第一届全国形式化方法与应用会议
（FMAC 2016）

主办：中国计算机学会

承办：中国计算机学会形式化方法专业组

中国科学院软件研究所

2016 年 11 月 12 日-13 日

北京

第一届全国形式化方法与应用会议
（FMAC 2016）
会议介绍

形式化方法以严格的数学化和机械化方法为基础来规约、构建和验证计算系统，是改善和确保计算系统质量的重要方法，其模型、技术和工具已延生成为计算思维的重要载体。

中国计算机学会形式化方法专业委员会成立于 2015 年 11 月，将立足于形式化方法核心内容，深化拓展形式化方法与相关领域的交叉，加强学术界与工业界合作，在科学研究、人才培养、国际交流、应用实践等方面努力开展卓有成效的工作，促进形式化方法在中国的发展。

第一届全国形式化方法与应用会议（FMAC 2016）由中国计算机学会主办，形式化方法专业委员会和中国科学院软件研究所承办，于 2016 年 11 月 12 日至 13 日在北京举行，并与 SETTA 2016 同地举办。大会将设置特邀报告、论文报告、专题论坛、青年学者论坛、墙贴报告等多种学术交流形式，会议还与《软件学报》等合作组织专题特约报告，为与会代表提供丰富的交流平台。会议特别欢迎形式化方法与理论计算机科学、软件工程、系统软件、嵌入式系统、网络与信息安全、人工智能等学科和领域交叉结合的研究成果和论文。会议征稿范围包括：

- 形式化方法的基础理论：与规约、验证、精化、静态与动态分析等相关的形式化理论
- 形式化方法的技术和工具：形式化方法支持的自动分析、模型检验、定理证明、系统设计与综合等技术和工具
- 形式化方法的应用与实践：形式化方法、技术和工具在实际中应用与实证研究、形式化方法与软件和系统工程的过程集成、方法集成和环境集成等
- 形式化方法的多学科交叉：形式化方法在多学科交叉（如控制科学、智能科学和生命科学）框架下的技术、工具和运用等
- 形式化方法的教育：形式化方法在大学课程和继续教育与培训中的作用、实践与经验

会议推荐部分优秀论文到《中国科学》（中英文版）、《International Journal of Software and Informatics》和《计算机学报》等期刊发表，会议其它收录论文将在《计算机工程与科学》上发表。

大会主席

林惠民　　中国科学院软件研究所，中国科学院院士

程序委员会主席

王　戟　　国防科学技术大学
李宣东　　南京大学

程序委员会

陈铭松　　华东师范大学
董云卫　　西北工业大学
方　菱　　中国科学院合肥物质分院
冯新宇　　中国科学技术大学
顾　斌　　北京控制工程研究所
关　楠　　香港理工大学
关　永　　首都师范大学
胡　宁　　中航工业西安航空计算技术研究所
贺　飞　　清华大学
金乃永　　新思科技
孔维强　　大连理工大学
李国强　　上海交大
李晓红　　天津大学
李宣东　　南京大学
李　智　　广西师范大学
刘　剑　　中国科学院信息工程研究所
刘　江　　中国科学院重庆绿色智能技术研究院
吕　帅　　吉林大学
孙　猛　　北京大学
田　聪　　西安电子科技大学
王　戟　　国防科学技术大学
王生原　　清华大学
魏　欧　　南京航空航天大学
吴尽昭　　广西民族大学
吴志林　　中国科学院软件研究所
肖美华　　华东交通大学
熊英飞　　北京大学
杨红丽　　北京工业大学
詹乃军　　中国科学院软件研究所
张广泉　　苏州大学

张　健　　中国科学院软件研究所
张苗苗　　同济大学
张兴元　　解放军理工大学
赵永望　　北京航空航天大学
周清雷　　郑州大学

组织委员会

王淑灵　　中国科学院软件研究所
吴　鹏　　中国科学院软件研究所
吴志林　　中国科学院软件研究所

FMAC 2016 会议程序

2016 年 11 月 12 日		
7:30am - 8:15 am	注册（中科院软件园区五号楼 4 层裙楼电梯口）	
8:15am - 8:30 am	开幕式（中科院软件园区五号楼 4 层大报告厅）	
	主持：詹乃军	
8:30am - 9:30 am	特邀报告（中科院软件园区五号楼 4 层大报告厅）	
	主持：王义	
	Deepak Kapur (University of New Mexico) Automatic Generation of Program Invariants from Traces	
9:30am - 10:00am	茶歇/墙贴报告	
10:00pm - 12:00pm	分组：自动机与逻辑 （中科院软件园区五号楼 4 层大报告厅）	YR-SETTA: Special Session （中科院软件园区五号楼 4 层第 4 会议室）
	主持：魏欧	Session Chair: Lijun Zhang
	Guoqiang Li, Yunqing Wen and Shoji Yuen: Updatable Timed Automata with One Updatable Clock	Yuting Chen: Coverage-Directed Differential Testing of JVM Implementations
	Fu Song, Min Zhang, Wanwei Liu and Yusi Lei: On the Complexity of ω-Pushdown Automata	Fengwei Xu, Ming Fu, Xinyu Feng, Xiaoran Zhang, Hui Zhang and Zhaohui Li: A Practical Verification Framework for Preemptive OS Kernels
	Jianhua Zhao and Xuandong Li: Formal Verification of `Programming to Interfaces' Programs	Yu-Fang Chen, Ondrej Lengal, Lei Song, Tony Tan and Zhilin Wu: The Commutativity Problem of the MapReduce Framework: A Transducer-based Approach
	Gang Chen: Second Order Bounded Quantification with If-expression	Andrea Turrini: A Simple Algorithm for Solving Qualitative Probabilistic Parity Games
12:00pm - 1:00pm	午餐	
1:00pm - 3:30pm	软件学报专刊：规约与分析 （中科院软件园区五号楼 4 层大报告厅）	YR-SETTA: System Analysis and Runtime Verification （中科院软件园区五号楼 4 层第 4 会议室）

	主持：董威	Session Chair: Zhilin Wu
	王善侠,马明辉,陈武,邓辉文： 正则模型类的时态可定义性	Zhe Chen, Zhemin Wang, Yunlong Zhu, Hongwei Xi and Zhibin Yang: Parametric Runtime Verification of C Programs
	常曦,薛建新,张卓,毛晓光： 面向收敛的并发程序执行轨迹静态简化方法	Xueguang Wu and Liqian Chen: Numerical Static Analysis of Embedded Software with Interrupts
	翟娟,汤震浩,李彬,赵建华,李宣东： 循环摘要的自动生成方法及其应用	Xin Li, Yongjuan Liang, Hong Qian, Yiqi Hu, Lei Bu, Yang Yu, Xin Chen and Xuandong Li: Symbolic Execution of Complex Program Driven by Machine Learning Based Constraint Solving
	刘立,李国强： 异步多进程时间自动机及其可覆盖性问题	Fan Ming and Ting Liu: Android Malware Detection and Family Identification through Frequent Subgraph
	李轶,冯勇： 一类多项式循环程序的终止性分析	Yingxia Wei, Rui Wang and Yu Jiang: From Off-line Towards Real-time : A Runtime Verification Approach for Robot Systems
	文习明,余泉,常亮,王驹： 不确定观测下离散事件系统的可诊断性	Yueling Zhang, Min Zhang, Geguang Pu, Fu Song and Jianwen Li: Towards Backbone Computing: A Greedy-Whitening Based Approach
3:30pm - 4:00pm	茶歇/墙贴报告	
4:00pm - 6:30pm	软件学报专刊：验证与测试 （中科院软件园区五号楼 4 层大报告厅）	YR-SETTA: Model Checking and Theorem Proving （中科院软件园区五号楼 4 层第 4 会议室）
	主持：董云卫	Session Chair: Fei He
	刘涛,詹乃军,王淑灵： 多机器人路径规划的安全性验证	Bingqing Xu and Qin Li: A Spatial Logic for Modeling and Verification of Collision-free Control of Vehicles
	张雨,董云卫,冯文龙,黄梦醒： 一种面向 CPS 的控制应用程序协同验证方法	Chunmiao Li and Xiaojuan Cai: Hardness Results for Coverability Problem of Well-Structured Pushdown Systems
	李晅松,陶先平,吕建,宋巍： 面向动作的上下文感知应用的规约与运行时验证	Yuwei Wang and Guoqiang Li: On Termination and Boundedness of Nested Updatable Timed Automata
	杜德慧,咎慧,姜凯,强程贝： 基于抽象和学习的统计模型检测方法研究	Xiuting Tao, Chihao Zhang and Guoqiang Li, The Complexity of a Modifiable Model Checking of Linear Temporal Logic
	赵岭忠,冯于平,钱俊彦,常亮,古天龙：	Xiyue Zhang, Weijiang Hong, Yi Li and Meng Sun:

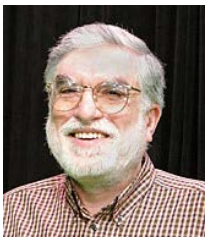
	基于 ASP 的 CSP 并发系统模型检测与调试技术研究	Reasoning about Connectors in Coq
		Gaogao Yan, Li Jiao, Yangjia Li, Shuling Wang and Naijun Zhan: Approximate Bisimulation and Discretization of Hybrid CSP
6:50pm - 8:10pm	会议宴会	
8:30pm – 10:00pm	CCF 形式化方法专业组会议	
2016 年 11 月 13 日		
8:30am - 9:30 am	特邀报告（中科院软件园区五号楼 4 层大报告厅）	
	主持：傅育熙	
	Joost-Pieter Katoen (RWTH Aachen University, Germany) Run-Time Analysis of Probabilistic Programs	
9:30am - 10:00am	茶歇	
10:00pm - 12:00pm	分组：分析与验证 （中科院软件园区五号楼 4 层大报告厅）	软件学报专刊：面向领域的形式化方法 （中科院软件园区五号楼 4 层第 4 会议室）
	主持：刘剑	主持：吕鸣松
	Kaiqiang Jiang, Ping Huang, Hui Zan and Dehui Du: AL-SMC: Optimizing Statistical Model Checking by Automatic Abstraction and Learning	鲍勇翔,陈铭松,孙海英,缪炜恺,陈小红,周庭梁: 基于通信的列车控制系统可信构造：形式化方法研究
	Haitao Zhang, Zhuo Cheng, Guoqiang Li and Shaoying Liu: autoC: an Efficient Translator for Model Checking Deterministic Scheduler based OSEK/VDX Applications	乔磊,杨孟飞,谭彦亮,蒲戈光,杨桦: 基于 Event-B 方法的航天器内存管理系统形式化验证
	阚双龙、黄志球、王飞: 嵌入偏序约简的状态事件时序逻辑验证	郭德贵,王冠成,吕帅,刘磊: peC 语言的部分求值器及在编译器测试中的应用
	姜加红、尹帮虎、陈立前: 基于区间线性模版约束的程序分析	宋建功,吕舜,李勤勇,马世龙,吕江花: 地震应急响应阶段任务系统自动化联调测试
		尚书,甘元科,石刚,王生原,董渊: 可信编译器 L2C 的核心翻译步骤及其设计与实现
12:00pm - 1:30pm	午餐	
1:30pm - 3:00pm	Panel：形式化方法教育（中科院软件园区五号楼 4 层大报告厅）	

	主持：朱惠彪
	朱惠彪、张广泉、裘宗燕等
3:00pm - 3:30pm	茶歇
3:30pm – 4:50pm	青年学者报告（中科院软件园区五号楼 4 层大报告厅）
	主持：王戟
	田聪（西安电子科技大学）：Model Checking via Dynamic Program Execution
	贺飞（清华大学）：Learning-based Assume-Guarantee Verification
4:50pm – 5:00pm	闭幕式（中科院软件园区五号楼 4 层大报告厅）
6:00pm – 7:00pm	晚餐

墙贴报告

1. Mingshuai Chen: Validated Simulation-Based Verification of Delayed Differential Dynamics
2. Chunmiao Li and Xiaojuan Cai: On Hardness of Recursive Integer Program Analysis
3. 丁泽文、黄志球、阚双龙，张 弛：一个基于两区间八边形约束的抽象域
4. 罗炜麟、魏欧、黄鸣宇：基于 SAT 的故障树最小割集求解算法
5. 龙腾、许智武：基于限界约束的安全相关性质的推理证明
6. 陈 松、胡 军、王明明：一种基于 SPIN 的 AltaRica 3.0 模型转换与验证方法研究
7. 陈英杰、陈振邦、董威：基于性质制导符号执行的 Linux 驱动程序缺陷检测研究

特邀报告：**Deepak Kapur**



Deepak Kapur, a distinguished professor at the University of New Mexico (UNM) since 1998. Kapur got his PhD degree in computer science from MIT in 1980, and before that he got M. Tech. (1973) and B. Tech. (1971) from Indian Institute of Technology (IIT). He served as chair of the Department of Computer Science in UNM from Dec. 1998 to June 2006. He has adjunct appointments at IIT, Delhi, India, as well as Tata Institute of Fundamental Research, Mumbai, India. From 1980-1987, he was on the research staff of General Electric Corporate Research and Development, Schenectady, NY. He was appointed tenured full professor at the University at Albany, SUNY, and Albany, NY, in 1988, where he also founded the Institute for Programming and Logics. He has had research collaborations all over the world including TIFR, India; MPI, Saarbrucken, Germany; Chinese Academy of Sciences, Beijing; IMDEA, Madrid, and UPC, Barcelona; Naval Research Lab, Washington. He serves on the editorial boards of numerous journals including the Journal of Symbolic Computation and Journal of Automated Reasoning, for which he also served as the editor-in-chief from 1993-2007. Kapur is on the board of United Nations University-International Institute for Software Technology as well as LIPIcs: Leibniz International Proceedings in Informatics. Kapur was honored with the Herbrand Award in 2009 for distinguished contributions to automated reasoning.

Title: Automatic Generation of Program Invariants from Traces

Abstract:

An effective approach for generating program invariants by dynamic analysis will be presented. Nonlinear equality and inequality invariants are shown to be generated automatically from observed program traces. The approach also considers invariants involving the array data structure, including relations among multi-dimensional array variables. These properties are nontrivial and challenging for current static and dynamic invariant analysis methods. More recently, methods have been developed to derive disjunctive invariants in which disjunctions are specified using max and min functions. The approach has been implemented as a software tool call DIG (Dynamic Invariant Generator). The key difference between DIG and existing dynamic methods such as DAIKON is its generative technique, which infers invariants directly from traces, instead of using traces to filter out pre-defined templates. Experimental results on numerical algorithms and an implementation of AES encryption provide evidence that DIG is effective at generating invariants for these programs.

This work is part of ThanhVu Nguyen's Ph.D. dissertation research.

特邀报告：Joost-Pieter Katoen

Joost-Pieter Katoen is part-time professor at the University of Twente (NL), and full-time professor at the RWTH Aachen University (Germany). Since 2013, he is a distinguished professor in Aachen and is member of the Academia Europaea. He is chair of the steering committee of ETAPS, Europe's largest conference on software theory and practice. He is an internationally recognized expert in the field of stochastic model checking and co-authored more than 200 publications (cited more than 13,000 times). He is senior member of the ACM, IFIP WGs 2.2 and 1.8, chaired a number of top conferences in the field, is steering committee member of several key conferences, and acted as keynote speaker at conferences such as LICS, CAV, ATVA, CONCUR and FM.

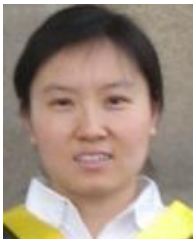
Title: Run-Time Analysis of Probabilistic Programs

Abstract:

This talk presents a weakest-precondition style reasoning a la Dijkstra for determining (bounds on) the expected run-time of probabilistic programs. Its application includes determining the (possibly infinite) expected termination time of a randomised algorithm and proving positive almost-sure termination: does a program terminate with probability one in finite expected time?

I'll present several proof rules for bounding the run-time of loops, and prove the soundness of the approach with respect to a simple operational model. The approach is shown to be a conservative extension of Nielson's approach for reasoning about the run-time of deterministic programs. It is shown how this wp-calculus can be applied to the well-known coupon collector benchmark, a case study covered by Erdös in the 1960s.

青年学者报告：田聪



田聪，博士，西安电子科技大学计算机学院教授。从事程序的形式化验证领域的研究工作。在相关领域国际期刊/会议(TSE，ICSE，TCS，和 IJCAI 等)发表论文 100 余篇。获国家自然科学基金优秀青年基金和教育部新世纪优秀人才计划资助。获陕西省科学技术一等奖和教育部自然科学一等奖。

Title: Model Checking via Dynamic Program Execution

Abstract:

This talk presents a unified model checking approach where the program to be verified is written in a Modeling, Simulation and Verification Language (MSVL) program M and the desired property is specified with a Propositional Projection Temporal Logic (PPTL) formula P. Different from the traditional model checking approach, the negation of the desired property, is translated into an MSVL program M' first. Then whether M violates P can be checked by evaluating whether there exists a feasible execution of the new MSVL program (M and M'). This problem can be efficiently conducted with the compiler of MSVL namely MSV. The proposed approach has been implemented in a tool called UMC4MSVL which is capable in verifying real-world programs.

青年学者报告：贺飞

贺飞，博士，清华大学副教授。2002 年 7 月毕业于国防科技大学计算机学院，获工学学士学位；2008 年 1 月毕业于清华大学计算机系，获工学博士学位。自 2008 年起于清华大学软件学院任教。主要研究方向为形式化验证理论及其在嵌入式系统、软件系统中的应用。

Title: Learning-based Assume-Guarantee Verification

Abstract:

Both symbolic model checking and assume-guarantee reasoning aim to circumvent the state explosion problem. Symbolic model checking explores many states simultaneously and reports numerous erroneous traces. Automated assume-guarantee reasoning, on the other hand, infers contextual assumptions by inspecting spurious erroneous traces. One would expect that their integration could further improve the capacity of model checking. Our technique successfully integrates symbolic model checking with automated assume-guarantee reasoning by directly inferring BDD's as implicit assumptions. A regressional assume-guarantee verification framework is further proposed to cope with the many revisions of an evolving system.

FMAC 2016 宴会地点：眉州东坡酒楼（中关村店）

地址：北京市海淀区中关村大街 27 号中关村大厦二层

地图：从 中科院软件所 到 眉州东坡酒楼（中关村店）