https://doi.org/10.1007/s00165-019-00481-4
BCS © 2019
Formal Aspects of Computing (2019) 31: 131–132

Formal Aspects of Computing

Editorial

Stefania Gnesi[1], Ana Cavalcanti[2], John Fitzgerald[3] and Constance Heitmeyer[4]

[1] Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo", National Research Council, Rome, Italy
[2] Department of Computer Science, University of York, York, UK
[3] School of Computing, Newcastle University, Newcastle, UK
[4] Center for High Assurance Computer Systems, Naval Research Laboratory, Washington DC, USA

FM 2016, the 21st International Symposium on Formal Methods, was held in Limassol, Cyprus. The meeting marked a high point in the regular symposium series with 162 submissions from 534 authors in 41 countries. The proceedings were the first to appear in the new Springer Formal Methods subline, an integral part of the Lecture Notes in Computer Science (LNCS) series. During FM 2016, the Lucas Award was presented to Jeremy Dick and Alain Faivre for their highly influential paper "Automating the Generation and Sequencing of Test Cases from Model-Based Specification," LNCS Vol. 670, pp. 268–284. This paper was presented at the first symposium in the FM series, namely, the International Symposium of FME (Formal Methods Europe) held in Odense, Denmark, April 19–23, 1993.

From the 43 regular papers accepted at FM 2016, the editors invited the authors of the most highly rated papers to submit extended versions for publication in this special issue of Formal Aspects of Computing. The five selected papers reflect the symposium's objective which is to advance both the foundations and the practical application of formal methods. They cover a wide range of topics of interest to the formal methods community—a synchronous program algebra for reasoning about concurrency, a hybrid statistical approach for reasoning about information flow, tools for proving safety properties for programs that manipulate data structures, an efficient method for identifying variability abstractions in software product lines, and formal techniques for improving resource management.

The benefits of foundational work are illustrated in the paper, "A Synchronous Program Algebra: A Basis for Reasoning about Shared-Memory and Event-Based Concurrency" by Ian J. Hayes, Larissa A. Meinicke, Kirsten Winter, and Robert J. Colvin. This paper describes advances in the machine-assisted verification and derivation of shared-memory concurrent systems using a rely/guarantee relational approach. The authors' emphasis on abstraction and careful theory structuring leads to a collection of abstract theories that may be applied widely to process algebraic approaches.

Statistical approaches are often used to evaluate and verify quantitative aspects of system behaviour. The paper, "Hybrid Statistical Estimation of Mutual Information and Its Application to Information Flow" by Fabrizio Biondi, Yusuke Kawamoto, Axel Legay, and Louis-Marie Traonouez, addresses the challenge of estimating entropy-based properties in probabilistic systems. The authors introduce a method called "hybrid statistical estimation" for statistically estimating mutual information. Their approach is hybrid in that it combines a statistical analysis, based on observation of the system as a 'black box,' with precise analysis that utilises prior knowledge of system components. Case studies demonstrate performance beyond the state of the art in estimating information leakage properties.

Correspondence and offprint requests to: John Fitzgerald, E-mail: John.Fitzgerald@ncl.ac.uk

The paper, “Automated Mutual Induction Proof in Separation Logic” by Quang-Trung Ta, Ton Chanh Le, Siau-Cheng Khoo, and Wei-Ngan Chin, describes efforts to enhance the performance of tools to reason about safety properties of programs that manipulate data structures. It introduces a deductive system for proving entailments based on a new mutual induction principle whereby entailments derived during a proof search can be used as hypotheses in each others’ proofs. The approach has been prototyped and evaluated against three benchmarks, achieving better performance than alternative provers that reason about separation logic.

Due to the large space of possible variability abstractions, modern software product lines are challenging to analyse. In the paper “Finding Suitable Variability Abstractions for Lifted Analysis,” Aleksandar S. Dimovski, Claus Brabrand, and Andrzej Wasowski introduce an efficient method for identifying variability abstractions suitable for static analysis. A pre-analysis estimates the impact of variability-specific parts of the program family based on the precision of the analysis. This information is then used to target subsequent ‘lifted’ analysis. The paper reports the results of evaluating the method on three benchmarks, showing that their method achieves better results than the standard lifted analysis method.

For a growing number of applications, techniques to improve resource management require a range of complementary formal techniques. In the paper, “Battery-Aware Scheduling in Low Orbit: The GomX-3 Case,” Morten Bisgaard, David Gerhardt, Holger Hermanns, Jan Krčál, Gilles Nies, and Marvin Stenger propose a procedure that performs task scheduling for a power-hungry, low-earth-orbit nanosatellite. The approach utilises a range of model-based analyses, coupling computational models using priced timed automata and potential optimal schedules with a kinetic battery model and stochastic methods. The paper reports improvements in the quality of schedules as well as shortened development times and the capability to perform ‘what if’ analyses before deploying schedules to remote devices.

We are grateful to all those who contributed to the success of FM 2016, and to the authors and reviewers who have made this special issue possible. The influential work of Dick and Faivre, recognised at the symposium, sought to bridge a gap between formal design and approaches to testing. The papers here show how formal methods are evolving to address the growing demands of the concurrent, cyber-physical and resource-limited systems on which we will depend in the future.

Stefania Gnesi
Ana Cavalcanti
John Fitzgerald
Constance Heitmeyer

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.