LOGICA PER LA PROGRAMMAZIONE - a.a. 2018-2019
Primo Appello - 23/01/2018 — 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. $\big((P \Rightarrow \neg Q) \Rightarrow R\big) \vee \neg(P \Rightarrow R) \;\Rightarrow\; (\neg P \Rightarrow R)$
2. $\big((P \Rightarrow R) \Rightarrow Q\big) \vee \neg(P \Rightarrow R) \;\Rightarrow\; (\neg P \Rightarrow R)$

SOLUZIONE ESERCIZIO 1

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

   $\big(\underline{(P \Rightarrow \neg Q)} \Rightarrow R\big) \vee \underline{\neg(P \Rightarrow R)}$

   $\equiv$ {(Elim-$\Rightarrow$), ($\neg \Rightarrow$)}

   $\underline{\big((\neg P \vee \neg Q) \Rightarrow R\big)} \vee (P \wedge \neg R)$

   $\equiv$ {(Elim-$\Rightarrow$),(De Morgan)}

   $(P \wedge Q) \vee \underline{R \vee (P \wedge \neg R)}$

   $\equiv$ {(Complemento)}

   $\underline{(P \wedge Q)} \vee (P \vee R)$

   $\Rightarrow$ {(Sempl-$\wedge$), occ. pos.}

   $\underline{P \vee P} \vee R$

   $\equiv$ {(Idempotenza)}

   $P \vee R$

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

   $\neg P \Rightarrow R$

2. La formula non è una tautologia. Per mostrarlo basta trovare una interpretazione che renda falsa la formula (un *controesempio*). Per esempio: $P = \mathbf{F}$, $Q = \mathbf{T}$ e $R = \mathbf{F}$.

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

- $\alpha(g)$ è la persona Gianni,
- $\alpha(P)(p, q)$ è vera se e solo se la persona p è parente di q,
- $\alpha(F)(p, q)$ è vera se e solo se la persona p si fida di q,

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

"Gianni si fida di tutti quelli che si fidano di qualche suo parente,
ma non si fida dei suoi parenti che non si fidano si se stessi."

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

$$(\forall x\,.\,(\exists p\,.\,P(g,p) \wedge F(x,p)) \;\Rightarrow\; F(g,x)) \wedge (\forall y\,.\,(P(g,y) \wedge \neg F(y,y)) \;\Rightarrow\; \neg F(g,y))$$

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

$$(\forall x\,.\,P \vee R \Rightarrow Q) \;\wedge\; (\exists x\,.\,Q \vee R \Rightarrow R) \;\Rightarrow\; (\exists x\,.\,P \Rightarrow R)$$

SOLUZIONE ESERCIZIO 3

Utilizzando la regola della **Skolemizzazione** è sufficiente dimostrare che:

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

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

$(\forall x\,.\,P \vee R \Rightarrow Q) \wedge \underline{(\exists x\,.\,Q \vee R \Rightarrow R)} \wedge (Q(a) \vee R(a) \Rightarrow R(a))$
$\Rightarrow$ {(Sempl-$\wedge$), occor. pos.}
$(\forall x\,.\,P \vee R \Rightarrow Q) \wedge \underline{(Q(a) \vee R(a) \Rightarrow R(a))}$
$\equiv$ {(Elim- $\Rightarrow$),(De Morgan)}
$(\forall x\,.\,P \vee R \Rightarrow Q) \wedge \underline{\big((\neg Q(a) \wedge \neg R(a)) \vee R(a)\big)}$
$\Rightarrow$ {(Complemento)}
$(\forall x\,.\,P \vee R \Rightarrow Q) \wedge \underline{(\neg Q(a) \vee R(a))}$
$\equiv$ {(Elim- $\Rightarrow$)}
$\underline{(\forall x\,.\,P \vee R \Rightarrow Q)} \wedge (Q(a) \Rightarrow R(a))$
$\Rightarrow$ {(Elim-$\forall$), occor. pos.}
$\underline{(P(a) \vee R(a) \Rightarrow Q(a))} \wedge (Q(a) \Rightarrow R(a))$
$\Rightarrow$ {(Intro-$\vee$), occor. neg. }
$\underline{(P(a) \Rightarrow Q(a))} \wedge (Q(a) \Rightarrow R(a))$
$\Rightarrow$ {(Trans.-$\Rightarrow$), occor. pos.}
$\underline{P(a) \Rightarrow R(a))}$
$\Rightarrow$ {(Intro-$\exists$), occor. pos. }
$(\exists x\,.\,P \Rightarrow R)$

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

"Ogni elemento dell'array **b** è multiplo della somma di un intervallo di elementi di **a**"

Per un *intervallo di elementi* si intende un insieme $\{a[x] \mid i \leq x \leq j\}$ per qualche $i, j \in [0, n)$ con $i \leq j$.

SOLUZIONE ESERCIZIO 4

$$\big(\forall x\,.\,x \in [0,n) \;\Rightarrow\; (\exists i\,.\,i \in [0,n) \;\wedge (\exists j\,.\,j \in [i,n) \wedge (b[x]\,mod\,(\Sigma y : y \in [i,j]\,.\,a[y])) = 0))\big)$$

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

$\{c = 0 \;\wedge\; y = 0\}$
$\{\mathsf{Inv}\colon\ y \in [0,n] \;\wedge\; \big(c = (\Sigma i : i \in [0,y) \wedge pari(i)\,.\,a[i])\big)\}\{\mathsf{t}\colon\ n - y\}$
`while y < n do`

```
    if (y mod 2 = 0)
        then c, y := c+a[y], y+1
        else y := y+1
    fi
endw
```
$\{c = (\Sigma i : i \in [0,n) \wedge pari(i)\,.\,a[i])\}$

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

SOLUZIONE ESERCIZIO 5

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

1. **Ipotesi di Invarianza**:

$\{y \in [0,n] \ \wedge \ \big(c = (\Sigma i : i \in [0,y) \wedge pari(i)\,.\,a[i])\big) \wedge y < n\}$
```
    if (y mod 2 = 0)
        then c, y := c+a[y], y+1
        else y := y+1   fi
```
$\{y \in [0,n] \ \wedge \ \big(c = (\Sigma i : i \in [0,y) \wedge pari(i)\,.\,a[i])\big) \wedge def(y < n)\ \}$

2. **Ipotesi di Progresso**:

$\{y \in [0,n] \ \wedge \ \big(c = (\Sigma i : i \in [0,y) \wedge pari(i)\,.\,a[i])\big) \ \wedge \ y < n \ \wedge \ n - y = V\}$
```
    if (y mod 2 = 0)
        then c, y := c+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) $Inv \wedge y < n \ \Rightarrow \ def(y \ mod \ 2 = 0)$

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

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

(5.1.1) Abbiamo che

$def(y \ mod \ 2 = 0)$

$\equiv$ {definizione di *def*}

T

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

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

Partiamo dalla conseguenza

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

$\equiv$ {definizione di def}

$\underline{y \in [0,n) \wedge \mathbf{T}} \wedge \big(Inv \wedge def(y < n)\big)^{[c+a[y],y+1}/_{c,y]}$

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

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

$\equiv$ {definizione di def, sostituzione}

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

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

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

$\equiv$ {(Intervallo-Σ), **Ip**: $y \ mod \ 2 = 0$ }

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

$\equiv$ {calcolo}

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

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

T

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

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

Partiamo dalla conseguenza

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

$\equiv$ {sostituzione, definizione di def}

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

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

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

$\equiv$ {(Intervallo-Σ), **Ip**: $\neg(y \, mod \, 2 = 0)$ }

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

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

T

ESERCIZIO 6
Si verifichi la seguente tripla di Hoare (assumendo **a, b: array [0, n) of int**):

$\{$
$x \in [1, n)$
$\wedge \ \big(\forall j \, . \, j \in [1, n) \ \Rightarrow \ \mathtt{a}[j] = (\Sigma y : y \in [0, j) \, . \, \mathtt{a}[y])\big)$
$\wedge \ \big(\forall i \, . \, i \in [0, x) \ \Rightarrow \ \mathtt{b}[i] = 2 * (\Sigma y : y \in [0, i) \, . \, \mathtt{a}[y])\big)$
$\}$

```
b[x] := a[x] * 2
```

$\{\big(\forall i \, . \, i \in [0, x] \ \Rightarrow \ \mathtt{b}[i] = 2 * (\Sigma y : y \in [0, i) \, . \, \mathtt{a}[y])\big)\}$

SOLUZIONE ESERCIZIO 6

Applicando la regola dell' **Aggiornamento Selettivo** dobbiamo verificare che:

$$x \in [1, n) \ \wedge \ P \ \wedge \ Q \quad \Rightarrow \quad x \in dom(\mathtt{b}) \ \wedge \ def(x) \ \wedge \ def(\mathtt{a}[x] * 2) \ \wedge \ R[^{\mathtt{c}}/_{\mathtt{b}}]$$

dove

- $\mathtt{c} = \mathtt{b}[^{\mathtt{a}[x]*2}/_{x}]$,

- $P = \big(\forall j \,.\, j \in [1, n) \Rightarrow (\mathtt{a}[j] = (\Sigma y : y \in [0, j) \,.\, \mathtt{a}[y]))\big)$,
- $Q = \ \big(\forall i \,.\, i \in [0, x) \ \Rightarrow\ \mathtt{b}[i] = 2 * (\Sigma y : y \in [0, i) \,.\, \mathtt{a}[y])\big)$ e
- $R = \big(\forall i \,.\, i \in [0, x] \ \Rightarrow\ \mathtt{b}[i] = 2 * (\Sigma y : y \in [0, i) \,.\, \mathtt{a}[y])\big)$.

Partiamo dalla conseguenza

$$
\begin{array}{ll}
 & x \in dom(\mathtt{b}) \ \wedge\ \underline{def(x) \ \wedge\ def(\mathtt{a}[x] * 2)} \ \wedge\ R[^{\mathtt{c}}/_{\mathtt{b}}] \\
\equiv & \{\text{definizione di } def\} \\
 & \underline{x \in dom(\mathtt{b}) \ \wedge\ x \in dom(\mathtt{a})} \ \wedge\ R[^{\mathtt{c}}/_{\mathtt{b}}] \\
\equiv & \{\mathbf{Ip}\text{: } x \in [1, n) \ \wedge\ dom(\mathtt{a}) = dom(\mathtt{b}) = [0, n)\} \\
 & R[^{\mathtt{c}}/_{\mathtt{b}}] \\
\equiv & \{\text{sostituzione}\} \\
 & \underline{\big(\forall i \,.\, i \in [0, x] \ \Rightarrow\ \mathtt{c}[i] = 2 * (\Sigma y : y \in [0, i) \,.\, \mathtt{a}[y])\big)} \\
\equiv & \{(\text{Intervallo-}\forall), \mathbf{Ip}\text{: } x > 0\} \\
 & \big(\forall i \,.\, i \in [0, x) \ \Rightarrow\ \mathtt{c}[i] = 2 * (\Sigma y : y \in [0, i) \,.\, \mathtt{a}[y])\big) \ \wedge\ \mathtt{c}[x] = \underline{2 * (\Sigma y : y \in [0, x) \,.\, \mathtt{a}[y])} \\
\equiv & \{\mathbf{Ip}\text{: } P, \mathbf{Ip}\text{: } x \in [1, n) \ \} \\
 & \big(\forall i \,.\, i \in [0, x) \ \Rightarrow\ \mathtt{c}[i] = 2 * (\Sigma y : y \in [0, i) \,.\, \mathtt{a}[y])\big) \ \wedge\ \mathtt{c}[x] = 2 * \mathtt{a}[x]) \\
\equiv & \{\text{definizione di } \mathtt{c},\ i \neq x \text{ per ogni } i \in [0, x)\} \\
 & \big(\forall i \,.\, i \in [0, x) \ \Rightarrow\ \mathtt{b}[i] = 2 * (\Sigma y : y \in [0, i) \,.\, \mathtt{a}[y])\big) \ \wedge\ \mathtt{a}[x] * 2 = 2 * \mathtt{a}[x]) \\
\equiv & \{\mathbf{Ip}\text{: } Q, \text{ calcolo } \} \\
 & \mathbf{T}
\end{array}
$$