Demostración de ciclos

> In many of the more relaxed civilizations on the Outer Eastern Rim of the Galaxy, the *Hitchhiker's Guide* has already suplanted the great *Encyclopedia Galactica* as the standard repository of all knowledge and wisdom, for though it has many omissions and contains much that is apocryphal, or at least wildly inaccurate, it scores over the older, more pedestrian work in two important respects.
>
> First, it is slighty cheaper; and second it has the words DON'T PANIC inscribed in large friendly letters on its cover.
>
> Douglas Adams
> *The Hitchhiker Guide to the Galaxy*

Ejemplo 0.1 (Suma)
Dados dos números, hay que encontrar la suma de ambos usando sólo incrementos y decrementos de una unidad.

Damos directamente el programa y procedemos a su verificación.

$[\![\text{var } m, n : Int$
$\{R : \quad m = A \wedge n = B \wedge m \geq 0 \wedge n \geq 0\}$ (precondición)
$\{P : \quad m + n = A + B\}$
$\underline{\textbf{do}}\ n \neq 0 \rightarrow$
$\quad m, n := m + 1, n - 1$
$\underline{\textbf{od}}$
$\{Q : \quad m = A + B\}$ (postcondición)
$]\!]$

Demostraremos la corrección (parcial, no nos ocupamos del problema de la terminación) del programa respecto de la especificación.

Primero veamos que el invariante P vale inicialmente (es decir que es implicado por la precondición). Esto es inmediato, dado que como vale que $m = A$ y $n = B$ reemplazando iguales por iguales sale que $m + n = A + B$

Para demostrar un ciclo tenemos que considerar dos cosas: que el invariante es invariante y que al terminar vale la postcondición.

La primera de estas propiedades puede escribirse como sigue:

$$P \wedge n \neq 0 \Rightarrow wlp.(m, n := m + 1, n - 1).P$$

mientras que la condición de terminación dice que:

$$P \wedge n = 0 \Rightarrow m = A + B$$

Para la primera demostración asumo que P es válido así también como $n \neq 0$ (esta última aserción no va a ser necesaria en la demostración) y procedo a demostrar el consecuente de la implicación:

$wlp.(m, n := m + 1, n - 1).P$
$\equiv$ { definición de wlp y de P }
$(m, n := m + 1, n - 1).(m + n = A + B)$

$\equiv$ { sustitución en predicados }

$(m+1)+(n-1) = A+B$

$\equiv$ { álgebra }

$m+n = A+B$

$\equiv$ { P }

$True$

Vamos a demostrar ahora que al terminar vale la postcondición, o sea que asumiendo que vale P y que $n = 0$ podemos demostrar que $m = A+B$

$m = A+B$

$\equiv$ { álgebra, nos orientamos a usar P }

$m+0 = A+B$

$\equiv$ { $n = 0$ vale dado que la guarda es falsa al terminar el ciclo }

$m+n = A+B$

$\equiv$ { P }

$True$