ESERCIZIO 1
Assumendo che $P$, $Q$ e $R$ contengano la variabile libera $x$, si provi che la seguente formula è valida:

$$(\forall x. P \Rightarrow Q) \land \neg(\exists x. \neg(R \Rightarrow Q)) \land (\exists x. P) \Rightarrow (\exists x. \neg(Q \Rightarrow \neg P))$$

SOLUZIONE ESERCIZIO 1
Utilizzando la regola della Skolemizzazione è sufficiente dimostrare allora che

$$(\forall x. P \Rightarrow Q) \land \neg(\exists x. \neg(R \Rightarrow Q)) \land (\exists x. P)$$

con $a$ costante nuova. Intuitivamente, è come chiamare $a$ un elemento del dominio che testimonia la verità di $(\exists x. P)$.

Nel seguito indicheremo $P[a/x]$, cioè la formula $P$ dove $x$ è sostituita con $a$, anche come $P(a)$. Partiamo allora dalla premessa:

$$\Rightarrow \{\text{(sempl-\land)}\}$$

$$(\forall x. P \Rightarrow Q) \land (\exists x. \neg(R \Rightarrow Q)) \land (\exists x. P) \land P[a/x] \Rightarrow (\exists x. \neg(Q \Rightarrow \neg P))$$

ESERCIZIO 2
Assumendo $a$: array $[0, n)$ of nat con $n > 0$, si formalizzi il seguente enunciato:

“Nell’array $a$ c’è una posizione tale che la somma di tutti gli elementi dell’array fino a quella posizione compresa è uguale alla somma degli elementi che la seguono.”

Per esempio, dei seguenti array il primo soddisfa la proprietà, il secondo no:

<table>
<thead>
<tr>
<th>4</th>
<th>0</th>
<th>1</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

SOLUZIONE ESERCIZIO 2

$$(\exists i : i \in [0, n].(\Sigma j : j \in [0, i] . a[j]) = (\Sigma k : k \in (i, n) . a[k]))$$

ESERCIZIO 3
Si dica se la seguente tripla è verificata, motivando formalmente la risposta:

$$\{x = A \land y = B; x = x + y; y = x - y; x = x - y; x = B \land y = A\}$$
SOLUZIONE ESERCIZIO 3
Applicando due volte la Regola della Sequenza, dobbiamo trovare due asserzioni \( R_1 \) e \( R_2 \) tali che le seguenti triple siano verificate:

(3.1) \( \{ x = A \land y = B \} \ x := x + y \ \{ R_1 \} \)
(3.2) \( \{ R_1 \} \ y := x - y \ \{ R_2 \} \)
(3.3) \( \{ R_2 \} \ x := x - y \ \{ x = B \land y = A \} \)

Per determinare \( R_2 \), usiamo l’Assioma dell’Assegnamento nella (3.3):

\[
\{ def(x - y) \land (x = B \land y = A)^{[x-y/x]} \} \ x := x - y \ \{ x = B \land y = A \}
\]

La condizione \( R_2 \) è quindi

\[
def(x - y) \land (x = B \land y = A)^{[x-y/x]} \equiv \{ \text{sostituzione}, definizione di def} \ x - y = B \land y = A
\]

Per determinare \( R_1 \), usiamo ancora l’Assioma dell’Assegnamento:

\[
\{ def(x - y) \land (x - y = B \land y = A)^{[x-y/y]} \} \ y := x - y \ \{ x - y = B \land y = A \}
\]

La condizione \( R_1 \) è quindi

\[
x - (x - y) = B \land x - y = A \equiv \{ \text{calcolo} \} \ y = B \land x - y = A
\]

Resta da verificare:

\[
\{ x = A \land y = B \} \ x := x + y \ \{ y = B \land x - y = A \}
\]
e quindi, usando la Regola dell’Assegnamento, che

\[
x = A \land y = B \Rightarrow \{ x = B \land y = A \}^{[x+y/x]}
\]

Partiamo dalla conseguenza, applicando la sostituzione

\[
(y = B \land x+y - y = A) \equiv \{ \text{calcolo} \} \ (y = B \land x = A)
\]

ESERCIZIO 4
Assumendo \( a, b: \text{array} [0, n) \text{ of int} \), si consideri il seguente frammento di programma annotato:

\[
\{ \text{cond = true} \land z = 0 \}
\{ \text{inv:} (z \in [0, n]) \land (\text{cond} \equiv (\forall x. x \in [0, z) \Rightarrow a[x] = b[x])) \} \{ t: n - z \}
\]
while (z < n) do
    if not(a[z] = b[z])
    then cond := false
    else skip
    fi;
    z := z + 1
endw
\{ \text{cond} \equiv (\forall x. x \in [0, n) \Rightarrow a[x] = b[x]) \}

Si scriva e si dimostri l’ipotesi di invarianza.

SOLUZIONE ESERCIZIO 4
Invariante $\text{Inv} : (z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]))$

Funzione di terminazione $t : n - z$

Condizione $E : z < n$

Comando $C : \text{if...fi;} z := z + 1$

L’ipotesi di Invarianza $((\text{Inv} \land E) \Rightarrow (\text{Inv} \land \text{def}(E)))$ in questo caso è

$\{(z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \land (z < n)\}$

se not($a[z] = b[z]$) allora cond := false else skip fi; z := z + 1

$\{(z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \land \text{def}(z < n)\}$

Applicando la Regola della Sequenza, dobbiamo trovare una asserzione $R$ tali che le seguenti triple siano verificate:

(4.1) $\{(z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \land (z < n)\}$ if...fi {R}

(4.2) {R} z := z + 1 $\{(z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \land \text{def}(z < n)\}$

Per determinare $R$, usiamo l’Assioma dell’Assegnamento in (4.2) e troviamo che è

$\text{def}(z + 1) \land (z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \land \text{def}(z < n)[t^{z+1}/z]$

$\equiv$

$\{(\text{sostituzione, definizione di def})$

$(z + 1 \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]))\}

Ci resta da verificare la tripla (4.1) per il valore di $R$ appena calcolato. Applicando la Regola del Condizionale, dobbiamo verificare che

1. $P \Rightarrow \text{def}(\text{not}(a[z] = b[z]))$

2. $\{P \land (\text{not}(a[z] = b[z]))\} \text{cond} := \text{false} \{R\}$

3. $\{P \land \text{not}(a[z] = b[z])\} \text{skip} \{R\}$

1. La 1) è vera dato che:

$\text{def}(\text{not}(a[z] = b[z]))$

$\equiv$

$\{(\text{definizione di def})$

$\text{def}(a[z]) \land \text{def}(b[z])$

$\equiv$

$\{(\text{definizione di def})$

$\text{def}(z) \land z \in \text{dom}(a) \land z \in \text{dom}(b)$

$\equiv$

$\{(\text{definizione di def, Ip: dom}(a) = \text{dom}(b) = [0, n], z \in [0, n], z < n)\}$

T

2. Per dimostrare la 2) appliciamo la Regola dell’Assegnamento

$P \land (\text{not}(a[z] = b[z])) \Rightarrow \text{def}(\text{false}) \land ((z + 1 \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])))[\text{false/cond}]$

dove $P = (z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \land (z < n)$

Partiamo dalla conseguenza, applicando la sostituzione

$\text{def}(\text{false}) \land (z + 1 \in [0, n]) \land (\text{false} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]))$

$\equiv$

$\{(\text{definizione di def})$

$(z + 1 \in [0, n]) \land (\text{false} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]))$

$\equiv$

$\{(\text{Ip: } z \in [0, n]) \land (z < n)\}$

$\text{false} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])$

$\equiv$

$\{(\text{Intervallo-}\forall)\}$

$\text{false} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]) \land a[z] = b[z]$

$\equiv$

$\{(\text{Ip: } \text{not}(a[z] = b[z]))\}$

3
false ≡ (∀x.x ∈ [0, z) ⇒ a[x] = b[x]) ∧ F
≡ {calcolo}
false ≡ F
≡ {calcolo}
T

3. Per la 3), applicando l’Assioma del Comando Vuoto e la regola (PRE), dobbiamo dimostrare

\[ P \land \neg(\text{not}(a[z] = b[z])) \Rightarrow (z + 1 \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \]

dove \( P = (z \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \land (z < n) \)

Partiamo dalla conseguenza

\[ (z + 1 \in [0, n]) \land (\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])) \]
≡ \{ \text{Ip: } (z \in [0, n]) \land (z < n) \}
\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])
≡ \{ (\text{Intervallo-∀}) \}
\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]) \land (a[z] = b[z])
≡ \{ \text{Ip: } a[z] = b[z] \}
\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]) \land T
≡ \{ \text{Assorb.} \}
\text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x])
≡ \{ \text{Ip: } \text{cond} \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]) \}
T

ESERCIZIO 5
Assumendo \( b: \text{array} \ [0, n] \) of int, si verifichi la seguente tripla:

\{ x \in [1, n) \land (\forall i.i \in [0, x) \Rightarrow b[i] = i^2) \}
\( b[x] := b[x - 1] + 2 \cdot x - 1 \)
\{(\forall i.i \in [0, x) \Rightarrow b[i] = i^2)\}

SOLUZIONE ESERCIZIO 5
Sfruttando l’Assioma dell’Aggiornamento Selettivo, e la regola PRE, dobbiamo verificare che:

\[ x \in [1, n) \land (\forall i.i \in [0, x) \Rightarrow b[i] = i^2) \Rightarrow \]
\[ \text{def}(x) \land \text{def}(b[x - 1] + 2 \cdot x - 1) \land x \in \text{dom}(b) \land (\forall i.i \in [0, x] \Rightarrow b[i] = i^2)_{/b}^{b'} \]

dove \( b' = b[b[x-1]+2x-1/x] \).
Partiamo dalla conseguenza
\[ \text{def}(x) \land \text{def}(b[x - 1] + 2 \cdot x - 1) \land x \in \text{dom}(b) \land (\forall i.i \in [0, x] \Rightarrow b[i] = i^2)_{/b}^{b'} \]
≡ \{ definizione di def \}
\[ \text{def}(b[x - 1]) \land \text{def}(2 \cdot x - 1) \land x \in \text{dom}(b) \land (\forall i.i \in [0, x] \Rightarrow b[i] = i^2)_{/b}^{b'} \]
≡ \{ definizione di def \}
\[ \text{def}(x - 1) \land x - 1 \in \text{dom}(b) \land x \in \text{dom}(b) \land (\forall i.i \in [0, x] \Rightarrow b[i] = i^2)_{/b}^{b'} \]
≡ \{ definizione di def \}
\[ x - 1 \in \text{dom}(b) \land x \in \text{dom}(b) \land (\forall i \in [0, x] \Rightarrow b[i] = i^2)^{b'/b} \]

\[ \equiv \{ \text{Ip: } x \in [1, n) \land \text{dom}(b) = [0, n) \} \]

\[ (\forall i \in [0, x] \Rightarrow b[i] = i^2)^{b'/b} \]

\[ \equiv \{ \text{sostituzione} \} \]

\[ (\forall i \in [0, x] \Rightarrow b'[i] = i^2) \]

\[ \equiv \{ (\text{Intervallo-} \forall) \} \]

\[ (\forall i \in [0, x] \Rightarrow b'[i] = i^2) \land (b'[x] = x^2) \]

\[ \equiv \{ \text{definizione di } b' = b \left[ b[x-1] + 2 \times x - 1 \right] / x \} \]

\[ (\forall i \in [0, x] \Rightarrow b'[i] = i^2) \land (b[x-1] + 2 \times x - 1 = x^2) \]

\[ \equiv \{ \text{Ip: } (\forall i \in [0, x] \Rightarrow b'[i] = i^2) \} \]

\[ (b[x-1] + 2 \times x - 1 = x^2) \]

\[ \equiv \{ \text{calcolo} \} \]

\[ \text{T} \]