软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(7):1901−1902 [doi: 10.13328/j.cnki.jos.005758]

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

软件形式化验证专题前言*

贺 飞[1,2,3], 张立军[4,5]

[1](清华大学 软件学院,北京 100084)

[2](北京信息科学与技术国家研究中心,北京 100084)

[3](信息系统安全教育部重点实验室,北京 100084)

[4](中国科学院 软件研究所,北京 100190)

[5](广州智能软件产业研究院,广东 广州 511458)

通讯作者: 贺飞, E-mail: hefei@tsinghua.edu.cn; 张立军, E-mail: zhanglj@ios.ac.cn

中文引用格式: 贺飞,张立军.软件形式化验证专题前言.软件学报,2019,30(7):1901−1902. http://www.jos.org.cn/1000-9825/5758.htm

形式化方法是建立在逻辑演算、形式语言、自动机理论、程序语义、类型系统等理论基础之上,对计算系统进行描述和分析的一系列符号与技术的集合.形式化方法可指导软/硬件系统的规约、设计和验证,是改善和确保计算系统质量的重要方法.历史上,形式化方法在硬件和协议验证方面取得巨大成功.近年来,随着相关技术的发展,形式化方法已在越来越多的软件系统中得到应用,并取得显著成效.为记录中国学者在形式化验证理论、方法、工具和应用等方面的最新研究成果,特设立此专题.

本专题采取定向邀请和自由投稿相结合的方式,共收到 22 篇投稿,其中 20 篇通过了形式审查.特约编辑邀请了 40 余位领域专家参与审稿,每篇稿件至少邀请 2 位专家进行评审,每篇稿件都经过两轮审稿.共计 11 篇稿件通过第 1 轮评审,并在 CCF 形式化方法专委会年度会议上进行了报告.经过第 2 轮终审,最终有 9 篇论文入选本专题.其中,

论文“基于 SVM 的多项式循环程序秩函数生成”研究程序终止性问题,将秩函数计算问题归结为二分类问题,并提出了利用支持向量机(SVM)计算程序秩函数的方法.

论文“高阶类型化软件体系结构建模和验证及案例”提出了一种高阶类型化的软件体系结构建模语言和相应的体系结构建模验证方法,支持主流 Web 应用体系结构的建模和验证.

论文“非交互式 Petri 网可覆盖性验证的高效实现”研究非交互式 Petri 网可覆盖性验证问题,在理论上给出了该问题的完备性判定方法,并给出了工具实现.

论文“基于实时自动机的连续时段演算的验证”研究在标准连续时间语义下基于实时自动机的扩展线性时段不变式的有界模型检验问题,证明了该问题是可判定的,并且给出模型检验算法.

论文“面向实时数据的 CPS 一体化建模方法”针对 CPS 在复杂环境中的安全性和可靠性问题,提出了一种面向实时数据的一体化建模方法,并针对移动机器人进行了案例分析.

论文“一种同步语言多线程代码自动生成工具”提出了一种从同步语言 SIGNAL 到多线程代码的自动生成工具,并在多核处理器上进行了实验验证.

论文“同步数据流语言可信编译器 Vélus 与 L2C 的比较”从源语言特性、编译器结构、翻译正确性验证等多个角度对同步数据流语言编译器 Vélus 和 L2C 进行了较为深入的分析与比较,能够为编译器可信构造研究提供参考.

收稿时间: 2019-03-07

论文“具有多传感器的 CPS 系统的攻击检测”研究存在瞬态故障的 CPS 中传感器的攻击检测问题,设计了一种基于融合间隔和历史测量的传感器攻击检测方法.

论文“有关时间自动机重置的若干问题的计算复杂性”研究完全确定时间自动机、部分规约的确定时间自动机以及非确定时间自动机的计算复杂性问题,并给出了有关复杂度估计的若干理论结果.

本专题面向形式化方法的研究人员和工程人员,内容涵盖系统软件、软件工程、嵌入式系统等领域,反映了我国学者在形式化验证理论、方法、工具和应用等方面的高水平研究成果.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的科研工作有所促进.

贺飞(1980－),男,博士,清华大学软件学院副教授,博士生导师,CCF 专业会员.主要研究领域为形式化方法,软件验证.

张立军(1979－),男,博士,中国科学院软件研究所研究员,博士生导师,CCF 专业会员,主要研究领域为概率模型检测,协议验证,学习算法.