

Peter Müller (Ed.)

ARCoSS

LNCS 12075

Programming Languages and Systems

**29th European Symposium on Programming, ESOP 2020
Held as Part of the European Joint Conferences
on Theory and Practice of Software, ETAPS 2020
Dublin, Ireland, April 25–30, 2020, Proceedings**



Springer Open

Founding Editors

Gerhard Goos, Germany
Juris Hartmanis, USA

Editorial Board Members

Elisa Bertino, USA
Wen Gao, China
Bernhard Steffen , Germany

Gerhard Woeginger , Germany
Moti Yung, USA


Advanced Research in Computing and Software Science

Subline of Lecture Notes in Computer Science

Subline Series Editors

Giorgio Ausiello, *University of Rome 'La Sapienza', Italy*
Vladimiro Sassone, *University of Southampton, UK*

Subline Advisory Board


Susanne Albers, *TU Munich, Germany*
Benjamin C. Pierce, *University of Pennsylvania, USA*
Bernhard Steffen , *University of Dortmund, Germany*
Deng Xiaotie, *Peking University, Beijing, China*
Jeannette M. Wing, *Microsoft Research, Redmond, WA, USA*

More information about this series at <http://www.springer.com/series/7407>

Peter Müller (Ed.)

Programming Languages and Systems

29th European Symposium on Programming, ESOP 2020
Held as Part of the European Joint Conferences
on Theory and Practice of Software, ETAPS 2020
Dublin, Ireland, April 25–30, 2020
Proceedings

Editor
Peter Müller 
ETH Zurich
Zurich, Switzerland



ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-44913-1 ISBN 978-3-030-44914-8 (eBook)
<https://doi.org/10.1007/978-3-030-44914-8>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© The Editor(s) (if applicable) and The Author(s) 2020. This book is an open access publication.

Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

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

ETAPS Foreword

Welcome to the 23rd ETAPS! This is the first time that ETAPS took place in Ireland in its beautiful capital Dublin.

ETAPS 2020 was the 23rd instance of the European Joint Conferences on Theory and Practice of Software. ETAPS is an annual federated conference established in 1998, and consists of four conferences: ESOP, FASE, FoSSaCS, and TACAS. Each conference has its own Program Committee (PC) and its own Steering Committee (SC). The conferences cover various aspects of software systems, ranging from theoretical computer science to foundations of programming language developments, analysis tools, and formal approaches to software engineering. Organizing these conferences in a coherent, highly synchronized conference program enables researchers to participate in an exciting event, having the possibility to meet many colleagues working in different directions in the field, and to easily attend talks of different conferences. On the weekend before the main conference, numerous satellite workshops took place that attracted many researchers from all over the globe. Also, for the second time, an ETAPS Mentoring Workshop was organized. This workshop is intended to help students early in the program with advice on research, career, and life in the fields of computing that are covered by the ETAPS conference.

ETAPS 2020 received 424 submissions in total, 129 of which were accepted, yielding an overall acceptance rate of 30.4%. I thank all the authors for their interest in ETAPS, all the reviewers for their reviewing efforts, the PC members for their contributions, and in particular the PC (co-)chairs for their hard work in running this entire intensive process. Last but not least, my congratulations to all authors of the accepted papers!

ETAPS 2020 featured the unifying invited speakers Scott Smolka (Stony Brook University) and Jane Hillston (University of Edinburgh) and the conference-specific invited speakers (ESOP) Işıl Dillig (University of Texas at Austin) and (FASE) Willem Visser (Stellenbosch University). Invited tutorials were provided by Erika Ábrahám (RWTH Aachen University) on the analysis of hybrid systems and Madhusudan Parthasarathy (University of Illinois at Urbana-Champaign) on combining Machine Learning and Formal Methods. On behalf of the ETAPS 2020 attendants, I thank all the speakers for their inspiring and interesting talks!

ETAPS 2020 took place in Dublin, Ireland, and was organized by the University of Limerick and Lero. ETAPS 2020 is further supported by the following associations and societies: ETAPS e.V., EATCS (European Association for Theoretical Computer Science), EAPLS (European Association for Programming Languages and Systems), and EASST (European Association of Software Science and Technology). The local organization team consisted of Tiziana Margaria (general chair, UL and Lero), Vasileios Koutavas (Lero@UCD), Anila Mjeda (Lero@UL), Anthony Ventresque (Lero@UCD), and Petros Stratis (Easy Conferences).

The ETAPS Steering Committee (SC) consists of an Executive Board, and representatives of the individual ETAPS conferences, as well as representatives of EATCS, EAPLS, and EASST. The Executive Board consists of Holger Hermanns (Saarbrücken), Marieke Huisman (chair, Twente), Joost-Pieter Katoen (Aachen and Twente), Jan Kofron (Prague), Gerald Lüttgen (Bamberg), Tarmo Uustalu (Reykjavik and Tallinn), Caterina Urban (Inria, Paris), and Lenore Zuck (Chicago).

Other members of the SC are: Armin Biere (Linz), Jordi Cabot (Barcelona), Jean Goubault-Larrecq (Cachan), Jan-Friso Groote (Eindhoven), Esther Guerra (Madrid), Jurriaan Hage (Utrecht), Reiko Heckel (Leicester), Panagiotis Katsaros (Thessaloniki), Stefan Kiefer (Oxford), Barbara König (Duisburg), Fabrice Kordon (Paris), Jan Kretinsky (Munich), Kim G. Larsen (Aalborg), Tiziana Margaria (Limerick), Peter Müller (Zurich), Catuscia Palamidessi (Palaiseau), Dave Parker (Birmingham), Andrew M. Pitts (Cambridge), Peter Ryan (Luxembourg), Don Sannella (Edinburgh), Bernhard Steffen (Dortmund), Mariëlle Stoelinga (Twente), Gabriele Taentzer (Marburg), Christine Tasson (Paris), Peter Thiemann (Freiburg), Jan Vitek (Prague), Heike Wehrheim (Paderborn), Anton Wijs (Eindhoven), and Nobuko Yoshida (London).

I would like to take this opportunity to thank all speakers, attendants, organizers of the satellite workshops, and Springer for their support. I hope you all enjoyed ETAPS 2020. Finally, a big thanks to Tiziana and her local organization team for all their enormous efforts enabling a fantastic ETAPS in Dublin!

February 2020

Marieke Huisman
ETAPS SC Chair
ETAPS e.V. President

Preface

Welcome to the European Symposium on Programming (ESOP 2020)! The 29th edition of this conference series was initially planned to be held April 27–30, 2020, in Dublin, Ireland, but was then moved to fall 2020 due to the COVID-19 outbreak. ESOP is one of the European Joint Conferences on Theory and Practice of Software (ETAPS). It is devoted to fundamental issues in the specification, design, analysis, and implementation of programming languages and systems.

This volume contains 27 papers, which the Program Committee (PC) selected among 87 submissions. Each submission received between three and six reviews. After an author response period, the papers were discussed electronically among the PC members and external reviewers. The one paper for which the PC chair had a conflict of interest was kindly handled by Sasa Misailovic.

Submissions authored by a PC member were held to slightly higher standards: they received at least four reviews, had an external reviewer, and were accepted only if they were not involved in comparisons of relative merit with other submissions. We accepted two out of four PC submissions.

The final program includes a keynote by Işıl Dillig on “Formal Methods for Evolving Database Applications.”

Any conference depends first and foremost on the quality of its submissions. I would like to thank all the authors who submitted their work to ESOP 2020! I am truly impressed by the members of the PC. They produced insightful and constructive reviews, contributed very actively to the online discussions, and were extremely helpful. It was an honor to work with all of you! I am also grateful to the external reviewers, who provided their expert opinions and helped tremendously to reach well-informed decisions. I would like to thank everybody who contributed to the organization of ESOP 2020, especially the ESOP 2020 Steering Committee and its chair Peter Thiemann as well as the ETAPS 2020 Steering Committee and its chair Marieke Huisman, who provided help and guidance on numerous occasions. Finally, I’d like to thank Linard Arquint and Vasileios Koutavas for their help with the proceedings.

February 2020

Peter Müller

Organization

Program Committee

Elvira Albert	Universidad Complutense de Madrid, Spain
Sophia Drossopoulou	Imperial College London, UK
Jean-Christophe Filliatre	LRI, CNRS, France
Arie Gurfinkel	University of Waterloo, Canada
Jan Hoffmann	Carnegie Mellon University, USA
Ranjit Jhala	University of California at San Diego, USA
Woosuk Lee	Hanyang University, South Korea
Rustan Leino	Amazon Web Services, USA
Rupak Majumdar	MPI-SWS, Germany
Roland Meyer	Technische Universität Braunschweig, Germany
Antoine Miné	LIP6, Sorbonne Université, France
Sasa Misailovic	University of Illinois at Urbana-Champaign, USA
Toby Murray	University of Melbourne, Australia
Peter Müller	ETH Zurich, Switzerland
David Naumann	Stevens Institute of Technology, USA
Zvonimir Rakamaric	University of Utah, USA
Francesco Ranzato	University of Padova, Italy
Sukyoung Ryu	KAIST, South Korea
Ilya Sergey	Yale-NUS College and National University of Singapore, Singapore
Alexandra Silva	University College London, UK
Nikhil Swamy	Microsoft Research, USA
Sam Tobin-Hochstadt	Indiana University Bloomington, USA
Caterina Urban	Inria Paris, France
Viktor Vafeiadis	MPI-SWS, Germany

Additional Reviewers

Amtoft, Torben	Brady, Edwin
Arenas, Puri	Brunet, Paul
Balabonski, Thibaut	Caires, Luís
Bernardy, Jean-Philippe	Charguéraud, Arthur
Bierman, Gavin	Chini, Peter
Blanchet, Bruno	Chudnov, Andrey
Bonchi, Filippo	Correas Fernández, Jesús
Bonelli, Eduardo	Costea, Andreea
Botbol, Vincent	Cousot, Patrick
Bourke, Timothy	Crole, Roy

Cusumano-Towner, Marco
Dagand, Pierre-Evariste
Dahlqvist, Fredrik
Dang, Hai
Danielsson, Nils Anders
Das, Ankush
Enea, Constantin
Finkbeiner, Bernd
Fromherz, Aymeric
Fuhs, Carsten
Genaim, Samir
Genitrini, Antoine
Ghica, Dan
Gordillo, Pablo
Gordon, Colin S.
Haas, Thomas
Hage, Jurriaan
He, Shaobo
Heljanko, Keijo
Jourdan, Jacques-Henri
Kahn, David
Kang, Jeehoon
Kuderski, Jakub
Lahav, Ori
Laurent, Olivier
Lee, Dongkwon
Lee, Wonyeol
Lesani, Mohsen
Levy, Paul Blain
Lindley, Sam
Martin-Martin, Enrique
Mohan, Anshuman
Mordido, Andreia
Morris, J. Garrett

Muller, Stefan
Ngo, Minh
Oh, Hakjoo
Ouedjaout, Abdelraouf
Ouederni, Meriem
Palamidessi, Catuscia
Pearlmutter, Barak
Peters, Kirstin
Pham, Long
Poli, Federico
Polikarpova, Nadia
Pottier, François
Rival, Xavier
Román-Díez, Guillermo
Sammartino, Matteo
Sasse, Ralf
Scalas, Alceste
Scherer, Gabriel
Sieczkowski, Filip
Sivaramakrishnan, Kc
Staton, Sam
Stutsman, Ryan
Tan, Yong Kiam
van den Brand, Mark
Vákár, Matthijs
Wang, Di
Wang, Meng
Wehrheim, Heike
Weng, Shu-Chun
Wies, Thomas
Wijesekera, Duminda
Wolff, Sebastian
Zufferey, Damien

Formal Methods for Evolving Database Applications (Abstract of Keynote Talk)

Işıl Dillig

University of Texas at Austin, USA
isil@cs.utexas.edu

Many database applications undergo significant schema changes during their life cycle due to performance or maintainability reasons. Examples of such schema changes include denormalization, splitting a single table into multiple tables, and consolidating multiple tables into a single table. Even though such schema refactorings are quite common in practice, programmers need to spend significant time and effort to re-implement parts of the code base that are affected by the schema change. Furthermore, it is not uncommon to introduce bugs during this code transformation process.

In this talk, I will present our recent work on using formal methods to simplify the schema refactoring process for evolving database applications. Specifically, I will first propose a definition of equivalence between database applications that operate over different schemas. Building on this definition, I will then present a fully automated technique for proving equivalence between a pair of applications. Our verification technique is capable of automatically synthesizing bisimulation invariants between two database applications and uses the inferred bisimulation invariant to automatically prove equivalence.

In the next part of the talk, I will explain how to leverage this verification technique to completely automate the code migration process. Specifically, given an original database application P over schema S and a new schema S' , I will discuss a practical program synthesis technique that can be used to generate a new program P' over schema S' such that P and P' are provably equivalent. In particular, I will first present a method for generating a program sketch of the new version; then, I will describe a novel synthesis algorithm that efficiently explores the space of all programs that are in the search space of the generated sketch.

Finally, I will describe experimental results on a suite of schema refactoring benchmarks, including real-world database applications written in Ruby-on-Rails. I will also outline remaining challenges in this area and motivate future research directions relevant to research in programming languages and formal methods.

Contents

Trace-Relating Compiler Correctness and Secure Compilation	1
<i>Carmine Abate, Roberto Blanco, Ștefan Ciobâcă, Adrien Durier, Deepak Garg, Cătălin Hrițcu, Marco Patrignani, Éric Tanter, and Jérémy Thibault</i>	
Runners in Action	29
<i>Danel Ahman and Andrej Bauer</i>	
On the Versatility of Open Logical Relations: Continuity, Automatic Differentiation, and a Containment Theorem	56
<i>Gilles Barthe, Raphaëlle Crubillé, Ugo Dal Lago, and Francesco Gavazzo</i>	
Constructive Game Logic	84
<i>Rose Bohrer and André Platzer</i>	
Optimal and Perfectly Parallel Algorithms for On-demand Data-Flow Analysis	112
<i>Krishnendu Chatterjee, Amir Kafshdar Goharshady, Rasmus Ibsen-Jensen, and Andreas Pavlogiannis</i>	
Concise Read-Only Specifications for Better Synthesis of Programs with Pointers	141
<i>Andreea Costea, Amy Zhu, Nadia Polikarpova, and Ilya Sergey</i>	
Soundness Conditions for Big-Step Semantics	169
<i>Francesco Dagnino, Viviana Bono, Elena Zucca, and Mariangiola Dezani-Ciancaglini</i>	
Liberate Abstract Garbage Collection from the Stack by Decomposing the Heap	197
<i>Kimball Germane and Michael D. Adams</i>	
SMT-Friendly Formalization of the Solidity Memory Model	224
<i>Ákos Hajdu and Dejan Jovanović</i>	
Exploring Type-Level Bisimilarity towards More Expressive Multiparty Session Types	251
<i>Sung-Shik Jongmans and Nobuko Yoshida</i>	
Verifying Visibility-Based Weak Consistency	280
<i>Siddharth Krishna, Michael Emmi, Constantin Enea, and Dejan Jovanović</i>	

Local Reasoning for Global Graph Properties	308
<i>Siddharth Krishna, Alexander J. Summers, and Thomas Wies</i>	
Aneris: A Mechanised Logic for Modular Reasoning about Distributed Systems	336
<i>Morten Krogh-Jespersen, Amin Timany, Marit Edna Ohlenbusch, Simon Oddershede Gregersen, and Lars Birkedal</i>	
Continualization of Probabilistic Programs With Correction	366
<i>Jacob Laurel and Sasa Misailovic</i>	
Semantic Foundations for Deterministic Dataflow and Stream Processing. . . .	394
<i>Konstantinos Mamouras</i>	
Connecting Higher-Order Separation Logic to a First-Order Outside World	428
<i>William Mansky, Wolf Honoré, and Andrew W. Appel</i>	
Modular Inference of Linear Types for Multiplicity-Annotated Arrows	456
<i>Kazutaka Matsuda</i>	
RustHorn: CHC-Based Verification for Rust Programs.	484
<i>Yusuke Matsushita, Takeshi Tsukada, and Naoki Kobayashi</i>	
A First-Order Logic with Frames	515
<i>Adithya Murali, Lucas Peña, Christof Löding, and P. Madhusudan</i>	
Proving the Safety of Highly-Available Distributed Objects	544
<i>Sreeja S. Nair, Gustavo Petri, and Marc Shapiro</i>	
Solving Program Sketches with Large Integer Values	572
<i>Rong Pan, Qinheping Hu, Rishabh Singh, and Loris D’Antoni</i>	
Modular Relaxed Dependencies in Weak Memory Concurrency	599
<i>Marco Paviotti, Simon Cooksey, Anouk Paradis, Daniel Wright, Scott Owens, and Mark Batty</i>	
ARMv8-A System Semantics: Instruction Fetch in Relaxed Architectures. . . .	626
<i>Ben Simner, Shaked Flur, Christopher Pulte, Alasdair Armstrong, Jean Pichon-Pharabod, Luc Maranget, and Peter Sewell</i>	
Higher-Ranked Annotation Polymorphic Dependency Analysis.	656
<i>Fabian Thorand and Jurriaan Hage</i>	
ConSORT: Context- and Flow-Sensitive Ownership Refinement Types for Imperative Programs.	684
<i>John Toman, Ren Siqi, Kohei Suenaga, Atsushi Igarashi, and Naoki Kobayashi</i>	

Mixed Sessions 715
*Vasco T. Vasconcelos, Filipe Casal, Bernardo Almeida,
and Andreia Mordido*

Higher-Order Spreadsheets with Spilled Arrays 743
*Jack Williams, Nima Joharizadeh, Andrew D. Gordon,
and Advait Sarkar*

Author Index 771