Informatica — 2021-07-26

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, anche qui commentandolo sinteticamente.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi di interi (regole $[T0], [T1]$), una proprietà $S \in \mathcal{P}(T)$ (regole $[S0], [S1]$), e una relazione $R \in \mathcal{P}(T \times \mathbb{Z})$ (regole $[R0], [R1]$). Sotto, a, b, x indicano interi mentre t, s, d indicano alberi in T.*

$$\frac{}{a}(a \in \mathbb{Z})[T0] \qquad \frac{s \quad d}{(s,d)}(a \in \mathbb{Z})[T1] \qquad \frac{a \geq 5}{S(a)}[S0] \qquad \frac{S(s) \quad S(d)}{S((s,d))}[S1]$$

$$\frac{b \leq a}{R(a,b)}[R0] \qquad \frac{R(s,a) \quad R(d,b) \quad b \leq a}{R((s,d),b)}[R1]$$

1. *[20%] Si fornisca un albero t con 5 interi distinti per cui valga $S(t) \wedge R(t,2)$ e 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:*

   $$\forall t \in T, x \in \mathbb{Z}.\ R(t,x) \wedge x \geq 10 \implies S(t)$$

   Si riscriva l'enunciato in modo logicamente equivalente nella forma

   $$\forall t \in T, x \in \mathbb{Z}.\ R(t,x) \implies p(t,x)$$

   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

Due possibili derivazioni:

$$\dfrac{\dfrac{\dfrac{}{S(5)} \quad \dfrac{}{S(7)}}{S((5,7))} \quad \dfrac{\dfrac{}{S(8)} \quad \dfrac{\dfrac{}{S(6)} \quad \dfrac{}{S(10)}}{S((6,10))}}{S((8,(6,10)))}}{S(((5,7),(8,(6,10))))}$$

$$\dfrac{\dfrac{\dfrac{}{R(5,2)} \quad \dfrac{}{R(7,2)}}{R((5,7),2)} \quad \dfrac{\dfrac{}{R(8,2)} \quad \dfrac{\dfrac{}{R(6,2)} \quad \dfrac{}{R(10,2)}}{R((6,10),2)}}{R((8,(6,10)),2)}}{R(((5,7),(8,(6,10))),2)}$$

Parte 2

Per dimostrare che, per ogni $t \in T, x \in \mathbb{Z}$ tali che $R(t,x)$ vale $p(t,x)$ basta verificare che:

$R0)$ $\forall a, b \in \mathbb{Z}.\ b \leq a \implies p(a,b)$
$R1)$ $\forall a, b \in \mathbb{Z}, s, d \in T.\ p(s,a) \wedge p(d,b) \wedge b \leq a \implies p((s,d),b)$

Parte 3

Basta definire $p(t, x)$ come $x \geq 10 \implies S(t)$.

Parte 4

Caso $R0$

Assumiamo $IP1: \ b \leq a$. Dobbiamo dimostrare $p(a, b)$. Per farlo assumiamo $IP2: \ b \geq 10$ e dimostriamo la nuova tesi $S(a)$.

Da $IP1, IP2$ ricaviamo $a \geq 10$ e quindi anche $a \geq 5$, da cui usando $[S0]$ ricaviamo la tesi $S(a)$.

Caso $R1$ Assumiamo

$$\begin{aligned} IP1: &\ \ b \leq a \\ IP2: &\ \ p(s, a) \\ IP3: &\ \ p(d, b) \end{aligned}$$

e quindi

$$\begin{aligned} IP2: &\ \ a \geq 10 \implies S(s) \\ IP3: &\ \ b \geq 10 \implies S(d) \end{aligned}$$

Dobbiamo dimostrare $p((s, d), b)$. Per farlo assumiamo $IP4: b \geq 10$ e dimostriamo la nuova tesi $S((s, d))$.

Da $IP4$ e $IP3$ ricaviamo $IP5: \ S(d)$.

Da $IP1, IP4$ ricaviamo $a \geq 10$, da cui con $IP2$ ricaviamo $IP6: \ S(s)$.

Possiamo ora applicare $[S1]$ a $IP6, IP7$ e ricavare la tesi $S((s, d))$.

□

Esercizio 3. *Si consideri una modifica del linguaggio IMP dove il risultato della valutazione delle espressioni non è più un singolo intero, ma un insieme di interi. Più in dettaglio, la sintassi delle espressioni viene estesa con l'espressione* $\diamond$ *che ha valore* $\{0, 1\}$*. Gli altri costrutti sintattici generano "l'insieme di tutti i risultati possibili", come illustrato dai seguenti esempi.*

$$\langle 3, \sigma\rangle \to_e \{3\} \qquad \langle 3 + \diamond, \sigma\rangle \to_e \{3, 4\} \qquad \langle \diamond + \diamond, \sigma\rangle \to_e \{0, 1, 2\}$$

$$\langle \diamond + 3 * \diamond, \sigma\rangle \to_e \{0, 1, 3, 4\} \qquad \langle \diamond + x * \diamond, \sigma\rangle \to_e \{0, 1, \sigma(x), 1 + \sigma(x)\}$$

1. *[50%] Si definisca tramite un insieme di regole di inferenza la semantica delle espressioni illustrata sopra* $(\to_e) \in \mathcal{P}(Exp \times State \times \mathcal{P}(\mathbb{Z}))$*. Si commentino brevemente le regole.*

2. *[25%] Siano* e_1, e_2 *due espressioni arbitrarie nelle quali non appare nessun* $\diamond$*. Si definisca una espressione* e_u *tale che*

   $$\forall \sigma \in State, V_1, V_2 \in \mathcal{P}(\mathbb{Z}). \quad \langle e_1, \sigma\rangle \to_e V_1 \wedge \langle e_2, \sigma\rangle \to_e V_2 \implies \langle e_u, \sigma\rangle \to_e V_1 \cup V_2$$

   Si giustifichi la risposta in modo informale.

3. *[25%] Si consideri la* e_u *definita sopra nel caso generale, dove* e_1, e_2 *sono espressioni nelle quali può anche apparire* $\diamond$*. Si stabilisca se la proprietà sopra continua a valere o meno, giustificando la risposta in modo informale.*

Soluzione (bozza).

Parte 1

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

$$\frac{}{\langle x, \sigma\rangle \to_e \{\sigma(x)\}}[Var]$$

$$\frac{}{\langle \diamond, \sigma\rangle \to_e \{0, 1\}}[Square]$$

$$\frac{\langle e_1, \sigma\rangle \to_e V_1 \quad \langle e_2, \sigma\rangle \to_e V_2}{\langle e_1 + e_2, \sigma\rangle \to_e \{z_1 + z_2 \mid z_1 \in V_1 \wedge z_2 \in V_2\}}[Plus]$$

Parte 2

Una possibile definizione è $e_u = e_1 + \diamond * (e_2 - e_1)$. Infatti, assumendo le ipotesi, le valutazioni di e_1 e e_2 possono dare un solo valore come risultato e quindi $V_1 = \{v_1\}$ e $V_2 = \{v_2\}$ per qualche $v_1, v_2 \in \mathbb{Z}$. In questo caso la valutazione di e_u ha come risultato $\{v_1 + 0 \cdot (v_2 - v_1), v_1 + 1 \cdot (v_2 - v_1)\} = \{v_1, v_2\} = V_1 \cup V_2$.

Parte 3

Nel caso generale la costruzione vista sopra non regge. Per esempio, se $e_1 = \diamond, e_2 = 5$ abbiamo come risultato $V_1 = \{0, 1\}$ e $V_2 = \{5\}$.

Tuttavia la valutazione di $e_u = \diamond + \diamond * (5 - \diamond)$ ha come risultato $V = \{0, 1, 4, 5, 6\}$ in cui compaiono anche $4 = 0 + 1 \cdot (5 - 1)$ e $6 = 1 + 1 \cdot (5 - 0)$, quindi $V \neq V_1 \cup V_2$.

Il problema di fondo è che in e_u il primo e l'ultimo $\diamond$ (originariamente provenienti da e_1) non vengono necessariamente valutati allo stesso valore.

□

Nome _____ Matricola _____

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

$\{k \geq 1\}$

$x := 0;$

$n := 1;$

---

while $n < k$ do

---

if $x < n$ then

$x := x + 1$

else

$n := n + 1$

$\{x + 1 = n = k\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

$\{k \geq 1\}$ (1)
$\{(0 = 1 - 1 \wedge 1 \leq k) \vee (0 = 1 \wedge 1 < k)\}$
$x := 0;$
$\{(x = 1 - 1 \wedge 1 \leq k) \vee (x = 1 \wedge 1 < k)\}$
$n := 1;$
$\{INV : \ (x = n - 1 \wedge n \leq k) \vee (x = n \wedge n < k)\}$
while $n < k$ do
    $\{INV \wedge n < k\}$
    if $x < n$ then
        $\{INV \wedge n < k \wedge x < n\}$ (2)
        $\{(x + 1 = n - 1 \wedge n \leq k) \vee (x + 1 = n \wedge n < k)\}$
        $x := x + 1$
    else
        $\{INV \wedge n < k \wedge \neg(x < n)\}$ (3)
        $\{(x = n + 1 - 1 \wedge n + 1 \leq k) \vee (x = n + 1 \wedge n + 1 < k)\}$
        $n := n + 1$
$\{INV \wedge \neg(n < k)\}$ (4)
$\{x + 1 = n = k\}$

Per le PrePost:

1) Dall'ipotesi si dimostra la parte sinistra dell'OR. Infatti, $0 = 1 - 1$ è banale, mentre $1 \leq k$ è l'ipotesi.

2) Siccome $x < n$ per ipotesi, non può valere la parte destra di INV $x = n \wedge n < k$, quindi deve essere vera la parte sinistra $x = n - 1 \wedge n \leq k$. Con questo e l'ipotesi $n < k$ otteniamo la parte destra della tesi $x + 1 = n \wedge n < k$.

3) Siccome $\neg(x < n)$ per ipotesi, non può valere la parte sinistra di INV $x = n - 1 \wedge n \leq k$, quindi deve essere vera la parte destra $x = n \wedge n < k$. Da questo si ottene la parte sinistra della tesi $x = n + 1 - 1 \wedge n + 1 \leq k$.

4) Siccome $\neg(n < k)$ per ipotesi, non può valere la parte destra di INV $x = n \wedge n < k$, quindi deve essere vera la parte sinistra $x = n - 1 \wedge n \leq k$. Da questo, usando ancora l'ipotesi $\neg(n < k)$, ricaviamo la tesi $x + 1 = n = k$.

□