Informatica — 2018-06-22

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

Esercizio 1. *Si forniscano tutte le regole della semantica big step* ($\to_b$) *relative ai comandi* skip, if *ed* $x := e$. *Si commenti* <u>*brevemente*</u> *su come vengono usati gli stati* σ *che compaiono in queste regole.*

Esercizio 2. *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* $[R0], [R1], [R2]$*). Sotto, si usano le variabili* $t, s, d, s', d' \in T$, $n, k \in \mathbb{N}$.

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

$$\frac{}{R(t,0,42)}[R0] \qquad \frac{}{R(n,k+1,n)}[R1] \qquad \frac{R(s,k,s') \qquad R(d,k,d')}{R((s,d),k+1,(s',d'))}[R2]$$

1. *[20%] Si fornisca* $t \in T$*, tali per cui* $R(((1,2),(3,((4,5),6))),3,t)$ *valga. Si giustifichi la risposta con una derivazione.*

2. *[20%] Si enunci il principio di induzione associato alla relazione* R.

3. *[60%] Si consideri l'enunciato seguente:*

$$\forall t_1, t_2, t_3 \in T.\ \forall k \in \mathbb{N}.\ R(t_1,k,t_2) \wedge R(t_2,k,t_3) \implies t_2 = t_3$$

L'enunciato si può riscrivere in modo logicamente equivalente come $\forall t_1, t_2 \in T.\ \forall k \in \mathbb{N}.\ R(t_1,k,t_2) \implies p(t_1,k,t_2)$ *dove il predicato* p *è dato da* $p(t_1,k,t_2) : \forall t_3 \in T.\ R(t_2,k,t_3) \implies t_2 = t_3$.

Si dimostri l'enunciato usando il principio di induzione <u>*associato ad R*</u>.

Soluzione (bozza).
Parte 1.

$$\dfrac{\dfrac{\dfrac{}{R(1,1,1)} \quad \dfrac{}{R(2,1,2)}}{R((1,2),2,(1,2))} \qquad \dfrac{\dfrac{}{R(3,1,3)} \quad \dfrac{\dfrac{}{R((4,5),0,42)} \quad \dfrac{}{R(6,0,42)}}{R(((4,5),6),1,(42,42))}}{R((3,((4,5),6)),2,(3,(42,42)))}}{R(((1,2),(3,((4,5),6))),3,((1,2),(3,(42,42))))}$$

Parte 2.

Per dimostrare $\forall t_1, t_2 \in T. \forall k \in \mathbb{N}.\ R(t_1,k,t_2) \implies p(t_1,k,t_2)$ è sufficiente verificare che

0) $\forall t \in T.\ p(t,0,42)$
1) $\forall n,k \in \mathbb{N}.\ p(n,k+1,n)$
2) $\forall s,d,s',d' \in T. \forall k \in \mathbb{N}.\ p(s,k,s') \wedge p(d,k,d') \implies p((s,d),k+1,(s',d'))$

Parte 3.

Dimostriamo quindi la forma equivalente $\forall t_1, t_2 \in T. \forall k \in \mathbb{N}.\ R(t_1, k, t_2) \implies p(t_1, k, t_2)$ procedendo per induzione su R.

(Caso $[R0]$**)** Dato $t \in T$, bisogna dimostrare $p(t, 0, 42)$, ovvero che

$$\forall t_3 \in T.\ R(42, 0, t_3) \implies 42 = t_3$$

Per farlo assumiamo $IP1 : R(42, 0, t_3)$ e dimostriamo $42 = t_3$.

Invertendo $IP1$, siccome solo $[R0]$ può derivarlo, otteniamo $t_3 = 42$, che è la tesi.

(Caso $[R1]$**)** Dati $n, k \in \mathbb{N}$, bisogna dimostrare $p(n, k+1, n)$, ovvero che

$$\forall t_3 \in T.\ R(n, k+1, t_3) \implies n = t_3$$

Per farlo assumiamo $IP1 : R(n, k+1, t_3)$ e dimostriamo $n = t_3$.

Invertendo $IP1$, siccome solo $[R1]$ può derivarlo, otteniamo $t_3 = n$, che è la tesi.

(Caso $[R2]$**)** Come ipotesi induttive si hanno $p(s, k, s')$ e $p(d, k, d')$, ovvero:

$$\begin{array}{l} IP1 : \forall t_3 \in T.\ R(s', k, t_3) \implies s' = t_3 \\ IP2 : \forall t_3 \in T.\ R(d', k, t_3) \implies d' = t_3 \end{array}$$

Dobbiamo quindi dimostrare $p((s, d), k+1, (s', d'))$, ovvero

$$\forall t_3 \in T.\ R((s', d'), k+1, t_3) \implies (s', d') = t_3$$

Per farlo assumiamo $IP3 : R((s', d'), k+1, t_3)$ e dimostriamo la nuova tesi $(s', d') = t_3$.

Invertiamo $IP3$: può essere ricavata da solo da $[R2]$, nel modo seguente:

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

Quindi otteniamo che $t_3 = (s'', d'')$, $IP4 : R(s', k, s'')$ e $IP5 : R(d', k, d'')$.

Da $IP1$, scegliendo $t_3 = s''$ otteniamo $R(s', k, s'') \implies s' = s''$, da cui con $IP4$ ricaviamo $s' = s''$. Da $IP2$, scegliendo $t_3 = d''$ otteniamo $R(d', k, d'') \implies d' = d''$, da cui con $IP5$ ricaviamo $d' = d''$.

Usando le uguaglianze ricavate otteniamo la tesi $t_3 = (s'', d'') = (s', d')$. $\square$

Esercizio 3. *Sia dato l'insieme $U = \mathbb{N}$ e una funzione $f : \mathcal{P}(U) \to \mathcal{P}(U)$. Si prendano in esame le seguente congetture:*

1) f *monotona* $\implies \forall X, Y \in \mathcal{P}(U).\ f(X \cup Y) \subseteq f(X) \cup f(Y)$
2) f *monotona* $\implies \forall X, Y \in \mathcal{P}(U).\ f(X \cup Y) \supseteq f(X) \cup f(Y)$
3) f *monotona* $\implies \forall X, Y \in \mathcal{P}(U).\ f(X \cup Y) = f(X) \cup f(Y)$

Per ogni congettura sopra, la si dimostri o la si refuti con un controesempio.

Soluzione (bozza).

Parte 1 La prima congettura è falsa. Un possibile controesempio è

$$f(X) = \begin{cases} \mathbb{N} & \text{se } X = \mathbb{N} \\ \emptyset & \text{altrimenti} \end{cases}$$

Verifichiamo che la funzione è monotona, assumendo $X \subseteq Y$ e dimostrando $f(X) \subseteq f(Y)$. Se $X \neq \mathbb{N}$, allora $f(X) = \emptyset \subseteq f(Y)$. Se invece $X = \mathbb{N}$, allora anche $Y = \mathbb{N}$ visto che $X \subseteq Y$. Di qui, $f(X) = f(Y)$, e a maggior ragione l'inclusione.

Infine la congettura non vale perché, se scegliamo $X = \{42\}$ e $Y = \mathbb{N} \setminus \{42\}$ si ha

$$f(X \cup Y) = f(\mathbb{N}) = \mathbb{N} \not\subseteq \emptyset = \emptyset \cup \emptyset = f(X) \cup f(Y)$$

Parte 2 La seconda congettura è vera.

Per dimostrarla, basta osservare che $X \subseteq X \cup Y$ e che $X \subseteq X \cup Y$. Per monotonia, si ricava $f(X) \subseteq f(X \cup Y)$ e $f(Y) \subseteq f(X \cup Y)$. Da queste ultime inclusioni, si ha $f(X) \cup f(Y) \subseteq f(X \cup Y)$.

Parte 3 La terza congettura è falsa. Infatti, se fosse vera, sarebbe vera pure la prima congettura. Lo stesso controesempio si applica qui.

$\square$

Nome ________________________________ Matricola ____________

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

$\{a = A\}$

___

$b := 0;$

___

while $a \neq 0$ do

___

___

$a := a - 1;$

___

$b := 2 * b + 3$

___

$\{b = 3 \cdot (2^A - 1)\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

Soluzione (bozza).

$$
\begin{array}{l}
\{a = A\} \\
\{0 = 3(2^{A-a} - 1)\}\ (1) \\
b := 0; \\
\{INV:\ b = 3(2^{A-a} - 1)\} \\
\textsf{while } a \neq 0 \textsf{ do} \\
\qquad \{INV \wedge a \neq 0\} \\
\qquad \{2b + 3 = 3(2^{A-(a-1)} - 1)\}\ (2) \\
\qquad a := a - 1; \\
\qquad \{2b + 3 = 3(2^{A-a} - 1)\} \\
\qquad b := 2 * b + 3 \\
\{INV \wedge \neg(a \neq 0)\} \\
\{b = 3(2^{A} - 1)\}\ (3)
\end{array}
$$

Per le PrePost:
1) Aritmetica: $3(2^{A-A} - 1) = 3(1 - 1) = 0)$
2) Sfruttando INV si ha

$$2b + 3 = 2(3(2^{A-a} - 1)) + 3 = 6(2^{A-a} - 1) + 3 = 6 \cdot 2^{A-a} - 3$$

e anche

$$3(2^{A-(a-1)} - 1) = 3(2^{A-a+1} - 1) = 3(2 \cdot 2^{A-a} - 1) = 6 \cdot 2^{A-a} - 3$$

Quindi risultano uguali.

3) Per ipotesi $a = 0$, quindi l'invariante diventa $b = 3(2^{A} - 1)$ che è la tesi.

$\square$