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
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)


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 Mandelbrot and Julia sets (Cincinnati, Ohio, January 1994)


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)
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
Contents

Preface ix
Acknowledgements xiii
Original AMS Short Course Announcement xv

Chapter I. An Invitation to Quantum Computation
A Rosetta stone for quantum mechanics with an introduction to quantum computation
SAMUEL J. LOMONACO, JR. 3
Qubit devices
HOWARD E. BRANDT 67

Chapter II. Quantum Algorithms and Quantum Complexity Theory
Introduction to quantum algorithms
PETER W. SHOR 143
Shor’s quantum factoring algorithm
SAMUEL J. LOMONACO, JR. 161
Grover’s quantum search algorithm
SAMUEL J. LOMONACO, JR. 181
A survey of quantum complexity theory
UMESH VAZIRANI 193

Chapter III. Quantum Error Correcting Codes and Quantum Cryptography
An introduction to quantum error correction
DANIEL GOTTESMAN 221
A talk on quantum cryptography: Or how Alice outwits Eve
SAMUEL J. LOMONACO, JR. 237

Chapter IV. More Mathematical Connections
Topological quantum codes and anyons
ALEXEI KITAEV 267
Quantum topology and quantum computing
LOUIS H. KAUFFMAN 273

An entangled tale of quantum entanglement
SAMUEL J. LOMONACO, JR. 305

Index 351
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


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 Perivali, 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.
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

3 – $SAT$, 195
$BPP^{NP}$, 195
$G$-connections, 271
$NP \subsetneq BQP$, 208
$P = PSPACE$, 204
$P \# P$, 194, 204
$\mathcal{P}$-tensor product decomposition, 45
c-local, 199
$n$-qubit register, 35
1-chain, 270
1-cochain, 270
3-SAT, 208, 213
4-dimensional amplitudes, 294
abelian anyons, 268, 270
abelian Chern-Simons theories, 268
abstract tensor expression, 285
accuracy threshold, 110
action, 280
adjoint, 12, 13, 247
advanced encryption standard, 241
AES, 241
Aharonov and Nave, 212
Aharonov-Bohm interaction, 268
Alexander polynomial, 288
algebra of polynomial entanglement invariants, 319
algebra of real valued functions, 340
Alice, 41, 43, 239
all-optical quantum information processors, 101
amplitude amplification, 188
ancilla, 45, 109, 224
ancilla qubit, 228
ancilla qubits, 224
annihilation, 283
annihilation bra, 283
anyonic model, 268
anyons, 267, 268
Artin braid group, 290, 292, 301
atlas, 335
authentication, 242
automorphism group, 51
average value, 23
averaged observed value, 248
B92, 258
B92 quantum cryptographic protocol, 258
B92 quantum protocol, 259
basic set of entanglement invariants, 319
BB84 protocol, 255
BB84 protocol with noise, 256
BB84 protocol without Eve present, 254
BB84 protocol without noise, 253
beamsplitter, 68, 69, 73, 93
beamsplitters, 101
Bell, 308
Bell basis, 88
Bell basis states, 332
Bell-state analyzer, 90, 91
Bell-state analyzers, 125
Bell-state measurement, 94, 97, 98
Bell-state projective measurement, 96
Bell-state synthesizer, 87
Bell-state synthesizers, 124
Bell-states, 88
Benioff, 145
Bennett, 40, 50, 201
Bernstein, 203, 205
big adjoint action, 307, 316
big adjoint representation, 32, 345
bit & phase, 223
bit flip, 223
bit flip error, 223
black box, 151
black box model, 209
blackbox, 33
Bloch sphere, 328
Blum, 210
Bob, 41, 43, 239
Boolean states, 106
Bose condensate quantum computer, 119
Bose condensate quantum computers, 118
Bose condensates, 119
bose condensates, 124
Bose-Einstein condensation, 118
Bose-Einstein statistics, 91
bounded-error probabilistic polynomial time, 203
bounded-error quantum polynomial time, 203
BPP, 152, 194, 203, 204, 207
BQNP, 195, 212, 214

351
INDEX

352

BQNP-complete problem, 212
BQNP-completeness, 214
BQP, 149, 152, 194, 203, 204, 207
bra, 9
bra vectors, 9
bra’s, 246
bracket, 9, 246
bracket model, 290
bracket polynomial, 292
braid generator, 292
braid group, 272, 292, 293
braiding, 268, 272
braiding cancellation, 287
bras, 246, 279
BSM, 94
Caesar cipher, 240
Calderbank, 231
cancellation of maxima and minima, 284, 285
cap, 283, 286
caps, 297
catalysis, 45
Catch 22, 240, 242, 260
categorical physics, 297
category, 297
cavity QED, 111, 112, 125
cavity quantum electrodynamics, 111
cavity-QED quantum computers, 112
certificate complexity, 209
chart, 335
Chern-Simons Lagrangian, 296
Chern-Simons three-form, 295
Church’s thesis, 145
Church-Turing principle, 103
Church-Turing thesis, 144, 193, 194
ciphertext, 240
circle in spacetime, 282
circuit family, 149
circularly polarized, 7
class BQP, 150
classical computing device, 50
classical crypto systems, 242
classical entropy, 45, 46, 48
classical randomized class BPP, 149
classical reversible computation, 51
classical Turing machine, 196
CNOT, 148
CNOT, see also controlled-NOT, 51
coding space, 223
cohere, 112
cohere, 76
cohere, 105
collapse of the wave function, 246
collision-intractible hashing, 208
commutator, 24, 32, 248
compatible, 23, 248
compatible operators, 23
complete linear operators, 15
complete set of entanglement invariants, 318, 328
complex general linear group, 342
complex projective (n – 1) space, 11
complex projective space, 146
complex projective space CP^{n-1}, 11
complex special linear group, 342
complexity class BQP, 149, 150
complexity class P, 144, 145
computable, 144
computational basis, 202
computational degrees of freedom, 103, 110
computational security, 242
computational step, 50
computationally secure, 242
constituent part, 31
CONT’, 53
CONT”’, 54, 56
continued fraction, 169
continued fraction expansion, 155
continued fractions, 169
control bit, 52
controlled NOT, 83, 148, 201
controlled-Z operations, 228
controlled-NOT, 51, 53, 54, 84, 101, 102
corvergent, 169, 172
Cook’s theorem, 214
Cook-Levin theorem, 212
Cooley-Tukey algorithm, 153
Cooley-Tukey fast Fourier transform, 156
Cooley-Tukey FFT, 156
Cooper-pair charge, 116
counter measures, 260
CRCD, see also Classical Reversible Computing Device, 51
creation, 283
creation ket, 283
crossings, 297
CSS code, 231
CSS construction, 231
cup, 283, 286
cups, 297
Dan Simon, 145
dark counts, 257
Data Encryption Standard, 183
David Deutsch, 145
DeBroglie, 274
decoherence, 77, 87, 112, 125, 150, 222, 224
decoherence-free subspaces, 110
degenerate code, 227
degenerate eigenvalues, 15
degenerate operator, 15
degenerate quantum codes, 228
degenerate quantum states, 228
density (2^1), 328
density operator, 26–32, 315
derivation, 339
DES, 183, 240
deterministic finite state control, 196
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>deterministic query complexity</td>
<td>195</td>
</tr>
<tr>
<td>Deutsch</td>
<td>35, 194, 196, 205</td>
</tr>
<tr>
<td>Deutsch-Jozsa problem</td>
<td>205</td>
</tr>
<tr>
<td>deviation density matrix</td>
<td>113</td>
</tr>
<tr>
<td>diagonalization</td>
<td>15, 27, 48</td>
</tr>
<tr>
<td>diagonalized</td>
<td>15</td>
</tr>
<tr>
<td>diagonalizes</td>
<td>27</td>
</tr>
<tr>
<td>Dieks</td>
<td>57</td>
</tr>
<tr>
<td>diffeomorphism</td>
<td>342</td>
</tr>
<tr>
<td>different perspectives</td>
<td>314</td>
</tr>
<tr>
<td>differential manifolds</td>
<td>335</td>
</tr>
<tr>
<td>differential operator</td>
<td>324</td>
</tr>
<tr>
<td>Diffie</td>
<td>242</td>
</tr>
<tr>
<td>digital encryption standard</td>
<td>240</td>
</tr>
<tr>
<td>Dirac amplitude</td>
<td>294</td>
</tr>
<tr>
<td>Dirac brackets</td>
<td>278</td>
</tr>
<tr>
<td>Dirac notation</td>
<td>9–13, 23, 245, 246</td>
</tr>
<tr>
<td>Dirac’s bra-ket notation</td>
<td>146</td>
</tr>
<tr>
<td>directional derivatives</td>
<td>327, 339</td>
</tr>
<tr>
<td>discrete Fourier transform</td>
<td>155</td>
</tr>
<tr>
<td>discrete logarithms</td>
<td>152</td>
</tr>
<tr>
<td>distance of a code</td>
<td>269</td>
</tr>
<tr>
<td>dynamical invariant</td>
<td>47</td>
</tr>
<tr>
<td>eavesdropper</td>
<td>239</td>
</tr>
<tr>
<td>eavesdropping strategies</td>
<td>260</td>
</tr>
<tr>
<td>Edward Witten</td>
<td>295</td>
</tr>
<tr>
<td>efficient universal QTM</td>
<td>197</td>
</tr>
<tr>
<td>efficiently computable</td>
<td>144</td>
</tr>
<tr>
<td>eigenket</td>
<td>14</td>
</tr>
<tr>
<td>eigenspace</td>
<td>14</td>
</tr>
<tr>
<td>eigenvalue</td>
<td>14</td>
</tr>
<tr>
<td>Einstein</td>
<td>275</td>
</tr>
<tr>
<td>Einstein, Podolsky, and Rosen</td>
<td>308</td>
</tr>
<tr>
<td>Einstein, Podolsky, Rosen</td>
<td>40</td>
</tr>
<tr>
<td>Einstein-Podolsky-Rosen (EPR)</td>
<td>87</td>
</tr>
<tr>
<td>embedding</td>
<td>50, 52, 296</td>
</tr>
<tr>
<td>energy spectrum</td>
<td>278</td>
</tr>
<tr>
<td>entangled</td>
<td>39, 166, 312</td>
</tr>
<tr>
<td>entangled multiparticle systems</td>
<td>96</td>
</tr>
<tr>
<td>entanglement</td>
<td>74, 104</td>
</tr>
<tr>
<td>entanglement class</td>
<td>316, 321</td>
</tr>
<tr>
<td>entanglement classes</td>
<td>43, 328</td>
</tr>
<tr>
<td>entanglement invariant</td>
<td>323</td>
</tr>
<tr>
<td>entanglement invariants</td>
<td>327</td>
</tr>
<tr>
<td>entanglement of quantum states</td>
<td>301</td>
</tr>
<tr>
<td>entanglement swapper</td>
<td>95</td>
</tr>
<tr>
<td>entanglement swappers</td>
<td>94</td>
</tr>
<tr>
<td>entanglement swapping</td>
<td>87, 94, 96</td>
</tr>
<tr>
<td>entanglement type</td>
<td>43, 311, 316</td>
</tr>
<tr>
<td>environment</td>
<td>87, 222</td>
</tr>
<tr>
<td>EPR, 40, 41, 97, 125</td>
<td></td>
</tr>
<tr>
<td>EPR pair</td>
<td>38, 97, 310</td>
</tr>
<tr>
<td>EPR pairs</td>
<td>259</td>
</tr>
<tr>
<td>EPR-pair</td>
<td>87, 94</td>
</tr>
<tr>
<td>EPR-pair source</td>
<td>87</td>
</tr>
<tr>
<td>EPR-pair sources</td>
<td>124</td>
</tr>
<tr>
<td>erasure errors</td>
<td>228</td>
</tr>
<tr>
<td>error estimation</td>
<td>255</td>
</tr>
<tr>
<td>error syndrome</td>
<td>230</td>
</tr>
<tr>
<td>Euclidean algorithm</td>
<td>163, 178</td>
</tr>
<tr>
<td>Euler’s constant</td>
<td>172</td>
</tr>
<tr>
<td>Euler’s totient function</td>
<td>172</td>
</tr>
<tr>
<td>Eve</td>
<td>239</td>
</tr>
<tr>
<td>excited state</td>
<td>270</td>
</tr>
<tr>
<td>EXP</td>
<td>195</td>
</tr>
<tr>
<td>expected value</td>
<td>23</td>
</tr>
<tr>
<td>exponential map</td>
<td>317, 343</td>
</tr>
<tr>
<td>exponentiation of vector fields</td>
<td>339</td>
</tr>
<tr>
<td>extended local moves</td>
<td>313</td>
</tr>
<tr>
<td>factoring algorithm</td>
<td>145</td>
</tr>
<tr>
<td>factoring numbers</td>
<td>123</td>
</tr>
<tr>
<td>fault-tolerant quantum computation</td>
<td>234</td>
</tr>
<tr>
<td>Fermi-Dirac statistics</td>
<td>91</td>
</tr>
<tr>
<td>ferromagnetic dot</td>
<td>115</td>
</tr>
<tr>
<td>Feynman</td>
<td>145, 194, 280</td>
</tr>
<tr>
<td>Feynman integral</td>
<td>281</td>
</tr>
<tr>
<td>filtration</td>
<td>21</td>
</tr>
<tr>
<td>final key</td>
<td>255</td>
</tr>
<tr>
<td>fineness of a partition</td>
<td>45</td>
</tr>
<tr>
<td>finite memoryless stochastic source</td>
<td>45</td>
</tr>
<tr>
<td>flat connections</td>
<td>296</td>
</tr>
<tr>
<td>flow</td>
<td>339</td>
</tr>
<tr>
<td>Fourier sampling</td>
<td>205</td>
</tr>
<tr>
<td>Fourier sampling tree</td>
<td>206</td>
</tr>
<tr>
<td>Fourier transform</td>
<td>152, 165, 166, 175, 202, 205</td>
</tr>
<tr>
<td>FPQE</td>
<td>312</td>
</tr>
<tr>
<td>fractional quantum Hall effect</td>
<td>267</td>
</tr>
<tr>
<td>framing cancellation</td>
<td>287</td>
</tr>
<tr>
<td>free Boolean ring</td>
<td>51</td>
</tr>
<tr>
<td>functional integrals</td>
<td>296</td>
</tr>
<tr>
<td>fundamental problem of quantum entanglement</td>
<td>312</td>
</tr>
<tr>
<td>G-qubit</td>
<td>271</td>
</tr>
<tr>
<td>Gödel</td>
<td>144</td>
</tr>
<tr>
<td>generalized amplitudes</td>
<td>288</td>
</tr>
<tr>
<td>generalized Feynman integral</td>
<td>295</td>
</tr>
<tr>
<td>generator matrix</td>
<td>231</td>
</tr>
<tr>
<td>global quantum system</td>
<td>31</td>
</tr>
<tr>
<td>global unitary transformation</td>
<td>42</td>
</tr>
<tr>
<td>global unitary transformations</td>
<td>316</td>
</tr>
<tr>
<td>Gottesman</td>
<td>35</td>
</tr>
<tr>
<td>graph category</td>
<td>298</td>
</tr>
<tr>
<td>group of local unitary transformations</td>
<td>307, 315</td>
</tr>
<tr>
<td>group of transformations</td>
<td>345</td>
</tr>
<tr>
<td>Grover, 157, 183, 208</td>
<td></td>
</tr>
<tr>
<td>Grover’s algorithm</td>
<td>114, 187, 189, 190</td>
</tr>
<tr>
<td>Grover’s search algorithm</td>
<td>156</td>
</tr>
<tr>
<td>Hadamard, 55</td>
<td></td>
</tr>
<tr>
<td>Hadamard gate</td>
<td>82, 151</td>
</tr>
<tr>
<td>Hadamard gates</td>
<td>84</td>
</tr>
<tr>
<td>Hadamard operator</td>
<td>106</td>
</tr>
<tr>
<td>Hadamard transform</td>
<td>82, 166, 186, 200, 202</td>
</tr>
</tbody>
</table>
Hadamard transformation, 151
Hadamard transforms, 184
Hamiltonian, 24
Hamming code, 231
Heisenberg, 275
Heisenberg model, 33
Heisenberg picture, 33, 35
Heisenberg uncertainty principle, 23, 24, 248
Heisenberg’s uncertainty principle, 248, 249
Hellman, 242
Hermitian operator, 13
Hermitian operators, 247, 278
hidden variables, 40
high-temperature-superconductor Josephson junctions, 117
Hilbert space, 8, 245
homology classes, 270
Hopf algebra, 271, 288
hybrid argument, 208, 209
implementation weaknesses, 261
implementations, 262
implicit frame wiring diagrams, 56
incompatible, 24, 248
incompatible operators, 24
induced infinitesimal action, 308, 321
inefficiently computable, 144
infinitesimal action, 319–324, 345
infinitesimal generator, 339
information capacity of the transmission channel, 89
insecure channel, 240
integral curve, 339
interaction-free detector, 68
intrusion detection, 242
invariant of regular isotopy, 290
invariants of three-manifolds, 296
inversion, 184
ion-trap quantum computer, 110
ion-trap quantum computers, 125
IP, 195
irreversible, 313
irreversible computation, 52
J gate, 114
Jacobian matrix, 38
Jones polynomial, 288, 290, 296
Jordan curve theorem, 284
Josephson junction quantum computer, 116
Josephson junction SQUID quantum computers, 126
Josephson junctions, 124
Jozsa, 194, 205
Julian Schwinger’s algebra of measurement operators, 20
juxtaposition, 35
juxtaposition of two quantum systems, 35
ket, 9
ket vectors, 9
kets, 245, 279
Key Problem 1, 242
Key Problem 2, 242
Key Problem 3, 242
Kitaev, 195, 203, 212
Knill-Laflamme bound, 228
knot, 296
knot amplitudes, 282
knot invariants, 268, 288
Kronecker sum, 43, 319, 329
Kuperberg, 268
left- and right-circularly polarized photons, 11
lg, 46
Lie algebra, 307, 315, 318, 339, 342–344
Lie algebra Der(C∞u(2)), 327
Lie bracket, 318, 339
Lie group, 42
Lie group G, 341
Lie groups, 341
Lie subgroup, 341
Linden, 333
linearly polarized, 7
link invariants, 296
little adjoint representation, 32, 346
local equivalence, 43
local interaction, 41
local Lie algebra, 43
local move, 313, 315
local moves, 312
local subgroup, 42
local unitary group, 307
local unitary transformation, 42
local unitary transformations, 315
locally equivalent, 43, 316
MA, 195, 205, 207
Mach-Zehnder interferometer, 82, 84
macroscopic superconducting quantum states, 116
Max Born, 275
Max Planck, 275
maximal entanglement, 88
mean squared standard deviation, 248
measurement, 18, 22, 27, 28
Merlin-Arthur, 207
method of quantum adversaries, 195, 208, 210
Michelson interferometer, 68
Miller-Rabin, 162
mirrors, 101
mixed ensemble, 26, 28, 29
mixed ensembles, 329
modern Church-Turing thesis, 194
morphisms, 297
Morse diagrams, 289
Morse knot decomposition, 286
Mott transitions, 119
multi-tape quantum Turing machines, 199
multipartite quantum system, 31, 49
nanotechnology, 117
neutral atom quantum computers, 118
Niels Bohr, 274
Nielsen, 40
nine-qubit code, 223
NMR, 78, 113, 124
NMR quantum computer, 113, 125
no-cloning theorem, 57, 100, 222, 228
non-computable functions, 144
non-deterministic polynomial time, 212
non-local computation, 300
non-locality, 40, 41
non-standard form, 199
nonabelian anyons, 268, 271
nonabelian Chern-Simons theories, 268
nondegenerate code, 227
nondegenerate eigenvalues, 15
nondegenerate operator, 15
nondegenerate quantum codes, 228
nonunitary, 110
normal, 14
normal operator, 14
NOT, 55
NOT’ operator, 81, 107
NP, 212
NP-complete, 212
NP-complete problems, 195, 208
nuclear magnetic resonance, 78, 113
number field sieve, 162
observable, 13
observables, 247
one parameter subgroup, 341
one-time-pad, 241, 252
opaque eavesdropping, 260
operator, 13
optical lattices, 117, 119
oracle problem, 151, 181
orbit, 346
orbital degrees of freedom, 116
orbits, 43, 316, 346
output symbols, 46, 48
P, 194, 204
parity check matrix, 231
partial differential equations, 323, 327
partial trace, 29, 30
partially secret, 256
partition, 45
path qubit, 69
path-ordered integral, 25
Pauli errors, 224
Pauli exclusion principle, 115
Pauli group, 223, 230
Pauli matrices, 18
Pauli operators, 227, 230, 268
Pauli spin matrices, 17, 107
perfect secrecy, 241
perfectly secure, 241
period, 164, 175
permutation group, 51
PGS, 243
phase flip, 223
phase flip error, 223
photic and atomic qubits, 112
PKS, 244
plaintext, 240
plaintext/ciphertext attack, 183
plaintext/ciphertext attack on DES, 183
Planck’s constant, 24
polarized light, 6, 7, 11, 21
polarizers, 101
polynomial-time, 144
Popescu, 333
Popescu and Rohrlich, 45
populations, 76
positive operator valued measure, 21
positive operator valued measure (POVM, 70
POVM, 21, 70, 71, 124
POVM receiver, 259
practical secrecy, 240
practically secure, 240
preparations, 28, 46
pretty good security, 243
prime factorization problem, 163
principle of non-locality, 40, 41
principle of reality, 40
Prisoner’s Dilemma, 79
privacy amplification, 256, 258
probabilistic polynomial time, 194
probabilistic Turing machine, 193, 194
probability amplitudes, 147
probability distribution, 46
probability operator valued measure, 21
projection operator, 13, 48
projection operator for the eigenspace, 14
projector, 13
pseudo-spin states, 116
PSPACE, 194, 204
public directory, 243
public key cryptographic communication system, 243
public key cryptographic system, 243
pure ensemble, 26, 48
pure ensembles, 329
Q5SAT, 213
QED, 111
QED cavity, 102
QIP, 195
QMA, 212
QSAT, 212, 214
INDEX

QSPACE, 195
QTM, 197, 202
quantum, 124
quantum adversary, 208
quantum adversary argument, 210
quantum algorithm, 162
quantum alphabet, 254
quantum amplitude functor, 300
quantum amplitudes, 297
quantum cellular automata model, 146
quantum chaos, 103
quantum circuit model, 146, 150
quantum circuits, 196, 199
quantum code, 268, 269, 271
quantum complexity classes, 203
quantum computer, 110, 162
quantum computer communication networks, 112
quantum computers, 110
quantum computing device, 50
quantum controlled-NOT (or XOR), 84
quantum controlled-NOT gate, 82
quantum copier, 100, 101
quantum cryptographic communication system, 253
quantum cryptographic protocols, 259
quantum cryptography, 70, 71, 124, 239, 251
quantum decoherence, 75, 124
quantum dense coder, 90
quantum dense coding, 88
quantum double, 271
quantum entangled, 35, 39, 45
quantum entanglement, 39, 42, 312
quantum entanglement classes, 316
quantum entanglement invariant, 318
quantum entanglement invariants, 317, 318, 327
quantum entropy, 46, 48
quantum error correction, 103, 107, 222
quantum error correctors, 107
quantum error-correcting code, 225, 226
quantum factorizer, 103, 104
quantum field theory, 103, 295, 296
quantum Fourier transform, 153, 155
quantum games, 77, 78
quantum gate, 148
quantum gates, 80, 148
quantum Gilbert-Varshamov bound, 228
quantum group, 288
quantum Hamming bound, 227
quantum key receiver, 70, 124
quantum link invariants, 301
quantum lower bounds, 208
quantum measurement, 27
quantum measurement rubric, 18
quantum measurement theory, 18
quantum mechanics, 274
quantum memory, 112
quantum NOT gate, 81
quantum NP, 212
quantum register, 35, 36, 105, 106, 116
quantum repeater, 58
quantum replicator, 57
quantum robot, 119, 123
quantum robots, 119, 126
quantum secrecy, 252, 253
quantum simulators, 103, 253
quantum Singleton bound, 228
quantum state space, 146
quantum telephone exchanges, 125
quantum teleportation, 58, 59, 62, 97, 100, 124
quantum teleporter, 97
quantum Turing machine model, 146
quantum Turing machines, 196, 197
quantum witness, 212
quantum-dot quantum computer, 115
qubit, 7, 8, 68, 146, 196, 244, 246, 268
qubit device, 68
qubit entangler, 85, 87
qubit entanglers, 85
qubit errors, 224, 225
qubits, 124
raw key extraction, 255, 256
raw keys, 255
real general linear group, 341
real orthogonal group, 341
real special linear group, 342
receiver, 239
reconciled key, 257
recursive Fourier sampling, 206
recursive Fourier sampling problem, 207
reduced density matrix, 77
reflection, 185, 187
regular isotopy, 288, 289
Reidemeister move, 286, 287
repeated squaring, 154
Reshetikhin, 268
Reshetikhin-Turaev, 296
restricted fundamental problem of quantum entanglement, 307, 315, 317
reversible, 313
reversible classical transformation, 152
reversible computation, 50
reversible computing devices, 53
RFPQE, 307, 315, 317
right (left) elliptically polarized, 7
right invariant, 342
right invariant derivations, 318
right invariant directional derivatives, 318
right invariant smooth vector fields, 318
right multiplication map, 342
rotation, 55, 200
RSA, 243
same entanglement type, 43
Schrödinger equation, 24
Schrödinger, 274
Schrödinger equation, 277
Schrödinger picture, 33, 35
search problem, 182
searching a city phone book, 182
searching a database, 123
secret key, 240
secure channel, 240
security parameter, 258
selective measurement, 21
selective measurement operator, 21
self-adjoint operator, 13
self-adjoint operators, 247
semiconductor technology, 125
sender, 239
Shannon bit, 244
Shannon entropy, 45
Shor, 194, 231, 234
Shor’s algorithm, 163, 165, 166
Shor’s quantum factoring algorithm, 106, 163
silicon-based nuclear spin quantum computer, 114
Simon, 194
Simon’s algorithm, 151
Simon’s problem, 151
single-tape QTM, 203
smooth, 335, 336
smooth manifold, 335
smooth vector field, 337
Solovay, 203
SPACE, 195
spacelike distance, 41
special orthogonal group, 342, 346
special unitary group, 315, 346
spectral decomposition, 14, 17
spectral decomposition theorem, 14
square root of NOT, 55
square root of SWAP, 55
square-root-of-not gate, 80
SQUID, 117
SQUID quantum computer, 117
SQUIDs, 116, 124
stabilizer, 229, 231, 232
stabilizer code, 230
stabilizer codes, 228, 233
stabilizer operators, 269, 270
standard deviation, 23
standard form, 198
standard local moves, 313
standard unitary representation, 53
state bras, 9
state kets, 9
state of a quantum system, 10
Steane, 231
stochastic source, 46
sufficiently local, 45
sufficiently local operator, 45
sufficiently local unitary transformation, see also unitary, 45
superconducting cavities, 112
superconducting loops, 117
superconducting quantum interference devices, 116
superluminal communication, 41
superposition, 7, 36, 147, 245, 246
superselection rules, 270
SWAP, 55
symmetric group, 53
tangent bundle, 337
tangent bundles, 335
tangent space, 318, 323
tangent vector, 336
tangentially equivalent, 336
target bit, 52
teleportation, 58
Temperley Lieb algebra, 290, 291
tensor product, 10, 146
tentative final keys, 255, 257
the probabilistic generalization of \(NP\), 205
tree-strand braid group, 294
Toffoli gate, 52, 54, 148
topological amplitude, 294
topological amplitudes, 295
topological cancellation, 284
topological defects, 267
topological invariants, 296
topological number, 267
topological quantum field theory, 268, 294
toys for aging children store, 309
TQFT, 268
trace, 29
transformation, 13
transformation group, 345
translucent eavesdropping with entanglement, 261
translucent eavesdropping without entanglement, 261
transmission coefficient, 69
trap-door function, 242
Turaev, 268
Turing machine, 144
Turing machine model, 146
two-qubit entangler, 85
uncertainty, 23
uniform family of circuits, 149
uniform model, 146
uniformity conditions, 149
unitary group, 307, 342
unitary operator, 24
unitary operators, 247
unitary ribbon category, 268, 272
unitary transformation, 24
unitary transformations, 247
universal QTM, 202
universal quantum computer, 102, 103
universal quantum computers, 125
universal quantum copier, 101
universal quantum gate, 102
universal quantum Turing machine, 194, 198
universal set of gates, 147
vacuum to vacuum amplitude, 279
vacuum-vacuum computation, 300
vacuum-vacuum expectation, 295
Vazirani, 205
vector field, 337
vector fields, 326, 331, 335
Vernam cipher, 241
vertically and horizontally linearly polarized, 11
Viro, 268
von Neumann entropy, 46, 48
von Neumann-type projective measurement, 70
vortex, 117
wave-packet, 275
weight of an operator, 224
Wilson loop, 296
winding number, 267
wiring diagram, 51–56
Witten, 268, 296
Witten’s integral, 295, 296
Witten’s invariant, 268
Wollaston prism, 72, 73
Wootters, 40, 57
Yang-Baxter equation, 288, 301
Yao, 194, 199, 203
Yao’s construction, 202
Yao’s lemma, 207
Young’s two slit experiment, 249–251
Yuri Manin, 145
Zalka, 155
Zurek, 57
Selected Titles in This Series

(Continued from the front of this publication)

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)

For a complete list of titles in this series, visit the AMS Bookstore at www.ams.org/bookstore/.