软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2023,34(8):3465−3466 [doi: 10.13328/j.cnki.jos.006871]

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

约束求解与定理证明专题前言*

蔡少伟[1], 陈振邦[2], 王 戟[2], 詹博华[1], 赵永望[3]

[1](中国科学院 软件研究所, 北京 100190)

[2](国防科技大学 计算机学院, 湖南 长沙 410073)

[3](浙江大学 计算机科学与技术学院, 浙江 杭州 310007)

通信作者: 蔡少伟, E-mail: caisw@ios.ac.cn

中文引用格式: 蔡少伟, 陈振邦, 王戟, 詹博华, 赵永望. 约束求解与定理证明专题前言. 软件学报, 2023, 34(8): 3465–3466. http://www.jos.org.cn/1000-9825/6871.htm

随着计算机系统在工业和生活中越来越广泛的应用, 软件和硬件的可靠性受到越来越多的关注. 形式化方法使用严格的数学语言对计算机系统建模, 并在计算机的辅助下验证系统的正确性. 与测试不同, 形式化方法可以完全排除某些类型的错误. 约束求解和定理证明是形式化方法中的两大关键技术. 在约束求解方面, SAT 和 SMT 求解器已经在学术界和工业界得到了广泛应用, 比如 SAT 求解器用于 EDA 领域的等价性验证, SMT 求解器用于程序验证和白盒模糊测试等. 交互式定理证明通过人和计算机之间的交互完成证明, 能够验证非常复杂的系统和性质, 例如编译器和操作系统的正确性验证. 约束求解与定理证明专题关注约束求解和定理证明的理论、技术、工具与应用, 包括在 EDA、符号执行、模型检测、程序分析与验证、系统安全等领域的应用.

本专题公开征文,共收到投稿 16 篇. 论文均通过了形式审查, 内容涉及约束求解、定理证明以及它们的应用. 特约编辑先后邀请了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 2022 会议宣读和终审 4 个阶段, 最终有 6 篇论文入选本专题.

《基于不可满足核的近似逼近可达性分析》 提出了一种新型的基于不变式求解的可达性分析方法, 通过构造一系列单调的候选不变式从而最终逼近真实不变式, 实现了一个高效的安全性模型检查验证算法. 实验表明, 该方法对现有成熟的模型检查技术在性能上起到了补充的作用.

《GC-MCR: 有向图约束指导的并发缺陷检测方法》对用于并发缺陷检测的最大因果约减算法提出了一种改善方法, 使用有向图对检测过程中产生的约束进行过滤和约减, 以提高约束求解的速度并减少求解器的调用次数. 实验表明该方法在基准案例上使检测时间减少约 30%.

《基于精化的 TrustZone 多安全分区建模与形式化验证》在 Isabelle/HOL 定理证明器中构建了一个基于精化的 TrustZone 多安全分区形式化模型 RMTEE, 针对 FF-A 规范中存在的信息流安全隐患, 设计了分区间调用自主访问控制的安全增强机制, 最终验证了 RMTEE 模型精化关系以及事件接口的正确性和信息流安全性, 表明 RMTEE 模型符合机密性和完整性.

《L4 虚拟内存子系统的形式化验证》构建了 L4 微内核虚拟内存子系统的完整形式模型, 给出了该子系统的功能正确性、功能安全性和信息流安全属性等关键性质的形式化定义, 在 Isabelle/HOL 定理证明器中完成了形式化证明, 并发现了源代码中存在 3 个安全缺陷.

《针对教学场景的 ZFC 集合论 Coq 形式化》在 Coq 定理证明器中构造了一个更易于学习使用的集合论证明环境, 通过对正向推理模式的支持和自动证明策略, 允许更贴近教科书风格的证明. 在实际离散数学课程的教学应用中引入该工具取得了良好的效果.

* 收稿时间: 2023-01-05; jos 在线出版时间: 2023-01-06

《强表达描述逻辑本体的后继式公理定位研究》针对表达能力较强的描述逻辑本体，提出了基于一种后继式判定算法的公理定位方法，并证明了算法的正确性．进一步地，从白盒和黑盒两个角度设计了后继式公里定位的推理工具．

本专题主要面向约束求解和定理证明领域的研究人员和工程人员，本次录用论文反映了我国在约束求解和定理证明的应用方面最新的研究进展．感谢《软件学报》编委会和 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．希望本专题能够对约束求解与定理证明及其应用的研究工作有所促进．

蔡少伟(1986－)，男，博士，研究员，博士生导师，主持国家优秀青年科学基金项目，多次获得约束求解领域著名国际比赛包括 SAT 比赛和 SMT 比赛冠军，获得 SAT 2021 会议最佳论文奖．主要研究领域为约束求解，组合优化．

陈振邦(1981－)，男，博士，教授，博士生导师，主持国家自然科学基金多项，获 NASAC 青年软件创新奖、ACM SIGSOFT 杰出论文奖两次．主要研究领域为程序分析，形式化方法及其应用．

王戟(1969－)，男，博士，研究员，博士生导师，CCF 会士，CCF 形式化方法专委会主任．主要研究领域为高可信软件．

詹博华(1989－)，男，博士，副研究员，硕士生导师．主要研究领域为交互式定理证明，嵌入式系统的建模与验证．

赵永望(1979－)，男，博士，教授，博士生导师，移动终端安全技术浙江工程研究中心主任，CCF 杰出会员．主要研究领域为形式逻辑与验证，操作系统安全，编程语言原理．