

Informatica — 2022-02-14

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

Esercizio 1. Si enuncino, senza dimostrarli, i risultati relativi al determinismo e alla totalità della semantica delle espressioni di IMP ($\rightarrow_e$) e della semantica dei comandi big step di IMP ($\rightarrow_b$).

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

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

1. [20%] Si forniscano due sequenze s_1, s_2 con 3 interi per cui valga $R(s_1, s_2)$ e 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:

$$\forall s_1, s_2, s_3 \in S. Q(s_1, s_2) \wedge R(s_2, s_3) \implies Q(s_1, s_3)$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall s_2, s_3 \in S. R(s_2, s_3) \implies p(s_2, s_3)$$

per un qualche predicato p .

4. [50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato a R .

Soluzione (bozza).

Parte 1

Una possibile soluzione è:

$$\frac{\frac{\frac{R(\epsilon, \epsilon)}{R(3 : \epsilon, 10 : \epsilon)}}{R(2 : 3 : \epsilon, 5 : 10 : \epsilon)}}{R(1 : 2 : 3 : \epsilon, 2 : 5 : 10 : \epsilon)}$$

Parte 2

Per dimostrare che $\forall s_2, s_3. R(s_2, s_3) \implies p(s_2, s_3)$ basta che:

- 1) $p(\epsilon, \epsilon)$
- 2) $\forall s, z \in S, a \in \mathbb{Z}. p(s, z) \implies p(a : s, a^2 + 1 : z)$

Parte 3

Basta prendere

$$p(s_2, s_3) : \forall s_1 \in S. Q(s_1, s_2) \implies Q(s_1, s_3)$$

Parte 4

Procediamo per induzione su R .

Caso [R0]. Dobbiamo dimostrare che $p(\epsilon, \epsilon)$, cioè che $\forall s_1. Q(s_1, \epsilon) \implies Q(s_1, \epsilon)$. L'implicazione è banale.

Caso [R1]. Per ipotesi induttiva assumiamo $p(s, z)$, cioè

$$IP1 : \forall \bar{s}_1, Q(\bar{s}_1, s) \implies Q(\bar{s}_1, z)$$

Dobbiamo dimostrare la tesi $p(a : s, a^2 + 1 : z)$, cioè

$$\forall s_1, Q(s_1, a : s) \implies Q(s_1, a^2 + 1 : z)$$

assumiamo quindi $IP2 : Q(s_1, a : s)$ e dimostriamo la nuova tesi $Q(s_1, a^2 + 1 : z)$.

Invertendo $IP2$, osserviamo che può essere ricavata solo da $Q1$. Quindi otteniamo che $s_1 = b : s'_1$ per qualche b, s'_1 tali che $IP3 : b \leq a$ e $IP4 : Q(s'_1, s)$.

Usiamo $IP1$ scegliendo $\bar{s}_1 = s'_1$ assieme a $IP4$, e otteniamo $IP5 : Q(s'_1, z)$. Di qui, siccome $b \leq a \leq a^2 + 1$, usando la regola $Q1$ otteniamo $Q(b : s'_1, a^2 + 1 : z)$ che è la tesi $Q(s_1, a^2 + 1 : z)$. □

Esercizio 3. Sia $c \in Com$ e siano P, Q, R asserzioni di Hoare. Definiamo le proprietà A, B, C come segue:

$$\begin{aligned} A : & \models \{P \vee Q\}c\{R\} \\ B : & (\models \{P\}c\{R\}) \vee (\models \{Q\}c\{R\}) \\ C : & \exists N \in \{0, 1\}. \models \{(P \wedge N = 0) \vee (Q \wedge N = 1)\}c\{R\} \end{aligned}$$

(Nota: sopra N è una variabile di specifica.)

1. [50%] Due proprietà tra le tre descritte sopra sono equivalenti. Le si identifichino e si dimostri la loro equivalenza, almeno in modo informale.
2. [50%] Si dimostri che la rimanente proprietà non è equivalente alle due di cui al punto precedente. Per farlo, si esibisca un controesempio definendo P, Q, R, c . Si giustifichi la risposta, almeno in modo informale.

Soluzione (bozza).

Parte 1 Le proprietà B e C sono equivalenti.

Infatti, la proprietà C è della forma $\exists N \in \{0, 1\}. p(N)$ e come tale è equivalente a $p(0) \vee p(1)$, e cioè:

$$\models \{(P \wedge 0 = 0) \vee (Q \wedge 0 = 1)\}c\{R\} \quad \vee \quad \models \{(P \wedge 1 = 0) \vee (Q \wedge 1 = 1)\}c\{R\}$$

Semplificando la prima parte osserviamo che

$$\models \{(P \wedge 0 = 0) \vee (Q \wedge 1 = 0)\}c\{R\}$$

è equivalente a

$$\models \{(P \wedge \text{vero}) \vee (Q \wedge \text{falso})\}c\{R\}$$

e quindi a

$$\models \{P \vee \text{falso}\}c\{R\}$$

e quindi a

$$\models \{P\}c\{R\}$$

Analogamente, la seconda parte

$$\models \{(P \wedge 1 = 0) \vee (Q \wedge 1 = 1)\}c\{R\}$$

è equivalente a

$$\models \{Q\}c\{R\}$$

Concludendo, C è equivalente a

$$\models \{P\}c\{R\} \vee \models \{Q\}c\{R\}$$

che è B .

Parte 2 Per vedere che A non è equivalente a B , prendiamo:

$$P : x = 2$$

$$Q : x = 3$$

$$c : \text{skip}$$

$$R : x = 2$$

La A diventa

$$\models \{x = 2 \vee x = 3\}\text{skip}\{x = 2\}$$

che è **falsa**. Infatti, prendendo uno stato iniziale con $\sigma(x) = 3$ questo soddisfa la precondizione, e eseguendo il comando terminiamo nello stesso stato che non soddisfa la postcondizione.

Invece la B è vera:

$$(\models \{x = 2\}\text{skip}\{x = 2\}) \vee (\models \{x = 3\}\text{skip}\{x = 2\})$$

Infatti la parte sinistra dell'OR è vera: la sua validità segue (anche) dal teorema di correttezza e dalla regola *Skip* del sistema deduttivo per le triple di Hoare.

□

Nome _____ Matricola _____

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

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

$a := 0;$

$b := 0;$

while $a < x$ do

if $a < b$ then

$a := a + 1$
else

$b := b + 1$

$\{a = b = N\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

```
{x = N ≥ 0} (1)
{INV : 0 ≤ 0 ≤ 0 ≤ x = N}
a := 0;
{INV : 0 ≤ a ≤ 0 ≤ x = N}
b := 0;
{INV : 0 ≤ a ≤ b ≤ x = N}
while a < x do
  {INV ∧ a < x}
  if a < b then
    {INV ∧ a < x ∧ a < b} (2)
    {0 ≤ a + 1 ≤ b ≤ x = N}
    a := a + 1
  else
    {INV ∧ a < x ∧ ¬(a < b)} (3)
    {0 ≤ a ≤ b + 1 ≤ x = N}
    b := b + 1
  {INV ∧ ¬(a < x)} (4)
{a = b = N}
```

Per le PrePost:

1) banale aritmetica.

2) Per ipotesi $0 \leq a$, da cui la tesi $0 \leq a + 1$. Per ipotesi $a < b$, da cui la tesi $a + 1 \leq b$, visto che sono tutti interi. Per ipotesi $b \leq x = N$, da cui la tesi identica.

3) Per ipotesi $0 \leq a \leq b$, da cui la tesi $0 \leq a \leq b + 1$. Per ipotesi $a \leq b$ e $\neg(a < b)$, quindi $a = b$, e siccome per ipotesi $a < x$, si ha $b < x$ da cui la tesi $b + 1 \leq x$. Per ipotesi $x = N$, da cui la tesi identica.

4) Per ipotesi $a \leq x$ e $\neg(a < x)$ da cui $a = x$. Da questo, siccome per ipotesi vale anche $a \leq b \leq x = N$, si ha la tesi $a = b = N$.

□