Informatica — 2017-09-11

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

Esercizio 1. *Si descriva, in modo conciso e senza formalizzarla, la nozione di complessità computazionale asintotica. Dopo, si fornisca un esempio semplice di algoritmo con relativa complessità asintotica, giustificandola in modo informale.*

Esercizio 2. *Le seguenti regole definiscono induttivamente l'insieme S delle sequenze finite di numeri naturali (regole $[S0], [S1]$) e una relazione $R \in \mathcal{P}(S \times \mathbb{N} \times S)$ (regole $[R0], [R1]$). Sotto, k, n indicano naturali mentre s, t indicano sequenze in S.*

$$\frac{}{\epsilon}[S0] \quad \frac{s}{n : s}[S1] \qquad \frac{}{R(\epsilon, k, \epsilon)}[R0] \quad \frac{R(s, k, t)}{R(n : s, k, kn : t)}[R1]$$

1. *[20%] Sia $s = 1 : 2 : 3 : 4 : \epsilon$. Si fornisca una sequenza t tale per cui valga $R(s, 5, t)$ e si giustifichi la risposta esibendo una derivazione.*
2. *[20%] Si enunci il principio di induzione associato alla relazione R.*
3. *[20%] Si consideri l'enunciato seguente:*

   $$\forall s, t, u \in S. \forall a, b \in \mathbb{N}.\ R(s, a, t) \wedge R(t, b, u) \implies R(s, ab, u)$$

   Si definisca un predicato $p(s, a, t)$ in modo tale che l'enunciato si possa riscrivere in modo equivalente a quanto segue.

   $$\forall s, t \in S. \forall a \in \mathbb{N}.\ R(s, a, t) \implies p(s, a, t)$$

4. *[40%] Si concluda la dimostrazione dell'enunciato visto sopra usando il principio di induzione associato ad R.*

Soluzione (bozza).
(Parte 1).

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{R(\epsilon, 5, \epsilon)}[R0]}{R(3 : \epsilon, 5, 15 : \epsilon)}[R1]}{R(2 : 3 : \epsilon, 5, 10 : 15 : \epsilon)}[R1]}{R(1 : 2 : 3 : \epsilon, 5, 5 : 10 : 15 : \epsilon)}[R1]}{R(1 : 2 : 3 : 4 : \epsilon, 5, 5 : 10 : 15 : 20 : \epsilon)}[R1]$$

(Parte 2).

Sia $p(s, n, t)$ un predicato $p \in \mathcal{P}(S \times \mathbb{N} \times S)$. Per dimostrare $\forall s, n, t.\ R(s, n, t) \implies p(s, n, t)$ è sufficiente dimostrare che

$R0)$ $\forall k \in \mathbb{N}.\ p(\epsilon, k, \epsilon)$
$R1)$ $\forall s, t \in S. \forall n, k \in \mathbb{N}.\ p(s, k, t) \implies p(n : s, k, kn : t)$

(Parte 3).

È sufficiente riscrivere la formula come segue

$$\forall s,t \in S. \forall a \in \mathbb{N}.\ R(s,a,t) \implies (\forall u \in S. \forall b \in \mathbb{N}.\ R(t,b,u) \implies R(s,ab,u))$$

e quindi definire di conseguenza

$$p(s,a,t) : \forall u \in S. \forall b \in \mathbb{N}.\ R(t,b,u) \implies R(s,ab,u)$$

(Parte 4). Procediamo quindi usando il principio di induzione su R, usando il predicato p.

(Caso R0)

Dobbiamo dimostrare $p(\epsilon,k,\epsilon)$, ovvero che

$$\forall u \in S. \forall b \in \mathbb{N}.\ R(\epsilon,b,u) \implies R(\epsilon,kb,u)$$

Assumiamo $IP1 : R(\epsilon,b,u)$ e dimostriamo la nuova tesi $R(\epsilon,kb,u)$.

Invertendo $IP1$, siccome è derivabile solo con la regola $[R0]$, otteniamo $u = \epsilon$. La tesi diventa $R(\epsilon,kb,\epsilon)$, che segue da $[R0]$.

(Caso R1)

Per ipotesi induttiva assumiamo $IP1 : p(s,k,t)$, ovvero che:

$$\forall u \in S. \forall b \in \mathbb{N}.\ R(t,b,u) \implies R(s,kb,u)$$

e dimostriamo la tesi $p(n : s, k, kn : t)$ ovvero che:

$$\forall u \in S. \forall b \in \mathbb{N}.\ R(kn : t,b,u) \implies R(n : s,kb,u)$$

Assumiamo l'ipotesi $IP2 : R(kn : t, b, u)$ e dimostriamo la nuova tesi $R(n : s, kb, u)$.

Invertendo $IP2$, siccome è derivabile solo con la regola $[R1]$, otteniamo $u = bkn : \bar{u}$ per qualche sequenza $\bar{u}$, dove $IP3 : R(t,b,\bar{u})$.

Da IP1, scegliendo $u = \bar{u}, b = b$, ricaviamo che

$$R(t,b,\bar{u}) \implies R(s,kb,\bar{u})$$

Siccome l'antecedente è proprio $IP3$, otteniamo $IP4 : R(s,kb,\bar{u})$. Da questa, usando $[R1]$, ricaviamo $R(n : s, kb, kbn : \bar{u})$, da cui riscrivendo $kbn : \bar{u} = bkn : \bar{u} = u$ otteniamo la tesi $R(n : s, kb, u)$.

$\square$

Esercizio 3. *Si consideri la seguente proprietà sulla validità ($\models$) delle triple di Hoare.*

$$\models \{P_1\}\ c\ \{Q_1\} \wedge \models \{P_2\}\ c\ \{Q_2\} \implies \models \{P_1 \vee P_2\}\ c\ \{Q_1 \vee Q_2\}$$

Si stabilisca se tale proprietà è vera per ogni comando (c) e pre-/post-condizione (P_1, P_2, Q_1, Q_2). La si dimostri, se è vera, e si fornisca un controesempio altrimenti.

(Suggerimento: si sfrutti il fatto che $\sigma \models (P \wedge Q)$ è equivalente a $(\sigma \models P) \wedge (\sigma \models Q)$, mentre $\sigma \models (P \vee Q)$ è equivalente a $(\sigma \models P) \vee (\sigma \models Q)$.)

Soluzione (bozza).
La proprietà vale.
Per ipotesi si ha, per ogni σ, σ',

$$\begin{array}{l} IP1: \ \sigma \models P_1 \wedge \langle c, \sigma \rangle \to_b \sigma' \implies \sigma' \models Q_1 \\ IP2: \ \sigma \models P_2 \wedge \langle c, \sigma \rangle \to_b \sigma' \implies \sigma' \models Q_2 \end{array}$$

Per dimostrare la tesi, assumiamo

$$\begin{array}{l} IP3: \ \sigma \models P_1 \vee P_2 \\ IP4: \ \langle c, \sigma \rangle \to_b \sigma' \end{array}$$

e facciamo vedere che vale $\sigma' \models Q_1 \vee Q_2$.

Usando $IP3$, otteniamo che $\sigma \models P_1$ oppure $\sigma \models P_2$. Consideriamo ambo i casi.

Caso 1. Se vale $\sigma \models P_1$, usando $IP4$ e $IP1$, ricaviamo $\sigma' \models Q_1$, da cui $\sigma' \models Q_1 \vee Q_2$.

Caso 2. Analogamente, se vale $\sigma \models P_2$, usando $IP4$ e $IP2$, ricaviamo $\sigma' \models Q_2$, da cui $\sigma' \models Q_1 \vee Q_2$.

In entrambi i casi, otteniamo la tesi $\sigma' \models Q_1 \vee Q_2$. $\square$

Nome ______________________________ Matricola ____________

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

$\{x = 2^K \wedge K \geq 0\}$

____

$y := 0;$

____

while $x \neq 1$ do

____

____

if x *pari* then

____

____

$x := \lfloor x/2 \rfloor;$

____

$y := y + 1$

else

____

____

$x := 0$

____

$\{y = K\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

Soluzione (bozza).

$$
\begin{array}{l}
\{x = 2^K\} \\
\{x = 2^{K-0}\}\ (1) \\
y := 0; \\
\{INV : x = 2^{K-y}\} \\
\textsf{while } x \neq 1 \textsf{ do} \\
\quad \{INV \wedge x \neq 1\} \\
\quad \textsf{if } x \text{ pari } \textsf{then} \\
\quad\quad \{INV \wedge x \neq 1 \wedge x \text{ pari}\} \\
\quad\quad \{\lfloor x/2 \rfloor = 2^{K-(y+1)}\}\ (2) \\
\quad\quad x := \lfloor x/2 \rfloor; \\
\quad\quad \{x = 2^{K-(y+1)}\} \\
\quad\quad y := y + 1 \\
\quad \textsf{else} \\
\quad\quad \{INV \wedge x \neq 1 \wedge \neg(x \text{ pari})\} \\
\quad\quad \{0 = 2^{K-y}\}\ (3) \\
\quad\quad x := 0 \\
\{INV \wedge \neg(x \neq 1)\} \\
\{y = K\}\ (4)
\end{array}
$$

Per le PrePost:

1) Banale aritmetica.

2) Per INV, $x = 2^{K-y}$ e dividendo per 2 ambo i lati (che sono pari) otteniamo $\lfloor x/2 \rfloor = x/2 = 2^{K-y-1} = 2^{K-(y+1)}$.

3) Dall'ipotesi si ricava un assurdo, da cui la tesi. Infatti, l'intero $x = 2^{K-y}$ non può essere diverso da 1 e non pari.

4) Per ipotesi $x = 1$, e quindi per INV si ha $x = 1 = 2^{K-y}$, da cui la tesi $y = K$.

$\square$