软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2020,31(8):2283−2284 [doi: 10.13328/j.cnki.jos.005965]

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

# 面向新兴系统的形式化建模与验证方法专题前言*

陈振邦[1], 冯新宇[2,3], 刘志明[4,5]

[1](国防科技大学 计算机学院,湖南 长沙 410073)

[2](南京大学 计算机科学与技术系,江苏 南京 210023)

[3](南京大学 计算机软件新技术国家重点实验室,江苏 南京 210023)

[4](西南大学 计算机与信息科学学院,重庆 400715)

[5](西南大学 软件研究与创新中心,重庆 400715)

通讯作者: 陈振邦, E-mail: zbchen@nudt.edu.cn; 冯新宇, E-mail: xyfeng@nju.edu.cn; 刘志明, E-mail: zhimingliu88@swu.edu.cn

中文引用格式: 陈振邦,冯新宇,刘志明.面向新兴系统的形式化建模与验证方法专题前言.软件学报,2020,31(8):2283−2284. http://www.jos.org.cn/1000-9825/5965.htm

形式化方法是计算机科学的重要理论基础.它以严格的数学化和机械化方法为基础来规约、构建和验证计算系统,是改善和确保计算系统质量的重要方法.近年来,随着相关技术的发展,形式化方法已经在越来越多的新兴系统中得到应用并取得显著效果.为了记录中国学者在新兴系统的形式化建模与验证理论、方法、工具和应用等方面的最新研究成果,特设立此专题.

本专题采取自由投稿的方式,共收到 17 篇投稿,其中 16 篇通过了形式审查.特邀编辑邀请 17 位领域专家参与审稿,每篇稿件邀请了 2 位专家进行评审,共计 10 篇稿件通过第 1 轮评审,并在 CCF 形式化专委年度会议上进行了报告,后对修改后稿件进行了又一轮的评审.经过 2 轮评审,最终 6 篇论文入选本专题.

《一种包解析器硬件配置描述语言及其编译结构》设计了一种用于实现可重构网络数据包解析器的专用硬件配置描述语言 P3,给出了 P3 的类型系统和操作语义,以及 P3 的可信编译结构.

《高阶类型化可验证应用系统体系结构建模及案例》面向应用系统体系结构设计及其验证,提出了一种高阶类型化模型驱动的可验证应用系统体系结构建模语言及建模方法.

《PaxosStore 中共识协议 TPaxos 的推导、规约与精化》给出了如何从 Paxos 出发逐步推导出 TPaxos,以及 TPaxos 协议的 TLA+形式化规约,并使用精化技术证明了 TPaxos 和 TPaxosAP 的正确性.

《基于 Coq 的 Paxos 形式化建模与验证》使用定理证明工具 Coq 形式化定义了 Lamport 的 Basic Paxos 算法,并且证明了算法满足共识性.

《基于 Coq 的操作系统任务管理需求层建模及验证》利用定理证明工具 Coq 对实际星上操作系统任务管理模块进行了形式化需求建模及验证,并提出了一种基于任务状态列表集合的验证框架.

《基本并行进程活性的限界模型检测》给出了基本并行进程上 EG 逻辑的限界语义,并给出了基于 SMT 的基本并行进程上 EG 逻辑的限界模型检验方法.

本专题面向包括形式化方法、软件工程、计算机系统、嵌入式系统及其相关领域的研究人员和专业软件工程师,内容聚焦新兴系统的形式化建模与验证方法,反映了我国学者在此方向的高水平研究成果.感谢《软件学报》编委会、中国计算机学会形式化方法专委会、中国计算机学会形式化专委 2019 年年会(FMAC 2019)组委会对专题工作的指导和帮助,感谢专题全体评审专家的辛勤工作,感谢所有的投稿作者.希望本专题能够对国内形式化方法的研究工作有所推动.

* 收稿时间: 2020-03-28

**陈振邦**(1981－),男,博士,副教授,CCF 专业会员.主要研究领域为程序分析,形式化方法及其应用.

**冯新宇**(1978－),男,博士,教授,CCF 专业会员.主要研究领域为程序验证,程序设计语言理论.

**刘志明**(1961－),男,博士,教授,博士生导师,CCF 高级会员.主要研究领域为软件理论与方法.