

Informatica — 2026-07-21

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 ($\rightarrow_e$) e dei comandi ($\rightarrow_b$) di IMP.

Esercizio 2. Le seguenti regole definiscono induttivamente l'insieme S delle sequenze finite di interi (regole $[S0], [S1]$), una relazione $Q \in \mathcal{P}(S \times \mathbb{Z})$ (regole $[Q0], [Q1]$), e una relazione $R \in \mathcal{P}(S \times S)$ (regole $[R0], [R1], [R2]$), Sotto, si assume $s, z \in S$ e $a, b, x, y \in \mathbb{Z}$.

$$\begin{array}{c} \frac{}{\epsilon} [S0] \quad \frac{s}{a : s} (a \in \mathbb{Z}) [S1] \quad \frac{}{Q(\epsilon, 1)} [Q0] \quad \frac{Q(s, b)}{Q(a : s, ab)} [Q1] \\ \frac{}{R(\epsilon, \epsilon)} [R0] \quad \frac{R(s, z)}{R(a : s, (a^2 + 1) : z)} [R1] \quad \frac{R(s, z)}{R(a : s, z)} [R2] \end{array}$$

1. [20%] Si trovi una sequenza s di lunghezza 5 e una sequenza z di lunghezza 3, per cui valga $R(s, z)$. 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:

$$\forall a \in \mathbb{Z}, s, z \in S. Q(z, a) \wedge R(s, z) \implies a > 0$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall s, z \in S. R(s, z) \implies p(s, z)$$

per un qualche predicato p .

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

Soluzione (bozza).

Parte 1.

Una possibile derivazione è:

$$\frac{\frac{\frac{\frac{\frac{\frac{}{R(\epsilon, \epsilon)} [R0]}{R(5 : \epsilon, \epsilon)} [R2]}{R(4 : 5 : \epsilon, \epsilon)} [R2]}{R(3 : 4 : 5 : \epsilon, 10 : \epsilon)} [R1]}{R(2 : 3 : 4 : 5 : \epsilon, 5 : 10 : \epsilon)} [R1]}{R(1 : 2 : 3 : 4 : 5 : \epsilon, 2 : 5 : 10 : \epsilon)} [R1]$$

Parte 2.

Affinché valga $\forall s, z. R(s, z) \implies p(s, z)$ basta che:

$$\begin{array}{l} R0) p(\epsilon, \epsilon) \\ R1) \forall a, s, z. p(s, z) \implies p(a : s, z) \\ R2) \forall a, s, z. p(s, z) \implies p(a : s, (a^2 + 1) : z) \end{array}$$

Parte 3.

Basta prendere $p(s, z) : \forall a. Q(z, a) \implies a > 0$.

Parte 4.

Caso $[R0]$. Dobbiamo dimostrare $p(\epsilon, \epsilon)$, ovvero che $\forall a. Q(\epsilon, a) \implies a > 0$.

Assumiamo quindi $IP1 : Q(\epsilon, a)$ e dimostriamo la nuova tesi $a > 0$.

Invertendo $IP1$, osserviamo che può solo derivare da $[Q0]$, e quindi $a = 1$. Ne segue $a = 1 > 0$ che è la tesi.

Caso $[R1]$. Assumiamo l'ipotesi induttiva $IP1 : p(s, z)$ e dimostriamo la tesi $p(a : s, (a^2 + 1) : z)$.

$$\begin{aligned} IP1 : \forall \bar{a}. Q(z, \bar{a}) &\implies \bar{a} > 0 \\ tesi : \forall \hat{a}. Q((a^2 + 1) : z, \hat{a}) &\implies \hat{a} > 0 \end{aligned}$$

Assumiamo quindi $IP2 : Q((a^2 + 1) : z, \hat{a})$ e dimostriamo la nuova tesi $\hat{a} > 0$.

Invertendo $IP2$, osserviamo che può solo derivare da $[Q1]$, e quindi otteniamo $\hat{a} = (a^2 + 1)b$ per qualche b tale che $IP3 : Q(z, b)$.

Usando $IP1$, scegliendo $\bar{a} = b$, assieme a $IP3$, otteniamo $b > 0$.

Si ha $\hat{a} = (a^2 + 1)b > 0$ perché entrambi i fattori sono positivi, da cui la tesi.

Caso $[R2]$. Assumiamo l'ipotesi induttiva $IP1 : p(s, z)$ e dimostriamo la tesi $p(a : s, z)$.

$$\begin{aligned} IP1 : \forall \bar{a}. Q(z, \bar{a}) &\implies \bar{a} > 0 \\ tesi : \forall a. Q(z, a) &\implies a > 0 \end{aligned}$$

La tesi è uguale a $IP1$ (a meno di rinominare la variabile quantificata), quindi segue banalmente. □

Esercizio 3.

1. [40%] Si definisca un comando c di IMP (con gli operatori aritmetici $+$, $-$, $*$, $/$) tale che, per ogni A naturale, renda valida la seguente tripla di Hoare. (Nota: la costante A non può apparire nella definizione di c .)

$$\begin{aligned} &\{a = A > 0\} \\ &\quad c \\ &\{r^2 \leq A < (r + 1)^2\} \end{aligned}$$

2. [10%] Si giustifichi informalmente la validità delle tripla sovrastante.
3. [30%] Si stimi l'andamento asintotico (per es. $O(A^4)$) della complessità computazionale $T(A)$ di c . Si supponga che ogni operazione elementare costi un'unità di costo, a prescindere dalla grandezza dei numeri che vengono calcolati durante la valutazione delle espressioni. Si giustifichi informalmente la risposta.
4. [20%] Si descriva come si potrebbe costruire un comando c efficiente in termini di complessità, da potere realisticamente essere usato per gestire anche numeri molto grandi come $A \approx 10^{100}$.

Soluzione (bozza).

Parte 1.

Un possibile comando c è:

```

r := 0;
while (r + 1) * (r + 1) ≤ a do
  r := r + 1
```

Parte 2.

Il comando cerca il primo naturale r che soddisfa la proprietà $p(r) : (r + 1)^2 > A$. La proprietà non è sempre falsa (per es., $r = A$ la soddisfa), quindi il minimo r viene trovato. Abbiamo $r > 0$ da $A > 0$ e $p(r)$. Dalla minimalità, si ha $\neg(p(r - 1))$, e quindi $r^2 \leq A$. Otteniamo quindi la postcondizione $r^2 \leq A < (r + 1)^2$.

Parte 3.

La complessità è $O(\sqrt{a})$, visto che il while esegue tante iterazioni quante la radice di A .

Parte 4.

È possibile usare una ricerca binaria per trovare r più velocemente. Indichiamo con x l'estremo inferiore del nostro intervallo di ricerca (inizialmente 0), e con y l'estremo superiore (inizialmente A),

```
 $x := 0;$   
 $y := a;$   
while  $x < y$  do  
     $m := (x + y + 1)/2;$   
    if  $m * m \leq a$  then  
         $x := m$   
    else  
         $y := m - 1;$   
 $r := x$ 
```

A ogni giro, prendiamo la media di x e y (arrotondata per eccesso) e confrontiamo il suo quadrato con A , spostando uno dei due estremi conseguentemente. A ogni iterazione la lunghezza dell'intervallo si dimezza, quindi la complessità diventa $O(\log(A))$.

□

Nome _____ Matricola _____

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

$$\{n = N \geq 0 \wedge m = M \geq 0\}$$
$$x := 0;$$
$$y := 0;$$

```
while  $y < n$  do
```

if $x < m$ then

$$x := x + 1;$$
$$y := y + 1$$

else

$$y := y + 1$$
$$\{x = \min(N, M)\}$$

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

[illegible]

Soluzione (bozza).

```
{n = N ≥ 0 ∧ m = M ≥ 0} (1)
{0 = min(0, M) ∧ 0 ≤ n = N ∧ m = M}
x := 0;
{x = min(0, M) ∧ 0 ≤ n = N ∧ m = M}
y := 0;
{INV : x = min(y, M) ∧ y ≤ n = N ∧ m = M}
while y < n do
  {INV ∧ y < n}
  if x < m then
    {INV ∧ y < n ∧ x < m} (2)
    {x + 1 = min(y + 1, M) ∧ y + 1 ≤ n = N ∧ m = M}
    x := x + 1;
    {x = min(y + 1, M) ∧ y + 1 ≤ n = N ∧ m = M}
    y := y + 1
  else
    {INV ∧ y < n ∧ ¬(x < m)} (3)
    {x = min(y + 1, M) ∧ y + 1 ≤ n = N ∧ m = M}
    y := y + 1
{INV ∧ ¬(y < n)} (4)
{x = min(N, M)}
```

Per le PrePost:

- 1) Banale aritmetica.
- 2) Dalle ipotesi si ha $x < m = M$ e $x = \min(y, M)$, da cui ricaviamo $x = y < M$. Da questo si ha $x + 1 = \min(y + 1, M)$. Dall'ipotesi $y < n = N$ siccome sono interi ricaviamo $y + 1 \leq n = N$. La tesi $m = M$ è una delle ipotesi.
- 3) Dalle ipotesi si ha $x \geq m = M$ e $x = \min(y, M)$, da cui ricaviamo $x = M \leq y$. Da questo si ha $x = \min(y + 1, M)$. Dall'ipotesi $y < n = N$ siccome sono interi ricaviamo $y + 1 \leq n = N$. La tesi $m = M$ è una delle ipotesi.
- 4) Dalle ipotesi si ha $y \leq n = N$ e $\neg(y < n)$, quindi $y = N$. Da questo e dall'ipotesi $x = \min(y, M)$ si ha la tesi $x = \min(N, M)$.

□