Informatica — 2025-02-19

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

Esercizio 1. *Si forniscano le regole della semantica big step per i comandi di IMP* $(\to_b)$*. Si fornisca anche la segnatura della relazione semantica* $(\to_b) \in \mathcal{P}(\ldots)$*, descrivendo brevemente gli insiemi che appaiono in essa.*

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

$$\frac{}{k}(k \in \mathbb{N})[T0] \quad \frac{s \quad d}{(s,d)}[T1] \quad \frac{}{R(n,k,k+n)}[R0] \quad \frac{R(n_1,s,s') \quad R(n_2,d,d')}{R(n_1+n_2,(s,d),(s',d'))}[R1]$$

1. *[20%] Si trovi un* $t \in T$ *per cui valga* $R(10,((1,2),3),t)$*. Si giustifichi la risposta esibendo una derivazione.*

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

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

$$\forall n_1, n_2 \in \mathbb{N}, t_1, t_2, t_3 \in T.\ R(n_1,t_1,t_2) \land R(n_2,t_2,t_3) \implies R(n_1+n_2,t_1,t_3).$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall n \in \mathbb{N}, t, u \in T.\ R(n,t,u) \implies p(n,t,u)$$

   per un qualche predicato p*, facendo corrispondere* $R(n,t,u)$ *a* $R(n_1,t_1,t_2)$*.*

4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a* R*.*

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

$$\dfrac{\dfrac{\dfrac{}{R(1,1,2)}[R0] \quad \dfrac{}{R(4,2,6)}[R0]}{R(5,(1,2),(2,6))}[R1] \quad \dfrac{}{R(5,3,8)}[R0]}{R(10,((1,2),3),((2,6),8))}[R1]$$

Parte 2.
Affinché valga $\forall n \in \mathbb{N}, t, u \in T.\ R(n,t,u) \implies p(n,t,u)$ basta che:

$R0)$ $\forall n, k.\ p(n,k,k+n)$
$R1)$ $\forall n_1, n_2, s, s', d, d'.\ R(n_1,s,s') \land R(n_2,d,d') \implies R(n_1+n_2,(s,d),(s',d'))$

Parte 3.
Basta prendere $p(n,t,u) :\ \forall n_2 \in \mathbb{N}, t_3 \in T.\ R(n_2,u,t_3) \implies R(n+n_2,t,t_3)$.
Parte 4. **Caso** $[R0]$.
Dobbiamo dimostrare $p(n,k,k+n)$ e cioè

$$\forall n_2 \in \mathbb{N}, t_3 \in T.\ R(n_2,k+n,t_3) \implies R(n+n_2,k,t_3)$$

Assumiamo quindi $IP1 : R(n_2,k+n,t_3)$ e dimostriamo la nuova tesi $R(n+n_2,k,t_3)$.
Invertendo $IP1$, osserviamo che può solo essere derivata da $[R0]$ e quindi $t_3 = k+n+n_2$.
La tesi si riscrive quindi come $R(n+n_2,k,k+n+n_2)$, che vale per $[R0]$.
Caso $[R1]$.

Assumendo le ipotesi induttive $IP1 : R(n_1, s, s')$ e $IP2 : R(n_2, d, d')$, dobbiamo dimostrare $R(n_1 + n_2, (s, d), (s', d'))$.

$$
\begin{array}{l}
IP1 : \ \forall \bar{n}_2 \in \mathbb{N}, \bar{t}_3 \in T.\ R(\bar{n}_2, s', \bar{t}_3) \implies R(n_1 + \bar{n}_2, s, \bar{t}_3) \\
IP2 : \ \forall \hat{n}_2 \in \mathbb{N}, \hat{t}_3 \in T.\ R(\hat{n}_2, d', \hat{t}_3) \implies R(n_2 + \hat{n}_2, d, \hat{t}_3) \\
tesi : \ \forall \tilde{n}_2 \in \mathbb{N}, \tilde{t}_3 \in T.\ R(\tilde{n}_2, (s', d'), \tilde{t}_3) \implies R(n_1 + n_2 + \tilde{n}_2, (s, d), \tilde{t}_3)
\end{array}
$$

Assumiamo quindi $IP3 : \ R(\tilde{n}_2, (s', d'), \tilde{t}_3)$ e dimostriamo la nuova tesi $R(n_1 + n_2 + \tilde{n}_2, (s, d), \tilde{t}_3)$.

Invertendo $IP3$, notiamo che può derivare solo da $[R1]$ e quindi otteniamo $IP4 : R(a, s', s'')$, $IP5 : \ R(b, d', d'')$, con $\tilde{n}_2 = a + b$ e $\tilde{t}_3 = (s'', d'')$.

Usiamo $IP1$ (scegliendo $\bar{n}_2 = a, \bar{t}_3 = s''$) con $IP4$ e otteniamo $IP6 : \ R(n_1 + a, s, s'')$.

Usiamo $IP2$ (scegliendo $\hat{n}_2 = b, \hat{t}_3 = d''$) con $IP5$ e otteniamo $IP7 : \ R(n_2 + b, d, d'')$.

Applicando la regola $[R1]$ a $IP6, IP7$, otteniamo $R(n_1 + a + n_2 + b, (s, d), (s'', d''))$ che grazie alle equazioni sopra si riscrive come $R(n_1 + n_2 + \tilde{n}_2, (s, d), \tilde{t}_3)$ che è la tesi.

□

Esercizio 3. *Si consideri una variante IMP^1 del linguaggio IMP ottenuta restringendo gli assegnamenti alle sole seguenti tre forme: (i) $x := z$ (con $z \in \mathbb{Z}$ costante), (ii) $x := x + 1$, (iii) $x := x - 1$. Le guardie dell'* if *e del* while *possono invece contenere espressioni aritmetico-logiche anche complesse, usando gli operatori $+, -, *, <, \leq, =, \wedge, \neg$ oltre a costanti e variabili.*

1. *[60%] Si costruisca un comando c di IMP^1 che abbia lo stesso effetto del comando $x := e$ di IMP, per qualunque $x \in Var, e \in Exp$ dove x non appare all'interno di e. Nel definire c è ammesso l'uso di variabili addizionali "di appoggio": la modifica del loro valore non viene considerata parte dell'effetto di c. Non si richiede che c sia efficiente. Si giustifichi informalmente la risposta.*

2. *[40%] Relativamente al punto sopra, si descriva come trattare anche il caso generale, dove x può apparire dentro e. Si giustifichi informalmente la risposta.*

Soluzione (bozza).
(Illustriamo qui solo una delle tante possibili soluzioni.)
Parte 1. Possiamo definire c come segue:

```
x := 0;
if e < 0 then
    while ¬(x = e) do
        x := x − 1
else
    while ¬(x = e) do
        x := x + 1
```

La modifica di x non ha effetti sulla valutazione di e, visto che x non appare in e. Quindi e mantiene il suo valore originale per tutto il comando sopra. Se $e < 0$, partendo da $x = 0$ prima o poi raggiungeremo il valore di e decrementando ripetutamente la x. Lo stesso vale per $e \geq 0$ quando la x viene invece incrementata.

Parte 2.

Dato un assegnamento arbitrario $x := e$, dove x può essere usata in e, procediamo come segue. Per prima cosa, prendiamo una variabile di appoggio t diversa da x e dalle variabili usate in e.

Ora osserviamo che $x := e$ può essere riscritto in forma essenzialmente equivalente come $t := e;\ x := t$: questo ha lo stesso effetto di $x := e$ se ignoriamo la variabile di appoggio t.

A questo punto basta notare che i due assegnamenti $t := e$ e $x := t$ soddisfano la ipotesi del punto precedente: t non appare nell'espressione e, e x non appare nell'espressione t. Possiamo quindi tradurli individualmente usando la tecnica precedente. Il risultato finale quindi è:

$t := 0;$
if $e < 0$ then
    while $\neg(t = e)$ do
        $t := t - 1$
else
    while $\neg(t = e)$ do
        $t := t + 1$
$x := 0;$
if $t < 0$ then
    while $\neg(x = t)$ do
        $x := x - 1$
else
    while $\neg(x = t)$ do
        $x := x + 1$

□

Nome _____ Matricola _____

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

$\{n = 2N \geq 0\}$

$x := 0;$

$y := 0;$

---

while $x < n$ do

---

if x *dispari* then

$y := y + 2;$

$x := x + 1$

else

$x := x + 1$

$\{y = 2N\}$

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

Soluzione (bozza).

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

Per le PrePost:

1) La prima tesi è parte delle ipotesi. La seconda tesi vale perché $0 = 0$ è vero. La terza tesi vale perché 0 non è dispari.

2) Dalle ipotesi si ha $x < n = 2N$, da cui la prima tesi $x \leq n = 2N$ visto che sono interi. Visto che x è dispari, da INV abbiamo $y = x - 1$ quindi $y + 2 = x + 1$ che dimostra la seconda tesi. La terza tesi vale perché $x + 1$ non è dispari visto che lo è x.

3) Dalle ipotesi si ha $x < n = 2N$, da cui la prima tesi $x \leq n = 2N$ visto che sono interi. La seconda tesi vale perché $x + 1$ non è pari visto che lo è x. Visto che x è pari, da INV abbiamo $y = x$ quindi $y = x + 1 - 1$ che dimostra la terza tesi.

4) Da INV e $\neg(x < n)$ ricaviamo $x = n = 2N$ pari, e quindi usando di nuovo INV anche $y = x = n = 2N$ pari.

□