Program Analysis

Data Flow Analysis (Part 5)

Prof. Dr. Michael Pradel

Software Lab, University of Stuttgart

Winter 2020/2021

Outline

- First example: Available expressions
- Basic principles
- More examples
- Solving data flow problems
- Inter-procedural analysis 
- Sensitivities

Intra- vs. Inter-procedural

- **Intra-procedural analysis**
  - Reason about a function in isolation
- **Inter-procedural analysis**
  - Reason about multiple functions
  - Calls and returns
- **Data flow analyses considered so far: Intra-procedural**

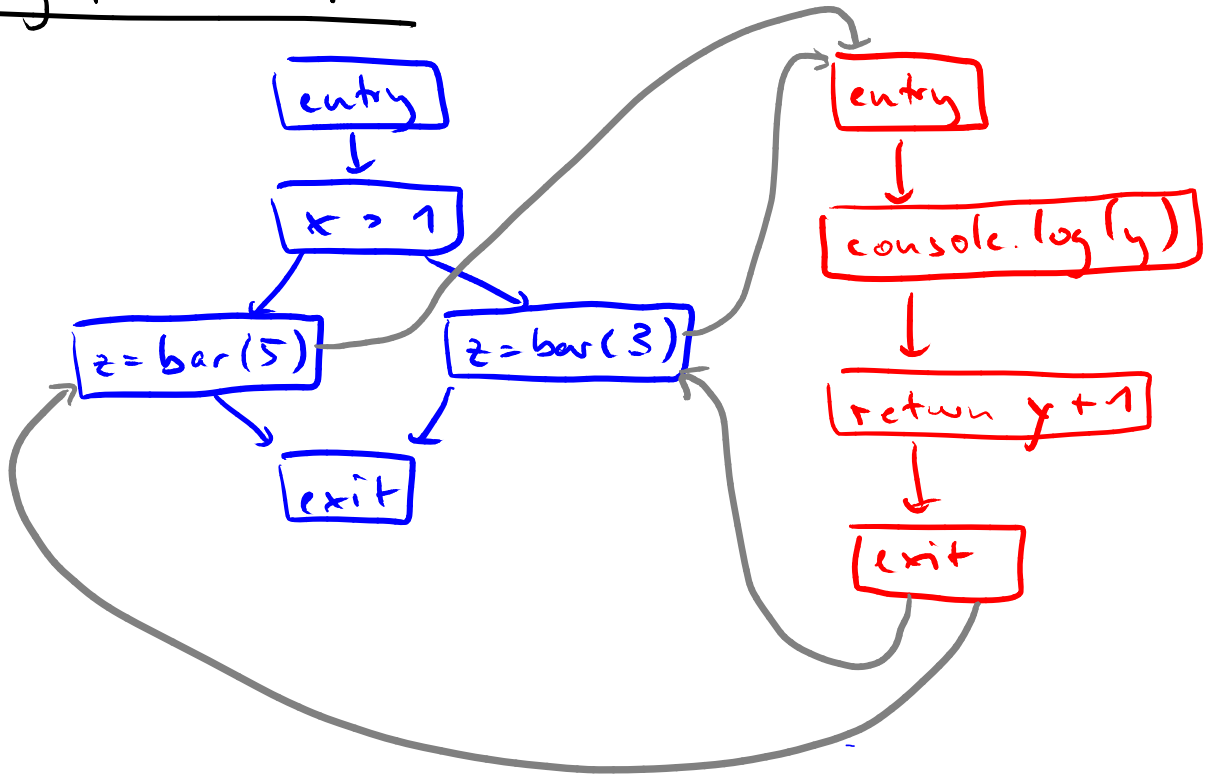
Inter-procedural Control Flow

- One control flow graph per function
- Connect call sites to entry node of callee
- Connect exit node back to call site

Inter-procedural control flow graph: Example

```
function foo (x) {
    if (x > 1)
        z = bar (5)
    else
        z = bar (3)
}

function bar (y) {
    console.log (y)
    return y + 1
}
```



Analysis considers only "possible" inter-proc. flows:

- After return, don't enter again
- When returning, go back to call site

Propagating Information

- **Arguments passed into call**
  - Propagate to formal parameters of callee
- **Return value**
  - Propagate back to caller
- **Local variables**
  - Do not propagate into callee
  - Instead, when call returned, continue with state just before call

Propagating Information

- **Arguments passed into call**
  - Propagate to formal parameters of callee
- **Return value**
  - Propagate back to caller
- **Local variables**
  - Do not propagate into callee
  - Instead, when call returned, continue with state just before call

For backward analysis: Everything in reverse