Verificación automática de corrección

Algoritmos y Estructuras de Datos I

Verificación automática de corrección

- La semántica axiomática basada en la precondición más débil reduce la demostración de corrección de un algoritmo a la verificación de la validez de una fórmula lógica.
- Es decir, la tripla $\{P\}S\{Q\}$ es válida si $P \Rightarrow wp(S, Q)$.
- Esto abre la posibilidad de tener verificadores automáticos de corrección:
  1. Obtenemos $wp(S, Q)$ y le pedimos a un demostrador de teoremas que verifique si vale $P \Rightarrow wp(S, Q)$.

Verificación automática de corrección

- Demostrar la validez de una fórmula lógica de primer orden es un problema indecidible.
- Sin embargo, en la práctica es posible desarrollar demostradores de teoremas que funcionen para fórmulas "razonables".
  1. Si el demostrador de teoremas encuentra una demostración, entonces la fórmula es válida.
  2. Si el demostrador de teoremas encuentra un contraejemplo, entonces la fórmula no es válida.
  3. Puede suceder, sin embargo, que el demostrador de teoremas no pueda obtener una respuesta concluyente.

Verificación automática de corrección

- Existen diversos verificadores automáticos de programas. Uno de ellos es Dafny, desarrollado por Microsoft Research.
  research.microsoft.com/dafny
  rise4fun.com/Dafny
- Utiliza un lenguaje intermedio llamado Boogie y un demostrador de teoremas llamado Z3.
- Dafny tiene su propio lenguaje de programación, que es similar a SmallLang.