软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2024,35(9):4011−4012 [doi: 10.13328/j.cnki.jos.007140]

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

形式化方法与应用专题前言*

曹钦翔[1], 宋 富[2], 詹乃军[2]

[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)

通信作者: 曹钦翔, E-mail: caoqinxiang@sjtu.edu.cn; 宋富, E-mail: songfu@ios.ac.cn; 詹乃军, E-mail: znj@ios.ac.cn

中文引用格式: 曹钦翔, 宋富, 詹乃军. 形式化方法与应用专题前言. 软件学报, 2024, 35(9): 4011–4012. http://www.jos.org.cn/1000-9825/7140.htm

随着硬件运算速度变得越来越快、体系结构变得越来越复杂, 软件的功能也变得越来越强大而复杂, 如何开发可靠的软件系统, 已经成为了一项巨大的挑战. 形式化方法是利用数学理论与方法论证检验软件系统可靠性与安全性的方法, 包括模型检验、定理证明等多种技术手段. 近年来, 利用形式化方法解决软件可靠性与安全性问题已经获得了越来越广泛的应用. 为此, 我们组织了本专题与 ChinaSoft 形式化方法与应用论坛, 探讨并交流最近一年以来, 国内学者在形式化方法与应用的研究中取得的新成果.

本专题采取公开征文的方式, 共收到稿件 44 份, 邀请了 30 多位专家对这些稿件进行了两轮审稿. 这些稿件中有 21 篇稿件进入第 2 轮审稿, 这些复审稿件中有 15 篇论文通过评审被邀请到 ChinaSoft2023 中国软件大会形式化方法与应用论坛做报告, 回答现场学者提问, 最终有 14 篇论文入选本专题.

论文《关于安全案例论证构建的综述》介绍了安全案例的 4 个基本构建步骤: 确定目标、收集证据、构建论证和评估安全案例, 详细介绍了现有的 8 种安全案例表达形式, 包括目标结构符号 (GSN)、声明-论点-证据 (CAE)、结构化安全案例元模型 (SACM) 等, 并分析了它们的优缺点.

论文《完备神经网络验证加速技术综述》是一篇介绍神经网络验证领域的通用技术的综述, 提出了一个完备神经网络验证的通用框架, 并在此框架中重点讨论了目前最先进的工具在约束求解、分支选择与边界计算这 3 个核心部分上所采用的优化方法.

论文《基于交互式定理证明的并发程序验证工作综述》对在交互式定理证明中可用于描述并发程序正确性的验证目标进行了梳理, 并对交互式定理证明方法中常用的程序逻辑与相应验证成果展开了细致地分析与总结.

论文《舰载机弹药保障作业调度的形式化建模与验证》基于分离逻辑的思想, 设计了一种简化的命令式程序语言对一类弹药保障系统的行为建模, 并利用定理证明器 Coq 对几个弹药保障作业规划方案进行了形式化验证.

论文《基于优先级时间 Petri 网的实时嵌入式多核系统分析》提出了优先级时间 Petri 网与带有资源分配与优先级的任务依赖图, 用于改进了现有点区间优先级时间 Petri 网分析实时嵌入式多核系统的效果.

论文《并发对象强可线性化性质的检测和验证》从并发对象的验证算法和证否方法两个方面研究了强可线性化性质, 一方面提出了两种强可线性化的验证算法, 另一方面给出了一个构造性的证否强可线性化的方法.

论文《基于 DH 标定的机器人正向运动学形式化验》在 Coq 中对 DH 坐标系进行形式化建模, 构建相邻坐标系间转换矩阵的形式化定义, 并验证了该转换矩阵与复合螺旋运动的等价性.

论文《微内核操作系统互斥量模块功能正确性的形式化验证》在交互式定理证明器 Coq 中对某抢占式微内核操作系统的互斥量模块进行了代码级形式化建模, 给出了其接口函数的形式化规范, 并验证了这些接口函数的功能正确性.

论文《基于形式化方法的区块链系统漏洞检测模型》综合了系统迁移状态、安全规约和节点间信任关系等

* 收稿时间: 2024-01-08; jos 在线出版时间: 2024-01-08

多种安全因素, 提出了基于形式化理论的区块链系统漏洞检测模型 VDMBS.

论文《命令式动态规划类算法程序推导及机械化验证》提出了在 Isabelle/HOL 定理证明器中验证一类基于命令式程序实现的动态规划算法的功能正确性方法.

论文《Trie+结构函数式建模、机械化验证及其应用》提出了一种匹配算法的通用验证规约, 并使用此方法与 Trie+结构的形式化在 Isabelle 中建模和验证了函数式的多模式匹配算法.

论文《基于 MTRDL 的自动飞行系统模式需求建模与验证方法》提出了面向自动飞行系统模式转换的领域需求建模语言 MTRDL, 并基于此提出了一种领域特定的建模验证框架.

论文《基于 AADL 的混合关键系统随机错误与突发错误安全性分析》提出了新的线程状态机语义理论来描述带有突发错误的线程执行过程, 还提出了模型转换规则和组装方法从而能从 AADL 模型推导出 PRISM 模型, 并基于此形成了一套随机错误与突发错误安全性分析的方法. 本文以动力艇自动驾驶仪系统为例, 验证了该方法的有效性.

论文《Büchi 自动机确定化分析工具》研究了 ω 自动机的确定化过程中索引能否继续被优化的问题, 实现了确定化研究工具 NB2DR, 其可以对非确定性 Büchi 自动机进行高效的确定化.

上面这些专题论文中既有对重要前沿领域研究成果的综述, 又包括模型检验、定理证明与自动机等研究的前沿成果, 还涵盖形式化方法在诸多安全攸关领域的应用. 感谢《软件学报》编委会和 CCF 形式化专委会对专题工作的指导和帮助, 感谢全体评审专家耐心细致的评审工作, 感谢所有来稿本专题的作者. 希望本专题能够对形式化方法的研究与应用有所促进.

曹钦翔(1990－), 男, 博士, 上海交通大学副教授, CCF 专业会员, 曾获上海浦江人才计划资助. 长期从事基于定理证明的程序验证与程序逻辑研究, 论文主要发表在 POPL、OOPSLA、JAR 等国际著名会议或期刊, 其代表性工作是其领衔开发的 VST 程序验证工具系列. 在此基础上, 还参与撰写了 Coq 定理证明知名教材《Software Foundations》的第 5 卷.

宋富(1983－), 男, 博士, 中国科学院软件研究所研究员, CCF 高级会员, 主要研究系统与软件安全验证和测试技术、及相关逻辑和自动机理论, 主持和参与多项国家自然科学基金委青年、面上和重点项目, 曾获上海市浦江人才和上海市晨光学者人才计划资助、2021 年秋季亚马逊研究奖、入选中国电子学会 2023 网络空间安全优秀论文, 已在国际著名会议或期刊 (如 IEEE S & P、USENIX Security、NDSS、POPL、OOPSLA、CAV、ESEC/FSE、ICSE、ASE、ISSTA、FM、ACM TOSEM、IEEE TSE、IEEE TDSC、I & C) 发表 80 多篇论文.

詹乃军(1971－), 男, 博士, 中国科学院软件研究所研究员, 中国科学院特聘研究员, 中国科学院大学岗位教授, 计算机科学国家重点实验室执行主任, CCF 杰出会员, 国家杰出青年科学基金获得者. 研究方向包括: 实时、嵌入式和混成系统设计理论以及程序理论等. 任《Journal of Automated Reasoning》《Formal Aspects of Computing》《Journal of Logical and Algebraic Methods in Programming》《Research Direction: Cyber-physical Systems》《软件学报》《计算机研究与发展》《电子学报》《前瞻科技》等期刊编委, 国际会议 MEMOCODE 和 SETTA 的指导委员会委员, 多个国际会议程序委员会共同主席 (如形式化方法旗舰会议 FM 2021) 和著名国际会议程序委员会委员 (如 CAV、RTSS、HSCC、ICCPS、EMSOFT 等); 在著名国际会议和杂志发表论文 100 多篇, 出版专著 2 部, 编著 4 部.