软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(6):1515−1516 [doi: 10.13328/j.cnki.jos.005473]

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

形式化方法的理论基础专题前言*

傅育熙[1], 李国强[1], 田 聪[2]

[1](上海交通大学 软件学院, 上海 200240)

[2](西安电子科技大学 计算机学院,陕西 西安 710071)

通讯作者: 傅育熙, E-mail: fu-yx@cs.sjtu.edu.cn

中文引用格式: 傅育熙,李国强,田聪.形式化方法的理论基础专题前言.软件学报,2018,29(6):1515−1516. http://www.jos.org.cn/1000-9825/5473.htm

形式化方法主要研究如何把具有清晰数学基础的模型、规范、分析以及验证融入软硬件设计开发的各个阶段,是改善和确保计算机系统正确性和可靠性的重要途径.在领域需求的推动下,形式化方法技术和工具方面的研究取得了显著成效的同时,需要研究新的理论和方法来解决更复杂的计算机系统问题,这些理论和方法包括新模型下形式化验证的可判定性及复杂性结论、算法实现以及面向领域形式化方法.

本专题公开征文,共收到投稿 18 篇,内容涉及形式化方法的理论基础各个方面.特约编辑先后邀请了 30 多位专家参与审稿工作,每篇投稿至少邀请 2 位专家进行评审.稿件经初审、复审,有 14 篇稿件进入复审阶段,并在中国计算机学会形式化方法专委会的年度会议“第二届形式化方法与应用 (FMAC 2017)”上宣读,经过终审环节,最终有 13 篇论文收录到本专题.

1. 形式化方法理论与算法

《互模拟准局部验证算法的扩展与实现》扩展了作者以前提出的准局部算法,使其更加适用于一般的标记迁移系统.并且通过大量的实验数据,表明了准局部算法比局部算法的性能更好.同时,该算法可以用于验证模拟关系以及弱互模拟关系.

《自动分析递归数据结构的归纳性质》提出了一种新的对递归数据结构的归纳性质进行自动化分析的框架,并且通过.案例分析和实验结果表明该分析框架可以有效地分析递归数据结构的归纳性质,并生成对程序证明过程有用的断言.

《自动合成数组不变式》提出了基于抽象解释框架自动合成数组程序不变式的方法,能够分析按照特定顺序访问一维或者多维数组的程序,然后合成不变式.论文在理论上证明了该方法的正确性和收敛性,同时实现的原型工具通过具体实验显示了方法的可行性和有效性.

《向量加法系统验证问题研究综述》对近些年来在向量加法系统验证领域取得的成果进行了系统总结,并展望了未来研究方向及可能面临的挑战.

2. 形式化验证技术与工具

《异构多智能体系统模型检查》提出了一种在语法层对智能体策略类型进行刻画的系统模型,研究了基于新模型的 ATL 模型检查,并实现了相应的工具.

《基于 SMT 的时钟约束语言 CCSL 的形式化分析方法与工具》提出一种基于 SMT 的 CCSL 形式化分析方法,可以用于有效性证明、迹分析、死锁检测、LTL 模型检测等方面的验证与分析,并且基于该方法开发了原型工具,集成了当前最高效的 SMT 求解器 Z3 和 CVC4.

《消息传递的 MSVL 通信机制及其实现》提出了在 MSVL 中开发和实现合适的机制来对分布式系统进行建模和验证的方法.并且通过实例说明了消息传递在 MSVL 中的工作原理.

《普适计算应用时空性质的运行时验证》本文通过引入三值逻辑语义,提出了三值 Ambient 逻辑——AL3,

收稿时间: 2017-12-25

设计实现了基于 AL3 的性质检验算法和运行时监控器.通过案例分析和详实的实验数据,验证了方法的有效性和可行性.

《APTL 公式的可满足性检查工具》根据作者前期所研究的检查 APTL 公式的可满足性的方法,开发实现了工具 APTL2BCG,并通过实验证明了工具的有效性.

3. 面向领域的形式化方法

《基于类型理论的领域数据建模和验证及案例》面向行业数据规范及其验证,提出了基于类型理论的领域数据建模语言和领域建模方法.实现了一种领域数据建模工具原型系统,并通过领域数据建模与自动验证的实际案例,完成了一个较大规模行业数据规范的制定与验证.

《一种嵌套中断系统的建模和分析方法》提出一种建模和验证嵌套中断系统的方法,并通过实例展现本文所提出的方法的正确性和实用性.

《考虑中断和上下文切换开销的响应时间分析》对中断和上下文切换的机制和时间流程进行详细的阐述,并给出包含中断和上下文切换开销的更加精确的响应时间计算方法和仿真工具.

《机器人关节通信总线系统的建模与验证》提出使用形式化方法对基于 CAN 现场总线型控制系统进行建模分析,通过 UPPAAL 工具实现系统各部件的时间自动机模型,并对机器人通信系统进行正确性验证和实时性分析.

本专题主要面向形式化方法理论与应用领域的研究人员,反映了我国研究者在形式化方法的理论、算法、技术最新的研究进展.感谢《软件学报》编委会和形式化方法专委会对专题工作的指导和帮助,感谢评审专家及时、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领域的研究工作、形式化方法在工业界的兴旺发展有所促进.

傅育熙(1962－),男,博士,上海交通大学特聘教授.研究领域为理论计算机科学,研究内容涉及程序理论、并发计算模型、验证、交互理论.国家杰出青年基金获得者,上海市优秀学科带头人.2000 年 2 月~2009 年 5 月任上海交通大学计算机科学与工程系主任,2001 年 5 月~2013 年 12 月任上海交通大学软件学院院长.学术兼职包括:上海市计算机行业协会副会长、国务院学位委员会第六届学科评议组成员(2010~2014)、上海市计算机学会理事长(2015~2018)、教育部计算机类专业教学指导委员会副主任(2013~2017).担任 Mathematical Structures in Computer Science 的编委、Asian Association for Foundation of Software 的执行委员.

李国强(1979－),男,博士,上海交通大学软件学院副教授,中国计算机学会形式化方法专委委员,研究方向为形式化方法、程序语言理论、理论计算机科学,在本领域国际重要期刊和会议上发表高水平学术论文 40 余篇.

田聪(1981－),女,博士,西安电子科技大学教授,中国计算机学会形式化方法专委委员,中国计算机学会青年工作委员会和女计算机工作者委员会委员.国家优秀青年基金获得者,教育部新世纪优秀人才获得者,2014 年陕西省青年科技新星获得者.主要研究领域为形式化方法、时序逻辑、模型检测.在本领域国际重要期刊和会议上发表高水平学术论文 70 余篇.