

# LOGICA PER LA PROGRAMMAZIONE – a.a. 2017/18

## Settima Esercitazione — 14/12/2017 — 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 consideri il seguente frammento di programma annotato

```
{x = 0 ∧ y = 0 ∧ n ≥ 0}
{Inv : y = x * n ∧ x ∈ [0, n]}{t: n - x}
while (x < n) do
  x, y := x + 1, y + n
endw
{y = n2}
```

1. Si scrivano le ipotesi di progresso, di invarianza e di terminazione.
2. Si dimostrino le ipotesi di progresso e di invarianza.

### SOLUZIONE ESERCIZIO 1

Invariante  $Inv : y = x * n \wedge x \in [0, n]$   
Funzione di terminazione  $t : n - x$   
Condizione  $E : x < n$   
Comando  $C : x, y := x + 1, y + n$   
Variabile di Specifica:  $V$  denota un generico valore

**Ipotesi di Progresso** ( $\{Inv \wedge E \wedge t = V\} C \{t < V\}$ )

$$\{y = x * n \wedge x \in [0, n] \wedge x < n \wedge n - x = V\}$$
$$x, y := x + 1, y + n$$
$$\{n - x < V\}$$

**Ipotesi di Invarianza** ( $\{Inv \wedge E\} C \{Inv \wedge def(E)\}$ )

$$\{y = x * n \wedge x \in [0, n] \wedge x < n\}$$
$$x, y := x + 1, y + n$$
$$\{y = x * n \wedge x \in [0, n] \wedge def(x < n)\}$$

**Ipotesi di Terminazione** ( $Inv \Rightarrow t \geq 0$ )

$$\{y = x * n \wedge x \in [0, n] \Rightarrow n - x \geq 0\}$$

- Per verificare l'Ipotesi di Progresso, sfruttiamo l'**Assioma dell'Assegnamento Multiplo**

(ASS - MULT)  $\{def(E_1) \wedge \dots \wedge def(E_k) \wedge P^{[E_1, \dots, E_k / x_1, \dots, x_k]}\} x_1, \dots, x_k := E_1, \dots, E_k \{P\}$

che richiede di valutare tutte le espressioni **prima** di tutti gli assegnamenti. Otteniamo quindi che la seguente tripla è automaticamente verificata:

$$\{def(x+1) \wedge def(y+n) \wedge (n-x < V)^{[x+1, y+n/x, y]}\} x, y := x+1, y+n \{n-x < V\}$$

Per la regola PRE

$$(PRE) \frac{P \Rightarrow P' \quad \{P'\} C \{R\}}{\{P\} C \{R\}}$$

ci rimane da dimostrare che

$$y = x * n \wedge x \in [0, n] \wedge x < n \wedge n - x = V \Rightarrow def(x+1) \wedge def(y+n) \wedge (n-x < V)^{[x+1, y+n/x, y]}$$

Partiamo dalla conseguenza:

$$\begin{aligned} & def(x+1) \wedge def(y+n) \wedge (n-x < V)^{[x+1, y+n/x, y]} \\ \equiv & \quad \{\text{definizione di } def, \text{ sostituzione, semplificazione}\} \\ & \mathbf{T} \wedge \mathbf{T} \wedge n - (x+1) < V \\ \equiv & \quad \{\text{calcolo}\} \\ & n - x - 1 < V \\ \equiv & \quad \{\mathbf{Ip}: n - x = V\} \\ & \mathbf{T} \end{aligned}$$

- Per verificare l'ipotesi di Invarianza, sfruttando ancora l'**Assioma dell'Assegnamento Multiplo** e la regola PRE, dobbiamo dimostrare:

$$y = x * n \wedge x \in [0, n] \wedge x < n \Rightarrow def(x+1) \wedge def(y+n) \wedge (y = x * n \wedge x \in [0, n] \wedge def(x < n))^{[x+1, y+n/x, y]}$$

Partiamo dalla conclusione:

$$\begin{aligned} & def(x+1) \wedge def(y+n) \wedge (y = x * n \wedge x \in [0, n] \wedge def(x < n))^{[x+1, y+n/x, y]} \\ \equiv & \quad \{\text{sostituzione e semplificazione}\} \\ & y + n = (x+1) * n \wedge x+1 \in [0, n] \\ \equiv & \quad \{\mathbf{Ip}: y = x * n\} \\ & (x * n) + n = (x+1) * n \wedge x+1 \in [0, n] \\ \equiv & \quad \{\mathbf{Ip}: x \in [0, n], (x < n), \text{ calcolo}\} \\ & \mathbf{T} \end{aligned}$$

- Per verificare l'ipotesi di Terminazione

$$y = x * n \wedge x \in [0, n] \Rightarrow n - x \geq 0$$

Partiamo dalla conclusione:

$$n - x \geq 0$$

$$\equiv \quad \{\mathbf{Ip}: x \in [0, n], \text{ calcolo}\}$$

**T**

**ESERCIZIO 2**      Si verifichi la seguente tripla di Hoare (assumendo **a**: array [0, n) of nat)

$$\begin{array}{l} \{P\} \\ \quad \mathbf{if} \ a[x] > a[x-1] \ \mathbf{then} \ sum := sum + 2 * a[x] \ \mathbf{else} \ \mathbf{skip} \ \mathbf{fi} \\ \{Q\} \end{array}$$

dove

- $P \equiv x \in [1, n) \wedge sum = (\sum i : i \in [1, x) \wedge a[i] > a[i-1]) \cdot 2 * a[i]$ ,
- $Q \equiv sum = (\sum i : i \in [1, x) \wedge a[i] > a[i-1]) \cdot 2 * a[i]$ .

### SOLUZIONE ESERCIZIO 2

Applicando la **Regola del Condizionale**

$$(COND) \quad \frac{P \Rightarrow def(E) \quad \{P \wedge E\} C_1 \{Q\} \quad \{P \wedge \neg E\} C_2 \{Q\}}{\{P\} \mathbf{if} \ E \ \mathbf{then} \ C_1 \ \mathbf{else} \ C_2 \ \mathbf{fi} \ \{Q\}}$$

dobbiamo verificare che

1.  $P \Rightarrow def(a[x] > a[x-1])$
2.  $\{P \wedge a[x] > a[x-1]\} sum := sum + 2 * a[x] \{Q\}$
3.  $\{P \wedge \neg(a[x] > a[x-1])\} skip \{Q\}$

1. La 1) è vera dato che:

$$\begin{array}{l} def(a[x] > a[x-1]) \\ \equiv \quad \{\text{definizione di } def\} \\ def(a[x]) \wedge def(a[x-1]) \\ \equiv \quad \{\text{definizione di } def\} \\ def(x) \wedge x \in dom(a) \wedge def(x-1) \wedge x-1 \in dom(a) \\ \equiv \quad \{\text{definizione di } def, \mathbf{Ip}: dom(a) = [0, n), x \in [1, n)\} \end{array}$$

**T**

2. Per dimostrare la 2) applichiamo la **Regola dell'Assegnamento**

$$(ASS) \quad \frac{R \Rightarrow def(E) \wedge P[E/x]}{\{R\} x := E \{P\}}$$

e ci riduciamo a dimostrare che

$$x \in [1, n) \wedge sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]) \wedge a[x] > a[x-1] \Rightarrow \\ def(sum + 2 * a[x]) \wedge (sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]))^{[sum+2*a[x]/sum]}$$

Partiamo dalla conseguenza

$$def(sum + 2 * a[x]) \wedge (sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]))^{[sum+2*a[x]/sum]} \\ \equiv \quad \{ \text{definizione di } def, \text{ sostituzione} \} \\ x \in dom(a) \wedge (sum + 2 * a[x] = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i])) \\ \equiv \quad \{ dom(a) = [0, n), \text{ legge (interv-}\Sigma), \mathbf{Ip}: x \in [1, n), a[x] > a[x-1] \} \\ sum + 2 * a[x] = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]) + 2 * a[x] \\ \equiv \quad \{ \mathbf{Ip}: sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]), \text{ sostituzione} \} \\ sum + 2 * a[x] = sum + 2 * a[x]$$

3. Per dimostrare la 3), sfruttando l'**Assioma del Comando Vuoto**

$$(SKIP) \quad \{Q\} \text{ skip } \{Q\}$$

e la regola PRE dobbiamo dimostrare che

$$x \in [1, n) \wedge sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]) \wedge \neg(a[x] > a[x-1]) \Rightarrow \\ sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i])$$

Partiamo dalla conseguenza:

$$sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]) \\ \equiv \quad \{ \text{legge (interv-}\Sigma), \mathbf{Ip}: x \in [1, n), \neg(a[x] > a[x-1]) \} \\ sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]) \\ \equiv \quad \{ \mathbf{Ip}: sum = (\Sigma i : i \in [1, x) \wedge a[i] > a[i-1] \cdot 2 * a[i]) \}$$

**T**

**ESERCIZIO 3** Si verifichi la seguente tripla di Hoare (assumendo **a: array [0, n) of nat**)

$$\{h \in dom(a) \wedge h \geq 1 \wedge (\forall i. i \in [0, h) \Rightarrow a[i] > k)\} \\ a[h] := a[0] + 1 \\ \{(\forall i. i \in [0, h) \Rightarrow a[i] > k)\}$$

### SOLUZIONE ESERCIZIO 3

Sfruttando l'Assioma dell'Aggiornamento Selettivo

$$(AGG-SEL) \quad \{def(E) \wedge def(E') \wedge E \in dom(\mathbf{a}) \wedge P[\mathbf{b}/\mathbf{a}]\} \mathbf{a}[E] := E' \{P\}, \quad \text{dove } \mathbf{b} = \mathbf{a}^{[E'/E]}$$

e la regola PRE, dobbiamo verificare la seguente implicazione:

$$h \in dom(a) \wedge h \geq 1 \wedge (\forall i. i \in [0, h] \Rightarrow a[i] > k) \Rightarrow \\ def(h) \wedge def(a[0] + 1) \wedge h \in dom(a) \wedge (\forall i. i \in [0, h] \Rightarrow a[i] > k)^{[\mathbf{a}'/a]}$$

dove  $\mathbf{a}' = a^{[a[0]+1/h]}$ .

Partiamo dalla conseguenza:

$$\begin{aligned} & def(h) \wedge def(a[0] + 1) \wedge h \in dom(a) \wedge (\forall i. i \in [0, h] \Rightarrow a[i] > k)^{[\mathbf{a}'/a]} \\ \equiv & \quad \{\text{definizione di } def\} \\ & 0 \in dom(a) \wedge h \in dom(a) \wedge (\forall i. i \in [0, h] \Rightarrow a[i] > k)^{[\mathbf{a}'/a]} \\ \equiv & \quad \{\mathbf{Ip}: h \in dom(a), 0 \in dom(a); \text{ sostituzione}\} \\ & (\forall i. i \in [0, h] \Rightarrow \mathbf{a}'[i] > k) \\ \equiv & \quad \{\text{definizione di } \mathbf{a}'\} \\ & (\forall i. i \in [0, h] \Rightarrow a^{[a[0]+1/h]}[i] > k) \\ \equiv & \quad \{\text{Intervallo-}\forall, h > 0\} \\ & (\forall i. i \in [0, h] \Rightarrow a^{[a[0]+1/h]}[i] > k) \wedge a^{[a[0]+1/h]}[h] > k \\ \equiv & \quad \{\text{definizione di } a^{[a[0]+1/h]}, (\forall i. i \in [0, h] \Rightarrow i \neq h)\} \\ & (\forall i. i \in [0, h] \Rightarrow a[i] > k) \wedge a[0] + 1 > k \\ \equiv & \quad \{\mathbf{Ip}: (\forall i. i \in [0, h] \Rightarrow a[i] > k)\} \\ & a[0] + 1 > k \\ \equiv & \quad \{(\forall i. i \in [0, h] \Rightarrow a[i] > k) \wedge h \geq 1 \Rightarrow a[0] > k, \text{ calcolo}\} \end{aligned}$$

**T**

**ESERCIZIO 4** Si consideri il seguente frammento di programma annotato

```

{x = 0 ∧ z = 1 ∧ n ≥ 0 ∧ m ≥ 0}
{Inv : x ∈ [0, max(n, m)] ∧ z = wx} {t: max(n, m) - x}
while (x < n or x < m) do
  z := z * w;
  x := x + 1
endw
{z = wmax(m, n)}

```

1. Si scrivano le ipotesi di invarianza, di progresso e di terminazione.
2. Si dimostri l'ipotesi di invarianza.

#### SOLUZIONE ESERCIZIO 4

Invariante  $Inv : x \in [0, \max(n, m)] \wedge z = w^x$

Funzione di terminazione  $t : \max(n, m) - x$

Condizione  $E : (x < n \vee x < m)$

Comando  $C : z := z * w; x := x + 1$

Variabile di Specifica:  $V$  denota un generico valore

1. **Ipotesi di Progresso** ( $\{Inv \wedge E \wedge t = V\} C \{t < V\}$ )

$$\begin{aligned} & \{x \in [0, \max(n, m)] \wedge z = w^x \wedge (x < n \vee x < m) \wedge \max(n, m) - x = V \} \\ & \quad z := z * w; \\ & \quad x := x + 1 \\ & \{ \max(n, m) - x < V \} \end{aligned}$$

**Ipotesi di Terminazione** ( $Inv \Rightarrow t \geq 0$ )

$$x \in [0, \max(n, m)] \wedge z = w^x \Rightarrow \max(n, m) - x \geq 0$$

**Ipotesi di Invarianza** ( $\{Inv \wedge E\} C \{Inv \wedge def(E)\}$ )

$$\begin{aligned} & \{x \in [0, \max(n, m)] \wedge z = w^x \wedge (x < n \vee x < m) \} \\ & \quad z := z * w; \\ & \quad x := x + 1 \\ & \{x \in [0, \max(n, m)] \wedge z = w^x \wedge def(x < n \text{ or } x < m) \} \end{aligned}$$

2. Per verificare l'Ipotesi di Invarianza, applicando la **Regola della Sequenza**

$$(SEQ) \quad \frac{\{P\} C \{\mathbf{R}\} \quad \{\mathbf{R}\} C' \{Q\}}{\{P\} C; C' \{Q\}}$$

dobbiamo trovare un'asserzione  $\mathbf{R}$  tale che le seguenti triple siano verificate:

$$(2.1) \quad \begin{aligned} & \{x \in [0, \max(n, m)] \wedge z = w^x \wedge (x < n \vee x < m) \} \\ & \quad z := z * w \end{aligned}$$

$$(2.2) \quad \begin{aligned} & \{\mathbf{R}\} \\ & \quad x := x + 1 \\ & \{x \in [0, \max(n, m)] \wedge z = w^x \wedge def(x < n \text{ or } x < m) \} \end{aligned}$$

Partiamo da (2.2) applicando l'**Assioma dell'Assegnamento**

$$(ASS) \quad \{def(E) \wedge P[E/x]\} x := E \{P\}$$

ed otteniamo il seguente valore di  $\mathbf{R}$ :

$$def(x + 1) \wedge (x \in [0, \max(n, m)] \wedge z = w^x)^{[x+1/x]}$$

≡ {definizione di *def*, sostituzione}

$$x + 1 \in [0, \max(n, m)] \wedge z = w^{x+1}$$

Per la **Regola dell'Assegnamento** (vedi soluzione Esercizio 2), la verifica della (2.1) con la postcondizione **R** appena calcolata si riduce a dimostrare che

$$x \in [0, \max(n, m)] \wedge z = w^x \wedge (x < n \vee x < m) \Rightarrow \\ \text{def}(z * w) \wedge (x + 1 \in [0, \max(n, m)] \wedge z = w^{x+1})^{[z*w/z]}$$

Partiamo dalla conseguenza:

$$\text{def}(z * w) \wedge (x + 1 \in [0, \max(n, m)] \wedge z = w^{x+1})^{[z*w/z]}$$

≡ {sostituzione, definizione di *def*}

$$x + 1 \in [0, \max(n, m)] \wedge z * w = w^{x+1}$$

≡ {**Ip**:  $z = w^x$ }

$$x + 1 \in [0, \max(n, m)] \wedge w^x * w = w^{x+1}$$

≡ {calcolo, def. di intervallo}

$$x + 1 \geq 0 \wedge x + 1 \leq \max(n, m)$$

≡ {**Ip**:  $x \in [0, \max(n, m)]$ ,  $x \in [0, \max(n, m)] \Rightarrow x + 1 \geq 0$ }

$$x + 1 \leq \max(n, m)$$

≡ {**Ip**:  $x < n \vee x < m$ ,  $x \in [0, \max(n, m)]$ ,  $x < n \vee x < m \Rightarrow x + 1 \leq \max(n, m)$ }

**T**