Resolución ejercicio 1 del Primer Parcial 1C2021

Algoritmos y Estructura de Datos 1

Comisión 3

4 octubre 2021

Enunciado

Ejercicio

1 Dado el siguiente ciclo con sus correspondientes pre y postcondición:

$$P_c : \{|s| > 0 \land i = 1 \land r = \text{true}\}$$

```
while (i < s.size()) do
  r := r && (s[i - 1] == s[i]); //S1
  i := i + 1                    //S2
endwhile
```

$$Q_c : \{r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < |s| \rightarrow_L s[k] = x)\}$$

proponer un invariante I para el ciclo y demostrar que se verifican los siguientes puntos del teorema del invariante:

1. $(I \land \neg B) \Rightarrow Q_c$
2. $\{I \land B\}$ $\langle$cuerpo del ciclo$\rangle$ $\{I\}$

Resolución

Recordemos la:

$$Q_c : \{r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < |s| \rightarrow_L s[k] = x)\}$$

Resolución

Recordemos la:

$$Q_c : \{r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < |s| \rightarrow_L s[k] = x)\}$$

Proponemos el siguiente invariante I:

Resolución

Recordemos la:

$$Q_c : \{r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < |s| \rightarrow_L s[k] = x)\}$$

Proponemos el siguiente invariante I:

$$\{1 \leq i \leq |s| \wedge_L (r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x))\}$$

La resolución no lo pide pero es fácil verificar que $P_c \implies I$.

Resolución

Recordemos la:

$$Q_c : \{r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < |s| \rightarrow_L s[k] = x)\}$$

Proponemos el siguiente invariante I:

$$\{1 \leq i \leq |s| \wedge_L (r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x))\}$$

La resolución no lo pide pero es fácil verificar que $P_c \implies I$.

Ahora empecemos con la primera parte de resolución:

$I \wedge \neg B \implies Q_c$:

Resolución

Recordemos la:

$$Q_c : \{r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < |s| \rightarrow_L s[k] = x)\}$$

Proponemos el siguiente invariante I:

$$\{1 \leq i \leq |s| \wedge_L (r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x))\}$$

La resolución no lo pide pero es fácil verificar que $P_c \implies I$.

Ahora empecemos con la primera parte de resolución:

$I \wedge \neg B \implies Q_c$:

Claramente cuando termina el ciclo la negación de la guarda es $|s| \leq i$ y tomando el invariante resulta que $i = |s|$.

Resolución

Recordemos la:

$$Q_c : \{r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < |s| \rightarrow_L s[k] = x)\}$$

Proponemos el siguiente invariante I:

$$\{1 \leq i \leq |s| \wedge_L (r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x))\}$$

La resolución no lo pide pero es fácil verificar que $P_c \implies I$.

Ahora empecemos con la primera parte de resolución:

$I \wedge \neg B \implies Q_c$:

Claramente cuando termina el ciclo la negación de la guarda es $|s| \leq i$ y tomando el invariante resulta que $i = |s|$.

Y así la segunda parte del invariante es igual a Q_c.

Resolución (cont.)

Veamos la segunda condición a probar

$\{I \wedge B\} S_c \{I\}$: Para determinar que esa tripla de Hoare es válida calculemos primero la $wp(S1, wp(S2, I))$. Porqué?

Resolución (cont.)

Veamos la segunda condición a probar

$\{I \land B\}S_c\{I\}$: Para determinar que esa tripla de Hoare es válida calculemos primero la $wp(S1, wp(S2, I))$. Porqué?

Empecemos por la wp más interna:
$wp(S2, I) = def(i+1) \land_L \{I\}^i_{i+1}) = True \land_L 1 \leq i+1 \leq |s| \land_L (r = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L s[k] = x)) = E2$

Resolución (cont.)

Veamos la segunda condición a probar

$\{I \wedge B\} S_c \{I\}$: Para determinar que esa tripla de Hoare es válida calculemos primero la $wp(S1, wp(S2, I))$. Porqué?

Empecemos por la wp más interna:
$wp(S2, I) = def(i+1) \wedge_L \{I\}^i_{i+1}) = True \wedge_L 1 \leq i+1 \leq |s| \wedge_L (r =$ true $\leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L s[k] = x)) = E2$

$wp(S1, E2) = def(r \ \&\& \ (s[i-1] == s[i])) \wedge_L 1 \leq i+1 \leq |s| \wedge_L$
$(r \ \&\& \ (s[i-1] == s[i]) =$ true $\leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L$
$s[k] = x))=$
$= 0 \leq i-1 < |s| \wedge_l 0 \leq i < |s| \wedge_L 1 \leq i+1 \leq |s| \wedge_L$

Resolución (cont.)

Veamos la segunda condición a probar

$\{I \wedge B\}S_c\{I\}$: Para determinar que esa tripla de Hoare es válida calculemos primero la $wp(S1, wp(S2, I))$. Porqué?

Empecemos por la wp más interna:
$wp(S2, I) = def(i+1) \wedge_L \{I\}^{i}_{i+1}) = True \wedge_L 1 \leq i+1 \leq |s| \wedge_L (r =$ true $\leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L s[k] = x)) = E2$

$wp(S1, E2) = def(r \;\&\&\; (s[i-1] == s[i])) \wedge_L 1 \leq i+1 \leq |s| \wedge_L$
$(r \;\&\&\; (s[i-1] == s[i]) =$ true $\leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L$
$s[k] = x))=$
$= 0 \leq i-1 < |s| \wedge_l 0 \leq i < |s| \wedge_L 1 \leq i+1 \leq |s| \wedge_L ((r \;\&\&\; (s[i-1] ==$
$s[i])) =$ true $\leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L s[k] = x))$

Resolución (cont.)

Veamos la segunda condición a probar

$\{I \wedge B\} S_c \{I\}$: Para determinar que esa tripla de Hoare es válida calculemos primero la $wp(S1, wp(S2, I))$. Porqué?

Empecemos por la wp más interna:
$wp(S2, I) = def(i+1) \wedge_L \{I\}^{i}_{i+1}) = True \wedge_L 1 \leq i+1 \leq |s| \wedge_L (r =$ true $\leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L s[k] = x)) = E2$

$wp(S1, E2) = def(r \ \&\& \ (s[i-1] == s[i])) \wedge_L 1 \leq i+1 \leq |s| \wedge_L$
$(r \ \&\& \ (s[i-1] == s[i]) = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L$
$s[k] = x))=$
$= 0 \leq i-1 < |s| \wedge_I 0 \leq i < |s| \wedge_L 1 \leq i+1 \leq |s| \wedge_L ((r \ \&\& \ (s[i-1] ==$
$s[i])) = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i+1 \rightarrow_L s[k] = x))$
$=1 \leq i < |s| \wedge_L ((r \ \&\& \ (s[i-1] == s[i])) = \text{true} \leftrightarrow (\exists x : \mathbb{Z})(\forall k :$
$\mathbb{Z})(0 \leq k < i+1 \rightarrow_L s[k] = x)) = E1$

Resolución (cont.)

Ahora tenemos que ver $\{I \wedge B\} \to E1$.

Resolución (cont.)

Ahora tenemos que ver $\{I \wedge B\} \rightarrow E1$.
La guarda $i < |S|$ conjuntamente con la primera parte del invariante implican la primera parte de $E1$.

Resolución (cont.)

Ahora tenemos que ver $\{I \wedge B\} \rightarrow E1$.
La guarda $i < |S|$ conjuntamente con la primera parte del invariante implican la primera parte de $E1$.

La segunda parte del invariante la probamos por partes:
$\rightarrow$: Suponemos que vale la segunda parte del invariante y $r \;\&\&\; (s[i-1] == s[i])) = \text{true}$.
Eso implica en particular que $r = \text{true}$ y aplicando modus ponens con el invariante tenemos:

$$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x))$$

Resolución (cont.)

Ahora tenemos que ver $\{I \wedge B\} \rightarrow E1$.
La guarda $i < |S|$ conjuntamente con la primera parte del invariante implican la primera parte de $E1$.

La segunda parte del invariante la probamos por partes:
$\rightarrow$: Suponemos que vale la segunda parte del invariante y r && $(s[i-1] == s[i])) = \text{true}$.
Eso implica en particular que $r = \text{true}$ y aplicando modus ponens con el invariante tenemos:

$$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x))$$

O sea que el caso que nos falta verificar es cuando en el antecedente de la implicación $k = i$.

Resolución (cont.)

Ahora tenemos que ver $\{I \wedge B\} \rightarrow E1$.
La guarda $i < |S|$ conjuntamente con la primera parte del invariante implican la primera parte de $E1$.

La segunda parte del invariante la probamos por partes:
$\rightarrow$: Suponemos que vale la segunda parte del invariante y r && $(s[i-1] == s[i])) = \text{true}$.
Eso implica en particular que $r = \text{true}$ y aplicando modus ponens con el invariante tenemos:

$$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x))$$

O sea que el caso que nos falta verificar es cuando en el antecedente de la implicación $k = i$. Como tenemos que la instancia del invariante es cierta podemos suponer un valor para el existe que llamaremos a. Entonces sabemos que $(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = a)$. Pero como además $(s[i-1] == s[i]) = \text{true}$ resulta que $s[i] = a$.

Resolución (cont.)

$\leftarrow$: Ahora supongamos que vale el lado derecho de la equivalencia de $E1$, i.e.

$$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L s[k] = x)$$

Resolución (cont.)

$\leftarrow$: Ahora supongamos que vale el lado derecho de la equivalencia de $E1$, i.e.

$$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L s[k] = x)$$

Por lo tanto en particular será cierto que
$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x)$ que es la parte derecha de la equivalencia del invariante.

Resolución (cont.)

$\leftarrow$: Ahora supongamos que vale el lado derecho de la equivalencia de $E1$, i.e.

$$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L s[k] = x)$$

Por lo tanto en particular será cierto que $(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x)$ que es la parte derecha de la equivalencia del invariante.

Aplicando un razonamiento transitivo concluimos que $r = \text{true}$. El caso $(s[i-1] == s[i]) = \text{true}$ surge considerando $k = i$ en nuestra hipótesis de que $E1$ es cierta.

Resolución (cont.)

$\leftarrow$: Ahora supongamos que vale el lado derecho de la equivalencia de $E1$, i.e.

$$(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i + 1 \rightarrow_L s[k] = x)$$

Por lo tanto en particular será cierto que $(\exists x : \mathbb{Z})(\forall k : \mathbb{Z})(0 \leq k < i \rightarrow_L s[k] = x)$ que es la parte derecha de la equivalencia del invariante.

Aplicando un razonamiento transitivo concluimos que $r = \text{true}$. El caso $(s[i-1] == s[i]) = \text{true}$ surge considerando $k = i$ en nuestra hipótesis de que $E1$ es cierta.

De esa manera probamos que la tripla de Hoare es válida.