

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

Esercizio 1. Si enuncino i risultati relativi alla totalità della semantica delle espressioni e dei comandi di IMP, commentandoli brevemente.

Esercizio 2. Le seguenti regole definiscono induttivamente l'insieme S delle sequenze di interi (regole $[S0], [S1]$) e una relazione $R \in \mathcal{P}(S \times S)$ (regole $[R0], [R1], [R2]$). Sotto, a, b indicano interi mentre s, s', s_1, s_2 indicano sequenze in S .

$$\frac{}{R(\epsilon, \epsilon)}[R0] \quad \frac{}{\epsilon}[S0] \quad \frac{s}{a : s}(a \in \mathbb{Z})[S1] \quad \frac{R(s, s')}{R(a : b : s, a : -b : s')}[R2]$$

1. [20%] Si fornisca una sequenza s per cui valga $R(10 : 2 : 7 : \epsilon, s)$ e si giustifichi la risposta esibendo una derivazione.
2. [30%] Si enunci il principio di induzione associato alla relazione R .
3. [1%] Si consideri l'enunciato seguente:

$$\forall s_1, s_2 \in S. R(s_1, s_2) \implies R(s_2, s_1)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall s_1, s_2 \in S. R(s_1, s_2) \implies p(s_1, s_2)$$

per un qualche predicato p .

4. [49%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a R .

Soluzione (bozza).

Parte 1

Una possibile soluzione:

$$\frac{\frac{}{R(7 : \epsilon, 7 : \epsilon)}[R1]}{R(10 : 2 : 7 : \epsilon, 10 : -2 : 7 : \epsilon)}[R2]$$

Parte 2

Sia $p(s_1, s_2)$ un predicato su due sequenze.

Per dimostrare che $\forall s_1, s_2. R(s_1, s_2) \implies p(s_1, s_2)$ basta verificare che:

$$\begin{aligned} R0) & p(\epsilon, \epsilon) \\ R1) & \forall a \in \mathbb{Z}. p(a : \epsilon, a : \epsilon) \\ R2) & \forall a, b \in \mathbb{Z}, s, s' \in S. p(s, s') \implies p(a : b : s, a : -b : s') \end{aligned}$$

Parte 3

Basta (ovviamente) definire $p(s_1, s_2)$ come $R(s_2, s_1)$.

Parte 4

Procediamo per induzione su R :

Caso $[R0]$

Dobbiamo dimostrare $p(\epsilon, \epsilon)$ e cioè $R(\epsilon, \epsilon)$ che vale per la regola $[R0]$.

Caso $[R1]$

Dobbiamo dimostrare $p(a : \epsilon, a : \epsilon)$ e cioè $R(a : \epsilon, a : \epsilon)$ che vale per la regola $[R1]$.

Caso $[R2]$

Dobbiamo dimostrare $\forall \bar{a}, \bar{b} \in \mathbb{Z}, \bar{s}, \bar{s}' \in S. p(s, s') \implies p(\bar{a} : \bar{b} : \bar{s}, \bar{a} : -\bar{b} : \bar{s}')$.

Assumiamo come ipotesi induttiva $p(\bar{s}, \bar{s}')$ e cioè $IP1 : R(\bar{s}', \bar{s})$. Dobbiamo ora dimostrare la tesi $p(\bar{a} : \bar{b} : \bar{s}, \bar{a} : -\bar{b} : \bar{s}')$ e cioè $R(\bar{a} : -\bar{b} : \bar{s}', \bar{a} : \bar{b} : \bar{s})$.

Nella regola $[R2]$ scegliamo $a = \bar{a}, b = -\bar{b}, s = \bar{s}', s' = \bar{s}$. La regola diventa

$$\frac{R(\bar{s}', \bar{s})}{R(\bar{a} : -\bar{b} : \bar{s}', \bar{a} : -(-\bar{b}) : \bar{s})}$$

Siccome la premessa vale per $IP1$, otteniamo la conseguenza che si semplifica come

$$R(\bar{a} : -\bar{b} : \bar{s}', \bar{a} : \bar{b} : \bar{s})$$

che è la tesi. □

Esercizio 3. Dato un nome di variabile $x \in Var$, si consideri la relazione di equivalenza tra stati $\sigma \sim_x \sigma'$ data da

$$\forall y \in Var \setminus \{x\}. \sigma(y) = \sigma'(y)$$

Inoltre, si definisca la relazione tra comandi $c_1 \equiv_x c_2$ nel modo seguente

$$\begin{aligned} & (\forall \sigma, \sigma'. \langle c_1, \sigma \rangle \rightarrow_b \sigma' \implies \exists \sigma''. \langle c_2, \sigma \rangle \rightarrow_b \sigma'' \wedge \sigma' \sim_x \sigma'') \\ \wedge & (\forall \sigma, \sigma'. \langle c_2, \sigma \rangle \rightarrow_b \sigma' \implies \exists \sigma''. \langle c_1, \sigma \rangle \rightarrow_b \sigma'' \wedge \sigma' \sim_x \sigma'') \end{aligned}$$

1. [50%] Si dimostri, almeno in modo informale, che $\equiv_x$ è una relazione di equivalenza, cioè che valgono le seguenti per ogni c, c', c'' :

- 1) $c \equiv_x c$
- 2) $c \equiv_x c' \implies c' \equiv_x c$
- 3) $c \equiv_x c' \wedge c' \equiv_x c'' \implies c \equiv_x c''$

2. [50%] Si dimostri, almeno in modo informale, che $\equiv_x$ non è una congruenza rispetto alla composizione, cioè che non vale:

$$\forall c_1, c_2, c'_1, c'_2. \quad c_1 \equiv_x c'_1 \wedge c_2 \equiv_x c'_2 \implies c_1; c_2 \equiv_x c'_1; c'_2$$

Soluzione (bozza). Parte 1

Per la riflessività (1) basta scegliere $\sigma'' = \sigma'$ in entrambe le parti. La tesi diventa quindi $\langle c, \sigma \rangle \rightarrow_b \sigma'$ che è uguale all'ipotesi.

Per la simmetria (2) basta notare che la definizione di $c \equiv_x c'$ è della forma $p \wedge q$ mentre la definizione di $c' \equiv_x c$ è $q \wedge p$ (con gli stessi p, q di prima), quindi sono equivalenti.

(Nota: la dimostrazione qui sotto è stata scritta in modo dettagliato per completezza, ma per l'esame era sufficiente una dimostrazione più sintetica che spiegasse solo l'idea generale, dando un'intuizione su come usare gli stati che si ricavano sfruttando gli $\exists \sigma'$.)

Per la transitività (3), assumiamo (tra le altre cose) che

$$\begin{aligned} IP1 : & \forall \sigma_1, \sigma'_1. \langle c, \sigma_1 \rangle \rightarrow_b \sigma'_1 \implies \exists \sigma''_1. \langle c', \sigma_1 \rangle \rightarrow_b \sigma''_1 \wedge \sigma'_1 \sim_x \sigma''_1 \\ IP2 : & \forall \sigma_2, \sigma'_2. \langle c', \sigma_2 \rangle \rightarrow_b \sigma'_2 \implies \exists \sigma''_2. \langle c'', \sigma_2 \rangle \rightarrow_b \sigma''_2 \wedge \sigma'_2 \sim_x \sigma''_2 \end{aligned}$$

e dimostriamo la prima “metà” della tesi, cioè che

$$\forall \sigma, \sigma'. \langle c, \sigma \rangle \rightarrow_b \sigma' \implies \exists \sigma''. \langle c'', \sigma \rangle \rightarrow_b \sigma'' \wedge \sigma' \sim_x \sigma''$$

Assumiamo quindi

$$IP3 : \langle c, \sigma \rangle \rightarrow_b \sigma'$$

Da $IP3$ e $IP1$, scegliendo $\sigma_1 = \sigma, \sigma'_1 = \sigma'$, ricaviamo $\langle c', \sigma \rangle \rightarrow_b \sigma''_1$ per qualche σ''_1 tale che $\sigma' \sim_x \sigma''_1$.

Di qui e $IP2$, scegliendo $\sigma_2 = \sigma, \sigma'_2 = \sigma''_1$, ricaviamo $\langle c'', \sigma \rangle \rightarrow_b \sigma''_2$ per qualche σ''_2 tale che $\sigma''_1 \sim_x \sigma''_2$.

Da $\sigma' \sim_x \sigma''_1$ e $\sigma''_1 \sim_x \sigma''_2$ ricaviamo $\sigma' \sim_x \sigma''_2$.

Per dimostrare la tesi

$$\exists \sigma''. \langle c'', \sigma \rangle \rightarrow_b \sigma'' \wedge \sigma' \sim_x \sigma''$$

basta quindi scegliere $\sigma'' = \sigma''_2$ e usare le ipotesi ottenute sopra.

Qui sopra abbiamo dimostrato “metà” della transitività. L'altra parte è analoga, e richiede di assumere che

$$\begin{aligned} IP1 : \forall \sigma_1, \sigma'_1. \langle c'', \sigma_1 \rangle \rightarrow_b \sigma'_1 &\implies \exists \sigma''_1. \langle c', \sigma_1 \rangle \rightarrow_b \sigma''_1 \wedge \sigma'_1 \sim_x \sigma''_1 \\ IP2 : \forall \sigma_2, \sigma'_2. \langle c'', \sigma_2 \rangle \rightarrow_b \sigma'_2 &\implies \exists \sigma''_2. \langle c, \sigma_2 \rangle \rightarrow_b \sigma''_2 \wedge \sigma'_2 \sim_x \sigma''_2 \end{aligned}$$

e di dimostrare che

$$\forall \sigma, \sigma'. \langle c'', \sigma \rangle \rightarrow_b \sigma' \implies \exists \sigma''. \langle c, \sigma \rangle \rightarrow_b \sigma'' \wedge \sigma' \sim_x \sigma''$$

Parte 2

Come controesempio, scegliamo:

$$c_1 = \text{skip} \quad c'_1 = x := 1 \quad c_2 = c'_2 = (\text{if } x \neq 0 \text{ then } y := 1 \text{ else } y := 2)$$

dove y è un nome di variabile diverso da x . L'ipotesi $c_1 \equiv_x c'_1$ diventa $\text{skip} \equiv_x (x := 1)$ e vale, visto che partendo da σ , eseguire skip porta a σ , mentre $x := 1$ porta a $\sigma[x \mapsto 1]$, e $\sigma \sim_x \sigma[x \mapsto 1]$ visto che la variabile x non viene considerata.

L'ipotesi $c_2 \equiv_x c'_2$ vale per riflessività.

Tuttavia la tesi $c_1; c_2 \equiv_x c'_1; c'_2$ non vale. Se partiamo da uno stato σ dove tutte le variabili valgono zero, eseguire $c_1; c_2$ ci porta in $\sigma[y \mapsto 2]$, mentre eseguire $c'_1; c'_2$ ci porta in $\sigma[x \mapsto 1][y \mapsto 1]$, e questi due stati differiscono per il valore di $y \neq x$ per cui non soddisfano $\sim_x$.

Una breve soluzione alternativa era $c_2 = c'_2 = (y := x)$. □

Nome _____ Matricola _____

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

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

$x := -5;$

$r := 42;$

while $x \neq n$ do

if $x = -1$ then

$r := 1$

else

$r := r * 2;$

$x := x + 1;$

$\{r = 2^N\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

```

{ $n = N \geq 0$ } (1)
{ $n = N \geq 0 \wedge (-5 \geq 0 \implies 42 = 2^{-5})$ }
 $x := -5$ ;
{ $n = N \geq 0 \wedge (x \geq 0 \implies 42 = 2^x)$ }
 $r := 42$ ;
{ $INV : n = N \geq 0 \wedge (x \geq 0 \implies r = 2^x)$ }
while  $x \neq n$  do
  { $INV \wedge x \neq n$ }
  if  $x = -1$  then
    { $INV \wedge x \neq n \wedge x = -1$ } (2)
    { $n = N \geq 0 \wedge (x + 1 \geq 0 \implies 1 = 2^{x+1})$ }
     $r := 1$ 
  else
    { $INV \wedge x \neq n \wedge \neg(x = -1)$ } (3)
    { $n = N \geq 0 \wedge (x + 1 \geq 0 \implies 2r = 2^{x+1})$ }
     $r := r * 2$ ;
    { $n = N > 0 \wedge (x + 1 \geq 0 \implies r = 2^{x+1})$ }
     $x := x + 1$ ;
  { $INV \wedge \neg(x \neq n)$ } (4)
  { $r = 2^N$ }

```

PrePost:

1) La prima parte della tesi $n = N \geq 0$ è l'ipotesi. La seconda parte è un'implicazione con antecedente falsa.

2) $n = N \geq 0$ fa parte di INV . La seconda parte della tesi è un'implicazione con conseguente $1 = 2^{x+1}$ che vale perché $x = -1$ per ipotesi.

3) $n = N \geq 0$ fa parte di INV . Per dimostrare $x + 1 \geq 0 \implies 2r = 2^{x+1}$ assumiamo $x + 1 \geq 0$, cioè $x \geq -1$, e dimostriamo $2r = 2^{x+1}$. Sapendo che $x \geq -1$ ma anche che $x \neq -1$ (per ipotesi), otteniamo $x \geq 0$ visto che x è intero. Da questo e INV ricaviamo $r = 2^x$ che implica la tesi $2r = 2^{x+1}$.

4) Dalle ipotesi si ha $x = n = N \geq 0$ quindi usando la parte di INV $x \geq 0 \implies r = 2^x$ si ottiene $r = 2^x$ e quindi $r = 2^N$ che è la tesi.

□