

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Bertrand Meyer Martin Nordio (Eds.)

# Tools for Practical Software Verification

LASER, International Summer School 2011  
Elba Island, Italy  
Revised Tutorial Lectures



Springer

## Volume Editors

Bertrand Meyer  
Martin Nordio  
ETH Zurich  
Clausiusstrasse 59  
8092 Zurich, Switzerland  
E-mail: {bertrand.meyer, martin.nordio}@inf.ethz.ch

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-35745-9 e-ISBN 978-3-642-35746-6  
DOI 10.1007/978-3-642-35746-6  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012954174

CR Subject Classification (1998): D.2.4, F.3.1, F.3.3, D.1.5-6, D.3.3, F.4.1, K.6.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

The LASER summer school, organized by the Chair of Software Engineering at ETH Zurich, brings together concepts and practices of software engineering. Since its inception in 2004, each year the LASER summer school has focused on an important software engineering topic. This volume contains selected lecture notes from the 8th LASER Summer School on Software Engineering: Tools for Practical Software Verification held during September 4–10, 2011 in Elba Island, Italy.

This book contains contributions by Edmund Clarke, William Klieber, Milos Novacek, and Paolo Zuliani on model checking; Patrice Godefroid and Shuvendu K. Lahiri on approaches for representing programs by logic formulas; Cesar Munoz and Ramiro Demasi on advanced theorem-proving techniques in PVS; Christine Paulin-Mohring on an introduction to the Coq proof-assistant; Julian Tschannen, Carlo Alberto Furia, Martin Nordio, and Bertrand Meyer on automatic verification of advanced object-oriented features; and Luke Herbert, K. Rustan, M. Leino, and Jose Quaresma on program verification using Dafny.

We would like to thank the lecturers and their co-authors for contributing to this volume. We thank Nazareno Aguirre, Cristina Cornes, Dino Distefano, Diego Garbervetsky, Max (Yu) Pei, Nadia Polikarpova, Julian Tschannen, and Christoph Wintersteiger for their feedback on drafts of the papers. We are grateful to Claudia Günthart, Nadia Polikarpova, Julian Tschannen, and the members of the ETH Chair of Software Engineering for assisting with the organization of the LASER summer school. We thank Microsoft and ETH Zurich for their financial support.

September 2012

Bertrand Meyer  
Martin Nordio

# Table of Contents

Model Checking and the State Explosion Problem . . . . .	1
<i>Edmund M. Clarke, William Klieber, Miloš Nováček, and Paolo Zuliani</i>	
From Program to Logic: An Introduction . . . . .	31
<i>Patrice Godefroid and Shuvendu K. Lahiri</i>	
Introduction to the Coq Proof-Assistant for Practical Software Verification . . . . .	45
<i>Christine Paulin-Mohring</i>	
Advanced Theorem Proving Techniques in PVS and Applications . . . . .	96
<i>César A. Muñoz and Ramiro A. Demasi</i>	
Automatic Verification of Advanced Object-Oriented Features: The AutoProof Approach . . . . .	133
<i>Julian Tschannen, Carlo Alberto Furia, Martin Nordio, and Bertrand Meyer</i>	
Using Dafny, an Automatic Program Verifier . . . . .	156
<i>Luke Herbert, K. Rustan M. Leino, and Jose Quaresma</i>	
<b>Author Index</b> . . . . .	183