Informatica — 2018-01-22

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

Esercizio 1. *Si fornisca la definizione della semantica delle espressioni ($\to_e$) di IMP. Si enuncino, senza dimostrarli, i risultati associati relativi al determinismo e alla totalità di tale semantica.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze finite di numeri naturali (regole $[S0], [S1]$), una proprietà $Q \in \mathcal{P}(S)$ (regole $[Q0], [Q1]$), e una relazione $R \in \mathcal{P}(S \times \mathbb{N})$ (regole $[R0], [R1]$). Sotto, k, l, m, n indicano naturali mentre s, t indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{n : s}[S1] \qquad \frac{}{Q(n : \epsilon)}[Q0] \quad \frac{Q(n : s)}{Q(2n : 2n : s)}[Q1]$$

$$\frac{}{R(m : \epsilon, 0)}[R0] \quad \frac{R(m : s, k)}{R(l : 2m : s, l + k)}[R1]$$

1. *[20%] Si fornisca una sequenza t contenente 5 naturali per cui valga $Q(t)$ e si giustifichi la risposta esibendo una derivazione.*

2. *[30%] Si enunci il principio di induzione associato alla relazione R.*

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

$$\forall s \in S. \forall k \in \mathbb{N}.\ R(s, k) \land Q(s) \implies k \text{ pari}$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma $\forall s \in S. \forall k \in \mathbb{N}.\ R(s, k) \implies p(s, k)$ per un qualche predicato p.

4. *[40%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato ad R.*

Soluzione (bozza).
Parte 1.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Q(1 : \epsilon)}}{Q(2 : 2 : \epsilon)}}{Q(4 : 4 : 2 : \epsilon)}}{Q(8 : 8 : 4 : 2 : \epsilon)}}{Q(16 : 16 : 8 : 4 : 2 : \epsilon)}$$

Parte 2. Per potere dimostrare che, per ogni s, k tali che $R(s, k)$ vale che $p(s, k)$, è sufficiente dimostrare che:

$R0$) $\forall m \in \mathbb{N}.\ p(m : \epsilon, 0)$
$R1$) $\forall m, l, k \in \mathbb{N}, s \in S.\ p(m : s, k) \implies p(l : 2m : s, l + k)$

Parte 3. Basta scegliere

$$p(s,k):\ Q(s) \implies k \text{ pari}$$

Parte 4. Applichiamo quindi il principio di induzione su R. Abbiamo due casi da dimostrare.

Caso $[R0]$**.** Senza ipotesi induttive, dobbiamo dimostrare $p(m:\epsilon,0)$. Quindi, assumendo $Q(m:\epsilon)$, dobbiamo dimostrare che 0 è pari. La tesi è banalmente vera.

Caso $[R1]$**.** Come ipotesi induttiva assumiamo $IP1 : p(m:s,k)$, ovvero

$$Q(m:s) \implies k \text{ pari}$$

e andiamo a dimostrare che vale $p(l:2m:s,l+k)$. Per farlo, assumiamo $IP2 : Q(l:2m:s)$ e dimostriamo che $l+k$ è pari.

Invertendo $IP2$, osserviamo che solo la regola $[Q1]$ può derivarlo, siccome $[Q0]$ genera solo una sequenza con un singolo naturale. Otteniamo che, per un qualche n, si deve avere $IP3 : l = 2m = 2n$ e $IP4 : Q(n:s)$. In particolare, l è pari.

Da $IP3$ segue $m = n$ e quindi $IP4$ diventa $Q(m:s)$ da cui con $IP1$ ricaviamo che k è pari.

Quindi, $l+k$ è una somma di pari, e quindi pari. □

Esercizio 3. *Dati due comandi di IMP c_1, c_2, si considerino le proprietà:*

$$P:\ \forall \sigma, \sigma'.\ \langle c_1, \sigma\rangle \to_b \sigma' \iff \langle c_2, \sigma\rangle \to_b \sigma'$$
$$Q:\ \forall \sigma, \sigma_1, \sigma_2.\ \langle c_1, \sigma\rangle \to_b \sigma_1 \wedge \langle c_2, \sigma\rangle \to_b \sigma_2 \implies \sigma_1 = \sigma_2$$

1. *[50%] Si dimostri che, in generale, P e Q* **non** *sono equivalenti. Nel farlo, si esibiscano due comandi c_1, c_2 come controesempio, e si giustifichi perché l'equivalenza tra P e Q non vale sui comandi esibiti.*

2. *[50%] Si dimostri che, anche se in generale non vale l'equivalenza, una delle due implicazioni vale. Si dica quale delle due implicazioni ($P \implies Q$ oppure $Q \implies P$) vale per ogni c_1, c_2, e la si dimostri.*

Soluzione (bozza).

Parte 1.

Basta prendere $c_1 = (\mathsf{while}\ 1 \neq 0\ \mathsf{do}\ \mathsf{skip})$ e $c_2 = \mathsf{skip}$. In questo modo, P diventa falsa, mentre Q diventa vera.

Infatti, P è falsa perché, scegliendo (per esempio) $\sigma(x) = \sigma'(x) = 0$ per ogni variabile x, si ha che $\langle c_2, \sigma\rangle \to_b \sigma'$ vale (lo skip termina nello stesso stato) mentre $\langle c_1, \sigma\rangle \to_b \sigma'$ non vale (il while non termina).

Invece, Q è vera perché l'implicazione ha l'antecedente falsa. Più in dettaglio, $\langle c_1, \sigma\rangle \to_b \sigma_1$ non vale, visto che il while non termina.

Parte 2. Vale che $P \implies Q$. Assumiamo dati $\sigma, \sigma_1, \sigma_2$, e le ipotesi $IP1 : \langle c_1, \sigma\rangle \to_b \sigma_1$ e $IP2 : \langle c_2, \sigma\rangle \to_b \sigma_2$.

Usando P (su σ, σ_1), possiamo riscrivere $IP1$ in modo equivalente come $IP3 : \langle c_2, \sigma \rangle \to_b \sigma_1$. Quindi, usando $IP3, IP2$, per il determinismo di $(\to_b)$ concludiamo che $\sigma_1 = \sigma_2$.

□

Nome _____ Matricola _____

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

$\{n = N\}$

$x := 0;$

$y := 2;$

$z := 0;$

---

while $z \neq n$ do

$x := 3 * x + y;$

$z := z + 1;$

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

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

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

Per le PrePost:
1) banale aritmetica.
2) Le prime due tesi sono uguali alle ipotesi. Per la tesi rimanente, si ha, usando le ipotesi $x = 3^z - 1$ e $y = 2$:

$$3x + y = 3(3^z - 1) + 2 = 3^{z+1} - 3 + 2 = 3^{z+1} - 1$$

3) Dall'ultima ipotesi, otteniamo $z = n$, che con l'ipotesi $n = N$ implica $z = N$. Questo e l'ipotesi $x = 3^z - 1$ dimostra la tesi.

□