Informatica — 2016-06-20

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

Esercizio 1. *Si dimostri il teorema del punto fisso di Kleene.*

Esercizio 2. *Sia $g : \mathbb{N}^2 \to \mathbb{N}$ una funzione fissata, e si considerino le regole*

$$\frac{-}{\epsilon}\,[S0] \qquad \frac{s}{n : s}\,[S1] \qquad \frac{}{\mathsf{app}(\epsilon, t, t)}\,[A0] \qquad \frac{\mathsf{app}(s,\ t,\ u)}{\mathsf{app}((i : s), t, (i : u))}\,[A1]$$

$$\frac{}{f(i, \epsilon, i)}\,[F0] \qquad \frac{f(i,\ s,\ k)}{f(i,\ (j : s),\ g(j, k))}\,[F1]$$

Sopra, n, i, j, k sono naturali. Con s, t, u si indicano sequenze finite di naturali, il cui insieme S è definito (induttivamente) da $[S0, S1]$. La relazione $\mathsf{app} \in \mathcal{P}(S \times S \times S)$, definita da $[A0, A1]$ vale tra (s, t, u) quando u si ottiene concatenando le sequenze s e t. La relazione $f \in \mathcal{P}(\mathbb{N} \times S \times \mathbb{N})$ è definita da $[F0, F1]$.

1. *[20%] Si enunci il principio di induzione su S.*
2. *[80%] Sia p la seguente proprietà sulle sequenze $s \in S$*

   $$p(s) :\ \forall i, j, k \in \mathbb{N}, t, u \in S.\ \mathsf{app}(s, t, u) \wedge f(i, t, j) \wedge f(j, s, k) \implies f(i, u, k)$$

   Si dimostri $\forall s \in S.\ p(s)$ per induzione su s.

Soluzione (bozza).
Parte 1.

Se valgono

$$\begin{array}{l} 1)\ p(\epsilon) \\ 2)\ \forall n \in \mathbb{N}, s.\ p(s) \implies p((n : s)) \end{array}$$

allora vale $\forall s \in S.\ p(s)$.

Parte 2.

Caso [S0]. Dobbiamo dimostrare $p(\epsilon)$,

$$\forall i, j, k \in \mathbb{N}, t, u \in S.$$

Assumiamo quindi $\mathsf{app}(\epsilon, t, u)$, $f(i, t, j)$ e $f(j, \epsilon, k)$ e andiamo a dimostrare $f(i, u, k)$. Invertendo $\mathsf{app}(\epsilon, t, u)$, notiamo che solo la regola [A0] pu derivarlo, e quindi si deve avere $t = u$. Invertendo $f(j, \epsilon, k)$, notiamo che solo la regola [F0] pu derivarlo, e quindi si deve avere $j = k$. Dall'ipotesi $f(i, t, j)$, sostituendo le uguaglianze appena ricavate, otteniamo la tesi $f(i, u, k)$.

Caso [S1]. Per ipotesi induttiva, assumiamo $IP1 : p(s)$. Dobbiamo dimostrare $p(n : s)$: per farlo assumiamo $IP2 : \mathsf{app}((n : s), t, u)$, $IP3 :\ f(i, t, j)$ e $IP4 :\ f(j, (n : s), k)$ e ricaviamo $f(i, u, k)$.

Invertendo $IP2$, notiamo che solo la regola [A1] può derivarlo, e quindi si deve avere $IP5 : \mathsf{app}(s, t, \bar{u})$ e $u = (n : \bar{u})$ per un qualche $\bar{u}$.

Invertendo $IP4$, notiamo che solo la regola [F1] può derivarlo, e quindi si deve avere $IP6 : f(j, s, \bar{k})$ e $k = g(n, \bar{k})$ per un qualche $\bar{k}$.

Usiamo l'ipotesi induttiva $IP1 : p(s)$. Questa è una formula quantificata da $\forall i, j, k, t, u$, che scegliamo come segue: $i = i, j = j, k = \bar{k}, t = t, u = \bar{u}$. Dopo tale scelta, si ha

$$\mathsf{app}(s, t, \bar{u}) \wedge f(i, t, j) \wedge f(j, s, \bar{k}) \implies f(i, \bar{u}, \bar{k})$$

L'antecedente sopra segue direttamente da $IP5, IP3, IP6$. Quindi otteniamo $IP7 : f(i, \bar{u}, \bar{k})$.

Possiamo quindi usare [F1] da $IP7$

$$\frac{f(i, \bar{u}, \bar{k})}{f(i, (n : \bar{u}), g(n, \bar{k}))}[F1]$$

da cui otteniamo $IP8 :\ \ f(i, (n : \bar{u}), g(n, \bar{k}))$. La tesi $f(i, u, k)$ segue da $IP8$ e dalle uguaglianze ricavate prima $u = (n : \bar{u}), k = g(n, \bar{k})$.

$\square$

Esercizio 3. *Si estenda IMP con il comando (dove $1 \leq n \in \mathbb{N}$)*

$$\mathsf{dloop}\ e \neq 0\ \mathsf{do}\ c$$

avente la seguente semantica intuitiva. Se all'inizio e risulta uguale a zero, dloop *termina senza effetti. Altrimenti, si esegue c una volta e si ricontrolla e. Se e è zero, ci si ferma. Altrimenti, si esegue c due volte e si ricontrolla e. Se e è zero, ci si ferma, altrimenti si procede ad eseguire c quattro (poi otto, ecc. volte, raddoppiando ad ogni iterazione), fino a quando e si azzera.*

1. *[75%] Si formalizzi la semantica big-step $\to_b$ del* dloop *con opportune regole di inferenza.*

2. *[25%] Sia $c =$ (while $e \neq 0$ do $\bar{c}$) un generico comando* while *in IMP, dove $\bar{c}$ non contiene altri* while *al suo interno. Sia $IMPD$ il linguaggio ottenuto da IMP rimuovendo il* while *e aggiungendo il* dloop*. Si definisca un comando d di $IMPD$ equivalente a c.*

Soluzione (bozza).
Parte 1.

$$\frac{\langle e\ ,\ \sigma\rangle \rightarrow_e 0}{\langle \mathsf{dloop}\ e \neq 0\ \mathsf{do}\ c\ ,\ \sigma\rangle \rightarrow_b \sigma}[DL - False]$$

$$\frac{\langle e,\ \sigma\rangle \rightarrow_e v \neq 0 \qquad \langle c; \mathsf{dloop}\ e \neq 0\ \mathsf{do}\ (c;c)\ ,\ \sigma\rangle \rightarrow_b \sigma}{\langle \mathsf{dloop}\ e \neq 0\ \mathsf{do}\ c\ ,\ \sigma\rangle \rightarrow_b \sigma}[DL - True]$$

Praticamente è uguale al while, salvo che il comando c viene "raddoppiato" in $c; c$ ogni volta che si usa la $[DL - True]$.

Parte 2.

$$
\begin{array}{l}
\mathsf{dloop}\ e \neq 0\ \mathsf{do} \\
\quad \mathsf{if}\ e \neq 0\ \mathsf{then} \\
\quad\quad \bar{c} \\
\quad \mathsf{else} \\
\quad\quad \mathsf{skip}
\end{array}
$$

In questo modo, anche se l'if viene "raddopiato" ad ogni iterazione del ciclo, il comando $\bar{c}$ viene eseguito solo il numero di volte che servono per rendere e uguale a zero.

$\square$

Nome ________________________________ Matricola ____________

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

$\{x = X \wedge N \geq 0\}$

____

$n := 0;$

____

while $n < 2 \cdot N$ do

____

____

$n := n + 1;$

____

$x := 10 - x;$

____

$\{x = X\}$

Giustificare qui sotto eventuali usi della regola $PrePost$.

____

____

____

____

____

____

____

____

____

____

Soluzione (bozza).

$\{x = X \wedge N \geq 0\}$
$\{INV: \; x = 5 + (-1)^0(X-5) \wedge 0 \leq 2 \cdot N\}$ (1)
$n := 0;$
$\{INV: \; x = 5 + (-1)^n(X-5) \wedge n \leq 2 \cdot N\}$
while $n < 2 \cdot N$ do
  $\{INV \wedge n < 2 \cdot N\}$
  $\{10 - x = 5 + (-1)^{n+1}(X-5) \wedge n+1 \leq 2 \cdot N\}$ (2)
  $n := n + 1;$
  $\{10 - x = 5 + (-1)^n(X-5) \wedge n \leq 2 \cdot N\}$
  $x := 10 - x;$
$\{INV \wedge \neg(n < 2 \cdot N)\}$
$\{x = X\}$ (3)

Per le PrePost:
1) Semplice aritmetica.

2) La parte $n+1 \leq 2 \cdot N$ segue da $n < 2 \cdot N$ visto che n è intero. Per la parte $10-x = 5+(-1)^{n+1}(X-5)$, da INV ricaviamo $x = 5+(-1)^n(X-5)$, da cui

$$\begin{aligned} 10 - x &= 10 - (5 + (-1)^n(X-5)) \\ &= 5 - (-1)^n(X-5) \\ &= 5 + (-1)^{n+1}(X-5) \end{aligned}$$

3) Da INV e $\neg(n < 2 \cdot N)$ si ricava $n = 2 \cdot N$. Da INV si ha quindi

$$\begin{aligned} x &= 5 + (-1)^n(X-5) \\ &= 5 + (-1)^{2 \cdot N}(X-5) \\ &= 5 + (X-5) = X \end{aligned}$$

Nota: invarianti alternative (ma sempre corrette) sono

$$INV: \; (n \text{ pari} \implies x = X) \wedge (n \text{ dispari} \implies x = 10 - X) \wedge n \leq 2 \cdot N$$
$$INV: \; ((n \text{ pari} \wedge x = X) \vee (n \text{ dispari} \wedge x = 10 - X)) \wedge n \leq 2 \cdot N$$

□