

# Testen

## SS 2019

Automatisches Testen

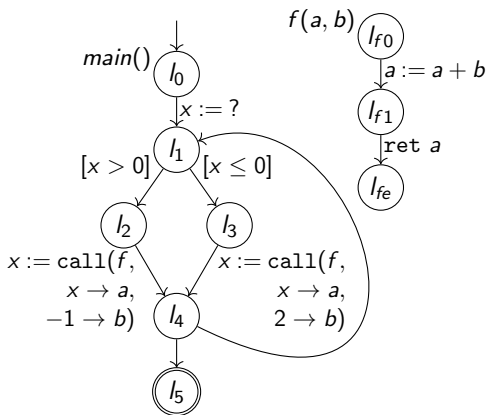
Prof. Dr. Dirk Beyer,  
Thomas Lemberger

- Einführung
- Automatische Testerzeugung
  - Blackbox Testing (Random)
  - Greybox Testing (Distanzmetriken)
  - Whitebox Testing (Symbolic Execution)
- Testziel-Spezifikation mit FQL
- Mutations-Testen
- Übungen: PRTest, AFL-fuzz, KLEE, CPAchecker, FShell, SRCIROR

# Programm-Repräsentation

# Control Flow Automaton (CFA)

- ▶ Automaten-basierte Repräsentation von Programm
- ▶ CFA  $G = (L, l_0, E)$ 
  - ▶ Program locations  $L$
  - ▶ Program entry  $l_0 \in L$  (initialer Zustand)
  - ▶ Kanten  $E = L \times Ops \times L$
- ▶ Operationen  $Ops$ 
  - ▶ Assumes  $[p]$
  - ▶ Assignments  $x := exp$
  - ▶ Function calls  $call(foo, arg_1 \rightarrow param_1, \dots, arg_n \rightarrow param_n)$
  - ▶ Function return  $ret returnVar$
  - ▶ No-effect  $nop$
- ▶ Bedeutung Kante  $(l, op, l')$ :  
Transfer von  $l$  nach  $l'$  mit Ausführung von  $op$ .



# Ergänzung: Control Flow Graph (CFG)

- ▶ Programm-Operationen in Graph-Knoten
- ▶ Bei Assume: Kanten-label *true* und *false*