



# 综述大作业

南京大学 软件学院 iSE实验室



# 目录

01. 作业概述

02. 综述选题

03. 联系方式



01

作业要求



## 软工研究四维



Presenting



Writing



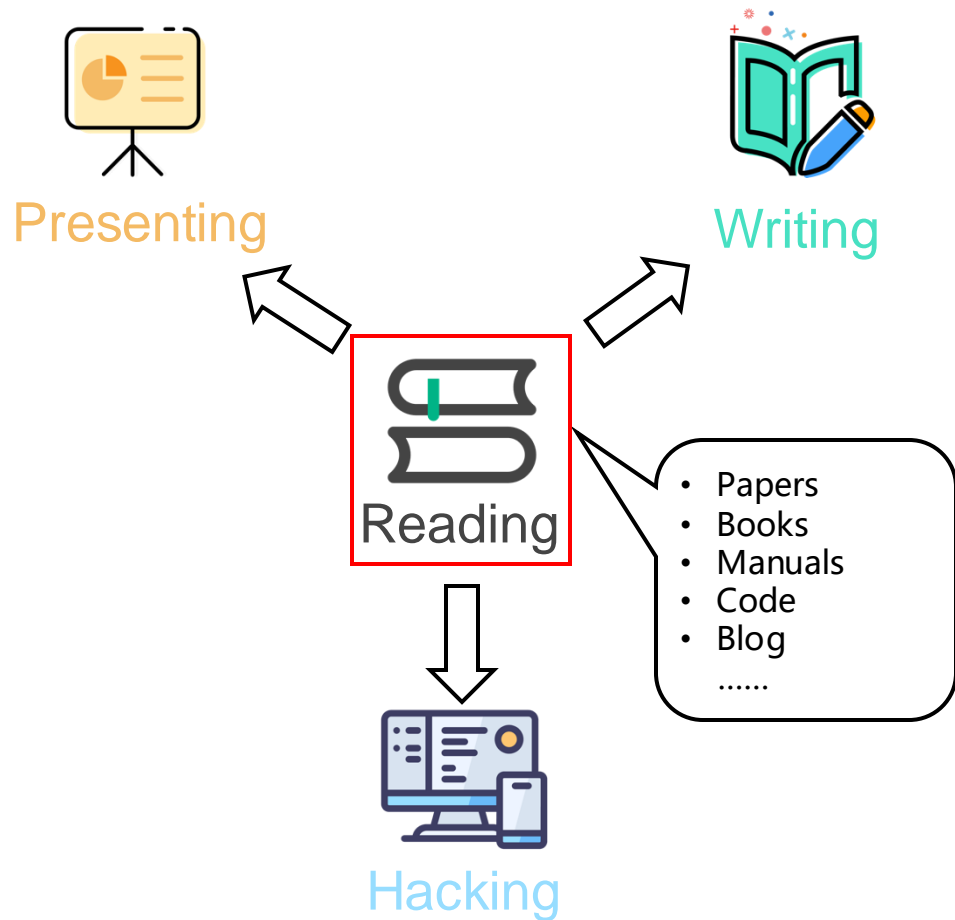
Reading



Hacking



## 软工研究四维





## 作业概述



- 小组作业：每组不超过4人
- 作业组成：综述作业 + 代码作业
- 作业方向：经典测试技术、智能软件测试、图形界面测试
- 分数组成：20%综述 + 30%工具 + 5%课堂汇报
- 选题方式：问卷收集
- 提交方式：
  - 综述：Moodle上提交PDF、文献分类Excel、LaTeX源代码.zip
  - 代码：提交开源仓库链接（Github、GitLink<sup>1</sup>等），**先私有**后公开

[1] <https://www.gitlink.org.cn/>



## 作业概述



- 时间节点 (DDLs, 都是当日的23:59)
  - 组队 (10月21日, DDL)
  - 作业选题 (10月28日, DDL)
  - 综述提交 (暂定11月25日, DDL)
  - 代码提交 (暂定12月9日, DDL)
  - 课堂汇报
    - 10月28日报名开始, 学期结束前可持续报名
    - 最早11月4日开始汇报, 发送邮件到qrx\_at@163.com报名



## 作业概述



- 课堂汇报

- 10月28日报名开始，学期结束前可持续报名
- 报名方式：发送邮件给助教
  - 最早11月4日开始汇报，提前发送邮件到qrx\_at@163.com报名
  - 邮件标题：课堂汇报-<组号>-<组长学号姓名>
  - 邮件内容：<汇报类型（综述|代码）>，<综述|代码选题方向>
  - 汇报时间：每组15分钟
  - 汇报顺序：由助教按照邮件发送的时间顺序安排
    - 每次上课的前一天发布下次上课报告顺序和内容





## 作业附件



### 附件

#### 附件-计算机学报模板

- 计算机学报例文-跨项目软件缺陷预测方法研究综述.pdf
- 计算机学报例文-任务型对话系统研究综述.pdf
- 计算机学报例文-一种执行轨迹驱动的移动应用功能分类方法.pdf
- 计算机学报例文-SiamCross-孪生交叉的目标跟踪对象感知网络.pdf
- 计算机学报 LaTeX 模板 Chinese Journal of Computer Template.zip

附件-评分细则-代码作业-PA+AI

如何得分!

附件-评分细则-文献综述

附件-拓展阅读-2024-CCS-Prompt\_Fuzzing\_for\_Driver\_Generation.pdf

附件-拓展阅读-2024-ISSTA-Exploring Large Language Model Based Fuzz Driver Generation.pdf

附件-拓展阅读-latex学习资料.zip

汲取力量，更好地完成作业

附件-拓展阅读-science\_writing\_for\_non-native\_english\_speakers.pdf

附件-中国计算机学会推荐国际学术会议和期刊目录- 2022.pdf

附件-综述文献表格模板.xlsx

选题描述-经典测试技术方向-变异测试&模糊测试

选题描述-经典测试技术方向-源码警告识别.pdf

选题描述-图形界面测试方向-工具选题.pdf

选题描述-图形界面测试方向-综述选题.pdf

选题描述-智能软件测试方向.pdf

不同选题的具体要求



02

综述选题



## 综述作业总体要求



- 题目选择：每组一个
- 文献来源：CCF-**A,B**,C类会议与期刊<sup>1</sup>
- 文献年限：时间近5~10年，越新越好
- 文献数量：每组30~40篇**初级研究** (Primary Study)
- 模板要求：计算机学报模板（英文摘要写，切忌机翻）
- 页数要求：10页正文+4页参考文献（上限），不超过14页
- 编写工具：Overleaf<sup>2</sup>、NJU Latex<sup>3</sup>、本机搭建Tex环境

[1] 中国计算机学会推荐国际学术会议和期刊目录（第五版），2022年修订， <https://ccf.atom.im/>

[2] <https://www.overleaf.com/>

[3] <https://tex.nju.edu.cn/>



## CCF推荐列表-会议

### 中国计算机学会推荐国际学术会议

(软件工程/系统软件/程序设计语言)

#### 一、A类

序号	会议简称	会议全称	出版社	网址
1	PLDI	ACM SIGPLAN Conference on Programming Language Design and Implementation	ACM	<a href="http://dblp.uni-trier.de/db/conf/pldi/">http://dblp.uni-trier.de/db/conf/pldi/</a>
2	POPL	ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages	ACM	<a href="http://dblp.uni-trier.de/db/conf/popl/">http://dblp.uni-trier.de/db/conf/popl/</a>
3	FSE/ESEC	ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering	ACM	<a href="http://dblp.uni-trier.de/db/conf/sigsoft/">http://dblp.uni-trier.de/db/conf/sigsoft/</a>
4	SOSP	ACM Symposium on Operating Systems Principles	ACM	<a href="http://dblp.uni-trier.de/db/conf/sosp/">http://dblp.uni-trier.de/db/conf/sosp/</a>
5	OOPSLA	Conference on Object-Oriented Programming Systems, Languages, and Applications	ACM	<a href="http://dblp.uni-trier.de/db/conf/oopsla/">http://dblp.uni-trier.de/db/conf/oopsla/</a>
6	ASE	International Conference on Automated Software Engineering	IEEE/ACM	<a href="http://dblp.uni-trier.de/db/conf/kbse/">http://dblp.uni-trier.de/db/conf/kbse/</a>
7	ICSE	International Conference on Software Engineering	ACM/IEEE	<a href="http://dblp.uni-trier.de/db/conf/icse/">http://dblp.uni-trier.de/db/conf/icse/</a>
8	ISSTA	International Symposium on Software Testing and Analysis	ACM	<a href="http://dblp.uni-trier.de/db/conf/issta/">http://dblp.uni-trier.de/db/conf/issta/</a>
9	OSDI	USENIX Symposium on Operating Systems Design and Implementation	USENIX	<a href="http://dblp.uni-trier.de/db/conf/osdi/">http://dblp.uni-trier.de/db/conf/osdi/</a>
10	FM	International Symposium on Formal Methods	FME	<a href="http://dblp.uni-trier.de/db/conf/fm/">http://dblp.uni-trier.de/db/conf/fm/</a>



## CCF推荐列表-会议



### 中国计算机学会推荐国际学术会议

(网络与信息安全)

#### 一、A类

序号	会议简称	会议全称	出版社	网址
1	CCS	ACM Conference on Computer and Communications Security	ACM	<a href="http://dblp.uni-trier.de/db/conf/ccs/">http://dblp.uni-trier.de/db/conf/ccs/</a>
2	EUROCRYPT	International Conference on the Theory and Applications of Cryptographic Techniques	Springer	<a href="http://dblp.uni-trier.de/db/conf/eurocrypt/">http://dblp.uni-trier.de/db/conf/eurocrypt/</a>
3	S&P	IEEE Symposium on Security and Privacy	IEEE	<a href="http://dblp.uni-trier.de/db/conf/sp/">http://dblp.uni-trier.de/db/conf/sp/</a>
4	CRYPTO	International Cryptology Conference	Springer	<a href="http://dblp.uni-trier.de/db/conf/crypto/">http://dblp.uni-trier.de/db/conf/crypto/</a>
5	USENIX Security	USENIX Security Symposium	USENIX Association	<a href="http://dblp.uni-trier.de/db/conf/uss/">http://dblp.uni-trier.de/db/conf/uss/</a>
6	NDSS	Network and Distributed System Security Symposium	ISOC	<a href="http://dblp.uni-trier.de/db/conf/ndss/">http://dblp.uni-trier.de/db/conf/ndss/</a>



## CCF推荐列表-期刊

### 中国计算机学会推荐国际学术期刊

(软件工程/系统软件/程序设计语言)

#### 一、A类

序号	刊物简称	刊物全称	出版社	网址
1	TOPLAS	ACM Transactions on Programming Languages and Systems	ACM	<a href="http://dblp.uni-trier.de/db/journals/toplas/">http://dblp.uni-trier.de/db/journals/toplas/</a>
2	TOSEM	ACM Transactions on Software Engineering and Methodology	ACM	<a href="http://dblp.uni-trier.de/db/journals/tosem/">http://dblp.uni-trier.de/db/journals/tosem/</a>
3	TSE	IEEE Transactions on Software Engineering	IEEE	<a href="http://dblp.uni-trier.de/db/journals/tse/">http://dblp.uni-trier.de/db/journals/tse/</a>
4	TSC	IEEE Transactions on Services Computing	IEEE	<a href="http://dblp.uni-trier.de/db/journals/tsc/">http://dblp.uni-trier.de/db/journals/tsc/</a>

(网络与信息安全)

#### 一、A类

序号	刊物简称	刊物全称	出版社	网址
1	TDSC	IEEE Transactions on Dependable and Secure Computing	IEEE	<a href="http://dblp.uni-trier.de/db/journals/tdsc/">http://dblp.uni-trier.de/db/journals/tdsc/</a>
2	TIFS	IEEE Transactions on Information Forensics and Security	IEEE	<a href="http://dblp.uni-trier.de/db/journals/tifs/">http://dblp.uni-trier.de/db/journals/tifs/</a>
3		Journal of Cryptology	Springer	<a href="http://dblp.uni-trier.de/db/journals/joc/">http://dblp.uni-trier.de/db/journals/joc/</a>



- 变异测试选题
  - 推荐期刊&会议
    - 软件工程领域的顶级期刊和会议
    - 期刊：TSE, TOSEM, IST, JSS, ESE
    - 会议：ISSTA, FSE/ESEC, ASE, ICSE, ISSRE, ICST



- 变异测试选题
  - 变异测试优化技术综述
    - 变异体的选择、约简、执行、分析
  - 变异测试应用综述
    - 优化回归测试、引导测试生成、AI测试
  - 变异技术综述
    - 变异测试中的、模糊测试中的变异、基于搜索的软件测试 (Evosuite) 中的变异、随机测试中的变异
    - DL框架测试中的变异、内核测试的变异、协议测试中的变异



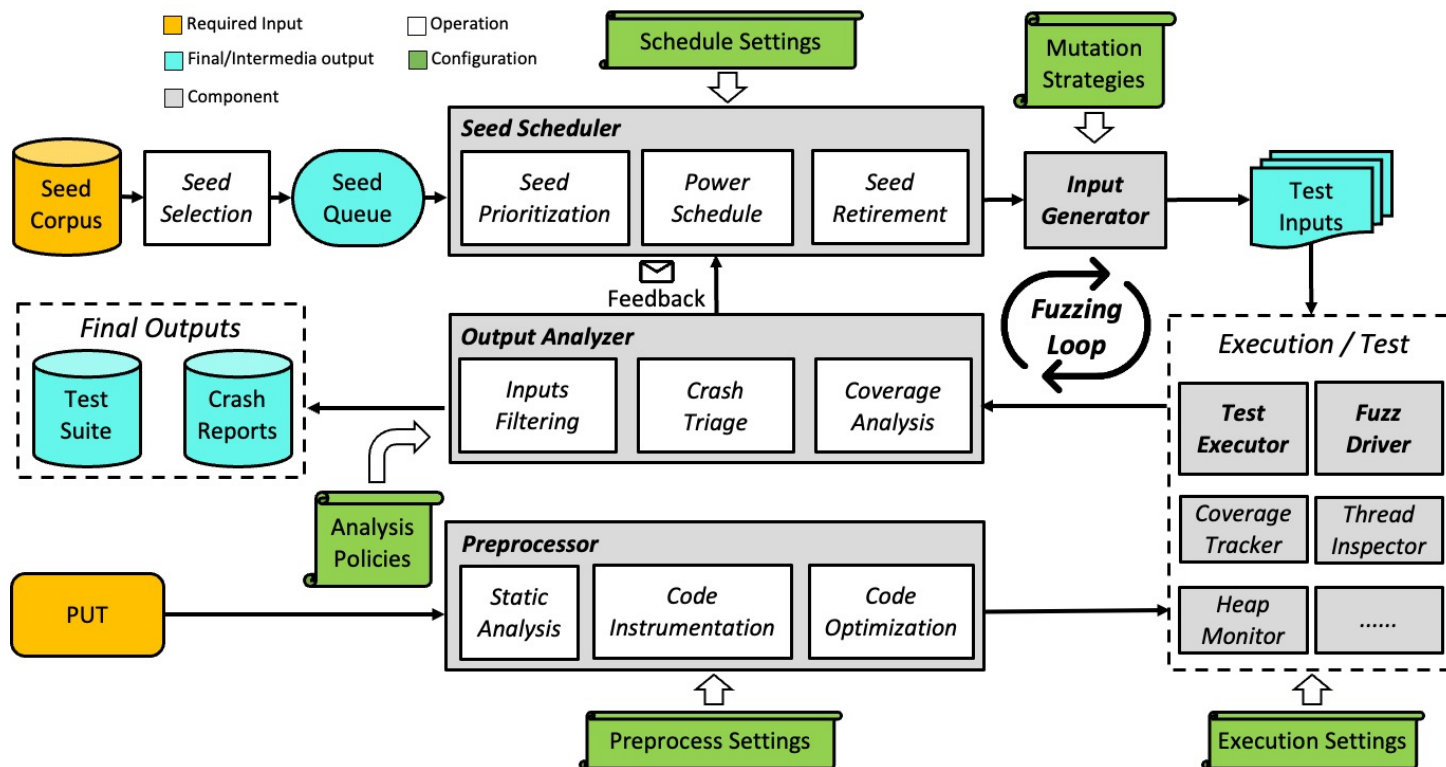


- 模糊测试选题
  - 推荐期刊&会议
    - 软件工程&安全领域的顶级期刊和会议
    - 期刊：TSE, TOSEM, TDSC
    - 会议：ISSTA, FSE/ESEC, ASE, ICSE, PLDI, Usenix Security, CCS, S&P, NDSS



- 模糊测试选题
  - 模糊测试技术中[特定环节]技术综述
    - 种子调度、测试生成、种子选择 -- 参考课上的框架图
  - 定向模糊测试技术综述
    - 白盒、灰盒、调度方式、程序分析技术
  - [变异式|生成式]模糊测试技术综述
  - [垂直领域]模糊测试技术综述
    - 垂直领域：某一类测试对象
    - 内核模糊测试、嵌入式系统模糊测试、协议模糊测试.....

## • 模糊测试选题






- 源码警告选题

- 基于大模型的源码警告识别综述

- 什么是源码警告?

- 源码警告 (Source Code Warning) 是指在编译或解释源码时, 编译器或解释器检测到代码中的潜在问题或不规范行为, 但并不严重到有可能阻止程序的正常编译或执行。这些警告通常提醒开发者代码中可能存在的问题, 如潜在的错误、性能问题、可移植性问题或安全隐患 ——  ChatGPT + 助教验证



- 源码警告选题
  - 基于大模型的源码警告识别综述
  - 亿些关键词

序号	目的	关键字
1	大模型	1) large language model, 2) LLM, 3) pre-trained model
2	后处理警告操作	1) elimination, 2) reduction, 3) simplification, 4) ranking, 5) classification, 6) reviewing, 7) inspection, 8) detection
3	静态分析	1) static analysis, 2) automated code analysis, 3) source code analysis, 4) automated defects detection, 5) false
4	警告	1) alarm, 2) warning, 3) alert, 4) violations

- 研究框架

- 从智能模型模糊测试的角度着手，按照不同的阶段，分别关注**测试数据的选择、生成以及测试结果的评估**





- 综述题目

- 方向一：深度学习模型测试数据选择技术综述
  - 关键词：测试数据选择、测试数据排序、测试数据度量
- 方向二：深度学习模型测试数据生成技术综述
  - 关键词：数据变异、蜕变关系、数据扩增
- 方向三：深度学习模型测试结果评估技术综述
  - 关键词：鲁棒性、公平性、后门检测、可解释性分析

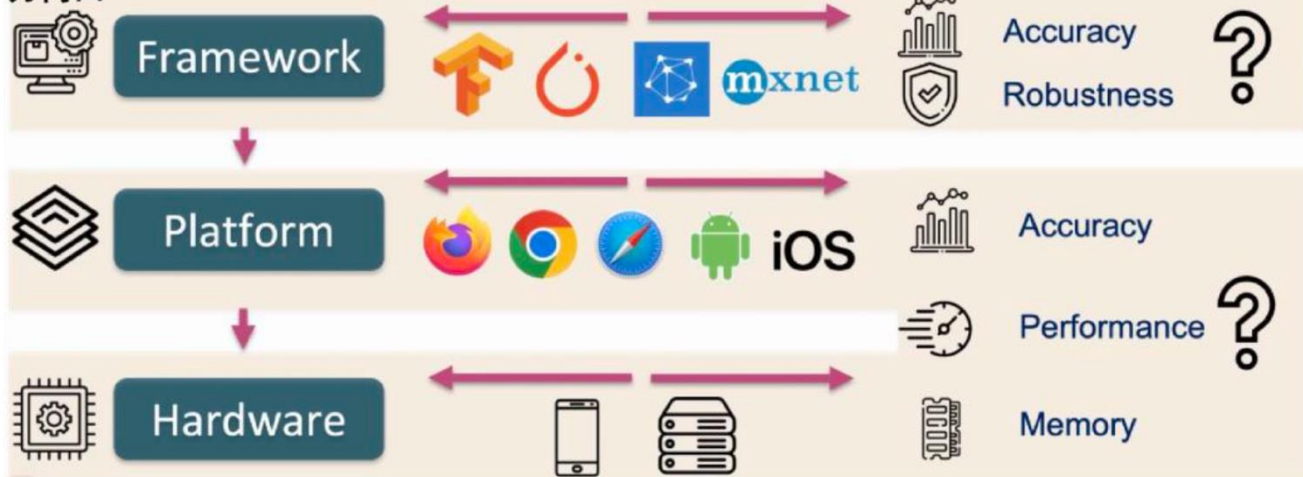


## • 综述题目

### • 方向四：深度学习框架缺陷检测和原因分析技术综述

- 关键词：深度学习框架/库测试、深度学习框架/库实证研究

方向四







- 综述题目

- 大模型引导的场景感知GUI自动化测试生成技术

- 现有GUI测试技术难以理解用户操作场景，难以模拟真实用户行为
    - LLM具备强大的理解和生成能力，拥有生成更正式测试用例的潜力

- 大模型引导的场景感知GUI测试脚本录制回放技术

- 录制回放：记录用户操作、生成测试脚本
    - 传统的录制回放技术面临跨平台和跨应用的难题
    - LLM具备强大推理能力，具有感知不同场景、引导录制回放的潜力



- 经典测试技术方向 - 变异测试&模糊测试
  - 变异测试优化技术综述
  - 变异测试应用综述
  - 变异技术综述
  - 模糊测试技术中[特定环节]技术综述
  - 定向模糊测试技术综述
  - [变异式|生成式]模糊测试技术综述
  - [垂直领域]模糊测试技术综述



- 经典测试技术方向 - 源码警告识别

- 基于大模型的源码警告识别综述

序号	目的	关键字
1	大模型	1) large language model, 2) LLM, 3) pre-trained model
2	后处理警告操作	1) elimination, 2) reduction, 3) simplification, 4) ranking, 5) classification, 6) reviewing, 7) inspection, 8) detection
3	静态分析	1) static analysis, 2) automated code analysis, 3) source code analysis, 4) automated defects detection, 5) false
4	警告	1) alarm, 2) warning, 3) alert, 4) violations



- 智能软件测试方向
  - 深度学习模型测试数据选择技术综述
  - 深度学习模型测试数据生成技术综述
  - 深度学习模型测试结果评估技术综述
  - 深度学习框架缺陷检测和原因分析技术综述



- 图形界面测试方向
  - 大模型引导的场景感知GUI自动化测试生成技术
    - <https://ieeexplore.ieee.org/document/10557505>
    - <https://dl.acm.org/doi/abs/10.1145/3597503.3639180>
    - <https://dl.acm.org/doi/abs/10.1145/3597503.3639118>
  - 大模型引导的场景感知GUI测试脚本录制回放技术
    - <https://dl.acm.org/doi/abs/10.1145/3650212.3680327>
    - <https://dl.acm.org/doi/abs/10.1145/3597503.3623322>
    - <https://arxiv.org/abs/2409.05028>



03

联系方式



## 联系方式



- 经典测试技术方向
  - 钱瑞祥, qrx\_at@163.com
  - 葛修婷, 1683245057@qq.com
- 智能软件测试方向
  - 刘佳玮, jw.liu@smail.nju.edu.cn
- 图形界面测试方向
  - 虞圣呈, yusc@smail.nju.edu.cn
  - 凌毓辰, yuchenling@smail.nju.edu.cn

养成先想再问的习惯!



[zychen@nju.edu.cn](mailto:zychen@nju.edu.cn)  
[fangchunrong@nju.edu.cn](mailto:fangchunrong@nju.edu.cn)

Thank you!