LOGICA PER LA PROGRAMMAZIONE - a.a. 2014-2015
Seconda prova di verifica intermedia - 18/12/2014 — 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 e R contengano la variabile libera x, si provi che la seguente formula è valida:

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

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

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

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:

$(\forall x.P \Rightarrow Q) \wedge \neg(\exists x.\neg(R \Rightarrow Q)) \wedge (\exists x.P) \wedge P[^a/_x]$
$\Rightarrow$ {(sempl-$\wedge$)}
$(\forall x.P \Rightarrow Q) \wedge P(a)$
$\Rightarrow$ {(elim-$\forall$), occ. pos.}
$(P(a) \Rightarrow Q(a)) \wedge P(a)$
$\equiv$ {(idempotenza)}
$(P(a) \Rightarrow Q(a)) \wedge P(a) \wedge P(a)$
$\Rightarrow$ {(Modus Ponens)}
$Q(a) \wedge P(a)$
$\equiv$ {(doppia negazione)}
$\neg\neg(Q(a) \wedge \neg\neg P(a))$
$\Rightarrow$ {($\neg - \Rightarrow$), al contrario}
$\neg(Q(a) \Rightarrow \neg P(a))$
$\Rightarrow$ {Intro-$\exists$}
$(\exists x.\neg(Q \Rightarrow \neg P))$

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:

4	0	1	3

1	8	4	3	5	2

SOLUZIONE ESERCIZIO 2

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

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

$$\{x = A \;\wedge\; y = B\}\ \mathtt{x = x + y;\ y = x - y;\ x = x - y}\ \{x = B \;\wedge\; y = A\}$$

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) $\{x = A \ \wedge \ y = B\}$ `x := x + y` $\{R_1\}$

(3.2) $\{R_1\}$ `y := x - y` $\{R_2\}$

(3.3) $\{R_2\}$ `x := x - y` $\{x = B \ \wedge \ y = A\}$

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

$$\{def(x - y) \wedge (x = B \ \wedge \ y = A)[^{x-y}/_{x}]\} \texttt{ x := x - y } \{x = B \ \wedge \ y = A\}$$

La condizione R_2 è quindi

$def(x - y) \wedge (x = B \ \wedge \ y = A)[^{x-y}/_{x}]$

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

$x - y = B \ \wedge \ y = A$

Per determinare R_1, usiamo ancora l'Assioma dell'Assegnamento:

$$\{def(x - y) \wedge (x - y = B \wedge y = A)[^{x-y}/_{y}]\} \texttt{ y := x - y } \{x - y = B \ \wedge \ y = A\}$$

La condizione R_1 è quindi

$x - (x - y) = B \wedge \ x - y = A$

$\equiv$ {calcolo}

$y = B \wedge \ x - y = A$

Resta da verificare:

$$\{x = A \wedge y = B\} \texttt{ x := x + y } \{y = B \wedge \ x - y = A\}$$

e quindi, usando la Regola dell'Assegnamento, che

$$x = A \wedge y = B \Rightarrow def(x + y) \wedge (y = B \wedge \ x - y = A)[^{x+y}/_{x}]$$

Partiamo dalla conseguenza, applicando la sostituzione

$(y = B \wedge \ x + y - y = A)$

$\equiv$ {calcolo}

$(y = B \wedge \ x = A)$

ESERCIZIO 4

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

$\{cond = \textbf{true} \ \wedge \ z = 0\}$
$\{\textsf{Inv: } (z \in [0, n]) \ \wedge \ (cond \equiv (\forall x.x \in [0, z) \Rightarrow a[x] = b[x]))\}\{\textsf{t: } n - z\}$

```
while (z < n) do
     if not(a[z] = b[z])
          then cond := false
          else skip
     fi;
     z := z + 1
endw
```

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

Si scriva e si dimostri l'ipotesi di invarianza.

SOLUZIONE ESERCIZIO 4

Invariante Inv : $(z \in [0,n]) \ \wedge \ (cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x]))$
Funzione di terminazione t : $n - z$
Condizione E : $z < n$
Comando C : `if...fi;z := z + 1`

L'Ipotesi di Invarianza ($\{Inv \wedge E\}\ C\ \{Inv \wedge def(E)\}$) in questo caso è

$\{(z \in [0,n]) \ \wedge \ (cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x])) \wedge (z < n)\}$
`if not(a[z] = b[z]) then cond := false else skip fi; z := z + 1`
$\{(z \in [0,n]) \ \wedge \ (cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x])) \ \wedge \ def(z < n)\}$

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

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

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

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

$def(z+1) \wedge ((z \in [0,n]) \wedge (cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x]) \ \wedge \ def(z < n))[^{z+1}/_{z}]$
$\equiv$ {sostituzione, definizione di def}
$(z+1 \in [0,n]) \ \wedge \ (cond \equiv (\forall x.x \in [0,z] \Rightarrow a[x] = b[x]))$

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

1. $P \Rightarrow def(not(a[z] = b[z]))$
2. $\{P \wedge (not(a[z] = b[z]))\}$ `cond := false` $\{R\}$
3. $\{P \wedge \neg(not(a[z] = b[z]))\}$ `skip` $\{R\}$

1. La 1) è vera dato che:
   $def(not(a[z] = b[z]))$
   $\equiv$ {definizione di def}
   $def(a[z]) \wedge def(b[z])$
   $\equiv$ {definizione di def}
   $def(z) \wedge z \in dom(a) \wedge z \in dom(b)$
   $\equiv$ {definizione di def, **Ip:** $dom(a) = dom(b) = [0,n), z \in [0,n], z < n$}
   T

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

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

   dove $P = (z \in [0,n]) \ \wedge \ (cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x])) \wedge (z < n)$
   Partiamo dalla conseguenza, applicando la sostituzione
   $def(false) \wedge (z+1 \in [0,n]) \wedge (false \equiv (\forall x.x \in [0,z] \Rightarrow a[x] = b[x]))$
   $\equiv$ {definizione di def}
   $(z+1 \in [0,n]) \ \wedge \ (false \equiv (\forall x.x \in [0,z] \Rightarrow a[x] = b[x]))$
   $\equiv$ {**Ip**: $(z \in [0,n]) \wedge (z < n)$}
   $false \equiv (\forall x.x \in [0,z] \Rightarrow a[x] = b[x])$
   $\equiv$ {(Intervallo-$\forall$)}
   $false \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x]) \wedge a[z] = b[z]$
   $\equiv$ {**Ip**: $not(a[z] = b[z])$}

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

$\equiv$ {calcolo}

$false \equiv \mathbf{F}$

$\equiv$ {calcolo}

$\mathbf{T}$

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

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

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

Partiamo dalla conseguenza

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

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

$cond \equiv (\forall x.x \in [0,z] \Rightarrow a[x] = b[x])$

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

$cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x]) \wedge (a[z] = b[z])$

$\equiv$ {**Ip**: $a[z] = b[z]$}

$cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x]) \wedge \mathbf{T}$

$\equiv$ {Assorb.}

$cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x])$

$\equiv$ {**Ip**: $cond \equiv (\forall x.x \in [0,z) \Rightarrow a[x] = b[x])$}

$\mathbf{T}$

ESERCIZIO 5

Assumendo **b: array [0, n) of int**, si verifichi la seguente tripla:

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

```
b[x] := b[x - 1] + 2 * 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:

$$x \in [1,n) \ \wedge \ (\forall i \,.\, i \in [0,x) \Rightarrow b[i] = i^2) \Rightarrow$$
$$def(x) \wedge def(b[x-1] + 2 * x - 1) \wedge x \in dom(b) \wedge (\forall i \,.\, i \in [0,x] \Rightarrow b[i] = i^2)[\mathbf{b}'/_b]$$

dove $\mathbf{b}' = b\left[{}^{b[x-1]+2*x-1}/_x\right]$.

Partiamo dalla conseguenza

$def(x) \wedge def(b[x-1] + 2 * x - 1) \wedge x \in dom(b) \wedge (\forall i \,.\, i \in [0,x] \Rightarrow b[i] = i^2)[\mathbf{b}'/_b]$

$\equiv$ {definizione di def}

$def(b[x-1]) \wedge def(2 * x - 1) \wedge x \in dom(b) \wedge (\forall i \,.\, i \in [0,x] \Rightarrow b[i] = i^2)[\mathbf{b}'/_b]$

$\equiv$ {definizione di def}

$def(x-1) \wedge x - 1 \in dom(b) \wedge x \in dom(b) \wedge (\forall i \,.\, i \in [0,x] \Rightarrow b[i] = i^2)[\mathbf{b}'/_b]$

$\equiv$ {definizione di def}

$x - 1 \in dom(b) \wedge x \in dom(b) \wedge (\forall i \,.\, i \in [0, x] \Rightarrow b[i] = i^2)[{}^{\mathbf{b}'}/_{b}]$

$\equiv$ $\{$**Ip**: $x \in [1, n) \wedge dom(b) = [0, n)\}$

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

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

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

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

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

$\equiv$ $\{$definizione di $\mathbf{b}' = b\left[{}^{b[x-1]+2*x-1}/_{x}\right]\}$

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

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

$(b[x - 1] + 2 * x - 1 = x^2)$

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

$((x - 1)^2 + 2 * x - 1 = x^2)$

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

T