南京大學
NANJING UNIVERSITY

自动化测试综述命题

程序分析方向

选题背景

南京大学 NANJING UNIVERSITY

- **程序分析（Program Analysis）**
  - 程序分析指的是，对计算机程序进行**自动化**的处理，以确认或发现其特性，比如性能、正确性、安全性等
  - 测试的目标在于验证待测程序是否满足预期的属性，程序分析是自动化测试的重要途径
  - 更关注程序分析类的技术在研究中的应用；关注白盒测试
- 分类
  - 按照是否需要运行程序：静态分析、动态分析
  - 按照具体的算法和技术：符号执行、数据流分析、指针分析、程序转换、代码优化、程序切片、依赖分析...

作业要求

南京大学 NANJING UNIVERSITY

- 相关文献整理
  - 收集近十年的相关文献（越新越好），除PPT中给出示例文章外总数**不得少于10篇**
  - 特别经典的文章也可以参考，数量控制在3篇之内
  - 整理成一份**Excel表格**（格式见作业附件）和一篇**文献综述**
  - 文献综述的相关要求，以及作业提交时间、提交方式等要求与总体要求保持一致；Excel与综述打包提交，命名与文献保持一致
  - 文献来源参考
    - CCF-A类：ISSTA 、ASE、ICSE、FSE、PLDI、 OOPSLA 、TSE、TOSEM
    - CCF-B类：ISSRE、 STVR 、 IST
    - CCF-C类：ICST

选题一

南京大学 NANJING UNIVERSITY

- **PA for AI**
  - 迁移或利用程序分析的技术或概念来理解、引导或验证人工智能相关软件
  - AI模型缺少可解释性和确定性，但仍然具备程序的特质
- 文献举例
  - Dynamic Slicing for Deep Neural Networks [ISSTA 21]
  - NEUROSPF: A Tool for the Symbolic Analysis of Neural Networks [ICSE 21 Companion]
  - Symbolic Execution for Importance Analysis and Adversarial Generation in Neural Networks [ISSRE 19]

选题二

南京大学 NANJING UNIVERSITY

- **Test Generation/Augmentation/Regeneration**
  - 按照一定的策略自动地为待测程序生成测试数据，或是扩增现有测试数据
  - 两类基本方法：基于搜索的测试生成（SBST）和基于启发式方法的测试生成（Meta-heuristic Based Test Generation）
- 文献举例
  - EvoSuite: Automatic Test Suite Generation for Object-Oriented Software [FSE 11 Demo]
  - Continuous Test Generation: Enhancing Continuous Integration with Automated Test Generation [ASE 14]
  - Test Data Regeneration Generating New Test Data from Existing Data [STVR 12]

选题三

南京大学 NANJING UNIVERSITY

- **Oracle Problem**
  - 测试预言（Test Oracle）：在经历了一系列操作之后程序的预期行为
  - 自动化地生成、选择测试预言，以及验证测试预言的正确性
- 文献举例
  - Supporting oracle construction via static analysis [ISSTA 16]
  - Mutation-driven Generation of Unit Tests and Oracles [ISSTA 10]
  - CrowdOracles: Can the Crowd Solve the Oracle Problem? [ICSE 13]

选题四

南京大学 NANJING UNIVERSITY

- **Program Slicing and Its Application**
  - 切片准则 $C = < i, V >$：以一条语句i为基准，获取目标程序中与i相关的所有语句
  - 切片的目的：约减目标代码、分离耦合逻辑、优化整体流程
  - 各种程序切片技术，以及应用程序切片的概念或工具的测试优化技术
- 文献举例
  - Log-based test slicing [ISSTA 21]
  - Test Case Purification for Improving Fault Localization [FSE 14]
  - Dynamic Slicing for Deep Neural Networks [FSE 20]

联系方式

南京大学 NANJING UNIVERSITY

程序分析方向助教联系方式

钱瑞祥　　qrx@smail.nju.edu.cn