Informatica — 2022-06-24

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 naturali (regole $[T0], [T1]$), una relazione $C \in \mathcal{P}(T \times \mathbb{N})$ (regole $[C0], [C1]$), e una relazione $D \in \mathcal{P}(T \times T)$ (regole $[D0], [D1], [D2]$). Sotto, n, k indicano naturali, mentre s, d, t indicano alberi in T.*

$$\frac{}{n}(n \in \mathbb{N})[T0] \qquad \frac{s \quad d}{(s,d)}[T1] \qquad \frac{}{C(n,1)}[C0] \qquad \frac{C(s,n_s) \qquad C(d,n_d)}{C((s,d), n_s+n_d)}[C1]$$

$$\frac{}{D(n,(n,n))}[D0] \qquad \frac{D(s,s') \qquad D(d,d')}{D((s,d),(s',d'))}[D1] \qquad \frac{D(s,s') \qquad D(d,d')}{D((s,d),((s',s'),(d',d')))}[D2]$$

1. *[20%] Si forniscano due alberi t_1, t_2 per cui valga $C(t_1,3) \wedge D(t_1,t_2)$ e si giustifichi la risposta esibendo due derivazioni.*

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

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

$$\forall t_1, t_2 \in T, k \in \mathbb{N}.\ D(t_1,t_2) \wedge C(t_2,k) \implies k \text{ pari}$$

Si riscriva l'enunciato in modo logicamente equivalente nella forma

$$\forall t_1, t_2 \in T.\ D(t_1,t_2) \implies p(t_1,t_2)$$

per un qualche predicato p.

4. *[50%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione <u>associato a D</u>.*

Soluzione (bozza).

Parte 1

Una possibile soluzione è:

$$\dfrac{\dfrac{}{C(1,1)} \qquad \dfrac{\dfrac{}{C(2,1)} \qquad \dfrac{}{C(3,1)}}{C((2,3),2)}}{C((1,(2,3)),3)}$$

$$\dfrac{\dfrac{}{D(1,(1,1))}[D0] \qquad \dfrac{\dfrac{}{D(2,(2,2))}[D0] \qquad \dfrac{}{D(3,(3,3))}[D0]}{D((2,3),((2,2),(3,3)))}[D1]}{D((1,(2,3)),((1,1),((2,2),(3,3))))}[D1]$$

Parte 2

Per dimostrare che $\forall t_1, t_2.\ D(t_1,t_2) \implies p(t_1,t_2)$ basta che:

$$\begin{array}{ll} D0) & \forall n \in \mathbb{N}.\ p(n,(n,n)) \\ D2) & \forall s,s',d,d' \in T.\ p(s,s') \wedge p(d,d') \implies p((s,d),(s',d')) \\ D2) & \forall s,s',d,d' \in T.\ p(s,s') \wedge p(d,d') \implies p((s,d),((s',s'),(d',d'))) \end{array}$$

Parte 3

Basta prendere

$$p(t_1,t_2) :\ \forall k \in \mathbb{N}.\ C(t_2,k) \implies k \text{ pari}$$

Parte 4

Procediamo per induzione su D.

Caso $[D0]$**.** Dobbiamo dimostrare $p(n,(n,n))$, quindi assumiamo $IP1 : C((n,n),k)$ e dimostriamo k pari.

Invertendo $IP1$ notiamo che può essere derivata solo in questo modo:

$$\dfrac{\dfrac{}{C(n,1)}[C0] \quad \dfrac{}{C(n,1)}[C0]}{C((n,n),k=1+1)}[C1]$$

e quindi $k = 2$ è pari.

Caso $[D1]$**.** Assumiamo come ipotesi induttive $IP1 : p(s,s')$ e $IP2 : p(d,d')$, cioè:

$$\begin{array}{c} IP1 : \forall k_1.C(s',k_1) \implies k_1 \text{ pari} \\ IP2 : \forall k_2.C(d',k_2) \implies k_2 \text{ pari} \end{array}$$

e dimostriamo la tesi $p((s,d),(s',d'))$, cioè:

$$\forall k.C((s',d'),k) \implies k \text{ pari}$$

Assumiamo quindi $IP3 : C((s',d'),k)$ e dimostriamo la nuova tesi k pari.

Invertendo $IP3$ notiamo che può essere derivata solo da $[C1]$ e quindi $IP4 : C(s',k_s)$, $IP5 : C(d',k_d)$ e $k = k_s + k_d$ per qualche $k_s, k_d \in \mathbb{N}$.

Usiamo $IP1$ scegliendo $k_1 = k_s$ assieme a $IP4$, e otteniamo k_s pari.

Analogamente, usiamo $IP2$ scegliendo $k_2 = k_d$ assieme a $IP5$, e otteniamo k_d pari.

Osserviamo infine che $k = k_s + k_d$ è somma di due pari e quindi pari.

Caso $[D2]$**.** Le ipotesi induttive sono le stesse del caso precedente: $IP1 : p(s,s')$ e $IP2 : p(d,d')$, e cioè

$$\begin{array}{c} IP1 : \forall k_1.C(s',k_1) \implies k_1 \text{ pari} \\ IP2 : \forall k_2.C(d',k_2) \implies k_2 \text{ pari} \end{array}$$

La tesi invece è $p((s,d),((s',s'),(d',d')))$, e cioè:

$$\forall k.C(((s',s'),(d',d')),k) \implies k \text{ pari}$$

Assumiamo quindi $IP3 : C(((s',s'),(d',d')),k)$ e dimostriamo la nuova tesi k pari.

Invertendo $IP3$ notiamo che può essere derivata solo in questo modo:

$$\dfrac{\dfrac{\dfrac{}{C(s',k_s)} \quad \dfrac{}{C(s',k'_s)}}{C((s',s'),k_s+k'_s)}[C1] \quad \dfrac{\dfrac{}{C(d',k_d)} \quad \dfrac{}{C(d',k'_d)}}{C((d',d'),k_d+k'_d)}[C1]}{C(((s',s'),(d',d')),k=k_s+k'_s+k_d+k'_d)}[C1]$$

Otteniamo quindi quattro ipotesi: $IP4 : C(s',k_s), IP5 : C(s',k'_s), IP6 : C(d',k_d), IP7 : C(d',k'_d)$.

Usiamo $IP1$ scegliendo $k_1 = k_s$ assieme a $IP4$, e otteniamo k_s pari.

Usiamo $IP1$ scegliendo $k_1 = k'_s$ assieme a $IP5$, e otteniamo k'_s pari.

Usiamo $IP2$ scegliendo $k_2 = k_d$ assieme a $IP6$, e otteniamo k_d pari.

Usiamo $IP2$ scegliendo $k_2 = k'_d$ assieme a $IP7$, e otteniamo k'_d pari.

Osserviamo infine che $k = k_s + k'_s + k_d + k'_d$ è somma di quattro numeri pari e quindi è pari.

$\square$

Esercizio 3. *Costruiamo un'estensione di IMP come segue. A ogni variabile x viene non solo associato un valore intero $\sigma(x) \in \mathbb{Z}$ come di consueto, ma anche un addizionale "valore comando" $\theta(x) \in Com$. Questo secondo valore è modificabile tramite un nuovo comando di IMP,* define x as c*, che associa a x il valore comando c come nuovo valore (il* *valore intero di x rimane invariato). Infine, il nuovo comando* exec x *esegue il comando* $\theta(x)$ *associato alla variabile* x. *Per esempio, eseguire*

$$y := 0;\ (\mathsf{define}\ x\ \mathsf{as}\ y := y + 1);\ \mathsf{exec}\ x;\ \mathsf{exec}\ x$$

fa sì che alla fine y valga 2. La nuova semantica dei comandi prende la forma

$$\begin{array}{l}(\to_b) \in \mathcal{P}(Com \times State \times CState \times State \times CState)\\ \langle c, \sigma, \theta\rangle \to_b \langle \sigma', \theta'\rangle\end{array}$$

dove $\theta, \theta' \in CState = (Var \to Com)$.

1. *[50%] Si formalizzi la semantica fornendo opportune regole di inferenza. Si gestiscano i casi relativi a tutti i comandi tranne il* while.

2. *[50%] Si consideri un generico ciclo* $c_1 = (\mathsf{while}\ e \neq 0\ \mathsf{do}\ c)$, *dove* c *non contiene cicli* while *al suo interno. Si descriva come, nell'estensione di IMP considerata, si può costruire un comando* c_2 *quasi equivalente a* c_1 *e privo di* while *al suo interno. Con "quasi equivalente" si intende un comando che ha lo stesso effetto sui valori interi delle variabili* ($\sigma(x)$) *ma non per forza lo stesso effetto sui valori comandi* ($\theta(x)$). *Giustificare informalmente la costruzione.*

Soluzione (bozza).
Parte 1.

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

$$\frac{\langle e, \sigma\rangle \to_e v}{\langle x := e, \sigma, \theta\rangle \to_b \langle \sigma[x \mapsto v], \theta\rangle}[Let]$$

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

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

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

$$\frac{}{\langle \mathsf{define}\ x\ \mathsf{as}\ c, \sigma, \theta\rangle \to_b \langle \sigma, \theta[x \mapsto c]\rangle}[Define]$$

$$\frac{\langle \theta(x), \sigma, \theta\rangle \to_b \langle \sigma', \theta'\rangle}{\langle \mathsf{exec}\ x, \sigma, \theta\rangle \to_b \langle \sigma', \theta'\rangle}[Exec]$$

Parte 2.

Per simulare $c_1 = (\mathsf{while}\ e \neq 0\ \mathsf{do}\ c)$, basta prendere un variabile x che non compare in c_1 e definire:

$$c_2 = (\mathsf{define}\ x\ \mathsf{as}\ (\mathsf{if}\ e \neq 0\ \mathsf{then}\ c; \mathsf{exec}\ x\ \mathsf{else}\ \mathsf{skip})); \mathsf{exec}\ x$$

Eseguendo c_2, $\theta(x)$ rimane invariato dopo la sua definizione. Quando la guardia $e \neq 0$ è vera, eseguiamo $c;$ exec x, quindi il corpo c seguito da $\theta(x)$, e quest'ultimo fa ripetere il ciclo. Quando la guardia diventa falsa usciamo dal ciclo eseguendo skip. □

Nome ______________________________________ Matricola ______________

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

$\{a = A \land b = B\}$

____

$n := 5;$

____

while $n \neq 0$ do

____

____

$n := n - 1;$

____

$c := a;$

____

$a := b;$

____

$b := c;$

____

$\{a = B \land b = A\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$\{a = A \wedge b = B\}$ (1)
$\{(5 \text{ pari} \wedge a = B \wedge b = A) \vee (5 \text{ dispari} \wedge a = A \wedge b = B)\}$
$n := 5;$
$\{INV : (n \text{ pari} \wedge a = B \wedge b = A) \vee (n \text{ dispari} \wedge a = A \wedge b = B)\}$
while $n \neq 0$ do
    $\{INV \wedge n \neq 0\}$ (2)
    $\{(n-1 \text{ pari} \wedge b = B \wedge a = A) \vee (n-1 \text{ dispari} \wedge b = A \wedge a = B)\}$
    $n := n - 1;$
    $\{(n \text{ pari} \wedge b = B \wedge a = A) \vee (n \text{ dispari} \wedge b = A \wedge a = B)\}$
    $c := a;$
    $\{(n \text{ pari} \wedge b = B \wedge c = A) \vee (n \text{ dispari} \wedge b = A \wedge c = B)\}$
    $a := b;$
    $\{(n \text{ pari} \wedge a = B \wedge c = A) \vee (n \text{ dispari} \wedge a = A \wedge c = B)\}$
    $b := c;$
$\{INV \wedge \neg(n \neq 0)\}$ (3)
$\{a = B \wedge b = A\}$

Per le PrePost:

1) Vale la seconda parte dell'OR, visto che 5 è dispari e le equazioni $a = A$ e $b = B$ fanno parte dell'ipotesi.

2) Nella tesi "$n - 1$ pari" è equivalente a "n dispari", e analogamente "$n - 1$ dispari" è equivalente a "n pari". Dopo questa semplificazione, e una semplice commutazione di AND e OR, la tesi diventa uguale a INV che è parte dell'ipotesi.

3) Dall'ipotesi $\neg(n \neq 0)$ si ha $n = 0$ che è pari, quindi dall'ipotesi INV si ricava $a = B \wedge b = A$ che è la tesi.

□