软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(8):2753−2754 [doi: 10.13328/j.cnki.jos.006611]

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 *

陈立前[1], 孙 猛[2]

[1](国防科技大学 计算机学院, 湖南 长沙 410073)

[2](北京大学 数学科学学院, 北京 100871)

通信作者: 陈立前, E-mail: lqchen@nudt.edu.cn

中文引用格式: 陈立前, 孙猛. 形式化方法与应用专题前言. 软件学报, 2022, 33(8): 2753–2754. http://www.jos.org.cn/1000-9825/6611.htm

形式化方法基于严格的数学方法规约、设计、构建、验证、演进计算系统, 是改善和保障计算系统可信性的重要方法. 形式化方法相关基础理论、技术和工具已成功应用于各种软硬件系统的设计与验证. 近年来, 在区块链、深度学习、量子计算等新兴领域, 形式化方法也逐步应用适配, 提升新兴领域计算系统的可信性.

本专题公开征文, 共收到投稿 40 篇. 特约编辑先后邀请了 20 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、中国软件大会 ChinaSoft 2021 会议宣读和终审 4 个阶段, 历时 7 个月, 最终有 15 篇论文入选本专题.

《面向 SQLite3 数据库 API 调用序列的并行运行时验证方法》针对 SQLite3 数据库 API 调用序列提出了一种基于多核系统的并行运行时验证方法, 能够有效发挥多核系统的硬件能力, 提高验证效率.

《一种利用非确定规划的 LTL 合成方法》提出了一种利用非确定规划求解 LTL 合成问题的方法, 证明了方法的正确性和完备性, 并通过实验表明了该方法在解质量方面具有优势, 能够获得规模较小的合成策略.

《基于基本并行进程的异步通信程序的验证方法》改进了一类为异步通信程序建模的 Actor 通信系统, 将其归约至基本并行进程, 并实现了相应的模型检测工具.

《运用时间分类树的确定单时钟时间自动机学习》针对确定性单时钟时间自动机学习的效率问题, 提出了一种改进的学习算法, 使用逻辑时间分类树作为学习算法的内部数据结构, 有效地减少了成员查询次数, 降低了算法的空间复杂度.

《面向 CPS 时空约束的资源建模及其安全性验证方法》针对信息物理空间中 CPS 资源安全性验证问题, 基于时间通信顺序进程 TCSP, 提出了一种面向 CPS 时空约束的资源建模及其安全性验证方法.

《基于消息传递关系网络的布尔可满足性预测》提出将 SAT 问题转化为一种多关系异构图, 并基于关系消息传递网络提出了一种预测精度更高、泛化能力更好的布尔可满足性预测方法.

《基于 SysML 的机载软件分层精化建模与验证方法》提出了一种基于 SysML 状态机图子集的机载软件分层精化建模与验证方法, 并以自动飞行控制软件为例验证了方法的有效性.

《智能合约的时间约束模式及其形式化验证》分析总结出智能合约的 5 种时间约束模式, 定义了 Solidity 智能合约到时间自动机的转换规则并实现其到实时模型检测工具 UPPAAL 入口模型的转换, 然后利用 UPPAAL 验证合约的时间相关性质.

《TSO 内存模型下限界可线性化的可判定性研究》研究了 k-限界 TSO-to-TSO 可线性化、k-限界 TSO-to-SC 可线性化和 k-限界 TSO 可线性化的可判定问题, 证明了 TSO 内存模型下可线性化的这三种限界版本都是可判定的.

《基于深度学习和反例制导的循环程序秩函数生成》针对非线性循环程序, 提出了一种基于反例制导的神经网络型秩函数的构造方法, 采用了学习组件和验证组件交互的迭代框架.

* 收稿时间: 2022-02-17; jos 在线出版时间: 2022-02-17

《基于时态测试器的实时分支时态逻辑模型检测》针对一种实时分支时态逻辑 RTCTL*的高效模型检测问题，提出了一种 RTCTL*正时态测试器构造方法以及相关符号化模型检测算法，并开发了基于该算法的模型检测工具.

《模拟实时系统的点区间优先级时间 Petri 网与 TCTL 验证》针对传统优先级时间 Petri 网对实时系统建模能力不足的问题，提出了一种点区间优先级时间 Petri 网，以模拟多核多任务实时系统，并设计了相应的模型检测算法，开发了相应的模型检测器.

《基于抽象解释的函数内联过程间分析优化方法》针对函数内联过程间分析方法存在的不足，在基于抽象解释的程序分析场景下，提出了一种面向内联函数块的程序环境降维优化方法，以降低分析过程的时空开销.

《基于锁耦合遍历算法的文件系统终止性验证》构建了一个终止性证明框架 CRL_T，并验证了文件系统 AtomFS 中保证了任何一个接口在公平调度的条件下都能返回，在 Coq 中对相关证明进行了形式化.

《软硬件综合 AADL 可靠性建模及分析方法》综合考虑软硬件错误发生失效后对系统可靠性的影响，提出了一种面向系统架构级别的软硬件综合可靠性分析方法.

本专题主要面向形式化方法相关理论研究、支撑工具、工业应用等领域的研究人员和工程人员，反映了我国学者在形式化方法与应用领域最新的研究进展.感谢《软件学报》编委会和 CCF 软件工程、系统软件、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与应用相关领域的研究工作有所促进.

陈立前(1982－)，男，博士，副教授，CCF 高级会员，主要研究领域为程序分析与验证，抽象解释.

孙猛(1978－)，男，博士，教授，CCF 高级会员，主要研究领域为程序理论，软件形式化方法.