迎新报告

朱雨田

2022 年 8 月 31 日

1 科研工作

目前参与的科研工作主要有两个:

- 参与开发 SESL-C 程序内存安全分析工具并成功参加 SV-COMP 比赛。SESL 是一个基于数组分离逻辑的内存安全分析工具，目前已实现符号执行和 BMC 两个分析引擎。数组分离逻辑在含有原子指向约束的分离逻辑的基础上，加入描述已分配但没有被赋值的内存空间的归纳谓词，便于描述 malloc, free 等对动态内存空间变化的描述。在利用数组分离逻辑公式描述程序状态语义的变化后，再通过求解分析内存安全问题（如内存泄漏、指针非法引用等）。符号执行通过公式的变化描述程序每一条路径的语义变化，在执行过程中的执行完成调用求解器进行分析。BMC 则将整个程序编码成迁移系统，其中用分离逻辑公式编码，后续分析跟 BMC 类似。
- 带指针算数和一般归纳定义的分离逻辑的判定算法。本研究旨在将指针算术和一般归纳谓词结合，探索一个可判定的分离逻辑子集，提出一个通用的分离逻辑求解算法。难点在于指针算术的引入使分离逻辑的蕴涵问题的求解变得困难，甚至不可判定。目前，已解决可满足性问题。也证明了在对语法不加额外限制的情况下的蕴涵问题是不可判定的。

2 感悟

珍惜时间，多交流!