Informatica — 2015-06-22

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

Esercizio 1. *Si forniscano le regole* $[Comp]$, $[Let]$ *e* $[If - True]$ *della semantica big-step* $(\rightarrow_b)$*, commentandole brevemente.*

Esercizio 2. *Sia* $D \subseteq \mathcal{P}(\mathbb{N})$ *l'insieme degli insiemi* X *di naturali con al massimo due elementi (* $D = \{X \subseteq \mathbb{N} \mid \nexists a, b, c \in X.\ a \neq b \neq c \neq a\}$*). Sia inoltre* $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ *definita da*

$$f(X) = \begin{cases} X \cup \{1\} & X \in D \\ X \cup \{1, 2\} & X \notin D \end{cases}$$

Si stabilisca <u>se</u> f *è continua secondo Scott, giustificando la risposta. (Suggerimento: se* $\bigcup_i X_i \in D$ *..., altrimenti ...)*

Soluzione (bozza). Sia $\{X_i\}_{i \in \mathbb{N}}$ una successione crescente di insiemi.

Caso 1 Se $\bigcup_i X_i$ contiene al massimo due elementi, allora ogni singolo X_i ne contiene al massimo due. Quindi:

$$\bigcup_i f(X_i) = \bigcup_i (X_i \cup \{1\}) = (\bigcup_i X_i) \cup \{1\} = f(\bigcup_i X_i)$$

Caso 2 Se $\bigcup_i X_i$ contiene più di due elementi, siccome la successione è crescente, deve esistere un $k \in \mathbb{N}$ tale che, quando $i \geq k$, X_i ha più di due elementi, mentre quando $i < k$ l'insieme X_i ne ha al massimo due. Quindi:

$$\begin{aligned} & \textstyle\bigcup_i f(X_i) = \bigcup_{i<k} f(X_i) \cup \bigcup_{i \geq k} f(X_i) \\ = \ & \textstyle\bigcup_{i<k} (X_i \cup \{1\}) \cup \bigcup_{i \geq k} (X_i \cup \{1, 2\}) \end{aligned}$$

Siccome ogni insieme della prima unione è incluso in $X_k \cup \{1, 2\}$, possiamo continuare con:

$$\begin{aligned} \ldots = \ & \textstyle\bigcup_{i<k} (X_i \cup \{1\}) \cup \bigcup_{i \geq k} (X_i \cup \{1, 2\}) = \bigcup_{i \geq k} (X_i \cup \{1, 2\}) \\ = \ & \textstyle(\bigcup_{i \geq k} X_i) \cup \{1, 2\} = f(\bigcup_{i \geq k} X_i) = f(\bigcup_i X_i) \end{aligned}$$

dove l'ultimo passaggio si deve al fatto che la successione è crescente.

Concludendo, f è continua. □

Esercizio 3. *Sia Pos l'insieme degli stati con valori non negativi, ovvero* $Pos = \{\sigma \in Store \mid \forall x \in Var.\ \sigma(x) \geq 0\}$. *Sia p la proprietà sui comandi di IMP definita come segue*

$$p(c): \qquad \forall \sigma, \sigma'.\ (\sigma \in Pos\ \wedge\ \langle c, \sigma\rangle \to_b \sigma')\ \Longrightarrow\ \sigma' \in Pos$$

1. *[10%] Si descriva informalmente la proprietà p.*

Si vuole definire induttivamente un sottoinsieme IMP^- *dei comandi di IMP che soddisfano la proprietà p di sopra. Una possibile definizione di* IMP^- *è data dalle regole seguenti.*

$$\frac{}{x := e * e}[L1] \qquad \frac{}{x := x + n}(n \geq 0)[L2]$$

$$\frac{c_1 \qquad c_2}{c_1; c_2}[C] \qquad \frac{c_1}{\mathsf{if}\ x + 1 \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2}[I]$$

2. *[75%] Si dimostri per induzione che ogni comando di* IMP^- *soddisfa effettivamente la proprietà p.*

3. *[15%] Si aggiunga alle regole di sopra una regola generale per il* while *in modo da includere dentro* IMP^- *anche il comando*

$$\mathsf{while}\ x - y \neq 0\ \mathsf{do}\ (y := y * y; z := z + 4)$$

Giustificare brevemente ed informalmente la regola aggiunta.

Soluzione (bozza).

Parte 1 Sono programmi che "preservano la non-negatività dello stato". Ovvero, se eseguiti in stati senza valori negativi in alcuna variabile, producono stati che ancora soddisfano la stessa proprietà.

Parte 2

Caso $[L1]$ Se $\sigma \in Pos$ e $\langle x := e * e, \sigma\rangle \to_b \sigma'$, posso invertire la derivazione ed avere

$$\frac{\dfrac{\langle e, \sigma\rangle \to_e z_1 \qquad \langle e, \sigma\rangle \to_e z_2}{\langle e * e, \sigma\rangle \to_e z_1 \cdot z_2 = z}}{\langle x := e * e, \sigma\rangle \to_b \sigma' = \sigma[x \mapsto z]}$$

Per il determinismo di $\to_e$, $z_1 = z_2$ e quindi $z = (z_1)^2 \geq 0$. Quindi $\sigma' \in Pos$.

Caso $[L2]$ Sia $n > 0$ come da condizione a lato. Devo dimostrare che se $\sigma \in Pos$ e $\langle x := x + n, \sigma\rangle \to_b \sigma'$, allora $\sigma' \in Pos$. Invertendo la derivazione si ha

$$\dfrac{\dfrac{\langle x, \sigma\rangle \to_e \sigma(x) \qquad \langle n, \sigma\rangle \to_e n}{\langle x + n, \sigma\rangle \to_e \sigma(x) + n}}{\langle x := x + n, \sigma\rangle \to_b \sigma' = \sigma[x \mapsto \sigma(x) + n]}$$

Siccome $\sigma(x) \geq 0$ per ipotesi, e $n \geq 0$, abbiamo che $\sigma' \in Pos$.

Caso $[C]$ Assumiamo come ipotesi induttive $p(c_1)$ e $p(c_2)$. Dobbiamo dimostrare che se $\sigma \in Pos$ e $\langle c_1; c_2, \sigma\rangle \to_b \sigma'$, allora $\sigma' \in Pos$. Invertendo la derivazione si ha

$$\dfrac{\langle c_1, \sigma\rangle \to_b \sigma'' \qquad \langle c_2, \sigma''\rangle \to_b \sigma'}{\langle c_1; c_2, \sigma\rangle \to_b \sigma'}$$

Da $\sigma \in Pos$, $\langle c_1, \sigma\rangle \to_b \sigma''$ e $p(c_1)$ (su σ, σ'') abbiamo che $\sigma'' \in Pos$. Da ciò, $\langle c_2, \sigma''\rangle \to_b \sigma'$ e $p(c_2)$ (su σ'', σ') abbiamo che $\sigma' \in Pos$, che è la tesi.

Caso $[I]$ Assumiamo come ipotesi induttiva $p(c_1)$. Dobbiamo dimostrare che se $\sigma \in Pos$ e $\langle \mathsf{if}\ x + 1 \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \to_b \sigma'$, allora $\sigma' \in Pos$. Invertendo la derivazione si hanno due casi.

Caso 1.

$$\dfrac{\langle x + 1, \sigma\rangle \to_e v \neq 0 \qquad \langle c_1, \sigma\rangle \to_b \sigma'}{\langle \mathsf{if}\ x + 1 \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \to_b \sigma'}[If - True]$$

Da $\sigma \in Pos$, $\langle c_1, \sigma\rangle \to_b \sigma'$ e $p(c_1)$ abbiamo che $\sigma' \in Pos$, che è la tesi.

Caso 2.

$$\dfrac{\dfrac{\langle x, \sigma\rangle \to_e \sigma(x) \qquad \langle 1, \sigma\rangle \to_e 1}{\langle x + 1, \sigma\rangle \to_e 0 = \sigma(x) + 1} \qquad \langle c_2, \sigma\rangle \to_b \sigma'}{\langle \mathsf{if}\ x + 1 \neq 0\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2, \sigma\rangle \to_b \sigma'}[If - False]$$

Da $\sigma \in Pos$, si ha $\sigma(x) + 1 \leq 1 > 0$, che contraddice $\sigma(x) + 1 = 0$. Quindi il caso $If - False$ è in realtà impossibile.

Parte 3

$$\dfrac{c}{\mathsf{while}\ e \neq 0\ \mathsf{do}\ c}$$

Anche se c viene eseguito un numero imprecisato di volte, preserverá comunque lo stato in Pos. □

Nome _____ Matricola _____

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

$\{n \geq 0\}$

$x := 0;$

---

while $x < n$ do

$x := x + 1;$

---

if $x \leq n - 3$ then

$x := x + 3$

else

---

skip

$\{x = n\}$

Giustificare qui sotto eventuali usi della regola *PrePost*.

Soluzione (bozza).

$\{n \geq 0\}$
$\{0 \leq n\}$ (1)
$x := 0;$
$\{INV : x \leq n\}$
while $x < n$ do
    $\{INV \wedge x < n\}$
    $\{x + 1 \leq n\}$ (2)
    $x := x + 1;$
    $\{x \leq n\}$
    if $x \leq n - 3$ then
        $\{x \leq n \wedge x \leq n - 3\}$
        $\{x + 3 \leq n\}$ (3)
        $x := x + 3$
    else
        $\{x \leq n \wedge x > n - 3\}$
        $\{INV\}$ (4)
        skip
$\{INV \wedge x \geq n\}$
$\{x = n\}$ (5)

Per le PrePost:
1) banale.
2) $x + 1 \leq n$ deriva da $x < n$, siccome si tratta di interi.
3) $x + 3 \leq n$ deriva da $x \leq n - 3$ per aritmetica.
4) La tesi è contenuta nelle ipotesi.
5) $x = n$ segue da $x \leq n$ (INV) e $x \geq n$.

□