

Table of Contents

Preface	V
List of Contributors	1
Symbolic Trajectory Evaluation	
Scott Hazelhurst and Carl-Johan H. Seger	3
1. Introduction	3
1.1 Overview of STE and Verification Method	3
1.2 History of Symbolic Trajectory Evaluation	5
1.3 Outline of Chapter	6
2. Related Work	7
2.1 Model Checking Algorithms	7
2.2 Abstraction	8
2.3 Compositional Reasoning	9
3. Basics	10
3.1 The Model Structure	11
3.2 The Quaternary Logic Q	12
3.3 The Temporal Logic	14
4. Modelling Hardware	21
4.1 Modelling Issues	21
4.2 Circuit Models as State Spaces	22
5. Specification and Proof Techniques	24
5.1 Verification Assertions	24
5.2 Trajectory Evaluation	25
5.3 Compositional Theory	32
5.4 The Voss Verification System: The Front End	39
5.5 Verification Style	40
6. Experimental Work	41
6.1 Benchmark 11: BlackJack Dealer	42
6.2 Benchmark 17: Multiplier	44
6.3 IEEE FP Multiplier	49
6.4 Benchmark 21: One Dimensional Systolic Array	49
6.5 Benchmark 22: Two Dimensional Systolic Array	54

VIII Table of Contents

6.6	Benchmark 20: Associative Memory	58
6.7	Liveness Properties: Benchmarks 7 and 12	62
7.	Conclusion	65
7.1	Summary	65
7.2	Limitations of Specification	65
7.3	Tool-Building Experience	66
7.4	Future work	68
A.	Appendix	69
A.1	Benchmark 17	69
A.2	FL Code for Proof of Multiplier	76

Verification with Abstract State Machines Using MDGs

E. Cerny, F. Corella, M. Langevin, X. Song, S. Tahar, and Z. Zhou . . . 79

1.	Introduction	79
1.1	Motivations	79
1.2	Limitations of the Approach	80
1.3	Related Work	81
1.4	Outline	83
2.	Foundations of the Methodology	84
2.1	Logic	84
2.2	Multiway Decision Graphs	87
2.3	Abstract State Machines	93
3.	Modeling Hardware with MDGs	96
4.	MDG-based Verification Techniques	99
4.1	Combinational Circuits	99
4.2	Sequential Circuits	100
5.	Verification of Benchmark Circuits	103
6.	Fairisle ATM Switch Fabric: A Case Study in Verification using MDGs	104
6.1	The Fairisle ATM Switch Fabric	105
6.2	MDG Models	107
6.3	Verification	109
7.	Conclusions and Future Work	112

Design Verification Using SYNCHRONIZED TRANSITIONS

Jørgen Staunstrup

1.	Introduction	114
2.	Related Work	115
3.	Basics	116
3.1	Notation	116
3.2	Design of a Black-Jack Dealer	122
3.3	Translation	124
4.	Modeling Hardware	124
4.1	Direct Realizations	125
4.2	Clocked Realizations	127

4.3	Modeling Existing Circuits	128
4.4	Evaluation	129
5.	Verification Technique	130
5.1	Inductive Verification	131
5.2	Mechanization	132
5.3	Modular Designs	133
5.4	Evaluation	135
5.5	Liveness Properties	136
6.	Refinement	137
6.1	Design of the Single-Pulser	138
6.2	Formal Verification of Refinement	140
6.3	Evaluation	142
7.	Synchronous Designs	142
7.1	The lSyst	142
7.2	The Synchronous Combinator	143
7.3	Quantification	145
8.	Experimental Results	146
8.1	Verifying the Black-Jack Design	146
8.2	Single Pulser	147
8.3	lSyst	148
8.4	FIFO Queue	148
8.5	Arbiter	151
8.6	Evaluation	153
9.	Conclusion	154

Hardware Verification Using PVS

Mandayam Srivas, Harald Rueß, and David Cyrluk	156
1. Introduction	156
2. Related Work	157
3. Basics	158
3.1 The Specification Language	158
3.2 The Proof Checker	160
3.3 Ground Decision Procedures and Rewriting	160
3.4 The Power of Interaction	162
3.5 Integration of Model Checking into PVS	162
3.6 High-Level Strategies	164
4. Modeling Hardware	164
4.1 Predicative Style Specifications	165
4.2 Functional Style Specifications	168
4.3 Functional Description of Combinational Circuits	171
4.4 Generic Hardware Components	173
5. Microprocessor Verification	174
5.1 A Historical Perspective of Microprocessor Verification	174
5.2 General Microprocessor Correctness	175

X Table of Contents

5.3	A General PVS Framework for Verifying Microprocessors	176
5.4	Formalizing the Correctness Condition	177
5.5	Verifying the Tamarack Processor	179
5.6	Verifying Pipelined Microprocessors	183
5.7	Mechanization of Proofs of Verification Conditions	189
5.8	Verification of Industrial-Strength Microprocessors	190
6.	Verification of Arithmetic Circuits	192
6.1	Verification of Iterative Array Multipliers	193
6.2	Verification of SRT Division	197
7.	Experimental Results	200
7.1	Verifying the Single Pulser	200
7.2	Verifying the Arbiter	201
7.3	Verifying the Black-Jack Design	204
7.4	Verifying the FIR Filter	204
8.	Conclusions	205

Verifying VHDL Designs with COSPAN

Kathi Fisler and Robert P. Kurshan	206
1. Introduction	206
2. Related Work	209
3. The Program Semantics	210
4. The Semantics of Verification	214
5. Operational Verification	219
6. Experimental Results	222
6.1 Single Pulser	223
6.2 Arbiter	228
6.3 Systolic Array Element	230
6.4 BlackJack Dealer	234
6.5 Car Seat Controller	235
7. Summary	244
A. Appendix: Automata Definitions	244
A.1 AssumeAlways_()	245
A.2 Never_()	245
A.3 After_Eventually_()	246
A.4 PHASE	246
A.5 After_Never_Unless_()	247
A.6 After_Eventually_Unless_()	247

The CQS System

Klaus Schneider and Thomas Kropf	248
1. Introduction	248
2. Related Work	252
2.1 Hardware Verification Using Temporal Logics	252
2.2 Hardware Verification Based on Predicate Logics	254

2.3 Combined Approaches	255
2.4 Outline of the Chapter	256
3. Basics	257
3.1 Underlying Formalism of CQS	257
3.2 Fair Prefix Automata	261
3.3 Rewrite-Based Theorem Proving for Abstract Data Types	262
4. Modelling Hardware	265
4.1 Describing Nongeneric Structures	266
4.2 Describing Regular Structures	268
5. Specification and Proof	273
5.1 The Unifying Principle	273
5.2 Strategies for Verifying Temporal Behavior	274
5.3 Translating LTL Formulas into Fair Prefix Formulae	275
5.4 Strategies for Verifying Abstract Data Types	282
5.5 Combining the Strategies	284
6. Experimental Results	285
6.1 Single Pulser	286
6.2 Black Jack Dealer	287
6.3 Safe Box	291
6.4 The Island Tunnel Controller	297
6.5 Arbiter	303
6.6 Von Neumann Adder	307
6.7 Sequential Multiplier Circuits	310
6.8 Systolic Arrays	312
6.9 GSM Speech Encoding	317
7. Conclusions	328

Appendix: The Common Book Examples

Thomas Kropf	330
1. Introduction	330
2. Single Pulser	330
2.1 Introduction	331
2.2 Specification	331
2.3 Implementation	331
2.4 Acknowledgements	332
3. Arbiter	332
3.1 Introduction	332
3.2 Specification	332
3.3 Implementation	333
3.4 Acknowledgments	334
4. Black-Jack Dealer	334
4.1 Specification	334
4.2 Implementation	334
4.3 Acknowledgments	337

XII Table of Contents

5. 1Syst (Filter) 337

5.1 Introduction 337

5.2 Specification 340

5.3 Implementation 341

5.4 Acknowledgements 343

References 349