



QUANTUM COMPUTING FUNDAMENTALS

From Basic Linear Algebra to Quantum Programming



DR. CHUCK EASTTOM

Quantum Computing Fundamentals

Quantum Computing Fundamentals

Table of Contents

Cover

Half Title

Title

Copyright Page

Credits

Dedication

Table of Contents

Preface

Part I: Preparatory Material

Chapter 1: Introduction to Essential Linear Algebra

1.1 What Is Linear Algebra?

1.2 Some Basic Algebra

1.2.1 Groups, Rings, and Fields

1.3 Matrix Math

1.3.1 Matrix Addition and Multiplication

1.3.2 Matrix Transposition

1.3.3 Submatrix

1.3.4 Identity Matrix

1.3.5 Deeper Into the Matrix

1.4 Vectors and Vector Spaces

1.5 Set Theory

1.6 Summary

Test Your Skills

Chapter 2: Complex Numbers

Table of Contents

2.1 What Are Complex Numbers?

2.2 Algebra of Complex Numbers

2.3 Complex Numbers Graphically

2.4 Vector Representations of Complex Numbers

2.5 Pauli Matrices

2.5.1 Algebraic Properties of Pauli Matrices

2.6 Transcendental Numbers

2.7 Summary

Test Your Skills

Chapter 3: Basic Physics for Quantum Computing

3.1 The Journey to Quantum

3.2 Quantum Physics Essentials

3.2.1 Basic Atomic Structure

3.2.2 Hilbert Spaces

3.2.3 Uncertainty

3.2.4 Quantum States

3.2.5 Entanglement

3.3 Summary

Test Your Skills

Chapter 4: Fundamental Computer Science for Quantum Computing

4.1 Data Structures

4.1.1 List

4.1.2 Binary Tree

4.2 Algorithms

4.2.1 Sorting Algorithms

4.3 Computational Complexity

4.3.1 Cyclomatic Complexity

4.3.2 Halstead Metrics

4.4 Coding Theory

4.5 Logic Gates

4.5.1 AND

Table of Contents

4.5.2 OR

4.5.3 XOR

4.5.4 Application of Logic Gates

4.6 Computer Architecture

4.7 Summary

Test Your Skills

Chapter 5: Basic Information Theory

5.1 Basic Probability

5.1.1 Basic Probability Rules

5.2 Set Theory

5.3 Information Theory

5.3.1 Theorem 1: Shannons Source Coding Theorem

5.3.2 Theorem 2: Noisy Channel Theorem

5.3.3 Information Entropy

5.3.4 Information Diversity

5.4 Quantum Information

5.5 Summary

Test Your Skills

Part II: Basic Quantum Computing

Chapter 6: Basic Quantum Theory

6.1 Further with Quantum Mechanics

6.1.1 Bra-Ket Notation

6.1.2 Hamiltonian

6.1.3 Wave Function Collapse

6.1.4 Schrödingers Equation

6.2 Quantum Decoherence

6.3 Quantum Electrodynamics

6.4 Quantum Chromodynamics

6.5 Feynman Diagram

6.6 Summary

Table of Contents

Test Your Skills

Chapter 7: Quantum Entanglement and QKD

7.1 Quantum Entanglement

7.2 Interpretation

7.2.1 The Copenhagen Interpretation

7.2.2 The Many-Worlds Interpretation

7.2.3 Decoherent Histories

7.2.4 Objective Collapse Theory

7.3 QKE

7.3.1 BB84 Protocol

7.3.2 B92 Protocol

7.3.3 SARG04

7.3.4 Six-State Protocol

7.3.5 E91

7.3.6 Implementations

7.4 Summary

Test Your Skills

Chapter 8: Quantum Architecture

8.1 Further with Qubits

8.2 Quantum Gates

8.2.1 Hadamard Gate

8.2.2 Phase Shift Gates

8.2.3 Pauli Gates

8.2.4 Swap Gates

8.2.5 Fredkin Gate

8.2.6 Toffoli Gates

8.2.7 Controlled Gates

8.2.8 Ising Gates

8.2.9 GottesmanKnill Theorem

8.3 More with Gates

8.4 Quantum Circuits

8.5 The D-Wave Quantum Architecture

Table of Contents

8.5.1 SQUID

8.6 Summary

Test Your Skills

Chapter 9: Quantum Hardware

9.1 Qubits

9.1.1 Photons

9.1.2 Electron

9.1.3 Ions

9.1.4 NMRQC

9.1.5 Bose-Einstein Condensate Quantum Computing

9.1.6 GaAs Quantum Dots

9.2 How Many Qubits Are Needed?

9.3 Addressing Decoherence

9.3.1 Supercooling

9.3.2 Dealing with Noise

9.3.3 Filtering Noise

9.4 Topological Quantum Computing

9.4.1 Basic Braid Theory

9.4.2 More on Braid Theory

9.4.3 More on Topological Computing

9.5 Quantum Essentials

9.5.1 Quantum Data Plane

9.5.2 Measurement Plane

9.5.3 Control Processor Plane

9.6 Quantum Networking

9.6.1 Tokyo QKD

9.6.2 Beijing-Shanghai Quantum Link

9.6.3 Micius Satellite

9.6.4 Distributed Quantum Computing

9.7 Summary

Test Your Skills

Chapter 10: Quantum Algorithms

Table of Contents

- 10.1 What Is an Algorithm?
- 10.2 Deutsch's Algorithm
- 10.3 Deutsch-Jozsa Algorithm
- 10.4 Bernstein-Vazirani Algorithm
- 10.5 Simon's Algorithm
- 10.6 Shor's Algorithm
 - 10.6.1 The Quantum Period-Finding Function
- 10.7 Grover's Algorithm
- 10.8 Summary
- Test Your Skills

Part III: Quantum Computing and Cryptography

Chapter 11: Current Asymmetric Algorithms

- 11.1 RSA
 - 11.1.1 RSA Example 1
 - 11.1.2 RSA Example 2
 - 11.1.3 Factoring RSA Keys
- 11.2 Diffie-Hellman
 - 11.2.1 ElGamal
 - 11.2.2 MQV
- 11.3 Elliptic Curve
 - 11.3.1 ECC Diffie-Hellman
 - 11.3.2 ECDSA
- 11.4 Summary
- Test Your Skills

Chapter 12: The Impact of Quantum Computing on Cryptography

- 12.1 Asymmetric Cryptography
 - 12.1.1 How Many Qubits Are Needed?
- 12.2 Specific Algorithms
 - 12.2.1 RSA
 - 12.2.2 Diffie-Hellman
 - 12.2.3 ECC

Table of Contents

12.2.4 Symmetric Ciphers

12.2.5 Cryptographic Hashes

12.3 Specific Applications

12.3.1 Digital Certificates

12.3.2 SSL/TLS

12.3.4 Public Key Infrastructure (PKI)

12.3.5 VPN

12.3.6 SSH

12.4 Summary

Test Your Skills

Chapter 13: Lattice-based Cryptography

13.1 Lattice-Based Mathematical Problems

13.1.1 Shortest Integer Problem

13.1.2 Shortest Vector Problem

13.1.3 Closest Vector Problem

13.2 Cryptographic Algorithms

13.2.1 NTRU

13.2.2 GGH

13.2.3 Peikerts Ring

13.3 Solving Lattice Problems

13.3.1 Lenstra-Lenstra-Lovász (LLL)

13.4 Summary

Test Your Skills

Chapter 14: Multivariate Cryptography

14.1 Mathematics

14.2 Matsumoto-Imai

14.3 Hidden Field Equations

14.4 Multivariate Quadratic Digital Signature Scheme (MQDSS)

14.5 SFLASH

14.6 Summary

Test Your Skills

Table of Contents

Chapter 15: Other Approaches to Quantum Resistant Cryptography

15.1 Hash Functions

15.1.1 Merkle-Damgaard

15.1.2 SWIFFT

15.1.3 Lamport Signature

15.2 Code-Based Cryptography

15.2.1 McEliece

15.2.2 Niederreiter Cryptosystem

15.3 Supersingular Isogeny Key Exchange

15.3.1 Elliptic Curves

15.3.2 SIDH

15.4 Summary

Test Your Skills

Part IV: Quantum Programming

Chapter 16: Working with Q#

16.1 Basic Programming Concepts

16.1.1 Variables and Statements

16.1.2 Control Structures

16.1.3 Object-Oriented Programming

16.2 Getting Started with Q#

16.3 Grover's Algorithm

16.3.1 Grover's Algorithm Reviewed

16.3.2 The Code for Grover's Algorithm

16.4 Deutsch-Jozsa Algorithm

16.4.1 Deutsch-Jozsa Algorithm Reviewed

16.4.2 The Code for Deutsch-Jozsa Algorithm

16.5 Bit Flipping

16.6 Summary

Test Your Skills

Chapter 17: Working with QASM

17.1 Basic Programming Concepts

Table of Contents

17.1.1 Instructions

17.1.2 Commands

17.2 Getting Started with QASM

17.3 Quantum Error Correction

17.4 Grovers Algorithm

17.4.1 Grovers Algorithm Reviewed

17.4.2 The Code for Grovers Algorithm

17.5 Deutsch-Jozsa Algorithm

17.5.1 Deutsch-Jozsa Algorithm Reviewed

17.5.2 The Code for the Deutsch-Jozsa Algorithm

17.6 Summary

Test Your Skills

Appendix: Answers to Test Your Skills Questions

Index