Static Program Analysis

Program Slicing

Steven Vormwald
02/19/2008
Outline

- Definitions
- Program Representation
- Example – Wisconsin Program-Slicing Tool
- Future Work
- Questions
Definitions

• Program Slicing
  - Determine what statements affect/are affected by a given state of a program.
    • Forward Slicing
      • What later statements are affected by this state?
    • Backward Slicing
      • What earlier statements affected this state?
Definitions

- **Control-Flow Graph (CFG)**
  - A graph showing the possible execution paths through a procedure.

- **Program Dependence Graph (PDG)**
  - A graph showing data and control dependences between statements in a procedure.

- **System Dependence Graph (SDG)**
  - An extension to PDG that includes dependences across function calls.
Program Representation (SDG)
Wisconsin Program-Slicing Tool

- Supports forward and backward slicing of C programs.
- Has been used on C sources containing over 51000 lines.

Future Work
(By Spring Break)

• Memory Aliasing
  - These slicing techniques all specify that the algorithms assume there are no aliasing problems, e.g. a call-by-reference system where the call $f(x,x)$ occurs. Aliasing is too common to ignore in languages such as C.

• Concurrent Programs
  - These slicing techniques work well for systems with a single thread of execution. What changes are necessary to analyze multi-threaded systems?
Questions?