Group Meeting - 3

April 28, 2021

Presentation for Scholarship

- SMACK:
  - Prev - Problem 1 (Done): How SMACK do the region splitting to modify the memory model?
    - DSA algorithm: to be introduced tomorrow.
      Data Structure Graph (can be regarded as memory model) is introduced to do pointer analysis.
    - Problem 1: What is the difference if we adapt separation logic to it?
  - Prev - Problem 2 (Ongoing): How to adapt the assertion of separation logic into the generating and parsing of Boogie IVL.
    Tool investigating:
    - Predator, on how they deal with separation assertions.

    Case study:
    - (1) Find a example program and write assertions in FOL and SL by hand to compare.
- Boogie Verifier: code reading (Ongoing).
  - Found where to modify to add separation logic parsing.
  - Found the interface to plug the SL-Solver to backend to do VC generation and verification.

MemSafety: A Simple Case

Example

```
int main(){
    // emp
    int *i = malloc(2*sizeof(int));
    // blk(i, i+2)
    int *j = malloc(sizeof(int));
    // blk(i, i+2) * blk(j, j+1)
    *i = 0;
    // i ↦ 0 * blk(i+1, i+2) * blk(j, j+1)
    *j = 1;
    // i ↦ 0 * blk(i+1, i+2) * j ↦ 1
    free(i);
    // blk(i+1, i+2) * j ↦ 1
    free(j);
    // blk(i+1, i+2)

}
```

MemSafety: TODOs

- Problem: How to adapt separation logic to current framework?
  - Code reading of Predator: how to deal with assertion in separation logic.
  - [1] Paper about shape analysis.
  - [2] Shape analysis based on separation logic.
- Combine termination and memory safety:
  - [1] Existing work: Proving Termination and Memory Safety for Programs with Pointer Arithmetic.
- Investigate and try the SL-Solver: Asterix, ComSPEN,...

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 $\rho = q_0 q_1 \ldots$ 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 $\exists i \geq 0, \forall j \geq i, \{q_j, q_{j+1}, \ldots, q_{j+d-1}\} \cap F \neq \emptyset$, 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 $\mathcal{L}(\mathcal{A}, \mathrm{d})$, 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.