Static and Dynamic Analysis: Synergy and Duality

Michael D. Ernst

MIT Lab for Computer Science

Presented by Bruno Dufour

dufour@cs.rutgers.edu

Rutgers University DCS

Background – Static Analysis

- Examines program code
- Considers *all* possible executions
- Positive
  - Sound
    - Results apply to all possible executions
- Negative
  - (Usually) conservative
    - Abstract model is limited
    - May report weaker properties than may be true
  - Complex analyses can be very slow

Background – Dynamic Analysis

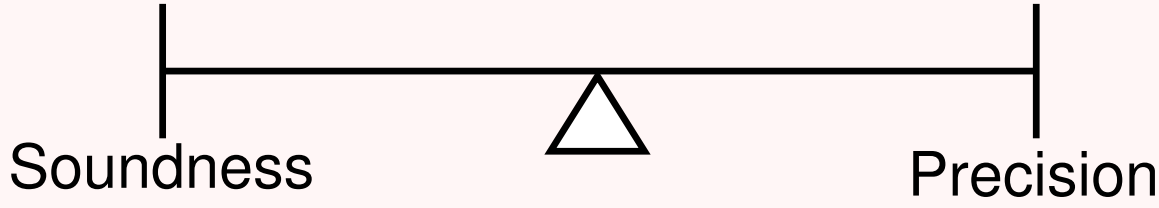
- Observes the execution of a program
- Positive
  - Precise
    - Examines *exact* runtime behaviour
    - (Almost) no uncertainty
  - Can be as fast as program execution
- Negative
  - Unsound
    - Results do not generalize
    - Requires representative input(s)
  - Amount of data is usually huge

Synergies

- Static and dynamic have complementary strenghts and weaknesses
- Applying both to a single problem
  - Program verification
  - Profile-directed compilation
  - Static analysis to guide instrumentation
- Different approaches to the same problem
  - Program slicing
  - Program specifications
    - Theorem proving vs assertions
    - Dynamic detection of likely invariants (Daikon)

Hybrid Analysis

- Idea: make both techniques meet “in the middle”
  - Sacrifice some soundness and some precision



Duality

- Key observation: analyses only consider a subset of all possible executions
  - Static: Possibly infinite set of executions based on properties
    - e.g. k-limiting analysis
  - Dynamic: enumerable set of test cases, difficult to formalize
- Execution not in the set are handled differently:
  - Static: pessimistic/conservative, sound
    - Generalization ▶ imprecision
  - Dynamic: optimistic, unsound
    - Generalization ▶ unsoundness

Duality (2)

- Complexity of set descriptions
  - Static: Given description find executions that induce data structures.
  - Dynamic: Given executions find how parts of the program are exercised.
  - ▶ No clear winner

Conclusions

- Static and dynamic analysis are not as different as they appear.
- When only one of static or dynamic exists, we should investigate the other.