LOGICA PER LA PROGRAMMAZIONE (A,B) - a.a. 2011-2012
SOLUZIONI PROPOSTE
PRIMO APPELLO - 17/01/2012

ESERCIZIO 1
Si provi che la seguente proposizione è una tautologia:

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

Soluzione 1

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

Soluzione 2

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

ESERCIZIO 2
Si provi che la seguente formula è valida (P, Q, R e S contengono la variabile libera x):

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

Soluzione

$$
\begin{array}{ll}
 & (\forall x.P \vee \neg Q \Rightarrow R) \\
\equiv & \{ \text{ Sempl.Sinistra-}\Rightarrow \} \\
 & (\forall x.(P \Rightarrow R) \wedge (\neg Q \Rightarrow R)) \\
\equiv & \{ \forall : \wedge \} \\
 & (\forall x.P \Rightarrow R) \wedge (\forall x.\neg Q \Rightarrow R) \\
\Rightarrow & \{ \text{ Intro-}\vee\text{, occorrenza positiva } \} \\
 & (\forall x.P \Rightarrow R \vee \neg S) \wedge (\forall x.\neg Q \Rightarrow R) \\
\equiv & \{ \text{ De Morgan, Doppia negazione } \} \\
 & (\forall x.P \Rightarrow \neg(\neg R \wedge S)) \wedge (\forall x.\neg Q \Rightarrow R) \\
\equiv & \{ \text{ Contropositiva } \} \\
 & (\forall x.P \Rightarrow \neg(\neg R \wedge S)) \wedge (\forall x.\neg R \Rightarrow Q)
\end{array}
$$

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

"LPP non è un esame fondamentale, ma perché uno studente si laurei
è necessario che abbia superato tutti gli esami fondamentali."

Soluzione

- **Linguaggio**
  - $\mathbf{C} = \{LPP\}$
  - $\mathbf{F} = \emptyset$
  - $\mathbf{P} = \{fondamentale(\cdot), laureato(\cdot), supera(\cdot, \cdot)\}$

- **Interpretazione**: $\mathbf{I} = (\mathbf{D}, \alpha)$
  - $\mathbf{D} = \mathcal{S} \cup \mathcal{E}$, con $\mathcal{S}$ insieme degli studenti e $\mathcal{E}$ insieme degli esami.
  - $\alpha(LPP)$ = l'esame LPP
  - $\alpha(fondamentale)(d) \equiv \mathbf{T}$ se e solo se d è un esame fondamentale
  - $\alpha(laureato)(d) \equiv \mathbf{T}$ se e solo se d è uno studente laureato
  - $\alpha(supera)(s, e) \equiv \mathbf{T}$ se e solo se lo studente s ha superato l'esame e

Una formalizzazione è allora

$$\neg fondamentale(LPP) \wedge (\forall x.laureato(x) \Rightarrow (\forall y.fondamentale(y) \Rightarrow superato(x, y)))$$

ESERCIZIO 4

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

"Il numero degli elementi di **a** che sono multipli di 3 e non compaiono in **b** è maggiore di 5."

Soluzione

$$\#\{x : x \in [0, n) \wedge \mathbf{a}[x] \ \mathbf{mod}\ 3 = 0 \wedge (\forall y.y \in [0, n) \Rightarrow \mathbf{a}[x] \neq \mathbf{b}[y])\} > 5$$

ESERCIZIO 5
Si consideri il seguente programma annotato:

$\{x = A \wedge z = B \wedge m \geq 0 \wedge y = 0\}$
$\{\mathsf{Inv} : x = A + (|z| * y) \wedge y \in [0, m]\ \}\{\text{t: } m - y\}$
while $y < m$ **do**
  if $z \geq 0$ **then** x:=x+z **else** x:=x-z **fi**;
  y:=y+1
endw
$\{x = A + (|B| * m)\}$

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

Soluzione

1. **Ipotesi di Invarianza**

   $\{x = A + (|z| * y) \wedge y \in [0, m] \wedge y < m\ \}$
     if $z \geq 0$ **then** x:=x+z **else** x:=x-z **fi**;
     y:=y+1
   $\{x = A + (|z| * y) \wedge y \in [0, m] \wedge def(y < m)\ \}$

   Ipotesi di Progresso

   $\{x = A + (|z| * y) \wedge y \in [0, m] \wedge y < m \wedge m - y = V\ \}$
     if $z \geq 0$ **then** x:=x+z **else** x:=x-z **fi**;
     y:=y+1
   $\{m - y < V\ \}$

   Ipotesi di Terminazione $x = A + (|z| * y) \wedge y \in [0, m] \wedge y < m \Rightarrow m - y \geq 0$

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) $\{x = A + (|z| * y) \land y \in [0, m] \land y < m\ \}$

if $z \geq 0$ **then** x:=x+z **else** x:=x-z **fi**;

$\{R\}$

(2.2) $\{R\ \}$

y:=y+1

$\{x = A + (|z| * y) \land y \in [0, m] \land def(y < m)\ \}$

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

$$R \equiv def(y + 1) \land (x = A + (|z| * y) \land y \in [0, m] \land def(y < m))^{y+1}_{y}$$
$$\equiv \ \{\text{definizione di } \textit{def}\text{, sostituzione}\}\ x = A + (|z| * (y + 1)) \land y + 1 \in [0, m]$$

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) $x = A + (|z| * y) \land y \in [0, m] \land y < m \Rightarrow def(z \geq 0)$

banalmente vera osservando che $def(z \geq 0) \equiv T$

(2.1.2) $\{x = A + (|z| * y) \land y \in [0, m] \land y < m \land z \geq 0\ \}$

x:=x+z

$\{x = A + (|z| * (y + 1)) \land y + 1 \in [0, m]\ \}$

Applicando la Regola dell'Assegnamento, dobbiamo dimostrare

$x = A + (|z| * y) \land y \in [0, m] \land y < m \land z \geq 0 \Rightarrow def(x + z) \land (x = A + (|z| * (y + 1)) \land y + 1 \in [0, m])^{x+z}_{x}$

Partiamo dalla conseguenza:

$def(x + z) \land (x = A + (|z| * (y + 1)) \land y + 1 \in [0, m])^{x+z}_{x}$

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

$x + z = A + (|z| * (y + 1)) \land y + 1 \in [0, m]$

$\equiv$ { **Ip:** $x = A + (|z| * y)$, $z \geq 0$ (quindi $|z| = z$) }

$A + (z * y) + z = A + (z * (y + 1)) \land y + 1 \in [0, m]$

$\equiv$ { **Ip:** $y \in [0, m]$, $y < m$ }

$A + (z * y) + z = A + (z * (y + 1))$

$\equiv$ { calcolo }

T

(2.1.3) $\{x = A + (|z| * y) \land y \in [0, m] \land y < m \land z < 0\ \}$

x:=x-z

$\{x = A + (|z| * (y + 1)) \land y + 1 \in [0, m]\ \}$

Applicando la Regola dell'Assegnamento, dobbiamo dimostrare

$x = A + (|z| * y) \land y \in [0, m] \land y < m \land z < 0 \Rightarrow def(x + z) \land (x = A + (|z| * (y + 1)) \land y + 1 \in [0, m])^{x-z}_{x}$

Partiamo dalla conseguenza:

$def(x + z) \land (x = A + (|z| * (y + 1)) \land y + 1 \in [0, m])^{x-z}_{x}$

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

$x - z = A + (|z| * (y + 1)) \land y + 1 \in [0, m]$

$\equiv$ { **Ip:** $x = A + (|z| * y)$, $z < 0$ (quindi $|z| = -z$) }

$A + (-z * y) - z = A + (-z * (y + 1)) \land y + 1 \in [0, m]$

$\equiv$ { **Ip:** $y \in [0, m]$, $y < m$ }

$A + (-z * y) - z = A + (-z * (y + 1))$

$\equiv$ { calcolo }

T

ESERCIZIO 6
Si verifichi la seguente tripla di Hoare:

$$\{k \in dom(a) \wedge k \geq 1 \wedge (\forall i.i \in [1,k) \Rightarrow a[i] = a[i-1] * 2)\}$$
a[k] := a[k-1] * 2
$$\{(\forall i.i \in [1,k] \Rightarrow a[i] = a[i-1] * 2)\}$$

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

$$k \in dom(a) \wedge k \geq 1 \wedge (\forall i.i \in [1,k) \Rightarrow a[i] = a[i-1] * 2) \Rightarrow$$
$$def(k) \wedge k \in dom(a) \wedge def(a[k-1] * 2) \wedge (\forall i.i \in [1,k] \Rightarrow a'[i] = a'[i-1] * 2)$$

dove $a' = a\left[{}^{a[k-1]*2}/_{k}\right]$.

Partiamo dalla conseguenza:

$def(k) \wedge k \in dom(a) \wedge def(a[k-1] * 2) \wedge (\forall i.i \in [1,k] \Rightarrow a'[i] = a'[i-1] * 2)$
$\equiv$ { definizione di def }
$k \in dom(a) \wedge def(k-1) \wedge k-1 \in dom(a) \wedge (\forall i.i \in [1,k] \Rightarrow a'[i] = a'[i-1] * 2)$
$\equiv$ { **Ip:** $k \in dom(a)$, $k \geq 1$, definizione di a', definizione di def }
$(\forall i.i \in [1,k] \Rightarrow a\left[{}^{a[k-1]*2}/_{k}\right][i] = a\left[{}^{a[k-1]*2}/_{k}\right][i-1] * 2)$
$\equiv$ { Intervallo-$\forall$, $k > 0$ }
$(\forall i.i \in [1,k) \Rightarrow a\left[{}^{a[k-1]*2}/_{k}\right][i] = a\left[{}^{a[k-1]*2}/_{k}\right][i-1] * 2) \wedge a\left[{}^{a[k-1]*2}/_{k}\right][k] = a\left[{}^{a[k-1]*2}/_{k}\right][k-1] * 2$
$\equiv$ { definizione di $a\left[{}^{a[k-1]*2}/_{k}\right]$, $(\forall i.i \in [0,k) \Rightarrow i \neq k)$ }
$(\forall i.i \in [1,k) \Rightarrow a[i] = a[i-1] * 2) \wedge a[k-1] * 2 = a[k-1] * 2$
$\equiv$ { **Ip:** $(\forall i.i \in [1,k) \Rightarrow a[i] = a[i-1] * 2)$, riflessività di $=$ }
T