

形式化方法与应用专题前言^{*}

安杰¹, 顾斌², 李建文³

¹(天基综合信息系统全国重点实验室(中国科学院软件研究所), 北京 100190)

²(北京控制工程研究所, 北京 100190)

³(华东师范大学软件工程学院, 上海 200062)

通信作者: 安杰, E-mail: anjie@iscas.ac.cn; 顾斌, E-mail: gubin@ios.ac.cn; 李建文, E-mail: jwli@sei.ecnu.edu.cn



中文引用格式: 安杰, 顾斌, 李建文. 形式化方法与应用专题前言. 软件学报, 2026, 37(9): 3405–3406. <http://www.jos.org.cn/1000-9825/7610.htm>

形式化方法以严格的数学方法为基础来规约、设计、构建、验证、演进计算系统, 是改善和确保系统质量的重要方法, 其模型、技术和工具已成为计算思维的重要载体. 形式化方法已成功应用于各种硬件的设计, 在处理软件开发复杂性和提高软件可靠性方面已显示出强大的能力, 在新兴领域, 形式化方法也逐步应用适配. 最近, 形式化方法与生成式人工智能的交叉结合也受到广泛关注. 本专题围绕形式化方法基础理论、技术、支撑工具及领域应用, 重点关注形式化方法与理论计算机科学、编程语言、软件工程、基础软件、实时嵌入式系统、人机物融合系统、网络与信息安全、可信人工智能、生成式人工智能等领域的交叉结合, 反映形式化方法领域的最新研究成果, 深入拓展形式化方法与相关领域的交叉, 为研究人员和工业界提供优质参考, 促进形式化方法、技术和工具在国内的应用和发展.

本专题采取公开征文的方式, 共收到投稿 25 篇. 论文通过形式审查后, 特约编辑先后邀请了 30 多位专家参与审稿工作, 每篇投稿邀请 2–3 位专家进行评审. 稿件经初审、复审、ChinaSoft 2025 中国软件大会“形式化方法与应用专题论坛”宣读和终审这 4 个阶段, 历时 6 个月, 最终有以下 9 篇论文入选本专题.

《[AWTaint: 面向 Web 应用漏洞检测的增量静态分析框架](#)》聚焦软件分析与漏洞检测领域, 面向 DevOps 场景下 Web 应用频繁迭代带来的静态漏洞检测低效问题, 提出一种高效、可落地的增量静态分析框架.

《[基于按需切片计算的并行化程序分析框架](#)》聚焦软件分析领域, 针对大规模软件分析中传统方法面临的“构图困难”与“冗余计算”性能瓶颈, 提出了一种基于高阶函数摘要机制按需切片计算的并行化程序分析框架.

《[数学分析机械化工 I: 一元微积分形式化系统](#)》聚焦数学形式化和机械化, 详细介绍了一项基于 Coq (现称为 Rocq) 的形式化系统. 该系统以华东师范大学编著的《数学分析》为蓝本, 在朴素集合论和初等数论及代数知识体系下开发, 对教材中的单变量微积分内容进行了严格形式化.

《[基于 Auto-active 与交互式集成的 L4 线程管理形式化验证](#)》聚焦操作系统微内核验证, 针对内核验证工作量大的问题, 提出了一个基于精化证明的半自动验证框架, 通过证明 L4 微内核的线程管理模块, 发现了若干违反正确性和安全性的问题并进行了修复, 表明了框架具有较好的验证能力.

《[混成精化逻辑](#)》聚焦混成系统领域, 研究了混成通信顺序进程, 提出了面向并发程序的并发混成精化逻辑和面向同步行为的同步混成精化逻辑, 通过对混成系统结构进行分解, 精化构造分层证明过程, 提升了证明模块化程度, 减轻了证明负担.

《[从设计到安全分析: 异构模型转换与交叉验证](#)》聚焦复杂安全攸关系统设计与验证领域, 针对模型驱动软件开发中的设计阶段和验证阶段的有效衔接面临的语义一致性不足、工具链互操作性受限、验证方法系统性薄弱等问题, 提出一种基于统一中间表示的建模与验证方法.

* 收稿时间: 2025-12-25; jos 在线出版时间: 2025-12-25

《模糊映射熵驱动的强化学习系统安全监控方法》聚焦系统运行时验证领域, 面向强化学习系统的安全性监控问题, 综合运用高斯混合模型聚类、模糊映射熵、模糊逻辑推理等理论和技术, 提出一种对深度强化学习策略进行在线安全监控和动作修正的方法.

《观察树驱动的确定性时间自动机主动学习》聚焦模型学习领域, 面向现有确定性时间自动机主动模型学习算法学习速度慢难以用于复杂系统的问题, 提出了一种名为时间观察树的数据结构存储学习过程中所获取的信息, 有效减少学习所需的查询数量, 从而优化了实际学习效率.

《基于大语言模型的 Python 到 Dafny 代码翻译》聚焦基于大语言模型的代码翻译领域, 面向 Python 到 Dafny 的大模型辅助代码翻译问题, 提出了一种结合提示词工程与动态修复方法的翻译框架和较为完善的测试驱动评估方法.

本专题主要面向形式化方法的研究人员和采用形式化方法开展系统设计与分析、软件开发与验证、工业应用的工程技术人员, 反映了我国学者在形式化方法与应用领域最新的研究进展. 感谢《软件学报》编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. 希望本专题能够对形式化方法与应用相关领域的研究工作有所促进.

作者简介

安杰, 博士, 中国科学院软件研究所副研究员, 博士生导师, 中国计算机学会形式化方法专业委员会委员, CCF 专业会员. 主持国家级青年人才项目、中国科学院“率先行动”引才计划项目 (择优). 主要研究领域为信息物理融合系统和形式化方法领域的基础研究, 以及与人工智能领域的交叉融合. 与合作者一起, 提出了信息物理融合系统的模型学习方法、信号时序逻辑的因果语义与运行时监控算法等, 相关成果在国家深空探测工程中得到应用. 在 CAV、FM、TACAS、HSCC、EMSOFT、TCAD 等形式化方法和嵌入式系统领域重要国际期刊和会议上发表论文 30 余篇, 曾获 FMAC 最佳论文、ATVA 杰出论文.

顾斌, 博士, 北京控制工程研究所研究员, 博士生导师, 中国计算机学会形式化方法专业委员会委员, CCF 高级会员. 长期从事空间飞行器控制系统和可信软件等方面的研究和研制工作. 主持和参与完成了国家自然科学基金重点项目、集成项目和重大项目等多项. 主要研究领域为计算机控制、可信软件、智能软件工程等.

李建文, 博士, 华东师范大学教授, 博士生导师, 中国计算机学会形式化方法专业委员会执行委员, CCF 专业会员. 入选上海市青年人才计划, 获得上海市浦江人才荣誉称号. 主持国家自然科学基金青年项目、重点项目子课题各一项. 主要研究领域为形式化自动验证技术, 可用于保障计算机软硬件系统的正确性和安全性, 重点应用场景包括芯片、航天、轨道交通等安全攸关领域. 近 10 年来从事模型检查算法方面的研究, 提出了新型模型检查技术 CAR (互补近似可达), 并在此基础上提出了一系列优化技术使得其成为和主流技术如 BMC、IC3 等有较强竞争力的新方法. 相关工作发表在 CAV、ICCAD 等形式化方法与 EDA 国际主流会议. 近年来与国内 EDA 企业如上海合见、芯华章等展开深度合作, 将 CAR 技术应用到它们的产品流程中.