

Informatica — 2026-09-04

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

Esercizio 1. Si forniscano le sei regole di inferenza che definiscono il sistema deduttivo (la relazione $\vdash \{P\} c \{Q\}$) delle triple di Hoare.

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

$$\frac{}{a} (a \in \mathbb{Z}) [T0] \quad \frac{s \quad d}{(s, d)} [T1] \quad \frac{}{R(a, b, a+b)} [R0] \quad \frac{R(s_1, s_2, x) \quad R(d_1, d_2, y)}{R((s_1, d_1), (s_2, d_2), x+y)} [R1]$$

1. [20%] Si trovino due alberi t_1, t_2 tali per cui t_1 contenga almeno tre interi al suo interno e valga $R(t_1, t_2, 10)$. Si giustifichi la risposta esibendo una derivazione.
2. [20%] Si enunci il principio di induzione associato all'insieme T .
3. [10%] Si consideri l'enunciato seguente:

$$\forall c \in \mathbb{Z}, t \in T. R(t, t, c) \implies c \text{ pari}$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t \in T. p(t)$$

per un qualche predicato p .

4. [50%] Si dimostri l'enunciato sopra usando il principio di induzione associato a T .

Soluzione (bozza).

Parte 1.

Una possibile derivazione è:

$$\frac{\frac{}{R(1, 0, 1)} [R0] \quad \frac{\frac{}{R(2, 3, 5)} [R0] \quad \frac{}{R(3, 1, 4)} [R0]}{R((2, 3), (3, 1), 9)} [R1]}{R((1, (2, 3)), (0, (3, 1)), 10)} [R1]$$

Parte 2.

Affinché valga $p(t)$ per ogni $t \in T$, basta che:

$$\begin{aligned} T0) & \forall a \in \mathbb{Z}. p(a) \\ T1) & \forall s, d. p(s) \wedge p(d) \implies p((s, d)) \end{aligned}$$

Parte 3. Basta prendere

$$p(t) : \forall c \in \mathbb{Z}. R(t, t, c) \implies c \text{ pari}$$

Parte 4.

Caso $[T0]$. Dobbiamo dimostrare $p(a)$ per ogni a intero. Assumiamo dunque $IP1$: $R(a, a, c)$ e dimostriamo c pari. Invertendo $IP1$, notiamo che può essere derivata solo da $R0$, e quindi $c = a + a$. Questo implica che c è un intero pari.

Caso $[T1]$. Assumendo le ipotesi induttive $IP1$: $p(s)$ e $IP2$: $p(d)$ dobbiamo dimostrare la tesi $p((s, d))$. In altre parole:

$$\begin{aligned} IP1 : & \forall c' \in \mathbb{Z}. R(s, s, c') \implies c' \text{ pari} \\ IP2 : & \forall c'' \in \mathbb{Z}. R(s, s, c'') \implies c'' \text{ pari} \\ \text{tesi} : & \forall c \in \mathbb{Z}. R((s, d), (s, d), c) \implies c \text{ pari} \end{aligned}$$

Assumiamo quindi $IP3 : R((s, d), (s, d), c)$ e dimostriamo c pari.

Invertendo $IP3$, notiamo che può essere derivata solo da $R1$, e quindi $IP4 : R(s, s, c_1)$ e $IP4 : R(d, d, c_2)$ per qualche c_1, c_2 tali che $c = c_1 + c_2$.

Usando $IP1$, scegliendo $c' = c_1$, assieme a $IP3$, otteniamo che c_1 è pari.

Analogamente, usando $IP2$, scegliendo $c'' = c_2$, assieme a $IP4$, otteniamo che c_2 è pari.

Concludiamo che $c = c_1 + c_2$ è somma di pari e quindi è pari, che è la tesi. $\square$

Esercizio 3. Si consideri un'estensione IMP^+ del linguaggio IMP ottenuta aggiungendo ad esso il nuovo comando ciclo **repeat** c **revert** $e \neq 0$. La semantica intuitiva di tale comando è quella di eseguire c e dopo controllare la guardia $e \neq 0$. Se è vera, viene ripetuto tutto il ciclo da capo. Se è falsa, il ciclo termina e viene annullato l'effetto dell'ultima esecuzione del comando c . Per esempio, il comando

$x := 5; y := 1; \text{repeat } y := y * 2; x := x - 1 \text{ revert } x \neq 0$

termina in uno stato dove x vale 1 (non 0) e y vale 2^4 (non 2^5).

1. [50%] Si formalizzi la semantica di IMP^+ fornendo le regole di inferenza che vanno aggiunte a quelle standard.
2. [50%] Si supponga che il nuovo comando ciclo venga esteso a guardie booleane arbitrarie, **repeat** c **revert** ϕ . Si sviluppi un comando c di IMP^+ privo di cicli **while** e tale che, dato un $y \geq 10$ arbitrario, calcoli il più grande intero x della forma $k^2 + 1$ tale che $x^2 + 4x - 2 \leq y$. Si giustifichi brevemente la risposta in modo informale.

Soluzione (bozza).

Parte 1.

$$\frac{\langle c, \sigma \rangle \rightarrow_b \sigma' \quad \langle e, \sigma' \rangle \rightarrow_e v \neq 0 \quad \langle \text{repeat } c \text{ revert } e \neq 0, \sigma' \rangle \rightarrow_b \sigma''}{\langle \text{repeat } c \text{ revert } e \neq 0, \sigma \rangle \rightarrow_b \sigma''} [\text{Revert} - \text{True}]$$

$$\frac{\langle c, \sigma \rangle \rightarrow_b \sigma' \quad \langle e, \sigma' \rangle \rightarrow_e 0}{\langle \text{repeat } c \text{ revert } e \neq 0, \sigma \rangle \rightarrow_b \sigma} [\text{Revert} - \text{False}]$$

Parte 2.

```

k := 0;
repeat
  x := k * k + 1;
  k := k + 1
revert x * x + 4 * x - 2 ≤ y

```

Il ciclo sopra prova tutti gli interi x della forma $k^2 + 1$. La condizione è verificata per $k = 0$ visto che $y \geq 10$ e $x^2 + 4x - 2 = 1 + 4 - 2 = 3 \leq 10 \leq y$. Il ciclo si ferma quando il valore di x è diventato troppo grande per soddisfare la condizione. Il ciclo **repeat** ritorna quindi al valore precedente di x , che è quindi il più grande intero che soddisfa la condizione. $\square$

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
```

$$y := y + 1;$$
$$x := x - 3 + 7 * y$$
$$\{2x = 7N^2 + N\}$$

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

[illegible]

Soluzione (bozza).

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

Per le PrePost:

- 1) Banale aritmetica.
- 2) La tesi $y + 1 \leq n$, siccome stiamo usando numeri interi, è equivalente a $y < n$ che è un'ipotesi. Anche $n = N$ è un'ipotesi. L'altra equazione nella tesi è $2(x - 3 + 7(y + 1)) = 7(y + 1)^2 + y + 1$ e si semplifica in $2x - 6 + 14y + 14 = 7y^2 + 14y + 7 + y + 1$ e quindi in $2x = 7y^2 + y$ che è un'ipotesi.
- 3) Da INV si ha $y \leq n = N$ ma per ipotesi $\neg(y < n)$, quindi $y = N$. La tesi segue quindi da $2x = 7y^2 + y$.

□