



Selected Extended Papers of NFM 2017: Preface

Clark Barrett¹  · Temesghen Kahsai²

Received: 12 October 2018 / Accepted: 15 October 2018 / Published online: 20 October 2018
© Springer Nature B.V. 2018

This special issue consists of extended versions of papers selected from the 9th NASA Formal Methods Symposium (NFM 2017). The symposium was held at the NASA Ames Research Center, Moffett Field, CA, on May 16–18, 2017.

NFM is a forum to foster collaboration between theoreticians and practitioners from NASA, academia, and industry, with the goal of identifying challenges and providing solutions to achieving assurance in mission- and safety-critical systems. Examples of such systems include advanced separation assurance algorithms for aircraft, next-generation air transportation, autonomous rendezvous and docking for spacecraft, autonomous on-board software for unmanned aerial systems (UAS), UAS traffic management, autonomous robots, and systems for fault detection, diagnosis, and prognostics. The topics covered by the NASA Formal Methods Symposium include: model checking, theorem proving, SAT and SMT solving, symbolic execution, automated testing and verification, static and dynamic analysis, model-based development, runtime verification, software and system testing, safety assurance, fault tolerance, compositional verification, security and intrusion detection, design for verification and correct-by-design techniques, techniques for scaling formal methods, formal methods for multi-core GPU-based implementations, generation, specification, and validation of requirements, human-machine interaction analysis, certification, and applications of formal methods in systems development.

Five papers from NFM 2017 were selected for this special issue (out of 31 papers presented at the conference) based on their technical quality. The authors of these papers were invited to submit extended versions of their papers, each of which underwent a new and thorough reviewing and revision process, ensuring that the accepted articles do indeed extend and improve the symposium submissions.

The first article, “Verifying Safety and Persistence in Hybrid Systems using Flowpipes and Continuous Invariants,” by Andrew Sogokon, Paul Jackson, and Taylor T Johnson, presents a new approach for verifying hybrid systems that combines flow-pipe computation with deductive reasoning. The second article, “Compositional Falsification of Cyber-Physical Systems with Machine Learning Components,” by Tommaso Dreossi, Alexandre Donz, and Sanjit

✉ Clark Barrett
barrett@cs.stanford.edu

Temesghen Kahsai
temesghen-kahsaiazene@uiowa.edu

¹ Stanford University, Stanford, CA 94305, USA

² University of Iowa, Iowa City, IA 52242, USA

Seshia, uses abstraction and compositionality to tackle the problem of verifying a closed-loop system containing machine learning components. The third article, “Explaining AI Decisions Using Efficient Methods for Learning Sparse Boolean Formulae,” by Susmit Jha, Tuhin Sahai, Vasumathi Raman, Alessandro Pinto, and Michael Francis, presents two novel algorithms for learning sparse Boolean formulae that correspond to explanations for decisions made by an AI algorithm. Such explanations help address a major barrier to the adoption of AI in safety-critical systems. The fourth article, “An Automata-Theoretic Approach to Model Checking Systems and Specifications Over Infinite Data Domains,” by Hadar Frenkel, Orna Grumberg, and Sarai Sheinvald, presents an automata-theoretic approach to VLTL (LTL with quantified variables) model checking. The paper defines Alternating Variable Buchi Word Automata, a new automata model over infinite alphabets which combines alternation with variable automata over infinite words. Last but not least, the fifth article, “Efficient Active Automata Learning via Mutation Testing,” by Bernhard K. Aichernig and Martin Tappler, presents a novel technique for test-case generation for testing conformance between a system and a model learned from it.

We are very grateful for everyone who contributed to make this special issue possible, starting with the steering committee, participants, and program committee of NFM 2017. We would especially like to thank the authors for their contributions and the reviewers for their thoughtful and thorough comments. We also thank Tobias Nipkow, editor in chief of the *Journal of Automated Reasoning*, for his invitation to prepare this special issue and for his assistance during the process.