Demostración de correctitud del programa 1

Demostración de correctitud

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

Por monotonia sabemos que $Pre \longrightarrow wp(\text{programa completo}, Post)$

Datos

- $Pre \equiv |s| > 0$
- $Post \equiv 0 \leq r < |s| \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \wedge ((\forall j : \mathbb{Z})\ r \leq j < |s| \ \longrightarrow_L s[r] > s[j])$
- $P_c \equiv |s| > 0 \wedge i = 0 \wedge r = 0$
- $Q_c \equiv 0 \leq r < |s| \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \wedge ((\forall j : \mathbb{Z})\ r \leq j < |s| \ \longrightarrow_L s[r] > s[j])$
- $I \equiv (0 \leq i \leq |s| \wedge 0 \leq r < |s|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \wedge ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j])$
- $B \equiv i < |s|$
- $f_v \equiv |s| - i$
- $S1 \equiv \textsf{if}\ s[i] \geq s[r]\ \textsf{then}\ r := i\ \textsf{else}\ skip\ \textsf{fi}$
- $S2 \equiv i := i + 1$
- $ciclo \equiv S1; S2$

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

$wp(i := 0, wp(r := 0, |s| > 0 \wedge i = 0 \wedge r = 0)) \equiv |s| > 0$
$Pre \longrightarrow wp(\text{codigo previo al cilco}, P_c) \equiv$
$|s| > 0 \longrightarrow |s| > 0 \equiv \text{true}$

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

$Q_c \longrightarrow wp(\text{codigo post ciclo}, Post) \equiv$
$0 \leq r < |s| \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \wedge ((\forall j : \mathbb{Z})\ r \leq j < |s| \ \longrightarrow_L s[r] > s[j]) \longrightarrow$
$0 \leq r < |s| \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \wedge ((\forall j : \mathbb{Z})\ r \leq j < |s| \ \longrightarrow_L s[r] > s[j]) \equiv \text{true}$

$P_c \longrightarrow wp(ciclo, Q_c)$

Teorema del invariante

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

$P_c \longrightarrow I$

- $P_c \equiv |s| > 0 \wedge i = 0 \wedge r = 0$
- $I \equiv (0 \leq i \leq |s| \wedge 0 \leq r < |s|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \wedge ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j])$

$|s| > 0 \wedge i = 0 \wedge r = 0 \longrightarrow$
$(0 \leq i \leq |s| \wedge 0 \leq r < |s|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \wedge ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j]) \equiv \text{true}$

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

- $Q_c \equiv 0 \leq r < |s| \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < |s| \ \longrightarrow_L s[r] > s[j])$
- $I \equiv (0 \leq i \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j])$
- $B \equiv i < |s|$
- $\neg B \equiv i \geq |s|$

$(0 \leq i \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j]) \land i \geq |s| \equiv$

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

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

- $I \equiv (0 \leq i \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j])$
- $B \equiv i < |s|$
- $S1 \equiv$ if $s[i] \geq s[r]$ then $r := i$ else $skip$ fi
- $S2 \equiv i := i + 1$
- $ciclo \equiv S1; S2$
- $wp(ciclo, I) \equiv wp(S1; S2, I) \overset{Ax3}{\equiv} wp(S1, wp(S2, I))$
- $wp(S2, I) \equiv$
  $wp(i := i+1, (0 \leq i \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j])) \equiv$
  $(0 \leq i+1 \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i+1 \ \longrightarrow_L s[r] > s[j]) \equiv$
- $wp(S1, wp(S2, I)) \equiv$
  $wp($if $s[i] \geq s[r]$ then $r := i$ else $skip$ fi$, (0 \leq i+1 \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i+1 \ \longrightarrow_L s[r] > s[j])) \overset{Ax4}{\equiv}$
  $\{(0 \leq i < |s| \land 0 \leq r < |s|) \land_L ($
  $(s[i] \geq s[r]) \land 0 \leq i+1 \leq |s| \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < i \ \longrightarrow_L s[i] \geq s[j]) \land ((\forall j : \mathbb{Z})\ i \leq j < i+1 \ \longrightarrow_L s[i] > s[j])) \lor$
  $(s[i] < s[r] \land (0 \leq i+1 \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i+1 \ \longrightarrow_L s[r] > s[j]))))\}$

$I \land B \equiv (0 \leq i < |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i \ \longrightarrow_L s[r] > s[j]) \longrightarrow$
$(0 \leq i < |s| \land 0 \leq r < |s|) \land_L ($
$(s[i] \geq s[r]) \land 0 \leq i+1 \leq |s| \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < i \ \longrightarrow_L s[i] \geq s[j]) \land ((\forall j : \mathbb{Z})\ i \leq j < i+1 \ \longrightarrow_L s[i] > s[j])) \lor$
$(s[i] < s[r] \land (0 \leq i+1 \leq |s| \land 0 \leq r < |s|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < r \ \longrightarrow_L s[r] \geq s[j]) \land ((\forall j : \mathbb{Z})\ r \leq j < i+1 \ \longrightarrow_L s[r] > s[j]))) \equiv \text{true}$

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

$|s| - i = v_0 \longrightarrow |s| - i - 1 < v_0 \equiv \text{true}$

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

$|s| - i \leq 0 \longrightarrow i \geq |s|$