Proceedings of Symposia in
APPLIED MATHEMATICS

Volume 58

Quantum Computation:
A Grand Mathematical Challenge for the Twenty-First Century and the Millennium

American Mathematical Society
Short Course
January 17–18, 2000
Washington, DC

Samuel J. Lomonaco, Jr.
Editor

American Mathematical Society

http://dx.doi.org/10.1090/psapm/058

Selected Titles in This Series

58 **Samuel J. Lomonaco, Jr., Editor,** Quantum computation: A grand mathematical challenge for the twenty-first century and the millennium (Washington, DC, January 2000)

57 **David C. Heath and Glen Swindle, Editors,** Introduction to mathematical finance (San Diego, California, January 1997)

56 **Jane Cronin and Robert E. O'Malley, Jr., Editors,** Analyzing multiscale phenomena using singular perturbation methods (Baltimore, Maryland, January 1998)

55 **Frederick Hoffman, Editor,** Mathematical aspects of artificial intelligence (Orlando, Florida, January 1996)

54 **Renato Spigler and Stephanos Venakides, Editors,** Recent advances in partial differential equations (Venice, Italy, June 1996)

53 **David A. Cox and Bernd Sturmfels, Editors,** Applications of computational algebraic geometry (San Diego, California, January 1997)

52 **V. Mandrekar and P. R. Masani, Editors,** Proceedings of the Norbert Wiener Centenary Congress, 1994 (East Lansing, Michigan, 1994)

51 **Louis H. Kauffman, Editor,** The interface of knots and physics (San Francisco, California, January 1995)

50 **Robert Calderbank, Editor,** Different aspects of coding theory (San Francisco, California, January 1995)

49 **Robert L. Devaney, Editor,** Complex dynamical systems: The mathematics behind the Mandlebrot and Julia sets (Cincinnati, Ohio, January 1994)

48 **Walter Gautschi, Editor,** Mathematics of Computation 1943–1993: A half century of computational mathematics (Vancouver, British Columbia, August 1993)

47 **Ingrid Daubechies, Editor,** Different perspectives on wavelets (San Antonio, Texas, January 1993)

46 **Stefan A. Burr, Editor,** The unreasonable effectiveness of number theory (Orono, Maine, August 1991)

45 **De Witt L. Sumners, Editor,** New scientific applications of geometry and topology (Baltimore, Maryland, January 1992)

44 **Béla Bollobás, Editor,** Probabilistic combinatorics and its applications (San Francisco, California, January 1991)

43 **Richard K. Guy, Editor,** Combinatorial games (Columbus, Ohio, August 1990)

42 **C. Pomerance, Editor,** Cryptology and computational number theory (Boulder, Colorado, August 1989)

41 **R. W. Brockett, Editor,** Robotics (Louisville, Kentucky, January 1990)

40 **Charles R. Johnson, Editor,** Matrix theory and applications (Phoenix, Arizona, January 1989)

39 **Robert L. Devaney and Linda Keen, Editors,** Chaos and fractals: The mathematics behind the computer graphics (Providence, Rhode Island, August 1988)

38 **Juris Hartmanis, Editor,** Computational complexity theory (Atlanta, Georgia, January 1988)

37 **Henry J. Landau, Editor,** Moments in mathematics (San Antonio, Texas, January 1987)

36 **Carl de Boor, Editor,** Approximation theory (New Orleans, Louisiana, January 1986)

35 **Harry H. Panjer, Editor,** Actuarial mathematics (Laramie, Wyoming, August 1985)

34 **Michael Anshel and William Gewirtz, Editors,** Mathematics of information processing (Louisville, Kentucky, January 1984)

33 **H. Peyton Young, Editor,** Fair allocation (Anaheim, California, January 1985)

32 **R. W. McKelvey, Editor,** Environmental and natural resource mathematics (Eugene, Oregon, August 1984)

31 **B. Gopinath, Editor,** Computer communications (Denver, Colorado, January 1983)

30 **Simon A. Levin, Editor,** Population biology (Albany, New York, August 1983)

(*Continued in the back of this publication*)

AMS SHORT COURSE LECTURE NOTES

Introductory Survey Lectures

published as a subseries of

Proceedings of Symposia in Applied Mathematics

Proceedings of Symposia in
APPLIED MATHEMATICS

Volume 58

Quantum Computation:
A Grand Mathematical Challenge for the Twenty-First Century and the Millennium

American Mathematical Society
Short Course
January 17–18, 2000
Washington, DC

Samuel J. Lomonaco, Jr.
Editor

American Mathematical Society
Providence, Rhode Island

LECTURE NOTES PREPARED FOR THE
AMERICAN MATHEMATICAL SOCIETY SHORT COURSE
QUANTUM COMPUTATION
HELD IN WASHINGTON, DC
JANUARY 17–18, 2000

The AMS Short Course Series is sponsored by the Society's Program Committee for National Meetings. The series is under the direction of the Short Course Subcommittee of the Program Committee for National Meetings.

2000 *Mathematics Subject Classification.* Primary 81–01, 81–02, 81P68, 68Q05, 94A60; Secondary 22E70, 57M99, 81V80, 94A15.

Library of Congress Cataloging-in-Publication Data

American Mathematical Society. Short course (2000 : Washington, DC)

Quantum computation : a grand mathematical challenge for the twenty-first century and the millennium : American Mathematical Society, Short Course, January 17–18, 2000, Washington, DC / Samuel J. Lomonaco, editor.

p. cm. – (Proceedings of symposia in applied mathematics, ISSN 0160-7634; v. 58 AMS short course lecture notes)

Includes bibliographical references and index.

ISBN 0-8218-2084-2 (alk. paper)

1. Quantum computers–Congresses. I. Lomonaco, Samuel J. II. American Mathematical Society. III. Title. IV. Proceedings of symposia in applied mathematics; v. 58. V. Proceedings of symposia in applied mathematics. AMS short course lecture notes.

QA76.889.A44 2000

004.1–dc21 2001055366

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at URL: `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 07 06 05 04 03 02

Contents

Preface

This book arose from an American Mathematical Society Short Course entitled:

Quantum Computation
A Grand Mathematical Challenge
for the
Twenty-First Century and the Millennium

held in Washington, DC, January 17–18, 2000 in conjunction with the Annual Meeting of the American Mathematical Society in Washington, DC, January 19–22, 2000.

This AMS Short Course was created with the objective of sharing with the scientific community the many exciting mathematical challenges arising from the new and emerging field of quantum computation and quantum information science. In so doing, it was hoped that this AMS Short Course would act as a catalyst to encourage, to entice, and, yes, ... to challenge and ultimately to dare mathematicians into working on the many diverse grand mathematical challenges arising in this field.

To meet this objective, the AMS Short Course was designed to demonstrate the great breadth and depth of this mathematically rich research field. Interrelationships with existing mathematical research areas were emphasized as much as possible. Moreover, the entire AMS Short Course was designed in such a way that course participants with little, if any, background in quantum mechanics would, on completion of the course, be prepared to begin reading the research literature on quantum computation and quantum information science.

Much to my surprise, the response to this AMS Short Course exceeded my most ambitious expectations. I thank the audience for their encouragement and enthusiastic response, and for their many helpful questions and suggestions in regard to the material presented.

This book is a written version of the eight lectures given in this AMS Short Course. Based on audience feedback and questions, the written versions of these lectures have been greatly expanded, and supplementary material has been added.

Chapter I of this book begins with two papers extending an invitation to this research field. The first by Samuel J. Lomonaco, Jr., entitled "A Rosetta Stone to Quantum Mechanics with an Introduction to Quantum Computation," provides the reader with an overview of the relevant parts of quantum mechanics, and with an entrée into the world of quantum computation. The second by Howard E. Brandt, entitled, "Qubit Devices," provides an overview of many potential quantum mechanical computing devices.

Chapter II consists of four papers devoted to quantum algorithms and quantum complexity theory. The first paper by Peter W. Shor, entitled "Introduction to Quantum Algorithms," gives an in-depth overview of quantum algorithms, explaining why recent results in this area are so surprising. It also illustrates the general technique of using the Fourier transform to find periodicity and discusses the quantum algorithms of Simon, Shor, and Grover. The second and third papers by Samuel J. Lomonaco, Jr., entitled respectively "Shor's Quantum Factoring Algorithm" and "Grover's Quantum Search Algorithm," were created in response to audience feedback, and focus more closely on the mathematical inner workings and underpinnings of Shor's and Grover's algorithms. The chapter closes with a fourth paper by Umesh Vazirani, entitled "Quantum Complexity Theory," devoted to the many intriguing and challenging issues of quantum complexity theory. The paper begins with a discussion of the current-day challenge to the Church-Turing thesis and then proceeds into a discussion of quantum complexity classes.

Chapter III is comprised of two papers focusing on quantum error correcting codes and quantum cryptography. The first paper by Daniel Gottesman, entitled "An Introduction to Quantum Error Correction," gives an introduction to quantum information science's first line of defense against the ravages of quantum decoherence, i.e., quantum error correcting codes. The paper begins with a discussion of error models, moves on to quantum error correction and the stabilizer formalism, ending with a quantum error correction sonnet. The second paper by Samuel J. Lomonaco, Jr., entitled "A Talk on Quantum Cryptography, or How Alice Outwits Eve," gives an in-depth analysis of quantum cryptographic protocols, including the BB84, B92, and possible eavesdropping countermeasures. All of this is interwoven into the context of a fictional story about how Alice invents quantum cryptographic protocols to outwit the archvillainess Eve, ... or does she?

The final Chapter IV consists of three papers discussing many more diverse connections between quantum computation and mathematics and physics. The first paper by Alexei Kitaev, entitled "Topological Quantum Codes and Anyons," discusses how anyons can be applied to quantum computation. Anyons are two-dimensional particles that have been found in two-dimensional electronic liquids exhibiting the fractional quantum Hall effect. This paper discusses how Aharonov-Bohm-like interactions of anyons can be used to create topological obstructions to quantum decoherence. Such topological obstructions can be used to construct quantum error correcting codes. Both abelian and nonabelian anyons are discussed. The second paper by Louis H. Kauffman, entitled "Quantum Topology and Quantum Computing," explores some of the tantalizing relationships among knots, links, three manifold invariants, and quantum information science. Many possible applications of quantum topology to quantum computing and vice versa are discussed. The third and final paper by Samuel J. Lomonaco, Jr., entitled "An Entangled Tale of Quantum Entanglement," discusses how Lie group invariant theory can be used to quantify a physical phenomenon that many believe to be at the very core of quantum computation, namely, quantum entanglement. The paper shows how to lift the big adjoint action of the group of local unitary transformations to the corresponding infinitesimal action to produce a system of partial differential equations whose solution is a complete set of entanglement invariants. Examples are given.

It is hoped that this book will encourage its readers to embrace and pursue the grand challenge of quantum computation.

Samuel J. Lomonaco, Jr.
Lomonaco@umbc.edu
http://www.csee.umbc.edu/~lomonaco

August 15, 2001

Acknowledgements

This work was partially supported by Army Research Office (ARO) Grant #P-38804-PH-QC, by the National Institute of Standards and Technology (NIST), by the Defense Advanced Research Projects Agency (DARPA) and Air Force Materiel Command USAF under agreement number F30602-01-0522, and by L-O-O-P Fund No. 2000WADC. The author gratefully acknowledges the hospitality of the University of Cambridge Isaac Newton Institute for Mathematical Sciences, Cambridge, England, where some of this work was completed.

Thanks are due to the other AMS Short Course lecturers, Howard Brandt, Dan Gottesman, Lou Kauffman, Alexei Kitaev, Peter Shor, Umesh Vazirani, and the many Short Course participants for their support and helpful discussions and insights. I would also like to thank Jeffrey Bub, Gilles Brassard, Lov Grover, Lucien Hardy, Tim Havel, Richard Jozsa, David Meyer, John Myers, and Nolan Wallach for their helpful suggestions and discussions. Thanks should also be given to Paul Black, Ron Boisvert, and Carl Williams of NIST for their encouragement and support.

At UMBC, I would like to thank the UMBC CSEE Quantum Computation Faculty Seminar participants Richard Chang, Dhananjay Phatak, John Pinkston, Alan Sherman, Jon Squire, Brooke Stephens, Yaacov Yesha, and my UMBC graduate course students Bianca Benincasa, Ali Bicak, Justin Brody, Mark Colangelo, Koustuv Dasgupta, Stan Finkler, Joan Grindell, Bryan Jacobs, Lalana Kagal, Yoon-Ho Kim, Brett Kurtin, Kimball Martin, Chris McCubbin, Jim Parker, Ravindra Peravali, Scott Rose, Andrew Skinner, and Anocha Yimsiriwattana for their many helpful questions, suggestions and insights.

Many thanks to Sergei Gelfand, Wayne Drady, Gil Poulin, Shirley Hill, and Christine Thivierge of the American Mathematical Society for their editorial support in this endeavor. I am also indebted to Christopher Martin whose computer support made this paper possible.

Finally, I would like to thank my wife Bonnie for her support during this endeavor.

Original AMS Short Course Announcement

Quantum Computation
A Grand Mathematical Challenge
for the
Twenty-First Century and the Millennium

AMS Short Course Overview

The Nobel Laureate Richard Feynman was one of the first individuals to observe that there is an exponential slowdown when computers based on classical physics, i.e., classical computers, are used to simulate quantum systems. Richard Feynman then went on to suggest that it would be far better to use computers based on quantum mechanical principles, i.e., quantum computers, to simulate quantum systems. Such quantum computers should be exponentially faster than their classical counterparts.

Interest in quantum computation suddenly exploded when Peter Shor devised an algorithm for quantum computers that could factor integers in polynomial time. The fastest known algorithm for classical computers factors much more slowly, i.e., in superpolynomial time. Shor's algorithm meant that, if quantum computers could be built, then cryptographic systems based on integer factorization, e.g., RSA, could easily be broken. These cryptographic systems are currently extensively used in banking and in many other areas. Lov Grover then went on to create a quantum algorithm that could search databases faster than anything possible on a classical computer. These algorithms are based on physical principles not implementable on classical computers, quantum superposition and quantum entanglement.

As a result, the race to build a quantum computer is on. But the mathematical, physical, and engineering challenges to do so are formidable, and are a worthy challenge for the best scientific minds. One of the chief obstacles to creating a quantum computer is quantum decoherence. By this we mean that quantum systems want to wander from their computational paths and quantum entangle with the rest of the environment.

This short course focuses on the mathematical challenges involved in the development of quantum computers and quantum algorithms, challenges worthy of the best mathematical minds. It is hoped that, as a result of this course, many mathematicians will be enticed into working on the grand challenge of quantum computation.

The Short Course will begin with an overview of quantum computation, given in an intuitive and conceptual style. No prior knowledge of quantum mechanics will be assumed.

In particular, the Short Course will begin with an introduction to the strange world of the quantum. Such concepts as quantum superposition, Heisenberg's uncertainty principle, the "collapse" of the wave function, and quantum entanglement (i.e., EPR pairs) will be introduced. This will also be interlaced with an introduction to Dirac notation, Hilbert spaces, unitary transformations, and quantum measurement.

Some of the topics covered in the course will be:

- Quantum teleportation
- Shor's quantum factoring algorithm
- Grover's algorithm for searching a database
- Quantum error-correcting codes
- Quantum cryptography
- Quantum information theory
- Quantum complexity theory, including the quantum Turing machine
- The problems of quantum entanglement and locality
- Implementation issues from a mathematical perspective

Each topic will be explained and illustrated with simple examples.

Index

Selected Titles in This Series

(*Continued from the front of this publication*)

29 **R. A. DeMillo, G. I. Davida, D. P. Dobkin, M. A. Harrison, and R. J. Lipton,** Applied cryptology, cryptographic protocols, and computer security models (San Francisco, California, January 1981)

28 **R. Gnanadesikan, Editor,** Statistical data analysis (Toronto, Ontario, August 1982)

27 **L. A. Shepp, Editor,** Computed tomography (Cincinnati, Ohio, January 1982)

26 **S. A. Burr, Editor,** The mathematics of networks (Pittsburgh, Pennsylvania, August 1981)

25 **S. I. Gass, Editor,** Operations research: mathematics and models (Duluth, Minnesota, August 1979)

24 **W. F. Lucas, Editor,** Game theory and its applications (Biloxi, Mississippi, January 1979)

23 **R. V. Hogg, Editor,** Modern statistics: Methods and applications (San Antonio, Texas, January 1980)

22 **G. H. Golub and J. Oliger, Editors,** Numerical analysis (Atlanta, Georgia, January 1978)

21 **P. D. Lax, Editor,** Mathematical aspects of production and distribution of energy (San Antonio, Texas, January 1976)

20 **J. P. LaSalle, Editor,** The influence of computing on mathematical research and education (University of Montana, August 1973)

19 **J. T. Schwartz, Editor,** Mathematical aspects of computer science (New York City, April 1966)

18 **H. Grad, Editor,** Magneto-fluid and plasma dynamics (New York City, April 1965)

17 **R. Finn, Editor,** Applications of nonlinear partial differential equations in mathematical physics (New York City, April 1964)

16 **R. Bellman, Editor,** Stochastic processes in mathematical physics and engineering (New York City, April 1963)

15 **N. C. Metropolis, A. H. Taub, J. Todd, and C. B. Tompkins, Editors,** Experimental arithmetic, high speed computing, and mathematics (Atlantic City and Chicago, April 1962)

14 **R. Bellman, Editor,** Mathematical problems in the biological sciences (New York City, April 1961)

13 **R. Bellman, G. Birkhoff, and C. C. Lin, Editors,** Hydrodynamic instability (New York City, April 1960)

12 **R. Jakobson, Editor,** Structure of language and its mathematical aspects (New York City, April 1960)

11 **G. Birkhoff and E. P. Wigner, Editors,** Nuclear reactor theory (New York City, April 1959)

10 **R. Bellman and M. Hall, Jr., Editors,** Combinatorial analysis (New York University, April 1957)

9 **G. Birkhoff and R. E. Langer, Editors,** Orbit theory (Columbia University, April 1958)

8 **L. M. Graves, Editor,** Calculus of variations and its applications (University of Chicago, April 1956)

7 **L. A. MacColl, Editor,** Applied probability (Polytechnic Institute of Brooklyn, April 1955)

6 **J. H. Curtiss, Editor,** Numerical analysis (Santa Monica City College, August 1953)