Diseño Iterativo

Yolanda Ortega Mallén

Dpto. de Sistemas Informáticos y Computación

Universidad Complutense de Madrid

Objetivos

1. Aprender un sistema de reglas de inferencia que nos permiten razonar sobre el comportamiento de algoritmos iterativos.
2. Utilizar las reglas para comprobar que un programa es correcto respecto a su especificación.
3. Implementar un programa correcto por derivación a partir de la especificación del problema.
4. Ver soluciones de problemas iterativos típicos para conocer diversas formas de solución.

Sumario

- Semántica axiomática.
- Verificación de algoritmos.
- Derivación formal de algoritmos.

Bibliografía

- R. Peña. *Diseño de programas. Formalismo y abstracción*. Tercera edición. Prentice Hall, 2005. Capítulo 4.
- N. Martí Oliet, C. Segura Díaz y J. A. Verdejo López. *Algoritmos correctos y eficientes: diseño razonado ilustrado con ejercicios*. Garceta Grupo Editorial, 2012. Capítulos 2 y 4.
- A. Kaldewaij. *The derivation of algorithms*. Prentice Hall, 1990.

Lenguaje imperativo	programa = secuencia de órdenes.
Estado	valores asociados a las variables del programa.
Cómputo	ejecución de la secuencia de órdenes desde un estado inicial hasta alcanzar un estado final.
Especificación	relación entre el estado inicial y el estado final del cómputo de un programa, $\{A\}\ P\ \{B\}$.
Semántica axiomática	axiomas + reglas de inferencia.

$$\frac{\textit{Premisas}}{\textit{Conclusión}}$$

Demostrar teoremas del tipo $\{A\}\ P\ \{B\}$.

Fortalecimiento de la precondición

Si P cumple la siguiente especificación:

$$\begin{array}{c} \{x \leq 5\} \\ P \\ \{x \leq 10\} \end{array}$$

¿Qué ocurre si cambiamos la precondición por un predicado que la implique?

$$x \leq -7 \Rightarrow x \leq 5$$

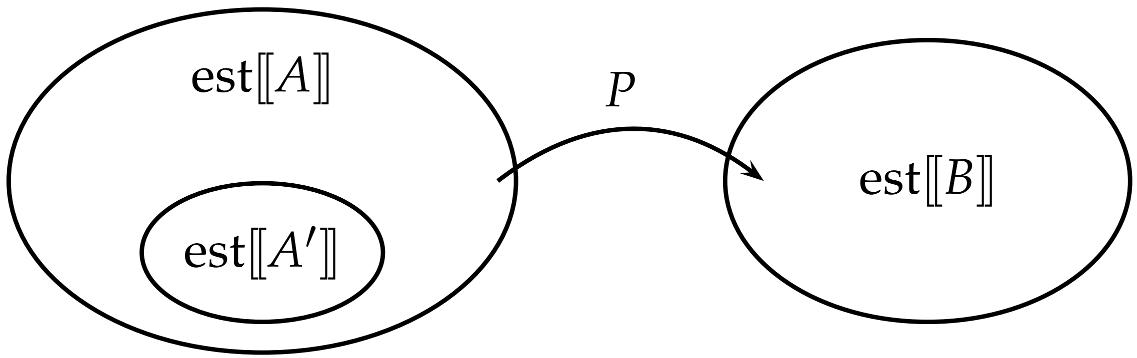
Se cumple también la especificación:

$$\begin{array}{c} \{x \leq -7\} \\ P \\ \{x \leq 10\} \end{array}$$

Regla de inferencia

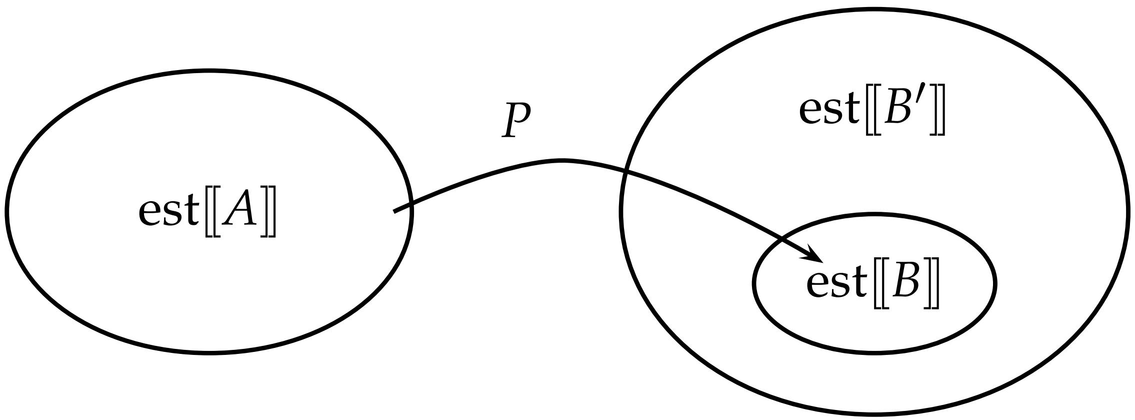
$$\frac{A' \Rightarrow A \qquad \{A\}\ P\ \{B\}}{\{A'\}\ P\ \{B\}}$$

Predicados como conjuntos de estados:



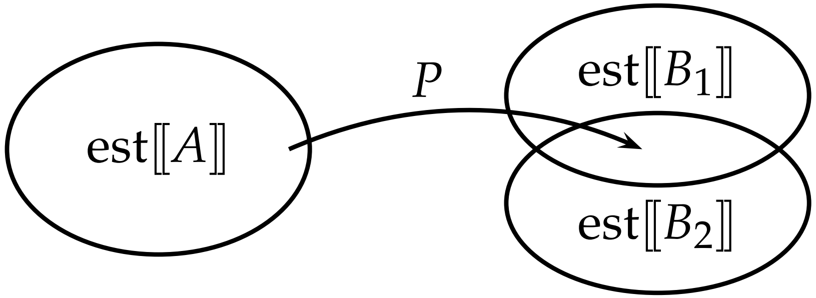
Debilitamiento de la postcondición

$$\frac{\{A\}\ P\ \{B\} \qquad B \Rightarrow B'}{\{A\}\ P\ \{B'\}}$$



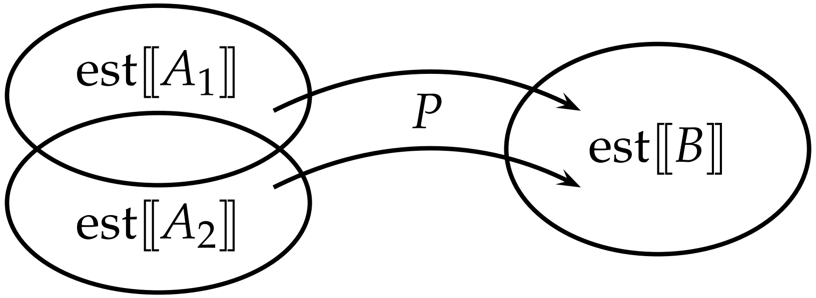
Conjunción en la postcondición

$$\frac{\{A\}\ P\ \{B_1\} \qquad \{A\}\ P\ \{B_2\}}{\{A\}\ P\ \{B_1\ \wedge\ B_2\}}$$



Disjunción en la precondición

$$\frac{\{A_1\}\ P\ \{B\} \qquad \{A_2\}\ P\ \{B\}}{\{A_1\ \vee\ A_2\}\ P\ \{B\}}$$



Precondición *lo más débil posible*

- Dados un programa P y una postcondición B, ¿qué es lo mínimo que hay que exigir a una precondición A para que se cumpla $\{A\}\ P\ \{B\}$?

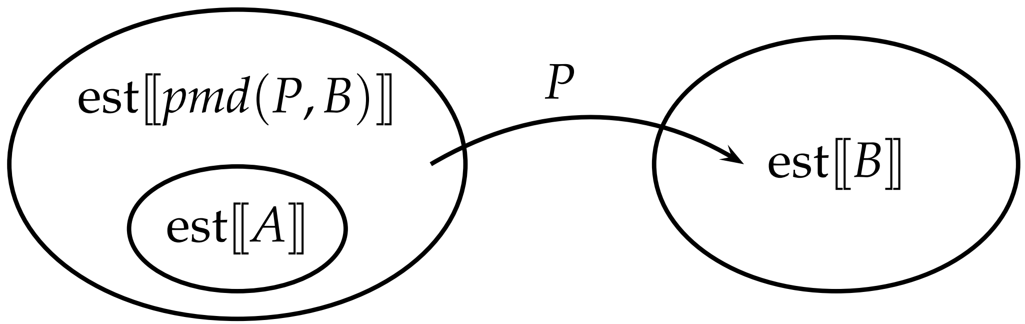
Precondición más débil del programa P con respecto a la postcondición B

$pmd(P,B)$ es el predicado que cumple:

1. $\{pmd(P,B)\}\ P\ \{B\}$,
2. Si A' cumple $\{A'\}\ P\ \{B\}$, entonces $A' \Rightarrow pmd(P,B)$.

- Por la regla de fortalecimiento de la precondición:

$$\frac{A \Rightarrow pmd(P,B)}{\{A\}\ P\ \{B\}}$$



Axioma para la instrucción que no realiza acción alguna:

$$\{A\}\ \text{nada}\ \{A\}$$

Siempre termina y su efecto sobre el estado del cómputo es nulo.

Combinando con las reglas básicas:

$$\frac{A \Rightarrow B}{\{A\}\ \text{nada}\ \{B\}}$$

Precondición más débil

$$pmd(\text{nada}, B) \Leftrightarrow B.$$

Predicado de definición

- Las funciones parciales no están definidas para ciertos valores de sus argumentos.

Ejemplos

$9 \text{ div } 0$, $v[888]$ si v es de tipo **vector** $[1..200]$ **de** *ent*, y $15 \bmod 0$.

Predicado de definición

$\text{def}(e)$: devuelve `cierto` si e es una expresión definida y `falso` en caso contrario.

Ejemplos

- $\text{def}(a \bmod b) \Leftrightarrow b \neq 0$,
- $\text{def}(a + b) \Leftrightarrow$ `cierto`,
- $\text{def}(x \text{ div } (a - b)) \Leftrightarrow a \neq b$,
- $\text{def}(x \text{ div } y + y \text{ div } x) \Leftrightarrow y \neq 0 \ \wedge \ x \neq 0$.

- Asumiremos que las operaciones son estrictas:

$$\neg\text{def}(e_i) \Rightarrow \neg\text{def}(f(e_1, \ldots, e_n))$$

- Axioma para la asignación:

$$\{\mathrm{def}(e) \ \wedge \ B_x^e\} \ x := e \ \{B\}$$

- Combinando con las reglas básicas:

$$\frac{A \Rightarrow \mathrm{def}(e) \ \wedge \ B_x^e}{\{A\} \ x := e \ \{B\}}$$

Precondición más débil

$$pmd(x := e, B) \Leftrightarrow \mathrm{def}(e) \ \wedge \ B_x^e$$

¿Cuál es la precondición más débil?

- $\{?\}\ x := 7\ \{x > 0\}$

$$(x > 0)_x^7 \Leftrightarrow 7 > 0 \Leftrightarrow \texttt{cierto}$$

- $\{?\}\ x := x + 1\ \{x > 0\}$

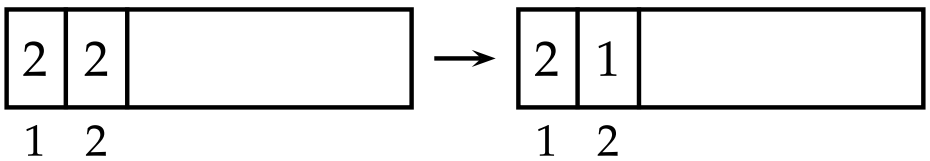
$$(x > 0)_x^{x+1} \Leftrightarrow x + 1 > 0 \Leftrightarrow x > -1 \Leftrightarrow x \geq 0$$

Asignación a vectores

¿Se puede verificar $\{v[1] = 2 \land v[2] = 2\}\ v[v[2]] := 1\ \{v[v[2]] = 1\}$?

$$
\begin{array}{rcl}
(v[v[2]] = 1)^{1}_{v[v[2]]} & \Leftrightarrow & 1 = 1 \\
 & \Leftrightarrow & \texttt{cierto} \\
 & \Leftarrow & v[1] = 2 \land v[2] = 2
\end{array}
$$

Pero la postcondición es falsa:



Asignación a vectores

¿Se puede verificar $\{i = j\}\ v[i] := 0\ \{v[j] = 0\}$?

$$
\begin{array}{rcl}
(v[j] = 0)^{0}_{v[i]} & \Leftrightarrow & v[j] = 0 \\
 & \not\Leftarrow & i = j
\end{array}
$$

- Enunciados falsos, pero que se pueden "verificar" (incorrectamente).
- Enunciados verdaderos pero imposibles de verificar.

La regla de la asignación no se puede aplicar a asignaciones de la forma

$$v[e] := e'$$

Asignación a vectores

Interpretar $v[i] := e$ como una asignación que modifica *todo* el vector v,

$$v := \text{asig}(v, i, e)$$

$\text{asig}(v, i, e)$ es un vector del mismo tipo que v que cumple:

$$\text{asig}(v,i,e)[j] = \begin{cases} e & \text{si } i = j \\ v[j] & \text{si } i \neq j \text{ y } j \text{ está en el rango de los índices de } v \end{cases}$$

Ejemplo

v : **vector** $[1..100]$ **de** *ent*, calculamos la *pmd* A que cumple

$$\{A\}\ v[v[2]] := 1\ \{v[v[2]] = 1\}$$

$$\begin{array}{ll}
\multicolumn{2}{l}{pmd(v[v[2]] := 1, v[v[2]] = 1)} \\
\Leftrightarrow & pmd(v := \mathsf{asig}(v, v[2], 1), v[v[2]] = 1) \\
\Leftrightarrow & \{\ pmd \text{ de la asignación } \} \\
 & (v[v[2]] = 1)_v^{\mathsf{asig}(v,v[2],1)}\ \wedge\ 1 \le v[2] \le 100 \\
\Leftrightarrow & \{ \text{ sustitución } \} \\
 & \mathsf{asig}(v, v[2], 1)[\mathsf{asig}(v, v[2], 1)[2]] = 1\ \wedge\ 1 \le v[2] \le 100 \\
\Leftrightarrow & \{ \text{ lógica y definición de } \mathtt{asig} \} \\
 & (v[2] = 2\ \wedge\ \mathsf{asig}(v, v[2], 1)[1] = 1)\ \vee \\
 & (v[2] \ne 2\ \wedge\ \mathsf{asig}(v, v[2], 1)[v[2]] = 1\ \wedge\ 1 \le v[2] \le 100) \\
\Leftrightarrow & \{ \text{ lógica y definición de } \mathtt{asig} \} \\
 & (v[2] = 2\ \wedge\ v[1] = 1)\ \vee \\
 & (v[2] \ne 2\ \wedge\ 1 = 1\ \wedge\ 1 \le v[2] \le 100) \\
\Leftrightarrow & \{ \text{ lógica } \} \\
 & (v[2] = 2\ \wedge\ v[1] = 1)\ \vee\ (v[2] \ne 2\ \wedge\ 1 \le v[2] \le 100)
\end{array}$$

$$v[1] = 2\ \wedge\ v[2] = 2 \not\Rightarrow (v[2] = 2\ \wedge\ v[1] = 1)\ \vee\ (v[2] \ne 2\ \wedge\ 1 \le v[2] \le 100)$$

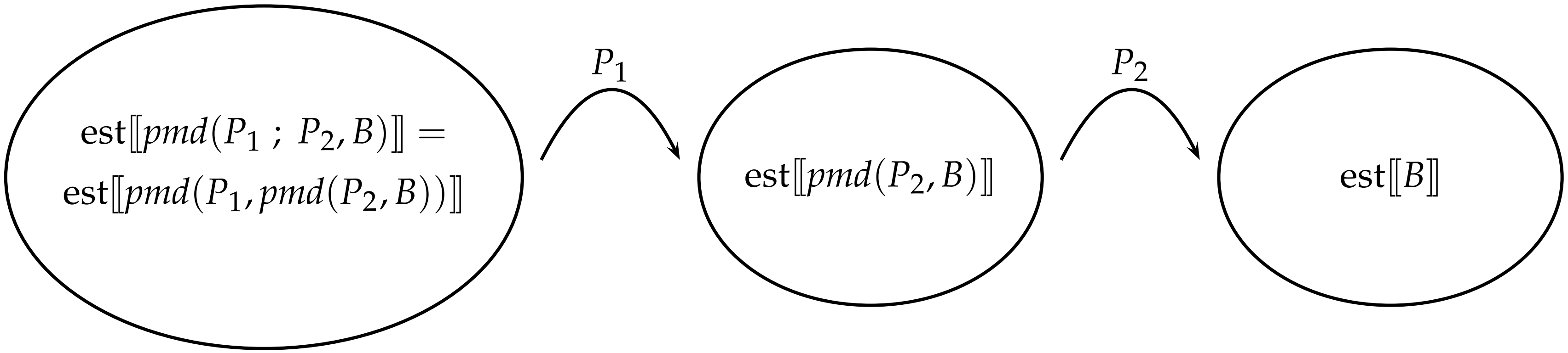
no se puede verificar $\{v[1] = 2\ \wedge\ v[2] = 2\}\ v[v[2]] := 1\ \{v[v[2]] = 1\}$

$$\frac{\{A\}\ P_1\ \{C\} \qquad \{C\}\ P_2\ \{B\}}{\{A\}\ P_1\ ;\ P_2\ \{B\}}$$

Se suele escoger como C la $pmd(P_2, B)$.

Precondición más débil

$$pmd(P_1\ ;\ P_2, B) \Leftrightarrow pmd(P_1, pmd(P_2, B))$$



Ejemplo: Intercambiar el valor de dos variables

$$\{A \equiv x = X \wedge y = Y\}$$
$$z := x\,;\; x := y\,;\; y := z$$
$$\{B \equiv x = Y \wedge y = X\}$$

- $\{C_2\}\ y := z\ \{B\}$

$$\begin{aligned} C_2 \equiv pmd(y := z, B) &\Leftrightarrow B_y^z \\ &\Leftrightarrow x = Y \wedge z = X \end{aligned}$$

- $\{C_1\}\ x := y\ \{C_2\}$

$$\begin{aligned} C_1 \equiv pmd(x := y, C_2) &\Leftrightarrow (C_2)_x^y \\ &\Leftrightarrow y = Y \wedge z = X \end{aligned}$$

- $\{A\}\ z := x\ \{C_1\}$

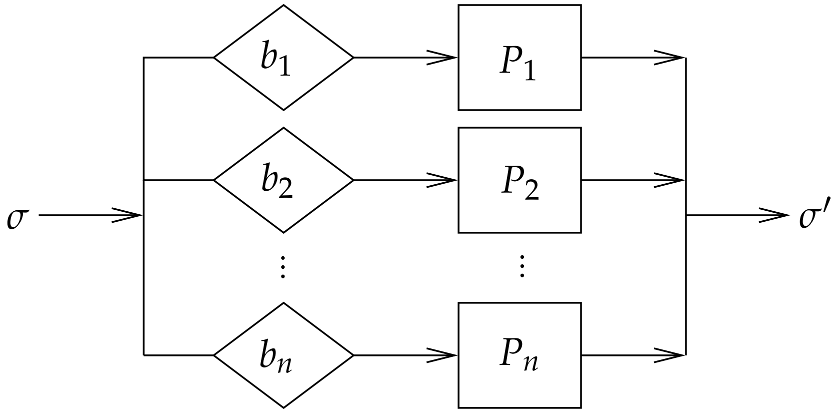
$$\begin{aligned} pmd(z := x, C_1) &\Leftrightarrow (C_1)_z^x \\ &\Leftrightarrow y = Y \wedge x = X \\ &\Leftarrow A \end{aligned}$$

Composición alternativa (distinción de casos)

casos

$$
\begin{array}{rccc}
 & b_1 & \rightarrow & P_1 \\
\square & b_2 & \rightarrow & P_2 \\
 & & \vdots & \\
\square & b_n & \rightarrow & P_n
\end{array}
$$

fcasos



$$A \Rightarrow \bigwedge_{i=1}^{n} \mathrm{def}(b_i) \qquad A \Rightarrow \bigoplus_{i=1}^{n} b_i$$

$$\frac{\{A \wedge b_1\}\ P_1\ \{B\} \ldots \{A \wedge b_n\}\ P_n\ \{B\}}{\{A\}\ \textbf{casos}\ b_1 \rightarrow P_1 \ \square\ \ldots\ \square\ b_n \rightarrow P_n\ \textbf{fcasos}\ \{B\}}$$

Precondición más débil

$$pmd(\textbf{casos}\ b_1 \rightarrow P_1 \ \square\ \ldots\ \square\ b_n \rightarrow P_n\ \textbf{fcasos}, B)$$

$$\Leftrightarrow \bigwedge_{i=1}^{n} \mathrm{def}(b_i) \wedge \bigoplus_{i=1}^{n} b_i \wedge (b_1 \Rightarrow pmd(P_1, B)) \wedge \ldots \wedge (b_n \Rightarrow pmd(P_n, B))$$

Caso particular con dos alternativas:

casos

$$\begin{array}{rl} & b \;\rightarrow\; P_1 \\ \square & \neg b \;\rightarrow\; P_2 \end{array}$$

fcasos

que se escribe como

si b **entonces** P_1 **si no** P_2 **fsi**

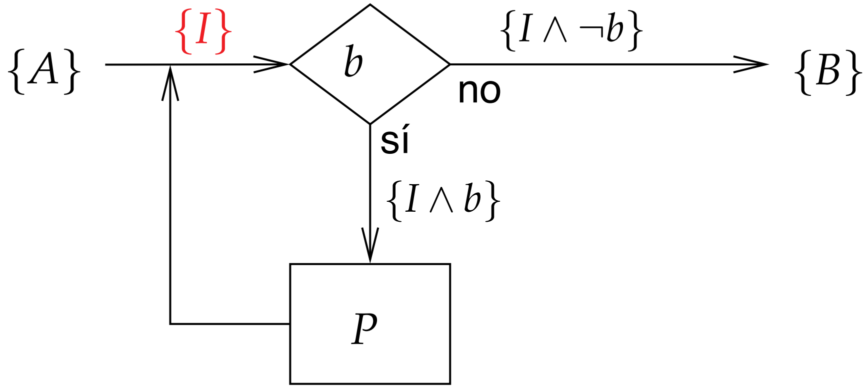
$$\frac{A \Rightarrow \mathrm{def}(b) \qquad \{A \wedge b\}\ P_1\ \{B\} \qquad \{A \wedge \neg b\}\ P_2\ \{B\}}{\{A\}\ \textbf{si}\ b\ \textbf{entonces}\ P_1\ \textbf{si no}\ P_2\ \textbf{fsi}\ \{B\}}$$

Precondición más débil

$$\begin{aligned} & pmd(\textbf{si}\ b\ \textbf{entonces}\ P_1\ \textbf{si no}\ P_2\ \textbf{fsi}, B) \\ & \quad \Leftrightarrow \mathrm{def}(b) \wedge \Big((b \wedge pmd(P_1, B)) \vee (\neg b \wedge pmd(P_2, B))\Big) \end{aligned}$$

Instrucción iterativa

mientras b **hacer**
    P
fmientras



Invariante: describe los distintos estados por los que pasa el bucle.

(i.1) Se satisface antes de empezar el bucle (antes de la primera iteración):

$$A \Rightarrow I$$

(i.2) Se mantiene al ejecutar el cuerpo P del bucle:

$$\{I \wedge b\}\ P\ \{I\}$$

(i.3) Se cumple al salir del bucle, cuando b se hace falsa:

$$I \wedge \neg b \Rightarrow B$$

Terminación: encontrar una función C que dependa de las variables del bucle, que tome valores enteros y tal que:

(c.1) Es mayor que cero cuando se cumple la condición b:

$$I \wedge b \Rightarrow C \geq 0.$$

(c.2) Decrece al ejecutar el cuerpo P del bucle:

$$\{I \wedge b \wedge C = T\}\ P\ \{C < T\}.$$

C es una cota superior del número de iteraciones que quedan por realizar: función de cota.

$$\frac{\begin{array}{c} A \Rightarrow I \\ \{I \wedge b\}\ P\ \{I\} \\ I \wedge \neg b \Rightarrow B \\ I \wedge b \Rightarrow C \geq 0 \\ \{I \wedge b \wedge C = T\}\ P\ \{C < T\} \end{array}}{\{A\}\ \textbf{mientras}\ b\ \textbf{hacer}\ P\ \textbf{fmientras}\ \{B\}}$$

Ejemplo: multiplicación

$\{A \equiv x = X \wedge y = Y \wedge y \geq 0\}$
$p := 0\,;$
$\{Inv.\ ?;\quad Cota\ ?\}$
mientras $y \neq 0$ **hacer**
    $p := p + x\,;$
    $y := y - 1$
fmientras
$\{B \equiv p = X * Y\}$

estado	x	y	p
σ_0	X	Y	0
σ_1	X	$Y-1$	X
σ_2	X	$Y-2$	$2*X$
$\vdots$			
σ_i	X	$Y-i$	$i*X$

Se mantienen invariantes las siguientes propiedades:

$$x = X$$
$$0 \leq y \leq Y$$
$$\texttt{cierto}$$
$$(\exists k : k \in nat : p = k * X)$$
$$X * Y = p + x * y$$

Proponemos como invariante $I \equiv x = X \wedge X * Y = p + x * y \wedge y \geq 0$

(i.1) $\{A\}\ p := 0\ \{I\}$

$$
\begin{aligned}
pmd(p := 0, I) \quad &\Leftrightarrow \quad (x = X \wedge X*Y = p + x*y \wedge y \geq 0)_p^0 \\
&\Leftrightarrow \quad x = X \wedge X*Y = x*y \wedge y \geq 0 \\
&\Leftarrow \quad x = X \wedge y = Y \wedge y \geq 0 \\
&\Leftrightarrow \quad A
\end{aligned}
$$

(i.2) $\{I \wedge y \neq 0\}\ p := p + x\ ;\ \ y := y - 1\ \{I\}$

$$
\begin{aligned}
&pmd(y := y - 1, I) \\
&\quad \Leftrightarrow \quad (x = X \wedge X*Y = p + x*y \wedge y \geq 0)_y^{y-1} \\
&\quad \Leftrightarrow \quad x = X \wedge X*Y = p + x*(y-1) \wedge y - 1 \geq 0 \equiv I'
\end{aligned}
$$

$$
\begin{aligned}
&pmd(p := p + x, I') \\
&\quad \Leftrightarrow \quad (x = X \wedge X*Y = p + x*(y-1) \wedge y - 1 \geq 0)_p^{p+x} \\
&\quad \Leftrightarrow \quad x = X \wedge X*Y = p + x*y \wedge y - 1 \geq 0 \\
&\quad \Leftarrow \quad I \wedge y \neq 0 \\
&\quad \Leftrightarrow \quad x = X \wedge X*Y = p + x*y \wedge y > 0
\end{aligned}
$$

(i.3) $I \wedge \neg b \Rightarrow B$

$$
\begin{aligned}
I \wedge \neg b \quad &\Leftrightarrow \quad x = X \wedge X*Y = p + x*y \wedge y \geq 0 \wedge y = 0 \\
&\Leftrightarrow \quad x = X \wedge X*Y = p + x*0 \wedge y = 0 \\
&\Leftrightarrow \quad x = X \wedge X*Y = p \wedge y = 0 \\
&\Rightarrow \quad B
\end{aligned}
$$

Terminación: podemos tomar como cota la variable y: $C = y$.

(c.1) La cota es positiva cuando entramos en el bucle:

$$\begin{array}{rcl} I \wedge b & \Leftrightarrow & x = X \wedge X * Y = p + x * y \wedge y \geq 0 \wedge y \neq 0 \\ & \Leftrightarrow & x = X \wedge X * Y = p + x * y \wedge y > 0 \\ & \Rightarrow & y \geq 0 \end{array}$$

(c.2) La cota decrece al pasar por el cuerpo del bucle:

$$\begin{array}{rcl} pmd(p := p + x \,;\ y := y - 1, y < T) & \Leftrightarrow & ((y < T)_y^{y-1})_p^{p+x} \\ & \Leftrightarrow & y - 1 < T \\ & \Leftarrow & y = T \\ & \Leftarrow & I \wedge b \wedge y = T \end{array}$$

Verificación de algoritmos

- Verificar = demostrar con un razonamiento suficientemente claro que un algoritmo cumple su especificación.
- Las reglas de la semántica axiomática sirven para verificar la corrección de un algoritmo con respecto a su especificación.
- Verificar un algoritmo complejo: descomponer en pequeños algoritmos anidados (cajas negras de las que solo se conoce su especificación) y verificar de dentro hacia fuera.

Ejemplo: Elevar al cuadrado

$\{ A \equiv n \geq 0 \}$
fun cuadrado $(n : nat)$ **dev** $q : nat$
var $i, p : nat$
$i := 0\ ;\ q := 0\ ;\ p := 1\ ;$
mientras $i < n$ **hacer**
    $i := i + 1\ ;$
    $q := q + p\ ;$
    $p := p + 2$
fmientras
$\{ B \equiv q = n^2 \}$

i	q	p
0	0	1
1	1	3
2	4	5
3	9	7
4	16	9

$$I \equiv q = i^2 \wedge p = 2 \cdot i + 1 \wedge 0 \leq i \leq n$$

(i.1) $\{A\}\ i := 0\ ;\ q := 0\ ;\ p := 1\ \{I\}$

$$
\begin{array}{ll}
& (((q = i^2 \wedge p = 2\cdot i + 1 \wedge 0 \le i \le n)_p^1)_q^0)_i^0 \\
\Leftrightarrow & ((q = i^2 \wedge 1 = 2\cdot i + 1 \wedge 0 \le i \le n)_q^0)_i^0 \\
\Leftrightarrow & (0 = i^2 \wedge 1 = 2\cdot i + 1 \wedge 0 \le i \le n)_i^0 \\
\Leftrightarrow & 0 = 0^2 \wedge 1 = 2\cdot 0 + 1 \wedge 0 \le 0 \le n \\
\Leftrightarrow & 0 \le n
\end{array}
$$

(i.2) $\{I \wedge i < n\}\ i := i+1\ ;\ q := q+p\ ;\ p := p+2\ \{I\}$

$$
\begin{array}{ll}
& (((q = i^2 \wedge p = 2\cdot i + 1 \wedge 0 \le i \le n)_p^{p+2})_q^{q+p})_i^{i+1} \\
\Leftrightarrow & ((q = i^2 \wedge p+2 = 2\cdot i + 1 \wedge 0 \le i \le n)_q^{q+p})_i^{i+1} \\
\Leftrightarrow & (q+p = i^2 \wedge p+2 = 2\cdot i + 1 \wedge 0 \le i \le n)_i^{i+1} \\
\Leftrightarrow & q+p = (i+1)^2 \wedge p+2 = 2\cdot (i+1) + 1 \wedge 0 \le (i+1) \le n \\
\Leftrightarrow & q+p = i^2 + 1 + 2\cdot i \wedge p = 2\cdot i + 1 \wedge 0 \le (i+1) \le n \\
\Leftarrow & q = i^2 \wedge p = 2\cdot i + 1 \wedge 0 \le i < n
\end{array}
$$

(i.3) $I \wedge \neg(i < n) \Rightarrow q = n^2$

$$
q = i^2 \wedge p = 2\cdot i + 1 \wedge 0 \le i \le n \wedge i \ge n \quad \Rightarrow \quad q = n^2
$$

$C = n - i$

(c.1) Positiva.

$$q = i^2 \wedge p = 2 \cdot i + 1 \wedge 0 \leq i \leq n \wedge i < n \quad \Rightarrow \quad n - i \geq 0$$

(c.2) $\{I \wedge i < n \wedge n - i = T\}\ i := i + 1\ ;\ q := q + p\ ;\ p := p + 2\ \{n - i < T\}$

$$\begin{array}{ll} \multicolumn{2}{l}{(((n - i < T)_p^{p+2})_q^{q+p})_i^{i+1}} \\ \Leftrightarrow & n - (i + 1) < T \\ \Leftrightarrow & n - i - 1 < T \\ \Leftarrow & q = i^2 \wedge p = 2 \cdot i + 1 \wedge 0 \leq i < n \wedge n - i = T \end{array}$$