Semantic Techniques in Quantum Computation

The study of computational processes based on the laws of quantum mechanics has led to the discovery of new algorithms, cryptographic techniques, and communication primitives. This book explores quantum computation from the perspective of the branch of theoretical computer science known as semantics, as an alternative to the more well-known studies of algorithmics, complexity theory, and information theory. It collects chapters from leading researchers in the field, discussing the theory of quantum programming languages, logics and tools for reasoning about quantum systems, and novel approaches to the foundations of quantum mechanics.

This book is suitable for graduate students and researchers in quantum information and computation, as well as those in semantics, who want to learn about a new field arising from the application of semantic techniques to quantum information and computation.

Simon Gay is a Senior Lecturer in the Department of Computing Science at the University of Glasgow. Prior to taking his current position, he worked as a research associate at Imperial College London, where he also earned his Ph.D. in computer science, and as a lecturer at Royal Holloway, University of London.

Ian Mackie earned his M.Sc. and Ph.D. degrees in computer science at Imperial College London. He is editor-in-chief of an undergraduate textbook series and coauthor of an advanced textbook on proof theory and automated deduction.

Cambridge University Press
978-0-521-51374-6 - Semantic Techniques in Quantum Computation
Edited by Simon Gay and Ian Mackie
Frontmatter
More information

Semantic Techniques in Quantum Computation

Edited by

SIMON GAY

IAN MACKIE

CAMBRIDGE
UNIVERSITY PRESS

© in this web service Cambridge University Press

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521513746

© Cambridge University Press 2010

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 2010

Printed in the United States of America

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

Library of Congress Cataloging in Publication data

Semantic techniques in quantum computation / edited by Simon Gay, Ian Mackie.
p. cm.
Includes index.
ISBN 978-0-521-51374-6 (hardback)
1. Quantum computers. 2. Programming languages (Electronic computers) – Semantics.
3. Quantum theory. I. Gay, Simon, 1969– II. Mackie, I. (Ian)
QA76.889.S36 2009
004.1–dc22 2009032804

ISBN 978-0-521-51374-6 Hardback

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

Cambridge University Press
978-0-521-51374-6 - Semantic Techniques in Quantum Computation
Edited by Simon Gay and Ian Mackie
Frontmatter
More information

Contents

© in this web service Cambridge University Press www.cambridge.org

Contributors

Samson Abramsky
Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Thorsten Altenkirch
School of Computer Science, University of Nottingham, Jubilee Campus, Wollaton Road, Nottingham NG8 1BB, UK

Samuel L. Braunstein
Department of Computer Science, University of York, Heslington, York YO10 5DD, UK

Bob Coecke
Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Vincent Danos
School of Informatics, University of Edinburgh, Informatics Forum, 10 Crichton Street, Edinburgh EH8 9AB, UK

Runyao Duan
Centre for Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, City Campus, 15 Broadway, Ultimo, NSW 2007, Australia; and State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Ross Duncan
Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

© in this web service Cambridge University Press

Yuan Feng
Centre for Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, City Campus, 15 Broadway, Ultimo, NSW 2007, Australia; and State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Simon J. Gay
Department of Computing Science, University of Glasgow, Sir Alwyn Williams Building, Lilybank Gardens, Glasgow G12 8QQ, UK

Alexander S. Green
School of Computer Science, University of Nottingham, Jubilee Campus, Wollaton Road, Nottingham NG8 1BB, UK

Peter Hines
Department of Computer Science, University of York, Heslington, York YO10 5DD, UK

Zhengfeng Ji
Perinmeter Institute for Theoretical Physics, 31 Caroline Street N., Waterloo, Ontario, Canada

Philippe Jorrand
Laboratoire d'Informatique de Grenoble, 220 me de la Chimie, 38400 Saint Martin d'Hères, France

Elham Kashefi
School of Informatics, University of Edinburgh, Informatics Forum, 10 Crichton Street, Edinburgh EH8 9AB, UK

Paulo Mateus
Security and Quantum Information Group, Instituto de Telecomunicações and Departmento de Matemática, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Rajagopal Nagarajan
Department of Computer Science, University of Warwick, Coventry CV4 7AL, UK

Prakash Panangaden
School of Computer Science, McGill University, 3480 University Street, Montréal, Québec H3A 2A7, Canada

Nikolaos Papanikolaou
International Digital Laboratory, WMG, University of Warwick, Coventry CV4 7AL, UK

Cambridge University Press
978-0-521-51374-6 - Semantic Techniques in Quantum Computation
Edited by Simon Gay and Ian Mackie
Frontmatter
More information

Éric Oliver Paquette
Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Dusko Pavlovic
Kestrel Institute, 3260 Hillview Avenue, Palo Alto, California 94304, USA; and Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Simon Perdrix
School of Informatics, University of Edinburgh, Informatics Forum, 10 Crichton Street, Edinburgh EH8 9AB, UK; and Laboratoire PPS, Université Paris Diderot-Paris 7, Case 7014, 75205 Paris Cedex 13, France

Jaime Ramos
Security and Quantum Information Group, Instituto de Telecomunicações and Departmento de Matemática, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Peter Selinger
Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia B3H 3J5, Canada

Amílcar Sernadas
Security and Quantum Information Group, Instituto de Telecomunicações and Departmento de Matemática, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Cristina Sernadas
Security and Quantum Information Group, Instituto de Telecomunicações and Departmento de Matemática, Instituto Superior Técnico, Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Benoît Valiron
INRIA and Laboratoire d'Informatique, Ecole Polytechnique, 91128 Palaiseau Cedex, France

Mingsheng Ying
Centre for Quantum Computation and Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, City Campus, 15 Broadway, Ultimo, NSW 2007, Australia; and State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

© in this web service Cambridge University Press

Cambridge University Press
978-0-521-51374-6 - Semantic Techniques in Quantum Computation
Edited by Simon Gay and Ian Mackie
Frontmatter
More information

Preface

The idea of quantum computation, in the algorithmic sense, originated from the suggestion by Feynman (1982) that a computer based on the principles of quantum mechanics might be capable of efficiently simulating quantum systems of interest to physicists; such simulation seems to be very difficult with classical computers. Feynman's suggestion was followed up by Deutsch (1985), who introduced the notion of the quantum Turing machine and investigated the possible computational power of physically realizable computers. He showed that a specific problem, now known as Deutsch's problem, can be solved more efficiently by a quantum algorithm than by a classical algorithm. Several years later, Shor (1994) discovered efficient quantum algorithms for two important practical problems – integer factorization and the "discrete logarithm" problem – and shortly afterwards, Grover (1996) discovered an efficient quantum algorithm for unstructured searching. Since then, quantum algorithmics and quantum complexity theory have developed into substantial and active research fields.

Meanwhile, the principles of quantum mechanics were being used as the foundation for a new approach to cryptography. Bennett and Brassard (1984) defined a protocol for key distribution whose security is guaranteed by the laws of quantum theory. Their system built on earlier work by Wiesner (1983), which remained unpublished until several years after its conception. We regard quantum cryptography as an aspect of quantum computation, in particular *distributed* quantum computation; alternatively, both quantum algorithmics and quantum cryptography can be viewed as branches of quantum information processing.

Although Deutsch had observed in 1985 that "quantum computers raise interesting questions for the design of programming languages" (Deutsch 1985), it took some time for computing scientists to begin to rise to the challenge. Knill (1996) introduced a structured pseudocode for quantum algorithms, as an alternative to circuit diagrams; later, Ömer (1998) began the systematic design of an imperative quantum programming language. Similar ideas, although not as extensively developed, had also been investigated by Baker (1996). An alternative approach, based

© in this web service Cambridge University Press

on λ-calculus, was introduced by Maymin (1996); the λ-calculus approach was also followed by Van Tonder (2004). Another early influential project was that of Sanders and Zuliani (2000).

During the next few years there was a rapid increase in interest in quantum computation from the research community in the theory of programming languages. Broadly speaking we refer to this community as the *semantic* side of theoretical computing science, in distinction to the *algorithmic* and *complexity-theoretic* side. Its interests encompass programming language semantics, type theory, semantics-based program analysis, and formal specification and verification of computational systems. There is a particular emphasis on compositional reasoning and connections with formal (and often nonclassical) logics. In relation to quantum computation, the logical and type-theoretic dimension of this community's activity had been foreshadowed by Pratt (1992) and Wehr (1996) but was given prominence by Abramsky and Coecke (2003, 2004).

A more comprehensive overview and a complete bibliography can be found in the survey by Gay (2006). By 2003 there was enough activity for Peter Selinger to organize a workshop on Quantum Programming Languages as part of the Fields Institute Summer School in Logic and Computation at the University of Ottawa. This meeting, as well as Selinger's own research (Selinger 2004), was influential in drawing more semanticists into quantum computation. Several of the speakers have written or coauthored chapters for the present volume. The QPL workshops have flourished as an annual series of meetings; more recently the scope has broadened and the title has changed to "Quantum Physics and Logic."

With this background, and noting that a substantial part of the activity in the area was taking place in the UK, in 2006 we obtained funding from the UK Engineering and Physical Sciences Research Council (EPSRC) for a research network on Semantics of Quantum Computation (Gay and Mackie 2006–2009), known informally as QNET. Through grants EP/E00623X/1 and EP/E006833/1, the network provided funding for travel within the UK and for international research visits and conference attendance, in order to build a research community. Membership of the network has grown significantly, and three successful workshops have been held, in Glasgow (2006), London (2007), and Edinburgh (2008). A final workshop will take place in Oxford at the end of 2009. Many members of QNET are also involved in the European Union FP6 STREP project "QICS: Foundational Structures in Quantum Information and Computation" (Coecke 2007–2009), which has broadly similar themes.

This volume provides a snapshot of research on the topics covered by QNET. We selected the authors in order to give complete coverage of the field; many, although by no means all, are members of QNET. Some of the chapters describe novel research, not published elsewhere, while others draw on several of their authors' publications to provide a coherent picture of recent research on a particular topic. We followed a process whereby authors submitted draft versions of their chapters,

© in this web service Cambridge University Press www.cambridge.org

Cambridge University Press
978-0-521-51374-6 - Semantic Techniques in Quantum Computation
Edited by Simon Gay and Ian Mackie
Frontmatter
More information

which were reviewed in order to provide feedback before preparation of the final version. In general, each chapter was reviewed by an author of another chapter and by an independent reviewer.

The first three chapters are set within the category-theoretic framework for quantum mechanics introduced by Abramsky and Coecke (2004). In Chapter 1, Samson Abramsky gives a category-theoretic analysis of the "no-cloning" property of quantum mechanics, which prevents arbitrary quantum information from being copied. The topic of Chapter 2, by Bob Coecke, Éric Paquette, and Dusko Pavlovic, is the representation and structure of classical data, which *can* be freely copied, within categorical quantum mechanics. Ross Duncan, in Chapter 3, further develops the graphical calculus that has been a feature of categorical quantum mechanics from the beginning, showing how it can include reasoning about measurement.

The next five chapters apply semantic techniques in several ways. Peter Selinger and Benoît Valiron, in Chapter 4, present a quantum λ-calculus. They describe an operational semantics, a category-theoretic semantics (which has much structure in common with Chapters 1–3) and a type system. Chapter 5, by Thorsten Altenkirch and Alexander Green, moves from λ-calculus to the functional programming language Haskell and shows how quantum operations can be structured as a monad. In Chapter 6, Philippe Jorrand and Simon Perdrix use the formal semantics of an imperative quantum programming language as the basis for an abstraction interpretation which enables static analysis of entanglement. Chapter 7 is by Vincent Danos, Elham Kashefi, Prakash Panangaden, and Simon Perdrix. It gathers together the results of their research programme on the measurement calculus, a formally defined language for measurement-based quantum computation. In Chapter 8, Mingsheng Ying, Runyao Duan, Yuan Feng, and Zhengfeng Ji study a different style of semantics – predicate transformers – that refers back to some of the first work on formal semantics of quantum programs (Sanders and Zuliani 2000).

The final three chapters return to the theme of quantum logic, introduced in categorical form in the first three chapters. Peter Hines and Samuel Braunstein, in Chapter 9, extend the Birkhoff–von Neumann approach to quantum logic by generalizing from projectors to partial isometries, and study the resulting categorical structures. In Chapter 10, Paulo Mateus, Jaime Ramos, Amílcar Sernadas, and Cristina Sernadas discuss a temporal extension of exogenous quantum propositional logic (EQPL) which is designed to support reasoning about the dynamic behaviour of quantum systems such as algorithms and protocols. Finally, in Chapter 11, Simon Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou describe a model-checking tool that, given a formal model of a quantum system, can automatically verify specifications expressed in terms of EQPL and its temporal extensions.

Simon Gay and Ian Mackie
May 2009

Bibliography

Abramsky, S., and Coecke, B. (2003) Physical traces: Quantum vs. classical information processing. In *Proceedings of the 9th Conference on Category Theory and Computer Science (CTCS 2002)*, volume 69 of *Electronic Notes in Theoretical Computer Science*. Elsevier Science. Also arXiv:cs.CG/0207057.

Abramsky, S., and Coecke, B. (2004) A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society. Also arXiv:quant-ph/0402130.

Baker, G. (1996) Qgol: A system for simulating quantum computations: Theory, implementation and insight. Honours thesis, Macquarie University; available as `www.ifost.org.au/∼gregb/q-gol/QgolThesis.pdf`.

Bennett, C. H., and Brassard, G. (1984) Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computer Systems and Signal Processing*, pages 175–179.

Coecke, B. (2007–2009) EU FP6 STREP QICS: Foundational Structures in Quantum Information and Computation. `se10.comlab.ox.ac.uk:8080/FOCS/FP6STREPQICS_en.html`.

Deutsch, D. (1985) Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A* **400**:97–117.

Feynman, R. P. (1982) Simulating physics with computers. *International Journal of Theoretical Physics* **21**(6–7):467–488.

Gay, S. J. (2006) Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science* **16**(4):581–600.

Gay, S. J., and Mackie, I. C. (2006–2009) EPSRC Network on Semantics of Quantum Computation. `www.qnet.org.uk`.

Grover, L. (1996) A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219. ACM Press. Also arXiv:quant-ph/9605043.

Knill, E. (1996) Conventions for quantum pseudocode. Technical Report LAUR-96-2724, Los Alamos National Laboratory.

Maymin, P. (1996) Extending the lambda calculus to express randomized and quantumized algorithms. arXiv:quant-ph/9612052.

Ömer, B. (1998) *A Procedural Formalism for Quantum Computing*. Master's thesis, Department of Theoretical Physics, Technical University of Vienna.

Pratt, V. (1992) Linear logic for generalized quantum mechanics. In *Proceedings of the IEEE Workshop on Physics and Computation*.

Sanders, J. W., and Zuliani, P. (2000) Quantum programming. In *Mathematics of Program Construction*, volume 1837 of *Lecture Notes in Computer Science*. Springer.

Selinger, P. (2004) Towards a quantum programming language. *Mathematical Structures in Computer Science* **14**(4):527–586.

Shor, P. W. (1994) Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 124–134. IEEE Press.

Van Tonder, A. (2004) A lambda calculus for quantum computation. *SIAM Journal on Computing* **33**(5):1109–1135. Also arXiv:quant-ph/0307150.

Wehr, M. (1996) Quantum computing: A new paradigm and its type theory. Lecture given at the Quantum Computing Seminar, Lehrstuhl Prof. Beth, Universität Karlsruhe.

Wiesner, S. (1983) Conjugate coding. *SIGACT News* **15**(1):78–88. Original manuscript written circa 1970.

© in this web service Cambridge University Press www.cambridge.org