

## Contents

	<i>Preface</i>	page ix
	<i>Acknowledgements</i>	xi
1	Introduction	1
	1.1 Second Quantum Revolution Requires New Verification Techniques	1
	1.2 Model-Checking Techniques for Classical Systems	2
	1.3 Difficulty in Model Checking Quantum Systems	2
	1.4 Current Research on Model Checking of Quantum Systems	3
	1.5 Structure of the Book	5
2	Basics of Model Checking	6
	2.1 Modelling Systems	6
	2.2 Temporal Logics	8
	2.2.1 Linear Temporal Logic	8
	2.2.2 Computation Tree Logic	11
	2.3 Model-Checking Algorithms	14
	2.3.1 LTL Model Checking	15
	2.3.2 CTL Model Checking	22
	2.4 Model Checking Probabilistic Systems	23
	2.4.1 Markov Chains and Markov Decision Processes	24
	2.4.2 Probabilistic Temporal Logics	25
	2.4.3 Probabilistic Model-Checking Algorithms	26
	2.5 Bibliographic Remarks	30
3	Basics of Quantum Theory	31
	3.1 State Spaces of Quantum Systems	31
	3.1.1 Hilbert Spaces	31
	3.1.2 Subspaces	33

3.1.3	Postulate of Quantum Mechanics I	34
3.2	Dynamics of Quantum Systems	35
3.2.1	Linear Operators	35
3.2.2	Unitary Operators	37
3.2.3	Postulate of Quantum Mechanics II	38
3.3	Quantum Measurements	39
3.3.1	Postulate of Quantum Mechanics III	39
3.3.2	Projective Measurements	40
3.4	Composition of Quantum Systems	42
3.4.1	Tensor Products	42
3.4.2	Postulate of Quantum Mechanics IV	43
3.5	Mixed States	44
3.5.1	Density Operators	44
3.5.2	Evolution of and Measurement on Mixed States	45
3.5.3	Reduced Density Operators	45
3.6	Quantum Operations	46
3.6.1	A Generalisation of Postulate of Quantum Mechanics II	46
3.6.2	Representations of Quantum Operations	48
3.7	Bibliographic Remarks	49
4	Model Checking Quantum Automata	50
4.1	Quantum Automata	50
4.2	Birkhoff-von Neumann Quantum Logic	53
4.3	Linear-Time Properties of Quantum Systems	57
4.3.1	Basic Definitions	58
4.3.2	Safety Properties	59
4.3.3	Invariants	60
4.3.4	Liveness Properties	63
4.3.5	Persistence Properties	64
4.4	Reachability of Quantum Automata	67
4.4.1	A (Meta-)Propositional Logic for Quantum Systems	67
4.4.2	Satisfaction of Reachability by Quantum Automata	68
4.5	Algorithm for Checking Invariants of Quantum Automata	71
4.6	Algorithms for Checking Reachability of Quantum Automata	73
4.6.1	Checking $\mathcal{A} \models \mathbf{I}f$ for the Simplest Case	75
4.6.2	Checking $\mathcal{A} \models \mathbf{I}f$ for the General Case	77
4.6.3	Checking $\mathcal{A} \models \mathbf{G}f$ and $\mathcal{A} \models \mathbf{U}f$	80
4.7	Undecidability of Checking Reachability of Quantum Automata	81
4.7.1	Undecidability of $\mathcal{A} \models \mathbf{G}f$ , $\mathcal{A} \models \mathbf{U}f$ and $\mathcal{A} \models \mathbf{I}f$	82
4.7.2	Undecidability of $\mathcal{A} \models \mathbf{F}f$	83

<i>Contents</i>		vii
4.8	Final Remark	85
4.9	Bibliographic Remarks	85
5	Model Checking Quantum Markov Chains	87
5.1	Quantum Markov Chains	88
5.2	Quantum Graph Theory	91
5.2.1	Adjacency and Reachability	91
5.2.2	Bottom Strongly Connected Components	94
5.3	Decomposition of the State Hilbert Space	101
5.3.1	Transient Subspaces	101
5.3.2	BSCC Decomposition	103
5.3.3	Periodic Decomposition	107
5.4	Reachability Analysis of Quantum Markov Chains	115
5.4.1	Reachability Probability	116
5.4.2	Repeated Reachability Probability	118
5.4.3	Persistence Probability	121
5.5	Checking Quantum Markov Decision Processes	124
5.5.1	Invariant Subspaces and Reachability Probability	126
5.5.2	Comparison of Classical MDPs, POMDPs and qMDPs	128
5.5.3	Reachability in the Finite Horizon	130
5.5.4	Reachability in the Infinite Horizon	132
5.6	Final Remarks	136
5.7	Bibliographic Remarks	136
6	Model Checking Super-Operator-Valued Markov Chains	138
6.1	Super-Operator-Valued Markov Chains	139
6.2	Positive Operator-Valued Measures on SVMCs	143
6.3	Positive Operator-Valued Temporal Logic	152
6.3.1	Quantum Computation Tree Logic	152
6.3.2	Linear Temporal Logic	154
6.4	Algorithms for Checking Super-Operator-Valued Markov Chains	154
6.4.1	Model Checking QCTL Formulas	154
6.4.2	Model Checking LTL Properties	161
6.5	Bibliographic Remarks	173
7	Conclusions and Prospects	175
7.1	State Space Explosion	175
7.2	Applications	176
7.2.1	Verification and Testing of Quantum Circuits	176
7.2.2	Verification and Analysis of Quantum Cryptographic Protocols	177

viii	<i>Contents</i>	
	7.2.3 Verification and Analysis of Quantum Programs	178
7.3	Tools: Model Checkers for Quantum Systems	179
7.4	From Model Checking Quantum Systems to Quantum Model Checking	179
<i>Appendix 1</i>	Proofs of Technical Lemmas in Chapter 4	181
A1.1	Proof of Lemma 4.36	181
A1.2	Proof of Lemma 4.39	182
A1.3	Skolem's Problem for Linear Recurrence Sequences	183
A1.4	Skolem's Problem in Matrix Form	184
A1.5	Constructing Quantum Automata from Minsky Machines	185
	A1.5.1 Encoding Classical States into Quantum States	185
	A1.5.2 Simulating Classical Transitions by Unitary Operators	186
	A1.5.3 Construction of $V$ and $W$	187
<i>Appendix 2</i>	Proofs of Technical Lemmas in Chapter 5	190
A2.1	Proof of Lemma 5.25 (ii)	190
A2.2	Proof of Lemma 5.30	191
A2.3	Proof of Lemma 5.34	191
A2.4	Proof of Lemma 5.58	192
<i>Appendix 3</i>	Proofs of Technical Lemmas in Chapter 6	196
A3.1	Proof of Theorem 6.21 (iii)	196
A3.2	Proof of Lemma 6.31	198
A3.3	Proof of Lemma 6.32	198
A3.4	Proof of Lemma 6.33	199
A3.5	Proof of Lemma 6.34	200
A3.6	Proof of Lemma 6.35	200
	<i>References</i>	201
	<i>Index</i>	208