

Algoritmos y Estructuras de Datos I

Digesto para la Programación Imperativa

Precondición más débil

$$wp.S : Predicados \mapsto Predicados$$

$$[wp.S.Q = P] \iff \begin{cases} (i) \{P\} S \{Q\} \\ (ii) \{P_0\} S \{Q\} \Rightarrow [P_0 \Rightarrow P] \end{cases}$$

Relación entre Terna de Hoare y Precondición más débil

$$\{P\} S \{Q\} \equiv [P \Rightarrow wp.S.Q]$$

1. Skip

Verificación con Terna de Hoare:

$$\{P\} \text{skip} \{Q\} \equiv P \Rightarrow Q$$

Precondición más débil:

$$wp.\text{skip}.Q \equiv Q$$

Verificación con Precondición más débil:

$$\{P\} \text{skip} \{Q\} \equiv P \Rightarrow wp.\text{skip}.Q$$

Programa anotado:

$$\begin{array}{c} \vdots \\ \{Q\} \\ \text{skip} \\ \{Q\} \\ \vdots \end{array}$$

2. Asignación

Verificación con Terna de Hoare:

$$\{P\} x_1, \dots, x_n := E_1, \dots, E_n \{Q\} \equiv P \Rightarrow Q(x_1 \leftarrow E_1, \dots, x_n \leftarrow E_n)$$

Nota: “ \leftarrow ” es el reemplazo sintáctico de una variable por una expresión.

Precondición más débil:

$$wp.(x_1, \dots, x_n := E_1, \dots, E_n).Q \equiv Q(x_1 \leftarrow E_1, \dots, x_n \leftarrow E_n)$$

Verificación con Precondición más débil:

$$\{P\} x_1, \dots, x_n := E_1, \dots, E_n \{Q\} \equiv P \Rightarrow wp.(x_1, \dots, x_n := E_1, \dots, E_n).Q$$

Programa anotado:

$$\begin{array}{c} \vdots \\ \{Q(x_1 \leftarrow E_1, \dots, x_n \leftarrow E_n)\} \\ x_1, \dots, x_n := E_1, \dots, E_n \\ \{Q\} \\ \vdots \end{array}$$

3. Composición o concatenación (;):

Verificación con Terna de Hoare:

$$\{P\} S; T \{Q\} \equiv \text{Existe } R \text{ tal que } \{P\} S \{R\} \wedge \{R\} T \{Q\}$$

Precondición más débil:

$$wp.(S; T).Q \equiv wp.S.(wp.T.Q)$$

Verificación con Precondición más débil:

$$\{P\} S; T \{Q\} \equiv P \Rightarrow wp.(S; T).Q$$

Programa anotado:

$$\begin{array}{c} \vdots \\ \{wp.S.(wp.T.Q)\} \\ S; \\ \{wp.T.Q\} \\ T \\ \{Q\} \\ \vdots \end{array}$$

4. Condicional o alternativa (if):

Verificación con Terna de Hoare:

$$\begin{array}{ll} \{P\} \text{ if } B_1 \rightarrow S_1 \{Q\} & \equiv P \Rightarrow (B_1 \vee B_2 \vee \dots \vee B_n) \\ \square B_2 \rightarrow S_2 & \wedge \{B_1 \wedge P\} S_1 \{Q\} \\ \vdots & \wedge \{B_2 \wedge P\} S_2 \{Q\} \\ \square B_n \rightarrow S_n & \vdots \\ \text{fi} & \wedge \{B_n \wedge P\} S_n \{Q\} \end{array}$$

Precondición más débil:

$$\begin{aligned} wp.(\text{if } \dots \text{fi}).Q & \equiv (B_1 \vee B_2 \vee \dots \vee B_n) \\ & \wedge (B_1 \Rightarrow wp.S_1.Q) \\ & \wedge (B_2 \Rightarrow wp.S_2.Q) \\ & \vdots \\ & \wedge (B_n \Rightarrow wp.S_n.Q) \end{aligned}$$

Verificación con Precondición más débil:

$$\begin{array}{ll} \{P\} \text{ if } B_1 \rightarrow S_1 \{Q\} & \\ \square B_2 \rightarrow S_2 & \\ \vdots & \\ \square B_n \rightarrow S_n & \\ \text{fi} & \end{array} \equiv P \Rightarrow wp.(\text{if } \dots \text{fi}).Q$$

Programa anotado:

| | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| $ \begin{array}{l} \vdots \\ \{(B_0 \vee B_1 \vee \dots \vee B_n) \wedge \\ (B_0 \Rightarrow wp.S_0.Q) \wedge \dots \wedge (B_n \Rightarrow wp.S_n.Q)\} \\ \text{if } B_0 \rightarrow \\ \quad \{B_0 \wedge wp.S_0.Q\} \\ \quad S_0 \\ \quad \{Q\} \\ \square B_1 \rightarrow \\ \quad \{B_1 \wedge wp.S_1.Q\} \\ \quad S_1 \\ \quad \{Q\} \\ \vdots \\ \square B_n \rightarrow \\ \quad \{B_n \wedge wp.S_n.Q\} \\ \quad S_n \\ \quad \{Q\} \\ \text{fi} \\ \{Q\} \\ \vdots \end{array} $ | ó | $ \begin{array}{l} \{P\} \\ \text{if } B_0 \rightarrow \\ \quad \{B_0 \wedge P\} \\ \quad S_0 \\ \quad \{Q\} \\ \square B_1 \rightarrow \\ \quad \{B_1 \wedge P\} \\ \quad S_1 \\ \quad \{Q\} \\ \vdots \\ \square B_n \rightarrow \\ \quad \{B_n \wedge P\} \\ \quad S_n \\ \quad \{Q\} \\ \text{fi} \\ \{Q\} \\ \vdots \end{array} $ |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

5. Ciclo o repetición (do):

Verificación con Ternas de Hoare:

$$\{P\} \text{ do } B \rightarrow S \text{ od } \{Q\} \quad \equiv \quad \left. \begin{array}{l}
 \text{Existe } I \text{ (invariante) tal que} \\
 P \Rightarrow I \\
 \wedge I \wedge \neg B \Rightarrow Q \\
 \wedge \{I \wedge B\} S \{I\} \\
 \wedge \\
 \text{Existe función de cota } t : \text{Estados} \mapsto \text{Int} \\
 \text{(i) } I \wedge B \Rightarrow t \geq 0 \\
 \text{(ii) } \{I \wedge B \wedge t = T\} S \{t < T\}
 \end{array} \right\} \text{ (terminación)}$$

Programa anotado:

$$\begin{array}{l}
 \vdots \\
 \{I\} \\
 \text{do } B \rightarrow \\
 \quad \{I \wedge B\} \\
 \quad S \\
 \quad \{I\} \\
 \text{od} \\
 \{I \wedge \neg B\} \\
 \vdots
 \end{array}$$

Anotaciones Apiladas

$$\begin{array}{ccc}
 \begin{array}{l} \{R\} \\ \{P\} \\ S \\ \{Q\} \end{array} & \equiv & R \Rightarrow P \wedge \begin{array}{l} \{P\} \\ S \\ \{Q\} \end{array}
 \end{array}
 \qquad
 \begin{array}{ccc}
 \begin{array}{l} \{P\} \\ S \\ \{Q\} \\ \{R\} \end{array} & \equiv & \begin{array}{l} \{P\} \\ S \\ \{Q\} \end{array} \wedge Q \Rightarrow R
 \end{array}$$

Nota: Las anotaciones apiladas funcionan como si hubiera un **skip**.

Propiedades

- $\{P\} S \{False\} \equiv (P \equiv False)$ (Exclusión de milagros)
- $wp.S.False \equiv False$
- $wp.S.Q \wedge wp.S.R \equiv wp.S.(Q \wedge R)$
- $wp.S.Q \vee wp.S.R \Rightarrow wp.S.(Q \vee R)$