-NCS 13360 Festschrift

Wolfgang Ahrendt Bernhard Beckert Richard Bubel Einar Broch Johnsen (Eds.)

The Logic of Software

A Tasting Menu of Formal Methods

Essays Dedicated to Reiner Hähnle on the Occasion of His 60th Birthday



Lecture Notes in Computer Science

13360

Founding Editors

Gerhard Goos Karlsruhe Institute of Technology, Karlsruhe, Germany Juris Hartmanis Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino Purdue University, West Lafayette, IN, USA Wen Gao Peking University, Beijing, China Bernhard Steffen TU Dortmund University, Dortmund, Germany Moti Yung Columbia University, New York, NY, USA More information about this series at https://link.springer.com/bookseries/558

Wolfgang Ahrendt · Bernhard Beckert · Richard Bubel · Einar Broch Johnsen (Eds.)

The Logic of Software

A Tasting Menu of Formal Methods

Essays Dedicated to Reiner Hähnle on the Occasion of His 60th Birthday



Editors Wolfgang Ahrendt Chalmers University of Technology Gothenburg, Sweden

Richard Bubel TU Darmstadt Darmstadt, Germany Bernhard Beckert Karlsruhe Institute of Technology Karlsruhe, Germany

Einar Broch Johnsen D University of Oslo Oslo, Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic) Lecture Notes in Computer Science ISBN 978-3-031-08165-1 ISBN 978-3-031-08166-8 (eBook) https://doi.org/10.1007/978-3-031-08166-8

© Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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



Quo Vadis Formal Methods? I can see clearly now \ldots

Preface

Distinguished, multi-valued reader, welcome to this festschrift to celebrate the 60th anniversary of our dear colleague Reiner Hähnle. As your hosts, it is our pleasure to introduce the menu. With a focus on certified modularity and variability, we present you with a history-based and resource-aware, carefully curated experience. The contributions mostly draw on seasonal, local products with the occasional exotic contribution in a cooperative and hopefully bug-free manner. With this festschrift, we can accommodate most allergies with fair constraint merging, except for the abstraction allergy.

For the aperitif, we propose the liberalised adventures of Alice and a dash of dynamic and unbounded clairvoyance, bridging the gap between formal and informal knowledge. For starters, we recommend a transparent treatment of loops to incrementally validate the boundary between the verified and the unverified. This is followed by the orderly resolution of contracts, both their design and their programming. We then consider the symbolic execution of locally abstract, globally concrete semantics of eternal, adaptable and evolving railway operations with anti-links and commodious axiomatization.

The *trou normand* of this festschrift will be saturated by information flow and soundness leaks, inferring secrets by guided experiments in Re-CorC-ing with a focus on naturalness. After that, we present a many-valued symphony of partiality and abstraction, spanning from the Karlsruhe Java Verification Suite, via JML, COSTA, KeY, KIV, Stipula, Łukasiewicz logic, AF-algebras, MaxSAT and MinSAT, to Snap! As for abstraction refinement and incremental validation to enable reuse and transformation, we are afraid that selection is no longer available at this point, without explicit dependency information.

To facilitate symbolic digestion, the grand finale offers a dash of automatic complexity analysis, an injection of sound and complete reasoning about actors and a note on their idleness. By suggesting normal forms for knowledge compilation, the menu is curated to facilitate lifelong learning and to better understand research quality.

We are proud to offer to you a menu with a wide variety of ingredients and preparation styles, reflecting the great repertoire of the master chef Reiner Hähnle, a repertoire of formal methods that he developed during his long journey as a scientist, which brought him from being a young PhD student working on many-valued logics to his long tenure as an eminent researcher in formal methods. Reiner's mastery inspired and influenced many chefs in their cooking, and their commitment to the best end-user gournet experience.

We hope you will enjoy this tasting menu!

April 2022

Wolfgang Ahrendt Bernhard Beckert Richard Bubel Einar Broch Johnsen

Organization

Editors

Wolfgang Ahrendt Bernhard Beckert Richard Bubel Einar Broch Johnsen

Reviewers

Ole Jørgen Abusdal

Elvira Albert Mads Dam Ferruccio Damiani Frank De Boer Crystal Chang Din Samir Genaim Jürgen Giesl Dilian Gurov Marieke Huisman Eduard Kamburjan Alexander Knüppel Cosimo Laneve Gary T. Leavens Rustan Leino Michael Lienhardt Felip Manyà Wojciech Mostowski Daniele Mundici André Platzer Violet Ka I Pun

Aarne Ranta Wolfgang Reif Philipp Ruemmer Ina Schaefer Rudolf Schlatte Bernhard Steffen Dominic Steinhöfel Chalmers University of Technology, Sweden Karlsruhe Institute of Technology (KIT), Germany Technische Universität Darmstadt, Germany University of Oslo, Norway

Western Norway University of Applied Sciences, Norway Universidad Complutense de Madrid, Spain KTH Royal Institute of Technology, Sweden Università di Torino, Italy Centrum Wiskunde and Informatica, The Netherlands University of Bergen, Norway Universidad Complutense de Madrid, Spain RWTH Aachen University, Germany KTH Royal Institute of Technology, Sweden University of Twente, The Netherlands University of Oslo, Norway Technische Universität Braunschweig, Germany University of Bologna, Italy University of Central Florida, USA Amazon Web Services, USA **ONERA**, France AI Research Institute (IIIA, CSIC), Spain Halmstad University, Sweden University of Florence, Italy Carnegie Mellon University, USA Western Norway University of Applied Sciences, Norway Chalmers University of Technology, Sweden University of Augsburg, Germany Uppsala University, Sweden Karlsruhe Institute of Technology (KIT), Germany University of Oslo, Norway University of Dortmund, Germany CISPA Helmholtz Center for Information Security, Germany

x Organization

Volker Stolz	Western Norway University of Applied Sciences,
	Norway
Silvia Lizeth Tapia Tarifa	University of Oslo, Norway
Mattias Ulbrich	Karlsruhe Institute of Technology (KIT), Germany
Adele Veschetti	University of Bologna, Italy

Contents

I Can See Clearly Now: Clairvoyant Assertions for Deadlock Checking Ole Jørgen Abusdal, Crystal Chang Din, Violet Ka I Pun, and Volker Stolz	1
When COSTA Met KeY: Verified Cost Bounds Elvira Albert, Samir Genaim, Alicia Merayo, and Guillermo Román-Díez	19
Lifelong Learning of Reactive Systems in Practice	38
A Case Study in Information Flow Refinement for Low Level Systems Roberto Guanciale, Christoph Baumann, Pablo Buiras, Mads Dam, and Hamed Nemati	54
Re-CorC-ing KeY: Correct-by-Construction Software Development Based	00
Tabea Bordis, Loek Cleophas, Alexander Kittelmann, Tobias Runge, Ina Schaefer, and Bruce W. Watson	80
Specifying the Boundary Between Unverified and Verified Code David R. Cok and K. Rustan M. Leino	105
Programming Legal Contracts: – A Beginners Guide to Stipula – Silvia Crafa and Cosimo Laneve	129
Towards a Modular and Variability-Aware Aerodynamic Simulator Ferruccio Damiani, Michael Lienhardt, Bruno Maugars, and Bertrand Michel	147
Reasoning About Active Objects: A Sound and Complete Assertional Proof Method	173
Improving Automatic Complexity Analysis of Integer Programs Jürgen Giesl, Nils Lommen, Marcel Hark, and Fabian Meyer	193
Alice in Wineland: A Fairy Tale with Contracts Dilian Gurov, Christian Lidström, and Philipp Rümmer	229
Teaching Design by Contract Using Snap! Marieke Huisman and Raúl E. Monti	243

On the Notion of Naturalness in Formal Modeling Eduard Kamburjan and Sandro Rama Fiorini	
The Karlsruhe Java Verification Suite Jonas Klamroth, Florian Lanzinger, Wolfram Pfeifer, and Mattias Ulbrich	290
Further Lessons from the JML Project Gary T. Leavens, David R. Cok, and Amirfarhad Nilizadeh	313
Inference in MaxSAT and MinSAT Chu Min Li and Felip Manyà	350
Implications of Deductive Verification on Research Quality: Field Study Wojciech Mostowski	370
Computing in Łukasiewicz Logic and AF-Algebras	382
Speaking About Wine: Another Case Study in Bridging the Gap Between Formal and Informal Knowledge	397
Software & System Verification with KIV Gerhard Schellhorn, Stefan Bodenmüller, Martin Bitterlich, and Wolfgang Reif	408
A Note on Idleness Detection of Actor Systems	437
Symbolic Execution: Foundations, Techniques, Applications, and Future Perspectives	446
Locally Abstract Globally Concrete Semantics of Time and Resource Aware Active Objects Silvia Lizeth Tapia Tarifa	481
Transparent Treatment of for-Loops in Proofs	500
Author Index	521

xii

Contents