# 软件分析技术 2025 Lab2 介绍

助教：方屹，老师：熊英飞

PL Lab, Peking University

December 02, 2025

# Contents

Contents

# Lab2 内容

- 目标：在 Python 中编写一个 concolic testing 工具，并用来分析实际 Python 软件.
- 内容：
  - (分数占比 65%，可能微调)基础部分：
    1. 基于一个已经实现好的框架，实现对 int 和 string 类型的 concolic testing.
    2. 设计并实现对实际软件的 concolic testing.
  - (分数占比 35%，可能微调)扩充部分(后续可能添加新数据结构)：
    1. 实现对 linked list 的 concolic testing.
    2. 保证 concolic testing 过程中产生的 linked list 结构上是合法的.
- Deadline: 2025/12/23 23:59
- Lab2 来源：
  1. MIT6.566 lab3: https://css.csail.mit.edu/6.858/2024/labs/lab3.html
  2. 在基础部分增加了一个任务
  3. 添加了扩充部分
- Hint: vibe coding 可以完成大部分任务.

# 评分标准

助教提供测试脚本，按照通过测试点的个数给分.

# 任务一: 完成 int/string 类型的 concolic testing

问题 Python 是没有静态类型的，那么转约束的时候，如何确定 smtlib 里面变量是什么类型呢？

- 答案: 使用 concolic testing，这样就可以获取动态类型信息，从而确定 smtlib 变量类型.
  1. 利用子类继承，将 if condition 中的布尔表达式插桩成符号执行的转移函数
  2. 对于无法插桩的函数，比如 sql 调用(在 C++中实现)，定义一个新函数，在实现原本函数功能的同时进行符号执行，用新函数替换原本的函数。
     - 例如，将 sql 数据库的 get 操作替换为，取出所有数据行，与待查找键值逐一比较

# 任务二: 使用 concolic testing 发现 bug

- 思路: 构造函数, 并在函数中加入 assertion, 使得对该函数进行 concolic testing 时, 能够触发 assertion 失败, 从而发现 bug.
- 要求:
  1. 完成 MIT6.566 lab3 中给出的检查任务.
  2. 设计并实现一个新的检查.

  要求提交代码时同时提交一个 pdf 文件, 说明检查的是什么性质, 检查是怎么做的

# 任务三:完成 linked list 类型的 concolic testing

- MIT6.566 lab3 中只要求实现对 int 和 string 类型的 concolic testing.
- 本任务要求实现对 object 的 concolic testing，在 Lab 中使用 singly linked list.
- 方法可以参考课上讲的内容.

# 任务四:保证 linked list 结构合法性

- 在 concolic testing 过程中，可能会产生不合法的 linked list 结构，比如有环，或者不同的 linked list 对象之间有共享节点.
- 预先定义的 `SafeSinglyLinkedList` 类，保证了不会有环、不同的 `SafeSinglyLinkedList` 对象之间不会有共享节点.
- 要求：在实现 concolic testing 时，保证产生的 list 结构合法、能够遍历所有可能分支 (在 list 结构合法的情况下).
- 可以考虑实现 Efficient Synthesis of Method Call Sequences for Test Generation and Bounded Verification. ASE'22 论文中的方法.

感谢倾听