Informatica — 2017-07-24

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

Esercizio 1. *Si forniscano tutte le regole del sistema deduttivo per le triple di Hoare. Dopo, si definisca la nozione di validità per le triple di Hoare. Infine, si enunci, senza dimostrarlo, il teorema di correttezza per tale sistema deduttivo.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme T degli alberi binari di numeri naturali (regole $[T0], [T1]$) e due predicati R, Q su alberi in T, ovvero $R, Q \in \mathcal{P}(T)$ (regole $[R0], [R1], [R2]$ e $[Q0], [Q1], [Q2]$). Sotto, k, n, m indicano naturali mentre t, u indicano alberi.*

$$\frac{}{n}[T0] \qquad \frac{t \quad u}{(t,u)}[T1]$$

$$\frac{}{R(n)}[R0] \qquad \frac{R(t)}{R((n,(t,m)))}[R1] \qquad \frac{R(t)}{R(((n,t),m))}[R2]$$

$$\frac{}{Q(k)}[Q0] \qquad \frac{Q(t)}{Q((k,t))}[Q1] \qquad \frac{Q(t)}{Q((t,k))}[Q2]$$

1. *[20%] Si trovi un albero $t \in T$ con almeno 4 naturali all'interno tale per cui valgano sia $R(t)$ che $Q(t)$, e si giustifichi la risposta esibendo una derivazione per $R(t)$ e una per $Q(t)$.*

2. *[30%] Si enunci il principio di induzione sul predicato R.*

3. *[40%] Si dimostri che $\forall t \in T.\ R(t) \implies Q(t)$.*
   (Suggerimento: si proceda per induzione su $R(t)$.)

4. *[10%] Si trovi un $t \in T$ per cui vale $Q(t)$ ma non vale $R(t)$.*

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

$$\frac{\dfrac{\dfrac{}{R(4)}[R0]}{R((3,(4,5)))}[R1]}{R((1,((3,(4,5)),2)))}[R1] \qquad \frac{\dfrac{\dfrac{\dfrac{}{Q(4)}[Q0]}{Q((4,5))}[Q2]}{Q((3,(4,5)))}[Q1]}{Q(((3,(4,5)),2))}[Q2]}{Q((1,((3,(4,5)),2)))}[Q1]$$

(**Parte 2.**) Sia p un predicato sugli alberi. Per dimostrare che

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

è sufficiente verificare che

$$\begin{array}{ll} R0) & \forall n \in \mathbb{N}.p(n) \\ R1) & \forall n, m \in \mathbb{N}, t \in T.p(t) \implies p((n,(t,m))) \\ R2) & \forall n, m \in \mathbb{N}, t \in T.p(t) \implies p(((n,t),m)) \end{array}$$

(**Parte 3.**)

Basta usare il principio di induzione con $p = Q$.

(Caso [**R0**])

Bisogna dimostrare $Q(n)$. Per farlo, basta usare la regola $[Q0]$.

(Caso [**R1**])

Per ipotesi induttiva, assumiamo $IP1 : Q(t)$. Bisogna dimostrare che vale $Q((n,(t,m)))$.

Da $IP1$ e la regola $[Q2]$, si ricava $Q((t,m))$. Da questo e la regola $[Q1]$, si ricava $Q((n,(t,m)))$ che è la tesi.

(Caso [**R2**])

Per ipotesi induttiva, assumiamo $IP1 : Q(t)$. Bisogna dimostrare che vale $Q(((n,t),m))$.

Da $IP1$ e la regola $[Q1]$, si ricava $Q((n,t))$. Da questo e la regola $[Q1]$, si ricava $Q(((n,t),m))$ che è la tesi.

(**Parte 4.**)

Un esempio è:

$$\dfrac{\dfrac{}{Q(1)}[Q0]}{Q((2,1))}[Q1]$$

Non si ha $R((2,1))$, visto che nessuna regola ha una conseguenza di questa forma. Più in generale, se vale $R(t)$ allora t contiene un numero dispari di naturali all'interno (contando le ripetizioni). Questo segue immediatamente dalle regole di R, per induzione.

□

Esercizio 3. *Sia $U = \mathbb{N}$ e $\mathcal{R}$ un insieme di regole di inferenza su U.*

1. *[20%] Si definisca $\mathcal{R}$ in modo che $\mathsf{fix}(\hat{\mathcal{R}}) = \{5n | n \in \mathbb{N}\}$ (senza dimostrarlo). Si richiede inoltre che in tale definizione di $\mathcal{R}$ non compaiano moltiplicazioni.*

2. *[80%] Si determini se, con la definizione di $\mathcal{R}$ data al punto precedente, vale la seguente proprietà, fornendo una dimostrazione o un controesempio.*

$$\forall X, Y \subseteq \mathbb{N}.\ \hat{\mathcal{R}}(X \cup Y) \subseteq \hat{\mathcal{R}}(X) \cup \hat{\mathcal{R}}(Y)$$

Soluzione (bozza). Una possbile definizione è

$$\dfrac{}{0}[R0] \qquad \dfrac{n}{n+5}[R1]$$

(non è l'unica soluzione)

La proprietà (2) vale. Siano $X, Y \subseteq \mathbb{N}$ arbitrari, e sia $k \in \hat{\mathcal{R}}(X \cup Y)$. Dobbiamo dimostrare la tesi $k \in \hat{\mathcal{R}}(X) \cup \hat{\mathcal{R}}(Y)$.

Siccome $k \in \hat{\mathcal{R}}(X \cup Y)$, abbiamo che 1) $k = 0$ o 2) $k = n + 5$ per qualche $n \in X \cup Y$.

Nel caso 1) $k = 0$, grazie a $[R0]$ si ha $k = 0 \in \hat{\mathcal{R}}(Z)$ per ogni Z da cui la tesi.

Nel caso 2) $k = n + 5$, si ha 2.1) $n \in X$ o 2.2) $n \in Y$. Se 2.1) $n \in X$, allora $k = n + 5 \in \hat{\mathcal{R}}(X)$ per la regola $[R1]$, da cui la tesi. Se invece 2.2) $n \in Y$, si procede in modo analogo.

□

Nome _____ Matricola _____

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

$\{A \geq 0 \wedge B > 0\}$

$x := 0;$

$y := 1;$

$z := 0;$

---

while $x < A$ do

$x := x + 1;$

$z := z + y;$

$y := y * B$

$\{z \cdot (B - 1) = B^A - 1\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

Soluzione (bozza).

$\{A \geq 0 \wedge B > 0\}$ (1)
$\{0 \leq A \wedge 1 = B^0 \wedge 0 \cdot (B-1) = B^0 - 1\}$
$x := 0;$
$\{x \leq A \wedge 1 = B^x \wedge 0 \cdot (B-1) = B^x - 1\}$
$y := 1;$
$\{x \leq A \wedge y = B^x \wedge 0 \cdot (B-1) = B^x - 1\}$
$z := 0;$
$\{INV: \ x \leq A \wedge y = B^x \wedge z \cdot (B-1) = B^x - 1\}$
while $x < A$ do
    $\{INV \wedge x < A\}$ (2)
    $\{x + 1 \leq A \wedge yB = B^{x+1} \wedge (z+y) \cdot (B-1) = B^{x+1} - 1\}$
    $x := x + 1;$
    $\{x \leq A \wedge yB = B^x \wedge (z+y) \cdot (B-1) = B^x - 1\}$
    $z := z + y;$
    $\{x \leq A \wedge yB = B^x \wedge z \cdot (B-1) = B^x - 1\}$
    $y := y * B$
$\{INV \wedge \neg(x < A)\}$ (3)
$\{z \cdot (B-1) = B^A - 1\}$

Per le PrePost:
1) Banale aritmetica.
2) Da $x < A$, visto che lavoriamo sugli interi, otteniamo $x + 1 \leq A$. La parte $yB = B^{x+1}$ si ottiene dall'invariante $y = B^x$. Per il resto, si ha:

$$(z+y)(B-1) = z(B-1) + y(B-1) \stackrel{*}{=} B^x - 1 + B^x(B-1) = B^{x+1} - 1$$

dove per $\stackrel{*}{=}$ abbiamo usato l'invariante $z \cdot (B-1) = B^x - 1$.
3) Dall'invariante $x \geq A$ e da $\neg(x < A)$ si ricava $x = A$. Usando questo e l'invariante otteniamo $z \cdot (B-1) = B^x - 1 = B^A - 1$.

□