LOGICA PER LA PROGRAMMAZIONE (A,B) - a.a. 2011-2012
SOLUZIONI PROPOSTE
SECONDO APPELLO - 7/02/2012

ESERCIZIO 1

Si provi che la seguente proposizione è una tautologia:

$$(P \Rightarrow S \vee \neg Q \vee \neg R) \wedge \neg(S \vee \neg R) \Rightarrow (Q \Rightarrow \neg P)$$

Soluzione 1

$$\begin{array}{ll}
 & (P \Rightarrow S \vee \neg Q \vee \neg R) \wedge \neg(S \vee \neg R) \\
\equiv & \quad \{ \text{Elim-}\Rightarrow \} \\
 & (\neg P \vee S \vee \neg Q \vee \neg R) \wedge \neg(S \vee \neg R) \\
\equiv & \quad \{ \text{Complemento} \} \\
 & (\neg P \vee \neg Q) \wedge \neg(S \vee \neg R) \\
\Rightarrow & \quad \{ \text{Sempl-}\wedge \} \\
 & \neg P \vee \neg Q \\
\equiv & \quad \{ \text{Elim-}\Rightarrow \} \\
 & Q \Rightarrow \neg P
\end{array}$$

Soluzione 2

$$\begin{array}{ll}
 & \neg P \\
\Leftarrow & \quad \{ \textbf{Ip: } P \Rightarrow S \vee \neg Q \vee \neg R, \text{ occorrenza negativa} \} \\
 & \neg(S \vee \neg Q \vee \neg R) \\
\equiv & \quad \{ \text{De Morgan} \} \\
 & \neg(S \vee \neg R) \wedge Q \\
\Leftarrow & \quad \{ \textbf{Ip: } \neg(S \vee \neg R) \} \\
 & Q
\end{array}$$

ESERCIZIO 2

Si provi che la seguente formula è valida (P, R e S contengono la variabile libera x):

$$(\forall x. \neg P \wedge R) \wedge (\exists x. \neg S \Rightarrow P \vee \neg R) \Rightarrow \neg(\forall x. \neg S)$$

Soluzione

Per la regola della skolemizzazione, è sufficiente dimostrare

$$(\forall x. \neg P \wedge R) \wedge (\exists x. \neg S \Rightarrow P \vee \neg R) \wedge (\neg S[^a/_x] \Rightarrow P[^a/_x] \vee \neg R[^a/_x]) \Rightarrow \neg(\forall x. \neg S)$$

dove a è una costante nuova.

$$\begin{array}{ll}
 & (\forall x. \neg P \wedge R) \wedge (\exists x. \neg S \Rightarrow P \vee \neg R) \wedge (\neg S[^a/_x] \Rightarrow P[^a/_x] \vee \neg R[^a/_x]) \\
\Rightarrow & \quad \{ \text{Sempl-}\wedge \} \\
 & (\forall x. \neg P \wedge R) \wedge (\neg S[^a/_x] \Rightarrow P[^a/_x] \vee \neg R[^a/_x]) \\
\Rightarrow & \quad \{ \text{Elim-}\forall, a \text{ termine chiuso} \} \\
 & \neg P[^a/_x] \wedge R[^a/_x] \wedge (\neg S[^a/_x] \Rightarrow P[^a/_x] \vee \neg R[^a/_x]) \\
\equiv & \quad \{ \text{Elim-}\Rightarrow \} \\
 & \neg P[^a/_x] \wedge R[^a/_x] \wedge (S[^a/_x] \vee P[^a/_x] \vee \neg R[^a/_x]) \\
\equiv & \quad \{ \text{Complemento} \} \\
 & \neg P[^a/_x] \wedge R[^a/_x] \wedge (S[^a/_x] \vee \neg R[^a/_x]) \\
\equiv & \quad \{ \text{Complemento} \} \\
 & \neg P[^a/_x] \wedge R[^a/_x] \wedge S[^a/_x] \\
\Rightarrow & \quad \{ \text{Sempl-}\wedge \} \\
 & S[^a/_x] \\
\Rightarrow & \quad \{ \text{Intro-}\exists \} \\
 & (\exists x. S) \\
\equiv & \quad \{ \text{De Morgan} \} \\
 & \neg(\forall x. \neg S)
\end{array}$$

ESERCIZIO 3
Utilizzando il calcolo del primo ordine si formalizzi il seguente enunciato dichiarativo, indicando esplicitamente l'interpretazione intesa:

"Tutti i conoscenti comuni a Mario e ad Antonio sono italiani, ma Mario ha anche conoscenti francesi."

Soluzione

- **Linguaggio**
  - $\mathbf{C} = \{Mario, Antonio, Italia, Francia\}$
  - $\mathbf{F} = \emptyset$
  - $\mathbf{P} = \{persona(\cdot), conoscente(\cdot,\cdot), cittadino(\cdot,\cdot)\}$
- **Interpretazione**: $\mathbf{I} = (\mathbf{D}, \alpha)$
  - $\mathbf{D} = \mathcal{P} \cup \mathcal{S}$, con $\mathcal{P}$ insieme delle persone e $\mathcal{S}$ insieme degli stati.
  - $\alpha(Mario)$ = la persona Mario
  - $\alpha(Antonio)$ = la persona Antonio
  - $\alpha(Italia)$ = lo stato Italia
  - $\alpha(Francia)$ = lo stato Francia
  - $\alpha(persona)(d) \equiv \mathbf{T}$ se e solo se d è una persona
  - $\alpha(conoscente)(p, q) \equiv \mathbf{T}$ se e solo se le persone p e q sono conoscenti
  - $\alpha(cittadino)(p, s) \equiv \mathbf{T}$ se e solo se p è cittadino dello stato s

Una formalizzazione è allora

$$(\forall x.persona(x) \land conoscente(x, Mario) \land conoscente(x, Antonio) \Rightarrow cittadino(x, Italia)) \land$$
$$(\exists y.persona(y) \land conoscente(y, Mario) \land cittadino(y, Francia))$$

ESERCIZIO 4

Assumendo **a, b : array [0, n) of nat**, si formalizzi il seguente enunciato:

"La somma degli elementi di **a** che sono multipli di 5 e compaiono in **b** in posizione pari è minore di 100."

Soluzione

$$(\Sigma x : x \in [0, n) \land \mathbf{a}[x] \ \mathbf{mod}\ 5 = 0 \land (\exists y.y \in [0, n) \land y \ \mathbf{mod}\ 2 = 0 \land \mathbf{a}[x] = \mathbf{b}[y]).\mathbf{a}[x]) < 100$$

ESERCIZIO 5
Si verifichi la seguente tripla di Hoare:

$\{x \geq 0 \land y = (\Sigma i : i \in [0, x) \land i \,\%\, 6 = 0 \,.\, i)\}$
  if $x \,\%\, 6 = 0$ **then** y := y + x **else** skip **fi**;
  x := x + 1
$\{y = (\Sigma i : i \in [0, x) \land i \,\%\, 6 = 0 \,.\, i)\}$

Soluzione
Applicando la Regola della Sequenza, dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

(1) $\{x \geq 0 \land y = (\Sigma i : i \in [0, x) \land i \,\%\, 6 = 0 \,.\, i)\}$
  if $x \,\%\, 6 = 0$ **then** y := y + x **else** skip **fi**
$\{R\}$

(2) $\{R\}$

x := x + 1

$\{y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)\}$

Per l'Assioma dell'Assegnamento, la (2) è verificata per

$$R \equiv def(x + 1) \wedge (y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)) \left[{}^{x+1}/_{x}\right]$$

Quindi, semplificando, assumiamo che

$$R \equiv y = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i)$$

Per la (1), trattandosi di un comando condizionale dobbiamo dimostrare

(1.1) $x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \Rightarrow def(x \,\%\, 6 = 0)$

ovvia essendo $def(x \,\%\, 6 = 0) \equiv T$

(1.2) $\{x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge x \,\%\, 6 = 0\}$

y := y + x

$\{R\}$

(1.3) $\{x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge x \,\%\, 6 \neq 0\}$

skip

$\{R\}$

Dimostrazione di (1.2)

Per la Regola dell'Assegnamento dobbiamo dimostrare (ignorando $def(y + x)$ che è equivalente a T):

$(x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge x \,\%\, 6 = 0)$

$\Rightarrow$

$(y + x = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i))$

Partiamo dalla conclusione.

$y + x = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i)$

$\equiv$ { **Ip:** $x \,\%\, 6 = 0 \wedge x \in [0, x]$, Intervallo-$\Sigma$ }

$y + x = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) + x$

$\equiv$ { **Ip:** $y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)$ }

$y + x = y + x$

Dimostrazione di (1.3)

Per l'Assioma del comando vuoto e la Regola PRE, dobbiamo dimostrare la seguente implicazione:

$(x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge x \,\%\, 6 \neq 0)$

$\Rightarrow$

$(y = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i))$

Partiamo dalla conclusione.

$y = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i)$

$\equiv$ { **Ip:** $x \,\%\, 6 \neq 0 \wedge x \in [0, x]$, Intervallo-$\Sigma$ }

$y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)$

$\equiv$ { **Ip:** $y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)$ }

T

ESERCIZIO 6
Si consideri il seguente programma annotato:

$\{x = A \wedge z = B \wedge n \geq 0 \wedge x \geq 0\}$
$\{\mathsf{Inv}: \ z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \ \}\{\text{t: } |n - x|\}$
while $x \neq n$ **do**
  if $x > n$ **then** x := x - 1 **else** x := x + 1 **fi**;
  z := z + n
endw
$\{z = B + (|n - A| * n)\}$

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

Soluzione

1. **Ipotesi di Invarianza**

   $\{z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \wedge x \neq n\}$
     if $x > n$ **then** x := x - 1 **else** x := x + 1 **fi**;
     z := z + n
   $\{z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \wedge def(x \neq n) \ \}$

   Ipotesi di Progresso

   $\{z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \wedge x \neq n \wedge |n - x| = V \ \}$
     if $x > n$ **then** x := x - 1 **else** x := x + 1 **fi**;
     z := z + n
   $\{|n - x| < V \ \}$

   Ipotesi di Terminazione $z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \Rightarrow |n - x| \geq 0$

2. L'Ipotesi di Terminazione è banalmente soddisfatta per la definizione di valore assoluto.

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

   (2.1) $\{z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \wedge x \neq n \wedge |n - x| = V \ \}$
     if $x > n$ **then** x := x - 1 **else** x := x + 1 **fi**
   $\{R\}$

   (2.2) $\{R \ \}$
     z := z + n
   $\{|n - x| < V \ \}$

   Per l'Assioma dell'Assegnamento, la (2.2) è verificata per

   $$R \equiv def(z + n) \wedge (|n - x| < V)[^{z+n}/z]$$

   e quindi per

   $$R \equiv |n - x| < V$$

   .

   Per la Regola del Condizionale, la verifica della (2.1) con la postcondizione R appena calcolata si riduce alle seguenti tre verifiche:

   (2.1.1) $z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \wedge x \neq n \wedge |n - x| = V \Rightarrow def(x > n)$
   banalmente vera osservando che $def(x > n) \equiv T$

(2.1.2) $\{z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \wedge x \neq n \wedge |n - x| = V \wedge x > n\ \}$

x := x - 1

$\{|n - x| < V\ \}$

Applicando la Regola dell'Assegnamento, dobbiamo dimostrare

$z = B+((|n-A|-|n-x|)*n)\wedge n \geq 0\wedge x \geq 0\wedge x \neq n\wedge|n-x| = V\wedge x > n \Rightarrow def(x-1)\wedge(|n-x| < V)[^{x-1}/_{x}]$

Partiamo dalla conseguenza:

$def(x - 1) \wedge (|n - x| < V)[^{x-1}/_{x}]$

$\equiv$ { definizione di *def*, sostituzione }

$|n - (x - 1)| < V$

$\equiv$ { **Ip:** $x > n$, $x > n \Rightarrow (n - (x - 1)) \leq 0$ }

$-n + x - 1 < V$

$\equiv$ { **Ip:** $|n - x| = V$,$x > n$, $x > n \Rightarrow |n - x| = x - n$ }

$V - 1 < V$

$\equiv$ { calcolo }

T

(2.1.3) $\{z = B + ((|n - A| - |n - x|) * n) \wedge n \geq 0 \wedge x \geq 0 \wedge x \neq n \wedge |n - x| = V \wedge \neg(x > n)\ \}$

x := x + 1

$\{|n - x| < V\ \}$

Applicando la Regola dell'Assegnamento, dobbiamo dimostrare

$z = B+((|n-A|-|n-x|)*n)\wedge n \geq 0\wedge x \geq 0\wedge x \neq n\wedge|n-x| = V\wedge\neg(x > n) \Rightarrow def(x+1)\wedge(|n-x| < V)[^{x+1}/_{x}]$

Partiamo dalla conseguenza:

$def(x + 1) \wedge (|n - x| < V)[^{x+1}/_{x}]$

$\equiv$ { definizione di *def*, sostituzione }

$|n - (x + 1)| < V$

$\equiv$ { **Ip:** $x \leq n$, $x \neq n$, quindi $x < n \Rightarrow (n - (x + 1)) \geq 0$ }

$n - x - 1 < V$

$\equiv$ { **Ip:** $|n - x| = V$,$x < n$, $x < n \Rightarrow |n - x| = n - x$ }

$V - 1 < V$

$\equiv$ { calcolo }

T