https://doi.org/10.1007/s00165-021-00559-y

Formal Aspects of Computing (2021) 33: 459–460

Formal Aspects of Computing

Editorial

Annabelle McIver[1] and Maurice H. ter Beek[2]

[1]Department of Computing, Macquarie University, Sydney, Australia
[2]Istituto di Scienza e Tecnologie dell'Informazione Consiglio Nazionale delle Ricerche, Pisa, Italy

This special issue arose from the 3rd World Congress on Formal Methods held in Porto, Portugal in 2019. This is an event occurring every 10 years, and attracts scientists from all over the world to celebrate and exchange ideas on the technical advances made and real-world experiences of the formal analysis of systems applied across a diversity of applications. The 3rd World Congress was both an optimistic look into "The Next 30 Years" as well as an opportunity to reflect on the 30 years since the first VDM symposium in 1987 brought together researchers with the common goal of creating methods to produce high quality software based on rigour and reason.

This issue includes papers evolved from some of the best submissions to the 2019 Formal Methods Symposium (FM2019); which was part of the World Congress; FM 2019 attracted 129 submissions out of which 39 were accepted for presentation. A total of 18 papers were selected to be significantly extended to journal-length papers; nine of the selections appear here and the remaining nine appear in a parallel special issue published in Formal Methods in System Design. All papers underwent a thorough review process, requiring two to three rounds of revision.

An Axiomatic Approach to Existence and Liveness for Differential Equations by Yong Kiam Tan and André Platzer is a presentation of an axiomatic approach for deductive verification of existence and liveness for ordinary differential equations (ODEs) with differential dynamic logic (dL). The authors demonstrate their work by showing how to derive on a number of liveness arguments from the literature. Moreover these insights are put into practice through an implementation of ODE liveness proofs in the KeYmaera X theorem prover for hybrid systems.

Verification of Piecewise Deep Neural Networks: A Star Set Approach with Zonotope Pre-Filter by Hoang-Dung Tran et al. describes a new verification analysis for deep neural networks (DNNs) with piecewise linear activation function. The main concept is based around a collection of reachability algorithms using star sets which is an effective symbolic representation of high-dimensional polytopes. These reachability algorithms have been implemented and applied to problems analysing the robustness of machine learning methods, such as safety and robustness verification of DNNs.

Verifying Correctness of Persistent Concurrent Data Structures: A Sound and Complete Method by John Derrick, Simon Doherty, Brijesh Dongol, Gerhard Schellhorn and Heike Wehrheim concerns non-volatile memory (also called persistent memory); it is a new memory paradigm that preserves its contents even after power loss. The authors present a formal proof technique for "durable linearisability", a generalisation extending "linearisability" to enable reasoning about the scenario for recovery after crashes when memory can endure. The technique is illustrated on topical examples based on a persistent memory queue.

Correspondence to: Annabelle McIver, email: annabelle.mciver@mq.edu.au

L^*-Based Learning of Markov Decision Processes by Martin Tappler, Bernhard K. Aichernig, Giovanni Bacci, Maria Eichlseder and Kim G. Larsen is about using ideas from learning to apply to Markov Decision processes. A characteristic of active machine learning is the idea that a learner asks questions about topics she does not know about herself. Such active learning frameworks have been implemented as strategies to learn eg regular languages, and in this paper the authors use the idea for learning Markov decision processes. The authors look at scenarios where a teacher is able to provide exact answers, and secondly where the information must be collected by sampling.

Symbolic Execution Formally Explained by Frank S. de Boer and Marcello Bonsangue provides a formal explanation of symbolic execution in terms of a symbolic transition system. This enables a proof of correctness and completeness with respect to an operational semantics which models the execution on concrete values.

Counterexample-Guided Inductive Synthesis for Probabilistic Systems by Milan Ceska, Christian Hensel, Sebastian Junges and Joost-Pieter Katoen concerns the synthesis of probabilistic models using counterexample-guided inductive synthesis. The starting point is a family of finite-state Markov chains which can be described by a "program sketch" i.e. programs which are incomplete, with the missing components the comparison the key elements for their functionality. The authors study several quantitative synthesis problems in this space, including a feasibility, optimal synthesis, and complete partitioning.

Quantitative Verification of Kalman Filters by Alexandros Evangelidis and David Parker describes how to formally analyse Kalman filters. Kalman filters are widely used in engineered systems for estimating the state of a system based on noisy or inaccurate sensor readings. This paper addresses problems of errors arising in their use. The authors propose novel formal verification technique and software to perform a rigorous quantitative analysis of the effectiveness of Kalman filter implementations.

From Generic Partition Refinement to Weighted Tree Automata Minimization by Thorsten Wißmann, Hans-Peter Deifel, Stefan Milius and Lutz Schröder describes new results in participation refinement for weighted tree automata. In this paper the authors use a generic approach based on coalgebras to refine the run time analysis of their algorithm to cover weighted automata and, more generally, weighted tree automata.

GR(1)**: GR*(1) *Specifications Extended with Existential Guarantees* by Gal Amram, Shahar Maoz and Or Pistiner studies an extension of GR(1). Reactive synthesis is an automated procedure for implementing a correct-by-construction method for designing reactive systems from a temporal logic specification. GR(1) is an expressive assume-guarantee fragment of LTL that enables efficient synthesis and has been recently used in different contexts and application domains. In this paper the authors introduce an extension of GR(1) called GR(1)* which enables existential guarantees, thereby enabling developers to present their requirements through use cases, which are naturally existential.

We are very grateful to Formal Aspects of Computing for supporting this special issue, and in particular to the editors Cliff Jones and John Cooke for their assistance and advice. We would like to thank all the authors of the selected papers as well as the reviewers for their contributions in compiling this special issue. The work of all concerned was made especially challenging by the exigencies of the COVID-19 pandemic during 2020 which, amongst other things, caused academics to become experts in online education practically over night. We are very thankful that, in spite of these difficulties, everyone was able to put together this excellent collection in a timely and cheerful manner.

Annabelle McIver
Maurice ter Beek

Accepted in revised form 22 July 2021