

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

Esercizio 1. *Si enunci e dimostri il lemma del minimo punto fisso.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi di interi (regole $[T0], [T1]$) e una relazione $R \in \mathcal{P}(T \times T)$ (regole $[R0], [R1], [R2]$). Sotto, a, b indicano interi, mentre s, s', d, d', t indicano alberi in T .*

$$\frac{}{a \in \mathbb{Z}}[T0] \quad \frac{s \quad d}{(s, d)}[T1] \quad \frac{}{R(a, a+2)}[R0] \quad \frac{}{R(a, a-2)}[R1] \quad \frac{R(s, s') \quad R(d, d')}{R((s, d), (s', d'))}[R2]$$

1. [20%] *Si forniscano due alberi t_1, t_2 per cui t_1 contenga tre interi e inoltre valga $R(t_1, t_2)$. Si giustifichi la risposta esibendo una derivazione.*
2. [20%] *Si enunci il principio di induzione associato alla relazione R .*
3. [5%] *Si consideri l'enunciato seguente:*

$$\forall t_1, t_2 \in T. R(t_1, t_2) \implies R(t_2, t_1)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t_1, t_2 \in T. R(t_1, t_2) \implies p(t_1, t_2)$$

per un qualche predicato p .

4. [55%] *Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a R .*

Soluzione (bozza).

Parte 1

Un possibile esempio è:

$$\frac{\frac{}{R(10, 12)} \quad \frac{\frac{}{R(20, 22)} \quad \frac{}{R(30, 28)}}{R((20, 30), (22, 28))}}{R((10, (20, 30)), (12, (22, 28)))}$$

Parte 2

Per dimostrare che per ogni $t_1, t_2 \in T$ tali che $R(t_1, t_2)$ vale $p(t_1, t_2)$ basta che:

$$\begin{aligned} R0) \quad & \forall a \in \mathbb{Z}. p(a, a+2) \\ R1) \quad & \forall a \in \mathbb{Z}. p(a, a-2) \\ R2) \quad & \forall s, s', d, d'. p(s, s') \wedge p(d, d') \implies p((s, d), (s', d')) \end{aligned}$$

Parte 3

Basta prendere $p(t_1, t_2) : R(t_2, t_1)$.

Parte 4

Caso $R0$

Bisogna dimostrare $p(a, a+2)$ e cioè $R(a+2, a)$. Dalla regola $[R1]$ abbiamo $R(b, b-2)$ per ogni intero b , e quindi prendendo $b = a+2$ abbiamo $R(a+2, a+2-2)$ che è la tesi $R(a+2, a)$.

Caso $R1$

Bisogna dimostrare $p(a, a-2)$ e cioè $R(a-2, a)$. Dalla regola $[R0]$ abbiamo $R(b, b+2)$

per ogni intero b , e quindi prendendo $b = a - 2$ abbiamo $R(a - 2, a - 2 + 2)$ che è la tesi $R(a - 2, a)$.

Caso R2

Assumiamo le ipotesi induttive $IP1 : p(s, s')$ e $IP2 : p(d, d')$, e dimostriamo la tesi $p((s, d), (s', d'))$.

Riscrivendo tutto, assumiamo $IP1 : R(s', s)$ e $IP2 : R(d', d)$, e dimostriamo la tesi $R((s', d'), (s, d))$.

In [R2] scegliamo come segue le variabili:

$$\frac{R(s', s) \quad R(d', d)}{R((s', d'), (s, d))} [R2]$$

Le premesse sono vere per $IP1, IP2$, quindi possiamo applicare la regola e ottenere la conclusione $R((s', d'), (s, d))$, che è la tesi. □

Esercizio 3. Siano $x \in Var, \sigma \in State$ una variabile e uno stato di IMP. Sia inoltre $\mathcal{C}$ l'insieme dei comandi dato da

$$\mathcal{C} = \{c \in Com \mid \forall z \in \mathbb{Z}. \langle c, \sigma[x \mapsto z] \rangle \rightarrow_b \sigma[x \mapsto z]\}$$

Si considerino le affermazioni seguenti. Si fornisca una dimostrazione informale per le affermazioni vere, e si fornisca invece un controesempio per quelle false. Si giustifichi la risposta.

1. [40%] $\forall c_1, c_2 \in \mathcal{C}. (x := x + 1; c_1; x := x - 2; c_2; x := x + 1) \in \mathcal{C}$
2. [30%] $\forall c_1, c_2 \in \mathcal{C}, e \in Exp. (\text{if } e \neq 0 \text{ then } c_1 \text{ else } c_2) \in \mathcal{C}$
3. [30%] $\forall c \in \mathcal{C}, e \in Exp. (\text{while } e \neq 0 \text{ do } c) \in \mathcal{C}$

Soluzione (bozza).

Parte 1. La proprietà è vera.

Sia $z \in \mathbb{Z}$. Partendo dallo stato iniziale $\sigma[x \mapsto z]$, eseguiamo il comando $x := x + 1; c_1; x := x - 2; c_2; x := x + 1$. Dopo $x := x + 1$, lo stato diventa $\sigma[x \mapsto z + 1]$. Visto che $c_1 \in \mathcal{C}$, possiamo prendere lo z nella definizione di $\mathcal{C}$ uguale al nostro $z + 1$ e ottenere $\langle c_1, \sigma[x \mapsto z + 1] \rangle \rightarrow_b \sigma[x \mapsto z + 1]$. Quindi, dopo c_1 lo stato diventa $\sigma[x \mapsto z + 1]$. Proseguendo, dopo $x := x - 2$ lo stato diventa $\sigma[x \mapsto z - 1]$. Visto che $c_2 \in \mathcal{C}$, possiamo prendere lo z nella definizione di $\mathcal{C}$ uguale al nostro $z - 1$ e ottenere $\langle c_2, \sigma[x \mapsto z - 1] \rangle \rightarrow_b \sigma[x \mapsto z - 1]$. Quindi, dopo c_2 lo stato diventa $\sigma[x \mapsto z - 1]$. Proseguendo, dopo $x := x + 1$ lo stato diventa $\sigma[x \mapsto z]$ che è quello che ci serve per concludere la dimostrazione.

Parte 2. La proprietà è vera.

Sia $z \in \mathbb{Z}$. Partendo dallo stato iniziale $\sigma[x \mapsto z]$, la guardia dell'if potrebbe essere vera o falsa. Esaminiamo i due casi.

Se la guardia è vera, l'if esegue c_1 e visto che $c_1 \in \mathcal{C}$, possiamo prendere lo z nella definizione di $\mathcal{C}$ proprio uguale al nostro z e ottenere $\langle c_1, \sigma[x \mapsto z] \rangle \rightarrow_b \sigma[x \mapsto z]$. Quindi, dopo c_1 (e l'if) lo stato diventa $\sigma[x \mapsto z]$ che è proprio quello che ci serve per concludere il ramo della dimostrazione.

Se la guardia è invece falsa, l'if esegue c_2 e visto che $c_2 \in \mathcal{C}$, possiamo prendere lo z nella definizione di $\mathcal{C}$ proprio uguale al nostro z e ottenere $\langle c_2, \sigma[x \mapsto z] \rangle \rightarrow_b \sigma[x \mapsto z]$. Quindi, dopo c_2 (e l'if) lo stato diventa $\sigma[x \mapsto z]$ che è proprio quello che ci serve per concludere l'ultimo ramo della dimostrazione.

Parte 3. La proprietà è falsa.

Possiamo prendere $c = \text{skip}$ e ottenere banalmente $c \in \mathcal{C}$. Scegliamo inoltre $e = 1$. In questo caso, la proprietà diventa

$$(\text{while } 1 \neq 0 \text{ do skip}) \in \mathcal{C}$$

e cioè

$$\forall z \in \mathbb{Z}. \langle \text{while } 1 \neq 0 \text{ do skip}, \sigma[x \mapsto z] \rangle \rightarrow_b \sigma[x \mapsto z]$$

Questa è falsa per $z = 0$ (e per tutti gli altri, ma non importa) in quanto questo ciclo **while** non termina mai in nessun stato e quindi a maggior ragione non termina in $\sigma[x \mapsto z]$. $\square$

Nome _____ Matricola _____

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

$\{x = X \wedge y = Y\}$

while $x \neq y$ do

if $x > y$ then

$x := x - 1$

else

$y := y - 1$

$\{x = y = \min(X, Y)\}$

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

Soluzione (bozza).

```
{ $x = X \wedge y = Y$ } (1)
{ $INV : \min(x, y) = \min(X, Y)$ }
while  $x \neq y$  do
  { $INV \wedge x \neq y$ }
  if  $x > y$  then
    { $INV \wedge x \neq y \wedge x > y$ } (2)
    { $\min(x - 1, y) = \min(X, Y)$ }
     $x := x - 1$ 
  else
    { $INV \wedge x \neq y \wedge \neg(x > y)$ } (3)
    { $\min(x, y - 1) = \min(X, Y)$ }
     $y := y - 1$ 
  { $INV \wedge \neg(x \neq y)$ } (4)
{ $x = y = \min(X, Y)$ }
```

Per le PrePost:

- 1) Banale sostituzione.
- 2) Visto che $x > y$ per ipotesi, siccome sono interi deve valere anche $x - 1 \geq y$ da cui $\min(x - 1, y) = \min(x, y)$ che è uguale a $\min(X, Y)$ per INV .
- 3) Per ipotesi $\neg(x > y)$ e $x \neq y$, da cui $x < y$. Siccome sono interi deve valere anche $x \leq y - 1$ da cui $\min(x, y - 1) = \min(x, y)$ che è uguale a $\min(X, Y)$ per INV .
- 4) Per ipotesi $x = y$, da cui $x = y = \min(x, y)$ che con INV dà la tesi $x = y = \min(X, Y)$.

□