LOGICA PER LA PROGRAMMAZIONE (A,B) - a.a. 2012-2013
SOLUZIONI PROPOSTE
14 Gennaio 2013 – PRIMO APPELLO

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

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

Soluzione Partiamo dalla premessa:

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

$\equiv$ { Controposizione }

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

$\equiv$ { De Morgan, Elim-$\Rightarrow$, Doppia Negazione }

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

$\equiv$ { De Morgan }

$R \wedge \neg S \Rightarrow \neg P \wedge \neg Q$

$\Rightarrow$ { Sempl-$\wedge$, occorrenza positiva }

$R \wedge \neg S \Rightarrow \neg P$

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

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

Soluzione Per la Regola di Skolemizzazione, è sufficiente dimostrare

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

dove d è una costante nuova. Partiamo dalla premessa:

$(\forall x.P) \wedge (\exists x.S \Rightarrow \neg P) \wedge (S[d/x] \Rightarrow \neg P[d/x])$

$\Rightarrow$ { Sempl-$\wedge$ }

$(\forall x.P) \wedge (S[d/x] \Rightarrow \neg P[d/x])$

$\Rightarrow$ { Elim-$\forall$ }

$P[d/x] \wedge (S[d/x] \Rightarrow \neg P[d/x])$

$\equiv$ { Contropositiva }

$P[d/x] \wedge (P[d/x] \Rightarrow \neg S[d/x])$

$\Rightarrow$ { Modus Ponens }

$\neg S[d/x]$

$\Rightarrow$ { Intro-$\vee$ }

$\neg S[d/x] \vee R[d/x]$

$\Rightarrow$ { Intro-$\exists$ }

$(\exists x\,.\,\neg S \vee R)$

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

"I conoscenti di Mario ed Antonio che sono residenti a Pisa hanno un conoscente in comune."

Soluzione

- **Linguaggio**
  - $\mathbf{C} = \{Antonio, Mario, Pisa\}$
  - $\mathbf{F} = \emptyset$
  - $\mathbf{P} = \{persona(\_), citta(\_), conosce(\_, \_), residente(\_, \_)\}$
- **Interpretazione**: $\mathbf{I} = (\mathbf{D}, \alpha)$
  - $\mathbf{D} = \mathcal{P} \uplus \mathcal{C}$, con $\mathcal{P}$ insieme delle persone e $\mathcal{C}$ insieme delle città.
  - $\alpha(Antonio) =$ "la persona chiamata Antonio"
  - $\alpha(Mario) =$ "la persona chiamata Mario"
  - $\alpha(Pisa) =$ "la città chiamata Pisa"
  - $\alpha(persona)(d) \equiv \mathbf{T}$ se e solo se d è una persona
  - $\alpha(citta)(d) \equiv \mathbf{T}$ se e solo se d è una città
  - $\alpha(conosce)(d, d') \equiv \mathbf{T}$ se e solo se d e d' sono persone e si conoscono
  - $\alpha(residente)(d, d') \equiv \mathbf{T}$ se e solo se d è una persona, d' è una città, e d risiede in d'

L'enunciato può essere formalizzato nel seguente modo:

$$(\forall x, y \,.\, persona(x) \land persona(y) \land conosce(x, Antonio) \land conosce(y, Mario) \land residente(x, Pisa) \land residente(y, Pisa) \Rightarrow (\exists z \,.\, persona(z) \land conosce(x, z) \land conosce(y, z)))$$

N.B.: Soluzioni come la seguente, in cui si quantifica su un solo conoscente di Antonio e/o Mario, non sono state considerate accettabili perché non consentono di formalizzare il concetto "avere un conoscente in comune":

$$(\forall x \,.\, persona(x) \land conosce(x, Antonio) \land conosce(x, Mario) \land residente(x, Pisa) \Rightarrow (\exists z \,.\, persona(z) \land conosce(x, z)))$$

ESERCIZIO 4
Assumendo **a, b: array [0, n) of nat** e **c: array [0, m) of nat**, si formalizzi il seguente enunciato:

"Il minimo degli elementi di **a** che sono multipli di 10 e compaiono in **b** o in **c** è maggiore di 30"

Soluzione

$$(min\ x \colon x \in [0, n) \land (a[x]\%10 = 0) \land ((\exists y \,.\, y \in [0, n) \land a[x] = b[y]) \lor (\exists z \,.\, z \in [0, m) \land a[x] = c[z])) \,.\, a[x]) > 30$$

ESERCIZIO 5
Si verifichi la seguente tripla di Hoare (assumendo **a: array [0, n) of nat**):

$\{k \in dom(a) \land y = (\sum i : i \in [0, k) \land i\%5 = 0 \,.\, a[i])\}$
if k *mod* 5 = 0 **then** y := y + a[k] **else** skip **fi**;
k := k + 1
$\{y = (\sum i : i \in [0, k) \land i\%5 = 0 \,.\, a[i])\}$

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

(1) $\{k \in dom(a) \land y = (\sum i : i \in [0, k) \land i\%5 = 0 \,.\, a[i])\}$
if k *mod* 5 = 0 **then** y := y + a[k] **else** skip **fi**
$\{R\}$

(2) $\{R\}$
k := k + 1
$\{y = (\sum i : i \in [0,k) \wedge i\%5 = 0\,.\,a[i])\}$

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

$$R \equiv def(k+1) \wedge \Big(y = (\sum i : i \in [0,k) \wedge i\,\%\,5 = 0\,.\,a[i])\Big)\,[^{k+1}/_{k}]$$

Quindi, semplificando, assumiamo che

$$R \equiv y = (\sum i : i \in [0,k] \wedge i\,\%\,5 = 0\,.\,a[i])$$

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

(1.1) $k \in dom(a) \wedge y = (\sum i : i \in [0,k) \wedge i\%5 = 0\,.\,a[i]) \Rightarrow def(k\ mod\ 5 = 0)$
ovvia essendo $def(k\ mod\ 5 = 0) \equiv T$

(1.2) $\{k \in dom(a) \wedge y = (\sum i : i \in [0,k) \wedge i\%5 = 0\,.\,a[i]) \wedge k\ mod\ 5 = 0\}$
y := y + a[k]
$\{R\}$

(1.3) $\{k \in dom(a) \wedge y = (\sum i : i \in [0,k) \wedge i\%5 = 0\,.\,a[i]) \wedge k\ mod\ 5 \neq 0\}$
skip
$\{R\}$

Dimostrazione di (1.2)
Per la Regola dell'Assegnamento dobbiamo dimostrare:
$(k \in dom(a) \wedge y = (\sum i : i \in [0,k) \wedge i\%5 = 0\,.\,a[i]) \wedge k\ mod\ 5 = 0)$
$\Rightarrow$
$def(y + a[k]) \wedge (y = (\sum i : i \in [0,k] \wedge i\,\%\,5 = 0\,.\,a[i]))[^{y+a[k]}/_{y}]$
Partiamo dalla conclusione, applicando la sostituzione e la definizione di *def*.
$k \in dom(a) \wedge y + a[k] = (\sum i : i \in [0,k] \wedge i\,\%\,5 = 0\,.\,a[i])$
$\equiv$ { Definizione di *def*, Intervallo-Σ, **Ip:** $k\,\%\,5 = 0 \wedge k \in [0,k]$ }
$y + a[k] = (\sum i : i \in [0,k) \wedge i\,\%\,5 = 0\,.\,a[i]) + a[k]$
$\equiv$ { **Ip:** $y = (\sum i : i \in [0,k) \wedge i\,\%\,5 = 0\,.\,a[i])$ }
$y + a[k] = y + a[k]$
$\equiv$ { rifl. di $=$ }
T

Dimostrazione di (1.3)
Per l'Assioma del comando vuoto e la Regola (PRE), dobbiamo dimostrare la seguente implicazione:
$(k \in dom(a) \wedge y = (\sum i : i \in [0,k) \wedge i\%5 = 0\,.\,a[i]) \wedge k\ mod\ 5 \neq 0)$
$\Rightarrow$
$y = (\sum i : i \in [0,k] \wedge i\,\%\,5 = 0\,.\,a[i])$
Partiamo dalla conclusione.
$y = (\sum i : i \in [0,k] \wedge i\,\%\,5 = 0\,.\,a[i])$
$\equiv$ { Intervallo-Σ, **Ip:** $k\,\%\,5 \neq 0 \wedge k \in [0,k]$ }
$y = (\sum i : i \in [0,k) \wedge i\,\%\,5 = 0\,.\,a[i])$
$\equiv$ { **Ip:** $y = (\sum i : i \in [0,k) \wedge i\,\%\,5 = 0\,.\,a[i])$ }
$y = y$
$\equiv$ { rifl. di $=$ }
T

ESERCIZIO 6
Si consideri il seguente programma annotato:

$\{x = 0 \wedge y = 0 \wedge z \geq 0\}$
$\{\mathsf{Inv}: \ x = y * y \wedge y \in [0, z] \ \}\{\text{t: } (z - y) * (z + y)\}$
while $y < z$ **do**
x, y := x + 2*y + 1, y + 1
endw
$\{x = z * z\}$

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

Soluzione

1. **Ipotesi di Invarianza**

$\{x = y * y \wedge y \in [0, z] \wedge y < x\}$
x, y := x + 2*y + 1, y + 1
$\{x = y * y \wedge y \in [0, z] \wedge def(y < x)\}$

Ipotesi di Progresso

$\{x = y * y \wedge y \in [0, z] \wedge y < x \wedge (z - y) * (z + y) = V\}$
x, y := x + 2*y + 1, y + 1
$\{(z - y) * (z + y) < V\}$

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

2. Per verificare l'Ipotesi di Progresso, applicando la Regola dell'assegnamento multiplo, dobbiamo dimostrare la seguente implicazione:

$x = y * y \wedge y \in [0, z] \wedge y < x \wedge (z - y) * (z + y) = V$

$\Rightarrow$

$def(x + 2 * y + 1) \wedge def(y + 1) \wedge ((z - y) * (z + y) < V)[^{x+2*y+1}/_{x}, ^{y+1}/_{y}]$

Partiamo dalla conclusione, applicando la sostituzione e la definizione di *def*.

$(z - (y + 1)) * (z + (y + 1)) < V$
$\equiv$ { **Ip:** $(z - y) * (z + y) = V$ }
$(z - (y + 1)) * (z + (y + 1)) < (z - y) * (z + y)$
$\equiv$ { calcolo (prodotto notevole) }
$z^2 - (y + 1)^2 < z^2 - y^2$
$\equiv$ { calcolo }
$-y^2 - 2 * y - 1 < -y^2$
$\equiv$ { calcolo }
$-2 * y - 1 < 0$
$\equiv$ { **Ip:** $y \in [0, z)$, quindi $y \geq 0$ }
T