Lecture Notes in Computer Science 11951

More information about this series at http://www.springer.com/series/7408

Nan Guan · Joost-Pieter Katoen ·
Jun Sun (Eds.)

Dependable Software Engineering

Theories, Tools, and Applications

5th International Symposium, SETTA 2019
Shanghai, China, November 27–29, 2019
Proceedings

Springer

Editors
Nan Guan
Hong Kong Polytechnic University
Kowloon, Hong Kong

Joost-Pieter Katoen
RWTH Aachen University
Aachen, Germany

Jun Sun
Singapore Management University
Singapore, Singapore

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-35539-5 ISBN 978-3-030-35540-1 (eBook)
https://doi.org/10.1007/978-3-030-35540-1

LNCS Sublibrary: SL2 – Programming and Software Engineering

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at the 5th Symposium on Dependable Software Engineering: Theories, Tools, and Applications (SETTA 2019) series of conferences – held during November 27–29, 2019, in Shanghai, China. The purpose of SETTA is to provide an international forum for researchers and practitioners to share cutting-edge advancements and strengthen collaborations in the field of formal methods and its interoperability with software engineering for building reliable, safe, secure, and smart systems. Past SETTA symposiums were successfully held in Nanjing (2015), Beijing (2016), Changsha (2017), and Beijing (2018).

SETTA 2019 attracted 26 submissions co-authored by researchers from 12 countries. Each submission was reviewed by at least three Program Committee members with help from additional reviewers. The Program Committee discussed the submissions online and decided to accept eight papers for presentation at the conference. The program also included three invited talks given by Prof. Wang Yi from Uppsala University, Sweden, Dr. Kuldeep S. Meel from National University of Singapore, Singapore, and Haibo Chen from Shanghai Jiaotong University, China. The 4th National Conference on Formal Methods and Applications in China was also co-located with SETTA 2019 during November 30–December 1, 2019.

We would like to express our gratitude to the authors for submitting their papers to SETTA 2019. We are particularly thankful to all members of Program Committee and the additional reviewers, whose hard and professional work in the review process helped us prepare the high-quality conference program. Special thanks go to our invited speakers for presenting their research at the conference. We would like to thank the Steering Committee for their advice. Finally, we thank the conference general chair, Prof. Yuxi Fu, and the publicity chairs, Dr. Yu Pei and Dr. Tom van Dijk.

October 2019

Jun Sun
Joost-Pieter Katoen
Nan Guan

Organization

Program Committee

Étienne André	Université Paris 13, LIPN, CNRS, UMR 7030, France
Mohamed Faouzi Atig	Uppsala University, Sweden
Ezio Bartocci	Vienna University of Technology, Austria
Sanjoy Baruah	Washington University in St. Louis, USA
Yan Cai	State Key Laboratory of Computer Science and Institute of Software, Chinese Academy of Sciences, China
Milan Ceska	Brno University of Technology, Czech Republic
Sudipta Chattopadhyay	Singapore University of Technology and Design, Singapore
Mingsong Chen	East China Normal University, China
Taolue Chen	Birkbeck, University of London, UK
Yu-Fang Chen	Academia Sinica, Taiwan
Alessandro Cimatti	Fondazione Bruno Kessler (FBK-irst), Italy
Yuxi Fu	Shanghai Jiao-tong University, China
Nan Guan	The Hong Kong Polytechnic University, Hong Kong SAR, China
Tingting Han	Birkbeck, University of London, UK
Arnd Hartmanns	University of Twente, The Netherlands
Nils Jansen	Radboud University, The Netherlands
Ran Ji	Carnegie Mellon University, USA
Yu Jiang	Tsinghua University, China
Lei Ju	Shandong University, China
Joost-Pieter Katoen	RWTH Aachen University, Germany
Guoqiang Li	Shanghai Jiao Tong University, China
Di Liu	Yunnan University, China
Shuang Liu	Singapore Institute of Technology, Singapore
Federico Olmedo	University of Chile, Chile
Yu Pei	The Hong Kong Polytechnic University, Hong Kong SAR, China
Mickael Randour	F. R .S.-FNRS and UMONS, Université de Mons, France
Anne Remke	WWU Münster, Germany
Philipp Ruemmer	Uppsala University, Sweden
Fu Song	School of Information Science and Technology, ShanghaiTech University, China
Jeremy Sproston	University of Turin, Italy
Jun Sun	Singapore Management University, Singapore

Cong Tian	Xidian University, China
Tarmo Uustalu	Reykjavik University, Iceland
Jaco van de Pol	Aarhus University, Denmark
Bow-Yaw Wang	Academia Sinica, Taiwan
Ji Wang	National Laboratory for Parallel and Distributed Processing, China
Xue-Yang Zhu	Institute of Software, Chinese Academy of Sciences, China

Additional Reviewers

Boiret, Adrien
Budde, Carlos
Budde, Carlos E.
Delgrange, Florent
Li, Xin
Lin, Hsin-Hung
Perelli, Giuseppe
Ramparison, Mathias
Sun, Youcheng
Xue, Jianxin
Zhao, Hengjun

Abstracts

The Rise of Model Counting: A Child of SAT Revolution

Kuldeep S. Meel

School of Computing, National University of Singapore, Singapore

Abstract. The paradigmatic NP-complete problem of Boolean satisfiability (SAT) is a central problem in Computer Science. The past 20 years have witnessed a *SAT revolution* with the development of conflict-driven clause-learning (CDCL) SAT solvers. Such solvers combine a classical backtracking search with a rich set of effective heuristics. While 20 years ago SAT solvers were able to solve instances with at most a few hundred variables, modern SAT solvers solve instances with up to millions of variables in a reasonable time. The SAT revolution opens up opportunities to design practical algorithms with rigorous guarantees for problems in complexity classes beyond NP by replacing a NP oracle with a SAT Solver. In this talk, we will discuss how we use SAT revolution to design practical algorithms for one of the fundamental problems in formal methods and artificial intelligence: model counting.

Model counting is a fundamental computational problem with applications in diverse areas spanning neural network verification, reliability estimation, explainable AI, probabilistic inference, security vulnerability analysis, and the like. While counting has been studied extensively by theoreticians for the past three decades. Yet, in spite of this extensive study, it has been extremely difficult to reduce this theory to practice. We examine how the process of revisiting and refining the theory to leverage the SAT revolution has led to the development of the first scalable framework for model counting: ApproxMC [1–4]. ApproxMC[1] can handle industrial-scale problem instances involving hundreds of thousands of variables, while providing provably strong approximation guarantees.

References

1. Chakraborty, S., Meel, K.S., Vardi, M.Y.: A scalable approximate model counter. In: Proceedings of CP (2013)
2. Chakraborty, S., Meel, K.S., Vardi, M.Y.: Algorithmic improvements in approximate counting for probabilistic inference: from linear to logarithmic SAT calls. In: Proceedings of IJCAI (2016)
3. Ivrii, A., Malik, S., Meel, K.S., Vardi, M.Y.: On computing minimal independent support and its applications to sampling and counting. Constraints, 1–18 (2016)
4. Soos, M., Meel, K.S.: BIRD: Engineering an efficient CNF-XOR SAT solver and its applications to approximate model counting. In: Proceedings of AAAI (2019)

[1] https://github.com/meelgroup/approxmc.

Building and Updating Safety-Critical Embedded Systems with Deterministic Timing and Functional Behaviours

Wang Yi

Uppsala University, Sweden

Today, the functionality as well as economical value of industrial systems and products, such as cars, air planes, and medical equipment, is defined and realized by software as embedded systems. Dynamical software updates are critical for security updates, new features, and customization, but are not supported for today's safety-critical systems, since we lack techniques to guarantee that the updated system remains safe.

In this talk, I will present a model for embedded systems with deterministic timing and functional behaviours. The model provides a foundation for a new design paradigm for building embedded systems which can be updated on demand dynamically, safely, and efficiently over their operational life-time.

Contents