

Verificación Axiomática de Programas (lógica de Hoare)

Ejercicio 1. Responder breve y claramente los siguientes incisos:

- 1.1. ¿En qué se diferencia una prueba semántica de una prueba sintáctica de un programa?
- 1.2. ¿Qué es un estado de un programa? ¿Cuándo un estado satisface un predicado?
- 1.3. ¿Cómo se especifica un programa?
- 1.4. ¿Cuál es el significado de la fórmula $\{p\} S \{q\}$?
- 1.5. ¿Qué son el invariante y el variante de un *while*?
- 1.6. ¿Cuándo un método axiomático es sensato, y cuándo es completo?
- 1.7. ¿Por qué la lógica de Hoare para los programas secuenciales es composicional?

Ejercicio 2. Especificar un programa que a partir de un estado inicial en el que x sea mayor que 0, termine en un estado final en el que y sea el cuadrado del valor inicial de x , y además x tenga su valor inicial.

Ejercicio 3. Decir y justificar informalmente (es decir sin usar la lógica de Hoare), si se cumplen o no las siguientes fórmulas.

Comentario: el predicado *true* representa cualquier estado:

- 3.1. $\{x > 0\} \text{ while } x > 0 \text{ do } x := x - 2 \text{ od } \{\text{true}\}$
- 3.2. $\{x > 0\} \text{ while } x > 0 \text{ do } x := x - 2 \text{ od } \{x = 0\}$
- 3.3. $\{x > 0\} \text{ while } x \neq 0 \text{ do } x := x - 2 \text{ od } \{\text{true}\}$

Ejercicio 4. Probar (usando la lógica de Hoare): $\{\text{true}\} x := 0 ; x := x + 1 ; x := x + 2 \{x = 3\}$.

Ejercicio 5. Se cumple $\{x = 10\} \text{ while } x > 0 \text{ do } x := x - 1 \text{ od } \{x = 0\}$. Se pide probar (usando la lógica de Hoare) que el predicado $p = (x \geq 0)$ es un invariante del *while*.

Ayuda: hay que probar, por un lado: $x = 10 \rightarrow p$, y por otro lado: $\{p \wedge x > 0\} x := x - 1 \{p\}$.

Ejercicio 6. La instrucción *repeat S until B* consiste en ejecutar S , luego evaluar B , si B es falsa volver a iterar, y en caso contrario terminar. Explicar informalmente por qué la siguiente regla para probar la instrucción es sensata (es decir, si se cumplen las premisas, entonces también se cumple la conclusión):

$$\frac{\{p\} S \{q\}, q \wedge \neg B \rightarrow p}{\{p\} \text{ repeat } S \text{ until } B \{q \wedge B\}}$$