LOGICA PER LA PROGRAMMAZIONE (A,B) - a.a. 2013-2014

Seconda prova di verifica intermedia - 19/12/2013

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 provi che la seguente formula è valida (P, Q e R contengono la variabile libera x):

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

Soluzione Partiamo dalla premessa:

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

$\equiv$ {(distributività), (De Morgan)}

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

$\equiv$ {(contraddizione)}

$((\forall x\,.\,P) \wedge (\forall x\,.\,Q \vee R \Rightarrow \neg P)) \vee \mathbf{F}$

$\equiv$ {($\forall : \wedge$), (unità)}

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

$\equiv$ {(contropositiva), (De Morgan)}

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

$\Rightarrow$ {(Modus Ponens), occorrenza positiva}

$(\forall x\,.\,\neg Q \wedge \neg R)$

$\Rightarrow$ {(semplificazione-$\wedge$), occorrenza positiva}

$(\forall x\,.\,\neg Q)$

$\equiv$ {(De Morgan)}

$\neg(\exists x\,.\,Q)$

ESERCIZIO 2

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

"Nell'array **a** ci sono esattamente due numeri pari, e la loro somma è uguale alla somma di tutti gli altri elementi"

Per esempio, dei seguenti array il primo soddisfa la proprietà, mentre gli altri due no:

3	10	5	11	12	3

10	9	5	3	1	6

2	9	8	5	4

Soluzione

$$\big(\#\{x : x \in [0,n) \mid pari(a[x])\} = 2\big) \wedge \big((\Sigma y : y \in [0,n) \ \wedge \ pari(a[y])\,.\,a[y]) = (\Sigma z : z \in [0,n) \ \wedge \ \neg pari(a[z])\,.\,a[z])\big)$$

ESERCIZIO 3
Dire se la seguente tripla è verificata, motivando formalmente la risposta.
[Si ricorda che $a\ div\ b$ è il risultato della divisione intera di a per b.]

$$\{\ y > 0\ \wedge\ x \geq 0\ \wedge\ z \in [0, y)\ \}\ z := z\ div\ y;\ y := y * x\ \{\ z \leq y\ \}$$

Soluzione. La tripla è verificata. Infatti, applicando la Regola della Sequenza (SEQ), dobbiamo trovare un'asserzione R tale che le seguenti triple siano verificate:

(2.1) $\{\ y > 0\ \wedge\ x \geq 0\ \wedge\ z \in [0, y)\ \}\ z := z\ div\ y\ \{\ R\ \}$

(2.2) $\{\ R\ \}\ y := y * x\ \{\ z \leq y\ \}$

Per l'Assioma dell'Assegnamento, la (2.2) è verificata per $R \equiv def(y * x) \wedge (z \leq y)\ [^{y*x}/_{y}]$.
Quindi, semplificando, assumiamo che $R \equiv z \leq y * x$.
Per la Regola dell'Assegnamento, la (2.1) è verificata se lo è la seguente implicazione:
$y > 0\ \wedge\ x \geq 0\ \wedge\ z \in [0, y)\ \Rightarrow\ def(z\ div\ y)\ \wedge\ \big(z \leq y * x)\big)[^{z\ div\ y}/_{z}]$
Partiamo dalla conseguenza, applicando la sostituzione:

$def(z\ div\ y)\ \wedge\ (z\ div\ y \leq y * x)$
$\equiv$ {definizione di def}
$def(z)\ \wedge\ def(y)\ \wedge\ y \neq 0\ \wedge\ (z\ div\ y \leq y * x)$
$\equiv$ {definizione di def, **Ip**: $y > 0$, unità}
$z\ div\ y \leq y * x$
$\equiv$ {**Ip:** $z \in [0, y)$, $z \in [0, y) \Rightarrow z\ div\ y = 0$}
$0 \leq y * x$
$\equiv$ {**Ip:** $x \geq 0$, $y > 0$}
T

ESERCIZIO 4
Si consideri il seguente programma annotato, dove **a: array [0, n) of int**:

$\{z = A\ \wedge\ count = 0\ \wedge\ x = 0\}$
$\{\mathsf{Inv} : x \in [0, n]\ \wedge\ z = A\ \wedge\ count = \#\{y : y \in [0, x) \mid a[y] > A\}\}\{\text{t: } n - x\}$
while $(x < n)$ **do**
  if $a[x] > z$ **then** $count := count + 1$ **else skip fi**;
  $x := x + 1$
endw
$\{count = \#\{y : y \in [0, n) \mid a[y] > A\}\}$

Scrivere e dimostrare l'ipotesi di invarianza.

Soluzione. L'ipotesi di invarianza è la seguente tripla:

$\{x \in [0, n]\ \wedge\ z = A\ \wedge\ count = \#\{y : y \in [0, x) \mid a[y] > A\}\ \wedge\ x < n\}$
if $a[x] > z$ **then** $count := count + 1$ **else skip fi**;
$x := x + 1$
$\{x \in [0, n]\ \wedge\ z = A\ \wedge\ count = \#\{y : y \in [0, x) \mid a[y] > A\}\ \wedge\ def(x < n)\}$

Trattandosi di una sequenza di comandi, per la regola (SEQ) dobbiamo trovare un'asserzione R che permetta di verificare le due triple seguenti:

(1) $\{x \in [0, n]\ \wedge\ z = A\ \wedge\ count = \#\{y : y \in [0, x) \mid a[y] > A\}\ \wedge\ x < n\}$
if $a[x] > z$ **then** $count := count + 1$ **else skip fi**
$\{\ R\ \}$

(2) $\{ R \}$

$x := x + 1$

$\{x \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x) \mid a[y] > A\} \ \wedge \ def(x < n)\}$

Cominciamo dalla (2): applicando l'assioma (ASS) la tripla è verificata per

$R \ \equiv \ def(x + 1) \ \wedge \ \big(x \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x) \mid a[y] > A\} \ \wedge \ def(x < n)\big)[^{x+1}/_{x}]$

Applicando la sostituzione e semplificando otteniamo

$R \ \equiv \ x + 1 \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x] \mid a[y] > A\} \ \wedge \ def(x + 1 < n)$

Sostituendo in (1) e applicando la regola (COND), dobbiamo verificare la seguente implicazione (1.1) e le triple (1.2) e (1.3):

(1.1) $x \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x) \mid a[y] > A\} \ \wedge \ x < n \ \Rightarrow \ def(a[x] > z)$

(1.2) $\{x \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x) \mid a[y] > A\} \ \wedge \ x < n \ \wedge \ a[x] > z\}$

$count := count + 1$

$\{x + 1 \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x] \mid a[y] > A\} \ \wedge \ def(x + 1 < n)\}$

(1.3) $\{x \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x) \mid a[y] > A\} \ \wedge \ x < n \ \wedge \ a[x] \le z\}$

skip

$\{x + 1 \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x] \mid a[y] > A\} \ \wedge \ def(x + 1 < n)\}$

Per la (1.1), partiamo dalla conseguenza:

$def(a[x] > z)$

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

$x \in dom(a)$

$\equiv$ {**Ip:** $dom(a) = [1, n)$, $x \in [0, n]$, $x < n$}

T

Per la (1.2), la regola (ASS) ci dice che è sufficiente dimostrare l'implicazione:

$$x \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x) \mid a[y] > A\} \ \wedge \ x < n \wedge a[x] > z \ \Rightarrow$$
$$def(count+1) \wedge \big(x+1 \in [0, n] \wedge z = A \wedge count = \#\{y : y \in [0, x] \mid a[y] > A\} \wedge def(x+1 < n)\big)[^{count+1}/_{count}]$$

Partiamo dalla conseguenza, applicando la sostituzione e semplificandola:

$x + 1 \in [0, n] \ \wedge \ z = A \ \wedge \ count + 1 = \#\{y : y \in [0, x] \mid a[y] > A\}$

$\equiv$ {**Ip:** $x \in [0, n], x < n, z = A$, unità}

$count + 1 = \#\{y : y \in [0, x] \mid a[y] > A\}$

$\equiv$ {**Ip:** $a[x] > z, z = A$, (intervallo-#)}

$count + 1 = \#\{y : y \in [0, x) \mid a[y] > A\} + 1$

$\equiv$ {$count = \#\{y : y \in [0, x) \mid a[y] > A\}$, calcolo}

T

Infine per la (1.3) applicando la regola (SKIP), dobbiamo dimostrare che la seguente implicazione è verificata:

$$x \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x) \mid a[y] > A\} \ \wedge \ x < n \wedge a[x] \le z \ \Rightarrow$$
$$x + 1 \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x] \mid a[y] > A\} \ \wedge \ def(x + 1 < n)$$

Partiamo come al solito dalla conseguenza:

$x + 1 \in [0, n] \ \wedge \ z = A \ \wedge \ count = \#\{y : y \in [0, x] \mid a[y] > A \ \wedge \ def(x + 1 < n)\}$

$\equiv$ {**Ip:** $x \in [0, n], x < n, z = A$, definizione di *def*}

$count = \#\{y : y \in [0, x] \mid a[y] > A\}$

$\equiv$ {**Ip:** $a[x] \le z, z = A$, (intervallo-#)}

$count = \#\{y : y \in [0, x) \mid a[y] > A\}$

$\equiv$ {**Ip:** $count = \#\{y : y \in [0, x) \mid a[y] > A\}$}

T

ESERCIZIO 5

Si verifichi la seguente tripla di Hoare (assumendo **a, b: array [0, n) of int**):

$$\{z \in [1,n) \ \wedge\ (\forall i \,.\, i \in [0,z) \Rightarrow a[i] = (\Sigma y : y \in [0,i] \,.\, b[y]))\}$$
$$a[z] := a[z-1] + b[z]$$
$$\{\ (\forall i \,.\, i \in [0,z] \Rightarrow a[i] = (\Sigma y : y \in [0,i] \,.\, b[y]))\}$$

Soluzione. Per l'assioma dell'aggiornamento selettivo e la regola (PRE) è sufficiente verificare la seguente implicazione, dove $a' = a\left[{}^{a[z-1]+b[z]}/_{z}\right]$:

$$z \in [1,n) \ \wedge\ (\forall i \,.\, i \in [0,z) \Rightarrow a[i] = (\Sigma y : y \in [0,i] \,.\, b[y])) \Rightarrow$$
$$def(z) \ \wedge\ z \in dom(a) \ \wedge\ def(a[z-1]+b[z]) \ \wedge\ \big(\forall i \,.\, i \in [0,z] \Rightarrow a[i] = (\Sigma y : y \in [0,i] \,.\, b[y])\big)[{}^{a'}/_{a}]$$

Partiamo dalla conseguenza:

$def(z) \ \wedge\ z \in dom(a) \ \wedge\ def(a[z-1]+b[z]) \ \wedge\ \big(\forall i \,.\, i \in [0,z] \Rightarrow a[i] = (\Sigma y : y \in [0,i] \,.\, b[y])\big)[{}^{a'}/_{a}]$

$\equiv$ {definizione di *def*, $dom(a) = [0,n)$, **Ip:** $z \in [1,n)$, *sostituzione*}

$z-1 \in dom(a) \ \wedge\ z \in dom(b) \ \wedge\ (\forall i \,.\, i \in [0,z] \Rightarrow a'[i] = (\Sigma y : y \in [0,i] \,.\, b[y]))$

$\equiv$ {$dom(a) = dom(b) = [0,n)$, **Ip:** $z \in [1,n)$, (intervallo-$\forall$)}

$(\forall i \,.\, i \in [0,z) \Rightarrow a'[i] = (\Sigma y : y \in [0,i] \,.\, b[y])) \ \wedge\ a'[z] = (\Sigma y : y \in [0,z] \,.\, b[y])$

$\equiv$ $\big\{$**Ip:** $a' = a\left[{}^{a[z-1]+b[z]}/_{z}\right]$, $z \notin [0,z)\big\}$

$(\forall i \,.\, i \in [0,z) \Rightarrow a[i] = (\Sigma y : y \in [0,i] \,.\, b[y])) \ \wedge\ a[z-1]+b[z] = (\Sigma y : y \in [0,z] \,.\, b[y])$

$\equiv$ {**Ip:** $(\forall i \,.\, i \in [0,z) \Rightarrow a[i] = (\Sigma y : y \in [0,i] \,.\, b[y]))$, (intervallo-$\Sigma$)}

$a[z-1]+b[z] = (\Sigma y : y \in [0,z) \,.\, b[y]) + b[z]$

$\equiv$ {**Ip:** $a[z-1] = (\Sigma y : y \in [0,z-1] \,.\, b[y])$, calcolo}

T