Informatica — 2021-09-03

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

Esercizio 1. *Dato un insieme di regole $\mathcal{R}$ su un universo U, si definisca l'associato operatore delle conseguenze immediate $\hat{\mathcal{R}} : \mathcal{P}(U) \to \mathcal{P}(U)$. Si dimostri che è monotono.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze finite di interi (regole $[S0], [S1]$) e una relazione $R \in \mathcal{P}(S \times S)$ (regole $[R0], [R1]$). Sotto, x, x_1, x_2 indicano interi mentre s, s_1, s_2 indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \qquad \frac{s}{x : s}(x \in \mathbb{Z})[S1] \qquad \frac{}{R(\epsilon, s)}[R0] \qquad \frac{R(s_1, s_2) \quad x_1 \leq x_2}{R(x_1 : s_1, x_2 : s_2)}[R1]$$

1. *[20%] Si fornisca una sequenza s_1 con 3 interi distinti per cui valga $R(s_1, s_2)$ per qualche s_2 e si giustifichi la risposta esibendo una derivazione.*
2. *[20%] Si enunci il principio di induzione associato alla relazione R.*
3. *[10%] Si consideri l'enunciato seguente:*

   $$\forall s_1, s_2 \in S.\ R(s_1, s_2) \wedge R(s_2, s_1) \implies s_1 = s_2$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall s_1, s_2 \in S.\ R(s_1, s_2) \implies p(s_1, s_2)$$

   per un qualche predicato p.
4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a R.*

Soluzione (bozza).

Parte 1

Una possibile soluzione è:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R(\epsilon, 0 : \epsilon)}}{R(4 : \epsilon, 8 : 0 : \epsilon)}}{R(6 : 4 : \epsilon, 6 : 8 : 0 : \epsilon)}}{R(2 : 6 : 4 : \epsilon, 3 : 6 : 8 : 0 : \epsilon)}$$

Parte 2

Sia $p(-, -)$ un predicato sulle sequenze. Per potere dimostrare che $p(s_1, s_2)$ per tutte le sequenze s_1, s_2 tali che $R(s_1, s_2)$ è sufficiente che valgano:

$R0)$ $\forall s.\ p(\epsilon, s)$
$R1)$ $\forall x_1, x_2, s_1, s_2.\ p(s_1, s_2) \wedge x_1 \leq x_2 \implies p(x_1 : s_1, x_2 : s_2)$

Parte 3

Basta prendere $p(s_1, s_2) :\ R(s_2, s_1) \implies s_1 = s_2$.

Parte 4

Caso R0

Dobbiamo dimostrare $p(\epsilon, s)$ cioè:

$$R(s, \epsilon) \implies \epsilon = s$$

Assumiamo quindi $IP1 : R(s, \epsilon)$ e dimostriamo $\epsilon = s$.

Invertendo $IP1$, notiamo che può essere derivata solo da $R0$, e quindi $S = \epsilon$, da cui la tesi.

Caso R1

Assumiamo l'ipotesi induttiva $IP1 : p(s_1, s_2)$ e la condizione a lato $IP2 : x_1 \leq x_2$, e dimostriamo la tesi $p(x_1 : s_1, x_2 : s_2)$. Queste si riscrivono come:

$$\begin{array}{ll} IP1: & R(s_2, s_1) \implies s_1 = s_2 \\ tesi: & R(x_2 : s_2, x_1 : s_1) \implies x_1 : s_1 = x_2 : s_2 \end{array}$$

Assumiamo quindi $IP3 : R(x_2 : s_2, x_1 : s_1)$ e dimostriamo la nuova tesi $x_1 : s_1 = x_2 : s_2$.

Invertendo $IP3$, notiamo che può essere derivata solo da $R1$, e quindi otteniamo $IP4 : R(s_2, s_1)$ e $IP5 : x_2 \leq x_1$.

Da $IP2$ e $IP5$ otteniamo $x_1 = x_2$.

Da $IP4$ e $IP1$ otteniamo $S_1 = s_2$.

La tesi quindi segue da queste uguaglianze.

□

Esercizio 3. *Nel linguaggio IMP la valutazione di un'espressione non ha effetti collaterali come modificare il valore delle variabili. Altri linguaggi (come, per esempio, Java), invece consentono l'assegnamento all'interno delle espressioni, la cui valutazione può quindi modificare lo stato corrente. Si consideri un'estensione di IMP dove l'assegnamento $x := e$ è anche un'espressione, la cui semantica prima valuta e (potenzialmente modificando lo stato) ottenendo un intero v e poi modifica il valore di x a v. Il risultato finale dell'espressione $x := e$ sarà quindi v. Inoltre, assumiamo che gli operatori binari come $e_1 + e_2$ valutino e_1 prima di e_2.*

Per esempio se inizialmente x vale 0, il comando c

$$x := (x := x + 1) + (x := x * 2)$$

modifica x prima a 1, poi a 2, e infine a 3.

1. *[35%] Si formalizzi la nuova semantica delle espressioni $(\rightarrow_e) \in \mathcal{P}(Exp \times State \times \mathbb{Z} \times State)$ dove $\langle e, \sigma\rangle \rightarrow_e \langle v, \sigma'\rangle$ indica che la valutazione di e nello stato iniziale σ ha risultato v e stato finale σ'. Per farlo, si forniscano le nuove regole $[Lit], [Var], [Plus]$ e $[Let]$ commentandole brevemente.*

2. *[35%]Nella semantica dei comandi, si forniscano le regole per tutti i comandi di IMP, opportunamente adattate alla nuova semantica delle espressioni. Si commentino brevemente le modifiche rispetto alle regole standard di IMP.*

3. *[30%]Si fornisca una derivazione, usando le nuove regole di $(\rightarrow_b)$ e $(\rightarrow_e)$, per l'esecuzione del comando c visto sopra in uno stato iniziale dove tutte le variabili hanno valore zero.*

Soluzione (bozza).

Parte 1

$$\frac{}{\langle z, \sigma\rangle \rightarrow_e \langle z, \sigma\rangle}[Lit]$$

$$\frac{}{\langle x, \sigma\rangle \rightarrow_e \langle \sigma(x), \sigma\rangle}[Var]$$

$$\frac{\langle e_1, \sigma\rangle \rightarrow_e \langle v_1, \sigma'\rangle \qquad \langle e_2, \sigma'\rangle \rightarrow_e \langle v_2, \sigma''\rangle}{\langle e_1 + e_2, \sigma\rangle \rightarrow_e \langle v_1 + v_2, \sigma''\rangle}[Plus]$$

$$\frac{\langle e, \sigma\rangle \rightarrow_e \langle v, \sigma'\rangle}{\langle x := e, \sigma\rangle \rightarrow_e \langle v, \sigma'[x \mapsto v]\rangle}[Let]$$

Parte 2

$$\frac{}{\langle \mathsf{skip}, \sigma\rangle \to_b \sigma}[Skip]$$

$$\frac{\langle e, \sigma\rangle \to_e \langle v, \sigma'\rangle}{\langle x := e, \sigma\rangle \to_b \sigma'[x \mapsto v]}[Let]$$

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

$$\frac{\langle e, \sigma\rangle \to_e \langle v, \sigma'\rangle \quad v \neq 0 \qquad \langle c_1, \sigma'\rangle \to_b \sigma''}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \to_b \sigma''}[If - True]$$

$$\frac{\langle e, \sigma\rangle \to_e \langle 0, \sigma'\rangle \qquad \langle c_2, \sigma'\rangle \to_b \sigma''}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \to_b \sigma''}[If - False]$$

$$\frac{\langle e, \sigma\rangle \to_e \langle v, \sigma'\rangle \quad v \neq 0 \qquad \langle c; \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma'\rangle \to_b \sigma''}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma\rangle \to_b \sigma''}[While - True]$$

$$\frac{\langle e, \sigma\rangle \to_e \langle 0, \sigma'\rangle}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c, \sigma\rangle \to_b \sigma'}[While - False]$$

Parte 3

Sotto scriviamo σ_v per $\sigma[x \mapsto v]$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\langle x, \sigma_0\rangle \to_e \langle 0, \sigma_0\rangle} \quad \dfrac{}{\langle 1, \sigma_0\rangle \to_e \langle 1, \sigma_0\rangle}}{\langle x + 1, \sigma_0\rangle \to_e \langle 1, \sigma_0\rangle}}{\langle x := x + 1, \sigma_0\rangle \to_e \langle 1, \sigma_1\rangle} \quad \dfrac{\dfrac{\dfrac{}{\langle x, \sigma_1\rangle \to_e \langle 1, \sigma_1\rangle} \quad \dfrac{}{\langle 2, \sigma_1\rangle \to_e \langle 2, \sigma_1\rangle}}{\langle x * 2, \sigma_1\rangle \to_e \langle 2, \sigma_1\rangle}}{\langle x := x * 2, \sigma_1\rangle \to_e \langle 2, \sigma_2\rangle}}{\langle (x := x + 1) + (x := x * 2), \sigma_0\rangle \to_e \langle 3, \sigma_2\rangle}}{\langle x := (x := x + 1) + (x := x * 2), \sigma_0\rangle \to_b \sigma_3}$$

□

Nome _____ Matricola _____

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

$\{n = N \geq 0\}$

$x := 0;$

$y := 0;$

---

while $x < n$ do

$x := x + 1;$

$y := y + 3 * x - 2$

$\{2y = N(3N - 1)\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

$\{n = N \geq 0\}$ (1)
$\{0 \leq n = N \wedge 2 \cdot 0 = 0(3 \cdot 0 - 1)\}$
$x := 0;$
$\{x \leq n = N \wedge 2 \cdot 0 = x(3x - 1)\}$
$y := 0;$
$\{INV : x \leq n = N \wedge 2y = x(3x - 1)\}$
while $x < n$ do
    $\{INV \wedge x < n\}$ (2)
    $\{x + 1 \leq n = N \wedge 2(y + 3(x + 1) - 2) = (x + 1)(3(x + 1) - 1)\}$
    $x := x + 1;$
    $\{x \leq n = N \wedge 2(y + 3x - 2) = x(3x - 1)\}$
    $y := y + 3 * x - 2$
$\{INV \wedge \neg(x < n)\}$ (3)
$\{2y = N(3N - 1)\}$

Per le PrePost:

1) Banale aritmetica.

2) La tesi $x + 1 \leq n = N$ deriva dalle ipotesi $x < n$ e $n = N$ visto che si tratta di interi. La tesi $2(y + 3(x + 1) - 2) = (x + 1)(3(x + 1) - 1)$ si risscrive usando INV come segue:

$$2y + 6(x + 1) - 4 = (x + 1)(3x + 3 - 1)$$
$$x(3x - 1) + 6(x + 1) - 4 = (x + 1)(3x + 2)$$
$$3x^2 - x + 6x + 6 - 4 = 3x^2 + 3x + 2x + 2$$
$$3x^2 + 5x + 2 = 3x^2 + 5x + 2$$

3) Da $x \leq n$ e $\neg(x < n)$ si ha $x = n$. Da qui e INV ricaviamo $x = N$ e quindi, usando ora $INV : 2y = x(3x - 1)$, si ha la tesi $2y = N(3N - 1)$.

□