推荐国家自然科学奖项目公示

项目名称	程序验证的基础理论研究
推荐单位	教育部

推荐单位意见：

我单位认真审阅了该项目公示材料，确认全部材料真实有效，相关栏目均符合国家自然科学奖材料的填写要求。

该项目建立了投影时序逻辑的模型理论和公理系统；提出了多核并发程序形式化模型，即柱面计算模型；解决了命题区间时序逻辑的判定难题；建立了基于区间的时序逻辑的复杂性和表达性理论。提出了集建模、仿真和验证为一体的并行程序设计语言MSVL的形式化语义，包括模型、操作和公理语义；建立了基于MSVL的统一验证理论，并开发了相应的支持工具。提出了高效的抽象模型检测、针对网络系统的状态空间缩减理论和分布式网络的验证算法，有效缓解了网络系统模型检测中的状态空间爆炸问题，提高了验证效率。项目成果得到了国内外同行专家的引用和好评，获得2015年度教育部自然科学一等奖。

该项目选题准确，理论上有创新，有重要的学术价值和理论意义，对学科建设和经济社会发展有重要的指导作用。

对照国家自然科学奖授奖条件，推荐该项目申报 2017 年国家自然科学奖一等奖。

项目简介：

如何保障软件系统的正确性和可靠性是计算机软件领域面临的重要挑战。图灵奖获得者 Clarke 等人提出的模型检测方法是迄今为止最成功的自动化程序验证方法之一。程序性质的描述、模型的提取以及检测算法是模型检测的三要素，但是在这三方面均存在一些亟待解决的问题：（1）性质描述语言表达能力不足；（2）系统模型难以提取；（3）状态空间爆炸。针对这些问题，本项目提出了一套基于时序逻辑的程序验证理论：用命题投影时序逻辑（PPTL）描述系统的性质，用投影时序逻辑统一验证技术使得系统和模型的描述在同一逻辑体系，用高效的抽象模型检测方法缩减状态空间，从三个方面克服程序验证的三个问题。具体创新点如下：

1、建立了投影时序逻辑 PTL 的模型理论，严格定义了 PTL 和 PPTL 的语法和语义，提出并证明了该逻辑的 182 个定理和 536 个逻辑规则；建立了 PTL 和 PPTL 的公理系统，并证明了其合理性和完备性；解决了 PPTL 和基于区间的命题时序逻辑 PITL 的判定问题；证明了基于区间的时序逻辑的非初等复杂性及 PPTL 的完全正则表达能力；提出了多核并发程序形式化模型，即柱面计算模型。

2、提出了以投影时序逻辑 PTL 可执行子集为基础的集建模、仿真和验证为一体的并行程序设计语言 MSVL，给出了 MSVL 的最小模型、操作和公理语义；解决了时序逻辑面向实际程序设计中的框架难题；建立了基于 MSVL 的统一验证理论，使得程序模型和性质的描述在同一逻辑体系，避免了程序验证中模型提取的困难。

3、提出了多项式抽象模型精化算法，避免了图灵奖获得者 Clarke 等人提出的精化方法中的指数爆炸；提出了线性虚假路径检测算法，缩减了图灵奖获得者 Clarke 等人提出的虚假反例路径检测的时间复杂度；提出了高效的网络系统模型状态空间缩减方法和分布式网络的验证算法，有效缓解了网络系统模型检测中的状态空间爆炸问题，提高了验证效率。

客观评价：

英国 Kent 大学著名学者 Bowman 和 Thompson 教授、加拿大滑铁卢大学 Peter R. King 和 Helen Cameron 教授对项目关于投影时序逻辑方面的贡献做了大段评论，他们指出段在以下方面发展了 ITL:（1）提出了过去操作,（2）定义了新的投影操作符,（3）研究了框架技术,（4）引入了无穷模型,（5）实现了并发和通信原语。项目在区间时序逻辑（ITL）理论方面所做的工作，得到了 ITL 的创始人 Ben Moszkowski 的引用好评。他指出本项目提出了命题投影时序逻辑在无穷区间的判定过程，研究了命题时序逻辑的理论和应用，它是 ITL 的扩展，有时序粒度和框架操作符。图灵奖获得者 Pnueli 曾指出现有的时序逻辑因仅限于全局的、非模块化的和非组合的系统验证而倍受指责。而 Moszkowski 指出本项目提出的投影时序逻辑支持过去操作，因此可以支持 Pnueli 期望的模块化分析方法。美国科学院院士 Moshe Y. Vardi 等人指出段等人提出了 PPTL 的范式和范式图，其中 PPTL 是 LTL 的超集；他们给出了可用于 PPTL 模型检测和可满足性检测的判定过程。西班牙巴斯克大学 Jose Gaintzarain 和 Paqui Lucio 指出段等人将 Tempura 方法扩展到框架 Tempura 和投影时序逻辑程序设计。德国马克斯普朗克计算机科学研究所 Katja Hose 和挪威科技大学 Akrivi Vlachou 指出本项目提出的 PaDSkyline 算法不仅用于 skyline 查询，而且可以更有效地处理带约束的 skyline 查询。日本东京大学 Shinichi Honiden 教授等人指出本项目提出的面向实际系统虚假反例分析方法是重要的。弗罗里达州立大学 Feifei Li 教授等人指出本项目提出的 iJoin 算法给出了最新结果。另外，德国奥登堡大学 Ernst-Rüdiger Olderog 教授、韩国科学技术信息研究所 Ryong Lee 以及日本京都产业大学 ShokoWakamiya 等人分别对本项目的成果给予了引用和好评。国家自然科学基金委员会信息科学部对国家自然科学基金重点项目“框架时序逻辑程序设计 60433010”进行了结题验收。专家组认为该项目按计划全面完成了研究任务，取得了很好的结果，综合评价为优。国家重点基础研究发展计划组织有关专家对 973 课题进行了结题验收，专家组评定该项目为优秀。

代表性论文专著目录：

[1] Duan Z. Temporal logic and temporal logic programming. Science Press, 2005.

[2] Duan Z.,Tian C, Zhang L. A decision procedure for propositional projection temporal logic with infinite models. Acta Informatica, 2008, 45(1): 43-78.

[3] Duan Z, Yang X, Koutny M. Framed temporal logic programming. Science of Computer Programming, 2008, 70(1): 31-61.

[4] Tian C, Duan Z, Zhang N. An efficient approach for abstraction-refinement in model checking. Theoretical Computer Science, 2012, 461: 76-85.

[5] Wu W, Du H, Jia X, et al. Minimum connected dominating sets and maximal independent sets in unit disk graphs. Theoretical Computer Science, 2006, 352(1): 1-7.

[6] Du H, Wu W, Ye Q, et al. CDS-based virtual backbone construction with guaranteed routing cost in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(4): 652-661.

[7] Lu R, Du H, Jia X, et al. A greedy approximation for minimum connected dominating sets. Theoretical Computer Science, 2004, 329(1): 325-330.

[8] Cui B, Lu H, Xu Q, et al. Parallel distributed processing of constrained skyline queries by filtering, IEEE 24th International Conference on Data Engineering (ICDE 2008), 546-555.

主要完成人情况：

1. 段振华，排名 1，无，教授，工作单位：西安电子科技大学，完成单位：西安电子科技大学，是该项目主要负责人，对发现点 1、2、3 均有重要贡献，具体包括建立了投影时序逻辑的模型理论和公理系统，建立了 MSVL 语言及其语义，提出了高效的抽象模型检测方法
2. 田聪，排名 2，无，教授，工作单位：西安电子科技大学，完成单位：西安电子科技大学，对发现点 1、3 均有重要贡献，具体包括证明了命题投影时序逻辑的可判定性并提出了高效的抽象模型检测理论和方法
3. 堵宏伟，排名 3，无，副教授，工作单位：哈工大深圳研究生院，完成单位：哈工大深圳研究生院，对发现点 3 有重要贡献，提出了针对网络系统的状态空间缩减理论
4. 崔斌，排名 4，无，研究员，工作单位：北京大学，完成单位：北京大学，对发现点 3 有重要贡献，提出了针对分布式网络的验证理论和方法
5. 张南，排名 5，无，副教授，工作单位：西安电子科技大学，完成单位：西安电子科技大学，对发现点 1 有重要贡献，提出了投影时序逻辑的公理系统及多核并行计算模型

完成人合作关系说明：

项目提出的基于时序逻辑的程序验证理论在对分布式网络系统进行验证时效率较低。崔斌研究员一直致力于分布式网络的研究，并取得了一系列优秀研究成果。因此，课题组于 2006 年起与崔斌研究员合作，双方经过多次研讨，提出了带约束的并行分布式 skyline 查询算法，可以对大规模的数据和网络进行高效分布式查询，提高了分布式系统的验证效率，并合作发表了“Satisfiability of Linear Time Mu-Calculus on Finite Traces”等文章。此外，课题组与崔斌研究员合作承担并完成了三项中国航天科技集团公司第五研究院第五〇二研究所的横向课题，取得了良好的合作效果。

项目提出了一套基于时序逻辑的程序验证理论。研究期间，针对特定网络系统的形式化验证碰到了严重的状态空间爆炸问题。堵宏伟副教授当时所在的香港城市大学课题组在这一方面有很好的研究基础。因此，课题组于 2004 年开始同香港城市大学课题组合作，期间堵宏伟作为香港城市大学的在读博士生长期往返于香港城市大学和西安电子科技大学之间，参与了项目组主持的多项自然基金课题，双方进行交叉合作，提出了改进的基于构建极大独立集的近似算法，使得构建最小联通支配集的效率得到提升；提出了一个创新的多项式时间常数近似算法，得到一个规模小且路由代价小的联通支配集，有效缩减网络软件系统模型检测中的状态空间，提高了验证效率。2010 年，堵宏伟以骨干成员的身份加入了西安电子科技大学可信软件创新团队，针对 SAT 求解问题提出了基于聚类和划分的分治算法，极大地改善了求解效率，合作发表了“Clustering and Partition Based Divide and Conquer for SAT Solving”等多篇文章。

知情同意证明：

IOWA STATE UNIVERSITY

To whom it may concern

16th May 2016

Certification

I hereby agree that the following journal paper:

Lu Ruan, Hongwei Du, Xiaohua Jia, Weili Wu, Yingshu Li, Ker-I Ko, A Greedy Approximation for Minimum Connected Dominating Sets, Theoretical Computer Science, 329(1-3): 325-330, December 2004.

be used in an application for the National Natural Science Award of the People's Republic of China by the second named author of the paper, my co-author, Associate Professor Hongwei Du of Harbin Institute of Technology Shenzhen Graduate School. I confirm that the main idea of the paper was given by him.

Sincerely yours,

Lu Ruan

Lu Ruan

Associate Professor Lu Ruan
Department of Computer Science
Iowa State University
USA

Newcastle University

To whom it may concern

16th May 2016

Certification

I hereby agree that the following journal paper:

Zhenhua Duan, Xiaoxiao Yang, Maciej Koutny: Framed temporal logic programming. Science of Computer Programming, Vol. 70, pp 31-61, Oct. 2007.

be used in an application for the National Natural Science Award of the People's Republic of China by the first named author of the paper, my co-author, Professor Zhenhua Duan of Xidian University. I confirm that the main idea of the paper was given by him.

Yours faithfully,

Maciej Koutny

Professor Maciej Koutny
School of Computing Science
Newcastle University
NE1 7RU
United Kingdom

CityU
香港城市大學
City University of Hong Kong
專業 創新 與心全球
Professional·Creative
For The World

To whom it may concern

16th May 2016

Certification

I hereby agree that the following journal paper:

Weili Wu, Hongwei Du, Xiaohua Jia, Yingshu Li, Scott C.-H. Huang: Minimum connected dominating sets and maximal independent sets in unit disk graphs. Theoretical Computer Science, 352(1-3): 1-7 (2006)

be used in an application for the National Natural Science Award of the People's Republic of China by the second named author of the paper, my co-author, Associate Professor Hongwei Du of Harbin Institute of Technology Shenzhen Graduate School. I confirm that the main idea of the paper was given by him.

Yours faithfully,

Xiaohua Jia

Professor Xiaohua Jia
Department of Computer Science
City University of Hong Kong
China

THE UNIVERSITY OF TEXAS AT DALLAS

To whom it may concern

16th May 2016

Certification

I hereby agree that the following two journal papers:

1) Weili Wu, Hongwei Du, Xiaohua Jia, Yingshu Li, Scott C.-H. Huang: Minimum connected dominating sets and maximal independent sets in unit disk graphs. Theoretical Computer Science, Vol. 352, pp 1-7, Mar. 2006.
2) Hongwei Du, Weili Wu, Qiang Ye, Deying Li, Wonjun Lee, Xuepeng Xu: CDS-based virtual backbone construction with guaranteed routing cost in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, Vol. 24, pp 652-661, Apr. 2013.

be used in an application for the National Natural Science Award of the People's Republic of China by my co-author, Associate Professor Hongwei Du of Harbin Institute of Technology Shenzhen Graduate School. I confirm that the idea and the main part of both the two papers were given by him.

Yours faithfully,

Weili Wu

Professor Weili Wu
Department of Computer Science
University of Texas at Dallas
USA