LOGICA PER LA PROGRAMMAZIONE - a.a. 2017-2018
Primo Appello - 18/01/2018 — 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. $\neg P \wedge (\neg(\neg Q \vee S) \Rightarrow P \wedge \neg R) \;\Rightarrow\; R \vee \neg Q$
2. $\big(\neg(P \Rightarrow Q) \Rightarrow (R \wedge \neg Q)\big) \wedge (P \;\Rightarrow\; Q)\neg(S \vee R)\big) \;\Rightarrow\; \big(\neg S \Rightarrow \neg P \vee Q\big)$

SOLUZIONE ESERCIZIO 1

1. La formula non è una tautologia. Per mostrarlo basta trovare una interpretazione che renda falsa la formula (un *controesempio*). Per esempio: $P = \mathbf{F}$, $Q = \mathbf{T}$, $R = \mathbf{F}$ e $S = \mathbf{T}$.
2. La formula è una tautologia. Sviluppiamo una dimostrazione partendo dalla premessa dell'implicazione per arrivare alla conclusione:

$$
\begin{array}{ll}
 & \big(\neg(P \Rightarrow Q) \Rightarrow (R \wedge \neg Q)\big) \wedge \big(S \vee \underline{\neg(S \vee R)}\big) \\
\equiv & \{(\text{De Morgan})\} \\
 & \big(\neg(P \Rightarrow Q) \Rightarrow (R \wedge \neg Q)\big) \wedge \underline{\big(S \vee (\neg S \wedge \neg R)\big)} \\
\equiv & \{(\text{Complemento})\} \\
 & \underline{\big(\neg(P \Rightarrow Q) \Rightarrow (R \wedge \neg Q)\big)} \wedge (S \vee \neg R) \\
\equiv & \{(\text{Elim-} \Rightarrow),(\text{Doppia Negazione})\} \\
 & \big((P \Rightarrow Q) \vee \underline{(R \wedge \neg Q)}\big) \wedge (S \vee \neg R) \\
\Rightarrow & \{(\text{Sempl-}\wedge), \text{ occ. pos.}\} \\
 & \underline{\big((P \Rightarrow Q) \vee R\big) \wedge (S \vee \neg R)} \\
\Rightarrow & \{(\text{Risoluzione}), \text{ occ. pos.}\} \\
 & \underline{(P \Rightarrow Q)} \vee S \\
\equiv & \{(\text{Elim-} \Rightarrow)\} \\
 & \underline{(\neg P \vee Q) \vee S} \\
\equiv & \{(\text{Elim-} \Rightarrow)\} \\
 & \neg S \;\Rightarrow\; \neg P \vee Q
\end{array}
$$

ESERCIZIO 2

Si consideri l'alfabeto del primo ordine $\mathcal{A}$ con simboli di predicato $\mathcal{P} = \{stud(-), univ(-), iscr(-,-), =(-,-)\}$ e l'interpretazione $I = (\mathcal{D}, \alpha)$, dove $\mathcal{D}$ è l'insieme studenti e delle università, e

- $\alpha(stud)(p)$ è vera se e solo se p è uno studente,
- $\alpha(univ)(p)$ è vera se e solo se p è una università,
- $\alpha(iscr)(p, q)$ è vera se e solo se lo studente p è iscritto all'università q,
- $\alpha(=)(p, q)$ è vera se e solo se p e q sono uguali.

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

"Ogni studente è iscritto ad una università e ogni università ha almeno due studenti iscritti"

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

$$(\forall x\, .\, stud(x) \;\Rightarrow\; (\exists y.\, univ(y) \wedge iscr(x,y))) \wedge (\forall w\, .\, univ(w) \;\Rightarrow\; (\exists v.\, \exists z.\, stud(v) \wedge stud(z) \wedge \neg(v=z) \wedge iscr(v,w) \wedge iscr(z,w)))$$

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

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

SOLUZIONE ESERCIZIO 3

Semplifichiamo la conseguenza:

$$\begin{array}{ll}
& (\exists x\, .\, Q) \vee \underline{\neg(\forall x\, .\, P)} \\
\equiv & \{(\text{De Morgan})\} \\
& (\exists x\, .\, Q) \vee (\exists x\, .\, \neg P) \\
\equiv & \{(\exists : \vee)\} \\
& (\exists x\, .\, Q \vee \neg P)
\end{array}$$

A questo punto utilizzando la regola della **Skolemizzazione** è sufficiente dimostrare che:

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

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

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

$(\exists x\,.\,\neg P \vee Q)$

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

"Per ogni elemento dell'array **a** esiste un elemento in **b** che è minore della somma degli elementi di **a** che lo precedono ed uno che è uguale al minimo tra gli elementi pari di **a** che lo seguono."

SOLUZIONE ESERCIZIO 4

$$\big(\forall x.\ x \in [0,n) \ \Rightarrow\ (\exists y.y \in [0,n) \wedge b[y] < (\Sigma i : i \in [0,x).a[i])) \wedge (\exists z.z \in [0,n) \wedge b[z] = (\mathbf{min}\, i : i \in [x,n) \wedge pari(a[i]).a[i]))\big)$$

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

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

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

$\{\big(c = \#\{i : i \in [0,n) \mid pari(i) \wedge a[i]^2 > b[i]\}\big)\}$

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

SOLUZIONE ESERCIZIO 5

Invariante $Inv : y \in [0,n] \ \wedge\ \big(c = \#\{i : i \in [0,y) \mid pari(i) \wedge a[i]^2 > b[i]\}\big)$
Funzione di terminazione $t : n - y$

1. **Ipotesi di Invarianza**:

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

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

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

2. **Ipotesi di Progresso**:

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

```
if (y mod 2 = 0 ∧ a[y] * a[y] > b[y])
 then c, y := c+1, 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) $Inv \wedge y < n \ \Rightarrow\ def(y \ mod\ 2 = 0 \wedge\ a[y] * a[y] > b[y])$

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

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

(5.1.1) Abbiamo che

$$\begin{aligned}
& def(y \ mod \ 2 = 0 \wedge \ a[y] * a[y] > b[y]) \\
\equiv \quad & \{\text{definizione di } def\} \\
& y \in dom(a) \wedge y \in dom(b) \wedge 2 \neq 0 \\
\equiv \quad & \{\mathbf{Ip}\text{: } dom(a) = dom(b) = [0, n), y \in [0, n], y < n\} \\
& \mathbf{T}
\end{aligned}$$

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

$$Inv \wedge y < n \wedge y \ mod \ 2 = 0 \wedge \ a[y] * a[y] > b[y] \ \Rightarrow$$

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

Partiamo dalla conseguenza

$$\begin{aligned}
& def(c + 1) \wedge def(y + 1) \wedge \big(Inv \wedge def(y < n)\big)[^{c+1, y+1}/_{c,y}] \\
\equiv \quad & \{\text{sostituzione, definizione di } def\} \\
& \underline{y + 1 \in [0, n]} \ \wedge \ \big(c + 1 = \#\{i : i \in [0, y + 1) \mid pari(i) \wedge a[i]^2 > b[i]\}\big) \\
\equiv \quad & \{\mathbf{Ip}\text{: } y \in [0, n], y < n\} \\
& c + 1 = \underline{\#\{i : i \in [0, y + 1) \mid pari(i) \wedge a[i]^2 > b[i]\}} \\
\equiv \quad & \{(\text{Intervallo-}\#), \mathbf{Ip}\text{: } y \ mod \ 2 = 0 \wedge \ a[y] * a[y] > b[y] \ \} \\
& c + 1 = \underline{\#\{i : i \in [0, y) \mid pari(i) \wedge a[i]^2 > b[i]\}} + 1 \\
\equiv \quad & \Big\{\mathbf{Ip}\text{: } c = \#\{i : i \in [0, y) \mid pari(i) \wedge a[i]^2 > b[i]\}\Big\} \\
& \mathbf{T}
\end{aligned}$$

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

$$Inv \wedge y < n \wedge \neg(y \ mod \ 2 = 0 \wedge \ a[y] * a[y] > b[y]) \ \Rightarrow$$

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

Partiamo dalla conseguenza

$$\begin{aligned}
& def(y + 1) \wedge \big(Inv \wedge def(y < n)\big)[^{y+1}/_{y}] \\
\equiv \quad & \{\text{sostituzione, definizione di } def\} \\
& \underline{y + 1 \in [0, n]} \ \wedge \ \big(c = \#\{i : i \in [0, y + 1) \mid pari(i) \wedge a[i]^2 > b[i]\}\big) \\
\equiv \quad & \{\mathbf{Ip}\text{: } y \in [0, n], y < n\} \\
& c = \underline{\#\{i : i \in [0, y + 1) \mid pari(i) \wedge a[i]^2 > b[i]\}} \\
\equiv \quad & \{(\text{Intervallo-}\#), \mathbf{Ip}\text{: } \neg(y \ mod \ 2 = 0 \wedge \ a[y] * a[y] > b[y]) \ \} \\
& c = \underline{\#\{i : i \in [0, y) \mid pari(i) \wedge a[i]^2 > b[i]\}} \\
\equiv \quad & \Big\{\mathbf{Ip}\text{: } \big(c = \#\{i : i \in [0, y) \mid pari(i) \wedge a[i]^2 > b[i]\}\big)\Big\} \\
& \mathbf{T}
\end{aligned}$$

ESERCIZIO 6

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

$\{h \in [1,k) \ \wedge \ \big(\forall i \,.\, i \in [0,h) \Rightarrow c[i] > (\Sigma y : y \in [0,i] \,.\, a[y])\big)\}$

```
c[h] := c[h-1] + a[h] + 1
```

$\{\big(\forall i \,.\, i \in [0,h] \Rightarrow c[i] > (\Sigma y : y \in [0,i] \,.\, a[y])\big)\}$

SOLUZIONE ESERCIZIO 6

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

$$h \in [1,k) \ \wedge \ \big(\forall i \,.\, i \in [0,h) \Rightarrow c[i] > (\Sigma y : y \in [0,i] \,.\, a[y])\big) \Rightarrow$$

$$h \in dom(c) \wedge def(h) \wedge def(c[h-1] + a[h] + 1) \wedge R[^b/_c]$$

dove $b = c[^{c[h-1]+a[h]+1}/_h]$ e $R = \big(\forall i \,.\, i \in [0,h] \Rightarrow c[i] > (\Sigma y : y \in [0,i] \,.\, a[y])\big)$.
Partiamo dalla conseguenza

$$
\begin{array}{ll}
 & h \in dom(c) \wedge \underline{def(h) \wedge def(c[h-1] + a[h] + 1)} \wedge R[^b/_c] \\
\equiv & \{\text{definizione di } def\} \\
 & \underline{h \in dom(c) \wedge h-1 \in dom(c) \wedge h \in dom(a)} \wedge R[^b/_c] \\
\equiv & \{\textbf{Ip}\text{: } h \in [1,k) \wedge dom(a) = dom(c) = [0,k)\} \\
 & R[^b/_c] \\
\equiv & \{\text{sostituzione}\} \\
 & \underline{\big(\forall i \,.\, i \in [0,h] \Rightarrow b[i] > (\Sigma y : y \in [0,i] \,.\, a[y])\big)} \\
\equiv & \{(\text{Intervallo-}\forall), \textbf{Ip}\text{: } h > 0\} \\
 & \big(\forall i \,.\, i \in [0,h) \Rightarrow \underline{b[i]} > (\Sigma y : y \in [0,i] \,.\, a[y])\big) \wedge \underline{b[h]} > (\Sigma y : y \in [0,h] \,.\, a[y]) \\
\equiv & \{\text{definizione di } b\} \\
 & \underline{\big(\forall i \,.\, i \in [0,h) \Rightarrow c[i] > (\Sigma y : y \in [0,i] \,.\, a[y])\big)} \wedge c[h-1] + a[h] + 1 > (\Sigma y : y \in [0,h] \,.\, a[y]) \\
\equiv & \big\{\textbf{Ip}\text{: } \big(\forall i \,.\, i \in [0,h) \Rightarrow c[i] > (\Sigma y : y \in [0,i] \,.\, a[y])\big)\big\} \\
 & c[h-1] + a[h] + 1 > \underline{(\Sigma y : y \in [0,h] \,.\, a[y])} \\
\equiv & \{(\text{Intervallo-}\Sigma)\} \\
 & c[h-1] + a[h] + 1 > (\Sigma y : y \in [0,h-1] \,.\, a[y]) + a[h] \\
\equiv & \{\textbf{Ip}\text{: } c[h-1] > (\Sigma y : y \in [0,h-1] \,.\, a[y]), \text{calcolo}\} \\
 & \mathbf{T}
\end{array}
$$