Informatica — 2016-01-20

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

Esercizio 1. *Si dimostri la monotonia di* $\hat{\mathcal{R}}$.

Esercizio 2. *Si consideri il predicato/relazione ternaria* $R \in \mathcal{P}(\mathbb{N}\times\mathbb{N}\times\mathbb{N})$ *induttivamente definito da*

$$\frac{}{R(0,m,m)}[R0] \qquad \frac{R(n,(n+1)\cdot m,r)}{R(n+1,m,r)}[R1]$$

1. *[10%] Per ogni naturale* $0 \leq n \leq 4$*, si trovi un valore* $r \in \mathbb{N}$ *tale che valga* $R(n,1,r)$.
2. *[20%] Definire una funzione* $f(n)$ *tale per cui* $R(n,1,f(n))$ *valga per ogni* $n \in \mathbb{N}$ *(non si chiede di dimostrarlo). Dopo, si generalizzi tale risultato definendo una funzione* $g(n,m)$ *tale per cui* $R(n,m,g(n,m))$ *valga per ogni* $n,m \in \mathbb{N}$ *(non si chiede di dimostrarlo).*
3. *[70%] Usando la* g *precedentemente definita, si dimostri che*

$$\forall n,m,r \in \mathbb{N}.\ R(n,m,r) \implies r = g(n,m)$$

procedendo per induzione su $R(n,m,r)$*, e menzionando esplicitamente i risultati teorici che si applicano nel ragionamento.*

Soluzione (bozza).

Parte 1 Si ha $R(0,1,1)$, $R(1,1,1)$, $R(2,1,2)$, $R(3,1,6)$, $R(4,1,24)$.

Parte 2 Basta prendere $f(n) = n!$ e $g(n,m) = n! \cdot m$.

Parte 3 Consideriamo la proprietà / relazione $p(n,m,r) =$ "$r = g(n,m)$". L'enunciato da dimostrare si riscrive quindi come $R \subseteq p$. Si ha che R, per definizione, è il minimo punto fisso di $\hat{\mathcal{R}}$ (dove $\mathcal{R}$ sono le regole fornite). Quindi, per il principio di induzione, per potere avere $R \subseteq p$ basta dimostrare che $\hat{\mathcal{R}}(p) \subseteq p$, cioè che p è preservata da ogni regola di R.

Caso [R0]. Dobbiamo dimostrare $p(0,m,m)$, cioè che $g(0,m) = m$, e infatti $0! \cdot m = 1 \cdot m = m$.

Caso [R1]. Per ipotesi induttiva, assumiamo $p(n,(n+1)\cdot m,r)$, cioè che $r = g(n,(n+1)\cdot m) = n! \cdot (n+1) \cdot m$. Dobbiamo fare vedere che $p(n+1,m,r)$, cioè che $r = g(n+1,m) = (n+1)! \cdot m$. Ma questo segue dall'ipotesi induttiva siccome $(n+1)! = n! \cdot (n+1)$.

$\square$

Esercizio 3. *Si estenda IMP con il comando (dove* $1 \leq n \in \mathbb{N}$*)*

$$\textsf{select}\ e\ \textsf{in}\ (e_1, e'_1) \to c_1\ , (e_2, e'_2) \to c_2\ , \cdots , (e_n, e'_n) \to c_n$$

avente la seguente semantica intuitiva. All'inizio si valutano tutte le espressioni e, e_i, e'_i*. Se esiste un* $j \in \{1 \ldots n\}$ *tale per cui il valore di* e *si trova nell'intervallo* $[e_j, e'_j]$ *si esegue il comando* c_j*, dove* j *è il minimo siffatto indice, e poi si riesegue tutto il* select *da capo. Se non esiste nessun* j*, il comando* select *non ha effetto.*

1. *[50%] Si formalizzi la semantica big-step* $\to_b$ *del* select *con opportune regole di inferenza. (Sopra le regole, potete usare i puntini* $\cdots$ *per indicare una sequenza o insieme di elementi analoghi)*
2. *[30%] Si traduca il generico* select *di sopra in un comando equivalente in IMP non esteso. Potete supporre che i* c_i *siano comandi di IMP, e che si possano usare condizioni complesse* ϕ *nel* while *e* if *(e non solo quelle della forma* $e \neq 0$*). Giustificate informalmente la traduzione.*
3. *[20%] Si definisca una o più regole da aggiungere al sistema deduttivo per le triple di Hoare per il* select*, che ne preservi la correttezza. Se ne dia una descrizione breve ed informale.*

Soluzione (bozza).

Parte 1

Sotto, sia $s = (\textsf{select}\ e\ \textsf{in}\ (e_1, e'_1) \to c_1\ , \cdots , (e_n, e'_n) \to c_n)$.

$$\frac{\begin{array}{c} \langle e, \sigma \rangle \to_e v \\ \langle e_1, \sigma \rangle \to_e v_1 \qquad \langle e'_1, \sigma \rangle \to_e v'_1 \\ \cdots \\ \langle e_n, \sigma \rangle \to_e v_n \qquad \langle e'_n, \sigma \rangle \to_e v'_n \\ v \notin [v_1, v'_1] \cdots v \notin [v_n, v'_n] \end{array}}{\langle s, \sigma \rangle \to_b \sigma} [S - False]$$

$$\frac{\begin{array}{c} \langle e, \sigma \rangle \to_e v \\ \langle e_1, \sigma \rangle \to_e v_1 \qquad \langle e'_1, \sigma \rangle \to_e v'_1 \\ \cdots \\ \langle e_n, \sigma \rangle \to_e v_n \qquad \langle e'_n, \sigma \rangle \to_e v'_n \\ v \notin [v_1, v'_1] \cdots v \notin [v_{j-1}, v'_{j-1}] \qquad v \in [v_j, v'_j] \\ \langle c_j; s, \sigma \rangle \to_b \sigma' \end{array}}{\langle s, \sigma \rangle \to_b \sigma'} [S - True]$$

Parte 2
Una possibile soluzione è:

$$
\begin{array}{l}
\textsf{while } (e_1 \leq e \wedge e \leq e'_1) \vee \cdots \vee (e_n \leq e \wedge e \leq e'_n) \textsf{ do} \\
\quad \textsf{if } (e_1 \leq e \wedge e \leq e'_1) \textsf{ then } c_1 \\
\quad \textsf{else if } (e_2 \leq e \wedge e \leq e'_2) \textsf{ then } c_2 \\
\quad \ldots \\
\quad \textsf{else if } (e_n \leq e \wedge e \leq e'_n) \textsf{ then } c_n \\
\quad \textsf{else skip}
\end{array}
$$

Parte 3
Sotto, sia $s = (\textsf{select } e \textsf{ in } (e_1, e'_1) \to c_1 \ , \cdots, (e_n, e'_n) \to c_n)$.

$$
\frac{\begin{array}{c}
\{P \wedge e_1 \leq e \leq e'_1\}\ c_1\ \{P\} \\
\{P \wedge \neg(e_1 \leq e \leq e'_1) \wedge e_2 \leq e \leq e'_2\}\ c_2\ \{P\} \\
\ldots \\
\{P \wedge (\nexists j \in [1 \ldots n-1].\ e_j \leq e \leq e'_j) \wedge e_n \leq e \leq e'_n\}\ c_n\ \{P\}
\end{array}}{\{P\}\ s\ \{P \wedge \nexists j \in [1 \ldots n].\ e_j \leq e \leq e'_j\}}
$$

La regola sopra può essere vista come un adattamento delle regole dell'if e del while alla traduzione del select data sopra. □

Nome ________________________________ Matricola ____________

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

$\{x = 5 \wedge y = 7\}$

____

while $n > 0$ do

____

____

$x := x + 1;$

____

$y := y * 2 + n;$

____

$n := n - 1$

____

$\{x < y\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$$\{x = 5 \wedge y = 7\}$$
$$\{INV:\ 0 \leq x < y\}\ (1)$$
while $n > 0$ do
$$\{0 \leq x < y \wedge n > 0\}$$
$$\{0 \leq x + 1 < 2y + n\}\ (2)$$
$$x := x + 1;$$
$$\{0 \leq x < 2y + n\}$$
$$y := y * 2 + n;$$
$$\{0 \leq x < y\}$$
$$n := n - 1$$
$$\{0 \leq x < y \wedge n \leq 0\}$$
$$\{x < y\}\ (3)$$

Per le PrePost:

La (1) è immediata.

Per la (2), $0 \leq x + 1$ segue da $0 \leq x$. Inoltre, dalle ipotesi si ha $0 < y$ quindi $1 \leq y$ e quindi $x + 1 \leq x + y < y + y < 2y + n$, usando anche $n > 0$.

La (3) è immediata: la tesi è parte dell'ipotesi.

□