迎新报告

朱雨田

导师：吴志林

2022 年 9 月 4 日

SESL: 内存安全分析工具

```
int main(){
    // emp
    int *i = malloc(2*sizeof(int));
    // blk(i, i+8)
    *i = 0;
    // i ↦ 0 * blk(i+4, i+8)
    free(i);
    // emp
}
```

- 利用数组分离逻辑对程序语义进行编码，通过求解分析内存安全问题。
- 目前实现了符号执行引擎和 BMC 引擎。效果一般 QAQ。
- https://spencerl-y.github.io/SESL/.

带指针算术和一般归纳谓词的分离逻辑判定算法

$$\varphi := x_1 + 1 = x_2 \wedge x_3 < x_4 \wedge y_1 < y_2 : x_1 \mapsto y_1 * x_2 \mapsto y_2 * P_2(x_3, x_4)$$
$$\psi := true : P_1(x_1, x_4)$$

- *satisfiability*: 存在对变量的赋值，满足公式；
- *entailment*: $\varphi \models \psi$, 证明所有满足 φ 的赋值，同时也满足 ψ.
- 目前解决了可满足性问题；
- 证明了在归纳谓词语法形式为

$$P(x, y) := \exists \vec{z}.\Pi : x \mapsto \{\xi\} * P_1(t_1, t_2) * \cdots * P_k(t_{2k-1}, t_{2k})$$

的 entailment 问题是不可判定的。

感悟

多交流，珍惜时间！