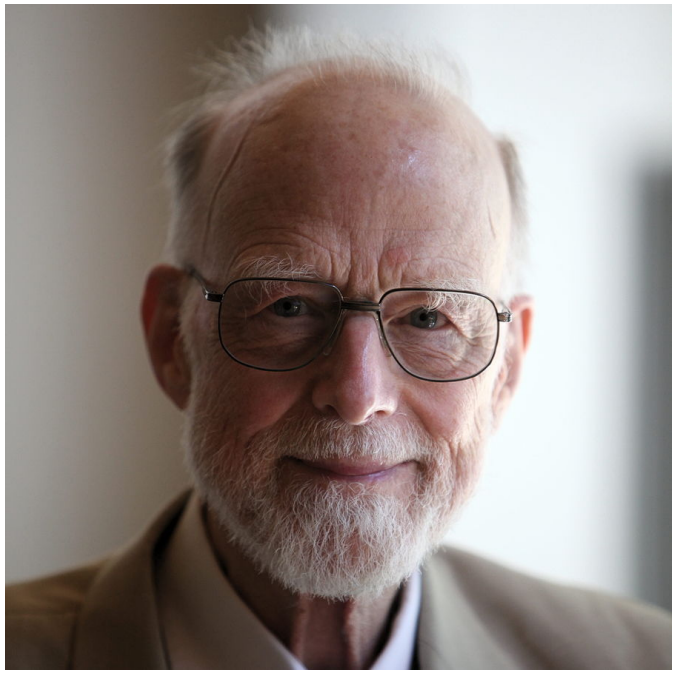
Correctitud de algoritmos

Introducción a la computación (Matemática)

Motivación



Tony Hoare - Turing Award 1980

"When the correctness of a program, its compiler, and the hardware of the computer have all been established with mathematical certainty, it will be possible to place great reliance on the results of the program, and predict their properties with a confidence limited only by the reliability of the electronics."

(**Especificación** de un **Problema**)

Encabezado: $sucesor: x \in \mathbb{Z} \to \mathbb{Z}$

Precondición: $\{x = x_0\}$

Poscondición: $\{RV = x_0 + 1\}$

(**Pseudocódigo** de un **Algoritmo**)

Algoritmo: $RV \leftarrow x + 1$

“una **demostración formal** de que el **algoritmo** transforma todos los posibles datos de entrada, en salidas de acuerdo con la **especificación**"

Demostración

$P = \{x = x_0\}$, $S = RV \leftarrow x + 1$, $Q = \{RV = x_0 + 1\}$

¿$sp(S, P) \Rightarrow Q$?

$sp(S, P)$

$\equiv sp(RV \leftarrow x + 1, x = x_0)$

$\equiv (\exists y) RV = (x + 1)[RV : y] \wedge (x = x_0)[RV : y]$

$\equiv (\exists y) RV = (x + 1) \wedge (x = x_0)$

$\equiv RV = (x + 1) \wedge (x = x_0)$

$\Rightarrow RV = x_0 + 1$

Demostrar que el siguiente algoritmo es correcto respecto de su especificación.

Encabezado:	$ocho{:}x \in \mathbb{Z} \to \mathbb{Z}$
Precondición:	$\{true\}$
Poscondición:	$\{RV = 8\}$
Algoritmo:	$RV \leftarrow 8$

Demostración

$P = \{true\}$, $S = RV \leftarrow 8$, $Q = \{RV = 8\}$ ¿$sp(S, P) \Rightarrow Q$?

$sp(S, P)$

$\equiv sp(RV \leftarrow 8, true)$

$\equiv (\exists v) RV = 8[RV : v] \wedge true[RV : v]$

$\equiv (\exists v) RV = 8 \wedge true$

$\equiv RV = 8 \wedge true$

$\Rightarrow RV = 8$

Demostrar que el siguiente algoritmo es correcto respecto de su especificación.

Encabezado:	*producto:*$x \in \mathbb{Z} \times y \in \mathbb{Z} \to \mathbb{Z}$
Precondición:	$\{x = x_0 \wedge y = y_0\}$
Poscondición:	$\{RV = x_0 * y_0\}$
Algoritmo:	$RV \leftarrow x$
	$RV \leftarrow RV * y$

$P = \{x = x_0 \wedge y = y_0\}$, $S = \{RV \leftarrow x; RV \leftarrow RV * y\}$,
$Q = \{RV = x_0 * y_0\}$ ¿$sp(S, P) \Rightarrow Q$?

$sp(S, P) \equiv sp(RV \leftarrow x; RV \leftarrow RV * y, x = x_0 \wedge y = y_0)$

$\equiv sp(RV \leftarrow RV * y, sp(RV \leftarrow x, x = x_0 \wedge y = y_0))$

$\equiv sp(RV \leftarrow RV * y, (\exists v)RV = x[RV : v] \wedge$
$(x = x_0 \wedge y = y_0)[RV : v])$

$\equiv sp(RV \leftarrow RV * y, (\exists v)RV = x \wedge x = x_0 \wedge y = y_0)$

$\equiv sp(RV \leftarrow RV * y, RV = x \wedge x = x_0 \wedge y = y_0)$

$\equiv (\exists v)RV = RV * y[RV : v] \wedge (RV = x \wedge x = x_0 \wedge y = y_0)[RV : v]$

$\equiv (\exists v)RV = v * y \wedge (v = x \wedge x = x_0 \wedge y = y_0)$

$\Rightarrow RV = x_0 * y_0$

Demostrar que el siguiente algoritmo es correcto respecto de su especificación.

Encabezado: *distintos*:$x \in \mathbb{Z} \times y \in \mathbb{Z} \to \mathbb{B}$

Precondición: $\{x = x_0 \wedge y = y_0\}$

Poscondición: $\{RV = (x_0 \neq y_0)\}$

Algoritmo:

```
if (x ≠ y) {
    RV ← true
} else {
    RV ← false
}
```

$P = \{x = x_0 \wedge y = y_0\}$, $S = \{\ldots\}$, $Q = \{RV = (x_0 \neq y_0)\}$

¿$sp(S, P) \Rightarrow Q$?

$sp(S, P) \equiv sp(S, x = x_0 \wedge y = y_0)$

$\equiv sp(RV \leftarrow true, x \neq y \wedge x = x_0 \wedge y = y_0) \vee$

$sp(RV \leftarrow false, x = y \wedge x = x_0 \wedge y = y_0)$

$\equiv (\exists v) RV = true[RV : v] \wedge (x \neq y \wedge x = x_0 \wedge y = y_0)[RV : v] \vee$

$(\exists w) RV = false[RV : w] \wedge (x = y \wedge x = x_0 \wedge y = y_0)[RV : w]$

$\equiv RV = true \wedge (x \neq y \wedge x = x_0 \wedge y = y_0) \vee$

$RV = false \wedge (x = y \wedge x = x_0 \wedge y = y_0)$

$\Rightarrow (RV = true \wedge x_0 \neq y_0) \vee (RV = false \wedge (x_0 = y_0))$

$\Rightarrow RV = (x_0 \neq y_0)$

¿El algoritmo es correcto respecto de la especificación?

Encabezado: $swap: x \in \mathbb{Z} \times y \in \mathbb{Z} \to \emptyset$

Precondición: $\{x = x_0 \wedge y = y_0\}$

Poscondición: $\{x = y_0 \wedge y = x_0\}$

Algoritmo:

$$x \leftarrow x + y$$
$$y \leftarrow x - y$$
$$x \leftarrow x - y$$

$P = \{x = x_0 \land y = y_0\}$, $S = \{\ldots\}$, $Q = \{x = y_0 \land y = x_0\}$

¿$sp(S, P) \Rightarrow Q$?

$sp(S, P) \equiv sp(x \leftarrow x + y; y \leftarrow x - y; x \leftarrow x - y, x = x_0 \land y = y_0)$

$\equiv sp(y \leftarrow x - y; x \leftarrow x - y, sp(x \leftarrow x + y, x = x_0 \land y = y_0))$

$\equiv sp(y \leftarrow x - y; x \leftarrow x - y,$
$(\exists v)x = x + y[x : v] \land (x = x_0 \land y = y_0)[x : v])$

$\equiv sp(y \leftarrow x - y; x \leftarrow x - y, (\exists v)x = v + y \land (v = x_0 \land y = y_0))$

$\equiv sp(y \leftarrow x - y; x \leftarrow x - y, x = x_0 + y \land y = y_0)$

$\equiv sp(x \leftarrow x - y, sp(y \leftarrow x - y, x = x_0 + y \land y = y_0))$

$\equiv sp(x \leftarrow x - y, (\exists v)y = x - y[y : v] \land (x = x_0 + y \land y = y_0)[y : v])$

$\equiv sp(x \leftarrow x - y, (\exists v)y = x - v \land x = x_0 + v \land v = y_0)$

$$\equiv sp(x \leftarrow x - y, (\exists v) y = x - v \wedge x = x_0 + v \wedge v = y_0)$$

$$\equiv sp(x \leftarrow x - y, y = x - y_0 \wedge x = x_0 + y_0)$$

$$\equiv sp(x \leftarrow x - y, y = x_0 \wedge x = x_0 + y_0)$$

$$\equiv (\exists v) x = x - y[x : v] \wedge (y = x_0 \wedge x = x_0 + y_0)[x : v]$$

$$\equiv (\exists v) x = v - y \wedge y = x_0 \wedge v = x_0 + y_0$$

$$\equiv x = x_0 + y_0 - x_0 \wedge y = x_0$$

$$\Rightarrow x = y_0 \wedge y = x_0$$

¿Preguntas?