Informatica — 2025-07-14

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

Esercizio 1. *Dato un insieme di regole $\mathcal{R}$ su U, si definisca l'associato operatore delle conseguenze immediate $\hat{\mathcal{R}} : \mathcal{P}(U) \to \mathcal{P}(U)$. Si dimostri che è monotono.*

Esercizio 2. *Le seguenti regole definiscono induttivamente una relazione $R \in \mathcal{P}(\mathbb{N} \times \mathbb{R})$ (regole $[R0], [R1]$). Sotto, si assume $n, n_1, n_2 \in \mathbb{N}, x, x_1, x_2 \in \mathbb{R}$.*

$$\frac{n > 0}{R(n, n \cdot \sqrt{2^n})}[R0] \qquad \frac{R(n_1, x_1) \quad R(n_2, x_2)}{R(n_1 + n_2\ ,\ x_1 \cdot x_2)}[R1]$$

1. *[20%] Si trovino tre valori distinti $x \in \mathbb{R}$ per cui valga $R(7, x)$. Si giustifichi la risposta esibendo tre derivazioni.*
2. *[20%] Si enunci il principio di induzione associato alla relazione R.*
3. *[10%] Si consideri l'enunciato seguente:*

$$\begin{array}{l} \forall n \in \mathbb{N}, x \in \mathbb{R}. \\ \quad \Big((R(n, x) \ \wedge \ n \text{ pari}) \implies x \in \mathbb{N}\Big) \wedge \\ \quad \Big((R(n, x) \ \wedge \ n \text{ dispari}) \implies \exists m \in \mathbb{N}.\ x = m \cdot \sqrt{2}\Big) \end{array}.$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

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

   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. Una possibile derivazione è:

$$\frac{}{R(7, 7\sqrt{2^7})}[R0]$$

con $7\sqrt{2^7} = 56\sqrt{2}$. Un'altra possibile derivazione è:

$$\frac{\dfrac{}{R(1, 1\sqrt{2^1})}[R0] \quad \dfrac{}{R(6, 6\sqrt{2^6})}[R0]}{R(7, \sqrt{2} \cdot 6 \cdot 2^3)}[R1]$$

con $\sqrt{2} \cdot 6 \cdot 2^3 = 48\sqrt{2}$. Un'altra possibile derivazione è:

$$\frac{\dfrac{}{R(3, 3\sqrt{2^3})}[R0] \quad \dfrac{}{R(4, 4\sqrt{2^4})}[R0]}{R(7, 6\sqrt{2} \cdot 16)}[R1]$$

con $6\sqrt{2} \cdot 16 = 96\sqrt{2}$.

Parte 2. Affinché valga $\forall n, x.\ R(n, x) \implies p(n, x)$ è sufficiente che:

$R0)$ $\forall n.\ n > 0 \implies p(n, n \cdot \sqrt{2^n})$
$R1)$ $\forall n_1, n_2, x_1, x_2.\ p(n_1, x_1) \wedge p(n_2, x_2) \implies p(n_1 + n_2, x_1 \cdot x_2)$

Parte 3.

Basta prendere

$$p(n, x) : \ (n \text{ pari } \implies x \in \mathbb{N}) \wedge (n \text{ dispari } \implies \exists m \in \mathbb{N}.\ x = m \cdot \sqrt{2})$$

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

Dato $n > 0$, dimostriamo $p(n, n\sqrt{2^n})$.

Se n è pari, diciamo $n = 2k$, allora la tesi si riduce a dimostrare $n\sqrt{2^n} \in \mathbb{N}$. Questo vale perché $n\sqrt{2^n} = 2k\sqrt{2^{2k}} = 2k \cdot 2^k \in \mathbb{N}$.

Se n è dispari, diciamo $n = 2k+1$, allora la tesi si riduce a dimostrare $\exists m \in \mathbb{N}.\ n\sqrt{2^n} = m\sqrt{2}$. Questo vale perché $n\sqrt{2^n} = (2k+1)\sqrt{2^{2k+1}} = (2k+1) \cdot 2^k\sqrt{2}$ e quindi basta scegliere $m = (2k + 1) \cdot 2^k \in \mathbb{N}$.

Caso $[R1]$.

Assumiamo le ipotesi induttive $IP1 :\ p(n_1, x_1)$ e $IP2 :\ p(n_2, x_2)$, e dimostriamo la tesi $p(n_1 + n_2, x_1x_2)$.

Ci sono quattro sottocasi da considerare, a seconda della parità di n_1 e n_2:

- Caso n_1 pari e n_2 pari: qui $n_1 + n_2$ è pari e quindi la tesi si riduce a dimostrare $x_1x_2 \in \mathbb{N}$. Da $IP1$ e $IP2$ otteniamo $x_1 \in \mathbb{N}$ e $x_2 \in \mathbb{N}$, da cui la tesi.

- Caso n_1 pari e n_2 dispari: qui $n_1 + n_2$ è dispari e quindi la tesi si riduce a dimostrare $\exists m \in \mathbb{N}.\ x_1x_2 = m\sqrt{2}$. Da $IP1$ e $IP2$ otteniamo $x_1 \in \mathbb{N}$ e $\exists m_2 \in \mathbb{N}. x_2 = m_2\sqrt{2} \in \mathbb{N}$. Per ottenere la tesi, basta scegliere $m = x_1m_2 \in \mathbb{N}$ da cui $m\sqrt{2} = x_1m_2\sqrt{2} = x_1x_2$.

- Caso n_1 dispari e n_2 pari: qui $n_1 + n_2$ è dispari e quindi la tesi si riduce a dimostrare $\exists m \in \mathbb{N}.\ x_1x_2 = m\sqrt{2}$. Da $IP1$ e $IP2$ otteniamo $\exists m_1 \in \mathbb{N}. x_1 = m_1\sqrt{2} \in \mathbb{N}$ e $x_2 \in \mathbb{N}$. Per ottenere la tesi, basta scegliere $m = m_1x_2 \in \mathbb{N}$ da cui $m\sqrt{2} = m_1x_2\sqrt{2} = x_1x_2$.

- Caso n_1 dispari e n_2 dispari: qui $n_1 + n_2$ è pari e quindi la tesi si riduce a dimostrare $x_1x_2 \in \mathbb{N}$. Da $IP1$ e $IP2$ otteniamo $\exists m_1 \in \mathbb{N}. x_1 = m_1\sqrt{2} \in \mathbb{N}$ e $\exists m_2 \in \mathbb{N}. x_2 = m_2\sqrt{2} \in \mathbb{N}$. Per ottenere la tesi, basta osservare $x_1x_2 = m_1\sqrt{2} \cdot m_2\sqrt{2} = 2m_1m_2 \in \mathbb{N}$.

$\square$

Esercizio 3. *Sia* $k \in \mathbb{N}^{>0}$, *e siano* $y, x_1, x_2, \ldots \in Var$ *nomi di variabili distinti fissati tali che* $Var \setminus \{y, x_1, x_2, \ldots\}$ *sia infinito. Una funzione* $f : \mathbb{N}^k \to \mathbb{N}$ *è detta* IMP-definibile *quando esiste un comando* c *di IMP tale che soddisfa la seguenti condizione:*

$$\begin{aligned}&\forall X_1, \ldots, X_k \in \mathbb{N}.\ \forall \sigma.\ \exists \sigma'.\\ &\quad \langle c, \sigma[x_1 \mapsto X_1, \ldots, x_k \mapsto X_k] \rangle \to_b \sigma' \quad \wedge \quad \sigma'(y) = f(X_1, \ldots, X_k)\end{aligned}$$

1. *[60%] Si dimostri che, se* $g : \mathbb{N}^2 \to \mathbb{N}$ *e* $h : \mathbb{N}^4 \to \mathbb{N}$ *sono funzioni IMP-definibili, allora anche la funzione* $f : \mathbb{N}^3 \to \mathbb{N}$ *definita induttivamente sotto è IMP-definibile. Per farlo, assumete che esistano due comandi* c_g *e* c_h *che IMP-definiscono le funzioni* g *e* h, *e costruite un comando* c_f *in modo da IMP-definire* f.

$$\begin{aligned} f(0, n, m) &= g(n, m) \\ f(i + 1, n, m) &= h(i, n, m, f(i, n, m)) \end{aligned}$$

2. *[40%] Si giustifichi informalmente la risposta, spiegando perché* c_f *soddisfa la condizione di IMP-definibilità.*

Soluzione (bozza).

Parte 1.

Una possibile IMP-definizione di f è:

$$
\begin{array}{l}
i := x_1; \\
n := x_2; \\
m := x_3; \\
x_1 := n; \\
x_2 := m; \\
c_g; \\
r := y; \\
j := 0; \\
\textsf{while } j < i \textsf{ do} \\
\qquad x_1 := j; \\
\qquad x_2 := n; \\
\qquad x_3 := m; \\
\qquad x_4 := r; \\
\qquad c_h; \\
\qquad r := y; \\
\qquad j := j + 1; \\
y := r
\end{array}
$$

dove i, n, m, r, j sono nomi di variabili distinti, diversi da $y, x_1, \ldots$, e che non appaiono in c_g e c_h. Una tale scelta è sempre possibile, visto che per ipotesi ci sono infinite variabili diversa da $y, x_1, \ldots$, e c_f, c_h ne possono usare solo un numero finito.

Parte 2. All'inizio il programma salva nelle variabili i, n, m gli argomenti di f, che chiamiamo X_1, X_2, X_3. Dopo, calcoliamo $g(n, m)$ impostando opportunamente x_1, x_2 ed eseguendo c_g. Il risultato di $f(0, n, m) = g(n, m)$ viene quindi messo in r, e j viene inizializzato a 0.

Qui parte il ciclo while, che ha come invariante

$$r = f(j, n, m) \land n = X_2 \land m = X_3 \land j \leq i = X_1$$

Come già descritto, l'invariante è vera prima che il while inizi.

Supponendo che l'invariante sia vera all'inizio di una qualunque iterazione del while, procediamo a calcolare $f(j + 1, n, m) = h(j, n, m, f(j, n, m)) = h(j, n, m, r)$ impostando opportunamente x_1, x_2, x_3, x_4 ed eseguendo c_h. Il risultato di $f(j + 1, n, m)$ viene quindi messo in r, e j viene incrementato. In questo modo, l'invariante viene preservata.

Alla fine del while abbiamo $j = i = X_1$, e quindi dall'invariante $r = f(X_1, X_2, X_3)$. Questo valore viene messo in y per soddisfare la condizione di IMP-definibilità

$\square$

Nome ______________________ Matricola ______________

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

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

____

$x := 0;$

____

$y := 0;$

____

while $y < n$ do

____

____

$x := x + 4 + 7 * y;$

____

$y := y + 1$

____

$\{2x = 7N^2 + N\}$

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

____

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$\{n = N \geq 0\}$ (1)
$\{2 \cdot 0 = 7 \cdot 0^2 + 0 \wedge 0 \leq n = N\}$
$x := 0;$
$\{2x = 7 \cdot 0^2 + 0 \wedge 0 \leq n = N\}$
$y := 0;$
$\{INV:\ 2x = 7y^2 + y \wedge y \leq n = N\}$
while $y < n$ do
  $\{INV \wedge y < n\}$ (2)
  $\{2(x + 4 + 7y) = 7(y + 1)^2 + y + 1 \wedge y + 1 \leq n = N\}$
  $x := x + 4 + 7 * y;$
  $\{2x = 7(y + 1)^2 + y + 1 \wedge y + 1 \leq n = N\}$
  $y := y + 1$
$\{INV \wedge \neg(y < n)\}$ (3)
$\{2x = 7N^2 + N\}$

Per le PrePost:

1) Banale aritmetica.

2) Dalle ipotesi $y < n = N$ e, visto che sono interi, si ricava $y+1 \leq n = N$. L'equazione nella tesi $2(x+4+7*y) = 7(y+1)^2+y+1$ si riscrive come $2x+8+14y = 7y^2+14y+7+y+1$ e quindi come $2x = 7y^2 + y$ che è parte dell'ipotesi INV.

3) Da INV si ha $y \leq n = N$ che assieme a $\neg(y < n)$ fornisce $y = n = N$. Dal questo e dal resto di INV si ha la tesi $2x = 7N^2 + N$.

□