Informatica — 2017-01-23

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

Esercizio 1. *Si definisca quando $f : \mathcal{P}(U) \to \mathcal{P}(U)$ è monotona. Si definisca l'operatore delle conseguenze immediate $\hat{\mathcal{R}}(X)$ e si dimostri che è monotono.*

Esercizio 2. *Sia $f : \mathbb{N} \to \mathbb{N}$ una funzione data. Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di numeri naturali (regole $[S0], [S1]$) e due relazioni tra sequenze $R, W \in \mathcal{P}(S \times S)$ (regole $[R0], [R1]$ e $[W0], [W1]$). Sotto, n, m indicano naturali mentre s, z indicano sequenze.*

$$\frac{}{\epsilon}[S0] \qquad \frac{s}{n : s}[S1] \qquad \frac{}{R(\epsilon, \epsilon)}[R0] \qquad \frac{R(s, z)}{R(n : s, f(n) : z)}[R1]$$

$$\frac{}{W(\epsilon, \epsilon)}[W0] \qquad \frac{W(s, z)}{W(n : m : s, m : n : z)}[W1]$$

1. *[15%] Si trovi $s \in S$ tale che $R(1 : 2 : 3 : 4 : \epsilon, s)$, mostrando una derivazione.*
2. *[15%] Si trovi $s \in S$ tale che $W(1 : 2 : 3 : 4 : \epsilon, s)$, mostrando una derivazione.*
3. *[70%] Si dimostri che*

$$\forall s, t, u \in S.\ W(s, t) \land R(t, u) \implies \exists v \in S.\ R(s, v) \land W(v, u)$$

(Suggerimento: si proceda per induzione su $W(s, t)$.)

Soluzione (bozza).

Parte 1

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{R(\epsilon, \epsilon)}[R0]}{R(4 : \epsilon, f(4) : \epsilon)}[R1]}{R(3 : 4 : \epsilon, f(3) : f(4) : \epsilon)}[R1]}{R(2 : 3 : 4 : \epsilon, f(2) : f(3) : f(4) : \epsilon)}[R1]}{R(1 : 2 : 3 : 4 : \epsilon, f(1) : f(2) : f(3) : f(4) : \epsilon)}[R1]$$

Parte 2

$$\cfrac{\cfrac{\cfrac{}{W(\epsilon, \epsilon)}[W0]}{W(3 : 4 : \epsilon, 4 : 3 : \epsilon)}[W1]}{W(1 : 2 : 3 : 4 : \epsilon, 2 : 1 : 4 : 3 : \epsilon)}[W1]$$

Parte 3 Dimostriamo

$$\forall s, t \in S.\ W(s,t) \implies p(s,t)$$

dove

$$p(s,t) : \quad \forall u \in S.\ R(t,u) \implies \exists v \in S.\ R(s,v) \land W(v,u)$$

Procedendo per induzione, verifichiamo che p è preservata da tutte le regole di W.

(Caso W0) Dimostriamo $p(\epsilon, \epsilon)$, ovvero

$$\forall u \in S.\ R(\epsilon, u) \implies \exists v \in S.\ R(\epsilon, v) \land W(v,u)$$

Assumiamo quindi $IP1 : \ R(\epsilon, u)$. Invertendo $IP1$, osserviamo che può essere ricavata solo da $R0$ e quindi $u = \epsilon$. La tesi diventa quindi

$$\exists v \in S.\ R(\epsilon, v) \land W(v, \epsilon)$$

Scegliendo $v = \epsilon$, la tesi deriva immediatamente dalle regole $R0$ e $W0$.

(Caso W1) Dimostriamo $p(s,z) \implies p(n : m : s, m : n : z)$. Assumiamo l'ipotesi induttiva $IP1 : \ p(s,z)$. Rimane da dimostrare la tesi

$$\forall u \in S.\ R(m : n : z, u) \implies \exists v \in S.\ R(n : m : s, v) \land W(v,u)$$

Assumiamo $IP2 : R(m : n : z, u)$. Per inversione, siccome solo la regola $R1$ può ricavarlo, si ha $u = f(m) : u_1$ per qualche u_1 con $IP3 : \ R(n : z, u_1)$. Invertendo anche $IP3$, per lo stesso motivo si ricava $u_1 = f(n) : u_2$ per qualche u_2 con $IP4 : \ R(z, u_2)$.

Ora, usiamo $IP1$ scegliendo $u = u_2$, e ricaviamo

$$R(z, u_2) \implies \exists v \in S.\ R(s,v) \land W(v, u_2)$$

L'antecedente vale per $IP4$, quindi ricaviamo $IP5 : \ R(s, \bar{v})$ e $IP6 : W(\bar{v}, u_2)$ per qualche $\bar{v}$.

Ora possiamo dimostrare la tesi

$$\exists v \in S.\ R(n : m : s, v) \land W(v,u)$$

Scegliendo $v = f(n) : f(m) : \bar{v}$, la tesi diventa

$$R(n : m : s, f(n) : f(m) : \bar{v}) \land W(f(n) : f(m) : \bar{v}, u)$$

La prima parte segue da $IP5$ e da due applicazioni della regola $R1$. La seconda si può riscrivere usando le quazioni per u_1 e u_2 come $W(f(n) : f(m) : \bar{v}, f(m) : f(n) : u_2)$. Questa segue da $IP6$ usando la regola $W1$.

$\square$

Esercizio 3.

1. *[50%] Si definisca induttivamente (tramite un insieme di regole) una relazione $P \in \mathcal{P}(Var \times Com \times Com)$ in modo che $P(x, c_1, c_2)$ valga quando c_2 è ottenuto rimpiazzando tutti gli assegnamenti della forma $x := e$ (per qualsiasi $e \in Exp$) presenti dentro c_1 con* skip. *(Suggerimento: fornite <u>due</u> regole per l'assegnamento, e <u>una</u> regola per ogni possibile altro comando. Potete usare come condizione a lato $y \neq x$.)*

2. *[50%] Si dimostri che la seguente proprietà è <u>falsa</u>, trovando un controesempio definendo $c_1, c_2, \sigma, \sigma_1, \sigma_2$ e costruendo le relative derivazioni per P e $(\to_b)$.*

$$\begin{array}{l} \forall x, y \in Var.\ \forall c_1, c_2 \in Com.\ \forall \sigma, \sigma_1, \sigma_2 \in State. \\ \quad P(x, c_1, c_2) \wedge \langle c_1, \sigma\rangle \to_b \sigma_1 \wedge \langle c_2, \sigma\rangle \to_b \sigma_2 \wedge y \neq x \\ \quad \Longrightarrow \\ \quad \sigma_1(y) = \sigma_2(y) \end{array}$$

Soluzione (bozza). Parte 1.

$$\frac{}{P(x, \mathsf{skip}, \mathsf{skip})} \qquad \frac{}{P(x, x := e, \mathsf{skip})} \qquad \frac{y \neq x}{P(x, y := e, y := e)}$$

$$\frac{P(x, c_1, c_1') \quad P(x, c_2, c_2')}{P(x, c_1; c_2, c_1'; c_2')}$$

$$\frac{P(x, c_1, c_1') \quad P(x, c_2, c_2')}{P(x, \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1'\ \mathsf{else}\ c_2')}$$

$$\frac{P(x, c, c')}{P(x, \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \mathsf{while}\ e \neq 0\ \mathsf{do}\ c')}$$

Parte 2.
Un possibile controesempio è dato da:

$$\begin{array}{l} c_1 = (x := 1;\ y := x) \\ c_2 = (\mathsf{skip};\ y := x) \\ \sigma(w) = 0 \qquad \forall w \in Var \\ \sigma_1 = \sigma[x \mapsto 1, y \mapsto 1] \\ \sigma_2 = \sigma \end{array}$$

Chiaramente la tesi non vale visto che $\sigma_1(y) = 1 \neq 0 = \sigma_2(y)$. Le ipotesi invece valgono per le seguenti derivazioni:

$$\frac{\dfrac{}{P(x, x := 1, \mathsf{skip})} \quad \dfrac{}{P(x, y := x, y := x)}}{P(x, x := 1;\ y := x, \mathsf{skip};\ y := x)}$$

$$\dfrac{\dfrac{\langle 1, \sigma\rangle \to_e 1}{\langle x := 1, \sigma\rangle \to_b \sigma[x \mapsto 1]} \quad \dfrac{\langle x, \sigma[x \mapsto 1]\rangle \to_e \sigma[x \mapsto 1](x) = 1}{\langle y := x, \sigma[x \mapsto 1]\rangle \to_b \sigma[x \mapsto 1, y \mapsto 1]}}{\langle x := 1;\ y := x, \sigma\rangle \to_b \sigma[x \mapsto 1, y \mapsto 1] = \sigma_1}$$

$$\dfrac{\dfrac{}{\langle \mathsf{skip}, \sigma\rangle \to_b \sigma} \quad \dfrac{\langle x, \sigma\rangle \to_e \sigma(x) = 0}{\langle y := x, \sigma\rangle \to_b \sigma[y \mapsto 0] = \sigma}}{\langle \mathsf{skip};\ y := x, \sigma\rangle \to_b \sigma = \sigma_2}$$

$\square$

Nome ________________________________ Matricola ____________

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

$\{n = N \geq 1\}$

____

$x := 1;$

____

$y := 1;$

____

while $x < n$ do

____

____

$x := x + 1$

____

$y := y * x;$

____

$\{y = N!\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$\{n = N \geq 1\}$ (1)
$\{1 = 1! \wedge 1 \leq 1 \leq n = N\}$
$x := 1;$
$\{1 = x! \wedge 1 \leq x \leq n = N\}$
$y := 1;$
$\{INV: \; y = x! \wedge 1 \leq x \leq n = N\}$
while $x < n$ do
  $\{INV \wedge x < n\}$ (2)
  $\{y \cdot (x+1) = (x+1)! \wedge 1 \leq x+1 \leq n = N\}$
  $x := x + 1$
  $\{y \cdot x = x! \wedge 1 \leq x \leq n = N\}$
  $y := y * x;$
$\{INV \wedge \neg(x < n)\}$ (3)
$\{y = N!\}$

Per le PrePost:

1) Banale aritmetica.

2) Da INV si ha $y = x!$, e quindi (visto che $x \geq 1$) $y \cdot (x+1) = x! \cdot (x+1) = (x+1)!$. Dall'ipotesi $x < n$, visto che lavoriamo sugli interi, si ha $x + 1 \leq n$. Da $1 \leq x$ si ha $1 \leq x + 1$. La tesi $n = N$ è una parte di INV.

3) Da INV si ha $x \leq n = N$ che con $\neg(x < n)$ fornisce $x = n = N$. Da INV si ha $y = x!$, che per $x = N$ diventa $y = N!$.

$\square$