



# QUANTUM COMPUTING FUNDAMENTALS

From Basic Linear Algebra to Quantum Programming



**DR. CHUCK EASTTOM**

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



# **Quantum Computing Fundamentals**

*This page intentionally left blank*

# Quantum Computing Fundamentals

Dr. Chuck Easttom

◆ Addison-Wesley

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town  
Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City  
São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

Visit us on the Web: [informit.com/aw](http://informit.com/aw)

Library of Congress Control Number: 2021903471

Copyright © 2021 Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit [www.pearson.com/permissions/](http://www.pearson.com/permissions/).

ISBN-13: 978-0-13-679381-6

ISBN-10: 0-13-679381-9

ScoutAutomatedPrintCode

**Editor-in-Chief**

Mark Taub

**Director, ITP Product Manager**

Brett Bartow

**Executive Editor**

James Manly

**Development Editor**

Christopher A. Cleveland

**Managing Editor**

Sandra Schroeder

**Project Editor**

Mandie Frank

**Copy Editor**

Bart Reed

**Indexer**

Cheryl Ann Lenser

**Proofreader**

Donna Mulder

**Technical Reviewers**

Izzat Alsmadi,

Renita Murimi

**Editorial Assistant**

Cindy Teeters

**Designer**

Chuti Prasertsith

**Compositor**

codeMantra

# Credits

Cover

Zinetron/Shutterstock

## Figure Number

## Credit Attribution

Figure 12-1A	Screenshot © Microsoft Corporation
Figure 16-1	Screenshot of Microsoft QDK for Visual Studio Code © Microsoft 2021
Figure 16-2	Screenshot of New Q# Program in Visual Studio Code © Microsoft 2021
Figure 16-3	Screenshot of Save Program in Visual Studio Code © Microsoft 2021
Figure 16-4	Screenshot of QDK Samples © Microsoft 2021
Figure 16-5	Screenshot of Q# Random Number Generator © Microsoft 2021
Figure 16-6	Screenshot of Q# Open Statements © Microsoft 2021
Figure 16-7	Screenshot of Operation QuantumPseudoRandomNumberGenerator © Microsoft 2021
Figure 16-8	Screenshot of Operation RandomNumberInRange © Microsoft 2021
Figure 16-9	Screenshot of Operation SampleRandomNumber © Microsoft 2021
Figure 16-10	Screenshot of Open Statements in Grover's Algorithm Code © Microsoft 2021
Figure 16-11	Screenshot of ReflectMarked © Microsoft 2021
Figure 16-12	Screenshot of ReflectUniform © Microsoft 2021
Figure 16-13	Screenshot of Additional Functions for Grover's algorithm © Microsoft 2021
Figure 16-14	Screenshot of Entry Point for Grover's Algorithm © Microsoft 2021
Figure 16-15	Screenshot of NumberOfIterations Function © Microsoft 2021
Figure 16-16	Screenshot of Beginning of Deutsch-Jozsa © Microsoft 2021
Figure 16-17	Screenshot of Deutsch-Jozsa Entry Point © Microsoft 2021
Figure 16-18	Screenshot of IsConstant Function © Microsoft 2021
Figure 16-19	Screenshot of Remaining Functions for Deutsch-Jozsa © Microsoft 2021
Figure 16-20	Screenshot of Entanglement © Microsoft 2021
Figure 17-1	Screenshot of Quantum Inspire Editor © 2021 Quantum Inspire
Figure 17-2	Screenshot of Two Qubits © 2021 Quantum Inspire
Figure 17-3	Screenshot of CNOT Gate © 2021 Quantum Inspire
Figure 17-4	Screenshot of Hadamard Gate © 2021 Quantum Inspire
Figure 17-5	Screenshot of Multiple Gates © 2021 Quantum Inspire
Figure 17-6	Screenshot of Start a New Project © 2021 Quantum Inspire
Figure 17-7	Screenshot of New Project Editor © 2021 Quantum Inspire
Figure 17-8	Screenshot of Error Correction © 2021 Quantum Inspire
Figure 17-9	Screenshot of Grover's Algorithm © 2021 Quantum Inspire
Figure 17-10	Screenshot of Grover's Algorithm Results © 2021 Quantum Inspire
Figure 17-11	Screenshot of Deutsch-Jozsa Algorithm © 2021 Quantum Inspire
Unnumbered Figure 17-1	Screenshot of CNOT Gate Symbol © 2021 Quantum Inspire

## **Dedication**

*As always, I dedicate my work to my wonderful wife Teresa. A quote from my favorite movie is how I usually thank her: “What truly is logic? Who decides reason? My quest has taken me to the physical, the metaphysical, the delusional, and back. I have made the most important discovery of my career—the most important discovery of my life. It is only in the mysterious equations of love that any logic or reasons can be found. I am only here tonight because of you. You are the only reason I am. You are all my reasons.”*

# Table of Contents

Preface	xvii
<b>Part I Preparatory Material</b>	
<b>Chapter 1: Introduction to Essential Linear Algebra</b>	<b>2</b>
1.1 What Is Linear Algebra? . . . . .	3
1.2 Some Basic Algebra . . . . .	4
1.2.1 Groups, Rings, and Fields . . . . .	6
1.3 Matrix Math . . . . .	10
1.3.1 Matrix Addition and Multiplication . . . . .	11
1.3.2 Matrix Transposition . . . . .	13
1.3.3 Submatrix . . . . .	14
1.3.4 Identity Matrix . . . . .	15
1.3.5 Deeper Into the Matrix . . . . .	16
1.4 Vectors and Vector Spaces . . . . .	23
1.5 Set Theory . . . . .	25
1.6 Summary . . . . .	29
Test Your Skills . . . . .	29
<b>Chapter 2: Complex Numbers</b>	<b>32</b>
2.1 What Are Complex Numbers? . . . . .	32
2.2 Algebra of Complex Numbers . . . . .	34
2.3 Complex Numbers Graphically . . . . .	38
2.4 Vector Representations of Complex Numbers . . . . .	45
2.5 Pauli Matrices . . . . .	48
2.5.1 Algebraic Properties of Pauli Matrices . . . . .	52
2.6 Transcendental Numbers . . . . .	56
2.7 Summary . . . . .	58
Test Your Skills . . . . .	58

<b>Chapter 3: Basic Physics for Quantum Computing</b>	<b>60</b>
3.1 The Journey to Quantum . . . . .	61
3.2 Quantum Physics Essentials . . . . .	65
3.2.1 Basic Atomic Structure . . . . .	65
3.2.2 Hilbert Spaces. . . . .	68
3.2.3 Uncertainty . . . . .	70
3.2.4 Quantum States . . . . .	73
3.2.5 Entanglement . . . . .	75
3.3 Summary . . . . .	77
Test Your Skills . . . . .	77
<b>Chapter 4: Fundamental Computer Science for Quantum Computing</b>	<b>80</b>
4.1 Data Structures . . . . .	81
4.1.1 List . . . . .	81
4.1.2 Binary Tree. . . . .	88
4.2 Algorithms . . . . .	88
4.2.1 Sorting Algorithms . . . . .	90
4.3 Computational Complexity. . . . .	93
4.3.1 Cyclomatic Complexity . . . . .	93
4.3.2 Halstead Metrics. . . . .	94
4.4 Coding Theory. . . . .	95
4.5 Logic Gates . . . . .	96
4.5.1 AND . . . . .	96
4.5.2 OR . . . . .	96
4.5.3 XOR . . . . .	96
4.5.4 Application of Logic Gates. . . . .	97
4.6 Computer Architecture . . . . .	100

4.7 Summary . . . . .	103
Test Your Skills . . . . .	103
<b>Chapter 5: Basic Information Theory</b>	<b>106</b>
5.1 Basic Probability . . . . .	107
5.1.1 Basic Probability Rules. . . . .	107
5.2 Set Theory . . . . .	108
5.3 Information Theory . . . . .	112
5.3.1 Theorem 1: Shannon's Source Coding Theorem. . . . .	113
5.3.2 Theorem 2: Noisy Channel Theorem. . . . .	113
5.3.3 Information Entropy . . . . .	113
5.3.4 Information Diversity. . . . .	116
5.4 Quantum Information . . . . .	118
5.5 Summary . . . . .	120
Test Your Skills . . . . .	120
<b>Part II Basic Quantum Computing</b>	
<b>Chapter 6: Basic Quantum Theory</b>	<b>122</b>
6.1 Further with Quantum Mechanics . . . . .	123
6.1.1 Bra-Ket Notation. . . . .	123
6.1.2 Hamiltonian . . . . .	124
6.1.3 Wave Function Collapse. . . . .	125
6.1.4 Schrödinger's Equation . . . . .	128
6.2 Quantum Decoherence. . . . .	129
6.3 Quantum Electrodynamics . . . . .	131
6.4 Quantum Chromodynamics . . . . .	133
6.5 Feynman Diagram . . . . .	134
6.6 Summary . . . . .	136
Test Your Skills . . . . .	136

<b>Chapter 7: Quantum Entanglement and QKD</b>	<b>138</b>
7.1 Quantum Entanglement . . . . .	138
7.2 Interpretation . . . . .	143
7.2.1 The Copenhagen Interpretation . . . . .	144
7.2.2 The Many-Worlds Interpretation . . . . .	144
7.2.3 Decoherent Histories . . . . .	145
7.2.4 Objective Collapse Theory . . . . .	145
7.3 QKE . . . . .	146
7.3.1 BB84 Protocol . . . . .	146
7.3.2 B92 Protocol . . . . .	149
7.3.3 SARG04 . . . . .	149
7.3.4 Six-State Protocol . . . . .	151
7.3.5 E91 . . . . .	151
7.3.6 Implementations . . . . .	151
7.4 Summary . . . . .	151
Test Your Skills . . . . .	152
<b>Chapter 8: Quantum Architecture</b>	<b>154</b>
8.1 Further with Qubits . . . . .	154
8.2 Quantum Gates . . . . .	158
8.2.1 Hadamard Gate . . . . .	159
8.2.2 Phase Shift Gates . . . . .	161
8.2.3 Pauli Gates . . . . .	161
8.2.4 Swap Gates . . . . .	162
8.2.5 Fredkin Gate . . . . .	163
8.2.6 Toffoli Gates . . . . .	163
8.2.7 Controlled Gates . . . . .	163
8.2.8 Ising Gates . . . . .	164
8.2.9 Gottesman–Knill Theorem . . . . .	165

8.3 More with Gates . . . . .	166
8.4 Quantum Circuits . . . . .	167
8.5 The D-Wave Quantum Architecture. . . . .	169
8.5.1 SQUID . . . . .	170
8.6 Summary . . . . .	172
Test Your Skills . . . . .	172
<b>Chapter 9: Quantum Hardware</b>	<b>174</b>
9.1 Qubits. . . . .	174
9.1.1 Photons . . . . .	175
9.1.2 Electron . . . . .	177
9.1.3 Ions . . . . .	178
9.1.4 NMRQC. . . . .	179
9.1.5 Bose-Einstein Condensate Quantum Computing . . . . .	179
9.1.6 GaAs Quantum Dots. . . . .	181
9.2 How Many Qubits Are Needed? . . . . .	181
9.3 Addressing Decoherence . . . . .	182
9.3.1 Supercooling . . . . .	185
9.3.2 Dealing with Noise . . . . .	185
9.3.3 Filtering Noise . . . . .	186
9.4 Topological Quantum Computing . . . . .	186
9.4.1 Basic Braid Theory . . . . .	186
9.4.2 More on Braid Theory. . . . .	187
9.4.3 More on Topological Computing . . . . .	187
9.5 Quantum Essentials . . . . .	187
9.5.1 Quantum Data Plane . . . . .	187
9.5.2 Measurement Plane . . . . .	188
9.5.3 Control Processor Plane . . . . .	188
9.6 Quantum Networking . . . . .	188

9.6.1 Tokyo QKD . . . . .	188
9.6.2 Beijing-Shanghai Quantum Link . . . . .	189
9.6.3 Micius Satellite . . . . .	189
9.6.4 Distributed Quantum Computing . . . . .	190
9.7 Summary . . . . .	191
Test Your Skills . . . . .	191
<b>Chapter 10: Quantum Algorithms</b>	<b>194</b>
10.1 What Is an Algorithm? . . . . .	194
10.2 Deutsch’s Algorithm . . . . .	197
10.3 Deutsch-Jozsa Algorithm . . . . .	199
10.4 Bernstein-Vazirani Algorithm . . . . .	201
10.5 Simon’s Algorithm . . . . .	202
10.6 Shor’s Algorithm . . . . .	203
10.6.1 The Quantum Period-Finding Function. . . . .	206
10.7 Grover’s Algorithm . . . . .	209
10.8 Summary . . . . .	211
Test Your Skills . . . . .	211
<b>Part III Quantum Computing and Cryptography</b>	
<b>Chapter 11: Current Asymmetric Algorithms</b>	<b>212</b>
11.1 RSA . . . . .	213
11.1.1 RSA Example 1 . . . . .	215
11.1.2 RSA Example 2 . . . . .	215
11.1.3 Factoring RSA Keys . . . . .	216
11.2 Diffie-Hellman . . . . .	216
11.2.1 Elgamal . . . . .	217
11.2.2 MQV . . . . .	219

11.3 Elliptic Curve . . . . .	219
11.3.1 ECC Diffie-Hellman . . . . .	224
11.3.2 ECDSA . . . . .	225
11.4 Summary . . . . .	227
Test Your Skills . . . . .	227
<b>Chapter 12: The Impact of Quantum Computing on Cryptography</b>	<b>228</b>
12.1 Asymmetric Cryptography . . . . .	229
12.1.1 How Many Qubits Are Needed? . . . . .	230
12.2 Specific Algorithms . . . . .	231
12.2.1 RSA . . . . .	231
12.2.2 Diffie-Hellman . . . . .	231
12.2.3 ECC . . . . .	232
12.2.4 Symmetric Ciphers . . . . .	232
12.2.5 Cryptographic Hashes . . . . .	232
12.3 Specific Applications . . . . .	233
12.3.1 Digital Certificates . . . . .	233
12.3.2 SSL/TLS . . . . .	234
12.3.4 Public Key Infrastructure (PKI) . . . . .	237
12.3.5 VPN . . . . .	239
12.3.6 SSH . . . . .	240
12.4 Summary . . . . .	241
Test Your Skills . . . . .	241
<b>Chapter 13: Lattice-based Cryptography</b>	<b>244</b>
13.1 Lattice-Based Mathematical Problems . . . . .	245
13.1.1 Shortest Integer Problem . . . . .	248
13.1.2 Shortest Vector Problem . . . . .	248
13.1.3 Closest Vector Problem . . . . .	248

13.2	Cryptographic Algorithms	249
13.2.1	NTRU	249
13.2.2	GGH	252
13.2.3	Peikert's Ring	253
13.3	Solving Lattice Problems	256
13.3.1	Lenstra-Lenstra-Lovász (LLL)	256
13.4	Summary	259
	Test Your Skills	259
<b>Chapter 14: Multivariate Cryptography</b>		<b>262</b>
14.1	Mathematics	262
14.2	Matsumoto-Imai	264
14.3	Hidden Field Equations	266
14.4	Multivariate Quadratic Digital Signature Scheme (MQDSS)	268
14.5	SFLASH	269
14.6	Summary	271
	Test Your Skills	271
<b>Chapter 15: Other Approaches to Quantum Resistant Cryptography</b>		<b>274</b>
15.1	Hash Functions	274
15.1.1	Merkle-Damgaard	275
15.1.2	SWIFFT	275
15.1.3	Lamport Signature	277
15.2	Code-Based Cryptography	279
15.2.1	McEliece	279
15.2.2	Niederreiter Cryptosystem	280
15.3	Supersingular Isogeny Key Exchange	281
15.3.1	Elliptic Curves	281
15.3.2	SIDH	285

15.4 Summary . . . . .	289
Test Your Skills . . . . .	289

## **Part IV Quantum Programming**

### **Chapter 16: Working with Q# 292**

16.1 Basic Programming Concepts . . . . .	292
16.1.1 Variables and Statements . . . . .	292
16.1.2 Control Structures . . . . .	295
16.1.3 Object-Oriented Programming . . . . .	297
16.2 Getting Started with Q# . . . . .	298
16.3 Grover’s Algorithm . . . . .	303
16.3.1 Grover’s Algorithm Reviewed . . . . .	303
16.3.2 The Code for Grover’s Algorithm . . . . .	304
16.4 Deutsch-Jozsa Algorithm . . . . .	307
16.4.1 Deutsch-Jozsa Algorithm Reviewed . . . . .	308
16.4.2 The Code for Deutsch-Jozsa Algorithm . . . . .	308
16.5 Bit Flipping . . . . .	310
16.6 Summary . . . . .	311
Test Your Skills . . . . .	311

### **Chapter 17: Working with QASM 314**

17.1 Basic Programming Concepts . . . . .	315
17.1.1 Instructions . . . . .	315
17.1.2 Commands . . . . .	319
17.2 Getting Started with QASM . . . . .	319
17.3 Quantum Error Correction . . . . .	320
17.4 Grover’s Algorithm . . . . .	322
17.4.1 Grover’s Algorithm Reviewed . . . . .	322
17.4.2 The Code for Grover’s Algorithm . . . . .	324

17.5 Deutsch-Jozsa Algorithm . . . . .	326
17.5.1 Deutsch-Jozsa Algorithm Reviewed . . . . .	326
17.5.2 The Code for the Deutsch-Jozsa Algorithm . . . . .	326
17.6 Summary . . . . .	328
Test Your Skills . . . . .	328
<b>Appendix: Answers to Test Your Skills Questions</b>	<b>330</b>
<b>Index</b>	<b>338</b>

## Preface

Writing a book is always a challenging project. But with a topic like quantum computing, it is much more so. If you cover too much, the reader will be overwhelmed and will not gain much from the book. If you cover too little, you will gloss over critical details. With quantum computing, particularly a book written for the novice, it is important to provide enough information without overwhelming. It is my sincere hope that I have accomplished this.

Clearly some readers will have a more robust mathematical background than others. Some of you will probably have some experience in quantum computing; however, for those of you lacking some element in your background, don't be concerned. The book is designed to give you enough information to proceed forward. Now this means that every single chapter could be much larger and go much deeper. In fact, I cannot really think of a single chapter that could not be a separate book!

When you are reading a section that is a new concept to you, particularly one you struggle with, don't be concerned. This is common with difficult topics. And if you are not familiar with linear algebra, Chapter 1, "Introduction to Essential Linear Algebra," will start right off with new concepts for you—concepts that some find challenging. I often tell students to not be too hard on themselves. When you are struggling with a concept and you see someone else (perhaps the professor, or in this case the author) seem to have an easy mastery of the topic, it is easy to get discouraged. You might think you are not suited for this field. If you were, would you not understand it as readily as others? The secret that no one tells you is that all of those "others," the ones who are now experts, struggled in the beginning, too. Your struggle is entirely natural. Don't be concerned. You might have to read some sections more than once. You might even finish the book with a solid general understanding, but with some "fuzziness" on specific details. That is not something to be concerned about. This is a difficult topic.

For those readers with a robust mathematical and/or physics background, you are likely to find some point where you feel I covered something too deeply, or not deeply enough. And you might be correct. It is quite difficult when writing a book on a topic such as this, for a novice audience, to find the proper level at which to cover a given topic. I trust you won't be too harsh in your judgment should you disagree with the level at which I cover a topic.

Most importantly, this book should be the beginning of an exciting journey for you. This is the cutting edge of computer science. Whether you have a strong background and easily master the topics in this book (and perhaps knew some already) or you struggle with every page, the end result is the same. You will be open to a bold, new world. You will see the essentials of quantum mechanics, understand the quantum computing revolution, and perhaps even be introduced to some new mathematics. So please don't get too bogged down in the struggle to master concepts. Remember to relish the journey!

Register your copy of *Quantum Computing Fundamentals* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to [informit.com/register](http://informit.com/register) and log in or create an account. Enter the product ISBN (9780136793816) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.

## **Acknowledgments**

There are so many people who made this book possible. Let me start with Professor Izzat Alsmadi (Texas A&M–San Antonio) and Professor Renita Murimi (University of Dallas) who were gracious enough to provide technical review of each and every chapter. Chris Cleveland was the lead editor, and I must confess, I am not the easiest person to edit. His patience and careful eye for detail were essential to this book. I also want to thank Bart Reed for his work in copy editing. All the people working on this book have done an extremely good job helping me create a book that can be clear and accurate for the reader to learn this challenging topic.

## About the Author

**Dr. Chuck Easttom** is the author of 31 books, including several on computer security, forensics, and cryptography. His books are used at more than 60 universities. He has also authored scientific papers (more than 70 so far) on digital forensics, cyber warfare, cryptography, and applied mathematics. He is an inventor with 22 computer science patents. He holds a Doctor of Science in cyber security (dissertation topic: a study of lattice-based cryptographic algorithms for post-quantum computing). He also has a Ph.D. in Technology, focusing on nanotechnology (dissertation title: “The Effects of Complexity on Carbon Nanotube Failures”) and a Ph.D. in Computer Science (dissertation title: “On the Application of Graph Theory to Digital Forensics”). He also has three master’s degrees (one in applied computer science, one in education, and one in systems engineering). He is a senior member of the IEEE and a senior member of the ACM (Association of Computing Machinery) as well as a member of IACR (International Association of Cryptological Research) and INCOSE (International Council on Systems Engineering). He is also a distinguished speaker of the ACM and a distinguished visitor of the IEEE Computer Society. He currently is an adjunct lecturer for Georgetown University.

# Chapter 6

## Basic Quantum Theory

### *Chapter Objectives*

**After reading this chapter and completing the quizzes, you will be able to do the following:**

- Use bra-ket notation
- Understand the Hamiltonian operator
- Have a working knowledge of wave functions and the wave function collapse
- Recognize the role of Schrödinger's equation
- Know the role of quantum decoherence and its impact on quantum computing
- Have a generalized understanding of quantum electrodynamics
- Demonstrate basic knowledge of quantum chromodynamics

This chapter will introduce you to various aspects of quantum theory. Some of these topics were briefly touched on in Chapter 3, “Basic Physics for Quantum Computing.” It is essential that you have a strong grasp of Chapters 1 through 3 in order to follow along in this chapter. The first issue to address is what precisely is quantum theory? It is actually a number of related theories, including quantum field theory, quantum electrodynamics (QED), and in some physicists’ opinion, even quantum chromodynamics, which deals with quarks. In this chapter, the goal is to deepen the knowledge you gained in Chapter 3 and to provide at least a brief introduction to a range of topics that all fit under the umbrella of quantum theory.

In this chapter, it is more important than ever to keep in mind our goal. Yes, I will present a fair amount of mathematics, some of which may be beyond some readers. However, unless your goal is to do actual work in the field of quantum physics or quantum computing research, then what you need is simply a general comprehension of what the equations mean. You do not need to have the level of mathematical acumen that would allow you to actually do the math. So, if you encounter some math

you find daunting, simply review it a few times to ensure you get the general gist of it and move on. You can certainly work with qubits,  $Q\#$ , and other quantum tools later in this book without a deep understanding of how to do the mathematics.

## 6.1 Further with Quantum Mechanics

Chapter 3 introduced some fundamental concepts in quantum physics. This section expands our exploration of quantum mechanics a bit. In 1932, Werner Heisenberg was awarded the Nobel Prize in Physics for the “creation of quantum mechanics.” I am not sure that one person can be solely credited with the creation of quantum mechanics, but certainly Heisenberg deserves that credit as much as anyone.

The publication that earned him the Nobel Prize was titled “Quantum-Theoretical Re-interpretation of Kinematic and Mechanical Relations.” This paper is rather sophisticated mathematically, and we won’t be exploring it in detail here. The paper introduced a number of concepts that formed the basis of quantum physics. The interested reader can consult several resources, including the following:

<https://arxiv.org/pdf/quant-ph/0404009.pdf>

<https://www.heisenberg-gesellschaft.de/3-the-development-of-quantum-mechanics-1925-ndash-1927.html>

[https://inis.iaea.org/collection/NCLCollectionStore/\\_Public/08/282/8282072.pdf](https://inis.iaea.org/collection/NCLCollectionStore/_Public/08/282/8282072.pdf)

### 6.1.1 Bra-Ket Notation

Bra-ket notation was introduced a bit earlier, in Chapter 3. However, this notation is so essential to understanding quantum physics and quantum computing that we will revisit it, with more detail. Recall that quantum states are really vectors. These vectors include complex numbers. However, it is often possible to ignore the details of the vector and work with a representation of the vector. This notation is called Dirac notation or bra-ket notation.

A *bra* is denoted by  $\langle V|$ , and a *ket* is denoted by  $|V\rangle$ . Yes, the terms are intentional, meaning *braket*, or *bracket*. But what does this actually mean? A bra describes some linear function that maps each vector in  $V$  to a number in the complex plane. Bra-ket notation is really about linear operators on complex vector spaces, and it is the standard way that states are represented in quantum physics and quantum computing. One reason for this notation is to avoid confusion. The term *vector* in linear algebra is a bit different from the term *vector* in classical physics. In classical physics, a vector denotes something like velocity that has magnitude and direction; however, in quantum physics, a vector (linear algebra vector) is used to represent a quantum state, thus the need for a different notation. It is important to keep in mind that these are really just vectors. Therefore, the linear algebra that you saw in Chapter 1, “Introduction to Essential Linear Algebra,” applies.

### 6.1.2 Hamiltonian

It is important that you be introduced to the Hamiltonian. A Hamiltonian is an operator in quantum mechanics. It represents the sum of the kinetic and potential energies (i.e., the total energy) of all the particles in a given system. The Hamiltonian can be denoted by an  $H$ ,  $\langle H \rangle$ , or  $\hat{H}$ . When one measures the total energy of a system, the set of possible outcomes is the spectrum of the Hamiltonian. The Hamiltonian is named after William Hamilton. As you may surmise, there are multiple different ways of representing the Hamiltonian. In Equation 6.1, you see a simplified version of the Hamiltonian.

$$\hat{H} = \hat{T} + \hat{v}$$

**EQUATION 6.1** The Hamiltonian

The  $\hat{T}$  represents the kinetic energy, and the  $\hat{v}$  represents the potential energy. The  $T$  is a function of  $p$  (the momentum), and  $V$  is a function of  $q$  (the special coordinate). This simply states that the Hamiltonian is the sum of kinetic and potential energies. This particular formulation is rather simplistic and not overly helpful. It represents a one-dimensional system with one single particle of mass,  $m$ . This is a good place to start understanding the Hamiltonian. Equation 6.2 shows a better formulation.

$$H_{\text{operator}} = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + v(x)$$

**EQUATION 6.2** The Hamiltonian (Detailed)

Let us examine this formula to understand it. The simplest part is  $V(x)$ , which simply represents potential energy. The  $x$  is the coordinate in space. Also rather simple to understand is the  $m$ , which is the mass. The  $-\hbar^2$ , as you will recall from Chapter 3, is the reduced Planck constant, which is the Planck constant  $h$  ( $6.626 \times 10^{-34}$  J·s) /  $2\pi$ . The  $\partial$  symbol indicates a partial derivative. For some readers, this will be quite familiar. If you are not acquainted with derivatives and partial derivatives, you need not master those topics to continue with this book, but a brief conceptual explanation is in order. It should also be noted that there are many other ways of expressing this equation. You can see an alternative way at <https://support.dwavesys.com/hc/en-us/articles/360003684614-What-Is-the-Hamiltonian->.

With any function, the derivative of that function is essentially a measurement of the sensitivity of the function's output with respect to a change in the function's input. A classic example is calculating an object's position with respect to change in time, which provides the velocity. A partial derivative is a function of multiple variables, and the derivative is calculated with respect to one of those variables.

So, you should now have a general conceptual understanding of the Hamiltonian. Our previous discussion only concerned a single particle. In a system with multiple particles (as are most systems), the Hamiltonian of the system is just the sum of the individual Hamiltonians, as demonstrated in Equation 6.3.

$$\hat{H} = \sum_{n=1}^N \hat{T}_n + \hat{V}$$

### EQUATION 6.3 Hamiltonian (Another View)

Let us delve a bit deeper into the Hamiltonian. Any operator can be written in a matrix form. Now recall our discussion of linear algebra in Chapter 1. The eigenvalues of the Hamiltonian are the energy levels of the system. For the purposes of this book, it is not critical that you understand this at a deep working level, but you should begin to see intuitively why linear algebra is so important for quantum physics.

It also is interesting to note the relationship between the Hamiltonian and the Lagrangian. First, it is necessary to define the Lagrangian. Joseph-Louis Lagrange developed Lagrangian mechanics in 1788. It is essentially a reformulation of classical mechanics. Lagrangian mechanics uses the Lagrangian function of the coordinates, the time derivatives, and the times of the particles.

In Hamiltonian mechanics, the system is described by a set of canonical coordinates. Canonical coordinates are sets of coordinates on a phase space, which can describe a system at any given point in time. You can, in fact, derive the Hamiltonian from a Lagrangian. We won't delve into that topic in this chapter, but the interested reader can learn more about that process, and other details about the Hamiltonian, at the following sources:

<https://scholar.harvard.edu/files/david-morin/files/cmchap15.pdf>

<https://www.damtp.cam.ac.uk/user/tong/dynamics/four.pdf>

<https://authors.library.caltech.edu/89088/1/1.5047439.pdf>

### 6.1.3 Wave Function Collapse

In physics, a wave function is a mathematical description of the quantum state of a quantum system. It is usually represented by the Greek letter psi, either lowercase ( $\psi$ ) or uppercase ( $\Psi$ ). A wave function is a function of the degrees of freedom for the quantum system. In such a system, degrees of freedom indicate the number of independent parameters that describe the system's state. As one example, photons and electrons have a spin value, and that is a discrete degree of freedom for that particle.

A wave function is a superposition of possible states. More specifically, it is a superposition of eigenstates that collapses to a single eigenstate based on interaction with the environment. Chapter 1 discussed eigenvalues and eigenvectors. An eigenstate is basically what physicists call an eigenvector.

Wave functions can be added together and even multiplied (usually by complex numbers, which you studied in Chapter 2, "Complex Numbers") to form new wave functions. Recall the dot product we discussed in Chapter 1; the inner product is just another term for the dot product. This is also sometimes called the scalar product. Recall the inner/dot product is easily calculated, as shown in Equation 6.4.

$$\sum_{i=1}^n X_i Y_i$$

**EQUATION 6.4** Inner Product

The inner product of two wave functions is a measure of the overlap between the two wave functions' physical state.

This brings us to another important aspect of quantum mechanics: the Born rule. This postulate was formulated by Max Born and is sometimes called the Born law or the Born postulate. The postulate gives the probability that a measurement of a quantum system will produce a particular result. The simplest form of this is the probability of finding a particle at a given point. That general description will be sufficient for you to continue in this book; however, if you are interested in a deeper understanding, we will explore it now. The Born rule more specifically states that if some observable (position, momentum, etc.) corresponding to a self-adjoint operator  $A$  is measured in a system with a normalized wave function  $|\psi\rangle$ , then the result will be one of the eigenvalues of  $A$ . This should help you become more comfortable with the probabilistic nature of quantum physics.

For those readers not familiar with self-adjoint operators, a brief overview is provided. Recall from Chapter 1 that matrices are often used as operators. A self-adjoint operator on a finite complex vector space, with an inner product, is a linear map from the vector to itself that is its own adjoint. Note that it is a complex vector space. This brings us to Hermitian. Recall from Chapter 2 that Hermitian refers to a square matrix that is equal to its own conjugate transpose. Conjugate transpose means first taking the transpose of the matrix and then taking the complex conjugate of the matrix. Each linear operator on a complex Hilbert space also has an adjoint operator, sometimes called a Hermitian adjoint.

Self-adjoint operators have applications in fields such as functional analysis; however, in quantum mechanics, physical observables such as position, momentum, spin, and angular momentum are represented by self-adjoint operators on a Hilbert space.

This is also a good time to discuss Born's rule, which provides the probability that a measurement of a quantum system will yield a particular result. More specifically, the Born rule states that the probability density of finding a particular particle at a specific point is proportional to the square of the magnitude of the particle's wave function at that point. In more detail, the Born rule states that if an observable corresponding to a self-adjoint operator is measured in a system with a normalized wave function, the result will be one of the eigenvalues of that self-adjoint operator. There are more details to the Born rule, but this should provide you enough information. The interested reader can find more information at the following sources:

<https://www.math.ru.nl/~landsman/Born.pdf>

<https://www.quantamagazine.org/the-born-rule-has-been-derived-from-simple-physical-principles-20190213/>

Now let us return to the collapse of a wave function, which takes the superposition of possible eigenstates and collapses to a single eigenstate based on interaction with the environment. What is this interaction with the environment? This is one of the aspects of quantum physics that is often misunderstood by the general public. A common interaction with the environment is a measurement, which physicists often describe as an observation. This has led many to associate intelligent observation as a necessary condition for quantum physics, and thus all of reality. That is simply not an accurate depiction of what quantum physics teaches us.

What is termed an observation is actually an interaction with the environment. When a measurement is taken, that is an interaction that causes the wave function to collapse.

The fact that a measurement causes the wave function to collapse has substantial implications for quantum computing. When one measures a particle, one changes the state. As you will see in later chapters, particularly Chapter 8, “Quantum Architecture,” and Chapter 9, “Quantum Hardware,” this is something that quantum computing must account for.

The wave function can be expressed as a linear combination of the eigenstates (recall this is the physics term for eigenvectors you learned in Chapter 1) of an observable (position, momentum, spin, etc.). Using the bra-ket notation discussed previously, this means a wave function has a form such as you see in Equation 6.5.

$$|\psi\rangle = \sum_i c_i |\phi_i\rangle$$

**EQUATION 6.5** Wave Function

This is not as complex as it seems. The Greek letter psi ( $\psi$ ) denotes the wave function. The  $\Sigma$  symbol is a summation of what is after it. The  $\phi_i$  represents various possible quantum states. The  $i$  is to enumerate through those possible states, such as  $\phi_1$ ,  $\phi_2$ ,  $\phi_3$ , etc. The  $c_i$  values (i.e.,  $c_1$ ,  $c_2$ ,  $c_3$ , etc.) are probability coefficients. The letter  $c$  is frequently used to denote these because they are represented by complex numbers.

Recall from Chapter 1 that if two vectors are both orthogonal (i.e., perpendicular to each other) and have a unit length (length 1), the vectors are said to be orthonormal. The bra-ket  $\langle \phi_i | \phi_j \rangle$  forms an orthonormal eigenvector basis. This is often written as follows:

$$\langle \phi_i | \phi_j \rangle = \delta_{ij}$$

The symbol  $\delta$  is the Kronecker delta, which is a function of two variables. If the variables are equal, the function result is 1. If they are not equal, the function result is 0. This is usually defined as shown in Equation 6.6.

$$\delta_{ij} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}$$

**EQUATION 6.6** Kronecker Delta

Now let us discuss the actual process of the wave collapse. Remember that for any observable, the wave function is some linear combination of the eigenbasis before the collapse. When there is some environmental interaction, such as a measurement of the observable, the function collapses to just one of the base's eigenstates. This can be described in the following rather simple formula:

$$|\psi\rangle \rightarrow |\phi_i\rangle$$

But which state will it collapse to? That is the issue with quantum mechanics being probabilistic. We can say that it will collapse to a particular eigenstate  $|\phi_k\rangle$  with the Born probability (recall we discussed this earlier in this chapter)  $P_k = |c_k|^2$ . The value  $c_k$  is the probability amplitude for that specific eigenstate. After the measurement, all the other possible eigenstates that are not  $k$  have collapsed to 0 (put a bit more mathematically,  $c_i \neq k = 0$ ).

Measurement has been discussed as one type of interaction with the environment. One of the challenges for quantum computing is that this is not the only type of interaction. Particles interact with other particles. In fact, such things as cosmic rays can interact with quantum states of particles. This is one reason that decoherence is such a problem for quantum computing.

### 6.1.4 Schrödinger's Equation

The Schrödinger equation is quite important in quantum physics. It describes the wave function of a quantum system. This equation was published by Erwin Schrödinger in 1926 and resulted in his earning the Nobel Prize in Physics in 1933. First, let us examine the equation itself and ensure you have a general grasp of it; then we can discuss more of its implications. There are various ways to present this equation; we will first examine the time-dependent version. You can see this in Equation 6.7.

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle$$

#### EQUATION 6.7 Schrödinger Equation

Don't let this overwhelm you. All of the symbols used have already been discussed, and I will discuss them again here to refresh your memory.

Given that we are discussing a time-dependent version of the Schrödinger equation, it should be clear to most readers that the  $t$  represents time. Remember that the  $\partial$  symbol indicates a partial derivative. So, we can see in the denominator that there is a partial derivative with respect to time. The  $\hbar$ , you will recall from Chapter 3 and from earlier in this chapter, is the reduced Planck constant, which is the Planck constant  $h$  ( $6.626 \times 10^{-34} \text{ J} \cdot \text{s}$ ) /  $2\pi$ . The  $\psi$  symbol we saw earlier in this chapter. You may also recall that the symbol  $\hat{H}$  denotes the Hamiltonian operator, which is the total energy of the particles in a system.

Before we examine the implications of the Schrödinger equation, let us first examine another form of the equation. You can see this in Equation 6.8.

$$\frac{\partial^2 \psi}{\partial x^2} + \frac{8\pi^2 m}{h^2} (E - V)\psi = 0$$

**EQUATION 6.8** Schrödinger (Another Form)

You already know that the  $\partial$  symbol indicates a partial derivative. The 2 superposed above it means this is a second derivative (i.e., a derivative of a derivative). For those readers who don't have a solid calculus background, or who don't recall their calculus, a second derivative is actually common. A first derivative tells you the rate of change for some function. A second derivative tells you the rate of change for that rate of change that you found in the first derivative. Probably the most common example is acceleration. Speed is the change in position with respect to time. That is the first derivative. Acceleration is the change in speed, which is a second derivative. The  $\psi$  symbol denotes the wave function, which you should be getting quite familiar with by now. Another symbol you are familiar with is the  $h$ , for Planck's constant. Note in this form of the Schrödinger equation that it is the Planck constant, not the reduced Planck constant. The  $E$  is the kinetic energy, and the  $V$  is the potential energy of the system. The  $X$  is the position.

Remember that in the subatomic world, we have the issue of wave-particle duality. The Schrödinger equation allows us to calculate how the wave function changes in time.

## 6.2 Quantum Decoherence

Quantum decoherence is a very important topic and is, in fact, critical for quantum computing. Decoherence is directly related to the previous section on wave functions. Recall that a wave function is a mathematical representation of the state of a quantum system. As long as there exists a definite phase relation between the states, that system is coherent. Also, recall that interactions with the environment cause a wave function to collapse. If one could absolutely isolate a quantum system so that it had no interaction at all with any environment, it would maintain coherence indefinitely. However, only by interacting with the environment can it be measured; thus, data can be extracted.

What does it mean to have a definite phase relation between states? First, we must examine the concept of *phase space*, which is a concept from dynamical system theory. It is a space in which all the possible states of the system are represented. Each state corresponds to a unique point in the phase space. Each parameter of the system represents a degree of freedom. In turn, each degree of freedom is represented as an axis of a multidimensional space. If you have a one-dimensional system, it is a phase line. Two-dimensional systems are phase planes.

Two values,  $p$  and  $q$ , play an important role in phase space. In classical mechanics, the  $p$  is usually momentum and the  $q$  the position. Now, in quantum mechanics, this phase space is a Hilbert space. Thus, the  $p$  and  $q$  are Hermitian operators in that Hilbert space. While momentum and position are the most common observables, and are most often used to define phase space, there are other observables such as angular momentum and spin.

To refresh your memory, a Hermitian operator is also called a self-adjoint operator. Remember, we are dealing with matrices/vectors, so the operators are themselves matrices. Most operators in quantum mechanics are Hermitian. Hermitian operators have some specific properties. They always have real eigenvalues, but the eigenvectors or eigenfunctions might include complex numbers. A Hermitian operator can be “flipped” to the other side if it appears in an inner product—something like what you see here:

$$\langle f | A g \rangle = \langle A f | g \rangle$$

Hermitian operators’ eigenfunctions form a “complete set.” That term denotes that any function can be written as some linear combination of the eigenfunctions.

In general, if we are dealing with a non-relativistic model, the dimensionality of a system’s phase space is the number of degrees of freedom multiplied by the number of systems-free particles. Non-relativistic spacetime is conceptually rather simple. Relativistic spacetime uses  $n$  dimensional space and  $m$  dimensional time. Non-relativistic spacetime fuses that into a single continuum. Put another way, it is simply ignoring the effects of relativity. At the subatomic level that is perfectly reasonable, as relativistic effects are essentially irrelevant.

So, when the system interacts with the environment, each environmental degree of freedom contributes another dimension to the phase space of the system. Eventually, the system becomes decoupled. There is actually a formula for this called the Wigner quasi-probability distribution. This is sometimes called the Wigner-Ville distribution or just the Wigner function. The details may be a bit more than are needed in this book; however, the general outline is certainly something we can explore. Eugene Wigner first introduced this formula in 1932 to examine quantum modifications to classical mechanics. The purpose was to link the wave function we have studied in Schrödinger’s equation to a probability distribution in phase space.

Equation 6.9 shows the Wigner distribution.

$$W(x, p) \stackrel{\text{def}}{=} \frac{1}{\pi \hbar} \int_{-\infty}^{\infty} \psi^*(x+y) \psi(x-y) e^{2ipy/\hbar} dy$$

#### EQUATION 6.9 Wigner Distribution

By this point, you should not be daunted by complex-looking equations, and much of this equation use symbols you already know. But let us briefly examine them. Obviously, the  $W$  is the Wigner distribution.  $X$  is usually position and  $p$  momentum, but they could be any pair (frequency and time of a signal, etc.). Of course,  $\psi$  is the wave function, and  $\hbar$  is the reduced Planck constant. We discussed the  $\int$  symbol earlier in the book; it denotes integration. For our purposes, you don’t have to have a detailed knowledge of the Wigner distribution, nor do you have to be able to “do the math.” Rather, you just need a general understanding of what is happening.

In classical mechanics, a harmonic oscillator’s motion could be completely described by a point in the phase space with the particle position  $x$  and momentum  $p$ . In quantum physics, this is not the case. Recall from Chapter 3 our discussion of Heisenberg’s uncertainty principle. You cannot know with

precision the position and momentum simultaneously, but by measuring  $x$ ,  $p$ , or their linear combination on a set of identical quantum states, you can realize a probability density associated with these observables ( $x$  and  $p$ ). The Wigner function accomplishes this goal. Our goal is to understand decoherence. The Wigner distribution shows the decoupling process because it shows the probability of various states.

## 6.3 Quantum Electrodynamics

Quantum electrodynamics (QED) is a topic that may be considered too advanced for an introductory book. The goal is simply for you to acquire a generalized understanding of the topic, and I believe that is an achievable goal. QED is the relativistic quantum field theory that applies to electrodynamics. It is the first theory wherein quantum mechanics and relativity are in full agreement. QED provides a mathematical description of phenomena that involve electrically charged particles.

Let us begin by defining the quantum field theory (QFT). QFT combines classical field theory, special relativity, and quantum mechanics. At this point, you should have a general working knowledge of quantum mechanics. Therefore, we will turn our attention to classical field theory and special relativity, providing a brief description of each.

Classical field theory describes how one or more fields interact with matter, via field equations. An easy-to-understand example is with weather patterns. The wind velocity at a given time can be described by a vector. Each vector describes the direction and movement of the air at a particular point. The set of all such vectors in a particular area at a given point in time would be a vector field. Over time, we would expect these vectors to change. This is the essence of a classical field theory. Maxwell's equations of electromagnetic fields were among the first rigorous field theories.

Special relativity is something you are likely familiar with. In case you need a bit of a refresher, it essentially gives us two concepts. The first is that the laws of physics are invariant; there are no privileged reference points. Also, the speed of light in a vacuum is constant.

The development of quantum electrodynamics began with the study of the interaction between light and electrons. When this research began, the only field known was the electromagnetic field, so it was an obvious place to begin. The term *quantum electrodynamics* was posited by Paul Dirac in 1927 in his paper "The quantum theory of the emission and absorption of radiation."

Classical electromagnetism would describe the force between two electrons as being an electric field produced by each electron's position. The force itself can be calculated using Coulomb's law. However, quantum field theory visualizes the force between electrons arising from the exchange of virtual photons.

Quantum electrodynamics is the fundamental theory that describes the interaction of light and matter. To be a bit more mathematically robust, the charged particles that provide the source for the electromagnetic fields are described by relativistic equations of motion (more specifically, the Klein-Gordon equation for integer spin and the Dirac equation for a spin). Let us briefly examine these equations.

Keep in mind that for the purposes of this book, you need not become an expert in these equations. You only need a general understanding of what they do.

Klein-Gordon is a relativistic wave equation that is actually related to the Schrödinger equation, so it will at least look a bit familiar to you. Equation 6.10 provides the equation.

$$\frac{1}{c^2} \frac{\partial^2}{\partial t^2} \psi - \nabla^2 \psi + \frac{m^2 c^2}{\hbar^2} \psi = 0.$$

**EQUATION 6.10** Klein-Gordon Equation

Now, much of this you already know. Refreshing your memory a bit,  $\psi$  is the wave function,  $\hbar$  is the reduced Planck constant, and  $m$  is mass. We have also discussed second derivatives and partial differential equations previously in this book. The  $c$  is the velocity of light in centimeters per second. I think you can already see some connection between this and Einstein's famous  $E = mc^2$ . I have yet to explain one other symbol,  $\nabla$ . This one actually shows up frequently in quantum physics. This is the Laplace operator, sometimes called the Laplacian. It is sometimes denoted by  $\nabla \cdot \nabla$  and sometimes by  $\nabla^2$ . The definition of the Laplacian might seem a bit confusing to you. It is a second-order differential operator defined as the divergence of the gradient. In this case, the term *gradient* is a vector calculus term. It refers to a scalar-valued function  $f$  of several variables that is the vector field. The Laplacian of that vector field at some point is the vector whose components are partial derivatives of the function  $f$  at point  $p$ .

Hopefully, this general explanation did not leave you totally confused. Recall from the introduction that you need not master all of the mathematics presented in this chapter. Just make sure you understand the general idea. So what is that general idea? The Klein-Gordon equation is a relativistic wave function that describes the motion for the field, as it varies in time and space.

The Dirac equation for the spin is also a relativistic wave function. It describes particles such as electrons and quarks. It should be noted that electrons and quarks are the particles that constitute ordinary matter and are known as fermions. We will have much more to say about quarks in the section on quantum chromodynamics. The spin number describes how many symmetrical facets a particle has in one full rotation. Thus, a spin of  $1/2$  means the particle has to be rotated twice (i.e., 720 degrees) before it has the same configuration as when it started. Protons, neutrons, electrons, neutrinos, and quarks all have a spin of  $1/2$ , and that is enough for you to move forward with the rest of this book. However, for some readers, you not only want to see more of the math, but by this point in this text you have become accustomed to it. So, in the interest of not disappointing those readers, Equation 6.11 presents the Dirac equation as Paul Dirac originally proposed it.

$$\left( \beta mc^2 + c \sum_{n=1}^3 \alpha_n p_n \right) \psi(x,t) = i\hbar \frac{\partial \psi(x,t)}{\partial t}$$

**EQUATION 6.11** Dirac Equation

Again, you see the now-familiar partial differential symbol, the reduced Planck constant, and the wave function—all of which should be quite familiar to you by now. You also see  $mc^2$ , and I anticipate most readers realize this is mass and the velocity of light, just as it is in  $E = mc^2$ . In this equation, the  $x$  and  $t$  are space and time coordinates, respectively. The  $p$  values that are being summed ( $p_1$ ,  $p_2$ , and  $p_3$ ) are components of the momentum. The symbols  $\alpha$  and  $\beta$  are  $4 \times 4$  matrices. These are  $4 \times 4$  matrices because they have four complex components (i.e. using complex numbers). Such objects are referred to in physics as a *bispinor*.

After our rather extensive excursions into the math of QED, let us complete this section with a return to the essential facts of QED. Electrodynamics, as the name suggests, is concerned with electricity. However, quantum electrodynamics provides a relativistic explanation of how light and matter interact. It is used to understand the interactions among electrically charged elementary particles, at a fundamental level. It is a very important part of quantum physics.

## 6.4 Quantum Chromodynamics

Strictly speaking, one could study quantum computing without much knowledge of quantum chromodynamics (QCD). However, this underpins the very structure of matter; therefore, one should have a basic idea of the topic. QCD is the study of the strong interaction between quarks and gluons. Quarks are the particles that make up protons and neutrons (also called hadrons). At one time, it was believed that protons and neutrons were fundamental particles; however, it was discovered that they are in turn made up of quarks. The names for the quarks are frankly whimsical, and not too much attention should be paid to the meanings of the names. Quarks have properties such as electric charge, mass, spin, etc. Combining three quarks can product a proton or neutron. There are six types of quarks. The whimsical nature of nomenclature will become clear here. The types are referred to as “flavors,” and these flavors are up, down, strange, charm, bottom, and top. Figure 6.1 illustrates the families of quarks.

First Generation	Second Generation	Third Generation
 Up	 Charm	 Top
 Down	 Strange	 Bottom

FIGURE 6.1 Quarks

Evidence for the existence of quarks was first found in 1968 at the Stanford Linear Accelerator Center. Since that time, experiments have confirmed all six flavors of quarks. Therefore, these are not simply hypothetical constructs, but the actual building blocks of hadrons, and have been confirmed by multiple experiments over several decades. As one example, a proton is composed of two up quarks and one down quark. The gluons mediate the forces between the quarks, thus binding them together.

The next somewhat whimsical nomenclature comes with the concept of *color charge*. This has no relation at all to the frequency of light generating visible colors. The term *color*, along with the specific labels of red, green, and blue, is being used to identify the charge of a quark. However, this term has had far-reaching impact. That is why the study of the interaction between quarks and gluons is referred to as *chromodynamics*.

There are two main properties in QCD. The first is color confinement. This is a result of the force between two color charges as they are separated. Separating the quarks in a hadron will require more energy the further you separate them. If you do indeed have enough energy to completely separate the quarks, they actually spontaneously produce a quark-antiquark pair, and the original hadron becomes two hadrons.

The second property is a bit more complex. It is called asymptotic freedom. In simple terms, it means that the strength of the interactions between quarks and gluons reduces as the distance decreases. That might seem a bit counterintuitive. And as I stated, it is complex. The discoverers of this aspect of QCD—David Gross, Frank Wilczek, and David Politzer—received the 2004 Nobel Prize in Physics for their work.

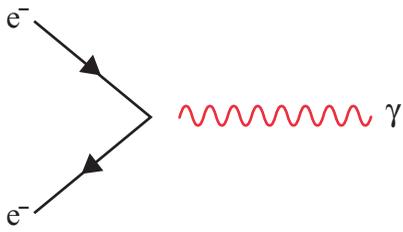
## 6.5 Feynman Diagram

For those readers who are a bit exhausted from all the mathematics presented in this chapter, there is help for you. Richard Feynman created the Feynman diagrams to provide a pictorial representation of the mathematical expressions used to describe the behavior of subatomic particles. This is a much easier way to at least capture the essence of what is occurring. Let us first look at the basic diagram symbols used and then see how they work together (see Table 6.1).

**TABLE 6.1** Feynman Diagram Symbols

Description	Symbol
A fermion (i.e., electron, positron, quark, etc.) is drawn as a straight line with an arrow pointing to the direction of the spin.	
An antifermion is drawn as a straight line with an arrow pointing to the direction of the spin, with the primary difference being the line over the f.	
A photon is drawn as a wavy line.	

Therefore, if you wish to draw two electrons with opposite spin, colliding and producing a photon, you can use Feynman diagrams without any math, as demonstrated in Figure 6.2.



**FIGURE 6.2** Feynman diagram of electrons colliding

This is just a very brief introduction to Feynman diagrams, but you will find these useful as you learn more about quantum interactions.

## 6.6 Summary

This chapter explored many concepts. It is really an extension of Chapter 3 and the application of some of the elements of Chapter 1. This is likely to be one of the more difficult chapters for many readers, and it is strongly suggested that you read it more than once. While many topics were explored, some are absolutely critical for your understanding of quantum computing. The bra-ket notation is used throughout quantum computing, so ensure you are quite comfortable with it. Hamiltonians also play a prominent role in quantum computing. Quantum decoherence is actually a substantial impediment to the progress of quantum computing. To fully understand decoherence, you need to understand the wave function and associated equations. Quantum electrodynamics and quantum chromodynamics were presented to help round out your basic introduction to quantum theory. However, those two topics are a bit less critical for you to move forward with quantum computing.

### Test Your Skills

#### REVIEW QUESTIONS

1. Why does the reduced Planck constant use  $2\pi$ ?
  - a.  $2\pi$  denotes the radius of the atom.
  - b.  $2\pi$  is 360 degrees in radians.
  - c.  $2\pi$  accounts for quantum fluctuations.
  - d.  $2\pi$  is a derivative of Einstein's universal constant.
2. In quantum mechanics, what does the Greek letter psi represent?
  - a. The Hamiltonian
  - b. The reduced Planck constant
  - c. The wave function
  - d. Superposition of states
3. What would be most helpful in determining the probability of finding a particle at a given point?
  - a. Born's rule
  - b. Hamiltonian
  - c. Reduced Planck constant
  - d. Wave function
4. Which of the following is the most accurate description of the wave function collapse?
  - a. The various possible quantum states coalesce into a single quantum state.
  - b. The probabilities coalesce to a single actuality based on an observer.

- c. The bra-ket  $\langle \phi_i | \phi_j \rangle$  forms an orthonormal eigenvector basis.
  - d. The superposition of possible eigenstates collapses to a single eigenstate based on interaction with the environment.
5. When using the Kronecker delta and inputting two eigenstates that are the same, what will be the output?
- a. The sum of the eigenstates
  - b. 1
  - c. The superposition of the eigenstates
  - d. 0
6. Schrödinger's equation is used to describe what?
- a. Superposition of eigenstates
  - b. Eigenstates
  - c. The wave function
  - d. The Hamiltonian operator
7. What equation is most closely related to the decoupling that occurs during decoherence?
- a. Hamiltonian
  - b. Schrödinger equation
  - c. Wigner function
  - d. Klein-Gordon
8. Which of the following is a wave function related to quantum electrodynamics that describes the motion for the field as it varies in time and space?
- a. Hamiltonian
  - b. Schrödinger equation
  - c. Wigner function
  - d. Klein-Gordon
9. What is a bispinor?
- a. A  $4 \times 4$  matrix with complex components
  - b. Superposition of two eigenstates
  - c. The product of the Dirac equation
  - d. The product of the Wigner function

## A

**abelian groups, 9, 282, 286**

**absolute zero, 185**

**abstract algebra, sets of numbers and, 6–8**

**abstraction, 297**

**addition**

of complex numbers, 35

identity element of, 8

of matrices, 11

of vectors, 47

**Adleman, Leonard, 213**

**AES standard, 232**

**aether, 61**

**affine transformations, 264**

**Ajtai, Milos, 249**

**Ajtai cryptographic primitive, 248**

**algebra**

books on, 4

of complex numbers, 34–37

defined, 4–5

**algebraic numbers, 56**

**algorithms. See also computational complexity; quantum algorithms**

asymmetric

Diffie-Hellman, 216–217, 231

ECDH (elliptic curve Diffie-Hellman),  
224–225

ECDSA (elliptic curve Digital Signature  
Algorithm), 225–226

Elgamal, 217–218

elliptic curves, 219–224, 232

MQV, 219

quantum computing impact on, 228–232

RSA, 213–216, 231

books on, 88

bubble sort, 91–92

code-based cryptography

McEliece cryptosystem, 279–280

Niederreiter cryptosystem, 280–281

coding theory, 95

as correct, 195

defined, 88, 195

efficacy of, 89–90

Euclidean, 92–93, 195–196

hash-based, 230, 232–233

Lamport signature, 277–278

Merkle-Damgaard construction, 275

requirements for, 274–275

SWIFFT, 275–277

lattice-based cryptography

GGH, 252–253

history of, 249

lattice reduction algorithms, 256–258

NTRU, 249–252

Peikert's Ring, 253–256

multivariate cryptography

HFE (Hidden Field Equations),  
266–268

Matsumoto-Imai algorithm, 264–266

MQDSS, 268–269

- SFLASH, 269–270
    - summary of, 270
  - qubits needed to crack, 181–182, 230–231
  - quick sort, 90–91
  - recursive, 197
  - symmetric, quantum computing impact on, 232
  - types of, 90
  - Algorithms, Fourth Edition (Sedgewick), 88**
  - Analytische Zahlentheorie (Bachmann), 89**
  - AND logic gate, 97**
  - AND operation, 96**
  - angle between vectors, 19**
  - antifermons, 134**
  - anyons, 187**
  - architecture. See computer architecture; quantum architecture**
  - area under curves, 72–73**
  - Argand, Jean Pierre, 41**
  - Argand diagrams, 41**
  - array data type, 293**
  - arrays**
    - lists as, 82
    - queues as, 83
  - assembly code, 100–101**
  - associativity**
    - defined, 5, 8
    - of sets, 28, 111
  - asymmetric cryptography, 95**
    - Diffie-Hellman, 216–217, 231
    - Elgamal, 217–218
    - elliptic curves, 219–224
      - ECDH (elliptic curve Diffie-Hellman), 224–225
      - ECDSA (elliptic curve Digital Signature Algorithm), 225–226
    - quantum computing impact on, 232
    - MQV, 219
    - quantum computing impact on, 228–232
    - RSA, 213–216
      - examples of, 215
      - factoring keys, 216
      - key generation process, 213–214
      - quantum computing impact on, 231
  - asymptotic analysis, 89**
  - asymptotic freedom, 134**
  - atomic orbitals, 65–68**
  - atomic structure, 65–68**
    - Bohr model, 65
    - orbitals, 65–68
    - Pauli exclusion principle, 68
  - azimuthal quantum number, 65**
- 
- B**
- B92 protocol, 149**
  - Babbage, Charles, 81**
  - Bachmann, Paul, 89**
  - balanced functions, 198**
  - basis vectors, 25, 50, 154–155**
  - BB84 protocol, 146–149**
  - Beijing-Shanghai link, 189**
  - Bell, John, 140**
  - Bell's inequality, 140–142**
  - Bennet, Charles, 146, 149**
  - Berger-Parker index, 117**
  - Bernstein-Vazirani algorithm, 201–202**
  - Big O notation, 89**
  - bigInt data type, 293**
  - bijjective, 158–159, 264**
  - binary Goppa codes, 280**
  - binary operations**
    - AND, 96
    - OR, 96
    - XOR, 96–97
  - binary trees, 88**
  - birthday problem, 277**
  - bispinors, 133**
  - bit flipping, 310**

- black bodies, 62
  - black body radiation, 62–63
  - Bloch sphere, 156–157
  - Bohm, David, 75, 140
  - Bohr, Neils, 144
  - Bohr model, 65
  - Boltzmann constant, 118
  - bool data type, 293
  - Born, Max, 126, 155
  - Born rule, 126, 155–156
  - Bose-Einstein condensate quantum computing, 179–180
  - bosons, 179–180
  - bounded queues, 84
  - BPP (bounded-error probabilistic polynomial time) problems, 201
  - BQP (bounded-error quantum polynomial time) problems, 201
  - Brahmagupta, 33
  - braid groups, 187
  - braid theory, 186–187
  - bra-ket notation, 74, 123, 155
  - Brassard, Gilles, 146
  - bubble sort algorithm, 91–92
- ## C
- 
- CA (certificate authority), 237–238
  - “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” (Einstein et al.), 139
  - canonical coordinates, 125
  - Cartesian coordinate system, 38–39, 69
  - Cauchy, Augustin-Louis, 69
  - Cauchy sequences, 69–70
  - Cayley, Arthur, 4
  - Cayley-Hamilton Theorem, 21
  - certificate authority (CA), 237–238
  - certificate revocation list (CRL), 237
  - Chaitin, Gregory, 57
  - Chaitin’s constant, 57
  - channels, 112, 113
  - characteristic function, 255
  - checksums, 95
  - chromodynamics, 134
  - Cirac, Ignacio, 179
  - circuits. *See* quantum circuits
  - circular polarization, 176
  - circular queues, 84
  - circularly linked lists, 87
  - CISC (complex instruction set) processors, 100
  - classes, 297
  - Closest Vector Problem (CVP), 230, 245, 248–249
  - closure, 8
  - code rate, 113
  - code-based cryptography, 230, 279
    - McEliece cryptosystem, 279–280
    - Niederreiter cryptosystem, 280–281
  - coding theory, 95
  - coefficients of quantum states, 74
  - coherence length, 176
  - collision entropy, 118
  - collision resistance, 275
  - color charge, 134
  - color confinement, 134
  - column matrices, 11
  - column vectors, 10
  - commands (in QASM), 319
  - comments, 302
  - commutativity
    - in abelian groups, 9, 282
    - defined, 5
    - matrix multiplication and, 13, 74
    - of multiplication, 74
    - of sets, 28, 111

**complement**

- in probability, 107
- of sets, 27, 110

**completeness, 69****complex conjugates**

- defined, 36, 156
- graphical representation, 44

**complex numbers**

- addition/subtraction, 35
- algebra of, 34–37
- complex conjugates, 36, 44
- defined, 6, 34
- distance between points, 41–43
- division, 36–37
- graphical representation, 38–44
- length of, 40–41
- multiplication, 35–36
- Pauli matrices
  - properties of, 52–56
  - representation of, 48–52
- polar coordinates, 47–48
- vector representation, 45–48

**complex plane, 41****complexity classes, 201****compression, 95****computational complexity**

- cyclomatic complexity, 93–94
- defined, 93
- Halstead metrics, 94

**computer architecture, 100–102****computer performance, 102****computer science**

- algorithms
  - books on, 88
  - bubble sort, 91–92
  - defined, 88
  - efficacy of, 89–90
  - Euclidean, 92–93
  - quick sort, 90–91
  - types of, 90

**binary operations**

- AND, 96
- OR, 96
- XOR, 96–97

**coding theory, 95****computational complexity**

- cyclomatic complexity, 93–94
- defined, 93
- Halstead metrics, 94

**computer architecture, 100–102****data structures**

- binary trees, 88
- defined, 81
- double-linked lists, 87
- linked lists, 86–87
- lists, 81–83
- queues, 83–84
- stacks, 85–86

**defined, 80–81****history of, 81****logic gates**

- AND, 97
- defined, 96
- electricity in, 99
- history of, 97
- NAND, 98–99
- NOR, 99
- OR, 97–98
- XOR, 98

**conditional entropy, 115****conditional probability, 108****conditional quantum entropy, 119****congruence in modulus operations, 204–205****conjugate transpose**

- defined, 49, 126, 167
- unitary matrices and, 159

**conjugations, 294****consistent histories interpretation, 145****constant functions, 198**

**continuous entropy, 115**  
**control processor plane, 188**  
**control structures, 295–296**  
**controlled gates, 163–164**  
**Copenhagen interpretation, 144**  
**counting numbers. See natural numbers**  
**CPU architecture, 101**  
**CRCs (cyclic redundancy checks), 95**  
**CRL (certificate revocation list), 237**  
**“Cryptanalysis of the Quadratic Zero-Testing of GGH” (Brakerski et al.), 253**  
**cryptography, 95. See also quantum-resistant cryptography**

- applications
  - digital certificates, 233–234
  - PKI (public key infrastructure), 237–238
  - SSH (Secure Shell), 240
  - SSL/TLS, 234–236
  - VPNs (virtual private networks), 239
- asymmetric
  - Diffie-Hellman, 216–217, 231
  - ECDH (elliptic curve Diffie-Hellman), 224–225
  - ECDSA (elliptic curve Digital Signature Algorithm), 225–226
  - Elgamal, 217–218
  - elliptic curves, 219–224, 232
  - MQV, 219
  - quantum computing impact on, 228–232
  - RSA, 213–216, 231
- symmetric, quantum computing impact on, 232

**curves, area under, 72–73**  
**CVP (Closest Vector Problem), 230, 245, 248–249**  
**cyclic groups, 9, 282, 286**  
**cyclic lattices, 20, 247**  
**cyclic redundancy checks (CRCs), 95**  
**cyclomatic complexity, 93–94**  
**cyclotomic polynomials, 254**

## D

---

***d* orbitals, 66–67**  
**data compression, 95**  
**data structures**

- binary trees, 88
- defined, 81
- double-linked lists, 87
- linked lists, 86–87
- lists, 81–83
- queues, 83–84
- stacks, 85–86

**data types in Q#293**  
**Davisson, Clinton, 64**  
**Davisson-Germer experiment, 64**  
**de Barros, Charles, 253**  
**de Broglie, Louis, 64**  
**de Moivre, Abraham, 208**  
**de Moivre number, 160, 208**  
**De Morgan’s laws, 28, 112**  
**decoherence, 129–131, 182–186**

- mechanics of, 182–184
- noise amplification, 185–186
- noise filtering, 186
- supercooling, 185

**decoherent histories interpretation, 145**  
**degrees, radian conversion, 48, 71**  
**degrees of freedom, 125, 156–157, 182–183**  
**dequeuing, 83**  
**derivatives, 124, 129**  
**Descartes, Rene, 69**  
**destinations, 112**  
**determinant**

- of matrices, 17–19, 247
- of Pauli matrices, 52–53

**determination, probability versus, 65**  
**Deutsch, David, 197**  
**Deutsch-Jozsa algorithm, 199–200, 308, 326**

Q# code for, 308–310  
 QASM code for, 326–327

**Deutsch's algorithm, 197–199**

**difference of sets, 26–27, 110**

**differential entropy, 115**

**differentiation, 73**

**Diffie, Whitfield, 216**

**Diffie-Hellman, 216–217, 231**

**digital certificates, 233–234**  
 PKI (public key infrastructure), 237–238  
 revoking, 237

**Digital Signature Algorithm, 225**

**Diophantus, 33**

**Dirac, Paul, 74, 131**

**Dirac equation, 132–133**

**Dirac notation, 74, 123, 155**

**discrete logarithm problem, 223–224, 231**

**disjoint sets, 110**

**distance between points for complex numbers, 41–43**

**distributed quantum computing, 190**

**distributivity**  
 defined, 5  
 of sets, 28, 112

**DiVencenzo, David, 177**

**diversity metrics in information theory, 116–118**

**division of complex numbers, 36–37**

**Dominance index, 117**

**dot products**  
 inner products and, 52, 69, 125–126, 166–167  
 in lattice-based mathematics, 247  
 of vectors, 19–20

**double complement of sets, 27, 110**

**double data type, 293**

**double-linked lists, 82, 87**

**double-slit experiment, 61–62**

**D-Wave architecture, 169–171**  
 quantum annealing, 169–170  
 SQUIDs, 170–171

## E

---

**E91 protocol, 151**

**Earnshaw, Samuel, 178**

**Earnshaw's theorem, 178**

**ECC (elliptic curve cryptography), 219–224**  
 ECDH (elliptic curve Diffie-Hellman), 224–225  
 ECDSA (elliptic curve Digital Signature Algorithm), 225–226  
 mathematics of, 281–284  
 super-singular elliptic curve cryptography, 230, 281, 285–288

**ECDH (elliptic curve Diffie-Hellman), 224–225**

**ECDLP (Elliptic Curve Discrete Logarithm Problem), 223–224**

**ECDSA (elliptic curve Digital Signature Algorithm), 225–226**

**efficacy of algorithms, 89–90**

**eigenfunctions of Hermitian operators, 130**

**eigenstates, 73, 125–128**

**eigenvalues**  
 defined, 20–23  
 of Hamiltonian, 125  
 of Pauli matrices, 53–54  
 in quantum states, 73

**eigenvectors**  
 defined, 20–23  
 of Pauli matrices, 54–56  
 in quantum states, 73

**Einstein, Albert, 63, 75, 76, 139**

**Eker, Martin, 231**

**Ekert, Artur, 151**

**electricity in logic gates, 99**

**electromagnetism, 131**

**electron spin quantum number, 65**

**electrons**  
 atomic orbitals, 65–68  
 Pauli exclusion principle, 68  
 for physical qubits, 177–178

**Elements (Euclid), 204**

**Elgamal, Taher, 217**

**Elgamal algorithm, 217–218****elliptic curve cryptography (ECC)**

ECDH (elliptic curve Diffie-Hellman), 224–225

ECDSA (elliptic curve Digital Signature Algorithm), 225–226

mathematics of, 219–224, 281–284

quantum computing impact on, 232

super-singular elliptic curve cryptography, 230, 281, 285–288

**elliptic curve Diffie-Hellman (ECDH), 224–225****elliptic curve Digital Signature Algorithm (ECDSA), 225–226****Elliptic Curve Discrete Logarithm Problem (ECDLP), 223–224****elliptical polarization, 176****encapsulation, 297****encryption. See cryptography****energy, Hamiltonian formulation, 124–125****ENIAC, 81****enqueueing, 83****entanglement, 75–76, 138–143, 151, 310****entropy**

in information theory, 113–116

defined, 114

diversity metrics, 116–118

formulas, 116

types of, 114–116

in quantum information theory, 119

in thermodynamics, 113

as uncertainty, 114

**environment, interference from, 183–184****EPR paradox, 75, 139–140, 142–143****equal matrices, 11****equations**

BB84 protocol

qubit states, 148

tensor product, 147, 148

Bell's inequality, 141

complex numbers

complex division, 37

complex multiplication, 37

division example answer, 37

multiplying by complex conjugate, 36

simplification, step 1, 37

simplification, step 2, 37

consistent histories, 145

cX gate matrix, 163

Dirac equation, 132

diversity metrics

collision entropy, 118

Gibbs entropy, 118

Hartley entropy, 117

Re'nyi entropy, 117

Shannon-Weaver index, 117

Shannon-Weaver index, form 2, 117

dot product, 19

entropy

conditional entropy, 115

conditional quantum entropy, 119

joint entropy, 115

limiting density of discrete points (LDDP), 115

list of, 116

mutual information, 115

Shannon entropy, 114

von Neuman entropy, 119

error correction, 320–321

$F_i$  function, state after, 199

Fourier transform, 71, 73, 160

Gram-Schmidt process

coefficients, 257

projection operator, 257

Hadamard transform, 150, 198, 200

state after, 199, 200

Hamiltonian

detailed, 124

- simplified, 124
- in systems, 125
- HFE (Hidden Field Equations)
  - decryption process, 267–268
  - encryption process, 267
- inner product, 126, 167
- inverse quantum Fourier transform, 208
- Ising XX coupling gate, 165
- Ising YY coupling gate, 165
- Ising ZZ coupling gate, 165
- Kirchoff's black body energy, 62
- Klein-Gordon equation, 132
- Kronecker delta, 51, 127
- lattices
  - cyclic, 247
  - definition of, 245
  - GGH algorithm, 252
  - NTRU key generation steps, 250–251
  - NTRU truncated polynomial ring, 250
- matrices
  - 3x2 matrix, 13
  - 3x3 matrix, 17
  - 3x3 matrix determinant, part 1, 17
  - 3x3 matrix determinant, part 2, 18
  - 3x3 matrix determinant, part 3, 18
  - 3x3 matrix determinant, part 4, 18
  - 5x5 matrix, 14
  - Hadamard, 159
  - multiplication, 13, 16
  - noncommutative matrices, 13, 74
  - removing rows and columns, 15
  - submatrix, 15
  - transposition, 13
  - unitary, 159
  - unitary conjugate transpose, 159
- Matsumoto-Imai algorithm
  - bijjective map, 265
  - encryption process, 265
  - inverted field, 265
  - isomorphism, 265
- MQDSS system, 268
- multivariate polynomial, 263
- nth cyclotomic polynomial, 254
- Pauli equation, 50
- Pauli matrices, 51
  - applying Kronecker delta, 51
  - compact form, 50
  - Kronecker delta with, 51
- phase shift gate, 161
- Planck's law, 63
- position and momentum, 73
- primitive roots of unity, 254
- probability
  - conditional probability, 108
  - independent event probability, 108
  - union of mutually exclusive events, 107
  - union of non-mutually exclusive events, 107
- quantum energy, 63
- quantum Fourier transform (QFT), 160, 161, 207
- roots of unity, 254
- SARG04 protocol
  - encoding, 149
  - qubit states, 150
- Schrödinger's equation, 128, 129
- SFLASH
  - exponent  $h$ , 269
  - public key, 269
  - univariate map, 269
- Shor's algorithm
  - initializing registers, 207
  - quantum function, 207
- Shor's error correction code, 175
- singlet state, 140
- spin matrices, 75
- univariate polynomial, 263

wave function, 127, 182  
 Wigner distribution, 130, 184  
**error detection and correction, 95. See also quantum error correction**  
**ether, 61**  
**Euclid, 204**  
**Euclidean algorithm, 92–93, 195–196**  
**Euclidean space, 69**  
**Euler, Leonhard, 56**  
**Euler's number, 56, 157**  
**Euler's totient, 213–214**  
**Everett, Hugh, 144–145**  
**excited states, 177**  
**expansion by minors, 17**  
**expression statements, 294**  
**extension fields, 263, 266–267**

## F

---

***f* orbitals, 67–68**  
**factoring**  
   integers, 213–216  
   RSA keys, 216  
**fail statements, 294**  
**fermions, 68, 132, 134, 180**  
**Feynman diagrams, 134–135**  
**FFT (fast Fourier transform), 275**  
**field theory, 131**  
**fields, 10, 262, 282**  
**FIFO (first in, first out), 83, 85**  
**filtering noise, 186**  
**finite fields, 282**  
**first derivatives, 129**  
**Fisher information, 115–116**  
**flux qubits, 169**  
**FOIL method, 35–36**  
**for loops, 295–296**  
**formulas. See equations**  
**Fourier transforms, 71–73, 160–161, 207–208**  
**Fredkin, Edward, 163**

**Fredkin gates, 163**  
**functions, 295**  
**functors, 306**

## G

---

**GaAs (gallium arsenide) quantum dots, 181**  
**Galois fields, 282**  
**Gap Closest Vector Problem (GapCVP), 249**  
**Gap Shortest Vector Problem (GapSVP), 248**  
**gauge bosons, 179–180**  
**Gauss, Carl, 204**  
**general number sieve, 213**  
**generators of groups, 9**  
**Germer, Lester, 64**  
**GGH algorithm, 252–253**  
**Gibbs entropy, 118**  
**Gini-Simpson index, 117**  
**gluons, 133–134**  
**Goldreich, Oded, 252**  
**Goldwasser, Shafi, 252**  
**Goppa, Valerii, 280**  
**Goppa codes, 280**  
**Gottesman, Daniel, 165–166**  
**Gottesman-Knill theorem, 165–166**  
**gradients, 132**  
**Gram-Schmidt process, 257**  
**graph theory, 94**  
**graphical representation**  
   of Cauchy sequence, 70  
   of complex numbers, 38–44  
**Grassman, Hermann, 4**  
**greatest common denominator, finding, 92–93**  
**Gross, David, 134**  
**groups**  
   abelian, 9, 282, 286  
   cyclic, 9, 282, 286  
   defined, 282

properties of, 8  
subgroups, 245–246

**Grover, Lov, 209**

**Grover's algorithm, 209–210, 232, 303–304, 322–323**

Q# code for, 304–307

QASM code for, 324–325

## H

---

**Hadamard, Jacques, 100**

**Hadamard matrices, 99–100, 159–160**

**Hadamard transform (gate), 99–100, 150, 159–161, 198–199**

**hadrons, 133, 180**

**Hahn, C.253**

**Halevi, Shai, 252**

**Halstead, Maurice, 94**

**Halstead metrics, 94**

**Hamilton, William, 124**

**Hamiltonian formulation, 124–125**

**Hamming codes, 279**

**handshake process (SSL/TLS), 235–236**

**hardware. See quantum hardware**

**Harris, Randy, 64**

**Hartley, Ralph, 117**

**Hartley entropy, 117**

**hash-based algorithms, 230, 232–233**

Lamport signature, 277–278

Merkle-Damgaard construction, 275

requirements for, 274–275

SWIFFT, 275–277

**head (in queues), 83**

**Heisenberg, Werner, 70, 123, 144**

**Heisenberg uncertainty principle, 70–73, 130–131**

**Hellman, Martin, 216**

**Hermite, Charles, 56**

**Hermitian matrices, 49, 126, 129–130, 167**

**Hermitian transpose, 156**

**Hertz, 71**

**Hertz, Heinrich, 62–63**

**heterogeneous lists, 82**

**HFE (Hidden Field Equations), 266–268**

**hidden variable hypothesis, 76, 140**

**Hilbert, David, 52, 56, 155**

**Hilbert spaces, 52, 68–70, 126, 129, 155**

**Hippasus, 33**

**history**

of computer science, 81

of information theory, 106

of irrational numbers, 33

of lattice-based cryptography, 249

of logic gates, 97

of natural numbers, 32–33

of negative numbers, 5–6, 33

of number systems, 32–34

of quantum physics

black body radiation, 62–63

nature of light, 61–62

photoelectric effect, 63–64

of rational numbers, 33

of zero, 33

**Hoffstein, Jeffery, 249**

**homeomorphism, 187**

**homogenous histories, 145**

**homogenous lists, 82**

**Hopf, Heinz, 157**

**Hopf fibration, 157**

**Huygens, Christian, 61**

**hyperspheres, 157**

## I

---

**idempotence, 257**

**identity elements, 8**

**identity matrices, 15–16**

**if statements, 295**

**imaginary numbers**

- on Cartesian coordinate system, 39
- defined, 6, 33–34
- symbol of, 34
- Imai, Hideki, 264**
- immutables, 294**
- “Incoherent and Coherent Eavesdropping in the 6-state protocol of Quantum Cryptography” (Bechmann-Pasquinnucc and Gisin), 151**
- independent event probability, 108**
- indicator function, 255**
- information source**
  - defined, 112
  - Shannon’s source coding theorem, 113
- information theory. See also probability**
  - diversity metrics, 116–118
  - entropy, 113–116
    - defined, 114
    - diversity metrics, 116–118
    - formulas, 116
    - types of, 114–116
  - history of, 106
  - importance of, 106
  - noisy channel theorem, 113
  - quantum information theory, 118–119
  - Shannon’s source coding theorem, 113
  - terminology, 112
- inheritance, 297**
- inhomogeneous histories, 145**
- injective, 158–159, 264**
- inner products, 52, 69, 125–126, 166–167**
- Instruction Set Architecture (ISA), 100**
- instructions (in computer architecture), 100**
- instructions (in QASM), 315–318**
- instructions per cycle, 102**
- int data type, 293**
- integers**
  - as abelian group, 9
  - as cyclic group, 9
  - defined, 5–6
  - factoring, 213–216
  - greatest common denominator, 92–93
  - as group, 8
  - as ring, 9
  - set of, 7
  - symbol of, 34
- integration, 72–73**
- Internet Protocol Security (IPsec), 239**
- interpretations**
  - Copenhagen, 144
  - decoherent histories, 145
  - many-worlds, 144–145
  - objective collapse theory, 145–146
  - purpose of, 143–144
  - summary of, 146
- intersection of sets, 26, 110**
- An Introduction to the Analysis of Algorithms, Second Edition (Sedgewick), 88***
- inverse images, 285**
- Inverse Simpson index, 117**
- invertibility, 8**
- involutory matrices, 51**
- ions for physical qubits, 178–179**
- IPsec (Internet Protocol Security), 239**
- irrational numbers**
  - defined, 6
  - history of, 33
  - symbol of, 34
- irreducible polynomials, 263**
- ISA (Instruction Set Architecture), 100**
- Ising, Ernst, 164**
- Ising gates, 164–165**
- isogeny, 285**
- isometric, 285**
- isomorphisms, 246, 264**
- iterations, 294**

**J**

**j-invariant of elliptic curves, 285**

**joint entropy, 115**

**joint probability, 108**

**Josephson, Brian, 169**

**Josephson junctions, 169**

**joules, 64**

**K**

**Kane, Bruce, 179**

**kelvin scale, 185**

**kernels, 285**

**key exchange. See QKE (quantum key exchange)**

**Kirchoff, Gustav, 62**

**Klein-Gordon equation, 132**

**Kline, Morris, 4**

**Knill, Emanuel, 165–166**

**Koblitz, Neil, 220, 282**

**Kronecker, Leopold, 51**

**Kronecker delta, 51, 127**

**L**

**Lagrange, Joseph-Louis, 125**

**Lagrangian formulation, 125**

**Lamport, Leslie, 277–278**

**Lamport signature algorithm, 277–278**

**Landau, Edmund, 89**

**Laplacian, 132**

**lattice reduction algorithms, 256–258**

**lattice-based cryptography**

algorithms

GGH, 252–253

history of, 249

lattice reduction, 256–258

NTRU, 249–252

Peikert's Ring, 253–256

problems used in, 230, 245, 248–249

**lattice-based mathematics**

CVP (Closest Vector Problem), 245, 248–249

definition of lattices, 245–246

SIS (Short Integer Solution), 248

SVP (Shortest Vector Problem), 245, 248

vectors in, 245–247

**lattices**

cyclic, 20, 247

defined, 245–246

**LDDP (limiting density of discrete points), 115**

**Lee, H.253**

**Leibniz, Gottfried, 81, 96**

**length**

of complex numbers, 40–41

of vectors, 16, 19, 68

**leptons, 180**

**LIFO (last in, first out), 85**

**light, nature of, 61–62**

**limiting density of discrete points (LDDP), 115**

**line coding, 95**

**linear algebra. See also matrices; sets; vectors**

books on, 4

defined, 3–4

importance of, 2

in quantum mechanics, 73–74, 123

**linear codes, 279**

**linear dependence, 25**

**linear equations, 3**

**linear functions. See linear transformations**

**linear independence, 25**

**linear mapping. See linear transformations**

**Linear Optical Quantum Computing (LOQC), 176**

**linear polarization, 175–176**

**linear transformations, 16**

**linearly dependent vectors, 245**

**linearly independent vectors, 245**

**linked lists, 82–83, 86–87**

**Liouville, Joseph, 56**

**lists, 81–83**

- double-linked lists, 87
- linked lists, 86–87
- queues, 83–84
- stacks, 85–86

**LLL (Lenstra-Lenstra-Lova'sz) lattice reduction algorithm, 256–258**

**logic gates. See also quantum logic gates**

- AND, 97
- defined, 96, 166
- electricity in, 99
- history of, 97
- NAND, 98–99
- NOR, 99
- OR, 97–98
- reversible, 158–159
- XOR, 98

**logical qubits. See quantum logic gates**

**LOQC (Linear Optical Quantum Computing), 176**

**Loss, Daniel, 177**

**Loss-DiVencenzo quantum computers, 177**

**lossless compression, 95**

**lossy compression, 95**

## M

**Mach-Zehnder interferometer, 176**

**magnetic quantum number, 65**

**manifolds, 187**

**many-worlds interpretation, 144–145**

**“A Mathematical Theory of Communication” (Shannon), 106**

***The Mathematical Theory of Communication* (Shannon and Weaver), 112**

***Mathematics for the Nonmathematician* (Kline), 4**

**Mathieu, Emile, 178**

**Mathieu function, 178–179**

**matrices. See also vectors**

- addition, 11
- cyclic lattices, 20
- defined, 4, 10
- determinant of, 17–19
- eigenvalues, 20–23
- Hadamard, 99–100, 159–160
- identity, 15–16
- involutory, 51
- multiplication, 11–13, 74
- notation, 10
- Pauli matrices
  - in controlled gates, 164
  - properties of, 52–56
  - representation of, 48–52, 161–162
- properties of, 14
- quantum state representation, 2
- submatrices, 14–15
- transformations of vectors, 20–21
- transposition, 13–14
- types of, 11
- unimodular, 20, 247

**Matsumoto, Tsutomu, 264**

**Matsumoto-Imai algorithm, 264–266**

**McCabe, Thomas, 93–94**

**McEliece, Robert, 230, 279**

**McEliece cryptosystem, 230, 279–280**

**measurement**

- in BB84 protocol, 148–149
- of particles, 127
- of qubits, 157
- symbol of, 168

**measurement plane, 188**

**measurement problem, 146**

**merge sort, quick sort versus, 90**

**Merkle, Ralph, 230, 275**

**Merkle-Damgaard construction, 230, 232–233, 275**

**mesons, 180**

**Micius satellite, 189–190**  
**microarchitecture, 101**  
**Microsoft Quantum Development Kit, 298–300**  
**Microsoft.Quantum.Canon namespace, 301**  
**Microsoft.Quantum.Convert namespace, 301**  
**Microsoft.Quantum.Intrinsic namespace, 305**  
**Microsoft.Quantum.Math namespace, 301**  
**Microsoft.Quantum.Measurement namespace, 301**  
**millennium prize problems, 93**  
**Miller, Victor, 220, 282**  
**min-entropy, 118**  
**modern algebra, sets of numbers and, 6–8**  
***Modern Physics, Second Edition* (Harris), 64**  
**modulus operations, 204–205**  
**momentum, 64, 70, 73**  
**Moody, Benjamin, 216**  
**“MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems” (IACR), 268**  
**MQDSS (Multivariate Quadratic Digital Signature Scheme), 268–269**  
**MQV, 219**  
**multiplication**  
   commutativity of, 74  
   of complex numbers, 35–36  
   identity element of, 8  
   of identity matrices, 15–16  
   of matrices, 11–13, 74  
   of vectors, 19–20, 23–25  
**multivariate cryptography, 230**  
   algorithms  
     HFE (Hidden Field Equations), 266–268  
     Matsumoto-Imai algorithm, 264–266  
     MQDSS, 268–269  
     SFLASH, 269–270  
     summary of, 270  
   mathematics of, 262–264

**multivariate polynomials, 263**  
**Multivariate Quadratic Digital Signature Scheme (MQDSS), 268–269**  
**mutual information, 115**

## N

---

**Nakashima, Akira, 97**  
**namespaces, 300–302**  
**NAND logic gate, 98–99**  
**natural numbers**  
   defined, 5, 32–33  
   history of, 32–33  
   set of, 7  
   symbol of, 34  
**negative numbers, history of, 5–6, 33**  
**NESSIE (New European Schemes for Signatures, Integrity and Encryption) project, 269**  
**networking. See quantum networking**  
**neutrons, 133**  
**Newton, Isaac, 61, 96**  
**Niederreiter, Harald, 280**  
**Niederreiter cryptosystem, 280–281**  
**NMRQC (nuclear magnetic resonance quantum computing), 179**  
**no-cloning theorem, 119**  
**noise**  
   amplification, 185–186  
   filtering, 186  
**noisy channel theorem, 113**  
**nonlocality, 139, 140**  
**non-relativistic spacetime, 130**  
**NOR logic gate, 99**  
**norm of vectors, 16, 20, 69, 245, 248**  
**normalizers, 165–166**  
**no-teleportation theory, 118–119**  
**NTRU (N-th degree Truncated polynomial Ring Units), 249–252**  
   key generation process, 250–251

polynomial rings, 249–250  
 standards, 251–252

**nuclear magnetic resonance quantum computing (NMRQC), 179**

**number systems**  
 history of, 32–34  
 properties of, 5  
 symbols of, 34

**numbers. See also complex numbers**  
 algebraic, 56  
 sets of, 6–8  
 transcendental, 56–57  
 types of, 5–6, 32–34  
 vectors as, 23

## O

---

**objective collapse theory, 145–146**

**object-oriented programming, 297**

**objects, 297**

**observations, 127**

**OCSP (Online Certificate Status Checking Protocol), 237**

**Omega notation, 89**

**operations. See also names of specific operations (addition, subtraction, etc.)**  
 in fields, 10  
 in groups, 8–9  
 on integer set, 7  
 on natural number set, 7  
 on real number set, 6–7  
 in rings, 9  
 on vectors, 24–25

**optimization problems, 170**

**OR logic gate, 97–98**

**OR operation, 96**

**oracles, 199, 304**

**orbital quantum number, 65**

**orbitals. See atomic orbitals**

**order**  
 in groups, 286  
 in sets, 27, 110

**orthogonal vectors, 20, 247**

**orthonormal vectors, 20, 127, 154–155**

**Overhauser effect, 181**

## P

---

***p* orbitals, 66**

**P vs. NP problem, 93**

**Pan, Jian-Wei, 189**

**parallelogram law, 47**

**parameters, 295**

**partial derivatives, 124**

**particles. See also wave-particle duality; names of types of particles (protons, neutrons, etc.)**  
 defined, 64  
 entanglement, 75–76, 138–143  
 Feynman diagrams, 134–135  
 light as, 61–62  
 measurement, 127  
 position versus momentum, 70  
 quasiparticles, 187  
 types of, 179–180  
 wavelengths of, 64

**Patarin, Jacques, 266**

**Paul, Wolfgang, 178**

**Paul ion traps, 178–179**

**Pauli, Wolfgang, 50, 68**

**pauli data type, 293**

**Pauli equation, 50**

**Pauli exclusion principle, 68**

**Pauli gates, 161–162**

**Pauli groups, 165–166**

**Pauli matrices**  
 in controlled gates, 164  
 properties of, 52–56  
 representation of, 48–52, 161–162

**Peano, Giuseppe, 4**

**Peikert's Ring, 253–256**

**period-finding function in Shor's algorithm, 206–209**

**phase shift gates, 161**

**phase space, 129–130**

**photoelectric effect, 63–64**

**photons**

defined, 63

entanglement, 151

in Feynman diagrams, 134

measurement in BB84 protocol, 148–149

in noise filtering, 186

for physical qubits, 175–177

**physical qubits, 174–182**

Bose-Einstein condensate quantum computing, 179–180

correlation with logical qubits, 175

electrons for, 177–178

GaAs quantum dots, 181

ions for, 178–179

NMRQC, 179

number needed, 181–182, 230–231

photons for, 175–177

summary of, 181

**physics. See also quantum physics**

black body radiation, 62–63

entropy in, 113

nature of light, 61–62

photoelectric effect, 63–64

**Pipher, Jill, 249**

**pivot points in quick sorts, 90–91**

**PKCS (Public-Key Cryptography Standards), 238**

**PKI (public key infrastructure), 237–238**

**PKIX (Public-Key Infrastructure X.509), 238**

**Planck, Max, 62–63, 64**

**Planck's constant, 63, 64, 71, 124**

**Podolsky, Boris, 75, 139**

**points, distance between, 41–43**

**polar coordinates, 47–48**

**polarization of photons, 175–176**

**Politzer, David, 134**

**polymorphism, 297**

**polynomial rings, 249–250, 253–254, 276**

**polynomial time, 212–213**

**polynomials, 263, 276**

**pop (in stacks), 85**

**position, momentum versus, 70, 73**

**post-quantum cryptography. See quantum-resistant cryptography**

**power sets, 27–28, 111**

**powers in cyclic groups, 9**

**PP (probabilistically polynomial) problems, 201**

**primitive elements of groups, 9**

**primitive roots of unity, 254**

**principal quantum number, 65**

**printer buffers, 87**

**printer queues, 84**

**probabilistically polynomial (PP) problems, 201**

**probability**

in atomic orbitals, 65–68

in Bell's inequality, 142

defined, 107

determination versus, 65

Heisenberg uncertainty principle, 70–73

importance of, 106–107

in qubits, 155–157

rules of, 107–108

in wave function collapse, 128

**programming languages**

concepts in

comments, 302

control structures, 295–296

functions, 295

object-oriented programming, 297

statements, 293–294

variables, 292–293

**Q#**

- bit flipping, 310
- data types, 293
- Deutsch-Jozsa algorithm code, 308–310
- Grover’s algorithm code, 304–307
- program structure, 294–295
- statement types, 294
- with Visual Studio Code, 298–303

**QASM (Quantum Assembly Language), 314–315**

- commands, 319
- Deutsch-Jozsa algorithm code, 326–327
- error correction, 320–322
- Grover’s algorithm code, 324–325
- instructions, 315–318
- project creation, 319–320

**projection operators, 257****properties**

- of groups, 8
- of matrices, 14
- of number systems, 5
- of Pauli matrices, 52–56
- of sets, 28, 111–112
- of vector spaces, 246

**protons, 133****public key infrastructure (PKI), 237–238****Public-Key Cryptography Standards (PKCS), 238****Public-Key Infrastructure X.509 (PKIX), 238****push (in stacks), 85****Pythagoras, 33****Q****Q# programming language**

- bit flipping, 310
- data types, 293
- Deutsch-Jozsa algorithm code, 308–310
- Grover’s algorithm code, 304–307
- program structure, 294–295

statement types, 294

with Visual Studio Code, 298–303

**QASM (Quantum Assembly Language), 314–315**

- commands, 319
- Deutsch-Jozsa algorithm code, 326–327
- error correction, 320–322
- Grover’s algorithm code, 324–325
- instructions, 315–318
- project creation, 319–320

**QCD (quantum chromodynamics), 133–134****QDK (Quantum Development Kit), 298–300****QED (quantum electrodynamics), 131–133****QFT (quantum field theory), 131****QFT (quantum Fourier transform), 160–161, 207–208****QKE (quantum key exchange)**

- B92 protocol, 149
- BB84 protocol, 146–149
- E91 protocol, 151
- implementations, 151
- purpose of, 146
- resources for information, 151
- SARG04 protocol, 149–150
- six-state protocol, 151
- Tokyo QKD, 188

**quanta, 62–63****quantum algorithms**

- Bernstein-Vazirani algorithm, 201–202
- defined, 197
- Deutsch-Jozsa algorithm, 199–200, 308, 326
  - Q# code for, 308–310
  - QASM code for, 326–327
- Deutsch’s algorithm, 197–199
- Grover’s algorithm, 209–210, 303–304, 322–323
  - Q# code for, 304–307
  - QASM code for, 324–325
- Shor’s algorithm, 203–209

- example of, 205–206
- modulus operations in, 204–205
- quantum period-finding function in, 206–209

- Simon's algorithm, 202–203

### **quantum annealing, 169–170**

### **quantum architecture**

- D-Wave, 169–171
  - quantum annealing, 169–170
  - SQUIDs, 170–171
- quantum circuits, 167–169
  - diagrams, 168–169
  - quantum gate notation, 167–168
  - reversible, 167
- quantum logic gates
  - controlled, 163–164
  - Fredkin, 163
  - Gottesman-Knill theorem, 165–166
  - Hadamard, 159–161
  - Ising, 164–165
  - notation, 167–168
  - operation of, 166–167
  - Pauli, 161–162
  - phase shift, 161
  - reversible, 158–159
  - swap, 162–163
  - Toffoli, 163

### **qubits**

- defined, 154
- mathematics of, 154–158
- measurement, 157
- probabilities, 155–157
- qubit states, 154–155

### **Quantum Assembly Language (QASM), 314–315**

- commands, 319
- Deutsch-Jozsa algorithm code, 326–327
- error correction, 320–322
- Grover's algorithm code, 324–325

- instructions, 315–318
- project creation, 319–320

### **quantum bits. See qubits**

### **quantum chromodynamics (QCD), 133–134**

### **quantum circuits, 167–169**

- diagrams, 168–169
- quantum gate notation, 167–168
- reversible, 167

### **quantum data plane, 187**

### **Quantum Development Kit (QDK), 298–300**

### **quantum dots, 177, 181**

### **quantum electrodynamics (QED), 131–133**

### **quantum error correction**

- decoherence and, 184
- in QASM, 320–322

### **quantum field theory (QFT), 131**

### **quantum Fourier transform (QFT), 160–161, 207–208**

### **quantum hardware**

- decoherence mitigation, 182–186
  - mechanics of decoherence, 182–184
  - noise amplification, 185–186
  - noise filtering, 186
  - supercooling, 185
- quantum computer components, 187–188
- quantum networking, 188–190
  - Beijing-Shanghai link, 189
  - distributed quantum computing, 190
  - Micius satellite, 189–190
  - Tokyo QKD, 188

### **qubits**

- Bose-Einstein condensate quantum computing, 179–180
- correlation of physical and logical qubits, 175
- electrons for, 177–178
- GaAs quantum dots, 181
- ions for, 178–179
- NMRQC, 179

number needed, 181–182, 230–231

photons for, 175–177

physical realization of, 174–182

summary of, 181

size of computers, 184

topological quantum computing, 186–187

### **quantum information theory, 118–119**

entropy in, 119

qubits, 118–119

resources for information, 119

### **quantum key exchange (QKE)**

B92 protocol, 149

BB84 protocol, 146–149

E91 protocol, 151

implementations, 151

purpose of, 146

resources for information, 151

SARG04 protocol, 149–150

six-state protocol, 151

Tokyo QKD, 188

### **quantum logic gates**

controlled, 163–164

correlation of physical and logical qubits, 175

Fredkin, 163

Gottesman-Knill theorem, 165–166

Hadamard, 99–100, 159–161

Ising, 164–165

matrix representation, 2

notation, 167–168

operation of, 166–167

Pauli, 161–162

phase shift, 161

in QASM, 316

reversible, 158–159

swap, 162–163

Toffoli, 163

### **quantum mechanics. See quantum physics**

### **quantum networking, 188–190**

Beijing-Shanghai link, 189

distributed quantum computing, 190

Micius satellite, 189–190

Tokyo QKD, 188

### **quantum oracles, 304**

### **quantum period-finding function in Shor's algorithm, 206–209**

### **quantum physics**

atomic structure, 65–68

Bohr model, 65

orbitals, 65–68

Pauli exclusion principle, 68

books on, 64

bra-ket notation, 74, 123

decoherence, 129–131

entanglement, 75–76, 138–143

Feynman diagrams, 134–135

Fourier transforms, 71–73

Hamiltonian formulation, 124–125

Heisenberg uncertainty principle, 70–73

Hilbert spaces, 68–70

history of

black body radiation, 62–63

nature of light, 61–62

photoelectric effect, 63–64

interpretations

Copenhagen, 144

decoherent histories, 145

many-worlds, 144–145

objective collapse theory, 145–146

purpose of, 143–144

summary of, 146

QCD (quantum chromodynamics), 133–134

QED (quantum electrodynamics), 131–133

QKE (quantum key exchange)

B92 protocol, 149

BB84 protocol, 146–149

E91 protocol, 151

implementations, 151

purpose of, 146

- resources for information, 151
- SARG04 protocol, 149–150
- six-state protocol, 151
- quantum states, 73–75
- resources for information, 123
- Schrödinger’s equation, 128–129
- wave function collapse, 125–128
- quantum states**
  - coefficients of, 74
  - vector representation, 2, 46, 73–75, 123
- quantum theory**
  - defined, 122
  - QCD (quantum chromodynamics), 133–134
  - QED (quantum electrodynamics), 131–133
- “The quantum theory of the emission and absorption of radiation” (Dirac), 131**
- quantum wells, 177**
- quantum wires, 177**
- quantum-resistant cryptography**
  - code-based cryptography, 230, 279
    - McEliece cryptosystem, 279–280
    - Niederreiter cryptosystem, 280–281
  - hash-based algorithms, 230, 232–233
    - Lamport signature, 277–278
    - Merkle-Damgaard construction, 275
    - requirements for, 274–275
    - SWIFFT, 275–277
  - lattice-based cryptography
    - GGH, 252–253
    - history of, 249
    - lattice reduction algorithms, 256–258
    - NTRU, 249–252
    - Peikert’s Ring, 253–256
    - problems used in, 230, 245, 248–249
  - multivariate cryptography, 230
    - HFE (Hidden Field Equations), 266–268
    - mathematics of, 262–264
    - Matsumoto-Imai algorithm, 264–266
    - MQDSS, 268–269
    - SFLASH, 269–270
    - summary of algorithms, 270
  - standards, 229
  - super-singular elliptic curve cryptography, 230, 281, 285–288
  - symmetric cryptography, 232
- quantum-safe cryptography. See quantum-resistant cryptography**
- “Quantum-Theoretical Re-interpretation of Kinematic and Mechanical Relations” (Heisenberg), 123**
- quarks, 133–134**
- quasiparticles, 187**
- qubit allocations, 294**
- qubit data type, 293**
- qubit states**
  - BB84 protocol, 148–149
  - SARG04 protocol, 150
  - six-state protocol, 151
  - vector representation, 154–155
- qubits**
  - correlation of physical and logical qubits, 175
  - defined, 118–119, 154
  - flux, 169
  - logic gates. *See* quantum logic gates
  - mathematics of, 154–158
    - measurement, 157
    - probabilities, 155–157
    - qubit states, 154–155
  - no-cloning theorem, 119
  - no-teleportation theory, 118–119
  - physical realization of, 174–182
    - Bose-Einstein condensate quantum computing, 179–180
    - electrons for, 177–178
    - GaAs quantum dots, 181
    - ions for, 178–179
    - NMRQC, 179
    - number needed, 181–182, 230–231

photons for, 175–177

summary of, 181

SQUIDS, 170–171

supercooling, 185

**queues, 83–84**

**quick sort algorithm, 90–91**

## R

---

**RA (registration authority), 238**

**radians, degree conversion, 48, 71**

**range data type, 293**

**rational numbers**

defined, 6

as field, 10

history of, 33

symbol of, 34

**real numbers**

on Cartesian coordinate system, 38

defined, 6, 33–34

in Euclidean space, 69

set of, 6–7

symbol of, 34

**receivers, 112**

**recursive algorithms, 90, 197**

**reduced Planck constant, 71**

**registration authority (RA), 238**

**relativistic spacetime, 130**

**Re'nyi entropy, 117–118**

**repeat statements, 294**

**result data type, 293**

**return statements, 294**

**reversible logic gates, 158–159**

**reversible quantum circuits, 167**

**revoking digital certificates, 237**

**Rijindael algorithm, 232**

**Ring Learning With Errors (RLWE), 253–254**

**rings**

defined, 9, 249, 276

polynomial, 249–250, 253–254, 276

**RISC (reduced instruction set) processors, 100**

**Rivest, Ron, 213**

**RLWE (Ring Learning With Errors), 253–254**

**roots of unity, 160, 208, 254**

**Rosen, Nathan, 75, 139**

**row matrices, 11**

**row vectors, 10**

**RSA, 213–216**

examples of, 215

factoring keys, 216

key generation process, 213–214

quantum computing impact on, 231

qubits needed to crack, 181–182, 230–231

**Rydberg, Johannes, 177**

**Rydberg formula, 177–178**

**Rydberg states, 177**

## S

---

**s orbitals, 65–66**

**sampling problems, 170**

**SARG04 protocol, 149–150**

**scalar products. See inner products**

**scalar values, 17**

**scalars**

defined, 11

eigenvalues, 20–23

matrix multiplication by, 11

vector multiplication by, 23–25

in vector space, 16

**scaling vectors, 23–25**

**Schechter, L. M. 253**

**Schläfli, Ludwig, 69**

**Schrödinger, Erwin, 128, 143**

**Schrödinger's cat, 144**

**Schrödinger's equation, 128–129**

**second derivatives, 129**

**Secure Shell (SSH), 240**

**Secure Socket Layer (SSL), 234–236**

**Sedgewick, Robert, 88**

**self-adjoint operators, 126, 129–130, 156**

**set theory, 25–28, 108–112**

**sets**

defined, 25, 108

lists as, 82

notation, 25–26, 109

order in, 27, 110

power sets, 27–28

properties of, 28, 111–112

relationships, 26–27, 109–110

subsets, 27, 110–111

**sets of numbers, 6–8**

fields, 10

groups

abelian, 9

cyclic, 9

properties of, 8

rings, 9

**SFLASH, 269–270**

**Shamir, Adi, 213**

**Shannon, Claude, 106, 112, 116**

**Shannon diversity index, 116–117**

**Shannon entropy, 114**

**Shannon's source coding theorem, 113**

**Shannon-Weaver index, 116–117**

**shells, 65**

**Shor, Peter, 88, 203, 216**

**Shor's algorithm, 88, 203–209**

Diffie-Hellman and, 217

example of, 205–206

modulus operations in, 204–205

quantum computing impact on, 231

quantum period-finding function in, 206–209

RSA and, 216

**Shor's error correction code, 175**

**Short Integer Solution (SIS), 248**

**Shortest Vector Problem (SVP), 230, 245, 248**

**SIDH (supersingular isogeny Diffie-Hellman), 285–288**

**signal function, 255**

**Silverman, Joseph, 249**

**Simon's algorithm, 202–203**

**Simpson index, 117**

**singlet state, 139**

**SIS (Short Integer Solution), 248**

**six-state protocol (SSP), 151**

**Sliding Windowed Infinite Fast Fourier Transform (SWIFFT), 275–277**

**sorting algorithms**

bubble sort, 91–92

quick sort, 90–91

types of, 90

**special relativity, 131**

**spin number, 132**

**square matrices**

defined, 11

determinant of, 17

Hermitian, 49

unitary, 49

**square roots**

imaginary numbers and, 6, 33–34

of swap gates, 163

**SQUIDs (superconducting qubits), 170–171**

**SSH (Secure Shell), 240**

**SSL (Secure Socket Layer), 234–236**

**SSP (six-state protocol), 151**

**stacks, 85–86**

**state space, 68**

**state vectors, 68**

**statements**

defined, 293–294

in Q#294

**Stewart, Balfour, 62**

**string data type, 293**

**subgroups, 245–246**

**submatrices, 14–15**  
**subsets, 27, 110–111**  
**subspaces, 25**  
**subtraction of complex numbers, 35**  
**superconducting qubits (SQUIDs), 170–171**  
**supercooling, 185**  
**super-singular elliptic curve cryptography, 230, 281, 285–288**  
**surjective, 158–159, 264, 285**  
**SVP (Shortest Vector Problem), 230, 245, 248**  
**swap gates, 162–163**  
**SWIFFT (Sliding Windowed Infinite Fast Fourier Transform), 275–277**  
**symbols**  
 of measurement, 168  
 of number systems, 34  
 of Pauli matrices, 50–51  
 of quantum gates, 167–168  
**symmetric cryptography, 95**  
 quantum computing impact on, 232

## T

---

**tail (in queues), 83**  
**teleportation, 118–119**  
**temperatures in quantum computing, 185**  
**tensor products**  
 in BB84 protocol, 147–148  
 defined, 20  
 in lattice-based mathematics, 247  
***Theory of Extension (Grassman), 4***  
**Theta notation, 89**  
**time-bin encoding, 176**  
**TLS (Transport Layer Security), 234–236**  
**Toffoli, Tommaso, 163**  
**Toffoli gates, 163**  
**Tokyo QKD, 188**  
**topological quantum computing, 186–187**  
**torsion subgroups, 286**  
**transcendental numbers, 56–57**

**transformations of vectors, 20–21**  
**transmitters, 112**  
**transmons, 161**  
**Transport Layer Security (TLS), 234–236**  
**transposition**  
 conjugate transpose, 49  
 of matrices, 13–14  
**transverse waves, 175–176**  
**trapdoor functions, 263**  
**tuple data type, 293**

## U

---

**unbounded queues, 84**  
**uncertainty**  
 entropy as, 114  
 Heisenberg uncertainty principle, 70–73, 130–131  
**unimodular matrices, 20, 247**  
**union**  
 in probability, 107  
 of sets, 26, 109  
**unit data type, 293**  
**unit vectors, 16, 20, 68**  
**unitary mapping, 166**  
**unitary matrices**  
 conjugate transpose and, 159  
 defined, 49  
**univariate polynomials, 263**  
**universal gates, 99**  
**using statements, 296**

## V

---

**variable declaration statements, 294**  
**variables, 292–293**  
**vector spaces**  
 defined, 16, 24–25  
 Hilbert spaces, 52, 68–70  
 in lattice-based mathematics, 246–247

linear dependence/independence, 25  
 properties of, 246  
 subspaces, 25  
 tensor products, 147–148

## vectors

addition, 47  
 angle between, 19  
 basis, 25, 50, 154–155  
 complex number representation, 45–48  
 CVP (Closest Vector Problem), 230, 245, 248–249  
 defined, 10, 19  
 dot product of, 19–20  
 eigenvectors, 20–23  
 in lattice-based mathematics, 245–247  
 length of, 16, 19, 68  
 as numbers, 23  
 orthogonal, 20  
 orthonormal, 20, 127, 154–155  
 polar coordinates, 47–48  
 quantum state representation, 2, 46, 73–75, 123  
 scalar multiplication of, 23–25  
 SVP (Shortest Vector Problem), 230, 245, 248  
 transformations of, 20–21

**Visual Studio Code, 298–303**

**von Neuman entropy, 119**

**VPNs (virtual private networks), 239**

## W

---

**Walsh-Hadamard transformation. See Hadamard transform (gate)**

**Washington, Lawrence, 220**

**wavelengths of particles, 64**

**wave-particle duality, 62, 63–64**

## waves

Dirac equation, 132–133  
 Fourier transforms, 71–73  
 Klein-Gordon equation, 132  
 light as, 61–62

quantum decoherence, 129–131  
 Schrödinger's equation, 128–129  
 wave function, 182  
 wave function collapse, 125–128

**Weaver, Warren, 112**

**Wessel, Caspar, 41**

**Wigner, Eugene, 130**

**Wigner distribution, 130–131, 183–184**

**Wilczek, Frank, 134**

**world lines, 187**

## X

---

**X.509 digital certificates, 233–234**

**XOR logic gate, 98**

**XOR operation, 96–97**

## Y

---

**Ylonen, Tatu, 240**

**Young, Thomas, 61**

## Z

---

**zero, history of, 33**

**zero matrices, 11**

**Zollar, Peter, 179**

**z-plane, 41**