

软件理论基础与实践

熊英飞 胡振江
信息学院计算机系
2021年3月12日



授课教师



熊英飞长聘副教授



熊英飞

理科1号楼143室

职称：长聘副教授

研究所：软件研究所

研究领域：软件工程、程序设计语言

办公电话：86-10-62757008

电子邮件：xiongyf@pku.edu.cn

个人主页：<http://sei.pku.edu.cn/~xiongyf04/>

致力于程序分析、综合和修复方法研究。针对软件自动化修复中的规约不精确问题，提出了修改策略编程语言、基于统计和逻辑推理的程序综合框架、交互式程序综合等应用基础技术，将程序修复正确率从不到40%提升到了80%以上，显著推进了修复技术的实用化进程，同时也被应用到编译器测试、变异测试、代码搜索、API演化，代码编辑等多个不同的问题上。针对浮点误差、内存泄漏等安全攸关软件常见缺陷提出检测和修复算法。领导开发的修复工具ACS和SimFix被认为是Java上综合表现最好的修复工具，在多篇第三方论文不同场景的验证中都表现最优。成果被应用于Linux内核配置、UWE网络应用开发工具等开源软件项目，华为、因特睿、武汉元光等企业，覆盖中国、瑞典、西班牙等多个国家。



胡振江讲席教授



胡振江

理科1号楼1247室

职称：教授

研究所：软件研究所

研究领域：程序设计语言，函数式语言，软件工程，程序演算

办公电话：86-10-62757974

电子邮件：huzj@pku.edu.cn

个人主页：<http://sei.pku.edu.cn/~hu>

欧洲科学院院士、日本工学院院长，ACM杰出科学家、IEEE Fellow

谢睿峰助教



- 助教：谢睿峰
- 电子邮件：xrf@pku.edu.cn
- 课程微信群：



- 课程网页：<https://xiongyingfei.github.io/SF>

课程目的和教学内容

可信软件

- 开发可信软件难!
 - 规模大，复杂度高，人员多



- 项目开发方法
 - e.g., extreme programming
- 设计原理与方法
 - e.g., model-view-controller
- 程序语言
 - e.g., OOP, FP
- 数理技术
 - e.g., 程序推理与验证

数理技术

- 程序推理逻辑
 - 数理逻辑
 - 程序性质的有效推论和证明的原则与标准
- 证明系统
 - 构造严格的逻辑证明
 - 自动证明系统: SAT, SMT, Model-Checker
 - 证明辅助系统: **Coq**, Agda, Isabelle
- 函数式程序设计
 - 宣言式程序设计和程序推理
 - 程序设计与逻辑的桥梁

程序逻辑：程序设计语言理论

- 程序验证：针对某个程序
 - 程序表示：抽象文法
 - 操作语义：大步语义，小步语义
 - 程序推理：
 - 程序语义相等
 - 霍尔程序逻辑：程序满足某个规范 (specification)
- 类型系统：针对某个语言的所有程序
 - 轻量级形式化方法（程序分析）
 - 正确性证明

课程目的

- 通过讲授定理证明器Coq和在Coq基础上构建的软件基础理论，使学生能够
 - 掌握可信软件的基础理论
 - 函数式程序设计
 - 数理逻辑
 - 形式语义
 - 程序验证
 - 类型系统
 - 掌握软件的形式化描述和推理方法
 - 通过动手实践加深对“构造性”理论的理解

教学内容

- Coq基础(函数式编程)
- 基于Coq构造数理逻辑
- 基于Coq表示和证明程序性质
- 基于Coq构造无类型编程语言
- 基于Coq构造类型系统



Thierry Coquand

主要教材



<https://www.seas.upenn.edu/~cis500/current/sf/index.html>

程序语言实验室开设的软件基础课程

本科

- 计算概论A（函数式程序设计）：胡振江/张伟
- 编程设计语言原理：赵海燕/熊英飞/胡振江
- 程序分析：熊英飞

研究生

- 软件理论基础与实践：熊英飞/胡振江/
- 编程设计语言原理：赵海燕/熊英飞/胡振江
- 概率编程：张昕

评分标准



评分标准

- 平时：30分
- 期中：30分
- 期末：40分

关于作业：

- 平时作业独立完成
- 如果和同学讨论后做出来的需在提交时说明
- 平时作业周二上课前提交

关于中期和期末考试：

- 形式未定

作业（无需提交）

- 下载教科书及相关Coq代码
<https://softwarefoundations.cis.upenn.edu>
- 安装Coq系统
 - Proof General
 - CoqIDE<https://coq.inria.fr/download>