

# Formal System Verification

Rolf Drechsler  
Editor

# Formal System Verification

State-of-the-Art and Future Trends

 Springer

*Editor*  
Rolf Drechsler  
DFKI  
University of Bremen  
Bremen  
Germany

ISBN 978-3-319-57683-1                      ISBN 978-3-319-57685-5 (eBook)  
DOI 10.1007/978-3-319-57685-5

Library of Congress Control Number: 2017938317

© Springer International Publishing 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.

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

*To Fatma Akin*

# Preface

For more than four decades the complexity of circuits and systems has grown according to Moore's Law resulting in chips of several billion components. While already the synthesis on the different levels from the initial specification down to the layout is a challenging task, for all the individual steps the correctness has to be considered.

In the past, classical approaches based on simulation or emulation have been used. But these techniques do not scale well and reach their limits. Correctness can only be ensured by the use of formal methods. These techniques were proposed more than 30 years ago in the context of circuit and system design, and in the meantime exist very powerful tools that are used in industry for specific tasks, like the equivalence check of netlists on the Register Transfer Level (RTL).

But with increasing complexity of the systems there is a high demand for tools that are better scalable and also consider modeling beyond plain digital circuits. In this context analog and mixed signal circuits have to be included on the lower level, but also hardware-dependent software towards the higher levels of abstraction.

In this book, these advanced topics of using formal verification along the design flow with a special focus on the system level are addressed. World's leading researchers have contributed chapters, where they describe the underlying problems, possible solutions, and directions for future work.

The chapters in the order as they appear in this book are:

- *Formal Techniques for Verification and Coverage Analysis of Analog Systems* by Andreas Fürtig and Lars Hedrich
- *Verification of Incomplete Designs* by Bernd Becker, Christoph Scholl and Ralf Wimmer
- *Probabilistic Model Checking: Advances and Applications* by Marta Kwiatkowska, Gethin Norman and David Parker
- *Software in a Hardware View: New Models for HW-dependent Software in SoC Verification* by Carlos Villarraga, Dominik Stoffel and Wolfgang Kunz
- *Formal Verification—The Industrial Perspective* by Raik Brinkmann and David Kelf

On the different abstraction layers it is shown in which way formal methods can assist today to ensure functional correctness. The contributed chapters cover not only the latest results in academia but also descriptions of industrial tools and perspectives.

Bremen, Germany  
June 2017

Rolf Drechsler

# Acknowledgements

All contributions in this edited volume have been anonymously reviewed. I would like to express my thanks for the valuable comments of the reviewers and their fast feedback. Here, I also like to thank all the authors who did a great job in submitting contributions of a very high quality. My special thanks go to Daniel Große and Jannis Stoppe from my group in Bremen in helping with the preparation of the book. Finally, I would like to thank Nicole Lowary and Charles Glaser from Springer. All this would not have been possible without their steady support.

Bremen, Germany  
June 2017

Rolf Drechsler

# Contents

<b>1 Formal Techniques for Verification and Coverage Analysis of Analog Systems</b> . . . . .	1
Andreas Fürtig and Lars Hedrich	
1.1 Introduction . . . . .	1
1.2 State of the Art . . . . .	2
1.3 State-Space Description . . . . .	4
1.3.1 Solving a DAE System . . . . .	5
1.3.2 Analog Transition System . . . . .	6
1.4 Verification Methodology . . . . .	9
1.4.1 Model Checking . . . . .	10
1.4.2 Analog Specification Language (ASL) . . . . .	10
1.4.3 ASL-Example: Verification of Oscillation and Oscillator Voltage Sensitivity . . . . .	11
1.4.4 Model Checking of an SRAM Cell . . . . .	13
1.5 State Space Coverage . . . . .	15
1.5.1 State-Space Coverage Calculation . . . . .	15
1.5.2 Coverage Maximization Algorithm . . . . .	17
1.5.3 Path Planning . . . . .	18
1.6 $\lambda$ State-Space Coverage . . . . .	19
1.7 Coverage Analysis and Optimization Results . . . . .	22
1.7.1 Detailed Case Study of a Level-Shifter Circuit . . . . .	25
1.8 System-Level Verification . . . . .	27
1.8.1 System Refinement and Verification . . . . .	30
1.9 Conclusion . . . . .	32
References . . . . .	33
<b>2 Verification of Incomplete Designs</b> . . . . .	37
Bernd Becker, Christoph Scholl and Ralf Wimmer	
2.1 Introduction . . . . .	37
2.2 Preliminaries . . . . .	40



2.3	Incomplete Combinational Circuits	42
2.3.1	The Partial Equivalence Checking Problem (PEC)	43
2.3.2	SAT-based Approximations	44
2.3.3	QBF-based Methods	46
2.3.4	DQBF-based Methods	47
2.4	Incomplete Sequential Circuits	48
2.4.1	BMC for Incomplete Designs	50
2.4.2	Model Checking for Incomplete Designs	56
2.5	Conclusion	69
	References	70
<b>3</b>	<b>Probabilistic Model Checking: Advances and Applications</b>	<b>73</b>
	Marta Kwiatkowska, Gethin Norman and David Parker	
3.1	Introduction	73
3.2	Probabilistic Model Checking	74
3.2.1	Discrete-Time Markov Chains	75
3.2.2	Markov Decision Processes	82
3.2.3	Stochastic Multi-player Games	85
3.2.4	Tool Support	87
3.3	Controller Synthesis	88
3.3.1	Controller Synthesis for MDPs	88
3.3.2	Multi-objective Controller Synthesis	91
3.4	Modelling and Verification of Large Probabilistic Systems	93
3.4.1	Compositional Modelling of Probabilistic Systems	94
3.4.2	Compositional Probabilistic Model Checking	95
3.4.3	Quantitative Abstraction Refinement	97
3.4.4	Case Study: The Zeroconf Protocol	99
3.5	Real-Time Probabilistic Model Checking	100
3.5.1	Probabilistic Timed Automata	100
3.5.2	Continuous-Time Markov Chains	107
3.6	Parametric Probabilistic Model Checking	109
3.6.1	Parametric Model Checking for DTMCs	109
3.6.2	Parametric Model Checking for Other Probabilistic Models	112
3.7	Future Challenges and Directions	112
	References	115
<b>4</b>	<b>Software in a Hardware View</b>	<b>123</b>
	Carlos Villarraga, Dominik Stoffel and Wolfgang Kunz	
4.1	Introduction	123
4.2	Program Netlists	125
4.2.1	Basic Idea	127
4.2.2	Model Generation	128
4.2.3	Modeling Memory and I/O	129

- 4.3 Verification Scenarios for HW-dependent Software . . . . . 131
- 4.4 Equivalence Checking of HW-dependent Software . . . . . 133
  - 4.4.1 Sequence-Based Model of the HW/SW Interface . . . . . 134
  - 4.4.2 Software Miter . . . . . 138
  - 4.4.3 Equivalence Checking Using SAT . . . . . 139
  - 4.4.4 Experimental Results . . . . . 140
- 4.5 Cycle-Accurate HW/SW Co-verification of Firmware-Based Designs . . . . . 144
  - 4.5.1 Joint Hardware/Firmware Model . . . . . 144
  - 4.5.2 Timed Interface Model . . . . . 145
  - 4.5.3 Experimental Results . . . . . 150
- 4.6 Conclusion . . . . . 152
- References . . . . . 153
- 5 Formal Verification—The Industrial Perspective . . . . . 155**
  - Raik Brinkmann and Dave Kelf
  - 5.1 Introduction . . . . . 155
  - 5.2 Automating Design Verification with Formal . . . . . 156
    - 5.2.1 Design Inspection . . . . . 156
    - 5.2.2 IP Integration Verification . . . . . 161
    - 5.2.3 Verification of Design Transformations . . . . . 168
  - 5.3 Assertion-Based Verification of IP Blocks . . . . . 171
    - 5.3.1 Assertions in the Verification Flow . . . . . 171
    - 5.3.2 Verification Planning . . . . . 174
    - 5.3.3 Quantitative Analysis and Coverage . . . . . 175
  - 5.4 Challenges Ahead . . . . . 177
    - 5.4.1 High-Level Design . . . . . 178
    - 5.4.2 High Reliability and Safety Critical Systems . . . . . 178
    - 5.4.3 Hardware Security . . . . . 180
    - 5.4.4 Low-Power Devices . . . . . 181
  - References . . . . . 182

# Editors and Contributors

## About the Editor

**Rolf Drechsler** received the Diploma and Dr. Phil. Nat. degrees in Computer Science from J. W. Goethe University Frankfurt am Main, Germany, in 1992 and 1995, respectively. He was with the Institute of Computer Science, Albert-Ludwigs University, Freiburg im Breisgau, Germany, from 1995 to 2000, and with the Corporate Technology Department, Siemens AG, Munich, Germany, from 2000 to 2001. Since October 2001, he has been with the University of Bremen, Bremen, Germany, where he is currently Full Professor and the Head of the Group for Computer Architecture, Institute of Computer Science. Since 2011 he is also the director of the Cyber-Physical Systems group at the German Research Center for Artificial Intelligence (DFKI) in Bremen. His research interests include the development and design of data structures and algorithms with a focus on circuit and system design.

## Contributors

**Bernd Becker** Institute of Computer Science, Albert-Ludwigs-Universität Freiburg, Freiburg im Breisgau, Germany

**Raik Brinkmann** OneSpin Solutions, Munich, Germany

**Andreas Fürtig** University of Frankfurt, Frankfurt/Main, Germany

**Lars Hedrich** University of Frankfurt, Frankfurt/Main, Germany

**Dave Kelf** OneSpin Solutions, Munich, Germany

**Wolfgang Kunz** Department of Electrical and Computer Engineering, University of Kaiserslautern, Kaiserslautern, Germany

**Marta Kwiatkowska** Department of Computer Science, University of Oxford, Oxford, UK

**Gethin Norman** School of Computing Science, University of Glasgow, Glasgow, UK

**David Parker** School of Computer Science, University of Birmingham, Birmingham, UK

**Christoph Scholl** Institute of Computer Science, Albert-Ludwigs-Universität Freiburg, Freiburg im Breisgau, Germany

**Dominik Stoffel** Department of Electrical and Computer Engineering, University of Kaiserslautern, Kaiserslautern, Germany

**Carlos Villarraga** Department of Electrical and Computer Engineering, University of Kaiserslautern, Kaiserslautern, Germany

**Ralf Wimmer** Institute of Computer Science, Albert-Ludwigs-Universität Freiburg, Freiburg im Breisgau, Germany