Informatica — 2025-01-30

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

Esercizio 1. *Si enuncino tutti i risultati relativi al determinismo e alla totalità della semantica delle espressioni ($\to_e$) e dei comandi ($\to_b$) di IMP.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di interi (regole $[S0], [S1]$), una relazione $R \in \mathcal{P}(S \times S)$ (regole $[R0], [R1]$), e una relazione $Q \in \mathcal{P}(S \times \mathbb{Z})$ (regole $[Q0], [Q1]$). Sotto, a, b indicano interi, mentre s, t, u, z indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{a : s}(a \in \mathbb{Z})[S1] \quad \frac{}{R(\epsilon, \epsilon)}[R0] \quad \frac{R(s,\ z)}{R(a : s,\ a : (-a) : z)}[R1]$$

$$\frac{}{Q(\epsilon, 0)}[Q0] \quad \frac{Q(s,\ b)}{Q(a : s,\ b + a)}[Q1]$$

1. *[20%] Si trovino $z \in S, a \in \mathbb{Z}$ per cui valga $R(4 : 6 : \epsilon, z) \wedge Q(1 : 2 : 4 : \epsilon,\ a)$. 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:*

$$\forall s_1, s_2 \in S, a \in \mathbb{Z}.\ Q(s_2, a) \wedge R(s_1, s_2) \implies a = 0$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

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

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.

$$\cfrac{\cfrac{\cfrac{}{R(\epsilon, \epsilon)}[R0]}{R(6 : \epsilon, 6 : -6 : \epsilon)}[R1]}{R(4 : 6 : \epsilon, 4 : -4 : 6 : -6 : \epsilon)}[R1]$$

$$\cfrac{\cfrac{\cfrac{\cfrac{}{Q(\epsilon,\ 0)}[Q0]}{Q(4 : \epsilon,\ 4)}[Q1]}{Q(2 : 4 : \epsilon,\ 6)}[Q1]}{Q(1 : 2 : 4 : \epsilon,\ 7)}[Q1]$$

Parte 2.
Affinché valga $\forall t, u \in S.\ R(t, u) \implies p(t, u)$ basta che:

$R0)\ p(\epsilon,\ \epsilon)$
$R1)\ \forall s, z \in S, a \in \mathbb{Z}.\ p(s, z) \implies p(a : s,\ a : (-a) : z)$

Parte 3.
Basta prendere

$$p(t, u) :\ \forall a \in \mathbb{Z}.\ Q(u, a) \implies a = 0$$

Parte 4. **Caso** $[R0]$.

Dobbiamo dimostrare $p(\epsilon,\ \epsilon)$ e cioè $\forall a \in \mathbb{Z}.\ Q(\epsilon, a) \implies a = 0$. Assumiamo quindi $IP1 : Q(\epsilon, a)$ e dimostriamo $a = 0$.

Invertendo l'ipotesi $IP1$, notiamo che può essere derivata solo dalla regola $[Q0]$, da cui $a = 0$ che è la tesi.

Caso $[R1]$. Assumiamo l'ipotesi induttiva $IP1 : p(s, z)$ e cioè

$$IP1 :\ \forall \bar{a} \in \mathbb{Z}.\ Q(z, \bar{a}) \implies \bar{a} = 0$$

e dimostriamo la tesi $p(a : s,\ a : -a : z)$ e cioè

$$\forall \hat{a} \in \mathbb{Z}.\ Q(a : -a : z, \hat{a}) \implies \hat{a} = 0$$

Assumiamo quindi $IP2 : Q(a : -a : z, \hat{a})$ e dimostriamo la nuova tesi $\hat{a} = 0$.

Invertendo l'ipotesi $IP2$, notiamo che può essere derivata solo dalla regola $[Q1]$, da cui otteniamo $\hat{a} = b + a$ per qualche b tale che $IP3 : Q(-a : z, b)$.

Invertendo l'ipotesi $IP3$, notiamo che può essere derivata solo dalla regola $[Q1]$, da cui otteniamo $b = b' + (-a)$ per qualche b' tale che $IP4 : Q(z, b')$.

Usando $IP1$ (scegliendo $\bar{a} = b'$) assieme a $IP4$, otteniamo $b' = 0$.

Da tutte le equazioni ricavate otteniamo $\hat{a} = b + a = b' + (-a) + a = b' = 0$ che è la tesi.

□

Esercizio 3. *Sia IMP^a il frammento di IMP ottenuto rimuovendo il ciclo* while *dal linguaggio. Sia IMP^b il linguaggio ottenuto rimuovendo il condizionale* if *da IMP^a, e aggiungendo il comando* postif $e \neq 0$ then c_1 else c_2 *con la semantica informale seguente.*

Il condizionale postif *è simile all'*if*, ma controlla se la condizione $e \neq 0$ sarebbe vera dopo l'esecuzione di c_1 invece che prima di esso. Per esempio, eseguendo* postif $x \neq 0$ then $x := x - 6; y := 1$ else $y := 2$ *in uno stato iniziale σ si ottiene uno stato finale σ' in questo modo: se $\sigma(x) \neq 6$, allora $\sigma' = \sigma[x \mapsto \sigma(x) - 6][y \mapsto 1]$, altrimenti $\sigma' = \sigma[y \mapsto 2]$.*

1. *[60%] Si definisca la semantica big step di IMP^b tramite regole di inferenza.*
2. *[40%] Si descriva, in maniera informale ma chiara, come trasformare un comando c_a di IMP^a in uno c_b di IMP^b in modo essenzialmente equivalente. Più precisamente, si indichi con la relazione $\sigma_1 \sim_V \sigma_2$ la proprietà $\forall x \in V.\ \sigma_1(x) = \sigma_2(x)$, dove $V \subseteq Var$ indica un insieme di variabili intuitivamente ritenute "importanti". Dato c_a e un arbitrario V finito che contiene (almeno) tutte le variabili menzionate in c_a, si costruisca c_b in modo che, per ogni $\sigma_1, \sigma_2, \sigma_1', \sigma_2'$,*

$$\sigma_1 \sim_V \sigma_2 \wedge \langle c_a, \sigma_1\rangle \to_b \sigma_1' \wedge \langle c_b, \sigma_2\rangle \to_b \sigma_2' \implies \sigma_1' \sim_V \sigma_2'$$

Soluzione (bozza).
Parte 1.

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

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

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

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

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

Parte 2.

Procediamo ricorsivamente: mentre trasformiamo c_a assumeremo di sapere come trasformare i suoi sotto-comandi in comandi di IMP^b.

I comandi skip e assegnamento non necessitano di traduzione.

Per $c_1; c_2$, possiamo trasformare ricorsivamente c_1 e c_2 nei comandi c'_1 e c'_2 di IMP^b, e poi prendere $c'_1; c'_2$.

Per il condizionale if $e \neq 0$ then c_1 else c_2, iniziamo con lo scegliere una variabile x non usata in nessun punto nel comando. Formalmente, dato V, scegliamo una qualunque $x \in Var \setminus V$ (che non è vuoto visto che V è finito). Poi, trasformiamo ricorsivamente c_1 e c_2 nei comandi c'_1 e c'_2 di IMP^b secondo il nuovo insieme finito $V \cup \{x\}$. In questo modo, siamo sicuri che c'_1 e c'_2 non interferiscono in nessun modo con la variabile x.

Infine, il comando tradotto sarà

$$\mathsf{postif}\ x \neq 0\ \mathsf{then}\ x := e; c'_1\ \mathsf{else}\ c'_2$$

Questo è equivalente all'if perché $x := e$ assegna a x il valore di e nello stato iniziale, e poi x non viene più modificata da c'_1. Quindi postif $x \neq 0$ controlla effettivamente la stessa condizione di if $e \neq 0$.

$\square$

Nome ______________________________________ Matricola ______________

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

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

____

$y := 0;$

____

while $n \geq 0$ do

____

____

if n *pari* then

____

____

$y := y + n;$

____

$n := n - 3$

else

____

____

$y := y + 2;$

____

$n := n - 1$

____

$\{y \ pari \wedge n \ dispari\}$

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

____

____

____

____

____

____

____

Soluzione (bozza).

$\{n = N \geq 0\}$ (1)
$\{0 \text{ pari} \land (n < 0 \implies n \text{ dispari})\}$
$y := 0;$
$\{INV : y \text{ pari} \land (n < 0 \implies n \text{ dispari})\}$
while $n \geq 0$ do
    $\{INV \land n \geq 0\}$
    if n pari then
        $\{INV \land n \geq 0 \land n \text{ pari}\}$ (2)
        $\{y + n \text{ pari} \land (n - 3 < 0 \implies n - 3 \text{ dispari})\}$
        $y := y + n;$
        $\{y \text{ pari} \land (n - 3 < 0 \implies n - 3 \text{ dispari})\}$
        $n := n - 3$
    else
        $\{INV \land n \geq 0 \land \neg(n \text{ pari})\}$ (3)
        $\{y + 2 \text{ pari} \land (n - 1 < 0 \implies n - 1 \text{ dispari})\}$
        $y := y + 2;$
        $\{y \text{ pari} \land (n - 1 < 0 \implies n - 1 \text{ dispari})\}$
        $n := n - 1$
$\{INV \land \neg(n \geq 0)\}$ (4)
$\{y \text{ pari} \land n \text{ dispari}\}$

Per le PrePost:

1) Banale aritmetica. L'implicazione vale perché l'antecedente è falsa per ipotesi.

2) Da INV abbiamo che y è pari, e siccome per ipotesi anche n è pari si ha che $y + n$ è pari. Da n pari otteniamo anche $n - 3$ dispari, quindi vale l'implicazione $n - 3 < 0 \implies n - 3$ dispari perché la conseguente è vera.

3) Da INV abbiamo che y è pari, quindi anche $y + 2$. Siccome n è dispari ma anche ≥ 0, deve essere $n \geq 1$. Quindi l'implicazione $n - 1 < 0 \implies n - 1$ dispari vale perché l'antecedente è falsa.

4) y pari deriva da INV. Siccome per ipotesi $n < 0$ dall'implicazione dentro INV ricaviamo n dispari.

□