软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(5):1049−1050 [doi: 10.13328/j.cnki.jos.005219]

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*

董 威[1], 赵建华[2], 吕鸣松[3]

[1](国防科学技术大学 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](东北大学 计算机科学与工程学院,辽宁 沈阳 110819)

通讯作者: 董威, E-mail: wdong@nudt.edu.cn

中文引用格式: 董威,赵建华,吕鸣松.形式化方法与应用专题前言.软件学报,2017,28(5):1049−1050. http://www.jos.org.cn/1000-9825/5219.htm

形式化方法以严格的数学化和机械化方法为基础来规约、设计、构建、验证、演进计算系统,是改善和确保计算系统质量的重要方法,其模型、技术和工具已延伸成为计算思维的重要载体,在国内外持续被关注和研究.在各种领域需求的推动下,形式化方法的相关理论、技术和工具越来越受重视,并在多种关键领域的应用中取得显著成效.

本专题主要关注国内形式化方法的最新研究进展及其在特定领域的应用,共征得投稿 37 篇,其中 36 篇通过特约编辑形式审查进入评审阶段.每篇稿件经过 2 位专家的评审,有 16 篇进入复审阶段,并在第 1 届全国形式化方法与应用会议(FMAC 2016)上宣读,最后有 13 篇文章通过终审被收录到本专题.

(1) 形式化规约与分析技术

《常用循环摘要的自动生成方法及其应用》通过分析循环代码的执行效果为操作常用数据结构的循环自动生成循环摘要,并以此为基础自动生成循环语句的规约,包括循环不变式、循环的前置条件以及循环的后置条件,能够有效提高自动化验证的效率.

《正则模型类的时态可定义性》研究了正则模型的互模拟及其在时态语言下的可定义性,定义了一系列与正则模型相关的运算,证明了正则模型类在时态语言中可定义的充要条件,明确了时态语言在正则模型类上的表达力.

《异步多进程时间自动机的可覆盖性问题》对时间自动机模型进行了扩展,允许自动机的部分状态触发新的进程,使得扩展后的模型可以描述进程的动态创建行为,并将扩展模型编码为可读边时间 Petri 网,证明了扩展模型的可覆盖性问题是可判定的.

《不确定观测下离散事件系统的可诊断性》定义了观测不确定条件下离散事件系统的可诊断性,给出各类观测不确定条件下的可诊断性判定方法,以及复合条件下判定可诊断性的方法.

《面向收敛的并发程序执行轨迹静态简化方法》提出了对并发程序执行轨迹进行静态简化的有效方法,针对执行区间寻找可合并的前置执行区间和后置执行区间,减少执行轨迹中的线程切换数量,有助于快速发现引发错误的线程交错.

(2) 形式化验证技术

《多机器人路径规划的安全性验证》采用混成通信顺序进程(HCSP)对多机器人的路径控制算法 D-CAPT 进行建模,并用定理证明工具 HProver 进行形式化验证,证明了该算法的正确性,即机器人团队在整个运行过程中不会发生碰撞.

《一种面向 CPS 的自适应统计模型检测方法》通过实验分析了不同统计模型检测技术的适用范围和性能

* 收稿时间: 2017-01-12; jos 在线出版时间: 2017-01-20
CNKI 网络优先出版: 2017-01-20 16:06:36, http://www.cnki.net/kcms/detail/11.2560.TP.20170120.1606.010.html

问题,提出了一种基于抽象和学习的统计模型检测方法 AL-SMC 以减少样本空间,并进一步提出一个自适应统计模型检测算法框架,能够自动选择 AL-SMC 或 BIE 算法从而提高验证效率.

《一种面向 CPS 的控制应用程序协同验证方法》针对嵌入式控制软件中控制环路等特点,提出了一种基于自动机理论对控制软件和受控对象进行建模与协同验证的方法以及优化算法.

《面向动作的上下文感知应用的规约与运行时验证》基于 Ambient Calculus 对面向动作的上下文感知(AOCA)应用的运行时状态进行形式化规约,采用 Ambient Logic 对运行时需要保证的性质进行描述,提出了 AOCA 应用的监控器生成和运行时验证方法.

(3) 面向领域的形式化方法

《基于通信的列车控制系统可信构造:形式化方法综述》从基于通信的列车控制(CBTC)系统的需求分析、设计建模、系统实现等不同层次出发,总结分析了 CBTC 系统可信构造面临的挑战,对与此相关的形式化方法研究与应用现状进行了综述.

《基于 Event-B 的航天器内存管理系统形式化验证》通过对航天器操作系统内存管理的特性进行分析,使用 Event-B 方法对航天器操作系统 SpaceOS 中的内存管理模块进行形式化建模,并采用基于分层模型精化和迭代的方式,验证该内存管理模块是否满足特定性质.

《peC 语言的部分求值器及在编译器测试中的应用》将部分求值技术应用到编译器测试中,设计了一个 C 语言子集 peC 并对该语言的部分求值策略进行了形式化描述,提出一个基于部分求值技术的编译器测试框架,实现了部分求值器对 GCC,LLVM 编译器进行测试.

《可信编译器 L2C 的核心翻译步骤及其设计与实现》对以同步数据流语言 Lustre*为源语言的可信编译器 L2C 的主体翻译框架、核心翻译步骤进行了介绍,并对采用 Coq 证明 L2C 的翻译正确性的过程和难点进行了分析与探讨.

本专题主要面向形式化方法与工具、计算机理论、软件工程、系统软件、嵌入式系统、人工智能等领域的相关科研人员和工程师.专题审稿过程历时 4 个月,有 30 余名相关领域的专家参与了审稿工作.在此,我们要特别感谢审稿专家和《软件学报》编辑部相关老师的辛勤工作,以及中国计算机学会形式化方法专业学组的指导和帮助.此外,我们还要感谢向本专题踊跃投稿的作者.最后,希望本专题的内容能够对广大读者的科学研究与工程实践工作起到促进作用.我国在形式化方法领域欲取得更大进展,离不开我们所有人的共同努力.

董威(1976－),男,陕西咸阳人,博士,教授,博士生导师,CCF 专业会员.现任中国计算机学会软件工程专委会委员、形式化方法专业学组委员.主要研究领域为软件分析与验证,群智化软件开发方法.

赵建华(1971－),男,博士,教授,博士生导师,CCF 高级会员.现任中国计算机学会形式化方法专业学组委员.主要研究领域为形式化方法,软件工程.

吕鸣松(1980－),男,博士,副教授,CCF 专业会员.主要研究领域为多核嵌入式系统设计,实时系统时间行为分析与验证.