Ejercicio 13

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

- $Pre \equiv \text{true}$
- $Post \equiv r = \text{true} \leftrightarrow (\forall i : \mathbb{Z})\ 0 \leq i < |s| \ \longrightarrow_L s[i] = s[|s| - (i + 1)]$
- $P_c \equiv i = 0 \land j = |s| - 1 \land r = \text{true}$
- $Q_c \equiv r = \text{true} \leftrightarrow (\forall i : \mathbb{Z})\ 0 \leq i < |s| \ \longrightarrow_L s[i] = s[|s| - (i + 1)]$
- $I \equiv (0 \leq i \leq |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k + 1)])$
- $B \equiv i < |s|$
- $S1 \equiv \textsf{if } s[i] \neq s[j] \textsf{ then } r := \text{false} \textsf{ else } skip \textsf{ fi}$
- $S2 \equiv i := i + 1$
- $S3 \equiv j := j - 1$
- $ciclo \equiv S1; S2; S3;$
- $f_v \equiv |s| - i$

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

$wp(i := 0, wp(j : |s| - 1, wp(r := \text{true}, i = 0 \land j = |s| - 1 \land r = \text{true}))) \equiv$
$0 = 0 \land |s| - 1 = |s| - 1 \land \text{true} = \text{true} \equiv \text{true}$
$Pre \longrightarrow \text{true} \equiv \text{true} \longrightarrow \text{true}$

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

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

$r = \text{true} \leftrightarrow (\forall i : \mathbb{Z})\ 0 \leq i < |s| \ \longrightarrow_L s[i] = s[|s| - (i + 1)]$
$Q_c \longrightarrow wp(\text{codigo posterior al ciclo}, Post) \equiv$

$r = \text{true} \leftrightarrow (\forall i : \mathbb{Z})\ 0 \leq i < |s| \ \longrightarrow_L s[i] = s[|s| - (i + 1)] \longrightarrow$
$r = \text{true} \leftrightarrow (\forall i : \mathbb{Z})\ 0 \leq i < |s| \ \longrightarrow_L s[i] = s[|s| - (i + 1)] \equiv \text{true}$

$P_c \longrightarrow wp(ciclo, Q_c)$

- $P_c \longrightarrow I$

  $i = 0 \land j = |s| - 1 \land r = \text{true} \longrightarrow (0 \leq i \leq |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]) \equiv \text{true}$

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

  $(0 \leq i \leq |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]) \land i \geq |s| \longrightarrow$
  $r = \text{true} \leftrightarrow (\forall i : \mathbb{Z})\ 0 \leq i < |s| \ \longrightarrow_L s[i] = s[|s| - (i+1)] \equiv$

  $(i = |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]) \longrightarrow$
  $r = \text{true} \leftrightarrow (\forall i : \mathbb{Z})\ 0 \leq i < |s| \ \longrightarrow_L s[i] = s[|s| - (i+1)] \equiv \text{true}$

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

  $wp(S1; S2; S3, I) \overset{Ax3}{\equiv} wp(S1, wp(S2, wp(S3, I)))$

  - $wp(S3, I) \equiv wp(j := j - 1, I)$
    $\{(0 \leq i \leq |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)])\}$
  - $wp(S2, wp(S3, I)) \equiv wp(i := i + 1, wp(S3, I)) \equiv$
    $\{(0 \leq i + 1 \leq |s| \land j = |s| - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)])\}$
  - $wp(S1, wp(S2, wp(S3, I))) \equiv$
    $wp(\textsf{if}\ s[i] \neq s[j]\ \textsf{then}\ r := \text{false}\ \textsf{else}\ skip\ \textsf{fi}, (0 \leq i + 1 \leq |s| \land j = |s| - i)) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)])) \overset{Ax4}{\equiv}$
    $(0 \leq i < |s| \land 0 \leq j < |s|) \land_L ($
    $(s[i] \neq s[j] \land ((0 \leq i + 1 \leq |s| \land j = |s| - i)) \land_L (\text{false} = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]))) \lor$
    $(s[i] = s[j] \land (0 \leq i + 1 \leq |s| \land j = |s| - i)) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)])))$

  $(0 \leq i \leq |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]) \land s < |s| \equiv$

  $(0 \leq i < |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]) \longrightarrow$
  $(0 \leq i < |s| \land 0 \leq j < |s|) \land_L ($
  $(s[i] \neq s[j] \land (0 \leq i + 1 \leq |s| \land j = |s| - i)) \land_L (\text{false} = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)])) \lor$
  $(s[i] = s[j] \land (0 \leq i + 1 \leq |s| \land j = |s| - i)) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]))) \equiv$

  $(0 \leq i < |s| \land j = |s| - 1 - i) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)]) \longrightarrow$
  $(0 \leq i < |s| \land 0 \leq j < |s|) \land_L ($
  $(s[i] = s[j] \land (0 \leq i + 1 \leq |s| \land j = |s| - i)) \land_L (r = \text{true} \leftrightarrow (\forall k : \mathbb{Z})\ 0 \leq k < i \ \longrightarrow_L s[k] = s[|s| - (k+1)])) \equiv \text{true}$

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

  $wp(j : j - 1, j < v_0) \equiv j - 1 < v_0$
  $wp(i : i + 1, j - 1 < v_0) \equiv j - 1 < v_0$
  $wp(\textsf{if}\ s[i] \neq s[j]\ \textsf{then}\ r := \text{false}\ \textsf{else}\ skip\ \textsf{fi}, j - 1 < v_0) \equiv 0 \leq j|s| \land j - 1 < v_0$
  $I \land B \land v_0 = j \longrightarrow 0 \leq j|s| \land j - 1 < v_0 \equiv \text{true}$

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

  $I \land j \leq 0 \longrightarrow i < |s| \equiv \text{true}$