Informatica — 2015-09-11

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

Esercizio 1. *Si forniscano le regole del sistema deduttivo per le triple di Hoare inerenti ai comandi* if*, composizione* $(c_1; c_2)$ *e* skip*, descrivendole brevemente.*

Esercizio 2. *Le regole sotto definiscono induttivamente tre oggetti. Le regole* $[S0], [S1]$ *definiscono l'insieme delle sequenze di naturali* S*, le regole* $[P0], [P1]$ *il predicato* $p \in \mathcal{P}(S \times S)$*, le regole* $[Q0], [Q1]$ *il predicato* $q \in \mathcal{P}(S \times \mathbb{N} \times S)$*. Sotto si ha* $a, b, c \in \mathbb{N}$*, mentre* $A, B \in S$*.*

$$\frac{}{\epsilon}[S0] \qquad \frac{A}{a : A}[S1] \qquad \frac{}{p(\epsilon,\ \epsilon)}[P0] \qquad \frac{p(A, B)}{p(a : A,\ b : B)}[P1]$$

$$\frac{}{q(\epsilon,\ b,\ b : \epsilon)}[Q0] \qquad \frac{q(A, b, B)}{q(a : A, b, a : B)}[Q1]$$

1. *[10%] Si descriva in termini intuitivi quale proprietà è formalizzata da* $p(A, B)$*.*

2. *[20%] Si costruisca un* B *tale che* $q(1 : 3 : 5 : \epsilon,\ 4,\ B)$*, giustificando tale proprietà con una derivazione.*

3. *[20%] Si provi a dimostrare che* $\forall A, B, b.\ q(A, b, B) \implies p(b : A, B)$*, procedendo direttamente per induzione su* $q(A, b, B)$*. Si spieghi dove tale tentativo fallisce.*

4. *[50%] Si dimostri la proprietà di sopra per induzione dopo averla resa più forte come segue:*

$$\forall A, B, b.\ q(A, b, B) \implies (\forall c.\ p(c : A, B))$$

Soluzione (bozza).

Parte 1 $p(A, B)$ vale quando A e B hanno la stessa lunghezza.

Parte 2 Prendiamo $B = 1 : 3 : 5 : 4 : \epsilon$. Si ha

$$\cfrac{\cfrac{\cfrac{\cfrac{}{q(\epsilon, 4, 4 : \epsilon)}[Q0]}{q(5 : \epsilon, 4, 5 : 4 : \epsilon)}[Q1]}{q(3 : 5 : \epsilon, 4, 3 : 5 : 4 : \epsilon)}[Q1]}{q(1 : 3 : 5 : \epsilon, 4, 1 : 3 : 5 : 4 : \epsilon)}[Q1]$$

Parte 3 Proviamo a dimostrare $q \subseteq q'$ con

$$q'(A, b, B) = p(b : A, B)$$

Usando il principio di induzione, dobbiamo verificare che $\hat{\mathcal{R}}(q') \subseteq q'$. Nel caso della regola $[Q1]$, dobbiamo fare vedere che

$$q'(A, b, B) \implies q'(a : A, b, a : B)$$

cioè che

$$p(b : A, B) \implies p(b : a : A, a : B)$$

Assumiamo l'ipotesi induttiva $p(b : A, B)$, e proviamo a dimostrare le tesi. La regola $[P0]$ non ci aiuta (parla solo di ϵ), e provando con $[P1]$ abbiamo

$$\cfrac{\cfrac{???}{p(a : A, B)}}{p(b : a : A, a : B)}[P1]$$

A questo punto, non si riesce a giustificare $p(a : A, B)$: nell'ipotesi induttiva c'è b al posto di a.

Parte 3 Riproviamo come prima, ma scegliendo

$$q'(A, b, B) = \text{“}\forall c.\ p(c : A, B)\text{”}$$

Caso Q0. Dobbiamo dimostrare $q'(\epsilon, b, b : \epsilon)$ cioè che $\forall c.\ p(c : \epsilon, b : \epsilon)$. Preso c arbitrario, si ha:

$$\cfrac{\cfrac{}{p(\epsilon, \epsilon)}[P0]}{p(c : \epsilon, b : \epsilon)}[P1]$$

Caso Q1. Per ipotesi induttiva assumiamo $q'(A, b, B)$ e cioè $\forall \bar{c}.\ p(\bar{c} : A, B)$. Dobbiamo fare vedere $q'(a : A, b, a : B)$ e cioè che $\forall c.\ p(c : a : A, a : B)$. Prendiamo un c arbitrario. Dall'ipotesi induttiva, scegliendo $\bar{c} = a$, ricavo $p(a : A, B)$. Per $[P1]$ si ricava $p(c : a : A, a : B)$, che è la tesi. $\square$

Esercizio 3. *Si aggiungano ad IMP i comandi* freeze x *e* unfreeze x. *Intuitivamente,* freeze x *ha l'effetto di "congelare" il valore di* x*: esso non viene modificato dai successivi assegnamenti* $x := e$*, che diventano equivalenti a* skip. *Solo dopo avere "scongelato"* x *con* unfreeze x *la variabile sarà di nuovo modificabile. I comandi* freeze *e* unfreeze *sono idempotenti. Per esempio, dopo il comando seguente* x *vale* 1.

$$\mathsf{unfreeze}\ x;\ x := 0;\ \mathsf{freeze}\ x;\ x := x + 1;\ \mathsf{unfreeze}\ x;\ x := x + 1$$

La semantica big step di IMP ora diventa

$$(\to_b) \in \mathcal{P}(Com \times Store \times \mathcal{P}(Var) \times Store \times \mathcal{P}(Var))$$
$$\langle c, \sigma, V \rangle \to_b \langle \sigma', V' \rangle$$

dove i due insiemi $V, V' \in \mathcal{P}(Var)$ indicano le variabili congelate prima e dopo avere eseguito il comando.

Si formalizzi la semantica di $\mathsf{freeze}\ x$, $\mathsf{unfreeze}\ x$, $x := e$, *e di* $c_1; c_2$ *nell'estensione di IMP, usando regole di inferenza.*

Soluzione (bozza).

$$\frac{}{\langle \mathsf{freeze}\ x, \sigma, V\rangle \to_b \langle \sigma, V \cup \{x\}\rangle}$$

$$\frac{}{\langle \mathsf{unfreeze}\ x, \sigma, V\rangle \to_b \langle \sigma, V \setminus \{x\}\rangle}$$

$$\frac{x \in V}{\langle x := e, \sigma, V\rangle \to_b \langle \sigma, V\rangle}[Let1]$$

$$\frac{\langle e, \sigma\rangle \to_e v \qquad x \notin V}{\langle x := e, \sigma, V\rangle \to_b \langle \sigma[x \mapsto v], V\rangle}[Let2]$$

$$\frac{\langle c_1, \sigma, V\rangle \to_b \langle \sigma', V'\rangle \qquad \langle c_2, \sigma', V'\rangle \to_b \langle \sigma'', V''\rangle}{\langle c_1; c_2, \sigma, V\rangle \to_b \langle \sigma'', V''\rangle}[Comp]$$

$\square$

Nome ______________________________ Matricola ____________

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

$\{y = 0\}$

____

$n := 10;$

____

while $n \leq 20$ do

____

____

if $x = n$ then

____

____

$y := 1$

else

____

____

skip;

____

$n := n + 1$

____

$\{(y = 1) \iff (10 \leq x \leq 20)\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

____

____

____

____

____

____

Soluzione (bozza).

$\{y = 0\}$
$\{10 \leq 10 \leq 20 \wedge (y = 1 \iff 10 \leq x < 10)\}$ (1)
$n := 10;$
$\{INV : 10 \leq n \leq 21 \wedge (y = 1 \iff 10 \leq x < n)\}$
while $n \leq 20$ do
  $\{INV \wedge n \leq 20\}$
  $\{10 \leq n \leq 20 \wedge (y = 1 \iff 10 \leq x < n)\}$ (2)
  if $x = n$ then
    $\{10 \leq n \leq 20 \wedge (y = 1 \iff 10 \leq x < n) \wedge x = n\}$
    $\{10 \leq n + 1 \leq 21 \wedge (1 = 1 \iff 10 \leq x < n + 1)\}$ (3)
    $y := 1$
  else
    $\{10 \leq n \leq 20 \wedge (y = 1 \iff 10 \leq x < n) \wedge x \neq n\}$
    $\{10 \leq n + 1 \leq 21 \wedge (y = 1 \iff 10 \leq x < n + 1)\}$ (4)
    skip;
  $\{10 \leq n + 1 \leq 21 \wedge (y = 1 \iff 10 \leq x < n + 1)\}$
  $n := n + 1$
$\{INV \wedge \neg(n \leq 20)\}$
$\{(y = 1) \iff (10 \leq x \leq 20)\}$ (5)

Per le PrePost:

1) $10 \leq 10 \leq 20$ è banale, mentre ambo i lati di $\iff$ sono falsi visto che $y = 0$ per ipotesi, e che non vale $10 < 10$.

2) $10 \leq n$ è da INV; $n \leq 20$ dall'altra ipotesi. La parte $\iff$ è in INV.

3) $n+1 \leq 21$ viene da $n \leq 20$. Per la parte $\iff$ basta dimostrare che vale $10 \leq x < n + 1$. Si ha per ipotesi $10 \leq n = x$. Inoltre, $x < x + 1 = n + 1$.

4) L'ipotesi $10 \leq n$ garantisce $10 \leq n + 1$. Inoltre, da $n \leq 20$ si ha $n + 1 \leq 21$. Infine, sapendo che $x \neq n$, si ha che $x < n \iff x < n + 1$ visto che sono interi.

5) Dalle ipotesi si ha $n = 21$, da cui $x < n \iff x \leq 20$ visto che sono interi. Da qui la tesi.

□