Informatica — 2026-02-19

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

Esercizio 1. *Si definiscano le regole del sistema deduttivo per le triple di Hoare.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi di naturali (regole $[T0], [T1]$), una relazione $R \in \mathcal{P}(T \times \mathbb{N})$ (regole $[R0], [R1]$), e una relazione $Q \in \mathcal{P}(T \times T)$ (regole $[Q0], [Q1]$). Sotto, si assume $s, d, t \in T$ e $n, a \in \mathbb{N}$.*

$$\frac{}{n}(n \in \mathbb{N})[T0] \quad \frac{s \quad d}{(s,d)}[T1] \quad \frac{}{Q(n\,,\,(n,n))}[Q0] \quad \frac{Q(s,s') \quad Q(d,d')}{Q((s,d),(s',d'))}[Q1]$$

$$\frac{}{R(n,1)}[R0] \quad \frac{R(s,n_s) \quad R(d,n_d)}{R((s,d),1+\max(n_s,n_d))}[R1]$$

1. *[20%] Si trovi un albero t per cui valga $R(t,3)$. Si giustifichi la risposta esibendo una derivazione.*

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

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

$$\forall t_1, t_2 \in T, a \in \mathbb{N}.\ R(t_1,a) \land Q(t_1,t_2) \implies R(t_2, a+1)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t_1, t_2 \in T.\ Q(t_1,t_2) \implies p(t_1,t_2)$$

per un qualche predicato p.

4. *[50%] Si dimostri l'enunciato sopra usando il principio di induzione associato a Q.*

Soluzione (bozza).
Parte 1.
Una possibile soluzione è:

$$\frac{\dfrac{}{R(30,1)}[R0] \qquad \dfrac{\dfrac{}{R(10,1)}[R0] \qquad \dfrac{}{R(20,1)}[R0]}{R((10,20),2)}[R1]}{R((30,(10,20)),3)}[R1]$$

Parte 2.
Affinché valga $\forall t_1, t_2 \in T.\ Q(t_1,t_2) \implies p(t_1,t_2)$ basta che

$$Q0)\ \forall n.\ p(n,(n,n))$$
$$Q1)\ \forall s, s', d, d'.\ p(s,s') \land p(d,d') \implies p((s,d),(s',d'))$$

Parte 3.
Basta prendere $p(t_1,t_2) :\ \forall a \in \mathbb{N}.\ R(t_1,a) \implies R(t_2,a+1)$.
Parte 4.
Caso [**Q0**]. Dobbiamo dimostrare $p(n,(n,n))$ ovvero $\forall a.\ R(n,a) \implies R((n,n),a+1)$.
Assumiamo quindi $IP1 : R(n,a)$ e dimostriamo la nuova tesi $R((n,n),a+1)$.
Invertendo $IP1$, osserviamo che può essere ricavata solo da $Q0$ e quindi $a = 1$. La tesi diventa $R((n,n),2)$ e si ricava come:

$$\frac{\dfrac{}{R(n,1)}[R0] \qquad \dfrac{}{R(n,1)}[R0]}{R((n,n),1+\max(1,1))}[R1]$$

(Nota: non è l'unica dimostrazione possibile, l'inversione non è davvero necessaria).

Caso [**Q1**].

Assumiamo le ipotesi induttive $IP1 : p(s, s')$ e $IP2 : p(d, d')$, e dimostriamo la tesi $p((s, d), (s', d'))$.

$$\begin{array}{l} IP1 : \ \forall a \in \mathbb{N}.R(s, a) \implies R(s', a + 1) \\ IP2 : \ \forall b \in \mathbb{N}.R(d, b) \implies R(d', b + 1) \\ tesi : \ \forall n \in \mathbb{N}.R((s, d), n) \implies R((s', d'), n + 1) \end{array}$$

Assumiamo quindi $IP3 : R((s, d), n)$ e dimostriamo la nuova tesi $R((s', d'), n + 1)$.

Invertendo $IP3$, osserviamo che può essere ricavata solo da $R1$ e quindi si ottiene $n = 1 + \max(n_s, n_d)$ con $IP4 : R(s, n_s)$ e $IP5 : R(d, n_d)$.

Usiamo $IP1$ scegliendo $a = n_s$ assieme a $IP4$, e otteniamo $IP6 : R(s', n_s + 1)$.

Usiamo $IP2$ scegliendo $b = n_d$ assieme a $IP5$, e otteniamo $IP7 : R(d', n_d + 1)$.

Applicando [$R1$] a $IP6, IP7$, ricaviamo $R((s', d'), 1 + \max(n_s + 1, n_d + 1)$ che è la tesi desiderata visto che $1 + \max(n_s + 1, n_d + 1) = 1 + \max(n_s, n_d) + 1 = n + 1$.

□

Esercizio 3. *Si consideri una variante del linguaggio IMP chiamata DIMP che contiene soltanto i seguenti comandi:* skip*, la composizione* $c_1 ; c_2$ *e il nuovo comando* dif *("doppio* if*") avente sintassi* (dif $e \neq 0$ then $x := e_1$ else $y := e_2$) *dove* $e, e_1, e_2 \in Exp$ *e* $x, y \in Var$ *sono arbitrarie. Le espressioni di DIMP sono le stesse di IMP.*

La semantica intuitiva di DIMP è la stessa di IMP per skip *e la composizione, mentre il comando* dif *ha lo stesso comportamento che si avrebbe in IMP se eseguissimo il comando* (if $e \neq 0$ then $x := e_1$ else $y := e_2$); (if $e \neq 0$ then $x := e_1$ else $y := e_2$).

1. *[40%] Si formalizzi la semantica big step* $(\rightarrow_b) \in \mathcal{P}(Com \times State \times State)$ *di DIMP con opportune regole di inferenza.*

2. *[30%] Sia* e *un'espressione al cui interno non appare la variabile* x*. Si costruisca un comando* c *di DIMP la cui semantica sia identica a quella che in IMP ha il comando* $x := e$*. Si giustifichi informalmente la soluzione.*

3. *[30%] Siano* x, y *variabili arbitrarie distinte ed* e *un'espressione arbitraria (*x *e* y *possono apparire dentro* e*). Si costruisca un comando* c *di DIMP la cui semantica sia identica a quella che in IMP ha il comando* $(y := 0; x := e)$*. Si giustifichi informalmente la soluzione.*

Soluzione (bozza).

Parte 1.

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

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

$$\frac{\begin{array}{lll}\langle e,\sigma\rangle \to_e v \neq 0 & \langle e_1,\sigma\rangle \to_e v_1 & \sigma' = \sigma[x \mapsto v_1] \\ \langle e,\sigma'\rangle \to_e v' \neq 0 & \langle e_1,\sigma'\rangle \to_e v_2 & \sigma'' = \sigma'[x \mapsto v_2]\end{array}}{\langle \mathsf{dif}\ e \neq 0\ \mathsf{then}\ x := e_1\ \mathsf{else}\ y := e_2\ ,\ \sigma\rangle \to_b \sigma''}[Dif - TT]$$

$$\frac{\begin{array}{lll}\langle e,\sigma\rangle \to_e v \neq 0 & \langle e_1,\sigma\rangle \to_e v_1 & \sigma' = \sigma[x \mapsto v_1] \\ \langle e,\sigma'\rangle \to_e 0 & \langle e_2,\sigma'\rangle \to_e v_2 & \sigma'' = \sigma'[y \mapsto v_2]\end{array}}{\langle \mathsf{dif}\ e \neq 0\ \mathsf{then}\ x := e_1\ \mathsf{else}\ y := e_2\ ,\ \sigma\rangle \to_b \sigma''}[Dif - TF]$$

$$\frac{\begin{array}{lll}\langle e,\sigma\rangle \to_e 0 & \langle e_2,\sigma\rangle \to_e v_1 & \sigma' = \sigma[y \mapsto v_1] \\ \langle e,\sigma'\rangle \to_e v' \neq 0 & \langle e_1,\sigma'\rangle \to_e v_2 & \sigma'' = \sigma'[x \mapsto v_2]\end{array}}{\langle \mathsf{dif}\ e \neq 0\ \mathsf{then}\ x := e_1\ \mathsf{else}\ y := e_2\ ,\ \sigma\rangle \to_b \sigma''}[Dif - FT]$$

$$\frac{\begin{array}{lll}\langle e,\sigma\rangle \to_e 0 & \langle e_2,\sigma\rangle \to_e v_1 & \sigma' = \sigma[y \mapsto v_1] \\ \langle e,\sigma'\rangle \to_e 0 & \langle e_2,\sigma'\rangle \to_e v_2 & \sigma'' = \sigma'[y \mapsto v_2]\end{array}}{\langle \mathsf{dif}\ e \neq 0\ \mathsf{then}\ x := e_1\ \mathsf{else}\ y := e_2\ ,\ \sigma\rangle \to_b \sigma''}[Dif - FF]$$

Parte 2.

Basta prendere una e' qualunque (per esempio $e' = 1$) ed eseguire

$$c = \ \mathsf{dif}\ e' \neq 0\ \mathsf{then}\ x := e\ \mathsf{else}\ x := e$$

Visto che i due rami hanno lo stesso assegnamento, qualunque sia e' questo comando esegue due volte $x := e$, come se in IMP eseguissimo $x := e\,;\, x := e$.

Siccome e non dipende da x per ipotesi, la valutazione di e non è influenzata dal primo dei due assegnamenti eseguiti, e quindi il secondo assegnamento riassegna lo stesso valore assegnato dal primo. Quindi il dif sopra è equivalente ad eseguire in IMP il comando $x := e$.

Parte 3.

Basta prendere

$$c = \ (\mathsf{dif}\ 1 \neq 0\ \mathsf{then}\ y := 1\ \mathsf{else}\ y := 1); (\mathsf{dif}\ y \neq 0\ \mathsf{then}\ y := 0\ \mathsf{else}\ x := e)$$

Il primo dif esegue $y := 1$ due volte. La variabile y diventa quindi 1.

Il secondo dif osserva che la guardia $y \neq 0$ è vera, ed esegue il ramo then $(y := 0)$ impostando ora y a 0. Dopo, si osserva che la guardia $y \neq 0$ è diventata falsa e si esegue il ramo else $(x := e)$.

Il risultato effettivo è quello di eseguire $y := 1; y := 1; y := 0; x := e$ che è equivalente a $y := 0; x := e$.

□

Nome _____ Matricola _____

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

$\{0 \leq n \text{ } pari\}$

$x := 0;$

$y := 0;$

---

while $y < n$ do

---

if y *pari* then

$x := x + 6 * y * y + 12 * y + 10$

else

$x := 123;$

$y := y + 2$

$\{x = n^3 + n\}$

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

Soluzione (bozza).

$\{0 \leq n \text{ pari}\}$ (1)
$\{0 \text{ pari} \wedge 0 = 0^3 + 0 \wedge 0 \leq n \text{ pari}\}$
$x := 0;$
$\{0 \text{ pari} \wedge x = 0^3 + 0 \wedge 0 \leq n \text{ pari}\}$
$y := 0;$
$\{INV : \ y \text{ pari} \wedge x = y^3 + y \wedge y \leq n \text{ pari}\}$
while $y < n$ do
    $\{INV \wedge y < n\}$
    if y pari then
        $\{INV \wedge y < n \wedge y \text{ pari}\}$ (2)
        $\{y + 2 \text{ pari} \wedge x + 6 * y * y + 12 * y + 10 = (y + 2)^3 + y + 2 \wedge y + 2 \leq n \text{ pari}\}$
        $x := x + 6 * y * y + 12 * y + 10$
    else
        $\{INV \wedge y < n \wedge \neg(y \text{ pari})\}$ (3)
        $\{y + 2 \text{ pari} \wedge 123 = (y + 2)^3 + y + 2 \wedge y + 2 \leq n \text{ pari}\}$
        $x := 123;$
    $\{y + 2 \text{ pari} \wedge x = (y + 2)^3 + y + 2 \wedge y + 2 \leq n \text{ pari}\}$
    $y := y + 2$
$\{INV \wedge \neg(y < n)\}$
$\{x = n^3 + n\}$

Per le PrePost:
1) Banale aritmetica.
2) Siccome y e n sono pari per ipotesi e $y < n$, ne segue che $y + 2$ è pari e $\leq n$.
Per ipotesi $x = y^3 + y$, quindi l'equazione a tesi diventa $(y^3 + y) + 6y^2 + 12 * y + 10 = (y + 2)^3 + y + 2$ e quindi $y^3 + 6y^2 + 13 * y + 10 = y^3 + 6y^2 + 12y + 8 + y + 2$ che è vera.
3) Per ipotesi abbiamo y pari e $\neg(y \text{ pari})$ da cui un assurdo. La tesi segue vacuamente.
4) Per ipotesi abbiamo $y \leq n$ e $\neg(y < n)$ da cui $y = n$. Sempre per ipotesi $x = y^3 + y$ da cui la tesi $x = n^3 + n$.

□