软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(6):1579−1580 [doi: 10.13328/j.cnki.jos.006256]

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*

田 聪[1], 邓玉欣[2], 姜 宇[3]

[1](西安电子科技大学 计算机学院,陕西 西安 710071)

[2](华东师范大学 软件学院,上海 200062)

[3](清华大学 软件学院,北京 100084)

通讯作者: 田聪, 邓玉欣, 姜宇, E-mail: ctian@mail.xidian.edu.cn, yxdeng@sei.ecnu.edu.cn, jiangyu198964@126.com

中文引用格式: 田聪,邓玉欣,姜宇.形式化方法与应用专题前言.软件学报,2021,32(6):1579−1580. http://www.jos.org.cn/1000-9825/6256.htm

计算机科学的发展主要涉及硬件和软件的发展,而软、硬件发展的核心问题之一是如何保证它们是安全可靠的.如今,硬件性能变得越来越高,运算速度也越来越快,体系结构、软件的功能也更加复杂,如何开发可靠的软、硬件系统,是计算机科学发展面临的巨大挑战.特别是现在计算机系统广泛应用于许多安全攸关系统中,如高速列车控制系统、航空航天控制系统、医疗设备控制系统等等,这些系统中的错误可能导致灾难性后果.

形式化方法已经成功应用于各种硬件设计,特别是芯片的设计.各大硬件制造商都有一个非常强大的形式化方法团队为保障系统的可靠性提供技术支持,例如IBM、AMD等等.近年来,随着形式验证技术和工具的发展,特别是在程序验证中的成功应用,形式化方法在处理软件开发复杂性和提高软件可靠性方面已显示出无可取代的潜力.各个著名的研究机构都投入了大量人力和物力从事这方面的研究.例如,美国宇航局(NASA)拥有的形式化方法研究团队在保证美国航天器控制软件正确性方面发挥了巨大作用,在研发“好奇号”火星探测器时,为了提高控制软件的可靠性和生产率,广泛使用了形式化方法.在新兴领域,如区块链及人工智能等领域,形式化方法也逐步得到应用,提升系统的整体安全可控.

本专题公开征文,共征得投稿 27 篇.特约编辑先后邀请了国内外在该领域比较活跃的学者参与审稿工作,每篇投稿至少邀请 2 位专家进行初审.大部分稿件经过初审和复审两轮评审,部分稿件经过了两轮复审.通过初审的稿件还在 FMAC 2020 大会上进行了现场报告,作者现场回答了与会者的问题,并听取了与会者的修改建议.最终有 18 篇论文入选本专题.

《C2P:基于 Pi 演算的协议 C 代码形式化抽象方法和工具》提出一种检测安全协议代码语义逻辑错误的形式化验证方法,通过将协议C源码自动化抽象为Pi演算模型,基于Pi演算模型对协议安全属性进行形式化验证.

《大粒度 Pull Request 描述自动生成》利用图神经网络和强化学习的技术,提出一种为 GitHub 平台中大粒度 Pull Request 自动生成描述的方法.

《Petri 网的反向展开及其在程序数据竞争检测的应用》针对安全 Petri 网的可覆盖性判定问题提出一种目标导向的反向展开算法,并应用于并发程序中数据竞争检测问题的形式化验证.

《面向 SPARC 处理器架构的操作系统异常管理验证》提出了基于 Hoare-logic 的验证框架,用于证明面向 SPARC 处理器架构操作系统异常管理的正确性,基于该框架验证了我国北斗三号在轨实际应用的航天器嵌入式实时操作系统 SpaceOS 异常管理功能的正确性.

《基于分支标记的数据流模型的代码生成方法》针对具有复杂分支组合的数据流模型提出了基于分支调度标记的代码生成方法.

《面向 AADL 模型的存储资源约束可调度性分析》提出一种面向软件架构级别、基于抢占调度序列的缓存相关抢占延迟计算方法,用来分析缓存相关抢占延迟约束下 AADL(架构分析和设计语言)模型的可调度性.

收稿时间: 2021-01-30

《基于锁增广分段图的多线程程序死锁检测》对已有的锁图和分段图模型进行改进,提出一种新的死锁检测方法,该方法能有效消除各种误报,提高死锁检测的准确率.

《基于污染变量关系图的 Android 应用污点分析工具》提出了一种基于污染变量关系图的污点分析方法,并描述了基于该方法所实现的工具 FastDroid 的架构、模块及算法细节.

《以太坊中间语言的可执行语义》对以太坊中间语言 Yul 进行形式化,利用 Isabelle/HOL 证明辅助工具给出了其类型系统和小步操作语义的形式化定义,为智能合约正确性、安全性验证奠定了基础.

《个体交互行为的平滑干预模型》提出一种基于个体交互行为系统平滑干预模型,能够很好地引导用户行为平滑变化,且产生足够的区分性使得行为伪装异常检测场景下模型的准确性显著提高.

《支持乱序执行的 Raft 协议》使用 TLA+为分布式共识协议 ParallelRaft 提供严格的形式化规约,并证明了在参与者数量较小的情形下算法的正确性.

《面向 CPS 时空性质验证的混成 AADL 建模与模型转换方法》提出了面向 CPS 时空性质验证的混成 AADL 建模与模型转换方法,并通过一个飞机避撞系统实例验证该方法的有效性.

《芯片开发功能验证的形式化方法》提出了一种新型验证设计模型和生成代码一致性的方法.该方法利用 MSVL 语言进行系统建模,通过统一模型检测的原理,验证模型是否满足性质的有效性.

《面向数据流的 ROS2 数据分发服务形式建模与分析》采用概率模型检验的方法,分析、验证机器人操作系统 ROS2 系统数据分发机制的实时性和可靠性.

《Ptolemy 离散事件模型形式化验证方法》提出了一种基于形式模型转换的方法来验证离散事件模型的正确性,通过在 Ptolemy 环境中实现一个插件,可以自动将离散事件模型转换为时间自动机模型,并通过调用 Uppaal 验证内核完成验证.

《面向 MSVL 的智能合约形式化验证》介绍了如何使用建模、仿真与验证语言(MSVL)和命题投影时序逻辑(PPTL)对智能合约进行建模和验证.

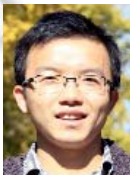
《面向 ROS 的差分模糊测试方法》提出了一种差分模糊测试方法对机器人操作系统 ROS 不同版本的功能包进行测试,找出其中的漏洞.

《基于 Coq 的分块矩阵运算的形式化》完善了基于 Coq 记录类型的矩阵形式化方法,其中包括提出新的矩阵等价定义、并证明了一组新的引理,最终实现了矩阵与分块矩阵形式化的不同类型的基础库.

本专题重点关注形式化基础方法、技术、支持工具以及领域交叉应用,反映了我国学者在该领域的最新研究进展.感谢《软件学报》编委会、CCF 形式化方法专委会对专题工作的指导和帮助,感谢编辑部各位老师从征稿启示发布、审稿专家邀请至评审意见汇总、论文修改、定稿及出版所付出的辛勤工作,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对《软件学报》的信任.希望本专题能够对形式化方法的科研工作有所促进.

田聪(1981－),女,博士,西安电子科技大学计算机科学与技术学院教授,博士生导师,CCF 杰出会员,主要研究领域为形式化方法,程序验证,等.

邓玉欣(1978－),男,博士,华东师范大学软件工程学院教授,博士生导师,CCF 高级会员,主要研究领域为形式化方法,程序理论,等.



姜宇(1989－),男,博士,清华大学软件学院副教授,博士生导师,CCF 会员,主要研究领域为形式化方法,程序分析,嵌入式软件,等.