

LOGICA PER LA PROGRAMMAZIONE - a.a. 2015-2016

Seconda prova di verifica intermedia - 17/12/2015 — 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

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

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

SOLUZIONE ESERCIZIO 1

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

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

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

Per dimostrare la formula partiamo allora dalla premessa:

$$\begin{aligned} & \neg(\exists x. (P \vee Q) \wedge (R \vee \neg S)) \wedge (\exists x. \neg(\neg R \wedge S)) \wedge \neg(\neg R[a/x] \wedge S[a/x]) \\ \Rightarrow & \quad \{(\text{semp}-\wedge), \text{occ. pos.}\} \\ & \neg(\exists x. (P \vee Q) \wedge (R \vee \neg S)) \wedge \neg(\neg R[a/x] \wedge S[a/x]) \\ \equiv & \quad \{(\text{De Morgan})\} \\ & (\forall x. \neg((P \vee Q) \wedge (R \vee \neg S))) \wedge \neg(\neg R[a/x] \wedge S[a/x]) \\ \Rightarrow & \quad \{(\text{elim-}\forall), \text{occ. pos.}\} \\ & \neg((P[a/x] \vee Q[a/x]) \wedge (R[a/x] \vee \neg S[a/x])) \wedge \neg(\neg R[a/x] \wedge S[a/x]) \\ \equiv & \quad \{(\text{De Morgan}), \text{due volte}\} \\ & (\neg(P[a/x] \vee Q[a/x]) \vee \neg(R[a/x] \vee \neg S[a/x])) \wedge (R[a/x] \vee \neg S[a/x]) \\ \equiv & \quad \{(\text{complemento})\} \\ & \neg(P[a/x] \vee Q[a/x]) \wedge (R[a/x] \vee \neg S[a/x]) \\ \Rightarrow & \quad \{(\text{semp}-\wedge), \text{occ. pos.}\} \\ & \neg(P[a/x] \vee Q[a/x]) \\ \equiv & \quad \{(\text{De Morgan})\} \\ & \neg P[a/x] \wedge \neg Q[a/x] \\ \Rightarrow & \quad \{(\text{intro-}\exists), \text{occ. pos.}\} \\ & (\exists x. \neg P \wedge \neg Q) \\ \equiv & \quad \{(\neg \Rightarrow), \text{doppia negazione}\} \\ & (\exists x. \neg(\neg P \Rightarrow Q)) \\ \equiv & \quad \{(\text{De Morgan})\} \\ & \neg(\forall x. \neg P \Rightarrow Q) \end{aligned}$$

ESERCIZIO 2

Assumendo \mathbf{a} , \mathbf{b} : **array** $[0, n)$ **of nat**, si formalizzi il seguente enunciato:

“Il numero di elementi dell’array \mathbf{a} che sono uguali all’elemento successivo è minore della somma degli elementi dell’array \mathbf{b} che sono uguali al doppio dell’elemento precedente.”

SOLUZIONE ESERCIZIO 2

$$\#\{i : i \in [0, n - 1] \mid a[i] = a[i + 1]\} < (\sum j : j \in (0, n) \wedge b[j] = 2 * b[j - 1] \cdot b[j])$$

ESERCIZIO 3

Si dica se la seguente tripla è verificata. Se lo è, fornire una dimostrazione formale; se non lo è, fornire un controesempio.

$$\{x = A \wedge y = B \wedge z = C\} \mathbf{x}, \mathbf{z} := \mathbf{x} + \mathbf{y}, \mathbf{x} - \mathbf{z} \{z = A + B - C\}$$

SOLUZIONE ESERCIZIO 3

La tripla non è verificata. Per mostrarlo, forniamo un controesempio, cioè uno stato σ che

1. soddisfa la preconditione ($\sigma \models x = A \wedge y = B \wedge z = C$), ma tale che
2. l'esecuzione del comando in σ porta in uno stato σ' che non soddisfa la postcondizione.

Consideriamo lo stato $\sigma = \{(x, 5), (y, 3), (z, 1)\}$. Eseguendo l'assegnamento multiplo $\mathbf{x}, \mathbf{z} := \mathbf{x} + \mathbf{y}, \mathbf{x} - \mathbf{z}$ otteniamo

$$\sigma' = \sigma^{[8,4/x,z]} = \{(x, 8), (y, 3), (z, 4)\}.$$

Si noti che lo stato σ' non soddisfa la postcondizione $z = A + B - C$. Infatti le variabili di specifica A , B e C si riferiscono ai valori di x , y e z nella preconditione. Quindi si dovrebbe avere $z = 5 + 3 - 1 = 7$.

ESERCIZIO 4

Assumendo \mathbf{a} : **array** $[0, n)$ of **int**, si verifichi la seguente tripla:

$$\{h \in [1, n) \wedge (\forall i. i \in [0, h) \Rightarrow a[i] = 2^i)\}$$

$$\mathbf{a}[h] := 2 * \mathbf{a}[h-1]$$

$$\{(\forall i. i \in [0, h) \Rightarrow a[i] = 2^i)\}$$

SOLUZIONE ESERCIZIO 4

Applicando l'Assioma dell'Aggiornamento Selettivo e la regola (PRE), dobbiamo verificare che:

$$h \in [1, n) \wedge (\forall i. i \in [0, h) \Rightarrow a[i] = 2^i) \Rightarrow$$

$$h \in \text{dom}(a) \wedge \text{def}(h) \wedge \text{def}(2 * a[h-1]) \wedge (\forall i. i \in [0, h) \Rightarrow a[i] = 2^i)^{[b/a]}$$

dove $\mathbf{b} = a^{[2 * a[h-1]/h]}$.

Partiamo dalla conseguenza

$$h \in \text{dom}(a) \wedge \text{def}(h) \wedge \text{def}(2 * a[h-1]) \wedge (\forall i. i \in [0, h) \Rightarrow a[i] = 2^i)^{[b/a]}$$

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

$$h \in \text{dom}(a) \wedge h - 1 \in \text{dom}(a) \wedge (\forall i. i \in [0, h) \Rightarrow a[i] = 2^i)^{[b/a]}$$

$$\equiv \{\mathbf{Ip}: h \in [1, n) \wedge \text{dom}(a) = [0, n)\}$$

$$(\forall i. i \in [0, h) \Rightarrow a[i] = 2^i)^{[b/a]}$$

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

$$(\forall i. i \in [0, h) \Rightarrow \mathbf{b}[i] = 2^i)$$

$$\equiv \{(\text{Intervallo-}\forall, \mathbf{Ips}: h > 0)\}$$

$$(\forall i. i \in [0, h) \Rightarrow \mathbf{b}[i] = 2^i) \wedge \mathbf{b}[h] = 2^h$$

$$\equiv \{\text{definizione di } \mathbf{b} = a^{[2 * a[h-1]/h]}\}$$

$$(\forall i. i \in [0, h) \Rightarrow a[i] = 2^i) \wedge 2 * a[h-1] = 2^h$$

$$\equiv \{\mathbf{Ip}: (\forall i. i \in [0, h) \Rightarrow a[i] = 2^i)\}$$

$$2 * a[h-1] = 2^h$$

$$\equiv \{\mathbf{Ip}: (\forall i. i \in [0, h) \Rightarrow a[i] = 2^i), a[h-1] = 2^{h-1}\}$$

$$2 * 2^{h-1} = 2^h$$

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

T

ESERCIZIO 5

Assumendo \mathbf{a} : array $[0, m)$ of \mathbf{int} , si consideri il seguente frammento di programma annotato:

```
{c = 0 ∧ z = 0}
{Inv: z ∈ [0, m] ∧ (c = (∑i: i ∈ [0, z) ∧ pari(i) . a[i]2))}{t: m - z}
while (z < m) do
  if (z mod 2 = 0)
    then c := c + a[z] * a[z]
    else skip
  fi;
  z := z + 1
endw
{c = (∑i: i ∈ [0, m) ∧ pari(i) . a[i]2)}
```

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

SOLUZIONE ESERCIZIO 5

Invariante Inv : $(z \in [0, m] \wedge (c = (\sum i: i \in [0, z) \wedge \text{pari}(i) . a[i]^2)))$
Funzione di terminazione t : $m - z$

1. Ipotesi di Invarianza:

```
{z ∈ [0, m] ∧ c = (∑i: i ∈ [0, z) ∧ pari(i) . a[i]2) ∧ (z < m)}
if (z mod 2 = 0) then c := c + a[z] * a[z] else skip fi; z := z + 1
{z ∈ [0, m] ∧ c = (∑i: i ∈ [0, z) ∧ pari(i) . a[i]2) ∧ def(z < m)}
```

2. Ipotesi di Progresso:

```
{z ∈ [0, m] ∧ c = (∑i: i ∈ [0, z) ∧ pari(i) . a[i]2) ∧ (z < m) ∧ m - z = V}
if (z mod 2 = 0) then c := c + a[z] * a[z] else skip fi; z := z + 1
{m - z < V}
```

Dimostriamo l'ipotesi di invarianza. Applicando la Regola della Sequenza, dobbiamo trovare una asserzione R tale che le seguenti triple siano verificate:

$$(5.1) \{z \in [0, m] \wedge (c = (\sum i: i \in [0, z) \wedge \text{pari}(i) . a[i]^2)) \wedge (z < m)\} \text{if} \dots \text{fi} \{R\}$$

$$(5.2) \{R\} \mathbf{z} := \mathbf{z} + 1 \{z \in [0, m] \wedge (c = (\sum i: i \in [0, z) \wedge \text{pari}(i) . a[i]^2)) \wedge \text{def}(z < m)\}$$

Per determinare R , usiamo l'Assioma dell'Assegnamento in (5.2) e troviamo che è

$$\begin{aligned} & \text{def}(z + 1) \wedge (z \in [0, m] \wedge c = (\sum i: i \in [0, z) \wedge \text{pari}(i) . a[i]^2) \wedge \text{def}(z < m))^{[z+1/z]} \\ \equiv & \{\text{sostituzione, definizione di def}\} \\ & z + 1 \in [0, m] \wedge (c = (\sum i: i \in [0, z] \wedge \text{pari}(i) . a[i]^2)) \end{aligned}$$

Quindi resta da verificare la tripla (5.1) per il valore di R appena calcolato e per la preconditione

$$P = z \in [0, m] \wedge (c = (\sum i: i \in [0, z) \wedge \text{pari}(i) . a[i]^2)) \wedge (z < m)$$

Applicando la Regola del Condizionale, dobbiamo verificare che

$$(5.1.1) P \Rightarrow \text{def}(z \bmod 2 = 0)$$

$$(5.1.2) \{P \wedge (z \bmod 2 = 0)\} \text{then } \mathbf{c} := \mathbf{c} + \mathbf{a}[\mathbf{z}] * \mathbf{a}[\mathbf{z}] \{R\}$$

$$(5.1.3) \{P \wedge \neg(z \bmod 2 = 0)\} \text{skip} \{R\}$$

(5.1.1) Vera, dato che:

$$\begin{aligned}
& def(z \bmod 2 = 0) \\
\equiv & \quad \{\text{definizione di } def\} \\
& def(z) \wedge def(2) \wedge def(0) \wedge 2 \neq 0 \\
\equiv & \quad \{\text{definizione di } def\} \\
& \mathbf{T}
\end{aligned}$$

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

$$\begin{aligned}
& P \wedge (z \bmod 2 = 0) \Rightarrow \\
& def(c + a[z] * a[z]) \wedge (z + 1 \in [0, m] \wedge c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)) [c + a[z] * a[z] / c]
\end{aligned}$$

dove

$$P = z \in [0, m] \wedge (c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)) \wedge (z < m)$$

Partiamo dalla conseguenza, applicando la sostituzione

$$\begin{aligned}
& def(c + a[z] * a[z]) \wedge z + 1 \in [0, m] \wedge c + a[z] * a[z] = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2) \\
\equiv & \quad \{\text{definizione di } def\} \\
& z \in [0, m] \wedge z + 1 \in [0, m] \wedge c + a[z] * a[z] = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2) \\
\equiv & \quad \{\mathbf{Ip}: (z \in [0, m]) \wedge (z < m)\} \\
& c + a[z] * a[z] = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2) \\
\equiv & \quad \{(\text{Intervallo-}\Sigma), \mathbf{Ip}: (z \bmod 2 = 0) \} \\
& c + a[z] * a[z] = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2) + a[z]^2 \\
\equiv & \quad \{\mathbf{Ip}: c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)\} \\
& c + a[z] * a[z] = c + a[z]^2 \\
\equiv & \quad \{\text{calcolo}\} \\
& \mathbf{T}
\end{aligned}$$

(5.1.3) Applicando la **Regola (SKIP)** (oppure l'Assioma (SKIP) e la regola (PRE)), dobbiamo dimostrare

$$P \wedge \neg(z \bmod 2 = 0) \Rightarrow z + 1 \in [0, m] \wedge (c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)) \wedge def(z < m)$$

dove

$$P = z \in [0, m] \wedge (c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)) \wedge (z < m)$$

Partiamo dalla conseguenza

$$\begin{aligned}
& z + 1 \in [0, m] \wedge (c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)) \wedge def(z < m) \\
\equiv & \quad \{\text{definizione di } def\} \\
& z + 1 \in [0, m] \wedge (c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)) \\
\equiv & \quad \{\mathbf{Ip}: (z \in [0, m]) \wedge (z < m)\} \\
& c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2) \\
\equiv & \quad \{(\text{Intervallo-}\Sigma), \mathbf{Ip}: \neg(z \bmod 2 = 0) \} \\
& c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2) \\
\equiv & \quad \{\mathbf{Ip}: c = (\Sigma i: i \in [0, z] \wedge pari(i) \cdot a[i]^2)\} \\
& \mathbf{T}
\end{aligned}$$