Group Meeting - 5

Member: Yong Li, Depeng Liu, Weizhi Feng, Xie Li, Shizhen Yu, Yutian Zhu and Zongxin Liu

May 19, 2021

MemSafety: Progress and Problems

Previous plan: add implementation at SMACK frontend to support symbolic execution of separation logic.

Problems encountered:

- How to express symbolic heap in data structure/generated boogie program? (Feasible)
  - Added definition of symbolic heap into `BoogieAST.h`.
- How to modify the symbolic heap? (Feasible)
  - $\langle \Pi \mid \Sigma \rangle$, assume Σ has a fix order during the execution, find pattern.
- VC generation and verification (Problematic):
  - Seems tedious to use Boogie IVL because it is hard to unified separation logic at backend. (TODO: a more thorough look into Boogie to find out capabilities.)
  - Only use SMACK frontend and implement our own VC generation. (Feasible)
- Interblock: construct the CFG during instruction visiting. (Feasible)

Plan: implement SE for `malloc`,`free` and assignment in one block.

Shizhen Yu

- Reading
    - Enhancing Symbolic Execution of Heap-based Programs with Separation Logic for Test Input Generation
        - Motivation and Illustration
        - Operational semantics of the core language
- Preparing for matrix test
- Plan
    - Continue reading "Details on symbolic execution using SL" part of "Enhancing Symbolic Execution of Heap-based Programs with Separation Logic for Test Input Generation"

Yutian Zhu

- Compositional Shape Analysis by means of Bi-Abduction(Done, prepare for ppt)

Recent:

- Prepare for tests. A lot of homework.

Plan:

- Static automated program repair for heap properties. ICSE 2018. Rijnard van Tonder, Claire Le Goues