

Informatica — 2026-06-24

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

Esercizio 1. Si dimostri il lemma del minimo punto fisso: se $f : \mathcal{P}(U) \rightarrow \mathcal{P}(U)$ è una funzione monotona e X è il suo minimo punto prefisso, allora X è anche il suo minimo punto fisso.

Esercizio 2. Le seguenti regole definiscono induttivamente l'insieme T degli alberi di interi (regole $[T0], [T1]$), una relazione $Q \in \mathcal{P}(T \times \mathbb{Z})$ (regole $[Q0], [Q1]$), e una relazione $R \in \mathcal{P}(T \times \mathbb{Z} \times T)$ (regole $[R0], [R1], [R2]$). Sotto, si assume $s, d, t \in T$ e $a, b, x, y \in \mathbb{Z}$.

$$\frac{}{a} (a \in \mathbb{Z}) [T0] \quad \frac{s \quad d}{(s, d)} [T1] \quad \frac{}{Q(a, a)} [Q0] \quad \frac{Q(s, a_s) \quad Q(d, a_d)}{Q((s, d), a_s a_d)} [Q1]$$

$$\frac{}{R(b, a, ab)} [R0] \quad \frac{R(s, a, s')}{R((s, d), a, (s', d))} [R1] \quad \frac{R(d, a, d')}{R((s, d), a, (s, d'))} [R2]$$

1. [20%] Si trovi un albero t con almeno 3 interi al suo interno per cui valga $R(t, 5, t')$ per qualche 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:

$$\forall x, y \in \mathbb{Z}, t_1, t_2 \in T. Q(t_1, x) \wedge R(t_1, y, t_2) \implies Q(t_2, xy)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall y \in \mathbb{Z}, t_1, t_2 \in T. R(t_1, y, t_2) \implies p(t_1, y, t_2)$$

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 soluzione:

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

Parte 2.

Affinché valga $\forall t_1, y, t_2. R(t_1, y, t_2) \implies p(t_1, y, t_2)$ è sufficiente che valgano:

$$\begin{aligned} R0) \quad & \forall ab \in \mathbb{Z}. p(b, a, ab) \\ R1) \quad & \forall s, d, a, s'. p(s, a, s') \implies p((s, d), a, (s', d)) \\ R2) \quad & \forall s, d, a, d'. p(d, a, d') \implies p((s, d), a, (s, d')) \end{aligned}$$

Parte 3.

Basta prendere

$$p(t_1, y, t_2) : \forall x \in \mathbb{Z}, Q(t_1, x) \implies Q(t_2, xy)$$

Parte 4.

Caso $[R0]$.

Dobbiamo dimostrare $p(b, a, ab)$ cioè $\forall x \in \mathbb{Z}, Q(b, x) \implies Q(ab, xa)$. Assumiamo $IP1 : Q(b, x)$ e dimostriamo la nuova tesi $Q(ab, xa)$.

Invertendo $IP1$ osserviamo che si può ricavare solo da $[Q0]$ e quindi $x = b$. Da qui, la tesi si riscrive come $Q(ab, ba)$, che segue immediatamente da $[Q0]$.

Caso [R1]. Assumiamo l'ipotesi induttiva $IP1 : p(s, a, s')$ e dimostriamo $p((s, d), a, (s', d))$.

$$\begin{aligned} IP1 : \quad & \forall \bar{x} \in \mathbb{Z}, Q(s, \bar{x}) \implies Q(s', \bar{x}a) \\ \text{tesi} : \quad & \forall x \in \mathbb{Z}, Q((s, d), x) \implies Q((s', d), xa) \end{aligned}$$

Assumiamo quindi $IP2 : Q((s, d), x)$ e dimostriamo la nuova tesi $Q((s', d), xa)$.

Invertendo $IP2$ osserviamo che si può ricavare solo da $[Q1]$ e quindi $x = bc$ per qualche $b, c \in Z$ tali che $IP3 : Q(s, b)$ e $IP4 : Q(d, c)$.

Usando $IP1$, scegliendo $\bar{x} = b$, assieme a $IP3$ si ricava $IP5 : Q(s', ba)$.

Applicando $[Q1]$ a $IP5$ e $IP4$ si ricava $Q((s', d), bac)$ che è la tesi visto che $bac = xa$.

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

$$\begin{aligned} IP1 : \quad & \forall \bar{x} \in \mathbb{Z}, Q(d, \bar{x}) \implies Q(d', \bar{x}a) \\ \text{tesi} : \quad & \forall x \in \mathbb{Z}, Q((s, d), x) \implies Q((s, d'), xa) \end{aligned}$$

Assumiamo quindi $IP2 : Q((s, d), x)$ e dimostriamo la nuova tesi $Q((s, d'), xa)$.

Invertendo $IP2$ osserviamo che si può ricavare solo da $[Q1]$ e quindi $x = bc$ per qualche $b, c \in Z$ tali che $IP3 : Q(s, b)$ e $IP4 : Q(d, c)$.

Usando $IP1$, scegliendo $\bar{x} = c$, assieme a $IP4$ si ricava $IP5 : Q(d', ca)$.

Applicando $[Q1]$ a $IP3$ e $IP5$ si ricava $Q((s, d'), bca)$ che è la tesi visto che $bca = xa$. $\square$

Esercizio 3. Si consideri una variante di IMP dove le espressioni sono limitate agli operatori $+$, $-$, $*$, $\leq$, $<$, $=$, $\wedge$, $\neg$.

1. [40%] Si definisca un comando c in questa variante di IMP tale che, per ogni A, B naturali, renda valida la seguente tripla di Hoare. (Nota: le costanti A e B non possono apparire nella definizione di c .)

$$\begin{array}{c} \{a = A \geq 0 \wedge b = B > 0\} \\ c \\ \{A = B * q + r \wedge 0 \leq r < B\} \end{array}$$

2. [10%] Si giustifichi informalmente la validità delle tripla sovrastante.
3. [30%] Si stimi l'andamento asintotico (per es. $O(A^2B)$) della complessità computazionale $T(A, B)$ di c . Si supponga che ogni assegnamento $x := e$ costi 1 unità di costo, a prescindere dalla grandezza dei numeri che vengono calcolati durante la valutazione di e . Si giustifichi informalmente la risposta.
4. [20%] Si trovi 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.

Una possibile soluzione per c è

```
q := 0;
while b ≤ a do
  a := a - b;
  q := q + 1;
r := a
```

Parte 2.

La tripla data chiede di calcolare quoziente e resto della divisione A/B . Il comando c sopra lo fa sottraendo b ad a ripetutamente, fino a quando a non diventa più piccolo di b . Il numero di sottrazioni fatte è quindi il quoziente q mentre il valore rimanente alla fine in a è il resto.

Parte 3.

La complessità asintotica è $T(A, B) = O(A/B)$, visto che il ciclo esegue tante volte quanto è il quoziente.

Parte 4 (bonus).

Un comando c più efficiente si può ottenere sottraendo ripetutamente ad a il numero $2^k b$ con k intero più grande possibile. Questo è simile a quanto avviene quando facciamo su carta una “divisione in colonna”, partendo dalle cifre più significative.

```

q := 0;
while b ≤ a do
  x := 1;
  y := b;
  while 2 * y ≤ a do
    y := 2 * y;
    x := 2 * x;
  a := a - y;
  q := q + x;
r := a

```

Per stimare la complessità, notiamo che il ciclo interno richiede $O(\log_2 a)$ passi. Dopo che il ciclo interno finisce, a viene diminuito di almeno la sua metà (togliamo da esso la potenza di due più grande per b che sia ancora $\leq a$). Quindi la complessità di tutto il comando è

$$O(\log_2 A + \log_2(A/2) + \log_2(A/4) + \dots)$$

che possiamo maggiorare con

$$O(\log_2^2 A)$$

Si noti infine che invece di usare la base 2 avremmo potuto usare qualunque altra base maggiore di 1 e l'andamento asintotico sarebbe stato lo stesso, visto che $\log_t N = O(\log_u N)$ per ogni $t, u > 1$ quando $N \rightarrow \infty$.

□

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
```

$$x := x + 5 - 7 * y;$$
$$y := y + 1$$
$$\{2x = -7N^2 + 17N\}$$

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

[illegible]

Soluzione (bozza).

$\{n = N \geq 0\}$ (1)
 $\{2 \cdot 0 = -7 \cdot 0^2 + 17 \cdot 0 \wedge 0 \leq n = N\}$
 $x := 0;$
 $\{2x = -7 \cdot 0^2 + 17 \cdot 0 \wedge 0 \leq n = N\}$
 $y := 0;$
 $\{INV : 2x = -7y^2 + 17y \wedge y \leq n = N\}$
while $y < n$ do
 $\{INV \wedge y < n\}$ (2)
 $\{2(x + 5 - 7y) = -7(y + 1)^2 + 17(y + 1) \wedge y + 1 \leq n = N\}$
 $x := x + 5 - 7 * y;$
 $\{2x = -7(y + 1)^2 + 17(y + 1) \wedge y + 1 \leq n = N\}$
 $y := y + 1$
 $\{INV \wedge \neg(y < n)\}$ (3)
 $\{2x = -7N^2 + 17N\}$

Per le PrePost:

1) Banale aritmetica.

2) Siccome $y < n = N$ per ipotesi, e sono numeri interi, segue che $y + 1 \leq n = N$. Per dimostrare $2(x + 5 - 7y) = -7(y + 1)^2 + 17(y + 1)$, possiamo semplificarla in $2x + 10 - 14y = -7y^2 - 14y - 7 + 17y + 17$ e quindi in $2x = -7y^2 + 17y$ che è l'ipotesi.

3) Dalle ipotesi $y \leq n = N$ e $\neg(y < n)$ si ricava $y = n = N$. Da INV si ricava quindi $2x = -7N^2 + 17N$ che è la tesi.

□