Informatica — 2024-07-15

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

Esercizio 1. *Si fornisca la definizione di validità per una tripla di Hoare, commentandola sinteticamente. Dopo, si enunci il teorema di correttezza per il sistema deduttivo delle triple di Hoare, commentandolo sinteticamente.*

Esercizio 2. *Sia $\mathbb{B} = \{\mathsf{t}, \mathsf{f}\}$ l'insieme dei valori booleani. Le seguenti regole definiscono induttivamente l'insieme T degli alberi binari di coppie intero-booleano (regole $[T0], [T1]$), una relazione $Q \in \mathcal{P}(T \times \mathbb{Z})$ (regole $[Q0], [Q1], [Q2]$), e una relazione $R \in \mathcal{P}(T \times T)$ (regole $[R0], [R1], [R2]$). Sotto, z indicano interi, b booleani, mentre s, d, t, u, v indicano alberi in T.*

$$\frac{}{[z, b]} \begin{pmatrix} z \in \mathbb{Z} \\ b \in \mathbb{B} \end{pmatrix} [T0] \quad \frac{s \quad d}{(s, d)} [T1] \quad \frac{}{Q([z, \mathsf{t}], z)} [Q0] \quad \frac{}{Q([z, \mathsf{f}], -z)} [Q1] \quad \frac{Q(t_1, z_1) \quad Q(t_2, z_2)}{Q((t_1, t_2), z_1 + z_2)} [Q2]$$

$$\frac{}{R([z, \mathsf{t}], [z, \mathsf{f}])} [R0] \quad \frac{}{R([z, \mathsf{f}], [z, \mathsf{t}])} [R1] \quad \frac{R(t_1, u_1) \quad R(t_2, u_2)}{R((t_1, t_2), (u_2, u_1))} [R2]$$

1. *[20%] Sia $t = ([1, \mathsf{t}], ([2, \mathsf{f}], [3, \mathsf{t}]))$. Si trovino $u \in T, z \in \mathbb{Z}$ per cui valga $R(t, u) \land Q(u, z)$. Si giustifichi la risposta esibendo due derivazioni.*

2. *[20%] Si enunci il principio di induzione associato alla relazione R.*

3. *[10%] Si consideri l'enunciato seguente:*

   $$\forall t, u \in T, z \in \mathbb{Z}.\ Q(t, z) \land R(t, u) \implies Q(u, -z)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall t, u \in T.\ R(t, u) \implies p(t, u)$$

   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:

$$\dfrac{\dfrac{}{R([1, \mathsf{t}], [1, \mathsf{f}])}[R0] \quad \dfrac{\dfrac{}{R([2, \mathsf{f}], [2, \mathsf{t}])}[R1] \quad \dfrac{}{R([3, \mathsf{t}], [3, \mathsf{f}])}[R0]}{R(([2, \mathsf{f}], [3, \mathsf{t}]), ([2, \mathsf{t}], [3, \mathsf{f}]))}[R2]}{R(([1, \mathsf{t}], ([2, \mathsf{f}], [3, \mathsf{t}])), ([1, \mathsf{f}], ([2, \mathsf{t}], [3, \mathsf{f}])))}[R2]$$

$$\dfrac{\dfrac{}{Q([1, \mathsf{f}], -1)}[Q1] \quad \dfrac{\dfrac{}{Q([2, \mathsf{t}], 2)}[Q0] \quad \dfrac{}{R([3, \mathsf{f}], -3)}[Q1]}{Q(([2, \mathsf{t}], [3, \mathsf{f}]), -1)}[Q2]}{Q(([1, \mathsf{f}], ([2, \mathsf{t}], [3, \mathsf{f}])), -2)}[Q2]$$

Parte 2.
Affinché valga $\forall t, u.\ R(t, u) \implies p(t, u)$ è sufficiente che:

$R0)$ $\forall z \in \mathbb{Z}.\ p([z, \mathsf{t}], [z, \mathsf{f}])$
$R1)$ $\forall z \in \mathbb{Z}.\ p([z, \mathsf{f}], [z, \mathsf{t}])$
$R2)$ $\forall t_1, t_2, u_1, u_2.\ p(t_1, u_1) \land p(t_2, u_2) \implies p((t_1, t_2), (u_2, u_1))$

Parte 3.

Basta prendere

$$p(t,u): \quad \forall z \in \mathbb{Z}.\ Q(t,z) \implies Q(u,-z)$$

Parte 4. Andiamo quindi per induzione su R.
Caso [**R0**]. Dobbiamo dimostrare $p([z,\mathsf{t}],[z,\mathsf{f}])$, ovvero

$$\forall z' \in \mathbb{Z}.\ Q([z,\mathsf{t}],z') \implies Q([z,\mathsf{f}],-z')$$

Assumiamo quindi $IP1 : Q([z,\mathsf{t}],z')$ e dimostriamo la tesi $Q([z,\mathsf{f}],-z')$.
Invertendo $IP1$, notiamo che può derivare solo da $[Q0]$ e quindi $z' = z$.
La tesi si riscrive quindi come $Q([z,\mathsf{f}],-z)$, che deriva da $[Q1]$.
Caso [**R1**]. Dobbiamo dimostrare $p([z,\mathsf{f}],[z,\mathsf{t}])$, ovvero

$$\forall z' \in \mathbb{Z}.\ Q([z,\mathsf{f}],z') \implies Q([z,\mathsf{t}],-z')$$

Assumiamo quindi $IP1 : Q([z,\mathsf{f}],z')$ e dimostriamo la tesi $Q([z,\mathsf{t}],-z')$.
Invertendo $IP1$, notiamo che può derivare solo da $[Q1]$ e quindi $z' = -z$.
La tesi si riscrive quindi come $Q([z,\mathsf{t}],z)$, che deriva da $[Q0]$.
Caso [**R2**]. Assumiamo le ipotesi induttive

$$IP1 : p(t_1,u_1) \qquad IP2 : p(t_2,u_2)$$

e dimostriamo la tesi $p((t_1,t_2),(u_2,u_3)))$. Riscriviamo le ipotesi come

$$\begin{array}{l} IP1: \ \forall \bar{z} \in \mathbb{Z}.\ Q(t_1,\bar{z}) \implies Q(u_1,-\bar{z}) \\ IP2: \ \forall \hat{z} \in \mathbb{Z}.\ Q(t_2,\hat{z}) \implies Q(u_2,-\hat{z}) \end{array}$$

e la tesi come $\forall z \in \mathbb{Z}.\ Q((t_1,t_2),z) \implies Q((u_2,u_1),-z)$.
Assumiamo quindi $IP3 : Q((t_1,t_2),z)$ e dimostriamo la nuova tesi $Q((u_2,u_1),z)$.
Invertendo $IP3$, notiamo che può essere ricavata solo da $[Q2]$. Assumiamo quindi $IP4 : Q(t_1,z_1)$, $IP5 : Q(t_2,z_2)$ e $z = z_1 + z_2$.
Usando $IP4$ e $IP1$ (con $\bar{z} = z_1$) otteniamo $IP6 : Q(u_1,-z_1)$.
Usando $IP5$ e $IP2$ (con $\hat{z} = z_2$) otteniamo $IP7 : Q(u_2,-z_2)$.
Possiamo quindi ottenere la tesi da $IP6, IP7$ tramite la derivazione seguente

$$\frac{Q(u_2,-z_2) \qquad Q(u_1,-z_1)}{Q((u_2,u_1)),(-z_2)+(-z_1))}[Q2]$$

grazie al fatto che $z = -(z_1+z_2) = (-z_2)+(-z_1)$.

□

Esercizio 3. *Si consideri una variante IMP_1 di IMP ottenuta togliendo il ciclo* while *e aggiungendo i due nuovi comandi* push x *e* pop x *con $x \in Var$. La semantica di IMP_1 differisce da quella di IMP nel modo seguente.*
Come insieme degli stati σ si usa $State = Var \to \mathbb{Z}^*$ dove $\mathbb{Z}^*$ è l'insieme delle sequenze finite di interi. Nello stato σ, il valore dell'espressione variabile x è il primo elemento delle sequenza $\sigma(x)$ (o zero se $\sigma(x)$ è vuota). Il comando push x *aggiunge all'inizio della sequenza $\sigma(x)$ il valore di x (definito come sopra). Il comando* pop x *rimuove il primo elemento della sequenza $\sigma(x)$ (o non fa nulla se è vuota). L'assegnamento $x := e$ modifica il primo elemento della sequenza $\sigma(x)$ (o le aggiunge un elemento se è vuota).*

1. *[60%] Si formalizzi la semantica delle espressioni e dei comandi di IMP_1 con opportune regole di inferenza.*

2. *[40%] Sia IMP_2 la restrizione di IMP_1 ottenuta vincolando le guardie degli* if *ad avere la forma $x \neq 0$ per qualche $x \in Var$. Si descriva in modo informale ma preciso come si può tradurre un comando di IMP_1 in uno di IMP_2 preservandone la semantica.*

Soluzione (bozza).
Parte 1.
Per le espressioni:

$$\frac{}{\langle z, \sigma\rangle \to_e z}[Lit]$$

$$\frac{\sigma(x) = z : s}{\langle x, \sigma\rangle \to_e z}[Var1]$$

$$\frac{\sigma(x) = \epsilon}{\langle x, \sigma\rangle \to_e 0}[Var2]$$

$$\frac{\langle e_1, \sigma\rangle \to_e z_1 \qquad \langle e_2, \sigma\rangle \to_e z_2}{\langle e_1 + e_2, \sigma\rangle \to_e z_1 + z_2}[Plus]$$

Per i comandi:

$$\frac{}{\langle \mathsf{skip}, \sigma\rangle \to_b \sigma}[Skip]$$

$$\frac{\langle e, \sigma\rangle \to_e z \qquad \sigma(x) = z' : s}{\langle x := e, \sigma\rangle \to_b \sigma[x \mapsto z : s]}[Let1]$$

$$\frac{\langle e, \sigma\rangle \to_e z \qquad \sigma(x) = \epsilon}{\langle x := e, \sigma\rangle \to_b \sigma[x \mapsto z : \epsilon]}[Let2]$$

$$\frac{\langle x, \sigma\rangle \to_e z}{\langle \mathsf{push}\ x, \sigma\rangle \to_b \sigma[x \mapsto z : \sigma(x)]}[Push]$$

$$\frac{\sigma(x) = z : s}{\langle \mathsf{pop}\ x, \sigma\rangle \to_b \sigma[x \mapsto s]}[Pop1]$$

$$\frac{\sigma(x) = \epsilon}{\langle \mathsf{pop}\ x, \sigma\rangle \to_b \sigma}[Pop2]$$

$$\frac{\langle c_1, \sigma\rangle \to_b \sigma' \qquad \langle c_2, \sigma'\rangle \to_b \sigma''}{\langle c_1; c_2, \sigma\rangle \to_b \sigma''}[Comp]$$

$$\frac{\langle e, \sigma\rangle \to_e v \neq 0 \qquad \langle c_1, \sigma\rangle \to_b \sigma'}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \to_b \sigma'}[If - true]$$

$$\frac{\langle e, \sigma\rangle \to_e 0 \qquad \langle c_2, \sigma\rangle \to_b \sigma'}{\langle \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \to_b \sigma'}[If - false]$$

Parte 2.
Basta riscrivere i comandi della forma $\mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2$ nella forma seguente:

$\mathsf{push}\ x;$
$x := e;$
$\mathsf{if}\ x \neq 0\ \mathsf{then}$
    $\mathsf{pop}\ x;$
    c_1
else
    $\mathsf{pop}\ x;$
    c_2

dove x è una variabile arbitraria.

Si noti che dopo $\mathsf{push}\ x$, anche se lo stato è cambiato, l'espressione x ha sempre lo stesso valore, e quindi anche l'espressione e ha sempre lo stesso valore.

L'assegnamento $x := e$ modifica solo il "primo" valore di x, quello appena aggiunto alla sequenza, mantenendo gli altri invariati.

I comandi pop x ripristinano i valori originale di x (tutta la sua sequenza associata), e quindi fanno sì che c_1 e c_2 vengano eseguiti nello stesso stato in cui sarebbero stati eseguiti usando l'if originale.

□

Nome _____ Matricola _____

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

$\{n = 35N > 0\}$

$x := 0;$

$y := 0;$

---

while $x < n$ do

---

if $x * 7 = n$ then

$y := 1$

else

---

skip;

$x := x + 1$

$\{y = 1\}$

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

Soluzione (bozza).

$\{n = 35N > 0\}$ (1)
$\{0 > 5N \implies 0 = 1 \wedge 0 \leq n = 35N > 0\}$
$x := 0;$
$\{x > 5N \implies 0 = 1 \wedge x \leq n = 35N > 0\}$
$y := 0;$
$\{INV : x > 5N \implies y = 1 \wedge x \leq n = 35N > 0\}$
while $x < n$ do
    $\{INV \wedge x < n\}$
    if $x * 7 = n$ then
        $\{INV \wedge x < n \wedge 7x = n\}$ (2)
        $\{x + 1 > 5N \implies 1 = 1 \wedge x + 1 \leq n = 35N > 0\}$
        $y := 1$
    else
        $\{INV \wedge x < n \wedge \neg(7x = n)\}$ (3)
        $\{x + 1 > 5N \implies y = 1 \wedge x + 1 \leq n = 35N > 0\}$
        skip;
    $\{x + 1 > 5N \implies y = 1 \wedge x + 1 \leq n = 35N > 0\}$
    $x := x + 1$
$\{INV \wedge \neg(x < n)\}$ (4)
$\{y = 1\}$

Per le PrePost:

1) La parte $0 > 5N \implies 0 = 1$ è vera perché per ipotesi $N > 0$ e quindi l'antecedente è falsa. La parte $0 \leq n = 35N > 0$ segue dall'ipotesi $n = 35N > 0$.

2) La parte $x+1 > 5N \implies 1 = 1$ è banalmente vera. La parte $x+1 \leq n = 35N > 0$ deriva dall'ipotesi $n = 35N > 0$ e $x < n$.

3) La parte $x + 1 \leq n = 35N > 0$ segue dall'ipotesi $n = 35N > 0$ e da $x < n$, visto che sono numeri interi. Per la parte $x + 1 > 5N \implies y = 1$, assumiamo $x + 1 > 5N$ (ovvero $x \geq 5N$) e dimostriamo $y = 1$. Esaminiamo i due casi: $x > 5N$ e $x = 5N$. Nel caso $x > 5N$, la tesi deriva da INV. Nel caso $x = 5N$, abbiamo $7x = 35N = n$ che contraddice l'ipotesi $\neg(7x = n)$.

4) Da INV si ha $x \leq n$ che con l'ipotesi $x < n$ dimostra $x = n$. Col resto di INV, si ha quindi $x = n = 35N > 0$. Da questo si ha $x > 5N$ e quindi da INV la tesi $y = 1$.

□