
Contents

- 1 Introduction 1**
 - 1.1 Formal Verification 2
 - 1.2 Model Checking and Infinite-State Systems 5
 - 1.3 Contents and Context of the Thesis 7
 - 1.4 Structure of the Thesis 9

- 2 Cut-offs on Parameterised Networks of Processes 11**
 - 2.1 Cut-off Results On Parameterised Process Networks 12
 - 2.1.1 A Single Control Process and Many Identical User Processes 12
 - 2.1.2 Networks of Processes Communicating by Token Passing 13
 - 2.1.3 Process Networks with Disjunctive or Conjunctive Guards 15
 - 2.1.4 Process Networks with Resource Sharing 15
 - 2.1.5 Cache Coherence Protocols 16
 - 2.1.6 Systems with Parameterised-Size Arrays 16
 - 2.2 RTR Families: Parametric Resource Sharing Networks 17
 - 2.2.1 RTR Families 19
 - 2.2.2 The Specification Logic 23
 - 2.2.3 Verification of Finite Behaviour 25
 - 2.2.4 Verification of Fair Behaviour 29
 - 2.2.5 Process Deadlockability 36
 - 2.2.6 RTR Families and Undecidability 37
 - 2.3 A Summary on Cut-offs and RTR Families 39

- 3 Regular Model Checking 41**
 - 3.1 Finite-State Automata and Transducers 42
 - 3.2 Regular Model Checking: The Basic Idea 43
 - 3.3 Verification by Regular Model Checking 46
 - 3.4 Acceleration in Regular Model Checking 48
 - 3.4.1 Acceleration Schemes 48

VIII Contents

3.4.2	Quotienting	49
3.4.3	Extrapolation	52
3.5	Abstract Regular Model Checking	53
3.5.1	A Running Example and Some Basic Assumptions	55
3.5.2	The Method of Abstract Regular Model Checking	56
3.5.3	Automata State Equivalences Based on Predicate Languages	59
3.5.4	Automata State Equivalences Based on Finite-Length Languages	63
3.5.5	Experiments with Abstract Regular Model Checking ...	65
3.6	Inference of Regular Languages	70
3.6.1	Inference of Regular Languages from Complete Training Sets	72
3.6.2	The Model Checking Algorithm	76
3.6.3	Experiments with the Inference-based RMC	79
3.7	Summary and Extensions of RMC	81
4	Regular Model Checking and Programs with Pointers	85
4.1	An Overview of the Existing Approaches	87
4.1.1	PALE	88
4.1.2	TVLA	89
4.1.3	Other Logic-based Approaches	90
4.1.4	Automata-based Approaches	92
4.1.5	Other Approaches	94
4.2	From Programs to Transducers	98
4.2.1	Encoding Stores as Words	99
4.2.2	Lists with Sharing and/or Loops	100
4.2.3	Encoding Program Statements as Transducers	100
4.3	Specialised Abstract Regular Model Checking	103
4.3.1	Piecewise 0- k Counter Abstractions	103
4.3.2	Closure Abstractions	105
4.4	Applications and Experimental Results	107
4.4.1	Checking Consistency of Working with the Dynamic Memory	107
4.4.2	Checking More Complex Properties	108
4.4.3	The Results of the Experiments	109
4.5	Summary and Further Work	110
5	Regular Tree Model Checking	113
5.1	Tree Automata and Transducers	114
5.2	RTMC: The Idea and Approaches	116
5.2.1	Acceleration in Regular Tree Model Checking	117
5.3	Abstract Regular Tree Model Checking	118
5.3.1	The Framework of Abstract Regular Tree Model Checking	119

5.3.2	Abstractions over Tree Automata.....	119
5.3.3	Experiments with Abstract Regular Tree Model Checking	122
5.4	Summary and Further Work on Regular Tree Model Checking.	124
6	Tree Automata with Size Constraints	127
6.1	Works Trying To Go Beyond RMC	128
6.2	Tree Automata with Size Constraints	133
6.2.1	A TASC-based Verification Methodology and a Running Example	136
6.2.2	The Notion of TASC.....	138
6.2.3	Closure and Decidability Properties of TASC	141
6.2.4	Semantics of Tree Updates	147
6.2.5	Representing Sets of Memory Configurations.....	149
6.2.6	A Case Study: The Red-Black Tree Insertion.....	156
6.3	Summary and Further Work	159
7	Conclusion	161
7.1	Summary.....	161
7.2	Future Research Directions	162
	References	165