https://doi.org/10.1007/s00165-018-0463-5
BCS © 2018
Formal Aspects of Computing (2018) 30: 493–494

Formal Aspects of Computing

Editorial

Nikolaj Bjørner[1], Frank de Boer[2], Andrew Butterfield[3]

[1] Microsoft Research, Redmond, USA
[2] Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
[3] Trinity College Dublin, Dublin, Ireland

Welcome to this special issue of the Formal Aspects of Computing. It is dedicated to the 20th anniversary edition of the International Symposium on Formal Methods, FM 2015, held in Oslo, June 21–25. This issue contains five extended versions of papers that originally appeared at the conference. Together with the special issue of Acta Informatica which focusses on theoretical foundations it consists of the most well received research papers covering a spectrum of advances in formal methods.

1. *A Fully Verified Container Library* by Nadia Polikarpova, Carlo Alberto Furia and Julian Tschannen describes how a full fledged container library in the Eiffel distribution is verified for full functional correctness using the automated deductive verifier AutoProof. It represents both a real-world use of verification techniques and a non-trivial task as the library contains 8000+ lines of code. Yet, the task is accomplished with a modest annotation overhead and negligible verification time.
2. *Detection of Design Flaws in the Android Permission Protocol through Bounded Verification* by Hamid Bagheri, Eunsuk Kang and Sam Malek presents analysis of the permission protocol implemented in the Android operating system. It proposes a formal model in Alloy, enabling a fully automated analysis that identifies potential protocol flaws. The flaws, which in some cases allow attackers to bypass permission checks, are reproduced in real-world Android applications.
3. *Model-Based Problem Solving for University Timetable Validation and Improvement* by David Schneider, Michael Leuschel and Tobias Witt takes the B formalism as a starting point for expressing university timetabling constraint satisfaction problems. The resulting tool, based on ProB, is used for validating timetables and it can also be used for modifying timetables while maintaining integrity constraints.
4. *Automated Circular Assume-Guarantee Reasoning* by Karam Abd Elkader, Orna Grumberg, Corina S. Păsăreanu and Sharon Shoham presents algorithms to automatically support circular assume-guarantee reasoning for systems containing components that have mutual dependencies. This work advances state-of-the-art which had so far automated acyclic assume-guarantee reasoning. It uses a counter-example guided approach to extract constraints on assumptions from spurious counter-examples. An implementation shows the advantages of the direct handling of cyclic reasoning over approaches based on acyclic reasoning.
5. *Mechanized proofs of opacity: A comparison of two techniques* by John Derrick, Simon Doherty, Brijesh Dongol, Gerhard Schellhorn, Oleg Travkin and Heike Wehrheim describes how two proof methodologies, and two tools, are studied for verifying opacity of implementations of software transactional memories. One methodology is based on a linearizability argument, and uses the KIV proof assistant. The other methodology relies on a refinement proof and uses the Isabelle interactive theorem prover. This second approach admits a decomposition of proof tasks, not available with a linearizability argument.

FM 2015 attracted 124 submissions to the main track out of which 32 papers were accepted by the Program Committee, resulting in an acceptance rate of 0.26. The Lecture Notes in Computer Science conference proceedings

Correspondence and offprint requests to: N. Bjørner Email: nbjorner@microsoft.com

further contains nine papers selected by the Program Committee of the Industry Track, which was chaired by Ralf Huuck (NICTA, Australia), Peter Gorm Larsen (Aarhus University, Denmark), and Andreas Roth (SAP, Germany). The program covered a wide spectrum of all the different aspects of the use of, and research on, formal methods for software development. It included 4 invited talks by Elvira Albert (Complutense University of Madrid, Spain), Werner Damm (Carl von Ossietzky Universität Oldenburg, DE), Valérie Issarny (INRIA, France), and Leslie Lamport (Microsoft Research, US), 11 workshops, 4 tutorials, a doctoral symposium, and a tool exhibition.

We decided to devote special issues of both Formal Aspects of Computing and Acta Informatica to FM 2015 in order to provide a focussed and coherent view on the wide range of topics.

We would like to thank Formal Aspects of Computing for providing the opportunity to generate this special issue, and to thank the reviewers for the thorough job they have undertaken. We would also like to give particular thanks to managing editor John Cooke for his very helpful support in getting this issue together.

Nikolaj Bjørner
Frank de Boer
Andrew Butterfield