Ejercicio 12

Correctitud

- $Pre \longrightarrow wp(\text{codigo previo al ciclo}, P_c)$
- $P_c \longrightarrow wp(ciclo, Q_c)$
- $Q_c \longrightarrow wp(\text{codigo posterior al ciclo}, Post)$

Por monotonía sabemos que Pre $\longrightarrow$wp(programa completo, Post)

Teorema del invariante

- $P_c \longrightarrow I$
- $(I \land \neg B) \longrightarrow Q_c$
- $\{I \land B\}$ ciclo $\{I\}$
- $\{I \land B \land (v_0 = f_v)\}$ ciclo $\{f_v < v_0\}$
- $(I \land f_v \leq 0) \longrightarrow \neg B$

Demostración

Datos

- $Pre \equiv \text{true}$
- $Post \equiv r = \text{true} \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e$
- $P_c \equiv i = 0 \land j = -1$
- $Q_c \equiv j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e$
- $I \equiv 0 \leq i \leq |s| \land_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i\ \land_L s[k] = e)$
- $B \equiv i < |s|$
- $S1 \equiv \textsf{if } s[i] = e \textsf{ then } j := i \textsf{ else } skip \textsf{ fi}$
- $S2 \equiv i := i + 1$
- $ciclo \equiv S1; S2;$
- $f_v \equiv |s| - i$

$Pre \longrightarrow wp(\textbf{codigo previo al ciclo}, P_c)$

$wp(\text{codigo previo al ciclo}, P_c) \equiv$
$wp(i := 0; j := -1, j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e) \overset{Ax3}{\equiv}$
$wp(i := 0, wp(j := -1, j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e)$

- $wp(j := -1, j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e) \overset{Ax1}{\equiv}$
  $\{-1 \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e\}$

$wp(i := 0, -1 \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e) \overset{Ax1}{\equiv}$
$-1 \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s|\ \land_L s[k] = e \equiv \text{true}$
$Pre \longrightarrow wp(\text{codigo previo al ciclo}, P_c)$
$\text{true} \longrightarrow \text{true} \equiv \text{true}$

$Q_c \longrightarrow wp(\textbf{codigo posterior al ciclo}, Post)$

$wp(\text{codigo posterior al ciclo}, Post) \equiv$

$wp(\textsf{if } j \neq -1 \textsf{ then } r := \text{true} \textsf{ else } r := \text{false} \textsf{ fi}, r = \text{true} \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e) \overset{Ax4}{\equiv}$

$\{((j \neq -1) \wedge (\text{true} = \text{true} \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e))\vee$
$((j = -1) \wedge (\text{false} = \text{true} \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e))\}$

$Q_c \longrightarrow wp(\text{codigo posterior al ciclo}, Post) \equiv$

$j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e \longrightarrow$
$((j \neq -1) \wedge (\text{true} = \text{true} \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e))\vee$
$((j = -1) \wedge (\text{false} = \text{true} \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e)) \equiv \text{true}$

$P_c \longrightarrow wp(ciclo, Q_c)$

- $P_c \longrightarrow I$

  $i = 0 \wedge j = -1 \longrightarrow 0 \leq i \leq |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i \ \wedge_L s[k] = e) \equiv \text{true}$

- $(I \wedge \neg B) \longrightarrow Q_c$

  $0 \leq i \leq |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i \ \wedge_L s[k] = e) \wedge i \geq |s| \longrightarrow$

  $j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e \equiv$

  $i = |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i \ \wedge_L s[k] = e) \longrightarrow$

  $j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < |s| \ \wedge_L s[k] = e \equiv$

- $\{I \wedge B\}$ ciclo $\{I\}$

  $wp(i := i + 1, 0 \leq i \leq |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i \ \wedge_L s[k] = e)) \equiv$

  $0 \leq i + 1 \leq |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e)$

  $wp(\textsf{if } s[i] = e \textsf{ then } j := i \textsf{ else } skip \textsf{ fi}, 0 \leq i + 1 \leq |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e)) \overset{Ax4}{\equiv}$

  $0 \leq i < |s| \wedge_L ($

  $(s[i] = e) \wedge (0 \leq i + 1 \leq |s| \wedge_L (i \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e))\vee$

  $(s[i] \neq e) \wedge (0 \leq i + 1 \leq |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e))) \equiv$

  $0 \leq i < |s| \wedge_L ($

  $(s[i] = e) \wedge (i \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e)\vee$

  $(s[i] \neq e) \wedge (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e))$

  $0 \leq i < |s| \wedge_L (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i \ \wedge_L s[k] = e) \longrightarrow$

  $0 \leq i < |s| \wedge_L ($

  $(s[i] = e) \wedge (i \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e)\vee$

  $(s[i] \neq e) \wedge (j \neq -1 \leftrightarrow (\exists k : \mathbb{Z})\ 0 \leq k < i + 1 \ \wedge_L s[k] = e)) \equiv \text{true}$

- $\{I \wedge B \wedge (v_0 = f_v)\}$ ciclo $\{f_v < v_0\}$

  $wp(i : i + 1, |s| - i < v_0) \equiv |s| - i - 1 < v_0$

  $wp(\textsf{if } s[i] = e \textsf{ then } j := i \textsf{ else } skip \textsf{ fi}, |s| - i - 1) \equiv 0 \leq i < |s| \wedge_L |s| - i - 1$

  $I \wedge B \wedge v_0 = i \longrightarrow 0 \leq i < |s| \wedge_L |s| - i - 1 \equiv \text{true}$

- $(I \wedge f_v \leq 0) \longrightarrow \neg B$

  $I \wedge |s| - i \leq 0 \longrightarrow i < |s| \equiv \text{true}$