RESEARCH TOPICS OVERVIEW

CS580A5

SPRING 2017

SUDIPTO GHOSH

2 TOPICS

- Metamorphic testing
- Fuzz testing
- Regression testing: selection, prioritization
- Test input generation
- Fault localization
- Automatic program repair
- UI Testing

3 METAMORPHIC TESTING

- When expected outputs of the program under test are not known, how do you define the oracle?
- Define metamorphic properties:
  - For two inputs i_1 and i_2, the outputs are o_1 and o_2
  - if i_1 and i_2 are related in a certain way, then o_1 and o_2 must also be related in a certain way (not the same way as the inputs though)

4 FUZZ TESTING

- Often applications crash when given unexpected input
  - Editors crash when files are corrupt
- Hackers can hack into a system by sending inputs that are unexpected
- How do we verify whether our applications are resilient to such problems/attacks?

5 REGRESSION TESTING: SELECTION, PRIORITIZATION

- Programs evolve: new features are added, faults are fixed and so on
- How do we ensure that existing functionality isn't broken?
  - Run existing tests that are still valid in the new context
- What if we don't have enough resources to run every test?
- We need some way to select a subset of test cases
  - Safety property: Every old test that exercises modified code must be executed
  - Precision (don't want to run more test cases than needed to achieve safety)
  - Other objectives: ensure same level of code coverage as before, fault detection, etc

6 TEST INPUT GENERATION

- How to automatically generate test inputs?
  - How about expected outputs?
- Categories of techniques
  - Random generation
  - Exhaustive generation
  - Based on symbolic execution
  - Combination of concrete and symbolic execution (aka concolic)

7 FAULT LOCALIZATION

- Debugging consists of finding a fault and fixing it.
- Typically manual, and lots of time spent
- Study automated techniques that help narrow down the possibilities
  - Slicing
  - Spectrum based approaches

8 AUTOMATIC PROGRAM REPAIR

- Solves the second part of debugging (finding a fix/patch)
- Study general approach framework
- Specific approach called GenProg

9 UI TESTING

- Challenges specific to UI testing
  - Various testing goals
  - Automation (capture and replay)
- Underlying principles
- Guest lecture from industry professional