Program Analysis

Prof. Sable

Independent Study Syllabus

1 Overview

Program analysis is a logic-based approach to analyzing software. One of the most important uses is to verify the correctness of programs – i.e., that it functions exactly as the programmer intends. For example, verification is useful for checking the correctness of new programming paradigms (such as declarative concurrent languages or intermittent programming). Other uses of program analysis are to find general bugs, augment software test frameworks, and optimize software. Possible resources for this I.S. are:

- Stanford: CS 357: Advanced Topics in Formal Methods

- CMU: 17-355/17-665/17-819 Program Analysis

- Resources for Teaching with Formal Methods

The primary text and schedule are based off of the CMU course. The text is *Program Analysis* by Jonathan Aldrich, Claire Le Goues, and Rohan Padhye.

2 Workload

The workload would mostly consist of readings and weekly class discussions. Supplementary exercises are also available on the CMU course webpage. There would also be a final project.

Two potential final projects are:

- Perform research on an advanced topic (e.g., the topics covered at the end of the CMU course), and present the knowledge in a report and verbal presentation.

- Show some of the results from the class using formal methods software, such as Coq.

3 Weekly Schedule

Some of the chapters are out of order – we mostly follow the CMU schedule.

1. Initial discussion and course planning
2. Ch1-3: Introduction, Program Representation, and Syntactic Analysis
3. Ch4: Dataflow Analysis and Abstract Interpretation
4. Ch5: Data Analysis Examples
5. Ch6: Dataflow Analysis Termination and Correctness
6. Ch7: Widening Operators and Collecting Semantics
7. Ch8: Interprocedural Analysis
8. Ch9: Control-Flow Analysis for Functional Languages
9. Ch11: Hoare-style Verification
10. Ch13: Symbolic Execution
11. Ch14: Concolic Testing
12. Ch16: Fuzz Testing
13. Ch12: Satisfiability Modulo Theories (SMT)
14. Ch15: Oracle-Guided Synthesis
15. Final Project Presentations