https://doi.org/10.1007/s00165-021-00552-5
BCS © 2021
Formal Aspects of Computing (2021) 33: 299–300

Formal Aspects of Computing

Editorial

Xiaoping Chen[1], Zhiming Liu[2], Ji Wang[3], Jim Woodcock[4]

[1]School of Computer, University of Science and Technolog, Anhui, China
[2]School of Software, Northwest Polytechnical University, Xi'an, China
[3]State Key Laboratory of High Performance Computing, University of National Defence Technology, Changsha, China
[4]Department of Computer Science, University of York, York, UK

Formal methods emerged as a discipline in computer science and software engineering half a century ago. Mathematics and logic underpin formal methods and provide the foundations for software development. This includes research on mathematical models, composition and adaptation, and rigorous approaches to verification, deployment, testing, and certification. These all remain active research areas. Difficulties remain in formulating requirements specifications. There is a lack of effective automation supporting formal refinement and verification in industrial projects. Recent advances of machine-learning-based artificial intelligence (AI), in both theory and applications, have been overwhelming. The formal methods community see the promise of AI and are now actively studying how it can help to improve the scalability of formal methods.

Artificial neural networks (ANN) are becoming more widely used in the implementation of autonomous intelligent control software in software-intensive systems. These systems are pervasive in our life, society, and all sectors of the economy and business. Many of these ubiquitous systems are human-cyber-physical systems (HCPS). They are safety and security-critical and demand high trustworthiness. Research is urgently needed to address the challenging problems of how to use ANNs safely and securely in engineering systems. These learning components must be interpretable, transferable, verifiable, controllable, and composable. Both the Formal Methods and AI communities believe that the models and verification techniques developed in formal methods will be a basis for this research.

The theme of this special issue is relating formal methods and AI. We invited and called for contributions to the modelling, design, and verification of ANNs. We especially welcomed papers related to HCPS and to applying ANNs to formal modelling and verification of systems for their scalability. We invited contributions from the speakers at two workshops. One was held at Southwest University (Chongqing, China) in October 2019, and the other at East China Normal University (Shanghai, China) in November 2019. This special issue includes the final version of six of the seven submitted manuscripts. They all underwent a thorough review process, with at least three referees. These papers cover different aspects of the theme originally proposed for the special issue.

Machine Learning Steered Symbolic Execution Framework for Complex Software Code by Lei Bu, et al. presents a framework, called MLBSE. This extends the classical symbolic execution framework with a machine-learning approach for constraint satisfaction. The approach samples and learns from different solutions to identify a potentially feasible area. This style of sampling-learning-solving is easily applicable to different classes of complex problems. When the solver fails on a path condition, it generates an estimation of the confidence in the satisfiability (ECS) of the problem. This gives users insights into how the problem is analysed and whether they could eventually find a solution. An implementation of MLBSE is given, based on Symbolic PathFinder (SPF), with promising evaluation results.

Correspondence to: Zhiming Liu e-mail: zliu@nwpu.edu.cn

SDLV: Verification of Steering Angle Safety for Self-Driving Cars by Huihui Wu, et al. presents an automated technique for verifying steering-angle safety for self-driving cars. The technique is an extension of an automated verification framework for the safety of image classification neural networks, called Deep Learning Verification (DLV). Two conditions are formulated to describe the deviation of operational output from the predicted output based on the input. These are called *slack conditions*. The technique then considers verification of steering-angle safety for self-driving cars by leveraging neuron coverage and slack conditions to solve the judgement problem of predicted behaviours. An evaluation of the techniques is given on NVIDIA's end-to-end self-driving architecture and the results show that the technique can successfully find adversarial misclassifications. That is, the technique can find incorrect steering decisions within given regions if they exist.

Exploiting Augmented Intelligence in the Modeling of Safety-Critical Autonomous Systems by Zhibin Yang, et al. proposes an approach to architectural modelling of safety-critical systems. The approach uses both conventional and machine learning (ML) components. The ML components are based on Augmented Intelligence (AuI) for restricted natural language requirements modelling. This allows several AI technologies, such as natural language processing and clustering, to be used to recommend candidate terms to the glossary, and machine learning to predict the category of requirements. A glossary is defined using the restricted natural language requirement specification, including a data dictionary, a domain glossary, and a category. Then an automatic generation of SysML architecture models from a restricted natural language requirement specification is presented. A prototype tool is implemented based on Papyrus, a tool for model-driven design. The approach and the tool are evaluated using an industrial Autonomous Guidance, Navigation and Control (AGNC) case study.

Inferring Switched Nonlinear Dynamical Systems by Bohua Zhan, et al. presents two algorithms for the identification problem for switched dynamical systems with polynomial ordinary differential equations. One is with prior segmentation of trajectories and the other is without. For methods with prior segmentation, they give a heuristic segmentation algorithm for inferring switched nonlinear dynamical systems algorithm. For methods without prior segmentation, they give an extension to the identification techniques for piecewise affine models for the problem. Also, Linear Multistep Methods are used to estimate derivatives along the given trajectories. Finally, the paper proposes how to compute a relative difference between the predicted and actual derivatives to evaluate an identified model.

Enhancing Robustness Verification for Deep Neural Networks via Symbolic Propagation by Pengfei Yang, et al. considers the problem of formal verification of robustness. It proposes a combination of complementary approaches. One of the approaches is use a novel symbolic propagation technique for analysing DNNs. The values of neurons are represented symbolically and propagated from the input layer to the output layer, on top of the underlying abstract domains. The other approach makes use of Lipschitz constants solved by semi-definite programming to prove global robustness of DNNs. It is also shown in the paper that the Lipschitz constant can be tightened if it is restricted to small regions. A tightened Lipschitz constant can be helpful in proving local robustness properties. The authors also show that the two approaches mutually benefit each other.

Learning Safe Neural Network Controllers with Barrier Certificates by Hengjun Zhao, et al. describes a new approach to synthesise controllers for nonlinear continuous dynamical systems with control against safety properties. The controllers are based on neural networks (NNs). To certify the safety property, barrier functions are used. These are also represented by NNs. The controller-NN and barrier-NN are trained simultaneously, achieving a verification-in-the-loop synthesis. A prototype tool *nncontroller* is implemented and illustrated with several case studies. The experiment results confirm the feasibility and efficiency of the approach.

We are grateful to *Formal Aspects of Computing* for allowing us to publish this collection of papers and in particular John Cooke for his help throughout the editorial process. We thank Annushrie Arravind for help with the Editorial Management System. Our special thanks go to the reviewers for their dedicated work and to the authors of the papers for their good cooperation.

Xiaoping Chen
Zhiming Liu
Ji Wang
Jim Woodcock

Accepted in revised form 19 May 2021
Published online 16 July 2021