Informatica — 2020-09-11

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 binari con numeri interi nei nodi interni (regole $[T0], [T1]$), una relazione $R \in \mathcal{P}(T \times T)$ (regole $[R0], [R1]$), e una relazione $Q \in \mathcal{P}(T \times \mathbb{Z})$ (regole $[Q0], [Q1]$). Sotto, a, x, y indicano interi mentre s, d, t indicano alberi in T.*

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

$$\frac{}{Q(\epsilon, 0)}[Q0] \qquad \frac{Q(s, x) \quad Q(d, y)}{Q((s, a, d), x + a + y)}[Q1]$$

1. *[20%] Si fornisca un albero t contenente esattamente 3 interi e un albero t' per cui valga $R(t, t')$ 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:*

   $$\forall t_1, t_2 \in T, x_1, x_2 \in \mathbb{Z}.\ R(t_1, t_2) \land Q(t_1, x_1) \land Q(t_2, x_2) \implies x_1 + x_2 = 0$$

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

Soluzione (bozza).
Parte 1
Un possibile esempio è:

$$\dfrac{\dfrac{\dfrac{}{R(\epsilon,\epsilon)} \quad \dfrac{}{R(\epsilon,\epsilon)}}{R((\epsilon,1,\epsilon),(\epsilon,-1,\epsilon))} \quad \dfrac{\dfrac{}{R(\epsilon,\epsilon)} \quad \dfrac{}{R(\epsilon,\epsilon)}}{R((\epsilon,-3,\epsilon),(\epsilon,3,\epsilon))}}{R(((\epsilon,1,\epsilon),2,(\epsilon,-3,\epsilon)),((\epsilon,-1,\epsilon),-2,(\epsilon,3,\epsilon)))}$$

Parte 2
Per dimostrare $p(t_1, t_2)$ per ogni $t_1, t_2 \in T$ tali che $R(t_1, t_2)$ è sufficiente verificare che:

1) $p(\epsilon, \epsilon)$
2) $\forall s, d, s', d', a.\ p(s, s') \land p(d, d') \implies p((s, a, d), (s', -a, d'))$

Parte 3
Basta prendere:

$$p(t_1, t_2) : \forall x_1, x_2 \in \mathbb{Z}.\ Q(t_1, x_1) \land Q(t_2, x_2) \implies x_1 + x_2 = 0$$

Parte 4 Procediamo per induzione su R:
Caso $[R0]$

Dobbiamo dimostrare $p(\epsilon, \epsilon)$. Per farlo, assumiamo come ipotesi

$$IP1 : Q(\epsilon, x_1)$$
$$IP2 : Q(\epsilon, x_2)$$

e dimostriamo la nuova tesi $x_1 + x_2 = 0$.

Invertiamo $IP1$: siccome può essere ricavata solo da $[Q0]$, otteniamo $x_1 = 0$.

Invertiamo $IP2$: siccome può essere ricavata solo da $[Q0]$, otteniamo $x_2 = 0$.

Di qui, la tesi si ricava facilmente: $x_1 + x_2 = 0 + 0 = 0$.

Caso $[R1]$

Assumendo come ipotesi induttive $IP1 : p(s, s')$ e $IP2 : p(d, d')$, ovvero

$$IP1 : \forall x_1', x_2' \in \mathbb{Z}.\ Q(s, x_1') \wedge Q(s', x_2') \implies x_1' + x_2' = 0$$
$$IP2 : \forall x_1'', x_2'' \in \mathbb{Z}.\ Q(d, x_1'') \wedge Q(d', x_2'') \implies x_1'' + x_2'' = 0$$

dimostriamo la tesi $p((s, a, d), (s', -a, d'))$. Per farlo, assumiamo come ipotesi

$$IP3 : Q((s, a, d), x_1)$$
$$IP4 : Q((s', -a, d'), x_2)$$

e dimostriamo la nuova tesi $x_1 + x_2 = 0$.

Invertiamo $IP3$: siccome può essere ricavata solo da $[Q1]$, otteniamo $x_1 = b_1 + a + c_1$ assieme a

$$IP4 : Q(s, b_1)$$
$$IP5 : Q(d, c_1)$$

Invertiamo $IP4$: siccome può essere ricavata solo da $[Q1]$, otteniamo $x_2 = b_2 + (-a) + c_2$ assieme a

$$IP6 : Q(s', b_2)$$
$$IP7 : Q(d', c_2)$$

Da $IP1$ (con $x_1' = b_1$ e $x_2' = b_2$) e da $IP4, IP6$ otteniamo $b_1 + b_2 = 0$.

Da $IP2$ (con $x_1'' = c_1$ e $x_2' = c_2$) e da $IP5, IP7$ otteniamo $c_1 + c_2 = 0$.

Concludendo, per dimostrare la tesi, basta usare tutte le uguaglianze così ricavate:

$$x_1 + x_2 = (b_1 + a + c_1) + (b_2 + (-a) + c_2) = (b_1 + b_2) + (a - a) + (c_1 + c_2) = 0 + 0 + 0 = 0$$

□

Esercizio 3. *Si consideri il linguaggio IMP con le sue espressioni e i suoi comandi. Si definiscano come segue le due relazioni* $E \in \mathcal{P}(Exp \times Exp)$ *e* $C \in \mathcal{P}(Com \times Com)$. $E(e, e')$ *vale se e solo se* e' *è ottenuta da* e *aumentando di uno tutte le costanti. Analogamente,* $C(c, c')$ *vale se e solo se il comando* c' *è ottenuto da* c *aumentando di uno tutte le costanti, eccetto il "*$\neq 0$*" che appare nella sintassi di* if *e* while*. Per esempio, valgono:*

$$E((x + 5) * y + 4, \quad (x + 6) * y + 5)$$
$$C(\textsf{while } x + 4 \neq 0 \textsf{ do } x := x - 5, \quad \textsf{while } x + 5 \neq 0 \textsf{ do } x := x - 6)$$

1. *[50%] Si formalizzino le relazioni* E, C *descritte sopra, definendole induttivamente tramite un insieme di regole. Per chiarezza, indicate con* $\oplus$ *la somma in* $\mathbb{Z}$ *e con* $+$ *la sintassi per la somma tra espressioni.*

2. *[50%] Si trovino due comandi* c *e* c' *che soddisfino la proprietà seguente. Sotto,* σ_0 *indica lo stato che associa il valore zero a tutte le variabili. Si giustifichi la risposta almeno in modo informale.*

$$C(c, c') \wedge \Big(\exists \sigma', \sigma''.\ \langle c, \sigma_0 \rangle \to_b \sigma' \wedge \langle c', \sigma_0 \rangle \to_b \sigma'' \wedge \sigma'(x) = 3 \wedge \sigma''(x) = 10\Big)$$

Soluzione (bozza).
Parte 1

$$\frac{}{E(z, z \oplus 1)}$$

$$\frac{}{E(x, x)}$$

$$\frac{E(e_1, e_1') \quad E(e_2, e_2')}{E(e_1 + e_2,\ e_1' + e_2')}$$

$$\frac{E(e_1, e_1') \quad E(e_2, e_2')}{E(e_1 - e_2,\ e_1' - e_2')}$$

$$\frac{E(e_1, e_1') \quad E(e_2, e_2')}{E(e_1 * e_2,\ e_1' * e_2')}$$

$$\frac{}{C(\mathsf{skip}, \mathsf{skip})}$$

$$\frac{E(e, e')}{C(x := e, x := e')}$$

$$\frac{C(c_1, c_1') \qquad C(c_2, c_2')}{C(c_1; c_2,\ c_1'; c_2')}$$

$$\frac{E(e, e') \qquad C(c_1, c_1') \qquad C(c_2, c_2')}{C(\mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2,\ \mathsf{if}\ e' \neq 0\ \mathsf{then}\ c_1'\ \mathsf{else}\ c_2')}$$

$$\frac{E(e, e') \qquad C(c, c')}{C(\mathsf{while}\ e \neq 0\ \mathsf{do}\ c,\ \mathsf{while}\ e' \neq 0\ \mathsf{do}\ c')}$$

Parte 2
Si prendano c, c' some segue

$$c = \mathsf{if}\ 1 + 1 - 2 \neq 0\ \mathsf{then}\ x := 9\ \mathsf{else}\ x := 3$$
$$c' = \mathsf{if}\ 2 + 2 - 3 \neq 0\ \mathsf{then}\ x := 10\ \mathsf{else}\ x := 4$$

È immediato vedere che $C(c, c')$ vale.

Eseguendo c dallo stato σ_0, siccome la guardia dell'if è falsa, si assegna 3 a x e si termina in $\sigma' = \sigma_0[x \mapsto 3]$ che soddisfa $\sigma'(x) = 3$.

Invece, eseguendo c' dallo stato σ_0, siccome ora la guardia dell'if è vera, si assegna 10 a x e si termina in $\sigma'' = \sigma_0[x \mapsto 10]$ che soddisfa $\sigma''(x) = 10$.

□

Nome _____ Matricola _____

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

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

$y := 0;$

---

while $x > 0$ do

$x := x - 2;$

$y := y + 10$

$\{y = 5N\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

Soluzione (bozza).

$\{x = N \text{ pari } \geq 0\}$ (1)
$\{x \geq 0 \wedge x \text{ pari} \wedge 5x + 0 = 5N\}$
$y := 0;$
$\{INV : x \geq 0 \wedge x \text{ pari} \wedge 5x + y = 5N\}$
while $x > 0$ do
    $\{INV \wedge x > 0\}$ (2)
    $\{x - 2 \geq 0 \wedge x - 2 \text{ pari} \wedge 5(x - 2) + y + 10 = 5N\}$
    $x := x - 2;$
    $\{x \geq 0 \wedge x \text{ pari} \wedge 5x + y + 10 = 5N\}$
    $y := y + 10$
$\{INV \wedge \neg(x > 0)\}$ (3)
$\{y = 5N\}$

PrePost:

1) Banale aritmetica.

2) La tesi $x - 2 \geq 0$ si ricava da $x > 0$ e dalla parità di x. La tesi $x - 2$ pari si ricava da x pari. La tesi $5(x - 2) + y + 10 = 5N$ si riscrive equivalentemente come $5x - 10 + y + 10 = 5N$ e quindi come $5x + y = 5N$ che è un'ipotesi.

3) Da $x \geq 0$ e $\neg(x > 0)$ si ha $x = 0$. Di qui e INV, si ha $5 \cdot 0 + y = 5N$ e quindi la tesi.

□