Informatica — 2015-02-02

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

Esercizio 1. *Si consideri la relazione $\to_s$ della semantica small step. La si descriva chiarendo su quali elementi è definita ($(\to_s) \in \mathcal{P}(\ldots)$) e fornendone le regole di inferenza per tutti i comandi di IMP (tranne l'*if*). Dopo, si definisca la nozione di complessità computazionale.*

Esercizio 2. *Sia $U = \mathbb{R}$, e $f : \mathcal{P}(U) \to \mathcal{P}(U)$ la funzione*

$$f(X) = \{0\} \cup \{x + 1 \mid x \in X\}$$

(Sotto, il peso di ogni domanda è dato in parentesi.)

1. *[10%] Si dimostri che f è continua secondo Scott.*
2. *[5%] Qual è il minimo punto fisso A di f? (Non si chiede di giustificarne la risposta)*
3. *[5%] Si costruisca un punto fisso B di f tale che $B \neq A$. Si giustifichi brevemente la risposta.*
4. *[80%] Si costruisca un insieme C tale che $f(C) \subset C$ (si noti l'inclusione stretta). Si giustifichi brevemente la risposta.*

Soluzione (bozza).

1) La continutità deriva direttamente osservando che $f = \hat{\mathcal{R}}$ dove $\mathcal{R}$ è definito come segue

$$\frac{}{0} \qquad \frac{x}{x+1}$$

e sfruttando la contnuità di $\hat{\mathcal{R}}$.

2) $A = \mathbb{N}$

3) $B = \mathbb{Z}$ (ma anche $\mathbb{Q}, \mathbb{R}$ e tanti altri). La funzione f li "trasla" a destra e aggiunge lo zero, e nessuna di queste due cose altera $\mathbb{Z}$.

4) Per esempio, $C = \mathbb{N} \cup \{n + 1/2 \mid n \in \mathbb{N}\}$, in quanto

$$f(C) = \mathbb{N} \cup \{n + 1/2 \mid 0 \neq n \in \mathbb{N}\} = C \setminus \{1/2\}$$

Alternativamente, $C = \mathbb{N} \cup \{-1\}$ funziona: $f(C) = \mathbb{N} \subset C$. □

Esercizio 3. *Sia $p \in \mathcal{P}(Var \times Com)$ il predicato definito induttivamente da:*

$$\frac{}{p(x, \mathsf{skip})}[S] \qquad \frac{y \neq x}{p(x, y := e)}[L] \qquad \frac{p(x, c_1) \qquad p(x, c_2)}{p(x, c_1; c_2)}[C]$$

$$\frac{p(x, c_1) \qquad p(x, c_2)}{p(x, \mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2)}[I] \qquad \frac{p(x, c)}{p(x, \mathsf{while}\ e \neq 0\ \mathsf{do}\ c)}[W]$$

1. *[10%] Si descriva p informalmente:*
   $p(x, c)$ *vale se e solo se all'interno di c ...*

2. *[90%] Sia* $q \in \mathcal{P}(Var \times Com)$ *definito come segue:*

$$q(x, c): \qquad \forall \sigma, \sigma'.\ \langle c, \sigma \rangle \to_b \sigma' \implies \sigma(x) = \sigma'(x)$$

   Si dimostri formalmente per induzione che $p \subseteq q$*. (Per brevità, si ignorino le regole* C, W*)*

Soluzione (bozza). 1) $p(x, c)$ vale se e solo se dentro c non si assegna mai alla variabile x.
2) $q(x, c)$ dice che la variabile x non cambia valore dopo avere eseguito c. Intuitivamente, se vale $p(x, c)$ non ci sono assegnamenti ad x che possono cambiarne il valore, e quindi $q(x, c)$ vale.

Per dimostrare $p \subseteq q$, usiamo il principio di induzione. Basta fare vedere che $\hat{\mathcal{R}}(q) \subseteq q$. Verifichiamolo, limitandoci ai casi richiesti S, L, I.

Caso S. Qui non abbiamo ipotesi induttive. Dobbiamo fare vedere che $q(x, \mathsf{skip})$. Supponiamo quindi che $\langle \mathsf{skip}, \sigma \rangle \to_b \sigma'$. Questo può essere derivabile solo con la regola *Skip*, che richiede $\sigma' = \sigma$. In tal caso, otteniamo direttamente la tesi $\sigma(x) = \sigma'(x)$.

Caso L. Qui non abbiamo ipotesi induttive, ma possiamo assumere la condizione a lato $y \neq x$. Dobbiamo fare vedere che $q(x, y := e)$. Supponiamo quindi che $\langle y := e, \sigma \rangle \to_b \sigma'$. Questo può essere derivabile solo con la regola *Let*, che richiede $\sigma' = \sigma[y \mapsto v]$, dove v è tale che $\langle e, \sigma \rangle \to_e v$. Cioè:

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

Avendo capito cosa è σ', ricaviamo la tesi:

$$\sigma'(x) = \sigma[y \mapsto v](x) = \sigma(x)$$

dove l'ultima equazione vale perché $y \neq x$.

Caso I. Qui abbiamo come ipotesi induttive $q(x, c_1)$ e $q(x, c_2)$. Chiamiamo c il comando $\mathsf{if}\ e \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2$). Dobbiamo fare vedere che $q(x, c)$. Supponiamo quindi che $\langle c, \sigma \rangle \to_b \sigma'$. Questo può essere derivabile con due regole: $If - true, If - False$. Facciamo due sottocasi:

Sottocaso $If - true$. Si ha:

$$\frac{\langle e, \sigma \rangle \to_b v \neq 0 \qquad \langle c_1, \sigma \rangle \to_b \sigma'}{\langle c, \sigma \rangle \to_b \sigma'}$$

Da $\langle c_1, \sigma \rangle \to_b \sigma'$ e dall'ipotesi induttiva $q(x, c_1)$, otteniamo direttamente la tesi $\sigma(x) = \sigma'(x)$.

Sottocaso $If - false$. (Completamente analogo al precedente, si può traquillamente omettere dicendo appunto che è analogo.)

Si ha:

$$\frac{\langle e, \sigma \rangle \to_b 0 \qquad \langle c_2, \sigma \rangle \to_b \sigma'}{\langle c, \sigma \rangle \to_b \sigma'}$$

Da $\langle c_2, \sigma \rangle \to_b \sigma'$ e dall'ipotesi induttiva $q(x, c_2)$, otteniamo direttamente la tesi $\sigma(x) = \sigma'(x)$.

$\square$

Nome ______________________________ Matricola ____________

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

$\{x = 0 \wedge f = 1\}$

____

while $f \neq 0$ do

____

____

if $x \cdot x = n$ then

____

____

$f := 0$

else

____

____

$x := x + 1$

____

____

$\{x^2 = n\}$

Giustificare qui sotto tutti gli usi della regola $PrePost$.

____

____

____

____

____

____

____

____

Soluzione (bozza).

$$
\begin{array}{l}
\{x = 0 \wedge f = 1\} \\
\{INV : f = 0 \implies x^2 = n\} \quad (1) \\
\textsf{while } f \neq 0 \textsf{ do} \\
\quad \{INV \wedge f \neq 0\} \\
\quad \textsf{if } x \cdot x = n \textsf{ then} \\
\quad\quad \{INV \wedge f \neq 0 \wedge x \cdot x = n\} \\
\quad\quad \{0 = 0 \implies x^2 = n\} \quad (2) \\
\quad\quad f := 0 \\
\quad \textsf{else} \\
\quad\quad \{INV \wedge f \neq 0 \wedge x \cdot x \neq n\} \\
\quad\quad \{f = 0 \implies (x+1)^2 = n\} \quad (3) \\
\quad\quad x := x + 1 \\
\quad \{INV\} \\
\{INV \wedge f = 0\} \\
\{x^2 = n\} \quad (4)
\end{array}
$$

Per le PrePost:
1) Per ipotesi $f = 1$, quindi $f = 0$ è falso e implica qualunque cosa.
2) La tesi $0 = 0 \implies x^2 = n$ si riscrive come $x^2 = n$, che è implicato dall'ipotesi $x \cdot x = n$.
3) Per ipotesi $f \neq 0$, quindi $f = 0$ implica ogni cosa.
4) Abbiamo $f = 0$ che è proprio l'ipotesi dell'invariante, da cui la tesi dell'invariante $x^2 = n$.

$\square$