

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
- 已有科研基础及研究计划

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

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

$$\text{Store} : \text{Var} \rightarrow \text{Val}, \quad \text{Heap} : \text{Loc} \rightarrow_+ (\text{Loc} \cup \text{Val})$$

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

$$y = x + 3 \wedge x > 0 \mid \text{blk}(x, y) * y \mapsto 2$$

$$i = 0 \wedge j = 0 \mid \text{emp}$$

$$\text{true} \mid \text{blk}(a, b) * \text{blk}(c, d)$$

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

$$\{\text{true} \mid \text{emp}\} C \{\text{true} \mid \text{emp}\}$$

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
- 指针算术
- 不确定的变量初始值

