Lecture Notes in Computer Science 9984

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Martin Fränzle · Deepak Kapur
Naijun Zhan (Eds.)

Dependable Software Engineering

Theories, Tools, and Applications

Second International Symposium, SETTA 2016
Beijing, China, November 9–11, 2016
Proceedings

Springer

Editors
Martin Fränzle
Carl von Ossietzky Universität
Oldenburg
Germany

Deepak Kapur
University of New Mexico
Albuquerque, NM
USA

Naijun Zhan
Chinese Academy of Sciences
Beijing
China

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-47676-6 ISBN 978-3-319-47677-3 (eBook)
DOI 10.1007/978-3-319-47677-3

Library of Congress Control Number: 2016953662

LNCS Sublibrary: SL2 – Programming and Software Engineering

Printed on acid-free paper

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

Preface

This volume contains the papers presented at the second in the SETTA (the Symposium on Dependable Software Engineering: Theories, Tools and Applications) series of conferences – held during November 9–11, 2016, in Beijing, China. The symposium series was inaugurated in 2015 to build a forum for computer scientists and software engineers from Chinese and international communities to exchange and inform each other of research ideas and activities, building new collaborations and strengthening existing collaborations among formal methods researchers inside and outside China. A key goal of SETTA is to especially encourage and nourish young researchers working in the use of formal methods in building software and cyber-physical systems.

SETTA 2016 received over 58 submissions of abstracts, with 45 of them as full-paper submissions by the submission deadline. These submissions were coauthored by researchers from 22 countries. Each submission was reviewed by at least three Program Committee (PC) members with help from reviewers outside the PC. After two weeks of online discussions, the committee decided to accept 20 papers for presentation at the conference (with the acceptance rate of 44 %); this includes 17 full papers and three short papers. It was decided to include short papers to provide a forum for participants to present research in progress. To alleviate presentational issues on some papers of good technical quality, shepherding by PC members was employed while preparing revisions. Such submissions were accepted after an additional round of reviewing leading to one submission being rejected.

We would like to express our gratitude to all the researchers who submitted their work to the symposium. We are particularly thankful to all colleagues who served on the PC, as well as the external reviewers, whose hard work in the review process helped us prepare a high-quality conference program. The international diversity of the PC as well as external reviewers is noteworthy as well: PC members and external reviewers have affiliations with institutes in 17 countries. Special thanks go to the invited speakers, Prof. Lee from the University of California, Berkeley, Prof. Sankaranarayanan of the University of Colorado, and Prof. Ying of the University of Sydney and Tsinghua University, for agreeing to present their research. The abstracts of the invited talks are included in this volume.

Like SETTA 2015, SETTA 2016 also had a young SETTA Researchers Workshop, which was held on November 12, 2016. Another inaugural event – the first National Conference on Formal Methods and Applications in China – was held during November 12–13, 2016.

A number of colleagues worked very hard to make this conference a success. We wish to express our gratitude especially to Prof. Shuling Wang for taking care of numerous activities related to the publicity, conference proceedings, and other aspects of the conference. We thank the conference chair, Huimin Lin, publicity chairs, Nils Muellner and Lijun Zhang, and the local Organizing Committee of Andrea Turini, Shuling Wang, Peng Wu, and Zhilin Wu. Finally, we enjoyed great institutional and

financial support from the Institute of Software, the Chinese Academy of Sciences (ISCAS), without which an international conference like SETTA and the colocated events could not have been be successfully organized. We also thank the Chinese Computer Federation (CCF) and the Natural Science Foundation of China (NSFC) for financial support.

August 2016

Martin Fränzle
Deepak Kapur
Naijun Zhan

Organization

Program Committee

Erika Abraham	RWTH Aachen University, Germany
Farhad Arbab	CWI and Leiden University, The Netherlands
Sanjoy Baruah	University of North Carolina, Chapel Hill, USA
Michael Butler	University of Southampton, UK
Deepak D'Souza	Indian Institute of Science, Bangalore, India
Yuxin Deng	East China Normal University, China
Xinyu Feng	University of Science and Technology of China, Suzhou, China
Goran Frehse	University of Grenoble Alpes - Laboratoire Verimag, Grenoble, France
Martin Fränzle	University of Oldenburg, Germany
Lindsay Groves	Victoria University of Wellington, New Zealand
Dimitar Guelev	Bulgarian Academy of Sciences, Bulgaria
Fei He	Tsinghua University, China
Holger Hermanns	Saarland University, Germany
Deepak Kapur	University of New Mexico, USA
Axel Legay	IRISA/Inria, Rennes, France
Xuandong Li	Nanjing University, China
Shaoying Liu	Hosei University, Tokyo, Japan
Zhiming Liu	Southwest University, Chongqing, China
Xiaoguang Mao	National University of Defense Technology, Changsha, China
Markus Müller-Olm	Westfälische Wilhelms-Universität Münster, Germany
Raja Natarajan	Tata Institute of Fundamental Research, Bombay, India
Jun Pang	University of Luxembourg, Luxenmbourg
Shengchao Qin	Teesside University, UK
Sriram Rajamani	Microsoft Research India, Bangalore, India
Jean-François Raskin	Université Libre de Bruxelles, Belgium
Stefan Ratschan	Czech Academy of Sciences, Prague, Czech
Martin Steffen	University of Oslo, Norway
Zhendong Su	UC Davis, USA
Cong Tian	Xidian University, China
Tarmo Uustalu	Tallinn University of Technology, Estonia
Chao Wang	University of Southern California, Los Angeles, USA
Farn Wang	National Taiwan University, ROC
Heike Wehrheim	University of Paderborn, Germany
Wang Yi	Uppsala University, Sweden

Naijun Zhan Institute of Software, Chinese Academy of Sciences, Beijing, China
Lijun Zhang Institute of Software, Chinese Academy of Sciences, Beijing, China

Additional Reviewers

Bu, Lei
Dan, Li
Fahrenberg, Uli
Fu, Ming
Geeraerts, Gilles
Guo, Shengjian
Hahn, Ernst Moritz
Hoang, Thai Son
Huang, Yanhong
Kekatos, Nikolaos
Kim, Jin Hyun
Krämer, Julia
Kucera, Antonin
Le Bouder, Hélène
Lei, Suhua
Liu, Bo
Moszkowski, Ben
Mukherjee, Suvam
Nordhoff, Benedikt
Norman, Gethin
Randour, Mickael
Ray, Rajarshi
Salehi Fathabadi, Asieh
Singh, Abhishek Kr
Sun, Chengnian
Sung, Chungha
Tacchella, Armando
Tinchev, Tinko
Travkin, Oleg
Turrini, Andrea
van Breugel, Franck
Velez, Martin
Veltri, Niccolò
Wu, Meng
Xu, Zhiwu
Yu, Hengbiao
Zhang, Miaomiao
Zhang, Qirun
Zhao, Jianhua

Keynote Abstracts

Dependable Cyber-physical Systems

Edward A. Lee

Electrical Engineering and Computer Sciences Department,
University of California, Berkeley, USA

Abstract. Cyber-physical systems are integrations of computation, communication networks, and physical dynamics. Applications include manufacturing, transportation, energy production and distribution, biomedical, smart buildings, and military systems, to name a few. Increasingly, today, such systems leverage Internet technology, despite a significant mismatch in technical objectives. A major challenge today is to make this technology reliable, predictable, and controllable enough for "important" things, such as safety-critical and mission-critical systems. In this talk, I will analyze how emerging technologies can translate into better models and better engineering methods for this evolving Internet of Important things.

From Finitely Many Simulations to Flowpipes

Sriram Sankaranarayanan

Computer Science Department, University of Colorado Boulder, Boulder, USA

Abstract. Flowpipe construction techniques generalize symbolic execution for continuous-time models by computing future trajectories for sets of inputs and initial states. In doing so, they capture infinitely many behaviors of the underlying system, thus promising exhaustive verification. We examine the progress in this area starting from techniques for linear systems to recent progress in reasoning about nonlinear dynamical systems. We demonstrate how this area of research transforms fundamental results from dynamical systems theory into useful computational techniques for reasoning about cyber-physical systems. This progress has led to increasingly popular tools for verifying cyber-physical systems with applications to important verification problems for medical devices and automotive software. We demonstrate how recent approaches have exploited commonly encountered properties of the underlying continuous models such as monotonicity, incremental stability and structural dependencies to verify properties for larger and more complex systems. Despite this progress, many challenges remain. We present some of the key theoretical and practical challenges that need to be met before flowpipe construction can be a true "technology" for verifying industrialscale systems.

Toward Automatic Verification of Quantum Programs (Extended Abstract)

Mingsheng Ying[1,2]

[1] Centre for Quantum Computation and Intelligent Systems,
University of Technology Sydney, Ultimo, Australia
Mingsheng.Ying@uts.edu.au
[2] Department of Computer Science and Technology,
Tsinghua University, Beijing, China
yingmsh@tsinghua.edu.cn

Keywords: Quantum programming · Hoare logic · Invariant generation · Algorithmic analysis of termination · Synthesis of ranking functions

Programming is error-prone. Programming a quantum computer and designing quantum communication protocols are even worse due to the weird nature of quantum systems [11]. Therefore, verification techniques for quantum programs and quantum protocols will be indispensable whence commercial quantum computers and quantum communication systems are available. In the last 10 years, various verification techniques for classical programs including program logics and model-checking have been extended to deal with quantum programs. This talk summaries several results obtained by the author and his collaborators in this line of research.

1 Quantum Hoare Logic

In quantum programming, the state space of a program variable is a Hilbert space. A quantum predicate in a Hilbert space was defined by D'Hondt and Panangaden in [4] as a Hermtian operator, i.e. an observable, between the zero and identity operators. A proof system for partial and total correctness of the Floyd-Hoare style was developed and its (relative) completeness was proved in [10] for the following quantum extension of **while**-language:

$$P ::= \textbf{skip} \mid P_1; P_2 \mid q := |0\rangle \mid \bar{q} := U[\bar{q}] \mid \textbf{if } (\square_m M[\bar{q}] = m \to P_m) \textbf{ fi} \\ \mid \textbf{while } M[\bar{q}] = 1 \textbf{ do } P \textbf{ od}$$

The command "$q := |0\rangle$" is an initialisation that sets quantum variable q to a basis state $|0\rangle$. The statement "$\bar{q} := U[\bar{q}]$" means that unitary transformation U is performed on quantum register $\bar{q}$, leaving the states of the variables not in $\bar{q}$ unchanged. The construct "**if** $\cdots$ **fi**" is a quantum generalisation of case or switch statement. In executing it,

measurement $M = \{M_m\}$ is performed on $\bar{q}$, and then a subprogram P_m is selected to be executed next according to the outcomes m of measurement. The statement "**while** $\cdots$ **od**" is a quantum generalisation of **while**-loop. The measurement in it has only two possible outcomes 0, 1. If the outcome 0 is observed, then the program terminates, and if the outcome 1 occurs, the program executes the loop body P and continues the loop. It is interesting to carefully compare the Hoare rule for loops:

$$\frac{\{\varphi \wedge b\}P\{\varphi\}}{\{\varphi\}\ \textbf{while}\ b\ \textbf{do}\ P\ \textbf{od}\{\varphi \wedge \neg b\}}$$

with the rule for quantum loops given in [10]:

$$\frac{\{B\}P\left\{M_0^\dagger A M_0 + M_1^\dagger B M_1\right\}}{\{M_0^\dagger A M_0 + M_1^\dagger B M_1\}\ \textbf{while}\ M[\bar{q}] = 1\ \textbf{do}\ P\ \textbf{od}\ \{A\}}$$

A theorem prover was built by Liu, Li, Wang et al. in [8] for quantum Hoare logic based on Isabelle/HOL.

2 Invariants of Quantum Programs

A super-operator in a Hilbert space is a completely positive mapping from (linear) operators to themselves. The control flow of a quantum program can be represented by a super-operator-valued transition system (SVTS):

Definition 1. *An SVTS is a 5-tuple $\mathcal{S} = \langle \mathcal{H}, L, l_0, \mathcal{T}, \Theta \rangle$, where: (1) $\mathcal{H}$ is a Hilbert space; (2) L is a finite set of locations; (3) $l_0 \in L$ is the initial location; (4) Θ is a quantum predicate in $\mathcal{H}$ denoting the initial condition; and (5) $\mathcal{T}$ is a set of transitions. Each transition $\tau \in \mathcal{T}$ is written as $\tau = l \xrightarrow{\mathcal{E}} l'$ with $l, l' \in L$ and $\mathcal{E}$ being a super-operator in $\mathcal{H}$. For each $l \in L$, it is required that $\mathcal{E}_l = \sum \{|\mathcal{E} : l \xrightarrow{\mathcal{E}} l' \in \mathcal{T}|\}$ is trace-preserving, i.e. $tr(\mathcal{E}_l(\rho)) = tr(\rho)$ for all ρ.*

The notion of invariant for quantum programs was recently introduced in [14]. A set Π of paths is said to be prime if for each $\pi = l_1 \xrightarrow{\mathcal{E}_1} \ldots \xrightarrow{\mathcal{E}_{n-1}} l_n \in \Pi$, its proper initial segments $l_1 \xrightarrow{\mathcal{E}_1} \ldots \xrightarrow{\mathcal{E}_{k-1}} l_k \notin \Pi$ for all $k < n$. We write $\mathcal{E}_\pi$ for the composition of $\mathcal{E}_1, \ldots, \mathcal{E}_{n-1}$ and $\mathcal{E}_\Pi = \sum \{|\mathcal{E}_\pi : \pi \in \Pi|\}$.

Definition 2. *Let $\mathcal{S} = \langle \mathcal{H}, L, l_0, \mathcal{T}, \Theta \rangle$ be an SVTS and $l \in L$. An invariant at location $l \in L$ is a quantum predicate O in $\mathcal{H}$ satisfying the condition: for any density operator ρ and prime set Π of paths from l_0 to l, we have:*

$$\mathrm{tr}(\Theta\rho) \leq 1 - \mathrm{tr}(\mathcal{E}_\Pi(\rho)) + \mathrm{tr}(O\mathcal{E}_\Pi(\rho)).$$

In [14], it was shown that invariants can be used to establish partial correctness of quantum programs, and by generalising the constraint-based technique of Colón et al. [3, 9], invariant generation for quantum programs is reduced to an SDP (Semidefinite Programming) problem.

3 Terminations of Quantum Programs

Algorithmic analysis of termination for quantum programs was first considered in [13] where the Jordan decomposition of complex matrices was employed as the main tool. It was further studied by the author and his collaborators in a series of papers [7, 15–17] by introducing quantum Markov chains as a semantic model of quantum programs and using matrix representation of super-operators.

The notion of ranking function was defined in [10] for proving total correctness of quantum programs. The synthesis problem of ranking functions for quantum programs was recently investigated in [12] where the fundamental Gleason theorem [6] in quantum foundations was used to determine the template of ranking functions. In the last few years, (super)martingales have been employed as a powerful mathematical tools for termination analysis of probabilistic programs [1, 2, 5]. It seems that the ideas of this line of research can be generalised to deal with quantum programs, but we need to systematically develop a mathematical theory of quantum (super)martingales first.

Acknowledgment. This work was partly supported by the Australian Research Council (Grant No: DP160101652) and the Overseas Team Program of Academy of Mathematics and Systems Science, Chinese Academy of Sciences.

References

1. Chakarov, A., Sankaranarayanan, S.: Probabilistic program analysis with martingales. In: CAV 2013. LNCS, vol. 8044, pp. 511–526. Springer, Berlin (2013)
2. Chatterjee, K., Fu, H.F., Novotný, P., Hasheminezhad, R.: Algorithmic analysis of qualitative and quantitative termination problems for affine probabilistic programs. In: Proceedings of the 43rd Annual ACM Symposium on Principles of Programming Languages (POPL), pp. 327–342 (2016)
3. Colón, M.A., Sankaranarayanan, S., Sipma, H.B.: Linear invariant generation using non-linear constraint solving. In: CAV 2003. LNCS, vol. 2725, pp. 420–433. Springer, Berlin (2003)
4. D'Hondt, E., Panangaden, P.: Quantum weakest preconditions. Math. Struct. Comput. Sci. **16,** 429–451 (2006)
5. Fioriti, L.M.F., Hermanns, H.: Probabilistic termination: soundness, completeness, and compositionality. In: Proceedings of the 42nd Annual ACM Symposium on Principles of Programming Languages (POPL), pp. 489–501 (2015)
6. Gleason, A.M.: Measures on the closed subspaces of a Hilbert space. J. Math. Mech. **6,** 885–893 (1957)

7. Li, Y.J., Yu, N.K., Ying, M.S.: Termination of nondeterministic quantum programs. Acta Informatica **51**, 1–24 (2014)
8. Liu, T., Li, Y.J., Wang, S.L. et al.: A theorem prover for quantum Hoare logic and its applications. arXiv:1601.03835
9. Sankaranarayanan, S., Sipma, H.B., Manna, Z.: Non-linear loop invariant generation using Gröbner bases. In: Proceedings of the 31st ACM Symposium on Principles of Programming Languages (POPL), pp. 318–329 (2004)
10. Ying, M.S.: Floyd-Hoare logic for quantum programs. ACM Trans. Program. Lang. Syst. **39**(19) (2011)
11. Ying, M.S.: Foundations of Quantum Programs. Morgan-Kaufmann (2016)
12. Ying, M.S.: Ranking function synthesis for quantum programs, Draft
13. Ying, M.S., Feng, Y.: Quantum loop programs. Acta Informatica **47**, 221–250 (2010)
14. Ying, M.S., Ying, S.G., Wu, X.D.: Invariants of quantum programs: characterisations and generation, Draft.
15. Ying, M.S., Yu, N.K., Feng, Y., Duan, R.Y.: Verification of quantum programs. Sci. Comput. Program. **78**, 1679–1700 (2013)
16. Ying, S.G., Feng, Y., Yu, N.K., Ying, M.S.: Reachability analysis of quantum Markov chains. In: Proceedings of the 24th International Conference on Concurrency Theory (CONCUR), pp. 334–348 (2013)
17. Yu, N.K., Ying, M.S.: Reachability and termination analysis of concurrent quantum programs. In: Proceedings of the 23th International Conference on Concurrency Theory (CONCUR), pp. 69–83 (2012)

Contents