VERIFICACIÓN DE PROGRAMAS IMPERATIVOS

Propiedades de la Tripla de Hoare

1. {P} Skip {P}
2. {P} $x := E$ {Q} $\equiv$ {P} $\rightarrow$ {Q}$[x := E]$
3. {P} S, T {Q} $\equiv$ ($\exists$ {Q} : : {P} S {Q'} $\wedge$ {Q'} T {Q})
4. {P}
   If B Then {P∧B} S_1 {Q}
   Else {P∧¬B} S_2 {Q}
   EndIf
   {Q}
5. {P}
   {P}→{I}
   While B Do
   {I∧B} A {I}
   {I∧B∧t=C} A {t<C}
   {I∧B}→$t \geq 0$
   Done
   {I∧¬B}→{Q}
   {Q}

La invariante {I} describe los distintos estados por los que pasa el ciclo, dando la relación existente entre las variables que intervienen en este.

La invariante {I} debe cumplir las siguientes condiciones:

- ⋆ **I.1** Se satisface antes de empezar el ciclo, es decir, antes de la primera iteración:

  {P}→{I}

- ⋆ **I.2** Se mantiene al ejecutar el cuerpo A del bucle:

  {I∧B} A {I}

- ⋆ **I.3** Se cumple al salir del ciclo, cuando B se hace falsa:

  {I∧¬B}→{Q}

  Además, se debe probar que el ciclo es finito. Para lo cual se debe buscar una función t que dependa de las variables del ciclo y que tome valores enteros, de tal forma que cumpla que:

- ⋆ **C.1** Es mayor que cero cuando se cumple la condición B:

  {I∧B}→$t \geq 0$

- ⋆ **C.2** Decrece al ejecutar el cuerpo A del ciclo

  {I∧B∧t=C} A {t<C}

  Donde, C es cualquier constante entera.

EJEMPLOS

A. Potencia n^m

$\{P \equiv m \geq 0 \wedge n > 0\}$
$r \leftarrow 1$
$i \leftarrow 0$
$\{I \equiv r = n^i \wedge i \leq m \wedge n > 0\}$
$WHILE\ (i < m)\ DO$
$\quad r \leftarrow r * n$
$\quad i \leftarrow i + 1$
END
$\{Q \equiv r = n^m\}$

I.1

$\{P \equiv m \geq 0 \wedge n > 0\}$
$r \leftarrow 1$
$i \leftarrow 0$
$\{I \equiv r = n^i \wedge i \leq m\}$

Demostración:

$\{I'' \equiv 1 = 1 \wedge 0 \leq m \wedge n > 0\}$ True $I'' \equiv P$
$r \leftarrow 1$
$\{I' \equiv r = n^0 \wedge 0 \leq m \wedge n > 0\}$
$i \leftarrow 0$
$\{I \equiv r = n^i \wedge i \leq m \wedge n > 0\}$

I.2

$\{I \wedge B \equiv r = n^i \wedge i \leq m \wedge n > 0 \wedge i < m\}$
$r \leftarrow r * n$
$i \leftarrow i + 1$
$\{I \equiv r = n^i \wedge i \leq m\}$

Demostración:

$\{I'' \equiv r * n = n^{i+1} \wedge i + 1 \leq m\}$ True $I'' \equiv I \wedge B$
$r \leftarrow r * n$
$\{I' \equiv r = n^{i+1} \wedge i + 1 \leq m\}$
$i \leftarrow i + 1$
$\{I \equiv r = n^i \wedge i \leq m\}$

I.3

$\{I \wedge \neg B \equiv r = n^i \wedge i \leq m \wedge n > 0 \wedge i \geq m\} \rightarrow \{Q \equiv r = n^m\}$

Demostración:

$\{I \wedge \neg B \equiv r = n^i \wedge i = m \wedge n > 0\} \rightarrow \{Q \equiv r = n^m\}$ True

C.1

$\{I \wedge B \equiv r = n^i \wedge i \leq m \wedge n > 0 \wedge i < m\} \rightarrow \{t \geq 0\}$ donde $t = m - i$

Demostración:

$\{I \wedge B \equiv r = n^i \wedge i < m \wedge n > 0\} \rightarrow \{m - i \geq 0\}$
$\{I \wedge B \equiv r = n^i \wedge i < m \wedge n > 0\} \rightarrow \{m > i \vee m = i\}$ True

C.2

$\{I \wedge B \wedge t = C \equiv r = n^i \wedge i \leq m \wedge n > 0 \wedge i < m \wedge m - i = C\}$
$r \leftarrow r * n$
$i \leftarrow i + 1$
$\{m - i < C\}$

Demostración:

$\{m - i - 1 < C\}$ True con $m - i = C$
$r \leftarrow r * n$
$\{m - i - 1 < C\}$
$i \leftarrow i + 1$
$\{m - i < C\}$

B. Factorial n

1: $\{P \equiv n \geq 0\}$
2: $f \leftarrow 1$
3: $i \leftarrow 1$
4: $\{I \equiv f = (i-1)! \wedge i \leq n + 1\}$
5: $WHILE\ (i \leq n)\ DO$
6: $\quad f \leftarrow f * i$
7: $\quad i \leftarrow i + 1$
8: END
9: $\{Q \equiv f = n!\}$

I.1

$\{P \equiv n \geq 0\}$
$f \leftarrow 1$
$i \leftarrow 1$
$\{I \equiv f = (i-1)! \wedge i \leq n + 1\}$

Demostración:

$\{I'' \equiv 1 = 0! \wedge 1 \leq n + 1\}$ True $I'' \equiv P$
$f \leftarrow 1$
$\{I' \equiv f = (1-1)! \wedge 1 \leq n + 1\}$
$i \leftarrow 1$
$\{I \equiv f = (i-1)! \wedge i \leq n + 1\}$

I.2

$\{I \wedge B \equiv f = (i-1)! \wedge i \leq n + 1 \wedge i \leq n\}$
$f \leftarrow f * i$
$i \leftarrow i + 1$
$\{I \equiv f = (i-1)! \wedge i \leq n + 1\}$

Demostración:

$\{I'' \equiv f * i = i! \wedge i \leq n\}$ True $I'' \equiv I \wedge B$
$f \leftarrow f * i$
$\{I' \equiv f = (i+1-1)! \wedge i + 1 \leq n + 1\}$
$i \leftarrow i + 1$
$\{I \equiv f = (i-1)! \wedge i \leq n + 1\}$

I.3

$\{I \wedge \neg B \equiv f = (i-1)! \wedge i \leq n+1 \wedge i > n\} \rightarrow \{Q \equiv f = n!\}$

Demostración:

$\{I \wedge \neg B \equiv f = (i-1)! \wedge i = n+1\} \rightarrow \{Q \equiv f = n!\}$ True

C.1

$\{I \wedge B \equiv f = (i-1)! \wedge i \leq n+1 \wedge i \leq n\} \rightarrow \{t \geq 0\}$ donde $t = n - i$

Demostración:

$\{I \wedge B \equiv f = (i-1)! \wedge i \leq n+1 \wedge i \leq n\} \rightarrow \{n \geq i\}$ True

C.2

$\{I \wedge B \wedge t = C \equiv f = (i-1)! \wedge i \leq n+1 \wedge i \leq n \wedge n - i = C\}$
$f \leftarrow f * i$
$i \leftarrow i + 1$
$\{n - i < C\}$

Demostración:

$\{n - i - 1 < C\}$ True con $n - i = C$
$f \leftarrow f * i$
$\{n - i - 1 < C\}$
$i \leftarrow i + 1$
$\{n - i < C\}$

C. Producto punto $A_{[0 \ldots n-1]} * B_{[0 \ldots n-1]}$

1: $\{P \equiv n \geq 0\}$
2: $k \leftarrow 0$
3: $i \leftarrow 0$
4: $\{I \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha)\}$
5: $WHILE\ (i < n)\ DO$
6: $\quad k \leftarrow k + A_i * B_i$
7: $\quad i \leftarrow i + 1$
8: END
9: $\{Q \equiv k = (\sum \alpha : 0 \leq \alpha < n : A_\alpha * B_\alpha)\}$

I.1

$\{P \equiv n \geq 0\}$
$k \leftarrow 0$
$i \leftarrow 0$
$\{I \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha\}$

Demostración:

True por propiedad de cuantificador $\sum$ con rango nulo es igual a 0 [1]
$\{I \equiv 0 \geq 0 \wedge n \geq 0 \wedge 0 = (\sum \alpha : 0 \leq \alpha < 0 : A_\alpha * B_\alpha\}$

[1] Peña Marí Ricardo. Diseño de programas: Formalismo y Abstracción. Segunda edición. Pág 44.

$k \leftarrow 0$
$\{I \equiv 0 \geq 0 \wedge n \geq 0 \wedge k = (\sum \alpha : 0 \leq \alpha < 0 : A_\alpha * B_\alpha\}$
$i \leftarrow 0$
$\{I \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha\}$

I.2

$\{I \wedge B \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha) \wedge i < n\}$
$k \leftarrow k + A_i * B_i$
$i \leftarrow i + 1$
$\{I \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha)\}$

Demostración:

True por $0 \leq i + 1 \leq n \equiv 0 \leq i < n$ y despejando k entonces $I'' \equiv I \wedge B$
$\{I'' \equiv i + 1 \geq 0 \wedge n \geq i + 1 \wedge k + A_i * B_i = (\sum \alpha : 0 \leq \alpha < i + 1 : A_\alpha * B_\alpha)\}$
$k \leftarrow k + A_i * B_i$
$\{I' \equiv i + 1 \geq 0 \wedge n \geq i + 1 \wedge k = (\sum \alpha : 0 \leq \alpha < i + 1 : A_\alpha * B_\alpha)\}$
$i \leftarrow i + 1$
$\{I \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha)\}$

I.3

$\{I \wedge \neg B \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha) \wedge n \leq i\} \rightarrow \{Q \equiv k = (\sum \alpha : 0 \leq \alpha < n : A_\alpha * B_\alpha)\}$

Demostración:

$\{I \wedge \neg B \equiv i \geq 0 \wedge n = i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha)\} \rightarrow \{Q \equiv k = (\sum \alpha : 0 \leq \alpha < n : A_\alpha * B_\alpha)\}$ True

C.1

$\{I \wedge B \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha) \wedge i < n\} \rightarrow \{t \geq 0\}$ donde $t = n - i$

Demostración:

$\{I \wedge B \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha) \wedge i < n\} \rightarrow \{n \geq i\}$ True

C.2

$\{I \wedge B \wedge t = C \equiv i \geq 0 \wedge n \geq i \wedge k = (\sum \alpha : 0 \leq \alpha < i : A_\alpha * B_\alpha) \wedge i < n \wedge n - i = C\}$
$k \leftarrow k + A_i * B_i$
$i \leftarrow i + 1$
$\{n - i < C\}$

Demostración:

$\{n - i - 1 < C\}$ True con $n - i = C$
$k \leftarrow k + A_i * B_i$
$\{n - i - 1 < C\}$
$i \leftarrow i + 1$
$\{n - i < C\}$