_2), g(n, g(k_1, k_2)))$ che segue da $[R0]$.

(Caso $[T1]$**)** Come ipotesi induttive si hanno $p(s)$ e $p(d)$, ovvero:

$$IP1 : \forall \bar{t}_2, \bar{t}_3 \in T.\ \forall \bar{k}_1, \bar{k}_2 \in \mathbb{N}.\ R(s, \bar{k}_1, \bar{t}_2) \wedge R(\bar{t}_2, \bar{k}_2, \bar{t}_3) \implies R(s, g(\bar{k}_1, \bar{k}_2), \bar{t}_3)$$
$$IP2 : \forall \hat{t}_2, \hat{t}_3 \in T.\ \forall \hat{k}_1, \hat{k}_2 \in \mathbb{N}.\ R(d, \hat{k}_1, \hat{t}_2) \wedge R(\hat{t}_2, \hat{k}_2, \hat{t}_3) \implies R(d, g(\hat{k}_1, \hat{k}_2), \hat{t}_3)$$

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

$$\forall t_2, t_3 \in T.\ \forall k_1, k_2 \in \mathbb{N}.\ R((s, d), k_1, t_2) \wedge R(t_2, k_2, t_3) \implies R((s, d), g(k_1, k_2), t_3)$$

Per farlo assumiamo $IP3 : R((s, d), k_1, t_2)$ e $IP4 : R(t_2, k_2, t_3)$ e dimostriamo la tesi $R((s, d), g(k_1, k_2), t_3)$.

Invertiamo $IP3$: può essere ricavata da solo da $[R1]$ ((s, d) non è un naturale), nel modo seguente:

$$\frac{R(s, k_1', s') \qquad R(d, k_1', d')}{R((s, d), k_1' + 1, (s', d'))}[R2]$$

Quindi otteniamo che $k_1 = k_1' + 1$, $t_2 = (s', d')$, $IP5 : R(s, k_1', s')$ e $IP6 : R(d, k_1', d')$.

Ora $IP4$ si riscrive come $IP4 : R((s', d'), k_2, t_3)$. Invertiamo anche questo: può essere ricavata da solo da $[R1]$ ((s', d') non è un naturale), nel modo seguente:

$$\frac{R(s', k_2', s'') \qquad R(d', k_2', d'')}{R((s', d'), k_2' + 1, (s'', d''))}[R2]$$

Quindi otteniamo che $k_2 = k_2' + 1$, $t_3 = (s'', d'')$, $IP7 : R(s', k_2', s'')$ e $IP8 : R(d', k_2', d'')$.

Ora, usiamo le ipotesi induttive. Da $IP1$, con $\bar{t}_2 = s', \bar{t}_3 = s'', \bar{k}_1 = k_1', \bar{k}_2 = k_2'$, sfruttando $IP5$ e $IP7$ otteniamo $IP9 : R(s, g(k_1', k_2'), s'')$. Analogamente, da $IP2$, con $\hat{t}_2 = d', \hat{t}_3 = d'', \hat{k}_1 = k_1', \hat{k}_2 = k_2'$, sfruttando $IP6$ e $IP8$ otteniamo $IP10 : R(d, g(k_1', k_2'), d'')$.

Da $IP9, IP10$, usando la regola $[R1]$ otteniamo $R((s, d), g(k_1', k_2') + 1, (s'', d''))$ che è equivalente a $R((s, d), g(k_1', k_2') + 1, t3)$. Per le proprietà di g, questa si riscrive come $R((s, d), g(k_1' + 1, k_2' + 1), t3)$ e cioè $R((s, d), g(k_1, k_2), t3)$ che è la tesi.

$\square$

Esercizio 3. *Sia dato un insieme U e due funzioni $f, g : \mathcal{P}(U) \to \mathcal{P}(U)$, entrambe monotone, e aventi minimi punti fissi $\mathsf{fix}(f), \mathsf{fix}(g)$. Assumendo che $\forall X.\ f(X) \subseteq g(X)$, si dimostri che $\mathsf{fix}(f) \subseteq \mathsf{fix}(g)$.*

Soluzione (bozza). Applicando il principio di induzione su $\mathsf{fix}(f)$, otteniamo che per ogni X:

$$f(X) \subseteq X \implies \mathsf{fix}(f) \subseteq X$$

quindi, in particolare, scegliendo $X = \mathsf{fix}(g)$:

$$f(\mathsf{fix}(g)) \subseteq \mathsf{fix}(g) \implies \mathsf{fix}(f) \subseteq \mathsf{fix}(g)$$

Per concludere, basta quindi verificare l'antecedente, che segue da

$$f(\mathsf{fix}(g)) \subseteq g(\mathsf{fix}(g)) = \mathsf{fix}(g)$$

Sopra, l'inclusione vale per ipotesi, mentre l'uguaglianza deriva dalla definizione di punto fisso di g. $\square$

Nome ______________________________ Matricola ___________

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

$\{a = A\}$

____

$b := 0;$

____

$q := 0;$

____

while $b \neq a$ do

____

____

$c := 2 * b + 1;$

____

$b := b + 1;$

____

$q := q + c;$

____

$\{q = A^2\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$$\{a = A\}\ (1)$$
$$\{0 = 0^2 \wedge a = A\}$$
$$b := 0;$$
$$\{0 = b^2 \wedge a = A\}$$
$$q := 0;$$
$$\{INV : q = b^2 \wedge a = A\}$$
$$\textsf{while } b \neq a \textsf{ do}$$
$$\quad \{INV \wedge b \neq a\}\ (2)$$
$$\quad \{q + 2b + 1 = (b+1)^2 \wedge a = A\}$$
$$\quad c := 2 * b + 1;$$
$$\quad \{q + c = (b+1)^2 \wedge a = A\}$$
$$\quad b := b + 1;$$
$$\quad \{q + c = b^2 \wedge a = A\}$$
$$\quad q := q + c;$$
$$\{INV \wedge \neg(b \neq a)\}\ (3)$$
$$\{q = A^2\}$$

Per le PrePost:

1) Banale aritmetica.

2) Per INV $q = b^2$, quindi $q + 2b + 1 = b^2 + 2b + 1 = (b+1)^2$. La parte delle tesi $a = A$ è banalmente parte di INV.

3) Dall'ipotesi $b = a$ e da INV $q = b^2$ e $a = A$. Quindi $q = b^2 = a^2 = A^2$ che è la tesi.

□