LOGICA PER LA PROGRAMMAZIONE - a.a. 2019-2020
Primo Appello - 10/01/2019 - 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 mostrando esplicitamente che rende la formula falsa.

1. $\neg(A \Rightarrow (B \vee C) \wedge \neg D) \;\Rightarrow\; (\neg D \Rightarrow C)$
2. $(A \wedge \neg C \Rightarrow B) \wedge (\neg D \Rightarrow \neg B) \wedge \neg D \;\Rightarrow\; (A \Rightarrow C)$

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: $A = \mathbf{T}$, $B = \mathbf{F}$, $C = \mathbf{F}$ e $D = \mathbf{F}$.
2. La formula è una tautologia. Sviluppiamo una dimostrazione partendo dalla premessa dell'implicazione per arrivare alla conclusione:

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

$\Rightarrow$ {(Modus Ponens), occ. positiva}

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

$\equiv$ {(Contropositiva)}

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

$\Rightarrow$ {(Modus Ponens)}

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

$\equiv$ {(De Morgan)}

$\neg A \vee C$

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

$A \Rightarrow C$

ESERCIZIO 2
Si consideri l'alfabeto del primo ordine $\mathcal{A}$ con simboli di predicato $\mathcal{P} = \{L(-), K(-), A(-,-)\}$ e l'interpretazione $I = (\mathcal{D}, \alpha)$, dove $\mathcal{D}$ è l'insieme di tutti i lucchetti e tutte le chiavi, e

- $\alpha(L)(d)$ è vera se e solo se d è un lucchetto
- $\alpha(K)(d)$ è vera se e solo se d è una chiave
- $\alpha(A)(d_1, d_2)$ è vera se e solo se il d_2 è un lucchetto e d_1 è una chiave che lo apre.

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

"Ogni lucchetto ha almeno una chiave che lo apre, ma non esiste una chiave che apra tutti i lucchetti."

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

$$(\forall x \,.\, L(x) \Rightarrow (\exists y \,.\, K(y) \wedge A(y,x))) \wedge \neg(\exists z \,.\, K(z) \wedge (\forall w \,.\, L(w) \Rightarrow A(z,w)))$$

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

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

Suggerimento: potrebbe essere utile la legge $A \Rightarrow B \vee C \;\equiv\; A \wedge \neg B \Rightarrow C$

SOLUZIONE ESERCIZIO 3

1. Sfruttando la legge suggerita, dimostriamo la formula

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

$\equiv$ {De Morgan}

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

Per la regola di **Skolemizzazione** è sufficiente dimostrare:

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

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

$$(\forall x \,.\, \neg P \vee \neg Q \vee R) \wedge \underline{(\exists x \,.\, \neg P \vee Q)} \wedge (\neg P(a) \vee Q(a))$$

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

$$\underline{(\forall x \,.\, \neg P \vee \neg Q \vee R)} \wedge (\neg P(a) \vee Q(a))$$

$\Rightarrow$ {(Elim-$\forall$), occor. pos.}

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

$\Rightarrow$ {(Risoluzione), occor. pos.}

$$\underline{\neg P(a)} \vee R(a) \vee \underline{\neg P(a)}$$

$\Rightarrow$ {(Idempotenza)}

$$\neg P(a) \vee R(a)$$

$\Rightarrow$ {(Intro-$\exists$), occor. pos. }

$$(\exists x \,.\, \underline{\neg P \vee R})$$

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

$$(\exists x \,.\, P \Rightarrow R)$$

2. Come dimostrazione alternativa, partiamo dalla formula data eliminando l'implicazione:

$$
\begin{array}{ll}
 & (\forall x \,.\, \neg P \vee \neg Q \vee R) \;\Rightarrow\; (\exists x \,.\, P \Rightarrow R) \vee (\forall x \,.\, P \wedge \neg Q) \\
\equiv & \{(\text{Elim-}\Rightarrow)\} \\
 & \underline{\neg(\forall x \,.\, \neg P \vee \neg Q \vee R)} \vee (\exists x \,.\, \underline{P \Rightarrow R}) \vee (\forall x \,.\, P \wedge \neg Q) \\
\equiv & \{(\text{De Morgan}), (\text{Elim-}\Rightarrow)\} \\
 & \underline{(\exists x \,.\, P \wedge Q \wedge \neg R)} \vee (\exists x \,.\, \neg P \vee R) \vee (\forall x \,.\, P \wedge \neg Q) \\
\equiv & \{(\exists : \vee)\} \\
 & (\exists x \,.\, (\underline{P} \wedge Q \wedge \underline{\neg R}) \vee (\underline{\neg P \vee R})) \vee (\forall x \,.\, P \wedge \neg Q) \\
\equiv & \{(\text{Complemento})\} \\
 & (\exists x \,.\, Q \vee \neg P \vee R) \vee \underline{(\forall x \,.\, P \wedge \neg Q)} \\
\equiv & \{(\text{De Morgan}), (\text{Doppia Negazione})\} \\
 & (\exists x \,.\, Q \vee \neg P \vee R) \vee \neg(\exists x \,.\, \neg P \vee Q) \\
\equiv & \{(\exists : \vee)\} \\
 & (\exists x \,.\, R) \vee \underline{(\exists x \,.\, Q \vee \neg P) \vee \neg(\exists x \,.\, \neg P \vee Q)} \\
\equiv & \{(\text{Terzo Escluso}), (\text{Zero})\} \\
 & \mathbf{T}
\end{array}
$$

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

"Ogni elemento di **a** compare anche in **b**, ma un numero diverso di volte."

SOLUZIONE ESERCIZIO 4

$$\big(\forall x \,.\, x \in [0, n) \;\Rightarrow\; (\exists y \,.\, y \in [0, k) \wedge b[y] = a[x]) \wedge \neg(\#\{i \colon i \in [0, n) \mid a[i] = a[x]\} = \#\{j \colon j \in [0, k) \mid b[j] = a[x]\})\big)$$

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

$\{c = 0 \;\wedge\; y = 0\}$

$\{\mathsf{Inv}\colon\ y \in [0, n] \;\wedge\; \big(c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge \mathit{dispari}(a[i])\}\big)\}\{\text{t: } n - y\}$

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

$\{c = \#\{i \colon i \in [0, n) \mid a[i] > 0 \wedge \mathit{dispari}(a[i])\}\}$

Si scrivano le ipotesi di progresso ed invarianza. Inoltre si dimostri l'ipotesi di invarianza **limitatamente alle due prime condizioni della regola del comando condizionale (si ignori il ramo else)**.

SOLUZIONE ESERCIZIO 5

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

1. **Ipotesi di Invarianza**:

$\{y \in [0, n] \;\wedge\; \big(c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}\big) \wedge y < n\}$
```
    if (a[y] > 0)
        then c, y := c + a[y] mod 2, y+1
        else y := y+1
```
$\{y \in [0, n] \;\wedge\; \big(c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}\big) \wedge def(y < n)\;\}$

2. **Ipotesi di Progresso**:

$\{y \in [0, n] \;\wedge\; \big(c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}\big) \wedge y < n \;\wedge\; n - y = V\}$
```
    if (a[y] > 0)
        then c, y := c + a[y] mod 2, y+1
        else y := y+1
```
$\{n - y < V\}$

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

(5.1.1) $Inv \wedge y < n \;\Rightarrow\; def(a[y] > 0)$

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

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

(5.1.1) Partiamo dalla conseguenza:

$def(a[y] > 0)$

$\equiv$ {definizione di *def*}

$y \in dom(a)$

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

T

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

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

Partiamo dalla conseguenza

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

$\equiv$ {definizione di def, $dom(a) = [0, n)$}

$\underline{y \in [0, n) \wedge \mathbf{T}} \wedge \big(Inv \wedge def(y < n)\big)[^{c+a[y]\ mod\ 2, y+1}/_{c,y}]$

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

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

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

$\underline{y+1 \in [0,n]} \;\wedge\; \big(c + a[y]\ mod\ 2 = \#\{i \colon i \in [0, y+1) \mid a[i] > 0 \wedge dispari(a[i])\}\big) \wedge \underline{def(y+1 < n)}$

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

$(\dagger)\quad c + a[y]\ mod\ 2 = \#\{i \colon i \in [0, y+1) \mid a[i] > 0 \wedge dispari(a[i])\}$

Abbiamo due casi. (1) Se $a[y]$ è dispari, allora $a[y]\ mod\ 2 = 1$ e quindi

$(\dagger)\quad c + \underline{a[y]\ mod\ 2} = \underline{\#\{i \colon i \in [0, y+1) \mid a[i] > 0 \wedge dispari(a[i])\}}$

$\equiv$ $\{$(Intervallo-#), **Ip**: $a[y] > 0, dispari(a[y])$ $\}$

$c + 1 = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\} + 1$

$\equiv$ $\{$calcolo, **Ip**: $c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}\}$

T

(2) Se invece $a[y]$ è pari, allora $a[y]\ mod\ 2 = 0$ e quindi

$(\dagger)\quad c + \underline{a[y]\ mod\ 2} = \underline{\#\{i \colon i \in [0, y+1) \mid a[i] > 0 \wedge dispari(a[i])\}}$

$\equiv$ $\{$(Intervallo-#), **Ip**: $a[y] > 0, pari(a[y])$ $\}$

$c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}$

$\equiv$ $\{$**Ip**: $c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}\}$

T

(5.1.3) Anche se non richiesto dal testo dell'esercizio, per completezza riportiamo anche la prova del ramo *else*.
Per dimostrare la tripla applichiamo la regola dell' **Assegnamento** e ci riduciamo a dimostrare

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

Partiamo dalla conseguenza

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

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

$\underline{y+1 \in [0,n]} \;\wedge\; \big(c = \#\{i \colon i \in [0, y+1) \mid a[i] > 0 \wedge dispari(a[i])\}\big) \wedge \underline{def(y+1 < n)}$

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

$c = \underline{\#\{i \colon i \in [0, y+1) \mid a[i] > 0 \wedge dispari(a[i])\}}$

$\equiv$ $\{$(Intervallo-#), **Ip**: $\neg(a[y] > 0)$ $\}$

$c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}$

$\equiv$ $\{$**Ip**: $c = \#\{i \colon i \in [0, y) \mid a[i] > 0 \wedge dispari(a[i])\}\}$

T

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

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

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

$\{(\Sigma i\colon i \in [0,x)\,.\,a[i]) = x^2\}$

SOLUZIONE ESERCIZIO 6

Applicando la regola della **Sequenza** è sufficiente trovare un'asserzione R che ci permetta di verificare:

(6.1) $\{x \in [0,n)\ \wedge\ (\Sigma i\colon i \in [0,x)\,.\,a[i]) = x^2\}$ `a[x] := 2 * x + 1` $\{R\}$

(6.2) $\{R\}$ `x := x + 1` $\{(\Sigma i\colon i \in [0,x)\,.\,a[i]) = x^2\}$

Applicando l'Assioma dell'Assegnamento alla seconda tripla, abbiamo che essa è soddisfatta per la formula $R \equiv \mathit{def}(x+1) \wedge \big((\Sigma i\colon i \in [0,x)\,.\,a[i]) = x^2\big)\,[^{x+1}/_x]$

Semplificando:

R

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

$(\Sigma i\colon i \in [0,x+1)\,.\,a[i]) = (x+1)^2$

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

$(\Sigma i\colon i \in [0,x]\,.\,a[i]) = x^2 + 2x + 1$

Per la tripla (6.1), applicando la regola dell' **Aggiornamento Selettivo** è sufficiente verificare che:

$$x \in [0,n)\ \wedge\ (\Sigma i\colon i \in [0,x)\,.\,a[i]) = x^2 \quad \Rightarrow \quad x \in \mathit{dom}(a)\ \wedge\ \mathit{def}(x)\ \wedge\ \mathit{def}(a[x] := 2*x+1)\ \wedge\ R[^b/_a]$$

dove $b = a[^{2*x+1}/_x]$ e $R \equiv (\Sigma i\colon i \in [0,x]\,.\,a[i]) = x^2 + 2x + 1$.
Partiamo dalla conseguenza

$x \in \mathit{dom}(a)\ \wedge\ \underline{\mathit{def}(x)}\ \wedge\ \underline{\mathit{def}(a[x] := 2*x+1)}\ \wedge\ R[^b/_a]$

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

$\underline{x \in \mathit{dom}(a)} \wedge R[^b/_a]$

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

$R[^b/_a]$

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

$\underline{(\Sigma i\colon i \in [0,x]\,.\,b[i])} = x^2 + 2x + 1$

$\equiv$ $\{$(Intervallo-Σ), **Ip**: $x > 0\}$

$(\Sigma i\colon i \in [0,x)\,.\,\underline{b[i]}) + \underline{b[x]} = x^2 + 2x + 1$

$\equiv$ $\{$definizione di b, $i \neq x$ per ogni $i \in [0,x)\}$

$\underline{(\Sigma i\colon i \in [0,x)\,.\,a[i])} + 2*x+1 = x^2 + 2x + 1$

$\equiv$ $\big\{$**Ip**: $(\Sigma i\colon i \in [0,x)\,.\,a[i]) = x^2\big\}$

$x^2 + 2*x + 1 = x^2 + 2x + 1$

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

T