Group Meeting - 2

Member: Yong Li, Depeng Liu, Weizhi Feng, Xie Li, Shizhen yu, Zongxin Liu

2021 年 4 月 21 日

MemSafety: Progress and Problem Encountered

- SMACK: code reading.
  - Problem 1: How SMACK do the region splitting to modify the memory model?
    Paper reading:
    [1] Making Context-sensitive Points-to Analysis with Heap Cloning Practical For The Real World.
    - DSA, Andersen style analysis, Steensgaard's analysis and shape analysis.
  - Problem 2: How to adapt the assertion of separation logic into the generating and parsing of Boogie IVL.
    Paper reading:
    [2] A Primer on Separation Logic.
    [3] Enhancing Symbolic Execution of Heap-based Programs with Separation Logic for Test Input Generation.

    Tool investigating:
    - Predator, on how they deal with separation assertions.

    Case study:
    - Find a example program and write assertions in FOL and SL by hand to compare.
  - Problem 3: Sorting a document about the whole procedure of SMACK.

MemSafety: Progress and Problem Encourtered

- SMACK: running SV-COMP cases.
  - Problem 1: Specify the detailed result: which property, consistent or not.
  - Problem 2: Report the issue in Github.

BBA: Outline

- Bounded Büchi automata.
- **Bounded:**
  - Definition of bounded Büchi automata and bounded languages.
  - Relationship of bounded languages and ω-regular languages.
- Plan.

BBA: Bounded Büchi Automaton & Bounded Language

Definition

Given an integer $d > 0$ and a Büchi automaton $\mathcal{A}$, we call the Büchi automaton with the integer d as a bounded Büchi automaton.

Definition

A run $\rho = q_0 q_1 ...$ is accepting iff there exists an integer $i \geq 0$, the distance between any two consecutive accepting states with index greater than i is at most d. Formally, a run is accepting iff $\exists i \geq 0, \forall j \geq i, \{q_j, q_{j+1}, ..., q_{j+d-1}\} \cap F \neq \emptyset$, where F is the set of accepting states. Then we call such an accepting run a bounded run. A bounded word w is accepted by $(\mathcal{A}, d)$ if there is an accepting bounded run of $(\mathcal{A}, d)$ on w. The bounded language recognized by $(\mathcal{A}, d)$, denoted $\mathcal{L}(\mathcal{A}, d)$, is the set of bounded words that $(\mathcal{A}, d)$ accepts.

BBA: Bounded Languages & ω-regular Languages

- Proved that bounded languages are ω-regular languages.
- Proved that ω-regular languages cannot be expressed by bounded languages.
- Therefore, bounded languages are the subset of ω-regular languages.

BBA: Plan

Thinking about the computation of bounded languages...

- Intersection ;
  - Two bounded automata with the same d and different d;
- Complement.