北京市科学技术奖自然科学奖提名材料公示

一、项目编号

918-2022-Z001

二、项目名称

安全攸关控制系统形式验证基础理论与方法

三、提名意见：

“安全攸关控制系统形式验证基础理论与方法”由中国科学院软件研究所牵头，该项目围绕安全攸关控制系统形式验证面临可扩展性及能力等挑战，解决了安全攸关控制系统形式验证中的若干基础性难题，提出了通用高效验证方法，取得了多项原创性成果，推动了安全攸关控制系统形式验证理论的发展，并在实践中得到成功应用。该项目提出了非线性 Craig 插值生成理论，极大拓展了基于插值方法的各种验证技术的应用范围；建立了基于半代数不变式充要条件和凸差分解技术的高效微分不变式完备生成方法，解决了安全攸关控制系统形式验证中长期存在的验证能力与效率无法平衡的难题；发现并证明了目前表达能力最强的三类非线性微分动态系统可达性问题的可判定性。

该项目成果在 Information and Computation、SIAM Journal on Control and Optimization、IEEE Transactions on Automatic Control、Journal of Symbolic Computation、CAV、FM、TACAS、ISSAC 等计算机科学和控制领域的著名国际期刊/会议上发表学术论文 150 余篇，出版著作 5 部；受邀在重要国际会议做邀请报告 20 余次；成果成功应用于我国首次火星探测任务“天问一号”等重大工程。相关成果获得国际同行高度评价及推广，在国际上产生重要影响，成果他引 2000 多次，5 篇代表性论著合计他引 100 余次。

提名该项目为北京市科学技术奖自然科学奖 一等奖。

四、项目简介：

该项目围绕开放环境下安全攸关控制系统形式验证问题开展前沿研究，取得多项重要成果，为安全攸关控制系统验证奠定了理论基础。主要科学发现包括：针对安全攸关控制系统形式验证可扩展性瓶颈，解决了非线性插值生成难题，推动了插值方法与已有各种验证技术结合；针对基于演绎验证方法面临的挑战，解决了一般半代数归纳不变式高效生成难题；针对基于可达集计算的验证方法面临的挑战，发现了三类非线性动态系统并证明了其可达性是可判定的。详述如下： 1. 创立了非线性 Craig 插值生成理论：根据 Positivstellensatz 定理及半定规划，提出了首个非线性 Craig 插值生成方法；证明了二次凹多项式不等式是可线性化的，从而给出非线性理论与含未解释函数等式逻辑（EUF）等理论组合的 Craig 插值生成算法；利用实代数几何和控制优化理论，建立了阿基米德条件下非线性插值的完备且高效的生成方法。上述结果显著提升了现有各种验证技术的可扩展性。 2. 建立了完备的半代数不变式生成理论：提出了在保证栅栏函数凸性条件下栅栏函数条件松弛的统一框架，首次实现了组合栅栏函数的构造，实质性拓展了栅栏函数的应用范围；建立了第一个弱完备的栅栏函数条件，揭示了栅栏函数方法在微分动态系统形式验证中的能力极限；利用凸差分解技术解耦双线性约束，实现了微分动态系统半代数不变式的高效生成，为计算机科学中普遍存在的双线性约束求解问题提供了理论支

撑。 3. 发现了三类目前表达能力最强且具有可判定可达性的动态系统：研究了著名的 Tarski 指数理论猜想，提出了一类特殊形式指数多项式理论的判定算法；基于此，发现了三类带有非线性输入（可能含超越函数）的线性向量场，证明了其可达性问题是可判定的，并将可判定性推广至三类具有可解性的非线性向量场。它们是目前具有可判定可达性的动态系统中表达能力最强的，拓展了动态系统可达性分析的理论边界。 该项目成果在 Information and Computation、SIAM Journal on Control and Optimization、IEEE Transactions on Automatic Control、Journal of Symbolic Computation、CAV、FM、ISSAC 等计算机科学和控制领域的著名国际期刊/会议上发表学术论文 150 余篇，出版著作 5 部；受邀在重要国际会议做邀请报告 20 余次；成果成功应用于我国首次火星探测任务“天问一号”等重大工程。相关成果获得国际同行高度评价及推广，在国际上产生重要影响，5 篇代表性论著合计他引 100 余次。

五、候选人

詹乃军、夏壁灿、顾斌、甘庭、陈明帅、王淑灵、代立云、李晓锋、 詹博华。

六、候选单位

中国科学院软件研究所，北京大学，北京控制工程研究所，武汉大学、浙江大学。

七、主要支撑材料目录

代表作发表情况（限 5 篇）

序号	代表作名称	刊名/出版社	发表时间	通讯作者	第一作者	全部作者	第一署名单位	年卷期页码
1	Generating Non-linear Interpolants by Semidefinite Programming	CAV 2013：25th International Conference on Computer Aided Verification	2013-07-13	代立云，夏壁灿，詹乃军	代立云	代立云，夏壁灿，詹乃军	北京大学	364-380
2	Nonlinear Craig Interpolant Generation	CAV 2020：32nd International Conference on Computer-Aided Verification	2020-07-21	夏壁灿，詹乃军	甘庭	甘庭，夏壁灿，薛白，詹乃军，代立云	武汉大学	415-438
3	Barrier certificates revisited	Journal of Symbolic Computation	2017-05-01	代立云，甘庭，夏壁灿，詹乃军	代立云	代立云，甘庭，夏壁灿，詹乃军	北京大学	80: 62-86
4	Reachability Analysis for Solvable Dynamical Systems	IEEE Transactions on Automatic Control	2018-07-01	夏壁灿，詹乃军	甘庭	甘庭，陈明帅，李杨佳，夏壁灿，詹乃军	武汉大学	63(7): 2003-2018
5	Brief Industry Paper: Modeling and Verification of Descent Guidance Control of Mars Lander	RTAS2021: IEEE 27th Real-Time and Embedded Technology and Applications Symposium	2021-5-18		詹博华	詹博华，顾斌，徐雄，金翔宇，王淑灵，薛白，李晓锋，陈尧，杨孟飞，詹乃军	中国科学院软件研究所	457-460

代表作被他人引用、应用情况（限 5 篇）

序号	引文名称/引文作者	引文刊名	引文发表时间 （年 月 日）
1	A Survey of Satisfiability Modulo Theory/ David Monniaux	Proceedings of the 18th International Workshop on Computer Algebra in Scientific Computing (CASC 2016)	2016-09-09
2	Sharper and Simpler Nonlinear Interpolants for Program Verification/ Takamasa Okudono，Yuki Nishida，Kensuke Kojima，Kohei Suenaga，Kengo Kido，Ichiro Hasuo	Proceedings of the 15th Asian Symposium on Programming Languages and Systems (APLAS 2017)	2017-11-01
3	Robustness of Control Barrier Functions for Safety Critical Control/ Xiangru Xu，Paulo Tabuada，Jessy W Grizzle，Aaron D Ames	IFAC 2015	2015-10-14
4	Pegasus: sound continuous invariant generation/ Andrew Sogokon，Stefan Mitsch，Yong Kiam Tan，Katherine Cordwell，Andre Platzer	Formal Methods in System Design	2021-01-20
5	Adaptive reachability algorithms for nonlinear systems using abstraction error analysis	Nonlinear Analysis: Hybrid Systems	2022-11-01