

Principled Software Development

Peter Müller • Ina Schaefer

Editors

Principled Software Development

Essays Dedicated to Arnd Poetzsch-Heffter
on the Occasion of his 60th Birthday



Springer

Editors

Peter Müller
Department of Computer Science
ETH Zürich
Zürich, Switzerland

Ina Schaefer
Institut für Softwaretechnik und
Fahrzeuginformatik
Technische Universität Braunschweig
Braunschweig, Germany

ISBN 978-3-319-98046-1 ISBN 978-3-319-98047-8 (eBook)
<https://doi.org/10.1007/978-3-319-98047-8>

Library of Congress Control Number: 2018951062

© Springer Nature Switzerland AG 2018

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, express 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.

Cover illustration: © Cover Photograph: Edel Modschiedler

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

Preface

University professors have the great privilege that they can impact society in three major ways: by contributing scientific results and advising PhD students, by educating students, and through political and managerial work that shapes the research and education infrastructures that will allow future generations to accomplish their goals.

Arnd Poetzsch-Heffter is among the few professors who have been very successful in all three dimensions. Throughout his career, he has made major scientific contributions in a wide range of topics related to programming languages, software technology, and formal methods; he has been a passionate and demanding teacher and advisor, and he advanced TU Kaiserslautern as Department Chair and Vice President for Research, Technology, and Innovation. This book honors Arnd's achievements on the occasion of his 60th birthday.

Arnd studied Computer Science at TU Munich, where he also obtained his PhD in 1991 with a thesis on the Formal Specification of Context-Sensitive Syntax of Programming Languages. In 1997, Arnd obtained his habilitation with a thesis on the Specification and Verification of Object-Oriented Programs, also from TU Munich. He was Associate Professor at the University of Hagen from 1996 to 2002, has been Full Professor at TU Kaiserslautern since 2002, and Vice President since 2014.

This book contains articles related to Arnd's broad research interests including, among others, implementation of programming languages, formal semantics, specification and verification of object-oriented and concurrent programs, programming language design, distributed systems, software modeling, and software product lines. We collected the contributions by contacting Arnd's collaborators, colleagues, and former students. We were overwhelmed by the positive reactions. As a result, this book contains a collection of high-quality articles, presenting original research results, major case studies, and inspiring visions. Some of the work included in this book will be presented at a symposium to be held in Kaiserslautern in November 2018.

We would like to thank the authors for contributing to this book, Alexandra Bugariu, Marco Eilers, Sascha Lity, Stephan Mennicke, Tobias Runge, Sven Schuster, and Arshavir Ter-Gabrielyan for their help with copy-editing, Alexander Knüppel for compiling the LaTeX sources, Arnd's wife Edel Modschiedler for her stealth operation to take the picture on the book cover, and Annette Bieniusa for her help with the organization of the symposium. Our biggest thanks goes to Arnd Poetzsch-Heffter for being a truly exceptional PhD advisor and a role model to aspire to. Happy Birthday!

Zürich, Switzerland
Braunschweig, Germany
June 2018

Peter Müller
Ina Schaefer

Contents

Smart Contracts: A Killer Application for Deductive Source Code Verification	1
Wolfgang Ahrendt, Gordon J. Pace, and Gerardo Schneider	
A Methodology for Invariants, Framing, and Subtyping in JML	19
Yuyan Bao and Gary T. Leavens	
Trends in Relational Program Verification	41
Bernhard Beckert and Mattias Ulbrich	
Collaborative Work Management with a Highly-Available Kanban Board	59
Annette Bieniusa, Peter Zeller, and Shraddha Barke	
A Case for Certifying Compilers in Industrial Automation	73
Jan Olaf Blech	
Compositional Semantics for Concurrent Object Groups in ABS.....	87
Frank S. de Boer and Stijn de Gouw	
Same Same But Different: Interoperability of Software Product Line Variants	99
Ferruccio Damiani, Reiner Hähnle, Eduard Kamburjan, and Michael Lienhardt	
A Hoare Logic Contract Theory: An Exercise in Denotational Semantics	119
Dilian Gurov and Jonas Westman	
Towards Reliable Concurrent Software	129
Marieke Huisman and Sebastiaan J. C. Joosten	
Dynamic Software Updates and Context Adaptation for Distributed Active Objects	147
Einar Broch Johnsen and Ingrid Chieh Yu	

Using CSP to Develop Quality Concurrent Software	165
Derrick G. Kourie, Tinus Strauss, Loek Cleophas, and Bruce W. Watson	
Modular Verification Scopes via Export Sets and Translucent Exports ...	185
K. Rustan M. Leino and Daniel Matichuk	
The Binomial Heap Verification Challenge in Viper	203
Peter Müller	
Abstract and Concrete Data Types vs Object Capabilities	221
James Noble, Alex Potanin, Toby Murray, and Mark S. Miller	
A Personal History of Delta Modelling	241
Ina Schaefer	
Are Synchronous Programs Logic Programs?	251
Klaus Schneider and Marc Dahlem	
Illi Isabellistes Se Custodes Egregios Praestabant	267
Simon Bischof, Joachim Breitner, Denis Lohner, and Gregor Snelting	
Reasoning About Weak Semantics via Strong Semantics	283
Roland Meyer and Sebastian Wolff	
Recipes for Coffee: Compositional Construction of JAVA Control	
Flow Graphs in GROOVE	305
Eduardo Zambon and Arend Rensink	