Organisation meeting: PhD Course on Symbolic Execution

Bengt Jonsson    Philipp Rümmer

http://user.it.uu.se/~bengt/SymbEx21/
Overview

● Symbolic execution is a technique to statically analyse programs
  ○ Path-wise
  ○ Symbolic inputs to explore the possible executions of a path
  ○ Proposed in 1976, but has become very successful mostly over the last 10-15 years
  ○ A basic overview will be given in this lecture (later)

● This course is about the theory and practice of symbolic execution
  ○ Main algorithms and components needed for symbolic execution
  ○ The ongoing research
  ○ Use of existing symbolic execution tools
  ○ Development or extension of tools

● Course credits: 5-10hp, depending on parts of the course included
Dates + Times

- Course will run in the spring term 2021
- Current plan: meet every week on Wednesday, 15:15 - 17:00
  - Can be rescheduled if time is too inconvenient
Block 1: Lectures

- Lectures/reading on basic theory and techniques
  - Complemented by papers, book chapters; some lectures provided as videos
- Small set of exercises

Preliminary schedule:

- Feb 10: Overview
- Feb 17: Constraint/SMT solving part I
- Mar 3: Constraint/SMT solving part II
- Mar 10: LLVM and Klee part I
- Mar 17: LLVM and Klee part II
Block 2: Seminars

- Reading and presentation of research papers on symbolic execution
- For each selected paper:
  - One student will organise a presentation, around 45min, for one of the Wednesday meetings
  - Two students will write conference-style reviews, and prepare questions that can be discussed after the seminar (the questions do not have to be answered by the presenter alone!)
- We will provide a template and instructions for the reviews
- By default, everybody should attend all seminars
- Preliminary list of papers in the Google doc, but we are still adding further papers. Feel free to propose or add papers!

Preliminary schedule:

- Seminars running March - May
Paper assignment

- Assignment will be handled through Easychair
  - Each course participant will be added as a PC member
  - We will submit the papers
- You have to bid for papers you are interested in, and we will assign presenters and reviewers
- Reviews have to be submitted through Easychair prior to the seminar
Block 3: Mini-project

- Define and carry out your own symbolic execution-related project
- Examples:
  - Do a larger case study with a symbolic execution tool
  - Extend an existing tool
  - Develop your own (minimalist) symbolic execution tool for some simple language

Preliminary schedule:

- Finished before summer
Summary: to earn credits, you need to ...

- **In the lecture part:**
  - Submit answers to all exercises

- **In the seminar part:**
  - Present 1 paper
  - Review 2 papers
  - Skip/miss at most 2 of the seminars

- **In the project part:**
  - Define and carry out your own symbolic execution-related project

*NB: actual credits are always awarded by the PhD supervisor!*
Participation

- People can still join the course (encourage other students!)

- Express your intention to participate by putting your name in the Google spreadsheet (link in the chat)

- Do you have any comments and questions?