

Tecnología de la Programación

Análisis estático

David Cabrero Souto

Facultad de Informática
Universidade da Coruña

Curso 2007/2008



- No se ejecuta el código
- Manual (desarrollador) o automático (herramienta) o mixto
- Se examina el código fuente
 - Sintaxis vs semántica
 - Heurísticas, herramientas de compiladores, métodos formales,
...
- Ejemplo simple: errores y warnings del compilador



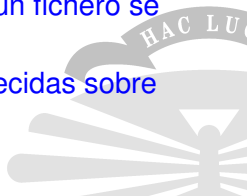
- El problema de la parada

Given a description of a program and a finite input, decide whether the program finishes running or will run forever, given that input.

- En general no es decidable para lenguajes Turing completos.
- El análisis del programa no puede determinar si termina o no en cualquier situación.



- Encontrar variables que se usan sin inicializar
- Encontrar *memory leaks*, incluyendo lenguajes con gestión de memoria implícita (i.e. referencias que nunca se establecen a null)
- Descubrir casos en los que un bloque de memoria se libera más de una vez
- Encontrar dereferencias de "dangling pointers"(punteros a zonas de memoria liberadas)
- Encontrar accesos fuera de los límites de los arrays.
- Comprobar propiedades tipo/estado (p.e. sobre un fichero se hace `open()` antes de `read()`)
- Verificar que se cumplen las propiedades establecidas sobre un método
- ...



- Checkstyle
 - No está directamente relacionado con la corrección del código, sí con la calidad
 - Comprueba que el código sigue las guía se estilo
 - Crea un AST (Abstract Syntax Tree)
 - Demo. La configuración por omisión comprueba las “Java Code Conventions”
- gcc
 - `-Wefc++` “Warn about violations of the following style guidelines from ...”
 - `-Wold-style-cast`
- lint
 - Ha dado origen a muchas herramientas *lint
deblint, weblint, jlint, pylint, ...
 - Demo splint.



- Análisis basado en una representación formal de los lenguajes y programas
- Es necesario definir una semántica formal del lenguaje
 - Semántica denotacional
 - Semántica axiomática
 - Semántica operacional
 - Interpretación abstracta
- Y, al menos, una técnica de análisis
 - Model checking
 - Interpretación abstracta
 - Lógica de Hoare
 - ...
- Ejemplo: ESC/Java

