LOGICA PER LA PROGRAMMAZIONE – a.a. 2014/15
Quinta esercitazione — 4/12/2014

ESERCIZIO 1 Cosa vuol dire "La tripla $\{P\}\ C\ \{Q\}$ è verificata"?

SOLUZIONE ESERCIZIO 1

Nella tripla $\{P\}\ C\ \{Q\}$, C è un comando, mentre P (detta *precondizione*) e Q (detta *postcondizione*) sono asserzioni, ovvero formule ben formate in cui possono comparire le variabili dello stato. Formalmente, la tripla è verificata o soddisfatta se per ogni stato σ che soddisfa P ($\sigma \models P$)

- l'esecuzione del comando C a partire dallo stato σ *termina* producendo uno stato σ';
- lo stato σ' soddisfa Q ($\sigma' \models Q$).

ESERCIZIO 2 Usando la risposta del punto precedente, per ognuna delle seguenti triple separatamente si dica cosa si può dedurre sul comando C e/o sull'asserzione P **se la tripla è verificata** (**T** sta per *true* e **F** sta per *false*):

1) $\{P\}\ C\ \{\mathbf{T}\}$ 2) $\{P\}\ C\ \{\mathbf{F}\}$ 3) $\{\mathbf{F}\}\ C\ \{P\}$

SOLUZIONE ESERCIZIO 2

1. L'esecuzione del comando C a partire da un qualunque stato σ che soddisfa P termina.
   Infatti la tripla è verificata se per ogni stato σ che soddisfa P, l'esecuzione del comando C a partire da σ termina, producendo uno stato σ' che soddisfa **T**. Dato che tutti gli stati soddisfano **T**, possiamo omettere la seconda parte della frase (sottolineata nel testo).
2. Nessuno stato soddisfa P.
   Infatti, se esistesse uno stato σ tale che $\sigma \models P$, allora l'esecuzione di C a partire da σ dovrebbe terminare in uno stato σ' tale che $\sigma' \models \mathbf{F}$, ma questo è assurdo, dato che, per definizione, non esistono stati che soddisfano **F**. Quindi si è sbagliato ad assumere che esista uno stato che soddisfa P. Di conseguenza, affinché la tripla sia verificata, deve essere necessariamente che $P \equiv \mathbf{F}$, indipendentemente dal comando C.
3. Non possiamo dedurre nulla né sul comando C né sull'asserzione P. Infatti, la tripla è verificata se per ogni stato σ che soddisfa **F**, l'esecuzione del comando C a partire da σ termina, producendo uno stato σ' che soddisfa P. Tuttavia dato che, per definizione, non esistono stati che possano soddisfare **F**, la condizione è sempre vera (in inglese si direbbe *vacuously true*) per qualunque comando C e per qualunque postcondizione P.

ESERCIZIO 3 Si verifichino le seguenti triple (A è una variabile di specifica).

1. $\{A > 0 \ \wedge \ x = A \ \wedge y < x\}$
   $x := 2 * x + y$
   $\{y < x\}$

2. $\{y > 0 \ \wedge \ x = y * y\}$
   $x := x + 2 * y + 1; \quad y := y + 1$
   $\{x = y * y\}$

3. $\{sum = (\Sigma i : \ i \in [0, x) \, . \, i)\}$
   $sum := sum + x; x := x + 1$
   $\{sum = (\Sigma i : \ i \in [0, x) \, . \, i)\}$

SOLUZIONE ESERCIZIO 3

1. $\{A > 0 \ \wedge \ x = A \ \wedge y < x\}$
   $x := 2 * x + y;$
   $\{y < x\}$

   Possiamo ricorrere alla Regola dell'Assegnamento

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

   dove $def(E)$ è vera in uno stato σ se il valore di E in σ (cioè $\mathcal{E}(E, \sigma)$) è ben definito. L'assegnamento $x := E$ parte dallo stato σ e arriva nello stato $\sigma[\mathcal{E}(E, \sigma)/x]$.

   La verifica si riduce allora a dimostrare che:

   $(A > 0 \ \wedge \ x = A \ \wedge y < x) \Rightarrow def(2 * x + y) \wedge (y < x)[(2 * x + y)/x]$

   Partiamo dalla conseguenza, applicando la sostituzione, ed utilizzando le premesse come ipotesi. Notiamo inoltre che $def(2 * x + y) \equiv \mathbf{T}$.

   $y < 2 * x + y$

   $\equiv$ $\{$**Ip:** $x = A\}$

   $y < (2 * A + y)$

   $\equiv$ $\{$**Ip:** $A > 0$, calcolo$\}$

   $\mathbf{T}$

2. $\{y > 0 \ \wedge \ x = y * y\}$
$x := x + 2 * y + 1; \quad y := y + 1$
$\{x = y * y\}$

Applicando la Regola della Sequenza, dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

(2.1) $\{y > 0 \ \wedge \ x = y * y\} \quad x := x + 2 * y + 1 \quad \{R\}$
(2.2) $\{R\} \quad y := y + 1 \quad \{x = y * y\}$

Per l'Assioma dell'Assegnamento, la (2.2) è verificata per il seguente valore di R:

$def(y + 1) \wedge (x = y * y)[y + 1/y]$

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

$x = (y + 1) * (y + 1)$

Allora, per la Regola dell'Assegnamento, la verifica di (2.1) con la postcondizione R appena calcolata, si riduce a dimostrare che:

$(y > 0 \ \wedge \ x = y * y) \Rightarrow def(x + 2 * y + 1) \wedge (x = (y + 1) * (y + 1))[x + 2 * y + 1/x]$

Partiamo dalla conseguenza:

$def(x + 2 * y + 1) \wedge (x = (y + 1) * (y + 1))[x + 2 * y + 1/x]$

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

$(x + 2 * y + 1) = (y + 1) * (y + 1)$

$\equiv$ {calcolo}

$(x + 2 * y + 1) = (y * y + 2 * y + 1)$

$\equiv$ {**Ip:** $x = y * y$}

T

3. $\{sum = (\Sigma i : i \in [0, x) \,.\, i)\}$
$sum := sum + x; x := x + 1$
$\{sum = (\Sigma i : i \in [0, x) \,.\, i)\}$

Applicando la Regola della Sequenza, dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

(3.1) $\{sum = (\Sigma i : i \in [0, x) \,.\, i)\}$
$sum := sum + x$
$\{R\}$

(3.2) $\{R\}$
$x := x + 1$
$\{sum = (\Sigma i \colon i \in [0, x) \,.\, i)\}$

Per l'Assioma dell'Assegnamento, la (3.2) è verificata per il seguente valore di R:

$def\,(x+1) \wedge sum = (\Sigma i \colon i \in [0, x) \,.\, i)[x+1/x]$

$\equiv$ {definizione di def e sostituzione}

$sum = (\Sigma i \colon i \in [0, x+1) \,.\, i)$

Per verificare (3.1), per la Regola dell'Assegnamento, con la postcondizione R appena calcolata, si riduce a dimostrare che:

$$sum = (\Sigma i \colon i \in [0, x) \,.\, i) \Rightarrow def\,(sum + x) \wedge (sum = (\Sigma i \colon i \in [0, x+1) \,.\, i))[sum + x/sum]$$

Partiamo dalla conseguenza, applicando la sostituzione, usando la premessa come ipotesi e notando che $def\,(sum + x) \equiv \mathbf{T}$:

$sum + x = (\Sigma i \colon i \in [0, x+1) \,.\, i)$

$\equiv$ {**Ip:** $sum = (\Sigma i \colon i \in [0, x) \,.\, i)$}

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

$\equiv$ {(Legge dell'intervallo per la sommatoria)}

$\mathbf{T}$

ESERCIZIO 4 Si dica se le seguenti triple sono verificate oppure no (A e B sono variabili di specifica). Motivare formalmente le risposte.

1. $\{x = A \wedge y = B \wedge B > 0 \wedge A \geq B \wedge z = 0\}\ z := x + y; \quad y := y - z\ \{y < 0\}$,
2. $\{x = A \wedge y = B \wedge B > 0 \wedge A \geq B \wedge z = 0\}\ z, y := x + y, y - z\ \{y < 0\}$

SOLUZIONE ESERCIZIO 4

1. $\{x = A \wedge y = B \wedge B > 0 \wedge A \geq B \wedge z = 0\}\ z := x + y; \quad y := y - z\ \{y < 0\}$,

   Applicando la Regola della Sequenza, dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

   (4.1) $\{x = A \wedge y = B \wedge B > 0 \wedge A \geq B\}\ z := x + y\ \{R\}$
   (4.2) $\{R\}\ y := y - z\ \{y < 0\}$

   Per l'Assioma dell'Assegnamento, la (4.2) è verificata per il seguente valore di R:

   $def\,(y - z) \wedge (y < 0)[(y - z)/y]$

   $\equiv$ {sostituzione, definizione di def}

   $(y - z < 0)$

Per la Regola dell'Assegnamento, la verifica di (4.1) con la postcondizione R appena calcolata, si riduce a dimostrare che:

$$(x = A \wedge y = B \wedge B > 0 \wedge A \geq B) \Rightarrow def(x + y) \wedge (y - z < 0)[x + y/z]$$

Partiamo dalla conseguenza:

$def(x + y) \wedge (y - z < 0)[x + y/z]$

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

$y - (x + y) < 0$

$\equiv$ {calcolo}

$-x < 0$

$\equiv$ {**Ip:** $x = A \wedge A \geq B \wedge B > 0$}

T

2. $\{x = A \wedge y = B \wedge B > 0 \wedge A \geq B \wedge z = 0\}\ z, y := x + y, y - z\ \{y < 0\}$

Abbiamo qui un caso di Assegnamento Multiplo e non Semplice, che prevede di valutare tutte le espressioni **prima** di tutti gli assegnamenti. Applicando la regola dell'Assegnamento Multiplo ci riduciamo a verificare:

$$(x = A \wedge y = B \wedge B > 0 \wedge A \geq B \wedge z = 0) \Rightarrow$$
$$def(x + y) \wedge def(y - z) \wedge (y < 0)[(x + y)/z, (y - z)/y]$$

Partiamo dalla conseguenza:

$def(x + y) \wedge def(y - z) \wedge (y < 0)[(x + y)/z, (y - z)/y]$

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

$y - z < 0$

$\equiv$ {**Ip:** $y = B \wedge z = 0)$}

$B < 0$

$\equiv$ {**Ip:** $B > 0$}

F

Quindi la tripla non è verificata.

ESERCIZIO 5 Si forniscano due espressioni E_1 ed E_2 in modo che la seguente tripla (A e B sono variabili di specifica) sia verificata e si dimostri formalmente la correttezza della soluzione proposta. Si ricordi che le variabili di specifica non possono comparire in un comando.

$\{x = A \wedge y = B\}$
if $x \leq y$ **then** $x := E_1$ **else** $x := E_2$ **fi**;
$\{x > A \wedge x > B\}$

SOLUZIONE ESERCIZIO 5

La tripla è verificata per qualunque coppia di espressioni $E_1 > max(x, y)$ e $E_2 > max(x, y)$, ad esempio $E_1 = y + 1$ e $E_2 = x + 1$.

Applicando la Regola del Condizionale, dobbiamo verificare che:

(5.1) $(x = A \wedge y = B) \Rightarrow def(x \leq y)$

(5.2) $\{(x = A \wedge y = B) \wedge (x \leq y)\}\ x := y + 1\ \{x > A \wedge x > B\}$

(5.3) $\{(x = A \wedge y = B) \wedge \neg(x \leq y)\}\ x := x + 1\ \{x > A \wedge x > B\}$

La (5.1) è vera dato che $def(x \leq y) \equiv \mathbf{T}$.

Per la Regola dell'Assegnamento, verificare la (5.2) si riduce a dimostrare che:
$((x = A \wedge y = B) \wedge (x \leq y)) \Rightarrow def(y + 1) \wedge (x > A \wedge x > B)[y + 1/x]$

Partiamo dalla conseguenza, applicando la sostituzione
$def(y + 1) \wedge (x > A \wedge x > B)[y + 1/x]$

$\equiv$ {sostituzione, definizione di *def*}
$(y + 1 > A \wedge y + 1 > B)$

$\equiv$ {**Ip:** $(x = A \wedge y = B) \wedge (x \leq y)$}
$\mathbf{T}$

Analogamente la Regola dell'Assegnamento, verificare la (5.3) si riduce a dimostrare che:
$((x = A \wedge y = B) \wedge \neg(x \leq y)) \Rightarrow def(y + 1) \wedge (x > A \wedge x > B)[x + 1/x]$

Partiamo dalla conseguenza, applicando la sostituzione
$def(y + 1) \wedge (x > A \wedge x > B)[x + 1/x]$

$\equiv$ {sostituzione, definizione di *def*}
$(x + 1 > A \wedge x + 1 > B)$

$\equiv$ {**Ip:** $(x = A \wedge y = B) \wedge (x > y)$}
$\mathbf{T}$

ESERCIZIO 6 Si verifichi la seguente tripla.

$\{x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)\}$
if $x \,\%\, 6 = 0$ **then** y := y + x **else** skip **fi**;
x := x + 1
$\{y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)\}$

SOLUZIONE ESERCIZIO 6

Applicando la Regola della Sequenza, dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

(6.1) $\{x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)\}$ **if** $x \,\%\, 6 = 0$ **then** $y := y + x$ **else** *skip* **fi** $\{R\}$

(6.2) $\{R\}$ $x := x + 1$ $\{y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)\}$

Per l'Assioma dell'Assegnamento, la (6.2) è verificata per R uguale a:

$$def(x + 1) \wedge (y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i))[x + 1/x]$$

Quindi semplificando, abbiamo che R è:

$$(y = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i))$$

Per la (6.1), applichiamo la Regola del Condizionale, per la quale dobbiamo verificare che

(6.1.1) $x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \Rightarrow def(x \,\%\, 6 = 0)$

ovvia essendo $def(x \,\%\, 6 = 0) \equiv \mathbf{T}$

(6.1.2) $\{x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge (x \,\%\, 6 = 0)\}$ $y := y + x$ $\{R\}$

(6.1.3) $\{x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge \neg(x \,\%\, 6 = 0)\}$ skip $\{R\}$

Per la (6.1.2), usiamo la Regola dell'Assegnamento, dobbiamo dimostrare, ignorando $def(y + x)$ che è equivalente a $\mathbf{T}$, l'implicazione

$$(x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge (x \,\%\, 6 = 0))$$
$$\Rightarrow$$
$$(y + x = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i))$$

Partiamo dalla conclusione:

$y + x = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i))$
$\equiv$ {**Ip:** $x \,\%\, 6 = 0$, (Intervallo-Σ)}
$y + x = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)) + x$
$\equiv$ {**Ip:** $y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)$}
$y + x = y + x$
$\equiv$ {calcolo}
$\mathbf{T}$

Per la (6.1.3), applichiamo l'Assioma del Comando Vuoto e la Regola PRE e ci riduciamo a dimostrare che:

$$x \geq 0 \wedge y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i) \wedge \neg(x \,\%\, 6 = 0) \;\Rightarrow\; y = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i)$$

Partiamo dalla conclusione

$$y = (\Sigma i : i \in [0, x] \wedge i \,\%\, 6 = 0 \,.\, i)$$

$\equiv$ $\{$**Ip:** $x \,\%\, 6 \neq 0$, (Intervallo-Σ)$\}$

$$y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)$$

$\equiv$ $\{$**Ip:** $y = (\Sigma i : i \in [0, x) \wedge i \,\%\, 6 = 0 \,.\, i)\}$

T