Informatica — 2025-09-01

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

Esercizio 1. *Si definiscano le regole del sistema deduttivo per le triple di Hoare. Si dia anche la definizione della validità di una tripla di Hoare e si enunci il teorema di correttezza.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di naturali dispari (regole $[S0], [S1]$), una relazione $R \in \mathcal{P}(S \times \mathbb{N})$ (regole $[R0], [R1]$), e una relazione $Q \in \mathcal{P}(S \times \mathbb{N})$ (regole $[Q0], [Q1]$). Sotto, si assume $s, z \in S$ e $n, k, a, b \in \mathbb{N}$.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{n : s}(n \text{ dispari})[S1] \quad \frac{}{R(\epsilon\,,\,0)}[R0] \quad \frac{R(s,k)}{R(n : s\ ,\ k+n)}[R1]$$

$$\frac{}{Q(\epsilon\,,\,0)}[Q0] \quad \frac{Q(s,k)}{Q(n : s\ ,\ k+1)}[Q1]$$

1. *[20%] Si trovino due naturali a, b per cui valga $R(1 : 3 : 5 : \epsilon\,,\,a) \wedge Q(1 : 3 : 5 : \epsilon\,,\,b)$. 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:*

   $$\forall s \in S, a, b \in \mathbb{N}.\ R(s,a) \wedge Q(s,b) \implies (a+b) \text{ pari}$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall s \in S, a \in \mathbb{N}.\ \ R(s,a) \implies p(s,a)$$

   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.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R(\epsilon,0)}[R0]}{R(5:\epsilon,5)}[R1]}{R(3:5:\epsilon,8)}[R1]}{R(1:3:5:\epsilon,9)}[R1]$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{Q(\epsilon,0)}[Q0]}{Q(5:\epsilon,1)}[Q1]}{Q(3:5:\epsilon,2)}[Q1]}{Q(1:3:5:\epsilon,3)}[Q1]$$

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

$R0)$ $p(\epsilon, 0)$
$R1)$ $\forall s \in S, k, n \in \mathbb{N}.\ p(s,k) \wedge n$ dispari $\implies p(n : s, k+n)$

Parte 3.
Basta prendere $p(s,a)$ uguale a

$$\forall b \in \mathbb{N}.\ Q(s,b) \implies (a+b) \text{ pari}$$

Parte 4. **Caso** $R0$.

Dobbiamo dimostrare $p(\epsilon, 0)$ ovvero

$$\forall b \in \mathbb{N}.\ Q(\epsilon, b) \implies (0 + b) \text{ pari}$$

Assumiamo quindi $IP1 : Q(\epsilon, b)$ e dimostriamo la nuova tesi b pari.

Invertendo $IP1$, osserviamo che può essere derivata solo da $Q0$, e quindi $b = 0$, da cui la tesi b pari.

Caso $R1$.

Assumiamo n dispari e l'ipotesi induttiva $IP1 : p(s, k)$, e dimostriamo la tesi $p(n : s, k + n)$. Si ha:

$$IP1 : \forall \bar{b} \in \mathbb{N}.\ Q(s, \bar{b}) \implies (k + \bar{b}) \text{ pari}$$
$$tesi : \forall b \in \mathbb{N}.\ Q(n : s, b) \implies (k + n + b) \text{ pari}$$

Assumiamo quindi $IP2 : Q(n : s, b)$ e dimostriamo la nuova tesi $k + n + b$ pari.

Invertendo $IP1$, osserviamo che può essere derivata solo da $Q1$, da cui ricaviamo $IP3 : Q(s, b')$ e $b = b' + 1$.

Usiamo $IP1$ scegliendo $\bar{b} = b'$, assieme a $IP3$, e ricaviamo $k + b'$ pari.

La tesi deriva quindi da $k + n + b = (k + b') + n + 1$ che è pari perché $k + b'$ è pari, mentre n e 1 sono dispari.

□

Esercizio 3. *Si fissi una variabile di IMP x e una costante intera z, e si indichi con Z l'insieme $\{\sigma \in State \mid \sigma(x) = z\}$ e con Com' l'insieme dei comandi che non hanno al loro interno alcun assegnamento alla variabile x.*

1. *[50%] Si definisca induttivamente una relazione* $\mathsf{simp\_exp} \in \mathcal{P}(Exp \times Exp)$ *tale che:*
   (a) $\mathsf{simp\_exp}$ *sia una funzione* $Exp \to Exp$.
   (b) *Quando vale* $\mathsf{simp\_exp}(e_1, e_2)$ *e si valutano ambo le espressioni in un* $\sigma \in Z$ *arbitrario, i due risultati devono coincidere.*
   (c) *Quando vale* $\mathsf{simp\_exp}(e_1, e_2)$ *e si valutano tali espressioni in* $\sigma \in Z$*, valutare* e_2 *richieda, ove ragionevolmente possibile, meno operazioni di* e_1*. Si sfrutti l'ipotesi* $\sigma \in Z$.
2. *[50%] Si definisca induttivamente una relazione* $\mathsf{simp\_com} \in \mathcal{P}(Com' \times Com')$ *che soddisfi condizioni sull'esecuzione dei comandi in* Com' *analoghe a quelle date sopra per la valutazione delle espressioni.*

Si giustifichi informalmente la risposta. Nelle espressioni, potete ignorare gli operatori diversi dall'addizione.

Soluzione (bozza).

Parte 1.

Una possibile soluzione è la seguente:

$$\frac{v \in \mathbb{Z}}{\mathsf{simp\_exp}(v, v)}[Lit]$$

$$\frac{y \in Var \qquad y \neq x}{\mathsf{simp\_exp}(y, y)}[Var1]$$

$$\frac{}{\mathsf{simp\_exp}(x, z)}[Var2]$$

$$\frac{v_1, v_2, v \in \mathbb{Z} \quad \mathsf{simp\_exp}(e_1, v_1) \quad \mathsf{simp\_exp}(e_2, v_2) \quad v = v_1 + v_2}{\mathsf{simp\_exp}(e_1 + e_2 \ , \ v)}[Plus1]$$

$$\frac{e_1' \notin \mathbb{Z} \quad \mathsf{simp\_exp}(e_1, e_1') \quad \mathsf{simp\_exp}(e_2, e_2')}{\mathsf{simp\_exp}(e_1 + e_2 \ , \ e_1' + e_2')}[Plus2]$$

$$\frac{e_2' \notin \mathbb{Z} \quad \mathsf{simp\_exp}(e_1, e_1') \quad \mathsf{simp\_exp}(e_2, e_2')}{\mathsf{simp\_exp}(e_1 + e_2 \ , \ e_1' + e_2')}[Plus3]$$

e regole analoghe per le altre operazioni. Molte altre varianti sono possibili, per esempio $0 + e$ è semplificabile a e', $0 * y$ è semplificabile a 0, e così via.

Parte 2.

Una possibile soluzione è la seguente:

$$\frac{}{\mathsf{simp\_com}(\mathsf{skip}, \mathsf{skip})}[Skip]$$

$$\frac{\mathsf{simp\_exp}(e, e')}{\mathsf{simp\_com}(y := e \ , \ y := e')}[Let]$$

$$\frac{\mathsf{simp\_com}(c_1 \ , \ c_1') \quad \mathsf{simp\_com}(c_2 \ , \ c_2')}{\mathsf{simp\_com}(c_1; c_2 \ , \ c_1'; c_2')}[Comp]$$

$$\frac{\mathsf{simp\_com}(c_1, c_1') \quad \mathsf{simp\_exp}(e, v) \quad 0 \neq v \in \mathbb{Z}}{\mathsf{simp\_com}(\mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2 \ , \ c_1')}[If - True]$$

$$\frac{\mathsf{simp\_com}(c_2, c_2') \quad \mathsf{simp\_exp}(e, v) \quad v = 0}{\mathsf{simp\_com}(\mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2 \ , \ c_2')}[If - False]$$

$$\frac{\mathsf{simp\_com}(c_1, c_1') \quad \mathsf{simp\_com}(c_2, c_2') \quad \mathsf{simp\_exp}(e, e') \quad e' \notin \mathbb{Z}}{\mathsf{simp\_com}(\mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2 \ , \ \mathsf{if}\ e' \neq 0\ \mathsf{then}\ c_1'\ \mathsf{else}\ c_2')}[If - Unknown]$$

$$\frac{\mathsf{simp\_com}(c, c') \quad \mathsf{simp\_exp}(e, v) \quad v = 0}{\mathsf{simp\_com}(\mathsf{while}\ e \neq 0\ \mathsf{do}\ c \ , \ \mathsf{skip})}[While - False]$$

$$\frac{\mathsf{simp\_com}(c, c') \quad \mathsf{simp\_exp}(e, e') \quad e' \neq 0}{\mathsf{simp\_com}(\mathsf{while}\ e \neq 0\ \mathsf{do}\ c \ , \ \mathsf{while}\ e' \neq 0\ \mathsf{do}\ c')}[While - Unknown]$$

Nota: sopra la condizione $e' \neq 0$ sta a indicare che l'espressione e' e l'espressione 0 sono diverse, sintatticamente. Non sta a indicare che la valutazione di e' in uno stato non precisato ha un risultato non nullo.

□

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 $y < n$ do

$y := y + 1;$

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

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

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

Soluzione (bozza).

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

Per le PrePost:

1) Banale aritmetica.

2) Siccome sono valori interi, da $y < n$ otteniamo $y + 1 \leq n$. La tesi $n = N$ deriva da INV. L'equazione nella tesi si semplifica in

$$x + 3 - 2y - 2 = 2y + 2 - y^2 - 1 - 2y$$

che si riduce a

$$x = 2y - y^2$$

che deriva da INV.

3) Da $y \leq n$ e $\neg(y < n)$ si ottiene $y = n$. Col resto di INV si ottiene quindi $x = 2y - y^2 = 2n - n^2 = 2N - N^2$ che è la tesi.

□