Formal Methods in System Design (2021) 57:119–120
https://doi.org/10.1007/s10703-021-00382-4

Preface of the special issue on the conference on formal methods in computer aided design 2018

Nikolaj Bjørner[1] · **Arie Gurfinkel**[2]

Accepted: 30 August 2021 / Published online: 20 October 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

The International Conference on Formal Methods in Computer Aided Design (FMCAD), held at Austin, Texas, from October 3 to November 2 in 2018, is the eighteenth in a series of meetings on the theory and applications of rigorous formal techniques for the automated design of systems. The FMCAD conference covers formal aspects of specification, verification, synthesis, testing, and security, and is a leading forum for researchers and practitioners in academia and industry alike.

This special issue of the journal on Formal Methods in System Design (FMSD) features extended and revised versions of select contributions from FMCAD 2018. Each contribution received at least two round of peer reviews by at least two experts. The issue contains the following contributions:

- *Interpolating bit-vector formulas using uninterpreted predicates and presburger arithmetic* an extended version of [1], establishes how solvers for integer linear and non-linear arithmetic can be used for computing interpolants when the original format of constraints are derived from bit-vector formulas.
- *Two SAT solvers for solving quantified Boolean formulas with an arbitrary number of quantifier alternations* an extended version of [2], shows how to invoke expansion based techniques, previously used for a single alternation of quantifiers, for an entire block of an arbitrary number of quantifier alternations.
- *Certifying proofs for SAT-based model checking* an extended version of [3], shows how to extract certificates from a SAT-based symbolic model checker implementing the k-liveness algorithm. Certificate generation is extended to also several pre-processing techniques with low overhead.
- *SAT modulo discrete event simulation applied to railway design capacity analysis* an extended version of [4], develops an integration of SAT solving for dispatch planning and discrete event simulation for continuous-domain dynamics. It is used for capacity planning of a railway design.

✉ Arie Gurfinkel
arie.gurfinkel@uwaterloo.ca

Nikolaj Bjørner
nbjorner@microsoft.com

1 Microsoft, Redmond, USA

2 University of Waterloo, Waterloo, Canada

- *Temporal prophecy for proving temporal properties of infinite-state systems* an extended version of [5], introduces prophecy variables to enable using safety verification for proving general temporal properties of infinite state systems. The paper establishes the relative gains of using prophecy variables to ensure provability is maintained and it establishes a robustness property of the proof method as it satisfies a cut-elimination property.
- *Rely–Guarantee bound analysis of parameterized concurrent shared-memory programs* an extended version of [6], formulates rely-guarantee rules for bounds analysis. This enables the authors to infer runtime and resource bounds using modular proof rules. It is applied to automatically infer runtime complexity for concurrent algorithms using lock-free data structures.

We thank the authors for the interesting contributions and the reviewers for their insightful reviews. In addition, we thank Nir Piterman, the Editor in Chief of FMSD for his help in putting this issue together and the outgoing editor, Daniel Kroening, for initial help on the volume. Finally, we thank Warren A. Hunt, Jr. for inviting us to organize FMCAD 2018 and help with the local organization.

References

1. Backeman P, Rümmer P, Zeljic A (2018) Bit-vector interpolation and quantifier elimination by lazy reduction. In: Bjørner N, Gurfinkel A (eds) 2018 Formal methods in computer aided design, FMCAD 2018, Austin, TX, USA, October 30–November 2, 2018. IEEE
2. Bloem R, Braud-Santoni N, Hadzic V, Egly U, Lonsing F, Seidl M (2018) Expansion-based QBF solving without recursion. In: Bjørner N, Gurfinkel A (eds)2018 Formal methods in computer aided design, FMCAD 2018, Austin, TX, USA, October 30–November 2, 2018. IEEE
3. Griggio A, Roveri M, Tonetta S (2018) Certifying proofs for LTL model checking. In: Bjørner N, Gurfinkel A (eds) 2018 Formal methods in computer aided design, FMCAD 2018, Austin, TX, USA, October 30–November 2, 2018. IEEE
4. Luteberget B, Claessen K, Johansen C (2018) Design-time railway capacity verification using SAT modulo discrete event simulation. In: Bjørner N, Gurfinkel A (eds) 2018 Formal methods in computer aided design, FMCAD 2018, Austin, TX, USA, October 30–November 2, 2018. IEEE
5. Padon O, Hoenicke J, McMillan KL, Podelski A, Sagiv M, Shoham S (2018) Temporal prophecy for proving temporal properties of infinite-state systems. In: Bjørner N, Gurfinkel A (eds) 2018 Formal methods in computer aided design, FMCAD 2018, Austin, TX, USA, October 30–November 2, 2018. IEEE
6. Pani T, Weissenbacher G, Zuleger F (2018) Rely-guarantee reasoning for automated bound analysis of lock-free algorithms. In: Bjørner N, Gurfinkel A (eds) 2018 Formal methods in computer aided design, FMCAD 2018, Austin, TX, USA, October 30–November 2, 2018. IEEE

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