Group Meeting - 7

Members: Yong Li, Depeng Liu, Weizhi Feng, Xie Li, Shizhen Yu, Yutian Zhu, Zongxin Liu

2021 年 6 月 23 日

差分隐私

这俩周:

- 中期答辩;
- Aplas 期刊：其他部分初步完成；由于 MDP 算法仅是充分的，Stream 例子的 pan-privacy 分析可能有点问题，需加以解释和根据实验情况确定。
- 在调研几个部分：预估通过学习算法学得 DP 模型可行性、实际代码中的 DP 部署及验证、APPLE 的差分隐私验证、隐私参数的选取等。
- 用 SageMath 做带有绝对值的连续噪声的带参定积分，分段积分是可计算的，解决简单连续机制如 Laplace 的验证；复杂机制刻画输入输出关系方面困难一些，需尝试。

计划:

- Aplas 期刊：计划完成
- 调研部分：报告讨论一下调研情况，再具体分析后续工作。

内存安全工具开发

进展情况：

- 添加了对于 `load` 语句的支持。
- 完成了对于一个基本块的符号执行、验证条件生成的框架，目前可以对一个基本块内的内存泄漏性质进行验证。

TODOs：

- 修复指针算术 bit 和 byte 的 bug (DONE)
- 修复 blk 语义导致的 entailment 不成功问题 (DONE)
- 修复 blk 分裂时，如果一开始 malloc 的大小是 0 的问题
- 加入对数组和结构体的支持
  - 对 alloca 指令进行相关的符号执行处理
  - 将所有变量在调用求解器之前转为字节为基本单位：需要在符号执行时所有变量的类型，等式翻译时的 cast 问题的处理，新旧变量之间的关系和新变量的取值约束
- 完成对从 SV-COMP 改造过来的例子内存泄漏的分析。

例子

```
typedef struct {
    void *lo;
    void *hi;
} TData;

int main(){
    TData data;
    TData* pdata = &data;
    pdata->lo = malloc(16);
    pdata->hi = malloc(24);
    void *lo = pdata->lo;
    void *hi = pdata->hi;
    if (lo == hi) {
        free(lo);
        free(hi);
    }
    pdata->lo = (void *) 0;
    pdata->hi = (void *) 0;
}
```

- 可能有机会完成的内容：将 BlockExecutor 用到 CFG 上，实现 CFG 上的符号执行。

内存安全工具开发

文献阅读:

[1] Thomas Ströder et al. Proving Termination and Memory Safety for Programs with Pointer Arithmetic. IJCAR'14.

冯维直

进展：

- 阅读 rank-based 和 slice-based 算法做 unambiguous Büchi automata 取补的 GandALF '20 文章，在李老师的指导下基于 spot 库实现 slice-based 的算法.
- 结合 NCSB 算法的 TACAS 文章读 seminator 和 spot 中实现 semi-deterministic Büchi automata 取补的代码.
- 基于 seminator 和 spot 提供的自动机库和接口等实现了 unambiguous Büchi automata 取补的 slice-based 的算法，运行结果有些问题，需要继续调试.

计划：

- Slice-based 算法正确实现成功运行，进行实验，和李老师讨论，在 GandALF '20 文章基础上写实验部分的章节.