软件分析

程序综合：基础

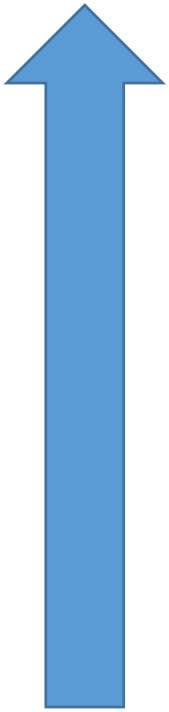
熊英飞
北京大学

软件分析课程内容

- 基于抽象解释的分析
  - 数据流分析
  - 过程间分析
  - 指向分析
  - 控制流分析
  - 抽象解释理论
  - 符号抽象
- 基于约束求解的分析
  - SAT求解算法
  - SMT求解算法
  - 符号执行
  - 霍尔逻辑和谓词变换
- 分析技术应用
  - 程序综合
  - 错误定位
  - 错误修复

Can grandmas program?

- The development of programming languages is to raise the level of abstraction



What is the next?

Haskell (1990), Prolog (1972)

Java

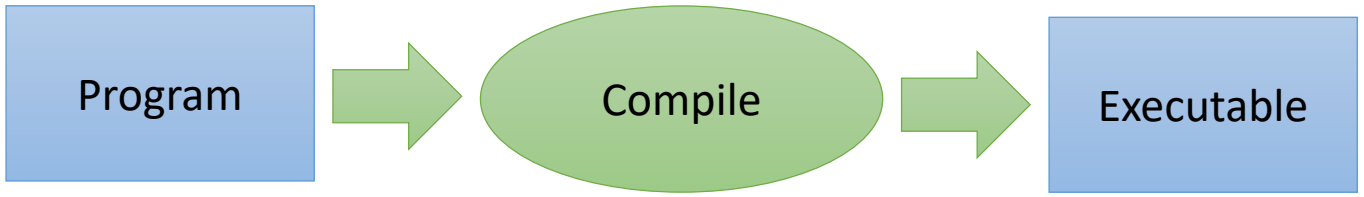
C

Assembly

Why cannot?

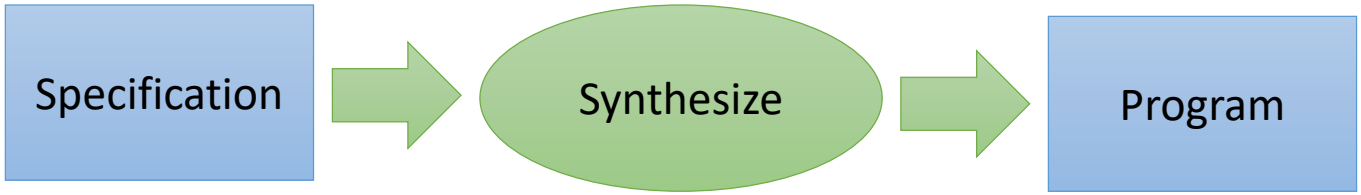
- Programming languages come with many guarantees
  - Well-typed programs are guaranteed to compile
  - Compiled programs have clear, well-defined semantics

- It is difficult to further raise the level of abstraction



Program Synthesis saves grandmas

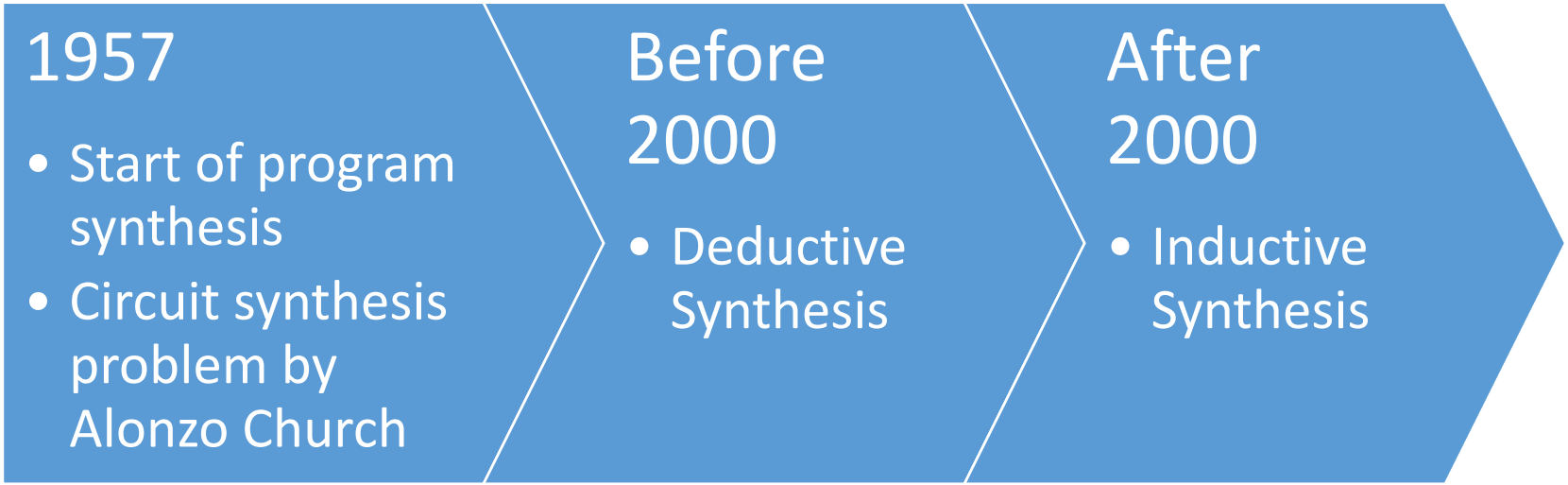
- Generate a program from a specification
  - Specification can be fuzzy
  - Generation is not guaranteed



"One of the most central problems in the theory of programming."
----Amir Pneuli
Turing Award Recipient

"The fundamental way to improve software productivity."
----Jiafu Xu
Founder of Software Research in China

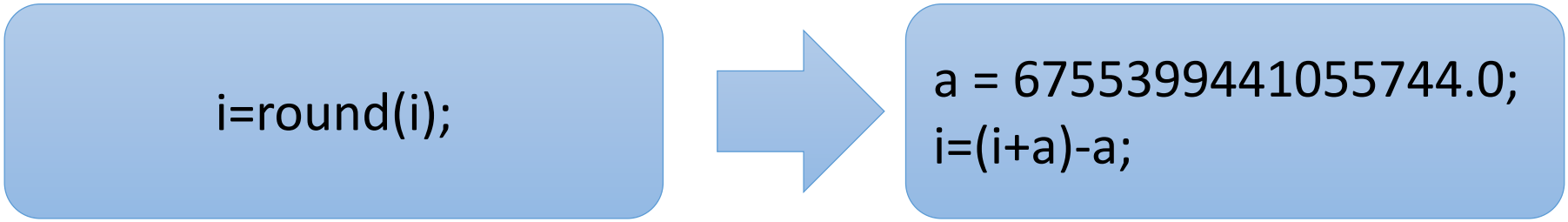
History of Program Synthesis



典型应用——Data Wrangling

	A	B
1	Email	Column 2
2	Nancy.FreeHafer@fourthcoffee.com	nancy freehafer
3	Andrew.Cencici@northwindtraders.com	andrew cencici
4	Jan.Kotas@litwareinc.com	jan kotas
5	Mariya.Sergienko@gradicdesigninstitute.com	mariya sergienko
6	Steven.Thorpe@northwindtraders.com	steven thorpe
7	Michael.Neipper@northwindtraders.com	michael neipper
8	Robert.Zare@northwindtraders.com	robert zare
9	Laura.Giussani@adventure-works.com	laura giussani
10	Anne.HL@northwindtraders.com	anne hl
11	Alexander.David@contoso.com	alexander david
12	Kim.Shane@northwindtraders.com	kim shane
13	Manish.Chopra@northwindtraders.com	manish chopra
14	Gerwald.Oberleitner@northwindtraders.com	gerwald oberleitner
15	Amr.Zaki@northwindtraders.com	amr zaki
16	Yvonne.McKay@northwindtraders.com	yvonne mckay
17	Amanda.Pinto@northwindtraders.com	amanda pinto

典型应用– Superoptimization



典型应用–自动编写重复程序


```
class AcidicSwampOoze(MinionCard):
    def __init__(self):
        super().__init__("Acidic Swamp Ooze", 2,
                CHARACTER_CLASS.ALL, CARD_RARITY.COMMON,
                battlecry=Battlecry(Destroy(),
                        WeaponSelector(EnemyPlayer())))

    def create_minion(self, player):
        return Minion(3, 2)
```

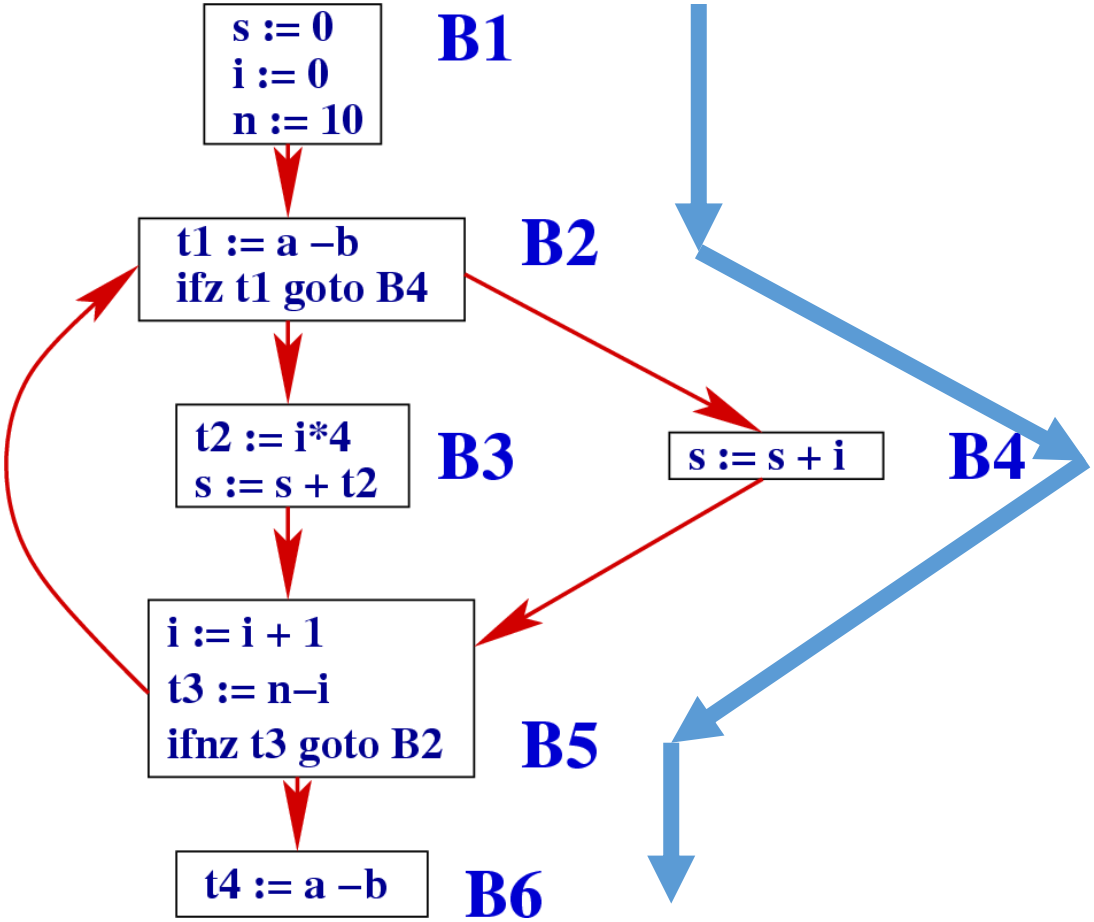
Application – Program Repair


```
/** Compute the maximum of two values
* @param a first value
* @param b second value
* @return b if a is lesser or equal to b, a otherwise
*/
public static int max(final int a, final int b) {
    return (a <= b) ? a : b;
}
```

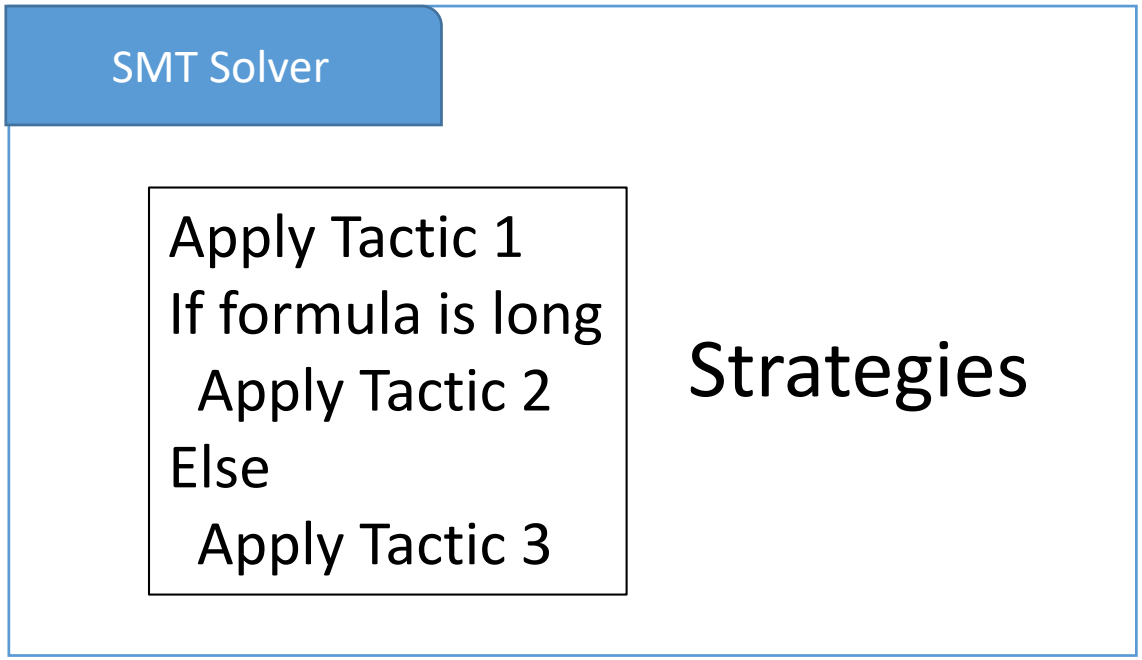
Synthesize an expression to replace the buggy one

Application – Testing

Synthesize a unit test to cover a path



Application – Analysis



Synthesize a strategy for a class of problems

Defining Program Synthesis

Classic Synthesis	Program Optimization	Program Estimation
• Input: • A specification • Output: A program that • meets the specification	• Input: • A specification • A cost function • Output: A program that • meets the specification, and • maximizes the cost function	• Input: • A specification • A dataset for target distribution • Output: A program that • meets the specification and • maximizes the probability represented by the dataset
Test Generation	Superoptimization	Program Repair

程序综合是软件分析问题

- 程序综合问题：编写程序实现函数f，满足$f(x,1) = x \wedge f(x,y) = f(y,x)$
  - expr = var op var
  - var = x | y
  - op = + | - | * | /

- 给空间里的所有程序编号，然后编写如下程序：

```
Int f(n, x, y) {
  switch(n) {
    case 1: return x+y;
    case 2: return x-y;
    case 3: return x*y; }}
```

- 软件分析问题：是否存在n，使得上述规约满足？

This Lecture

Classic Synthesis

- Problem Definition
- Enumerative
- Constraint-based
- Presentation-based

Program Estimation

- Problem Definition
- Estimating Probabilities
- Locating the most-likely one

SyGuS:
程序综合问题的标准化

- 输入：语法G，约束C
- 输出：程序P，P符合语法G并且满足C

- 输入输出格式：Synth-Lib
  - http://sygus.seas.upenn.edu/files/SyGuS-IF.pdf

例子：max问题

- 语法：

$$
\begin{array}{rcl}
\texttt{Expr} & ::= & 0 \mid 1 \mid x \mid y \\
& \mid & \texttt{Expr} + \texttt{Expr} \\
& \mid & \texttt{Expr} - \texttt{Expr} \\
& \mid & (\texttt{ite BoolExpr Expr Expr}) \\
\texttt{BoolExpr} & ::= & \texttt{BoolExpr} \wedge \texttt{BoolExpr} \\
& \mid & \neg\texttt{BoolExpr} \\
& \mid & \texttt{Expr} \leq \texttt{Expr}
\end{array}
$$

- 规约：

$$
\begin{aligned}
\forall x, y : \mathbb{Z}, \quad & max_2\,(x, y) \geq x \wedge max_2\,(x, y) \geq y \\
& \wedge (max_2\,(x, y) = x \vee max_2\,(x, y) = y)
\end{aligned}
$$

- 期望答案：ite (x <= y) y x

Sync-Lib：定义逻辑

- 和SMT-Lib完全一致
- (set-logic LIA)
- 该逻辑定义了我们后续可以用的符号以及这些符号的语法/语义，程序的语法应该是该逻辑语法的子集。

Sync-Lib：语法

```
(synth-fun max2 ((x Int) (y Int)) Int
    ((Start Int (x
                 y
                 0
                 1
                 (+ Start Start)
                 (- Start Start)
                 (ite StartBool Start Start)))
     (StartBool Bool ((and StartBool StartBool)
                      (or  StartBool StartBool)
                      (not StartBool)
                      (<=  Start Start)
                      (=   Start Start)
                      (>=  Start Start)))))
```

约束


```
(declare-var x Int)
(declare-var y Int)

(constraint (>= (max2 x y) x))
(constraint >= (max2 x y) y)
(constraint(or (= x (max2 x y))
               (= y (max2 x y))))


(check-synth)
```

约束表示方式和SMTLib一致

期望输出

输出：

```
(define-fun max2 ((x Int) (y Int)) Int (ite (<= x y) y x))
```

输出必须：

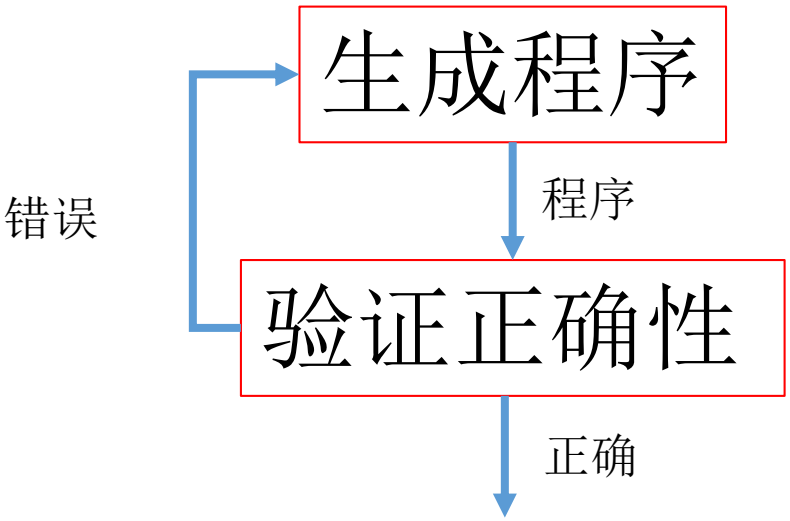
- 满足语法要求
  - 即，语法和SMTLib/Logic不一致就合成不出正确的程序
- 满足约束要求
  - 一般要求可以通过SMT验证

课程项目2

感谢曾沐焓刘鑫远同学准备课程项目！

- 编写程序求解SyGuS问题
- 每小组提交：
  - 一个SyGuS求解器
  - 一个测试样例，至少用自己的求解器2分钟可以解出
- 限制：只考虑基础算术和逻辑表达式
- 截止日期：12月22日提交，12月25日报告
- 程序包包括：
  - 完整的测试环境（含所有官方测试用例）
  - 最基本的solver（解不出来几道题）
- 评分：根据解出来的样例个数评分（每个时限5分钟）

程序综合作为搜索问题



Q1:如何产生下一个被搜索的程序？

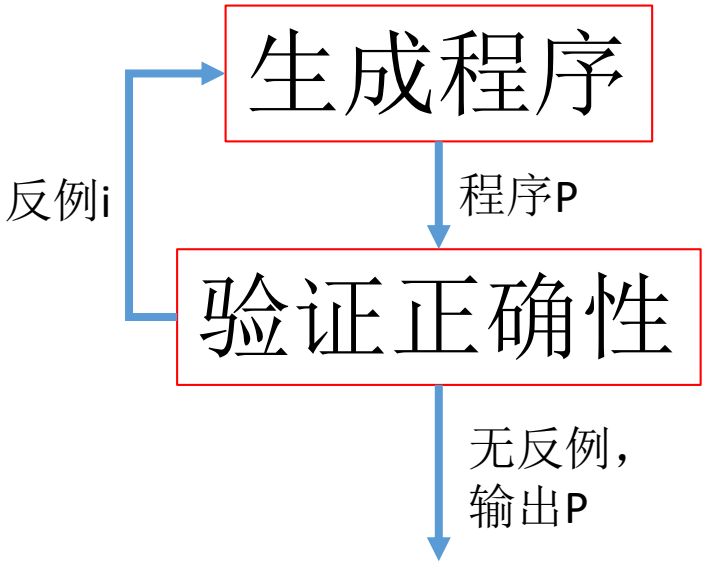
Q2:如何验证程序的正确性？

如何验证程序的正确性？

- 采用本课程学习的技术
  - 抽象解释
  - 符号执行

- 目前大多数程序综合技术都只处理表达式
  - 可直接转成约束让SMT求解
  - Synth-lib直接提供支持

CEGIS——基于反例的优化



- 采用约束求解验证程序的正确性较慢
- 执行测试较快
  - 大多数错误被一两个测试过滤掉
- 将约束求解器返回的反例作为测试输入保存
- 验证的时候首先采用测试验证

如何产生下一个被搜索的程序？

- 多种不同方法
  - 枚举法 —— 按照固定格式搜索
  - 约束求解法 —— 将程序搜索问题整体转成约束求解问题
  - 启发式搜索法 ——采用启发式搜索
  - 统计法 —— 采用机器学习等方法寻找概率最高的程序

枚举法

自顶向下遍历

- 按语法依次展开
  - S
  - x, y, S+S, S-S, if(B, S, S)
  - y, S+S, S-S, if(B, S, S)
  - S+S, S-S, if(B, S, S)
  - x+S, y+S, S+S+S, S-S+S, if(B, S, S)+S, S-S, if(B, S, S)
  - …

自顶向下遍历


```
function EnumTopDownSearch(grammar G, spec φ)
    P̃ ← [S] // An ordered list of partial derivations in G
    P̃_v ← {S} // A set of programs
    while P̃ ≠ ∅ do
        p ← RemoveFirst(P̃)
        if φ(p) then // Specification φ is satisfied
            return p
        α̃ ← NonTerminals(p)
        foreach α ∈ RankNonTerminals(α̃, φ) do
            β̃ ← {β|(α, β) ∈ R}
            foreach β ∈ RankProductionRule(β̃, φ) do
                p′ ← p[α → β]
                if ¬Subsumed(p′, P̃_v, φ) then
                    P̃.Insert(p′)
                    P̃_v ← P̃_v ∪ p′
```

对非终结符排序

对产生式排序

检查程序是否和之前的等价，比如x+S和S+x
为什么φ也是参数？

自底向上遍历

- 从小到大组合表达式
  - size=1
    - x, y
  - size=2
  - size=3
    - x+y, x-y
  - size=4
  - size=5
    - x+(x+y), x-(x+y), …
  - size=6
    - if(x<=y, x, y), …

自底向上遍历


```
function EnumBottomUpSearch(grammar G, spec φ)
    Ẽ ← {Φ} // Set of expressions in G
    progSize ← 1
    while True do
        C̃ ← EnumerateExprs(G, Ẽ, progSize)
        foreach c ∈ C̃ do
            if φ(c) then // Specification φ is satisfied
                return c
            if ¬∃ e ∈ Ẽ : Equiv(e, c, φ) then
                Ẽ.Insert(c)
        progSize ← progSize + 1
```

根据语法G，用$\tilde{E}$组合出大小等于progSize的所有表达式

判断e和c是否等价。

双向搜索

- 自底向上遍历可以看做是从输入开始搜索
- 自顶向下遍历可以看做是从输出开始搜索
- 也可以从输入输出同时开始搜索
- 要求能计算最强后条件或者最弱前条件
- 通常用于pipeline程序或者系统状态固定的程序
  - 如：汇编语言的合成
  - Phitchaya Mangpo Phothilimthana, Aditya Thakur, Rastislav Bodík, Dinakar Dhurjati: Scaling up Superoptimization. ASPLOS 2016. 297-310

双向搜索

function BIDIRECTIONALSEARCH(grammar G, spec $\phi \equiv (\phi_{\texttt{pre}}, \phi_{\texttt{post}})$)
  $\widetilde{F} \leftarrow \phi$ // Set of expressions from Forward search
  $\widetilde{B} \leftarrow \phi$ // Set of expressions from Backward search
  progSize $\leftarrow 1$
  while $\neg \exists f \in \widetilde{F}, b \in \widetilde{B}$: MATCHSTATE(f, b) **do**
    $\widetilde{F} \leftarrow$ ENUMFORWARDEXPRS$(G, \widetilde{F}, \phi_{\texttt{pre}}, \texttt{progSize})$
    $\widetilde{B} \leftarrow$ ENUMBACKWARDEXPRS$(G, \widetilde{B}, \phi_{\texttt{post}}, \texttt{progSize})$
    progSize $\leftarrow$ progSize $+ 1$
  $p \leftarrow f \oplus b$, where $\exists f \in \widetilde{F}, b \in \widetilde{B}$: MATCHSTATE(f, b)
  return p

Optimization

- Discard a partial program early
- Pruning
  - None of the expansions could satisfy the specification
  - ~~Ite BoolExpr x x~~
- Equivalence reduction
  - Equivalent to a previous program
  - Expr+x, ~~x+Expr~~

Pruning

- Generate constraints from the partial program

Ite BoolExpr x x 

```
(declare-fun boolExpr () Int)
(declare-fun max2 ((x Int) (y Int)) Int
   (ite boolExpr x x))
```

- Generate constraints from each test

max2(1,2)=2 

```
(assert (= (max2 1 2) 2))

(check-sat)
```


Needs to balance between the benefit and the cost.

判断程序是否等价

- 通过SMT求解器可以判断
  - 判断$f(x,y) \neq f'(x,y)$是否可以满足
  - 开销较大，不一定划算

- 通过测试判断
  - 运行所有测试检测 $f = f'$
  - 并不能保证结果的正确性
  - 对于不完整程序不能运行测试

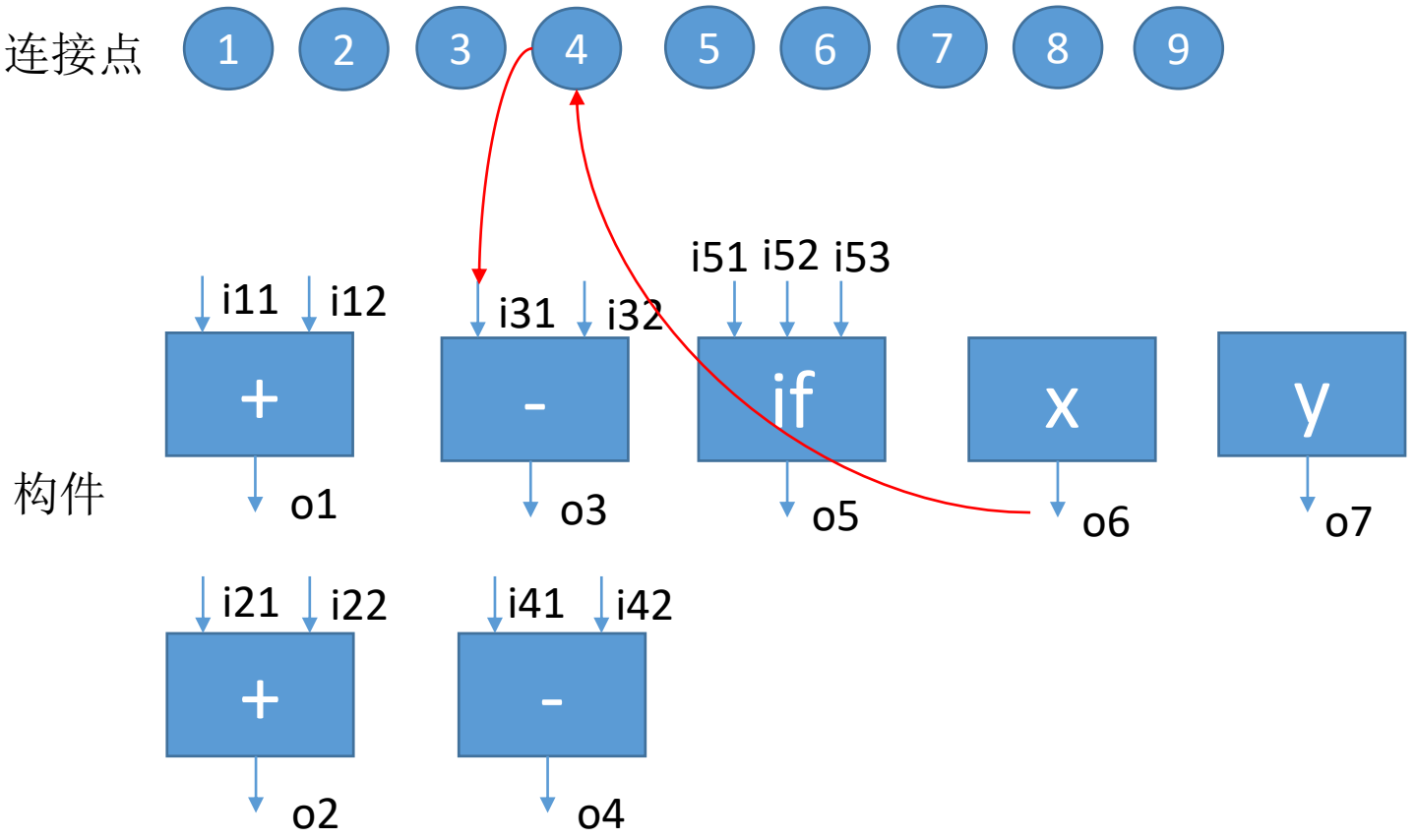
- 通过预定义规则判断
  - 如S+x和x+S的等价性

约束求解法

约束求解法

- 将程序综合问题整体转换成约束求解问题，由SMT求解器求解

基于构件的程序综合
Component-Based Program Synthesis



添加标签变量：

- $l_{i11}, l_{i22}, \ldots$
- $l_{o1}, l_{o2}, \ldots$
- l_o：程序输出

$l_{o6} = l_{i31} = 4$

产生约束

- 产生规约约束：
  - $\forall x, y: o \geq x \wedge o \geq y \wedge (o = x \vee o = y)$
- 对所有component产生语义约束：
  - $o1 = i11 + i12$
- 对所有的输入输出标签对产生连接约束：
  - $l_{o1} = l_{i11} \rightarrow o_1 = i_{11}$
- 对所有的输出标签产生编号范围约束
  - $l_{o1} \geq 1 \wedge l_{o1} \leq 9$
- 对所有的o_i对产生唯一性约束
  - $l_{o1} \neq l_{o2}$
- 对统一构件的输入和输出产生防环约束
  - $l_{i11} < l_{o1}$

能否去掉连接点和输出标签l_{ox}…，直接用l_{ixx}的值表示应该连接第几号输出？

约束限制

- 之前的约束带有全称量词，不好求解
- 实践中通常只用于规约为输入输出样例的情况
- 假设规约为
  - $f(1,2) = 2$
  - $f(3,2) = 3$
- 则产生的约束为：
  - $x = 1 \wedge y = 2 \rightarrow o = 2$
  - $x = 3 \wedge y = 2 \rightarrow o = 3$
- 通过和CEGIS结合可以求解任意规约

启发式搜索法

启发式搜索法

- 定义fitness函数
  - 通过的测试样例的数量
- 初始程序
  - 通常随机产生
- 定义变异操作（爬山法、模拟退火、遗传算法）
  - 随机将一颗子树替换成另一颗子树
- 定义交叉操作
  - 随机交换两个程序的两颗子树

参考资料

- Syntax-Guided Synthesis. R. Alur, R. Bodik, G. Juniwal, P. Madusudan, M. Martin, M. Raghothman, S. Seshia, R. Singh, A. Solar-Lezama, E. Torlak and A. Udupa. In 13th International Conference on Formal Methods in Computer-Aided Design, 2013.
- Sumit Gulwani, Oleksandr Polozov, Rishabh Singh: Program Synthesis. Foundations and Trends in Programming Languages 4(1-2): 1-119 (2017)