软件分析技术 2018 课程大作业二

Syntax-Guided Program Synthesize

小组成员： 黄杨洋 张博洋 刘渊强

一、 目标

- 给定文法 G 和约束 C ，生成程序 P 使得 P 属于 L(G) 并且 P 满足约束 C
- 文法 G 的形式为 Synth-lib
- 约束 C 的形式为 SMTlib
- 输出 P 的形式为 SMTlib
- 基于课程上给的Python框架
- 使用 z3 作为 checker

二、 评测结果

- 在本机评测中，已通过 open_tests 中的 three.sl tutorial.sl max*.sl(所有max类型) array_search_*.sl(所有array_search类型)
- 尚未通过的为 s1 s2 s3 这三个测试
- 具体评测结果见附录

三、 算法主要设计思想

- 将“删去的两行”补上了，因此能通过 three.sl tutorial.sl 这两个测试
- 为max系列和array_search系列设计了专为数组生成循环的功能
    - 首先根据启发式规则，区分出“作为数组元素的参数”和“作为额外参数的参数”
        - 如在array_search_3中，x1 x2 x3为“作为数组元素的参数”，而k1为“作为额外参数的参数”
    - 通过暴力BFS搜索生成“边界条件式”、“迭代式”两个程序
        - 其中，迭代式中可使用“$NEXT”、“$AELE”、“$AIDX”这三个特殊值，它们分别代表“上一次迭代结果”、“当前迭代数组元素”、“当前迭代数组下标”
        - 如在array_search_3中
            - “边界条件式”为：3
            - “迭代式”为：(ite (< $AELE k1) $NEXT $AIDX)
    - 将“边界条件式”与“迭代式”编译成 Z3 所能理解的格式
        - 首先对每一次迭代生成一个独立的函数

```
(define-fun LBOUND_findIdx (...) Int 3)
(define-fun L2_findIdx (...) Int (ite (< $AELE k1) $NEXT $AIDX))
(define-fun L1_findIdx (...) Int (ite (< $AELE k1) $NEXT $AIDX))
(define-fun findIdx (...) Int (ite (< $AELE k1) $NEXT $AIDX))
```

        - 然后使用字符串替换，将“$NEXT”、“$AELE”、“$AIDX”分别替换为“对下一次迭代对应的函数调用”、“对应数组元素”、“对应数组下标”
        - 替换后的结果为

```
(define-fun LBOUND_findIdx (...) Int 3)
(define-fun L2_findIdx (...) Int (ite (< y3 k1) (LBOUND_findIdx
y1 y2 y3 k1) 2))
(define-fun L1_findIdx (...) Int (ite (< y2 k1) (L2_findIdx y1
y2 y3 k1) 1))
(define-fun findIdx (...) Int (ite (< y1 k1) (L1_findIdx y1 y2
y3 k1) 0))
```

- 将编译后的版本送到 z3 中进行检验
  - 若符合要求，再将原程序替换为单个函数的版本（具体方法为，将多函数版本中的函数调用，直接用函数体替代）

```
(define-fun findIdx (...) Int (ite (< y1 k1) (ite (< y2 k1) (ite
(< y3 k1) 3 2) 1) 0))
```

  - 这样做的缺点在于，如果迭代式中多次引用了下一次迭代的结果，会导致“指数爆炸”
    - 如 max15 的迭代式为

```
(ite (<= $NEXT $AELE) $AELE $NEXT))
```

    - 最后生成出的代码大小约为 700KB
- 一些简单优化
  - 若检测到数组输入，则从语法中删去“作为数组输入的变量”、“1、2……数组输入个数”
  - 若检测到语法中同时有“<”和“>=”，则删去“>=”
  - 若检测到语法中同时有“>”和“<=”，则删去“<=”
  - 调整语法中各元素的顺序，将容易出结果的元素提前

四、 小组

- 黄杨洋 1801213684
- 张博洋 1801111368
- 刘渊强 1500012883

附录：具体评测结果（仅供参考）

- 评测环境：
  - OS : Ubuntu 18.04.1 LTS
  - Memory : 8 GB
  - Processor : Intel(R) Core(TM) i7-4650U CPU @ 1.70GHz
  - OS type : 64-bit
- 详细评测结果：

file	time
array_search_2.sl	Passed(10.022810)
array_search_3.sl	Passed(12.009904)

file	time
array_search_4.sl	Passed(14.020320)
array_search_5.sl	Passed(16.128435)
array_search_6.sl	Passed(18.327113)
array_search_7.sl	Passed(20.761182)
array_search_8.sl	Passed(23.382021)
array_search_9.sl	Passed(25.832454)
array_search_10.sl	Passed(28.349099)
array_search_11.sl	Passed(31.356275)
array_search_12.sl	Passed(34.535173)
array_search_13.sl	Passed(37.414635)
array_search_14.sl	Passed(40.971171)
array_search_15.sl	Passed(44.707254)
max2.sl	Passed(14.262785)
max3.sl	Passed(15.247076)
max4.sl	Passed(15.833403)
max5.sl	Passed(16.454156)
max6.sl	Passed(17.111743)
max7.sl	Passed(17.797536)
max8.sl	Passed(18.548729)
max9.sl	Passed(19.305919)
max10.sl	Passed(20.008272)
max12.sl	Passed(21.514607)
max13.sl	Passed(22.293114)
max14.sl	Passed(23.040831)
max15.sl	Passed(23.833102)
max_11.sl	Passed(20.969262)
s1.sl	timeout after 300
s2.sl	timeout after 300
s3.sl	timeout after 300
three.sl	Passed(1.659181)

file	time
tutorial.sl	Passed(30.903244)