Informatica — 2024-09-04

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

Esercizio 1. *Dato un insieme di regole $\mathcal{R}$ su 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 interi (regole $[S0], [S1]$), una relazione $Q \in \mathcal{P}(S \times S)$ (regole $[Q0], [Q1]$), e una relazione $R \in \mathcal{P}(S \times S \times S)$ (regole $[R0], [R1]$). Sotto, a, b indicano interi, mentre s, t, u indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{a : s}(a \in \mathbb{Z})[S1] \quad \frac{}{Q(\epsilon, \epsilon)}[Q0] \quad \frac{Q(s,t)}{Q(a : s, (-a) : t)}[Q1]$$

$$\frac{}{R(\epsilon, \epsilon, \epsilon)}[R0] \quad \frac{R(s,t,u)}{R(a : s, b : t, (a+b) : u)}[R1]$$

1. *[20%] Si trovino $s, t \in S$ per cui valga $Q(s,t) \wedge R(10 : 20 : 30 : \epsilon,\ t,\ 1 : 2 : 3 : \epsilon)$. Si giustifichi la risposta esibendo due derivazioni.*

2. *[20%] Si enunci il principio di induzione associato alla relazione R.*

3. *[10%] Si consideri l'enunciato seguente:*

   $$\forall s_1, s_2, s_3, t_1 \in S.\ Q(s_1, t_1) \wedge R(s_1, s_2, s_3) \implies R(s_3, t_1, s_2)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

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

   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:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R(\epsilon,\epsilon,\epsilon)}[R0]}{R(30 : \epsilon, -27 : \epsilon, 3 : \epsilon)}[R1]}{R(20 : 30 : \epsilon, -18 : -27 : \epsilon, 2 : 3 : \epsilon)}[R1]}{R(10 : 20 : 30 : \epsilon, -9 : -18 : -27 : \epsilon, 1 : 2 : 3 : \epsilon)}[R1]$$

$$\dfrac{\dfrac{\dfrac{}{Q(\epsilon,\epsilon)}[Q0]}{Q(27 : \epsilon, -27 : \epsilon)}[Q1]}{Q(18 : 27 : \epsilon, -18 : -27 : \epsilon)}[Q1]}{Q(9 : 18 : 27 : \epsilon, -9 : -18 : -27 : \epsilon)}[Q1]$$

Parte 2.
Affinché valga $\forall s, t, u.\ R(s,t,u) \implies p(s,t,u)$ è sufficiente che:

$R0)$ $p(\epsilon, \epsilon, \epsilon)$
$R1)$ $\forall s, t, u \in S, a, b \in \mathbb{Z}.\ p(s,t,u) \implies p(a : s, b : t, (a+b) : u)$

Parte 3.
Basta prendere $p(s,t,u) :\ \forall t_1 \in S.\ Q(s, t_1) \implies R(u, t_1, t)$.
Parte 4.

Caso $[R0]$. Dimostriamo $p(\epsilon, \epsilon, \epsilon)$, cioè

$$\forall t_1 \in S.\ Q(\epsilon, t_1) \implies R(\epsilon, t_1, \epsilon)$$

Assumiamo $IP1 :\ Q(\epsilon, t_1)$ e dimostriamo la nuova tesi $R(\epsilon, t_1, \epsilon)$.

Invertendo $IP1$, osserviamo che può derivare solo da $[Q0]$, da cui $t_1 = \epsilon$. La tesi diventa $R(\epsilon, \epsilon, \epsilon)$, che segue dalla regola $[R0]$.

Caso $[R1]$. Assumiamo l'ipotesi induttiva $IP1 : p(s, t, u)$ e dimostriamo $p(a : s, b : t, (a + b) : u)$. In altri termini,

$$\begin{array}{l} IP1 :\ \forall t' \in S.\ Q(s, t') \implies R(u, t', t) \\ tesi :\ \forall t_1 \in S.\ Q(a : s, t_1) \implies R((a + b) : u, t_1, b : t) \end{array}$$

Assumiamo $IP2 : Q(a : s, t_1)$ e dimostriamo la nuova tesi $R((a + b) : u, t_1, b : t)$.

Invertendo $IP2$ osserviamo che può derivare solo da $[Q1]$, da cui $t_1 = (-a) : \bar{t}$ per qualche $\bar{t}$ per cui vale $IP3 : Q(s, \bar{t})$.

Usiamo $IP1$ scegliendo $t' = \bar{t}$ assieme a $IP3$ e otteniamo $IP4 : R(u, \bar{t}, t)$.

Applichiamo $[R1]$ su $IP4$ (scegliendo le variabili della regola a e b come $a + b$ e $-a$) e otteniamo $R((a + b) : u, (-a) : \bar{t}, (a + b - a) : t)$ e quindi $R((a + b) : u, t_1, b : t)$ che è la tesi.

□

Esercizio 3. *Si consideri una variante di IMP ottenuta aggiungendo i vettori di interi al linguaggio. Lo stato σ ora associa a ogni variabile x sia un valore intero $\sigma_i(x)$ che un valore vettore di interi $\sigma_v(x)$. Formalmente, abbiamo:*

$$\begin{array}{l} \sigma = (\sigma_i, \sigma_v) \in State = State_i \times State_v \qquad State_i = Var \to \mathbb{Z} \qquad State_v = Var \to Vec \\ Vec = \{(n, w) \mid n \in \mathbb{N} \wedge w : \{0, 1, \ldots, n-1\} \to \mathbb{Z}\} \\ (\to_e) \in \mathcal{P}(Exp \times State \times \mathbb{Z}) \qquad (\to_b) \in \mathcal{P}(Com \times State \times State) \end{array}$$

Per esempio, possiamo avere $\sigma_i(x) = 12$ e $\sigma_v(x) = (3, w)$ con $w(0) = 1$, $w(1) = -4$, $w(2) = 42$, e w indefinito altrove. In generale, un vettore $\sigma_v(x) = (n, w)$ ha lunghezza $n \geq 0$ e indici validi $\{0, 1, \ldots, n-1\}$. La semantica di espressioni e comandi non è totale quando vengono usati indici non validi per accedere ai vettori.

1. *[40%] Usando opportune regole di inferenza, si formalizzi la semantica delle espressioni z (costante), x (variabile intera), $x[e]$ (accesso al vettore, fallisce se e non è un indice valido), $\mathsf{length}(x)$ (lunghezza del vettore), $e_1 + e_2$ (somma).*

2. *[40%] Usando opportune regole di inferenza, si formalizzi la semantica dei comandi $x := e$ (assegnamento variabile intera), $x := \mathsf{new\ int}[e]$ (nuovo vettore, inizializzato con zeri, fallisce se $e < 0$), $x[e_1] := e_2$ (modifica vettore, fallisce se e_1 non è un indice valido per x), $c_1; c_2$ (composizione).*

3. *[20%] Si costruisca un comando in questo linguaggio che calcoli la somma di tutti gli elementi del vettore x. Si possono usare espressioni complesse nelle guardie.*

Soluzione (bozza).

Parte 1.

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

$$\frac{}{\langle x, (\sigma_i, \sigma_v)\rangle \to_e \sigma_i(x)}[Var]$$

$$\frac{\langle e, (\sigma_i, \sigma_v)\rangle \to_e z \qquad 0 \le z < n \qquad \sigma_v(x) = (n, w)}{\langle x[e], (\sigma_i, \sigma_v)\rangle \to_e w(z)}[VecRead]$$

$$\frac{\sigma_v(x) = (n, w)}{\langle \mathsf{length}(x), (\sigma_i, \sigma_v)\rangle \to_e n}[Length]$$

$$\frac{\langle e_1, \sigma\rangle \to_e z_1 \qquad \langle e_2, \sigma\rangle \to_e z_2}{\langle e_1 + e_2, \sigma\rangle \to_e z_1 + z_2}[Plus]$$

Parte 2.

$$\frac{\langle e, (\sigma_i, \sigma_v)\rangle \to_e z}{\langle x := e, (\sigma_i, \sigma_v)\rangle \to_b (\sigma_i[x \mapsto z], \sigma_v)}[Let]$$

$$\frac{\langle e, (\sigma_i, \sigma_v)\rangle \to_e n \ge 0 \qquad w : \{0, \ldots, n-1\} \to \mathbb{Z} \qquad \forall j.\ w(j) = 0}{\langle x := \mathsf{new\ int}[e], (\sigma_i, \sigma_v)\rangle \to_b (\sigma_i, \sigma_v[x \mapsto (n, w)])}[VecNew]$$

$$\frac{\langle e_1, (\sigma_i, \sigma_v)\rangle \to_e j \qquad \langle e_2, (\sigma_i, \sigma_v)\rangle \to_e z \qquad \sigma_v(x) = (n, w) \qquad 0 \le j < n}{\langle x[e_1] := e_2, (\sigma_i, \sigma_v)\rangle \to_b (\sigma_i, \sigma_v[x \mapsto (n, w[j \mapsto z])])}[VecWrite]$$

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

Parte 3.

$s := 0;$
$i := 0;$
$\mathsf{while}\ i < \mathsf{length}(x)\ \mathsf{do}$
    $s := s + x[i];$
    $i := i + 1$

□

Nome _____ Matricola _____

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

$\{n = 3N \geq 0\}$

$x := 0;$

$y := 0;$

---

while $y < n$ do

$x := (2 + 5 * x - 3 * x * x)/2;$

$y := y + 1$

$\{x = 0\}$

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

Soluzione (bozza).

$\{n = 3N \geq 0\}$ (1)
$\{INV: \ 0 = 0 \bmod 3 \wedge 0 \leq n = 3N\}$
$x := 0;$
$\{INV: \ x = 0 \bmod 3 \wedge 0 \leq n = 3N\}$
$y := 0;$
$\{INV: \ x = y \bmod 3 \wedge y \leq n = 3N\}$
while $y < n$ do
    $\{INV \wedge y < n\}$ (2)
    $\{(2 + 5 * x - 3 * x * x)/2 = (y + 1) \bmod 3 \wedge y + 1 \leq n = 3N\}$
    $x := (2 + 5 * x - 3 * x * x)/2;$
    $\{x = (y + 1) \bmod 3 \wedge y + 1 \leq n = 3N\}$
    $y := y + 1$
$\{INV \wedge \neg(y < n)\}$ (3)
$\{x = 0\}$

Per le PrePost:

1) Banale aritmetica.

2) La parte $y+1 \leq n$ deriva dall'ipotesi $y < n$. Per $(2+5*x-3*x*x)/2 = (y+1) \bmod 3$, usiamo l'ipotesi $x = y \bmod 3$ come segue. L'ipotesi garantisce $x \in \{0, 1, 2\}$ quindi possiamo considerare solo questi tre casi.

Se $x = y \bmod 3 = 0$ allora $(2 + 5 * x - 3 * x * x)/2 = 2/2 = 1 = (y + 1) \bmod 3$.

Se $x = y \bmod 3 = 1$ allora $(2 + 5 * x - 3 * x * x)/2 = 4/2 = 2 = (y + 1) \bmod 3$.

Se $x = y \bmod 3 = 2$ allora $(2+5*x-3*x*x)/2 = (2+10-12)/2 = 0 = (y+1) \bmod 3$.

3) Dalle ipotesi $y \leq n = 3N$ e $\neg(y < n)$ si ottiene $y = n = 3N$. Con questo e INV otteniamo $x = y \bmod 3 = 3N \bmod 3 = 0$ che è la tesi.

□