Datos

- $Q_c \equiv \{|s| = |s_0| \wedge_L (\forall k : \mathbb{Z})\ 0 \leq k < |s| \ \longrightarrow_L s[k] = s_0[k] \cdot n\}$
- $I \equiv \{-1 \leq i \leq |s| - 1 \wedge |s| = |s_0| \wedge_L$
  $(\forall j : \mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
  $(\forall j : \mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j])\}$
- $B \equiv \{i \geq 0\}$
- $S1 \equiv s[i] := s[i] \cdot n;$
- $S2 \equiv i := i - 1$
- $ciclo \equiv S1; S2;$
- $(I \wedge \neg B) \longrightarrow Q_c$
- $\{I \wedge B\}$ ciclo $\{I\}$

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

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

    $wp(S2, I) \equiv wp(i := i - 1, I) \overset{Ax1}{\equiv}$

    $\{\ def(i-1) \wedge I^i_{i-1}\ \} \equiv$

    $\{\ \text{true} \wedge I^i_{i-1}\ \} \equiv$

    $\{\ I^i_{i-1}\ \} \equiv$

    $\{\ -1 \leq i - 1 \leq |s| - 1 \wedge |s| = |s_0| \wedge_L$
    $(\forall j : \mathbb{Z})(i - 1 < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
    $(\forall j : \mathbb{Z})(0 < j \leq i - 1 \longrightarrow_L s[j] = s_0[j])\ \}$
  - $wp(S1, wp(S2, I))$

    $wp(S1, wp(S2, I)) \equiv wp(s[i] := s[i] \cdot n; , wp(S2; I)) \equiv wp(s := setAt(s, i, s[i] \cdot n); , wp(S2, I)) \overset{Ax1}{\equiv}$

    $\{def(setAt(s, i, s[i] \cdot n)) \wedge wp(S2, I)^s_{setAt(s,i,s[i] \cdot n)}\} \equiv$

    $\{((def(s) \wedge def(i)) \wedge_L 0 \leq i \leq |s|) \wedge (s[i] \cdot n) \wedge wp(S2, I)^s_{setAt(s,i,s[i] \cdot n)}\} \equiv$

    $\{0 \leq i \leq |s| \wedge wp(S2, I)^s_{setAt(s,i,s[i] \cdot n)}\} \equiv$

    $\{\ 0 \leq i \leq |s| \wedge -1 \leq i - 1 \leq |setAt(s, i, s[i] \cdot n)| - 1 \wedge |setAt(s, i, s[i] * n)| = |s_0| \wedge_L$
    $(\forall j : \mathbb{Z})(i - 1 < j < |setAt(s, i, s[i] \cdot n)| \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j] \cdot n) \wedge$
    $(\forall j : \mathbb{Z})(0 < j \leq i - 1 \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j])\ \} \equiv$

    $\{\ 0 \leq i \leq |s| \wedge |setAt(s, i, s[i] \cdot n)| = |s_0| \wedge_L$
    $(\forall j : \mathbb{Z})(i - 1 < j < |setAt(s, i, s[i] \cdot n)| \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j] \cdot n) \wedge$
    $(\forall j : \mathbb{Z})(0 < j \leq i - 1 \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j])\ \}$
- $\{\ I \wedge B\ \}$

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

  $\{-1 \leq i \leq |s|-1 \wedge |s| = |s_0| \wedge_L$
  $(\forall j : \mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
  $(\forall j : \mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j]) \wedge i \geq 0\} \stackrel{(-1 \leq i \leq |s|-1) \wedge (i \geq 0) \longrightarrow (0 \leq i \leq |s|-1)}{\equiv}$

  $\{0 \leq i \leq |s|-1 \wedge |s| = |s_0| \wedge_L$
  $(\forall j : \mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
  $(\forall j : \mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j])\}$

- QvQ $\{I \wedge B\} \longrightarrow wp(ciclo, I)$
  $\{I \wedge B\} \longrightarrow wp(ciclo, I) \equiv$

  $\Big\{0 \leq i \leq |s|-1 \wedge |s| = |s_0| \wedge_L$
  $(\forall j : \mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
  $(\forall j : \mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j])\Big\} \longrightarrow$
  $\Big\{0 \leq i \leq |s| \wedge |setAt(s, i, s[i] \cdot n)| = |s_0| \wedge_L$
  $(\forall j : \mathbb{Z})(i-1 < j < |setAt(s, i, s[i] \cdot n)| \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j] \cdot n) \wedge$
  $(\forall j : \mathbb{Z})(0 < j \leq i-1 \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j])\Big\}$

  - $\{0 \leq i \leq |s|-1 \wedge |s| = |s_0|\} \longrightarrow$
    $\{0 \leq i \leq |s| \wedge |setAt(s, i, s[i] \cdot n)| = |s_0|\}$ es tautología ya que el antecedente es mas fuerte
  - $\{(\forall j : \mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j])\} \longrightarrow$
    $\{(\forall j : \mathbb{Z})(0 < j \leq i-1 \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j])\}$ es tautología ya que el antecedente es mas fuerte
  - $\{(\forall j : \mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n)\} \longrightarrow$
    $\{(\forall j : \mathbb{Z})(i-1 < j < |setAt(s, i, s[i] \cdot n)| \longrightarrow_L setAt(s, i, s[i] \cdot n)[j] = s_0[j] \cdot n)\}$

    es tautología ya que cuando $j = i \longrightarrow$
    $setAt(s, i, s[i] \cdot n)[j] = setAt(s, i, s[i] \cdot n)[i] \stackrel{Por\ defición\ de\ setAt()}{=} s[i] \cdot n = s[j] \cdot n = s_0[i] \cdot n$
    y cuando $j \neq i \longrightarrow setAt(s, i, s[i] \cdot n)[j] = s[j]$

  Por lo tanto cuando se ejecuta el cuerpo del ciclo se preserva el invariante. $\square$

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

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

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

  $-1 \leq i \leq |s|-1 \wedge |s| = |s_0| \wedge_L$
  $(\forall j : \mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
  $(\forall j : \mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j]) \wedge \neg(i \geq 0) \longrightarrow$
  $|s| = |s_0| \wedge_L (\forall k : \mathbb{Z}) \ 0 \leq k < |s| \ \longrightarrow_L s[k] = s_0[k] \cdot n \stackrel{\neg(i \geq 0) \equiv i < 0}{\equiv}$

$-1 \leq i \leq |s|-1 \wedge |s| = |s_0| \wedge_L$
$(\forall j:\mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
$(\forall j:\mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j]) \wedge i < 0 \longrightarrow$
$|s| = |s_0| \wedge_L (\forall k:\mathbb{Z})\ 0 \leq k < |s| \ \longrightarrow_L s[k] = s_0[k] \cdot n \overset{((i<0)\ \wedge\ (-1 \leq i \leq |s|-1)) \longrightarrow i=-1}{\equiv}$

$i = -1 \wedge |s| = |s_0| \wedge_L$
$(\forall j:\mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
$(\forall j:\mathbb{Z})(0 < j \leq i \longrightarrow_L s[j] = s_0[j]) \longrightarrow$
$|s| = |s_0| \wedge_L (\forall k:\mathbb{Z})\ 0 \leq k < |s| \ \longrightarrow_L s[k] = s_0[k] \cdot n \overset{por\ vacuidad}{\equiv}$

$i = -1 \wedge |s| = |s_0| \wedge_L$
$(\forall j:\mathbb{Z})(i < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \wedge$
true $\longrightarrow$
$|s| = |s_0| \wedge_L (\forall k:\mathbb{Z})\ 0 \leq k < |s| \ \longrightarrow_L s[k] = s_0[k] \cdot n \overset{p\ \wedge\ \text{true} \longrightarrow p}{\equiv}$

$|s| = |s_0| \wedge_L$
$(\forall j:\mathbb{Z})(-1 < j < |s| \longrightarrow_L s[j] = s_0[j] \cdot n) \ \longrightarrow$
$|s| = |s_0| \wedge_L (\forall k:\mathbb{Z})\ 0 \leq k < |s| \ \longrightarrow_L s[k] = s_0[k] \cdot n$

Que son la misma proposición con distinto nombre de variable (j y k) que se mueven dentro del mismo rango, por lo tanto es una tautología y al ejecutar el programa se cumple la postcondición. $\square$