硕士开题答辩
基于分离逻辑的内存安全分析与验证

学生：李勰　　导师：张立军

2021 年 6 月 25 日

提纲

- 选题的背景及意义
- 本题目的研究内容
- 研究计划及已有科研基础

背景和意义

- 什么是内存安全问题
  - 程序中的内存操作：`malloc, free, load, store...`
  - 常见的内存安全问题：内存泄漏、空指针解引用、访问越界等..
  - 可能出现的场景：嵌入式开发、网络编程、并发编程等
- 内存安全的重要性

本题目的研究内容

基于分离逻辑的内存安全分析与验证

本题目的研究内容

基于分离逻辑的内存安全分析与验证

定义 (霍尔三元组)

霍尔三元组的语法形式：

$$\{P\}C\{Q\}$$

其中 P, Q 分别是用逻辑公式表示的前置条件和后置条件，C 是执行的程序。

本题目的研究内容

基于分离逻辑的内存安全分析与验证

定义 (霍尔三元组)

霍尔三元组的语法形式：

$$\{P\}C\{Q\}$$

其中 P, Q 分别是用逻辑公式表示的前置条件和后置条件，C 是执行的程序。

这里 C 是含有内存操作的程序，程序的状态可以表示为

$$\mathsf{States} = \mathsf{Store} \times \mathsf{Heap}$$

$$\mathsf{Store} : Var \to (Val \cup Loc), \quad \mathsf{Heap} : Loc \to_+ (Loc \cup Val)$$

分离逻辑

定义 (符号堆)

符号堆 (Symbolic Heap) **的语法形式**:

$$\Pi \mid \Sigma$$

Π **为纯公式** Σ **为空间公式**。

例

$$y = x + 3 \wedge x > 0 \mid \mathtt{blk}(x, y) * y \mapsto 2$$
$$i = 0 \wedge j = 0 \mid \mathtt{emp}$$
$$\mathtt{true} \mid \mathtt{blk}(a, b) * \mathtt{blk}(c, d)$$

本题目研究内容

基于已有的利用分离逻辑公式的符号执行思想，对关心的内存安全性质进行归约验证。

例

main 函数中的代码片段 C，内存泄漏

$$\{\mathsf{true} \mid \mathsf{emp}\}\, C\, \{\mathsf{true} \mid \mathsf{emp}\}$$

需要的工作：

- 给出符合程序语义的分离逻辑推导规则
- 根据性质，定位需要进行验证的位置，并生成验证条件

其他问题

- 循环的处理
  - 循环展开
  - 合成循环不变式 - 抽象解释 - 抽象域
  - 循环摘要 (summary).
- 指针算术
- 和终止性、Incorrectness Logic 等的结合

研究计划

- 第一阶段：更深入的调研，对相关工具的调研。如 PREDATOR，SMACK 等内存分析工具，以及抽象解释框架 CRAB 等.
- 第二阶段：基于已有的工具搭建分析验证平台，从符号执行开始对工具迭代增强。
- 第三阶段：通过对实例的研究，探索能够提高验证工具的效率和能力的理论途径和技术手段，包括设计设计抽象域并进行抽象解释、对内存操作的具体细节进行技术上的优化。
- 第四阶段：在以上的工作中形成并发表学术论文，撰写学位论文。

已有研究基础

已发表两篇论文，

[1] Xie Li, Yi Li, Yong Li, Xuechao Sun, Andrea Turrini and Lijunzhang. SVMRanker: a general termination analysis framework of loop programs via SVM. ESEC/SIGSOFT FSE 2020: 1635-1639

[2] Xie Li, Taolue Chen, Zhilin Wu, Mingji Xia. Computing Linear Arithmetic Representation of Reachability Relation of One-Counter Automata. SETTA 2020: 89-107

对利用 SMT 做程序性质验证、逻辑归约等方法和技术手段较为熟悉。并在以上两个项目中进行了工具的开发，在实现方面也有一定经验。

谢谢!