Verificación de programas

Eva Lucrecia Gibaja Galindo

Dpto. Informática y Análisis Numérico

Especificación de un programa

- Los datos de entrada de un programa están sujetos a unas restricciones denominadas **precondiciones**.
- Los datos de salida cumplen unos criterios denominados **postcondiciones**.

- Las **especificaciones de un programa** son el conjunto formado por las precondiciones y postcondiciones que debe cumplir.
- El lenguaje usado para la especificación se llama **lenguaje de especificación** (LE). Este lenguaje hace uso de la lógica proposicional.

Especificación de un programa

- El **programa** transformará el estado inicial (precondición) en sucesivos estados intermedios hasta alcanzar el estado final (postcondición).
- Un **estado** queda definido por los valores que tienen las variables del programa en un instante determinado.
- Un estado se describe mediante una **aserción** o **predicado** que es una expresión de tipo lógico que se incorpora al programa como comentario (entre llaves { }).

Reglas formales de prueba

- La verificación de programas tiene como objetivo la **aplicación de la lógica matemática** para demostrar formalmente que el programa incluido entre la precondición y la postcondición cumple esas especificaciones bajo cualquier circunstancia de ejecución posible.
- La verificación formal hace uso de las **reglas de inferencia de la lógica** de proposiciones y de predicados y, además **define su propio sistema de inferencia**, el cual consta de un conjunto de reglas de inferencia asociada a las sentencias de programas.

El proceso de verificación

- Un ***tableau vacío*** es un listado del programa completado con precondiciones y postcondiciones vacías antes y después de cada instrucción.
- El objetivo de la verificación es rellenar el **tableau** con asertos válidos.
- Demostración de la corrección de un programa: demostrar que cada instrucción conduce de una situación que satisface el aserto que le precede a otra situación que satisface el aserto que le sigue.
- Una **demostración** se compone de un conjunto de asertos P_1, P_2, ..., P_{n+1} que se insertan entre las instrucciones s_1, s_2, s_n de un *tableau* vacío.

Programa Ejemplo(; ;)

Inicio

{Precondicion}

{ }

sentencia 1

{ }

sentencia 2

{ }

.....

{ }

sentencia n

{Postcondición}

Fin