

## MODEL CHECKING QUANTUM SYSTEMS

Model checking is one of the most successful verification techniques and has been widely adopted in traditional computing and communication hardware and software industries.

This book provides the first systematic introduction to model-checking techniques applicable to quantum systems, with broad potential applications in the emerging industry of quantum computing and quantum communication as well as quantum physics.

Suitable for use as a course textbook and for self-study, graduate and senior undergraduate students will appreciate the step-by-step explanations and the exercises included. Researchers and engineers in the related fields can further develop these techniques in their own work, with the final chapter outlining potential future applications.

MINGSHENG YING is Distinguished Professor in the Centre for Quantum Software and Information, University of Technology Sydney; Deputy Director for Research of the Institute of Software, Chinese Academy of Sciences; and Cheung Kong Chair Professor in the Department of Computer Science and Technology, Tsinghua University. His research interests are quantum computing, programming theory and logics in artificial intelligence. He is the author of the books *Foundations of Quantum Programming* (2016) and *Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrent Programs* (2001). Currently, he serves as (Co-)Editor-in-Chief of *ACM Transactions on Quantum Computing*.

YUAN FENG is Professor in the Centre for Quantum Software and Information, University of Technology Sydney. His research interests include formal verification of quantum systems, the theory of quantum programming, quantum information and computation and probabilistic systems. He has published more than 70 research papers in international leading journals and mainstream conferences. He was awarded an ARC (Australian Research Council) Future Fellowship in 2010.

Cambridge University Press  
978-1-108-48430-5 — Model Checking Quantum Systems  
Mingsheng Ying , Yuan Feng  
Frontmatter  
[More Information](#)

---

# MODEL CHECKING QUANTUM SYSTEMS

Principles and Algorithms

MINGSHENG YING

*University of Technology Sydney*

YUAN FENG

*University of Technology Sydney*



CAMBRIDGE  
UNIVERSITY PRESS

Cambridge University Press  
978-1-108-48430-5 — Model Checking Quantum Systems  
Mingsheng Ying, Yuan Feng  
Frontmatter  
[More Information](#)

## CAMBRIDGE UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom  
One Liberty Plaza, 20th Floor, New York, NY 10006, USA  
477 Williamstown Road, Port Melbourne, VIC 3207, Australia  
314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India  
79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

[www.cambridge.org](http://www.cambridge.org)

Information on this title: [www.cambridge.org/9781108484305](http://www.cambridge.org/9781108484305)

DOI: 10.1017/9781108613323

© Mingsheng Ying and Yuan Feng 2021

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2021

Printed in the United Kingdom by TJ Books Limited, Padstow Cornwall

*A catalogue record for this publication is available from the British Library.*

*Library of Congress Cataloging-in-Publication Data*

Names: Ying, Mingsheng, author. | Feng, Yuan, 1977– author.

Title: Model checking quantum systems : principles and algorithms / Mingsheng Ying,

University of Technology, Sydney, Yuan Feng, University of Technology, Sydney.

Description: Cambridge, UK ; New York, NY : Cambridge University Press, 2020. | Includes bibliographical references and index.

Identifiers: LCCN 2020041998 (print) | LCCN 2020041999 (ebook) | ISBN 9781108484305 (hardback) | ISBN 9781108613323 (epub)

Subjects: LCSH: Quantum computing. | Computer systems—Verification.

Classification: LCC QA76.889 .Y564 2020 (print) | LCC QA76.889 (ebook) | DDC 006.3/843—dc23

LC record available at <https://lcn.loc.gov/2020041998>

LC ebook record available at <https://lcn.loc.gov/2020041999>

ISBN 978-1-108-48430-5 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

## 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

*Contents*

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



## Preface

Model checking is an algorithmic technique for verification of dynamic properties of (mainly) finite state systems. After the development of more than 35 years, it has become a prominent verification technique for both hardware and software systems and has found numerous successful applications in the information and communications technology industries. The special attractiveness of model checking is due mainly to the following two features:

- It is completely automatic.
- It provides counterexamples whenever the properties are not satisfied and thus is very useful in debugging.

Since various stochastic phenomena occur in computing and communication systems, model checking has been systematically extended for verifying probabilistic systems, such as Markov chains and Markov decision processes.

With the emergence of quantum computing and quantum communication and, in particular, their rapid progress in the past few years, one may naturally expect to further extend the model-checking technique for verification of quantum systems. Indeed, research on model checking quantum systems has already been conducted for more than 10 years, starting from directly applying probabilistic model checking to quantum systems, in particular, quantum communication protocols. In dealing with more and more general quantum systems, it has been gradually realised that model checking quantum systems requires certain principles fundamentally different from those for classical systems (including probabilistic systems). Some basic principles for model checking quantum systems have been developed in recent research, but they are scattered in various conference and journal papers.

This book attempts to provide a systematic exposition of the principles for model checking quantum systems and the algorithms based on them, which have been proposed up to the writing of this book. Some potential applications and topics for

future research are briefly discussed at the end of the book. We hope that the book can serve as an introduction to this new area for researchers and provide a basis for further development of the area.

The book is also intended to serve as a textbook for graduate students. It is therefore organised with a careful pedagogical consideration. Since the students in quantum computing and information may come from either a computer science or physics background, two preliminary chapters are given at the beginning of the book: the first briefly introduces model checking for those from physics, and the second briefly introduces quantum theory for those from computer science. After that, model-checking technique for quantum systems is presented step by step, from simpler models and checked properties to more sophisticated ones.

## Acknowledgements

The materials of this book mainly come from a series of articles by the authors and their collaborators. The authors would like to thank Drs Nengkun Yu, Yangjia Li, Shenggang Ying and Ji Guan for pleasant and fruitful collaborations. Without their contributions, this book would not have been possible.

The work presented in this book has been partially supported by the National Key R&D Program of China (Grant No. 2018YFA0306701), the Australian Research Council (Grant Nos. DP160101652 and DP180100691), the National Natural Science Foundation of China (Grant No. 61832015) and the Key Research Program of Frontier Sciences, Chinese Academy of Sciences. All of them are gratefully acknowledged.

Cambridge University Press  
978-1-108-48430-5 — Model Checking Quantum Systems  
Mingsheng Ying , Yuan Feng  
Frontmatter  
[More Information](#)

---