LOGICA PER LA PROGRAMMAZIONE (A,B) - a.a. 2012-2013
SOLUZIONI PROPOSTE
SECONDO COMPITINO - 21/12/2012

ESERCIZIO 1
Assumendo **a: array [0, n) of nat** e **b : array [0, m) of nat** con $n \leq m$ si formalizzi il seguente enunciato:

"Ogni elemento di **a** è uguale al prodotto dell'elemento corrispondente di **b** e del massimo valore di **b**"

Soluzione

$$(\forall i \,.\, i \in [0, n) \Rightarrow a[i] = b[i] * (max\ j\ :\ j \in [0, m)\,.\, b[j]))$$

Questa soluzione usa il quantificatore funzionale *max* presentato a lezione. Una soluzione che non lo usa, più complicata ma sempre corretta, è la seguente:

$$(\forall i \,.\, i \in [0, n) \Rightarrow (\exists k.k \in [0, m) \wedge (\forall j.j \in [0, m) \Rightarrow b[k] \geq b[j]) \wedge a[i] = b[i] * b[k]))$$

ESERCIZIO 2

Determinare le espressioni E_1 ed E_2 in modo tale da verificare la seguente tripla di Hoare (motivando la risposta):

$\{x = A \wedge y = B \wedge A \geq 0 \wedge B \geq 0\}$
if $x - y \geq 0$ **then** $m := E_1$ **else** $m := E_2$ **fi**;
z := 2 * m
$\{z > 2 * A \wedge z > 2 * B\}$

Soluzione
La tripla è verificata per qualunque coppia di valori $E_1 > x$ ed $E_2 > y$, per esempio $E_1 = x + 1$ ed $E_2 = y + 1$. Procediamo con la verifica.

Applicando la regola (SEQ), dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

(1) $\{x = A \wedge y = B \wedge A \geq 0 \wedge B \geq 0\}$
if $x - y \geq 0$ **then** $m := E_1$ **else** $m := E_2$ **fi**
$\{R\}$

(2) $\{R\}$
z := 2 * m
$\{z > 2 * A \wedge z > 2 * B\}$

Per l'Assioma dell'Assegnamento, la (2) è verificata per il seguente valore di R:

$def(2 * m) \wedge (z > 2 * A \wedge z > 2 * B)[^{2*m}/_z]$
$\equiv$ { definizione di *def*, sostituzione, calcolo }
$m > A \wedge m > B$

Per la Regola del Condizionale, la verifica della (1) con la postcondizione R appena calcolata si riduce alle seguenti tre verifiche:

(1.1) $x = A \wedge y = B \wedge A \geq 0 \wedge B \geq 0 \Rightarrow def(x - y \geq 0)$
banalmente vera osservando che $def(x - y \geq 0) \equiv T$

(1.2) $\{x = A \wedge y = B \wedge A \geq 0 \wedge B \geq 0 \wedge x - y \geq 0\ \}$
m := E_1
$\{m > A \wedge m > B\ \}$
Applicando la Regola dell'Assegnamento, dobbiamo dimostrare
$x = A \wedge y = B \wedge A \geq 0 \wedge B \geq 0 \wedge x - y \geq 0 \Rightarrow def(E_1) \wedge (m > A \wedge m > B)[^{E_1}/_m]$

Partiamo dalla conseguenza:

$def(E_1) \wedge (m > A \wedge m > B)[^{E_1}/_m]$

$\equiv$ { sostituzione }

$def(E_1) \wedge E_1 > A \wedge E_1 > B$

$\equiv$ { **Ip:** $x = A \wedge y = B$ }

$def(E_1) \wedge E_1 > x \wedge E_1 > y$

$\equiv$ { **Ip:** $E_1 = x + 1$ }

$def(x + 1) \wedge x + 1 > x \wedge x + 1 > y$

$\equiv$ { definizione di *def*, calcolo, **Ip:** $x - y \geq 0$, $x - y \geq 0 \Rightarrow x + 1 > y$ }

T

(1.3) $\{x = A \wedge y = B \wedge A \geq 0 \wedge B \geq 0 \wedge x - y < 0\}$

m := E_2

$\{m > A \wedge m > B\}$

Applicando la Regola dell'Assegnamento, dobbiamo dimostrare

$x = A \wedge y = B \wedge A \geq 0 \wedge B \geq 0 \wedge x - y < 0 \Rightarrow def(E_2) \wedge (m > A \wedge m > B)[^{E_2}/_m]$

Partiamo dalla conseguenza:

$def(E_2) \wedge (m > A \wedge m > B)[^{E_2}/_m]$

$\equiv$ { sostituzione }

$def(E_2) \wedge E_2 > A \wedge E_2 > B$

$\equiv$ { **Ip:** $x = A \wedge y = B$ }

$def(E_2) \wedge E_2 > x \wedge E_2 > y$

$\equiv$ { **Ip:** $E_2 = y + 1$ }

$def(y + 1) \wedge y + 1 > x \wedge y + 1 > y$

$\equiv$ { definizione di *def*, calcolo, **Ip:** $x - y < 0$, $x - y < 0 \Rightarrow x < y + 1$ }

T

N.B.: La soluzione $E_1 = A + 1$, $E_2 = B + 1$ (o simili) non è corretta perché A e B sono variabili di specifica e non possono essere usate nel programma.

ESERCIZIO 3

Si consideri il seguente programma annotato:

$\{x = 0 \wedge z = 1 \wedge n \geq 0 \wedge m \geq 0\}$

$\{\mathsf{Inv}: x \in [0, max(n, m)] \wedge z = w^x\ \}\{\text{t: } max(n, m) - x\}$

while ($x < n$ or $x < m$) **do**

z := z * w;

x := x+1

endw

$\{z = w^{max(m,n)}\}$

1. Scrivere le ipotesi di invarianza, di progresso e di terminazione.
2. Dimostrare l'ipotesi di invarianza.

Soluzione

1. **Ipotesi di Progresso**

$\{x \in [0, max(n, m)] \wedge z = w^x \wedge (x < n \vee x < m) \wedge max(n, m) - x = V\ \}$

z := z * w;

x := x+1

$\{max(n, m) - x < V\ \}$

Ipotesi di Terminazione $x \in [0, max(n,m)] \wedge z = w^x \Rightarrow max(n,m) - x \geq 0$

Ipotesi di Invarianza

$\{x \in [0, max(n,m)] \wedge z = w^x \wedge (x < n \vee x < m)\ \}$
z := z * w;
x := x+1
$\{x \in [0, max(n,m)] \wedge z = w^x \wedge def(x < n \text{ or } x < m)\ \}$

2. Per verificare l'Ipotesi di Invarianza, applicando la Regola della Sequenza dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

(2.1) $\{x \in [0, max(n,m)] \wedge z = w^x \wedge (x < n \vee x < m)\ \}$
z := z * w
$\{R\}$

(2.2) $\{R\ \}$
x := x+1
$\{x \in [0, max(n,m)] \wedge z = w^x \wedge def(x < n \text{ or } x < m)\ \}$

Per l'Assioma dell'Assegnamento, la (2.2) è verificata per il seguente valore di R:

$def(x+1) \wedge (x \in [0, max(n,m)] \wedge z = w^x)[^{x+1}/_x]$
$\equiv$ { definizione di *def*, sostituzione }
$x + 1 \in [0, max(n,m)] \wedge z = w^{x+1}$

Per la Regola dell'Assegnamento, la verifica della (2.1) con la postcondizione R appena calcolata si riduce a dimostrare

$x \in [0, max(n,m)] \wedge z = w^x \wedge (x < n \vee x < m) \Rightarrow def(z * w) \wedge (x + 1 \in [0, max(n,m)] \wedge z = w^{x+1})[^{z*w}/_z]$

Partiamo dalla conseguenza:

$def(z * w) \wedge (x + 1 \in [0, max(n,m)] \wedge z = w^{x+1})[^{z*w}/_z]$
$\equiv$ { sostituzione, definizione di *def* }
$x + 1 \in [0, max(n,m)] \wedge z * w = w^{x+1}$
$\equiv$ { **Ip:** $z = w^x$ }
$x + 1 \in [0, max(n,m)] \wedge w^x * w = w^{x+1}$
$\equiv$ { calcolo, def di intervallo }
$x + 1 \geq 0 \wedge x + 1 \leq max(n,m)$
$\equiv$ { **Ip:** $x \in [0, max(n,m)]$, $x \in [0, max(n,m)] \Rightarrow x + 1 \geq 0$ }
$x + 1 \leq max(n,m)$
$\equiv$ { **Ip:** $x < n \vee x < m$, $x < n \vee x < m \Rightarrow x + 1 \leq max(n,m)$ }
T

ESERCIZIO 4
Si verifichi la seguente tripla di Hoare (assumendo **a: array [0, n) of nat**):

$\{h \in dom(a) \wedge h \geq 1 \wedge (\forall i.i \in [0,h) \Rightarrow a[i] > k)\}$
a[h] := a[0] + 1
$\{(\forall i.i \in [0,h] \Rightarrow a[i] > k)\}$

Soluzione Per la Regola dell'Aggiornamento Selettivo, dobbiamo verificare la seguente implicazione:

$h \in dom(a) \wedge h \geq 1 \wedge (\forall i.i \in [0,h) \Rightarrow a[i] > k) \Rightarrow$
$def(h) \wedge def(a[0] + 1) \wedge h \in dom(a) \wedge (\forall i.i \in [0,h] \Rightarrow a[i] > k)[^{a'}/_a]$

dove $a' = a\left[^{a[0]+1}/_h\right]$.

Partiamo dalla conseguenza:

$$
\begin{aligned}
& def(h) \wedge def(a[0]+1) \wedge h \in dom(a) \wedge (\forall i.i \in [0,h] \Rightarrow a[i] > k)[{}^{a'}/_{a}] \\
\equiv \quad & \{ \text{ definizione di } def \ \} \\
& 0 \in dom(a) \wedge h \in dom(a) \wedge (\forall i.i \in [0,h] \Rightarrow a[i] > k)[{}^{a'}/_{a}] \\
\equiv \quad & \{ \textbf{Ip: } h \in dom(a),\ h \geq 1, \text{ quindi } 0 \in dom(a); \text{ sostituzione } \} \\
& (\forall i.i \in [0,h] \Rightarrow a'[i] > k) \\
\equiv \quad & \{ \text{ definizione di } a' \ \} \\
& (\forall i.i \in [0,h] \Rightarrow a \left[{}^{a[0]+1}/_{h}\right] [i] > k) \\
\equiv \quad & \{ \text{ Intervallo-}\forall,\ h > 0 \ \} \\
& (\forall i.i \in [0,h) \Rightarrow a \left[{}^{a[0]+1}/_{h}\right] [i] > k) \wedge a \left[{}^{a[0]+1}/_{h}\right] [h] > k \\
\equiv \quad & \{ \text{ definizione di } a \left[{}^{a[0]+1}/_{h}\right],\ (\forall i.i \in [0,h) \Rightarrow i \neq k) \ \} \\
& (\forall i.i \in [0,h) \Rightarrow a[i] > k) \wedge a[0]+1 > k \\
\equiv \quad & \{ \textbf{Ip: } (\forall i.i \in [0,h) \Rightarrow a[i] > k) \wedge h \geq 1,\ (\forall i.i \in [0,h) \Rightarrow a[i] > k) \wedge h \geq 1 \Rightarrow a[0] > k, \text{ calcolo } \} \\
& T
\end{aligned}
$$