

形式化方法与应用专题前言^{*}

陈明帅¹, 田 聪², 熊英飞³

¹(浙江大学 计算机科学与技术学院, 浙江 杭州 310027)

²(西安电子科技大学 计算机科学与技术学院, 陕西 西安 710126)

³(北京大学 计算机学院, 北京 100871)

通信作者: 陈明帅, E-mail: m.chen@zju.edu.cn; 田聪, E-mail: ctian@mail.xidian.edu.cn;

熊英飞, E-mail: xiongyf@pku.edu.cn



中文引用格式: 陈明帅, 田聪, 熊英飞. 形式化方法与应用专题前言. 软件学报, 2025, 36(8): 3429–3430. <http://www.jos.org.cn/1000-9825/7355.htm>

形式化方法基于严格的数学化和机械化方法来规约、设计、构建、验证、演进计算系统, 是改善和确保计算系统质量的重要方法, 其模型、技术和工具已延伸成为计算思维的重要载体. 本专题聚焦形式化方法理论前沿, 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、软件工程、基础软件(操作系统、编译器等)、嵌入式系统、人机物融合系统、概率/量子系统、网络与信息安全、可信人工智能(智能制造、智能交通、智能控制、可信机器学习)等领域的交叉结合, 旨在我国标志性学术刊物上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, 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 18 篇, 先后邀请了 30 余位相关领域专家参与审稿工作, 每篇投稿邀请了 2–3 位专家进行评审. 稿件经初审、复审、ChinaSoft 2024 中国软件大会“形式化方法与应用专题论坛”汇报和终审 4 个阶段, 历时 6 个月, 最终有 12 篇论文入选本专题.

论文《[Fast-USYN: 从酉矩阵到高质量量子电路的快速合成](#)》提出了一种根据酉矩阵合成量子电路的快速合成方法 Fast-USYN, 相较于当前最优的合成方法实现了门数量减少、速度提升的显著性能优化.

论文《[神经网络的增量验证](#)》针对神经网络结构与参数修改后的安全性质验证需求, 提出了一种基于 Reluplex 框架的增量可满足性模理论算法 DeepInc, 实现了相较于 Marabou 和 α, β -CROWN 的显著加速.

论文《[单球驱动平衡机器人运动学和动力学形式化验证](#)》基于定理证明器 HOL Light 及其数学、物理学相关的定理证明库, 实现了在高阶逻辑框架下对单球驱动平衡机器人运动学与动力学模型的构建、推导与证明.

论文《[基于记忆策略的元解释学习](#)》针对元解释学习中的冗余证明问题, 提出了一种基于 Prolog 数据库机制的剪枝策略, 证明了其正确性, 在理论上计算了程序空间的缩减比例, 并实证了其对于现有系统学习时间的优化.

论文《[GhostFunc: 一种针对 Rust 操作系统内核的验证方法](#)》面向基于 Rust 构建的微内核中 unsafe 代码段的验证需求, 提出了 GhostFunc 的 safe 和 unsafe 代码段组合验证方法, 针对任务管理与调度模块在交互式定理证明器 Coq 中完成了正确性验证.

论文《[面向自动驾驶系统的场景建模及边缘关键场景生成](#)》基于自动驾驶领域本体建模场景, 结合形式化量化评估与重要性采样, 提出并实现了一种基于 SML4ADS2.0 的自动驾驶场景建模及边缘关键场景生成方法.

论文《[动态顺序统计树类结构的函数式建模及其自动化验证](#)》针对动态顺序统计树结构这类数据结构, 设计了函数式建模方法和自动化验证方法, 可对模型中的数据结构实例自动生成正确性验证.

论文《[基于下推自动机的同步数据流语言可信编译](#)》提出了同步数据流语言可信编译方法, 可将 Lustra 语言

* 收稿时间: 2024-12-11; jos 在线出版时间: 2024-12-11

程序转换为 C 语言程序, 并使用 Isabelle 对翻译转换过程进行严格的正确性证明.

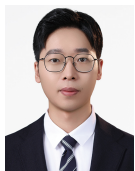
论文《[操作系统内核权限访问控制的形式验证](#)》以并发精化程序逻辑 CSL-R 为基础, 通过证明权限 API 函数和其抽象规范之间的精化关系, 来验证航天嵌入式领域某微内核操作系统权限访问控制的功能正确性.

论文《[基于混成自动机路径过滤与动态选择的 CPS 系统反例生成](#)》针对 CPS 系统中生成反例的路径爆炸问题, 提出了路径过滤与动态选择两种技术, 可提高 CPS 系统反例生成的效率和性能.

论文《[面向 Rust 语言的形式化验证方法研究综述](#)》综述了 Rust 语言的形式化验证工作, 通过语义模型、自动化验证方法及实例分析, 探讨了提升 Rust 安全性的途径与挑战, 并展望了未来研究方向.

论文《[因果时空语义驱动的深度强化学习抽象建模方法](#)》针对智能信息物理融合系统中深度强化学习决策效率低下和泛化性不足的问题, 提出基于因果时空语义的深度强化学习抽象建模方法, 通过实验验证了该方法在抽象表达能力、准确性及语义等价性方面的效果.

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软件设计开发、软件分析验证、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》编委会和 CCF 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. 希望本专题能够对形式化方法与应用相关领域的研究工作有所促进.



陈明帅(1990—), 男, 博士, 浙江大学研究员, 博士生导师, CCF 高级会员, 形式化方法专委会执行委员, 杭州市钱江特聘专家, 国家优秀青年科学基金(海外)获得者. 主要研究领域为形式验证, 程序理论, 概率/量子系统, 信息物理融合系统等. 与合作者一起, 提出新型安全攸关系统形式验证理论, 解决了概率程序不动点估计、微分系统可达性判定、时滞系统高效控制生成等若干软件理论难题, 研究成果应用于我国探月二期工程“嫦娥”三号等重大工程, 在 Information and Computation、OOPSLA、CAV、FM、ASPLOS 等领域旗舰期刊/会议上发表学术论文 30 余篇, 曾获中国科学院院长特别奖、ATVA 杰出论文奖、FMAC 最佳论文奖.



田聪(1981—), 女, 博士, 西安电子科技大学二级教授, 博士生导师, CCF 杰出会员, 科学研究院院长, 陕西省安全攸关智能软件重点科技创新团队负责人. 担任中国计算机学会形式化方法专委会副主任、中国自动化学会网络信息服务专委会副主任、全国信息技术标准化技术委员会软件与系统工程分技术委员会委员; 《软件学报》、IEEE Trans. on Reliability、Journal of Combinatorial Optimization、《西安电子科技大学学报》等期刊编委. 长期从事可信软件、形式化验证理论与方法研究.



熊英飞(1982—), 男, 博士, 北京大学长聘副教授, CCF 专业会员, 软件研究所副所长. 主要研究领域为程序合成、修复、分析和验证. 工作帮助产生了一系列不同规模的效果同期最优代码生成神经网络模型, 如 DeepSeek-Coder 模型; 大幅提升了缺陷修复的正确率、修复数量和修复效率; 提出了最广泛使用的两大双向变换模型之一——基于差别的双向变换; 成功自动求解大量算法问题, 包括世界顶级算法竞赛中的问题. 在 IEEE TSE 担任编委, PLDI、ICSE、FSE、OOPSLA、ASE、ISSTA 等会议定期担任 PC, 5 次在 ICSE 和 FSE 会议上获得杰出审稿人奖. 获得国家技术发明一等奖(排名 6)、电子学会自然科学一等奖(排名 1)、CCF-IEEE CS 青年科学家奖、MODELS 十年最有影响力论文奖, 5 次获得 ACM SIGSOFT/IEEE TCSE 杰出论文奖, 是 IFIP WG 2.4 唯一来自中国的成员.