Ejercicio 14

Teorema del invariante

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

Demostración

Datos

- $P_c \equiv |r| = |a| + |b| \wedge |r| = |R_0| \wedge i := 0 \wedge (\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]$
- $Q_c \equiv |r| = |R_0| \wedge ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \wedge ((\forall j : \mathbb{Z})\ 0 \leq j < |b| \ \longrightarrow_L r[j + |a|] = b[j])$
- $I \equiv (0 \leq i \leq |b| \wedge |r| = |R_0| \wedge |r| = |a| + |b|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \wedge ((\forall j : \mathbb{Z})\ 0 \leq j < i \ \longrightarrow_L r[|a| + j] = b[j])$
- $B \equiv i < |b|$
- $S1 \equiv r[|a| + i] = b[i]$
- $S2 \equiv i := i + 1$
- $ciclo \equiv S1; S2$
- $f_v \equiv |b| - i$

$P_c \longrightarrow I$

$|r| = |a| + |b| \wedge |r| = |R_0| \wedge i := 0 \wedge (\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j] \longrightarrow$
$(0 \leq i \leq |b| \wedge |r| = |R_0| \wedge |r| = |a| + |b|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \wedge ((\forall j : \mathbb{Z})\ 0 \leq j < i \ \longrightarrow_L r[|a| + j] = b[j]) \equiv \text{true}$

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

$(0 \leq i \leq |b| \wedge |r| = |R_0| \wedge |r| = |a| + |b|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < |b| \ \longrightarrow_L r[|a| + j] = b[j]) \wedge i \geq |b| \equiv$

$(i = |b| \wedge |r| = |R_0| \wedge |r| = |a| + |b|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < |b| \ \longrightarrow_L r[|a| + j] = b[j]) \longrightarrow$
$(0 \leq i \leq |b| \wedge |r| = |R_0| \wedge |r| = |a| + |b|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \wedge ((\forall j : \mathbb{Z})\ 0 \leq j < i \ \longrightarrow_L r[|a| + j] = b[j]) \equiv \text{true}$

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

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

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

  - $wp(S2, I) \equiv wp(i := i + 1, I)$
    $\{(0 \leq i \leq |b| \wedge |r| = |R_0| \wedge |r| = |a| + |b|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \wedge ((\forall j : \mathbb{Z})\ 0 \leq j < i + 1 \ \longrightarrow_L r[|a| + j] = b[j])\}$
  - $wp(S1, wp(S2, I)) \equiv wp(r[|a| + i] = b[i], wp(S2, I)) \equiv$
    $\{(0 \leq i < |b| \wedge |r| = |R_0| \wedge |r| = |a| + |b|) \wedge_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \wedge ((\forall j : \mathbb{Z})\ 0 \leq j < i + 1 \ \longrightarrow_L setAt(r, |a| + j, b[i])[|a| + j] = b[j])\}$

$(0 \leq i \leq |b| \land |r| = |R_0| \land |r| = |a| + |b|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \land ((\forall j : \mathbb{Z})\ 0 \leq j < i \ \longrightarrow_L r[|a| + j] = b[j]) \land i < |b| \equiv$

$(0 \leq i < |b| \land |r| = |R_0| \land |r| = |a| + |b|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \land ((\forall j : \mathbb{Z})\ 0 \leq j < i \ \longrightarrow_L r[|a| + j] = b[j]) \longrightarrow$
$(0 \leq i < |b| \land |r| = |R_0| \land |r| = |a| + |b|) \land_L ((\forall j : \mathbb{Z})\ 0 \leq j < |a| \ \longrightarrow_L r[j] = a[j]) \land ((\forall j : \mathbb{Z})\ 0 \leq j < i + 1 \ \longrightarrow_L setAt(r, |a| + j, b[i])[|a| + j] = b[j]) \equiv \text{true}$

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

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

$wp(r[i] = a[i], |b| - i - 1 < v_0) \equiv 0 \leq i < |b| \land |b| - i - 1 < v_0$

$I \land B \land v_0 = |a| - i \longrightarrow 0 \leq i < |b| \land |b| - i - 1 < v_0 \equiv \text{true}$

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

$I \land |b| - i \leq 0 \longrightarrow i < |b| \equiv \text{true}$