软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*, 2022,33(6):2113−2114 [doi: 10.13328/j.cnki.jos.006582]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

# 定理证明理论与应用专题前言*

曹钦翔[1], 詹博华[2], 赵永望[3]

[1](上海交通大学 电子信息与电气工程学院, 上海 200240)

[2](中国科学院 软件研究所, 北京 100190)

[3](浙江大学 计算机科学与技术学院, 浙江 杭州 310027)

通信作者: 赵永望, E-mail: zhaoyw@zju.edu.cn

中文引用格式: 曹钦翔, 詹博华, 赵永望. 定理证明理论与应用专题前言. 软件学报, 2022, 33(6): 2113–2114. http://www.jos.org.cn/1000-9825/6582.htm

随着计算机系统在工业和生活中越来越广泛的应用, 软件和硬件的可靠性受到越来越多的关注. 定理证明方法将程序和系统的正确性表达为数学命题, 然后使用逻辑推导的方式证明正确性. 不同于基于程序测试的技术, 定理证明方法能保证覆盖所有边缘情况, 完全排除一些特定类型的错误. 而基于逻辑推导的交互式定理证明技术还能不受系统状态空间大小和复杂性的限制, 验证非常复杂的系统和性质. 因此, 定理证明技术不仅是形式化方法领域, 也是众多其他应用领域国内外学者的关注焦点和研究新热点. 近年来, 定理证明已经逐步用于越来越多的软件、硬件系统验证, 这一方面为软硬件系统的安全性保障提供了新的有力工具, 另一方面也成为定理证明技术发展的有利契机. 目前, 定理证明的规模化问题、定理证明工具本身的底层逻辑理论问题、适应于定理证明方案的程序验证理论问题等变得越来越重要, 对于数学分析、离散数学、概率等基础定理证明库或求解方案的需求也越来越迫切.

本专题公开征文, 共收到投稿 10 篇. 论文均通过了形式审查, 内容涉及定理证明的理论与应用. 特约编辑先后邀请了 20 多位专家参与审稿工作, 每篇投稿都邀请了 2–3 位专家进行评审. 稿件经初审、复审、ChinaSoft 2021 会议宣读和终审 4 个阶段, 历时 6 个月, 最终有 9 篇论文入选本专题, 文章主题涵盖了程序验证逻辑、形式化数学、编译器和操作系统验证的应用等多个方面.

《机械化验证一个高效的迭代数据流求解算法》利用 Isabelle/HOL 验证了迭代求解严格支配结点的 CHK 算法的正确性与完备性. 该算法是编译器优化分析中数据流分析的常用方法.

《步进索引模型下的语义及其形式化》研究了两种步进索引模型下的语义以及它们之间的关系, 并且利用 Coq 定理证明器形式化了这些理论结果.

《多旋翼飞控推进子系统的 Coq 形式化验证》将飞控领域的领域知识整理为具有层次结构、适合进行形式验证的文档, 并利用 Coq 定理证明器对一些飞控程序中使用到的函数的功能进行了形式化, 验证了其功能正确性. 在此基础上该文还利用 Coq 定理证明器自带的功能抽取出了可以执行的 OCaml 代码.

《支持索引式的 PPTL 定理证明器的实现》利用 Coq 定理证明器对索引式 PPPL 逻辑的语法和推理系统进行了形式化.

《基于精化的可信执行环境内存隔离机制验证》使用 Isabelle/HOL 形式化了 TEE 内存隔离机制的关键硬件和软件, 包括 TrustZone 地址空间控制器、MMU 和 TrustZone monitor 等. 作者验证了这些组件满足无干扰、无泄露、无影响等信息流安全属性.

《基于 Coq 的杨忠道定理形式化证明》在 Coq 中以 Morse-Kelley 集合论公理体系为基础, 将杨忠道定理的证明进行了形式化.

* 收稿时间: 2022-02-16

《基于 Coq 的矩阵代码生成技术》以矩阵运算在 Coq 中的形式化为基础，在 Coq 中实现了由高级矩阵算子到 C 代码的矩阵运算代码生成，能够将函数式的矩阵运算代码转换为高效的命令式代码.

《机器人碰撞检测方法形式化》提出用胶囊体来抽象地描述机器人的各个部件的几何形状，并在 HOL-light 定理证明器中形式化了球体、胶囊体等三维几何图形之间的碰撞条件判定公式. 以此为基础，作者验证了一些碰撞问题的复杂判定公式的正确性.

《一种基于分离逻辑的块云存储系统验证工具》在 Coq 中形式化了一个块云存储系统的伪代码，并在 Coq 中开发了一种可以用于验证相关代码的分离逻辑验证工具，文章中也展示了一些使用该验证工具验证简单云存储系统模型的实例.

本专题主要面向形式化方法、定理证明、程序验证、系统软件等多领域的研究人员和工程人员，反映了我国学者在定理证明领域最新的研究进展. 感谢《软件学报》编委会和形式化方法专委会对专题工作的指导和帮助，感谢专题全体评审专家及时、耐心、细致的评审工作，感谢踊跃投稿的所有作者. 希望本专题能够对定理证明理论与应用方面的研究工作有所促进.

**曹钦翔**(1990－)，男，博士，上海交通大学副教授，博士生导师，CCF 专业会员，形式化专委会执行委员. 长期从事基于定理证明的程序验证与程序逻辑研究，参与开发了 VST (Verified Software Toolchain)验证工具，并参与撰写了 Coq 定理证明知名教材《Software Foundations》的第 5 卷.

**詹博华**(1989－)，男，博士，中国科学院软件研究所副研究员，CCF 专业会员，形式化专委会执行委员. 主要研究方向是交互式定理证明，关注证明自动化方法和工具设计，以及嵌入式系统的建模和验证. 在 Isabelle 定理证明器中开发了 auto2 证明自动化工具，应用于基于集合论的形式化数学和基于分离逻辑的程序验证. 此外，参与开发了量子程序验证工具 QHLProver. 目前正在开发 HolPy 交互式定理证明器.

**赵永望**(1979－)，男，博士，浙江大学教授，博士生导师，移动终端安全浙江省工程实验室主任，工信部重大专项首席科学家，CCF 杰出会员. 担任 ARINC 653 国际操作系统标准委员会委员、CCF 系统软件专委会和形式化方法专委会执行委员、国际标准化组织 ISO/IEC JTC1 SOA 研究组组长等. 主要研究方向包括形式逻辑与验证、操作系统安全、编程语言原理等.主持和参与国家自然基金重点项目、工信部重大专项、载人航天工程重点项目等 20 余项，2011 年和 2017 年分别获得中国电子学会和山东省科技进步一等奖.