Quantum Computing

Quantum Computing provides an introduction to one of the hottest current topics not only in computing and physics, but also in modern science and technology in general.

In quantum computing, we witness an exciting and very promising merge of two of the deepest and most successful scientific and technological developments of this century: quantum physics and computer science. Both of them are fascinating; each has brought a new view of the world and has been a basis of enormously successful technological developments.

The book takes a very broad view of quantum computing and information processing in general. It deals with such areas as quantum algorithms, automata, complexity theory, information and communication, cryptography and theoretical results. These include such topics as quantum error correcting codes and methods of quantum fault tolerance computing, which have made the vision of a real quantum computer come closer. No previous knowledge of quantum mechanics is required.

The book is written as a self-study introduction to quantum computing and can be used for a one-semester course on quantum computing, especially for computer scientists. To meet this aim the book contains numerous examples, figures and exercises. An extensive Appendix provides a concentrated presentation of some of the basic frameworks within which quantum computing develops: quantum mechanics, Hilbert spaces and computational complexity theory. Supporting material for the book can be found on the Author's website, http://www.mcgraw-hill.co.uk/gruska

Key features:

- one of the first books to present the subject starting with the basics and requiring a minimum of previous knowledge of the subject;
- requires a minimum of mathematics from the reader;
- contains many examples and exercises.

Jozef Gruska is Professor of Computer Science at Masaryk University, Brno, The Czech Republik. He has held visiting professorships in many universities in North America and Europe and has been a member of many international organisations in computer science. He was the author of *Foundations of Computing* (1997). His many achievements have included the post of Founding Chair (1989–1997) of the IFIP Specialist Group on Foundations of Computer Science and being the recipient of the IEEE Computer Pioneer Award (1997).

ISBN 0-07-709503-0

9 780077 095031

McGraw-Hill

A Division of The McGraw-Hill Companies

Quantum Computing

Contents v

Preface xi

1 FUNDAMENTALS 1
1.1 Why Quantum Computing . . . 2
1.2 Prehistory of Quantum Computing . . . 7
1.3 From Randomized to Quantum Computation . . . 11
1.3.1 Probabilistic Turing machines . . . 12
1.3.2 Quantum Turing machines . . . 15
1.4 Hilbert Space Basics . . . 19
1.4.1 Orthogonality, bases and subspaces . . . 23
1.4.2 Operators . . . 24
1.4.3 Observables and measurements . . . 26
1.4.4 Tensor products in Hilbert spaces . . . 27
1.4.5 Mixed states and density operators . . . 28
1.5 Experiments . . . 31
1.5.1 Classical experiments . . . 32
1.5.2 Quantum experiments—single particle interference . . . 33
1.5.3 Quantum experiments—measurements . . . 37
1.6 Quantum Principles . . . 39
1.6.1 States and amplitudes . . . 40
1.6.2 Measurements—the projection approach . . . 42
1.6.3 Evolution of quantum systems . . . 45
1.6.4 Compound quantum systems . . . 47
1.6.5 Quantum theory interpretations . . . 48
1.7 Classical Reversible Gates and Computing . . . 49
1.7.1 Reversible gates . . . 49
1.7.2 Reversible Turing machines . . . 52
1.7.3 Billiard ball model of (reversible) computing . . . 54

2 ELEMENTS 57
2.1 Quantum Bits and Registers . . . 58
2.1.1 Qubits . . . 58
2.1.2 Two-qubit registers . . . 65
2.1.3 No-cloning theorem . . . 68
2.1.4 Quantum registers . . . 69

2.2 Quantum Entanglement . . . 73
2.2.1 Entanglement of pure states . . . 73
2.2.2 Quantifying entanglement . . . 77
2.2.3 Substituting entanglement for communication . . . 78
2.3 Quantum Circuits . . . 81
2.3.1 Quantum gates . . . 81
2.3.2 Measurement gates . . . 88
2.3.3 Universality of quantum gates . . . 90
2.3.4 Arithmetical circuits . . . 95
2.3.5 Quantum superoperator circuits . . . 97

3 ALGORITHMS **101**
3.1 Quantum Parallelism and Simple Algorithms . . . 103
3.1.1 Deutsch's problem . . . 104
3.1.2 The Deutsch–Jozsa promise problem . . . 107
3.1.3 Simon's problems . . . 109
3.2 Shor's Algorithms . . . 111
3.2.1 Number theory basics . . . 112
3.2.2 Quantum Fourier Transform . . . 115
3.2.3 Shor's factorization algorithm . . . 119
3.2.4 Shor's discrete logarithm algorithm . . . 124
3.2.5 The hidden subgroup problems . . . 125
3.3 Quantum Searching and Counting . . . 127
3.3.1 Grover's search algorithm . . . 127
3.3.2 Reflections of Grover's iterate and search principles . . . 131
3.3.3 G-BBHT search algorithm . . . 132
3.3.4 Minimum-finding algorithm . . . 134
3.3.5 Generalizations and modifications of search problems . . . 136
3.4 Methodologies to Design Quantum Algorithms . . . 138
3.4.1 Amplitude amplification—boosting search probabilities . . . 138
3.4.2 Amplitude amplification—speeding of the states searching . . . 140
3.4.3 Case studies . . . 140
3.5 Limitations of Quantum Algorithms . . . 141
3.5.1 No quantum speed-up for the parity function . . . 142
3.5.2 Framework for proving lower bounds . . . 144
3.5.3 Oracle calls limitation of quantum computing . . . 148

4 AUTOMATA **151**
4.1 Quantum Finite Automata . . . 152
4.1.1 Models of classical finite automata . . . 153
4.1.2 One-way quantum finite automata . . . 154
4.1.3 One-measurement model of one-way QFA . . . 156
4.1.4 Equivalence of MO-1QFA and their simulation by PFA . . . 158
4.1.5 1QFA versus 1FA . . . 158
4.1.6 Two-way quantum finite automata . . . 161
4.1.7 2QFA versus 1FA . . . 164
4.2 Quantum Turing Machines . . . 168
4.2.1 One-tape quantum Turing machines . . . 168
4.2.2 Variations on the basic model . . . 173

4.2.3 Are quantum Turing machines analogue or discrete? . . . 175
4.2.4 Programming techniques for quantum Turing machines . . . 178
4.3 Quantum Cellular Automata . . . 181
4.3.1 Classical cellular automata . . . 181
4.3.2 One-dimensional quantum cellular automata . . . 184
4.3.3 Partitioned quantum one-dimensional cellular automata . . . 186
4.3.4 Quantum cellular automata versus quantum Turing machines . . . 189

5 COMPLEXITY **193**
5.1 Universal Quantum Turing Machines . . . 194
5.1.1 Efficient implementation of unitary transformations . . . 194
5.1.2 Design of a universal quantum Turing machine . . . 198
5.2 Quantum Computational Complexity . . . 201
5.2.1 Basic quantum versus classical complexity classes . . . 201
5.2.2 Relativized quantum complexity . . . 206
5.3 Quantum Communication Complexity . . . 209
5.3.1 Classical and quantum communication protocols and complexity . . . 210
5.3.2 Quantum communication versus computation complexity . . . 212
5.4 Computational Power of Quantum Non-linear Mechanics . . . 214

6 CRYPTOGRAPHY **217**
6.1 Prologue . . . 218
6.2 Quantum Key Generation . . . 220
6.2.1 Basic ideas of two parties quantum key generation . . . 220
6.2.2 Security issues of QKG protocols . . . 222
6.2.3 Quantum key generation protocols BB84 and B92 . . . 224
6.2.4 Multiparty key generation . . . 229
6.2.5 Entanglement-based QKG protocols . . . 230
6.2.6 Unconditional security of QKG* . . . 232
6.2.7 Experimental quantum cryptography . . . 236
6.3 Quantum Cryptographic Protocols . . . 238
6.3.1 Quantum coin-flipping and bit commitment protocols . . . 240
6.3.2 Quantum oblivious transfer protocols . . . 242
6.3.3 Security of the quantum protocols . . . 245
6.3.4 Security limitations of the quantum cryptographic protocols . . . 248
6.3.5 Insecurity of quantum one-sided two-party computation protocols . . . 251
6.4 Quantum Teleportation and Superdense Coding . . . 251
6.4.1 Basic principles . . . 252
6.4.2 Teleportation circuit . . . 254
6.4.3 Quantum secret sharing . . . 256
6.4.4 Superdense coding . . . 257

7 PROCESSORS **259**
7.1 Early Quantum Computers Ideas . . . 260
7.1.1 Benioff's quantum computer . . . 261
7.1.2 Feynman's quantum computer . . . 261
7.1.3 Peres' quantum computer . . . 262
7.1.4 Deutsch's quantum computer . . . 263
7.2 Impacts of Imperfections . . . 264

7.2.1 Internal imperfections . . . 264
7.2.2 Decoherence . . . 265
7.3 Quantum Computation and Memory Stabilization . . . 268
7.3.1 The symmetric space . . . 269
7.3.2 Stabilization by projection into the symmetric subspace . . . 270
7.4 Quantum Error-correcting Codes . . . 271
7.4.1 Classical error-detecting and -correcting codes . . . 272
7.4.2 Framework for quantum error-correcting codes . . . 278
7.4.3 Case studies . . . 284
7.4.4 Basic methods to design quantum error-correcting codes . . . 289
7.4.5 Stabilizer codes . . . 292
7.5 Fault-tolerant Quantum Computation . . . 296
7.5.1 Fault-tolerant quantum error correction . . . 297
7.5.2 Fault-tolerant quantum gates . . . 300
7.5.3 Concatenated coding . . . 304
7.6 Experimental Quantum Processors . . . 306
7.6.1 Main approaches . . . 307
7.6.2 Ion trap . . . 308
7.6.3 Cavity QED . . . 310
7.6.4 Nuclear magnetic resonance (NMR) . . . 311
7.6.5 Other potential technologies . . . 313

8 INFORMATION **315**
8.1 Quantum Entropy and Information . . . 316
8.1.1 Basic concepts of classical information theory . . . 317
8.1.2 Quantum entropy and information . . . 318
8.2 Quantum Channels and Data Compression . . . 320
8.2.1 Quantum sources, channels and transmissions . . . 320
8.2.2 Shannon's coding theorems . . . 323
8.2.3 Schumacher's noiseless coding theorem . . . 324
8.2.4 Dense quantum coding . . . 328
8.2.5 Quantum Noisy Channel Transmissions . . . 330
8.2.6 Capacities of erasure and depolarizing channels . . . 332
8.3 Quantum Entanglement . . . 332
8.3.1 Transformation and the partial order of entangled states . . . 332
8.3.2 Entanglement purification/distillation . . . 333
8.3.3 Entanglement concentration and dilution . . . 336
8.3.4 Quantifying entanglement . . . 337
8.3.5 Bound entanglement . . . 338
8.4 Quantum Information-Processing Principles and Primitives . . . 339
8.4.1 Search for quantum information principles . . . 339
8.4.2 Quantum information-processing primitives . . . 340

9 APPENDIX **341**
9.1 Quantum Theory . . . 341
9.1.1 Pre-history of quantum theory . . . 342
9.1.2 Heisenberg's uncertainty principle . . . 345
9.1.3 Quantum theory versus physical reality . . . 349
9.1.4 Quantum measurements . . . 350

9.1.5 Quantum paradoxes . . . 352
9.1.6 The quantum paradox . . . 357
9.1.7 Interpretations of quantum theory . . . 358
9.1.8 Incompleteness of quantum mechanics . . . 363
9.2 Hilbert Space Framework for Quantum Computing . . . 365
9.2.1 Hilbert spaces . . . 365
9.2.2 Linear operators . . . 368
9.2.3 Mixed states and density matrices . . . 371
9.2.4 Probabilities and observables . . . 375
9.2.5 Evolution of quantum states . . . 376
9.2.6 Measurements . . . 376
9.2.7 Tensor products and Hilbert spaces . . . 377
9.2.8 Generalized measurements–POV measurements . . . 378
9.3 Deterministic and Randomized Computing . . . 380
9.3.1 Computing models . . . 380
9.3.2 Randomized computations . . . 385
9.3.3 Complexity classes . . . 387
9.3.4 Computational theses . . . 390
9.4 Exercises . . . 391
9.5 Historical and Bibliographical References . . . 395

Bibliography **401**

Index **419**