# LOGICA PER LA PROGRAMMAZIONE - a.a. 2018-2019
# Quinto Appello - 6/09/2019 — Soluzioni Proposte

**Attenzione:** Le soluzioni che seguono sono considerate corrette dai docenti. Per ogni esercizio possono esistere altre soluzioni corrette, anche molto diverse da quelle proposte.

**ESERCIZIO 1**
Si dica se le seguenti proposizioni sono tautologie oppure no. Se una proposizione è una tautologia, lo si deve dimostrare senza usare le tabelle di verità; altrimenti va prodotto un controesempio che rende la formula falsa.

1. $\big(((B \Rightarrow \neg C) \wedge \neg A) \Rightarrow (B \wedge (B \Rightarrow A))\big) \;\Rightarrow\; \big(\neg A \Rightarrow (B \wedge C)\big)$
2. $\big(((B \Rightarrow \neg C) \wedge \neg A) \Rightarrow (B \wedge (B \Rightarrow A))\big) \;\equiv\; \big(\neg A \Rightarrow (B \wedge C)\big)$

**SOLUZIONE ESERCIZIO 1**

1. La formula è una tautologia. Sviluppiamo una dimostrazione partendo dalla premessa dell'implicazione per arrivare alla conclusione:

$((B \Rightarrow \neg C) \wedge \neg A) \underline{\Rightarrow} (B \wedge (B \Rightarrow A))$

$\equiv$ $\{(\text{Elim-}\Rightarrow)\}$

$\neg((B \underline{\Rightarrow} \neg C) \wedge \neg A) \vee (B \wedge (B \underline{\Rightarrow} A))$

$\equiv$ $\{(\text{Elim-}\Rightarrow)\}$

$\underline{\neg((\neg B \vee \neg C) \wedge \neg A)} \vee (B \wedge (\neg B \vee A))$

$\equiv$ $\{(\text{De Morgan}), (\text{Doppia negazione})\}$

$((B \wedge C) \vee A) \vee (\underline{B \wedge (\neg B \vee A}))$

$\equiv$ $\{(\text{Complemento})\}$

$((B \wedge C)\underline{\vee A) \vee (B \wedge A)}$

$\equiv$ $\{(\text{Associatività}), (\text{Assorbimento})\}$

$(B \wedge C) \vee A$

$\equiv$ $\{(\text{Elim-}\Rightarrow)\}$

$\neg A \Rightarrow (B \wedge C)$

2. La formula è una tautologia. Infatti si puó utilizzare la stessa dimostrazione di sopra.

**ESERCIZIO 2**
Si consideri l'alfabeto del primo ordine $\mathcal{A}$ con simboli di costante $\mathcal{C} = \{M, G, L\}$, i simboli predicato $\mathcal{P} = \{A(-,-)\}$ e l'interpretazione $I = (\mathcal{D}, \alpha)$, dove $\mathcal{D}$ è l'insieme di tutte le persone

- $\alpha(M)$ è la persona Marco,
- $\alpha(G)$ è la persona Giovanni,
- $\alpha(L)$ è la persona Luca,
- $\alpha(A)(p, q)$ è vera se e solo se la persona $p$ è amica della persona $q$,

Formalizzare il seguente enunciato usando l'alfabeto $\mathcal{A}$ rispetto all'interpretazione $I$:

"Se ogni amico di Marco è anche amico di Giovanni e Luca non è amico di Marco, allora Luca non è amico di Giovanni."

**SOLUZIONE ESERCIZIO 2**
L'enunciato può essere formalizzato nel seguente modo:

$$\big((\forall x \,.\, A(x, M) \Rightarrow A(x, G)) \wedge \neg A(L, M)\big) \Rightarrow \neg A(L, G)$$

**ESERCIZIO 3**
Si provi che la seguente formula è valida ($Q$, $R$ e $S$ contengono la variabile libera $x$):

$$\big((\forall x \,.\, Q \vee R) \;\wedge\; (\exists x \,.\, \neg(Q \vee R) \vee \neg R \vee (R \wedge S)\big) \;\Rightarrow\; (\exists x \,.\, R \Rightarrow S)$$

**SOLUZIONE ESERCIZIO 3**

Adesso, utilizzando la regola della **Skolemizzazione** è sufficiente dimostrare che:

$$\big((\forall x \,.\, Q \vee R) \;\wedge\; (\,\exists x \,.\, \neg(Q \vee R) \vee \neg R \vee (R \wedge S)\,) \;\wedge\; (\neg(Q(a) \vee R(a)) \vee \neg R(a) \vee (R(a) \wedge S(a)))\big) \;\Rightarrow\; (\exists x \,.\, R \Rightarrow S)$$

con $a$ costante nuova. Per dimostrare la formula partiamo dalla premessa:

$$\begin{array}{ll}
 & (\forall x \,.\, Q \vee R) \;\wedge\; \underline{(\,\exists x \,.\, \neg(Q \vee R) \vee \neg R \vee (R \wedge S)\,)} \;\wedge\; (\neg(Q(a) \vee R(a)) \vee \neg R(a) \vee (R(a) \wedge S(a))) \\
\Rightarrow & \{(\text{Sempl-}\wedge),\ \text{occor. pos.}\} \\
 & \underline{(\forall x \,.\, Q \vee R)} \;\wedge\; (\neg(Q(a) \vee R(a)) \vee \neg R(a) \vee (R(a) \wedge S(a))) \\
\Rightarrow & \{(\text{Elim-}\forall),\ \text{occor. pos.}\} \\
 & (Q(a) \vee R(a)) \;\wedge\; (\neg(Q(a) \vee R(a)) \vee \underline{\neg R(a) \vee (R(a) \wedge S(a)))} \\
\equiv & \{(\text{Complemento})\} \\
 & (Q(a) \vee R(a)) \;\wedge\; (\underline{\neg(Q(a) \vee R(a)) \vee \neg R(a) \vee S(a))} \\
\equiv & \{(\text{Elim-} \Rightarrow\,)\} \\
 & \underline{(Q(a) \vee R(a))} \;\wedge\; \underline{((Q(a) \vee R(a)) \Rightarrow (\neg R(a) \vee S(a)))} \\
\equiv & \{(\text{Modus Ponens})\} \\
 & \underline{\neg R(a) \vee S(a)} \\
\equiv & \{(\text{Elim-} \Rightarrow\,)\} \\
 & \underline{R(a) \Rightarrow S(a)} \\
\Rightarrow & \{(\text{Intro-}\exists),\ \text{occor. pos. }\} \\
 & (\exists x \,.\, R \Rightarrow S)
\end{array}$$

**ESERCIZIO 4**
Si formalizzi il seguente enunciato (assumendo **a: array [0, n) of int** e **b: array [0, m) of int**):

"Per ogni numero in posizione dispari nell'array **a**, esiste un numero maggiore in posizione pari nell'array **b**"

**SOLUZIONE ESERCIZIO 4**
Proponiamo due soluzioni, entrambe corrette, la seconda delle quali utilizza il quantificatore funzionale **max**:

$$\big(\forall i \,.\, i \in [0,n) \wedge Dispari(i) \Rightarrow (\exists j \,.\, j \in [0,m) \wedge Pari(j) \wedge a[i] \leq b[j])\big)$$

$$\big(\mathbf{max}\, i : i \in [0,n) \wedge Dispari(i) \,.\, a[i]\big) \leq \big(\mathbf{max}\, j : j \in [0,m) \wedge Pari(j) \,.\, b[j]\big)$$

**ESERCIZIO 5**
Assumendo **a: array [0, n) of int**, si consideri il seguente frammento di programma annotato,

$\{c = 0 \ \wedge \ y = 0\}$
$\{\mathsf{Inv}\text{: } y \in [0, n] \ \wedge \ \big(c = (\Sigma i : i \in [0, y) \wedge pari(a[i]) \,.\, a[i]^2)\big)\}\{\text{t: } n - y\}$

```
while y < n do
     if (a[y] mod 2 = 0)
          then c, y := c+a[y]*a[y], y+1
          else y := y+1
     fi
endw
```

$\{c = (\Sigma i : i \in [0, n) \wedge pari(a[i]) \,.\, a[i]^2)\}$

Si scrivano le ipotesi di progresso ed invarianza. Inoltre si dimostri l'ipotesi di invarianza.

**SOLUZIONE ESERCIZIO 5**

Invariante $Inv : y \in [0, n] \ \wedge \ \big(c = (\Sigma i : i \in [0, y) \wedge pari(a[i]) \,.\, a[i]^2)\big)$
Funzione di terminazione $t : n - y$

1. **Ipotesi di Invarianza**:

$\{y \in [0, n] \ \wedge \ \big(c = (\Sigma i : i \in [0, y) \wedge pari(a[i]) \,.\, a[i]^2)\big) \wedge y < n\}$

```
     if (a[y] mod 2 = 0)
          then c, y := c+a[y]*a[y], y+1
          else y := y+1   fi
```

$\{y \in [0, n] \ \wedge \ \big(c = (\Sigma i : i \in [0, y) \wedge pari(a[i]) \,.\, a[i]^2)\big) \wedge def(y < n) \ \}$

2. **Ipotesi di Progresso**:

$\{y \in [0, n] \ \wedge \ \big(c = (\Sigma i : i \in [0, y) \wedge pari(a[i]) \,.\, a[i]^2)\big) \ \wedge \ y < n \ \wedge \ n - y = V\}$

```
     if (a[y] mod 2 = 0)
          then c, y := c+a[y]*a[y], y+1
          else y := y+1   fi
```

$\{n - y < V\}$

Dimostriamo l'ipotesi di invarianza applicando la regola del **Condizionale**. Quindi dobbiamo verificare che

(5.1.1) $Inv \wedge y < n \ \Rightarrow \ def(a[y] \ mod \ 2 = 0)$

(5.1.2) $\{Inv \wedge y < n \wedge (a[y] \ mod \ 2 = 0)\}$ `c, y := c+a[y]*a[y], y+1` $\{Inv \wedge def(y < n)\}$

(5.1.3) $\{Inv \wedge y < n \wedge \neg(a[y] \ mod \ 2 = 0)\}$ $\mathtt{y := y + 1}$ $\{Inv \wedge def(y < n)\}$

(5.1.1) Abbiamo che

$def(a[y] \ mod \ 2 = 0)$

$\equiv$ {definizione di *def*}

$y \in dom(a)$

$\equiv$ $\{dom(a) = [0, n)$, **Ip**: $y \in [0, n] \wedge y < n\}$

**T**

(5.1.2) Per dimostrare la tripla applichiamo la regola dell' **Assegnamento Multiplo** e ci riduciamo a dimostrare

$$Inv \wedge y < n \ \wedge \ a[y] \ mod \ 2 = 0 \quad \Rightarrow \quad def(c + a[y] * a[y]) \ \wedge \ def(y + 1) \ \wedge \ \big(Inv \ \wedge \ def(y < n)\big)[^{c+a[y]*a[y],y+1}/_{c,y}]$$

Partiamo dalla conseguenza

$\underline{def(c + a[y] * a[y]) \wedge def(y + 1)} \wedge \big(Inv \wedge def(y < n)\big)[^{c+a[y]*a[y],y+1}/_{c,y}]$

$\equiv$ $\{$definizione di $def\}$

$\underline{y \in dom(a) \wedge \mathbf{T}} \wedge \big(Inv \wedge def(y < n)\big)[^{c+a[y]*a[y],y+1}/_{c,y}]$

$\equiv$ $\{dom(a) = [0, n)$, **Ip**: $y \in [0, n], y < n\}$

$\underline{\big(Inv \wedge def(y < n)\big)[^{c+a[y]*a[y],y+1}/_{c,y}]}$

$\equiv$ $\{$sostituzione$\}$

$y + 1 \in [0, n] \;\wedge\; \big(c + a[y] * a[y] = (\Sigma i : i \in [0, y + 1) \wedge pari(a[i]) \,.\, a[i]^2)\big) \wedge \underline{def(y + 1 < n)}$

$\equiv$ $\{$definizione di $def\}$

$\underline{y + 1 \in [0, n]} \;\wedge\; \big(c + a[y] * a[y] = (\Sigma i : i \in [0, y + 1) \wedge pari(a[i]) \,.\, a[i]^2)\big)$

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

$\big(c + a[y] * a[y] = (\Sigma i : i \in [0, y + 1) \wedge pari(a[i]) \,.\, a[i]^2)\big)$

$\equiv$ $\{$(Intervallo-$\Sigma$), **Ip**: $a[y]\ mod\ 2 = 0$ $\}$

$\big(c + a[y] * a[y] = (\Sigma i : i \in [0, y) \wedge pari(a[i]).a[i]^2) + a[y]^2\big)$

$\equiv$ $\{$calcolo$\}$

$c = (\Sigma i : i \in [0, y) \wedge pari(a[i]).a[i]^2)$

$\equiv$ $\big\{$**Ip**: $c = (\Sigma i : i \in [0, y) \wedge pari(a[i]).a[i]^2)\big\}$

$\mathbf{T}$

(5.1.3) Per dimostrare la tripla applichiamo la regola dell' **Assegnamento** e ci riduciamo a dimostrare

$$Inv \wedge y < n \wedge \neg(a[y]\ mod\ 2 = 0) \quad \Rightarrow \quad def(y + 1) \wedge \big(Inv \wedge def(y < n)\big)[^{y+1}/_y]$$

Partiamo dalla conseguenza

$def(y + 1) \wedge \big(Inv \wedge def(y < n)\big)[^{y+1}/_y]$

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

$\underline{y + 1 \in [0, n]} \;\wedge\; \big(c = (\Sigma i : i \in [0, y + 1) \wedge pari(a[i]).a[i]^2)\big)$

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

$c = (\Sigma i : i \in [0, y + 1) \wedge pari(a[i]).a[i]^2)$

$\equiv$ $\{$(Intervallo-$\Sigma$), **Ip**: $\neg(a[y]\, mod\, 2 = 0)$ $\}$

$c = (\Sigma i : i \in [0, y) \wedge pari(a[i]).a[i]^2)$

$\equiv$ $\big\{$**Ip**: $c = (\Sigma i : i \in [0, y) \wedge pari(a[i]).a[i]^2)\big\}$

$\mathbf{T}$

**ESERCIZIO 6**

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

$$\{\ x \in [1,n) \wedge \big(\forall i\,.\, i \in [0,x)\ \Rightarrow\ \mathtt{a}[i]\ mod\ 2 = 0\big)\}$$

```
a[x] := a[x-1]*2;
x := x+1
```

$$\{\big(\forall i\,.\, i \in [0,x)\ \Rightarrow\ \mathtt{a}[i]\ mod\ 2 = 0\big)\}$$

**SOLUZIONE ESERCIZIO 6**

Applicando la regola della **Sequenza di comandi** dobbiamo trovare un'asserzione $R$ per cui le seguenti triple siano siddisfatte:

(6.1) $\{\ x \in [1,n) \wedge \big(\forall i\,.\, i \in [0,x)\ \Rightarrow\ \mathtt{a}[i]\ mod\ 2 = 0\big)\}$ `a[x] := a[x-1]*2` $\{R\}$

(6.2) $\{R\}$ `x := x+1` $\{(\forall i\,.\, i \in [0,x)\ \Rightarrow\ \mathtt{a}[i]\ mod\ 2 = 0)\}$

Cominciamo con la tripla (6.2). Per la Regola dell'**Assegnamento**, abbiamo che la tripla è soddisfatta per

$$R = def(x+1) \wedge \big(\forall i\,.\, i \in [0,x) \Rightarrow \mathtt{a}[i]\ mod\ 2 = 0\big)[^{x+1}/_{x}]$$

Verifichiamo ora la tripla (6.1). Per la Regola dell'**Aggiornamento Selettivo**, abbiamo che la tripla è soddisfatta se

$$x \in [1,n) \wedge \big(\forall i\,.\, i \in [0,x)\ \Rightarrow\ \mathtt{a}[i]\ mod\ 2 = 0\big)\ \Rightarrow$$
$$def(x) \wedge def(\mathtt{a}[x-1]*2) \wedge x \in dom(\mathtt{a}) \wedge R[^{\mathtt{b}}/_{\mathtt{a}}]$$

dove $\mathtt{b} = \mathtt{a}[^{\mathtt{a}[x-1]*2}/_{x}]$.

Partiamo dalla conseguenza

$$\underline{def(x) \wedge def(\mathtt{a}[x-1]*2)} \wedge x \in dom(\mathtt{a}) \wedge R[^{\mathtt{b}}/_{\mathtt{a}}]$$

$\equiv$ $\{$definizione di $def\}$

$$\underline{x-1 \in dom(\mathtt{a}) \wedge x \in dom(\mathtt{a})} \wedge R[^{\mathtt{b}}/_{\mathtt{a}}]$$

$\equiv$ $\{$**Ip**: $x \in [1,n)$, $dom(\mathtt{a}) = [0,n)\}$

$$\underline{R}[^{\mathtt{b}}/_{\mathtt{a}}]$$

$\equiv$ $\{$definizione di $R\}$

$$\underline{\big(def(x+1) \wedge \big(\forall i\,.\, i \in [0,x) \Rightarrow \mathtt{a}[i]\ mod\ 2 = 0\big)[^{x+1}/_{x}]\big)}[^{\mathtt{b}}/_{\mathtt{a}}]$$

$\equiv$ $\{$sostituzione$\}$

$$\underline{\big(def(x+1) \wedge \big(\forall i\,.\, i \in [0,x+1) \Rightarrow \mathtt{a}[i]\ mod\ 2 = 0\big)\big)[^{\mathtt{b}}/_{\mathtt{a}}]}$$

$\equiv$ $\{$sostituzione$\}$

$$\underline{def(x+1)} \wedge \big(\forall i\,.\, i \in [0,x] \Rightarrow \mathtt{b}[i]\ mod\ 2 = 0\big)$$

$\equiv$ $\{$definizione di def$\}$

$$\underline{\big(\forall i\,.\, i \in [0,x] \Rightarrow \mathtt{b}[i]\ mod\ 2 = 0\big)}$$

$\equiv$ $\{$(Intervallo-$\forall$), **Ip**: $x \geq 0\}$

$$\underline{\big(\forall i\,.\, i \in [0,x) \Rightarrow \mathtt{b}[i]\ mod\ 2 = 0\big)} \wedge \mathtt{b}[x]\ mod\ 2 = 0$$

$\equiv$ $\{$Definizione di $\mathtt{b}$, $x \notin [0,x)\}$

$$\underline{\big(\forall i\,.\, i \in [0,x) \Rightarrow \mathtt{a}[i]\ mod\ 2 = 0\big)} \wedge \mathtt{b}[x]\ mod\ 2 = 0$$

$\equiv$ $\big\{$**Ip**: $\big(\forall i\,.\, i \in [0,x) \Rightarrow \mathtt{a}[i]\ mod\ 2 = 0\big)\big\}$

$$\underline{\mathtt{b}[x]}\ mod\ 2 = 0$$

$\equiv$ $\{$(Definizione di $\mathtt{b}$)$\}$

$$\underline{(\mathtt{a}[x-1]*2)\ mod\ 2 = 0}$$

$\equiv$ $\{$**Ip**: $x \in [1,x)$, quindi $def(\mathtt{a}[x-1]) = \mathbf{T}$, (calcolo)$\}$

$$\mathbf{T}$$