COM S/CPRE 513X Course Work

Instructor: Wei Le

January 11, 2016

Reading

1. [Points-to analysis] Pointer Analysis: Haven’t We Solved This Problem Yet?
2. [Type inference and call graphs] Scalable Propagation Based Call Graph Construction Algorithms
3. [Soundness, completeness and complexity of program analysis] New results on the computability and complexity of points-to analysis
4. [Abstract interpretation] An Introduction to Abstract Interpretation
5. [Abstract interpretation, dataflow analysis, model checking] Data Flow Analysis is Model Checking of Abstract Interpretations
6. [Static slicing] Program Slicing
7. [IFDS] Precise Interprocedural Dataflow Analysis via Graph Reachability
8. [Dataflow analysis] ESP: Path-Sensitive Program Verification in Polynomial Time
9. [Infeasible paths] Refining Data Flow Information Using Infeasible Paths
10. [Symbolic execution] KLEE: Unassisted and Automatic Generation of High-coverage Tests for Complex Systems Programs
11. [Interprocedural analysis] Interprocedural Conditional Branch Elimination
13. [Delta-debugging] Simplifying and Isolating Failure-Inducing Input
14. [Dynamic slicing] Precise Dynamic Slicing Algorithms
15. [Dynamic analysis, invariants] Dynamically discovering likely program invariants to support software evolution (ICSE version)

* Survey due date: Week 8 (Mar 4)

Implementation

1. [required] icfg (call graph and control flow graphs)
2. [required] points-to analysis
3. [optional] dependency graphs and program slicing (static or dynamic)
4. [optional] taint analysis (static or dynamic)
5. [optional] infeasible paths detection
6. [optional] typestate checker
7. [optional] detecting loop invariants (dynamic)
8. [optional] type inference and call graph optimization

Research projects

* Proposal date: week 5 (Feb 12)
* Mid-term presentation: week 9 (Mar 11)
* Final project: week 16 (May 2)