Informatica — 2023-09-08

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

Esercizio 1. *Dato un insieme di regole $\mathcal{R}$ su un insieme 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 di naturali (regole $[S0], [S1]$), una relazione $R \in \mathcal{P}(S \times S \times S)$ (regole $[R0], [R1]$), e una relazione $\Sigma \in \mathcal{P}(S \times \mathbb{N})$ (regole $[\Sigma 0], [\Sigma 1]$), Sotto, n, k indicano naturali, mentre s, w, z indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{n : s}(n \in \mathbb{N})[S1] \quad \frac{}{\Sigma(\epsilon, 0)}[\Sigma 0] \quad \frac{\Sigma(s, k)}{\Sigma(n : s, n + k)}[\Sigma 1]$$

$$\frac{}{R(\epsilon,\ z,\ z)}[R0] \quad \frac{R(s,\ n : z,\ w)}{R(n : s,\ z,\ w)}[R1]$$

1. *[20%] Si trovino tre sequenze s, z, w con almeno due naturali ciascuna, tali per cui valga $R(s, z, w)$. 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:*

   $$\forall s_1, s_2, s_3 \in S, n_1, n_2, n_3 \in \mathbb{N}.\\ R(s_1, s_2, s_3) \land \Sigma(s_1, n_1) \land \Sigma(s_2, n_2) \land \Sigma(s_3, n_3) \implies n_1 + n_2 = n_3$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall s_1, s_2, s_3 \in S.\ R(s_1, s_2, s_3) \implies p(s_1, s_2, s_3)$$

   per un qualche predicato p.
4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a R. Nel farlo, si sfrutti il determinismo di Σ:*

   $$\forall s, n_1, n_2.\ \Sigma(s, n_1) \land \Sigma(s, n_2) \implies n_1 = n_2$$

Soluzione (bozza).
Parte 1.

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

Parte 2.
Affinché valga $\forall s, z, w.\ R(s, z, w) \implies p(s, z, w)$ basta che:

$R0)$ $\forall z \in S.\ p(\epsilon, z, z)$
$R1)$ $\forall s, z, w \in S, n \in \mathbb{N}.\ p(s, n : z, w) \implies p(n : s, z, w)$

Parte 3. È sufficiente prendere

$$p(s_1, s_2, s_3) :\ \forall n_1, n_2, n_3 \in \mathbb{N}.\ \Sigma(s_1, n_1) \land \Sigma(s_2, n_2) \land \Sigma(s_3, n_3) \implies n_1 + n_2 = n_3$$

Parte 4.
Caso $[R0]$**.** Dobbiamo dimostrare $p(\epsilon, z, z)$ e cioè:

$$\forall n_1, n_2, n_3 \in \mathbb{N}.\ \Sigma(\epsilon, n_1) \land \Sigma(z, n_2) \land \Sigma(z, n_3) \implies n_1 + n_2 = n_3$$

Assumiamo quindi $IP1 : \Sigma(\epsilon, n_1)$, $IP2 : \Sigma(z, n_2)$, $IP3 : \Sigma(z, n_3)$ e dimostriamo la nuova tesi $n_1 + n_2 = n_3$.

Invertendo $IP1$ notiamo che può derivare solo da [$\Sigma 0$] e quindi $n_1 = 0$.

Da $IP2, IP3$, per il determinismo di Σ, ricaviamo $n_2 = n_3$.

La tesi si riscrive quindi come $0 + n_2 = n_2$, che è vero.

Caso [$R1$]**.**

Assumiamo l'ipotesi induttiva $p(s, n : z, w)$ e dimostriamo la tesi $p(n : s, z, w)$. Queste si riscrivono come:

$$\begin{array}{ll} IP1: & \forall n_1', n_2', n_3' \in \mathbb{N}.\ \Sigma(s, n_1') \wedge \Sigma(n : z, n_2') \wedge \Sigma(w, n_3') \implies n_1' + n_2' = n_3' \\ tesi: & \forall n_1, n_2, n_3 \in \mathbb{N}.\ \Sigma(n : s, n_1) \wedge \Sigma(z, n_2) \wedge \Sigma(w, n_3) \implies n_1 + n_2 = n_3 \end{array}$$

Introducendo nella tesi, assumiamo

$$\begin{array}{ll} IP2: & \Sigma(n : s, n_1) \\ IP3: & \Sigma(z, n_2) \\ IP4: & \Sigma(w, n_3) \end{array}$$

e dimostriamo la nuova tesi $n_1 + n_2 = n_3$.

Invertendo $IP2$, osserviamo che può essere derivata solo da [$\Sigma 1$], e quindi otteniamo $IP5 : \Sigma(s, k)$ con $n_1 = n + k$.

Applicando la regola [$\Sigma 1$] a $IP3$, otteniamo $IP6 : \Sigma(n : z, n + n_2)$.

Usiamo quindi $IP1$, scegliendo $n_1' = k, n_2' = n + n_2, n_3' = n_3$, assieme a $IP5, IP6, IP4$, e otteniamo così $k + (n + n_2) = n_3$. Da qui si ottiene $(n + k) + n_2 = n_3$ e la tesi $n_1 + n_2 = n_3$. □

Esercizio 3. *Si consideri una variante di IMP priva del ciclo* while*, e con le guardie dell'*if *limitate alla forma* $e \neq 0$*. Su questo linguaggio possiamo definire una semantica "a intervalli". Questa relazione semantica ha segnatura* $(\rightarrow_i) \in \mathcal{P}(Com \times State \times State \times State \times State)$*, dove* $\langle c, \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}} \rangle \rightarrow_i \langle \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}} \rangle$ *indica che eseguendo il comando* c *con la semantica usuale* $(\rightarrow_b)$ *partendo da uno stato iniziale dove le variabili* $x \in Var$ *hanno un valore compreso tra* $\sigma_{\mathsf{min}}(x)$ *e* $\sigma_{\mathsf{max}}(x)$*, si giungerebbe a uno stato finale dove le variabili* $y \in Var$ *hanno un valore compreso tra* $\sigma'_{\mathsf{min}}(y)$ *e* $\sigma'_{\mathsf{max}}(y)$*.*

1. *[20%] Si descriva la segnatura dell'analoga relazione semantica "a intervalli" per le espressioni* $(\rightarrow_{ie}) \in \mathcal{P}(\ldots)$*. Non è richiesto definire la relazione.*
2. *[60%] Si definisca* $(\rightarrow_i)$ *tramite regole di inferenza, sfruttando anche* $(\rightarrow_{ie})$*. Si commentino le regole, prestando particolare attenzione al comando* if*. La semantica così definita deve essere deterministica. (Potete assumere che* $\bar{\sigma}_{\min}(x) \leq \bar{\sigma}_{\mathsf{max}}(x)$ *su ogni coppia di stati associati* $\bar{\sigma}_{\min}, \bar{\sigma}_{\mathsf{max}}$*.)*
3. *[20%] Si giustifichi informalmente il determinismo.*

Soluzione (bozza).

Parte 1.

$$(\rightarrow_{ie}) \in \mathcal{P}(Exp \times State \times State \times \mathbb{Z} \times \mathbb{Z})$$

Parte 2.

Una delle soluzioni possibili è:

$$\frac{}{\langle \mathsf{skip},\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle}[Skip]$$

$$\frac{\langle e,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_{ie} \langle v_{\mathsf{min}}, v_{\mathsf{max}}\rangle}{\langle x := e,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma_{\mathsf{min}}[x \mapsto v_{\mathsf{min}}], \sigma_{\mathsf{max}}[x \mapsto v_{\mathsf{max}}]\rangle}[Let]$$

$$\frac{\langle c_1,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}}\rangle \qquad \langle c_2,\ \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma''_{\mathsf{min}}, \sigma''_{\mathsf{max}}\rangle}{\langle c_1; c_2,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma''_{\mathsf{min}}, \sigma''_{\mathsf{max}}\rangle}[Comp]$$

$$\frac{\langle e,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_{ie} \langle v_{\mathsf{min}}, v_{\mathsf{max}}\rangle \qquad 0 \notin [v_{\mathsf{min}}, v_{\mathsf{max}}] \qquad \langle c_1,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}}\rangle}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}}\rangle}[If - True]$$

$$\frac{\langle e,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_{ie} \langle v_{\mathsf{min}}, v_{\mathsf{max}}\rangle \qquad [v_{\mathsf{min}}, v_{\mathsf{max}}] = \{0\} \qquad \langle c_2,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}}\rangle}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}}\rangle}[If - False]$$

$$\frac{\langle e,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_{ie} \langle v_{\mathsf{min}}, v_{\mathsf{max}}\rangle \qquad \{0\} \subset [v_{\mathsf{min}}, v_{\mathsf{max}}] \qquad \langle c_1,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma'_{\mathsf{min}}, \sigma'_{\mathsf{max}}\rangle \qquad \langle c_2,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \sigma''_{\mathsf{min}}, \sigma''_{\mathsf{max}}\rangle}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2,\ \sigma_{\mathsf{min}}, \sigma_{\mathsf{max}}\rangle \rightarrow_i \langle \min(\sigma'_{\mathsf{min}}, \sigma''_{\mathsf{min}}), \max(\sigma'_{\mathsf{max}}, \sigma''_{\mathsf{max}})\rangle}[If - Both]$$

Sopra, $\min(\sigma', \sigma'')$ è definito come $\min(\sigma', \sigma'')(x) = \min(\sigma'(x), \sigma''(x))$ per ogni $x \in Var$. Lo stato $\max(\sigma', \sigma'')$ è definito analogamente.

Si noti come la regola $If - True$ tratta il caso in cui la guardia è sicuramente vera, la regola $If - False$ tratta il caso in cui la guardia è sicuramente falsa, e la regola $If - Both$ tratta il caso in cui la guardia potrebbe essere sia vera che falsa.

Una soluzione alternativa potrebbe usare solo la regola $If - Both$, modificando la condizione a lato in modo da prendere tutti i casi. Questo definirebbe una relazione semantica "meno precisa" (nello stato finale gli intervalli sono più grandi) ma comunque compatibile con le richieste dell'esercizio.

Queste due soluzioni non sono le uniche possibili.

Parte 3.

Il determinismo per i comandi $\mathsf{skip}, x := e, c_1; c_2$ deriva dal fatto che c'è solo una regola semantica per ogni comando. Il determinismo dell'if deriva dal fatto che le regole $[If - True], [If - False], [If - Both]$ hanno condizioni a lato incompatibili. □

Nome _____ Matricola _____

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

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

$x := 0;$

$y := 42;$

---

while $n > 0$ do

$x := 3 * x;$

$y := 1;$

$n := n - y;$

$x := x + y;$

$y := 10 * x + y$

$\{2x = 3^N - 1\}$

Si giustifichino qui sotto gli eventuali usi della regola *PrePost*.

Soluzione (bozza).

$\{n = N \geq 0\}$
$\{2 \cdot 0 = 3^{N-n} - 1 \wedge n \geq 0\}$ (1)
$x := 0;$
$\{2x = 3^{N-n} - 1 \wedge n \geq 0\}$
$y := 42;$
$\{INV : 2x = 3^{N-n} - 1 \wedge n \geq 0\}$
while $n > 0$ do
    $\{INV \wedge n > 0\}$ (2)
    $\{2(3x + 1) = 3^{N-(n-1)} - 1 \wedge n - 1 \geq 0\}$
    $x := 3 * x;$
    $\{2(x + 1) = 3^{N-(n-1)} - 1 \wedge n - 1 \geq 0\}$
    $y := 1;$
    $\{2(x + y) = 3^{N-(n-y)} - 1 \wedge n - y \geq 0\}$
    $n := n - y;$
    $\{2(x + y) = 3^{N-n} - 1 \wedge n \geq 0\}$
    $x := x + y;$
    $\{2x = 3^{N-n} - 1 \wedge n \geq 0\}$
    $y := 10 * x + y$
$\{INV \wedge \neg(n > 0)\}$ (3)
$\{2x = 3^N - 1\}$

Per le PrePost:

1) Banale aritmetica.

2) La parte di tesi $2(3x + 1) = 3^{N-(n-1)} - 1$ si riscrive come $6x + 2 = 3 \cdot 3^{N-n} - 1$, e sfruttando l'ipotesi INV si riscrive di nuovo come $3(3^{N-n} - 1) + 2 = 3 \cdot 3^{N-n} - 1$ che è vero.

La parte di tesi $n - 1 \geq 0$ deriva da $n > 0$ siccome n è intero.

3) Da $n \geq 0$ e $\neg(n > 0)$ segue $n = 0$. Dal resto di INV si ricava la tesi $2x = 3^N - 1$.

□