

Contents

1	Formal Techniques for Verification and Coverage Analysis of Analog Systems	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	λ 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
2	Verification of Incomplete Designs	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
3	Probabilistic Model Checking: Advances and Applications	73
	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
4	Software in a Hardware View	123
	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

Formal System Verification

State-of the-Art and Future Trends

Drechsler, R. (Ed.)

2018, XVI, 182 p. 71 illus., 49 illus. in color., Hardcover

ISBN: 978-3-319-57683-1