Mahn-Soo Choi (Korea University)

A Quantum Computation Workbook

September 28, 2021

Springer

For students

A draft provided with the perimission of Springer

Notice

N.B. This book will be published with Springer later this year. This draft is provided for educational purposes with the permission of Springer. Redistribution of this draft is strictly prohibited.

N.B. Two digital materials accompany the book. Both are freely available through the respective GitHub repositories at the links below.

- Q3, a Mathematica application (Appendix D):
  https://github.com/quantum-mob/Q3App
- QuantumWorkbook, a compilation of the demonstrations in this book written in the Wolfram Language (Appendix E):
  https://github.com/quantum-mob/QuantumWorkbook

A draft provided with the perimission of Springer

Preface

This book is intended as an introductory text for a university course on quantum computation and as a self-learning guide. It is an attempt to collect some fundamental principles and elementary methods in the field of quantum computation and quantum information and then reorganize them in a compact and integrated form. A proper introduction to (and hence learning of) quantum computation and quantum information turns out to be demanding, especially to undergraduate students, because it needs to cover various subjects from different fields of science including the physics of quantum mechanics, the mathematics of advanced linear algebra, and the computer science of information theory, to list the least. Each field of science usually favors its specific language, so another layer of difficulties is to organize the subjects consistently in a unified language.

Two digital materials accompany the book. Both are freely available through the respective GitHub repositories at the links below.

- Q3, a Mathematica application (Appendix D):
  https://github.com/quantum-mob/Q3App
- QuantumWorkbook, a compilation of the demonstrations in this book written in the Wolfram Language (Appendix E):
  https://github.com/quantum-mob/QuantumWorkbook

Q3 consists of tools and utilities that perform symbolic calculations and numerical simulations useful in the study of quantum information processing, quantum many-body systems, and quantum spin systems. With Q3, one can avoid many of the tedious calculations involved in various principles and theorems of quantum theory. Furthermore, numerous visualization and simulation tools can help deepen the understanding of core concepts. *QuantumWorkbook* is a compilation of Mathematica Notebook files that contain the code used to generate the demonstrations in the book. Readers themselves can run and modify the code to build their own examples from the demonstrations and to experiment with fresh ideas. Both materials can be helpful companions, particularly in a course of self-learning, of the various subjects of quantum physics present in the book and for the general study of the overall subject as well.

This book is a result of several years of experience in teaching quantum computation and quantum information. It is a helpful resource to select and present particular topics of the subject at the undergraduate level. Although

the book aims to be self-contained, it nonetheless assumes some basic knowledge of quantum mechanics. Chapter 1 summarizes the fundamental postulates of quantum mechanics and effectively provides a brief review of basic concepts and fundamental principles of quantum mechanics. Chapter 2 presents and describes the properties of elementary quantum gates for universal quantum computation. These are the building blocks of quantum algorithms and quantum communication protocols. Chapter 3 discusses physical methods and principles to implement elementary quantum gates and also introduces different quantum computation schemes. Chapter 4 introduces some widely known quantum algorithms to help grasp the idea of the so-called 'quantum supremacy' of quantum algorithms over their classical counterparts. Chapter 5 is dedicated to decoherence effects and introduces mathematical methods including the Kraus representation and the Lindblad equation to describe the phenomena. Chapter 6 is devoted to quantum error-correction codes through a discussion of the basic principles, procedures, and examples. Chapter 7 introduces quantum information theory. It discusses distance measures for quantum information, measures for quantum entanglement degree, and entropies of information content. To maintain a coherent structure and to focus on the primary topics, we collect the corresponding mathematical theories in the appendices and refer to them from the main text as necessary.

The author is indebted to students in his classes for pointing out numerous mistakes and typographical errors in the manuscript. Many people have contributed to the development of Q3 by testing and actively using it. The author gives particular thanks to Ha-Eum Kim, Myeongwon Lee, and Su-Ho Choi for their energetic discussions and constructive feedback in the early stages of the development of Q3. He also appreciates bug reports and valuable comments by Boris Laurent, Mi Jung So, Yeong-ho Je, and Dongni Chen.

Seoul, Korea
August 2021 *Mahn-Soo Choi*

A draft provided with the perimission of Springer

Contents

1 The Postulates of Quantum Mechanics **13**
- 1.1 Quantum States . . . 14
  - 1.1.1 Pure States . . . 14
  - 1.1.2 Mixed States . . . 19
- 1.2 Time Evolution of Quantum States . . . 28
  - 1.2.1 Unitary Dynamics . . . 28
  - 1.2.2 Quantum Noisy Dynamics . . . 32
- 1.3 Measurements on Quantum States . . . 33
  - 1.3.1 Projection Measurements . . . 33
  - 1.3.2 Generalized Measurements . . . 38

2 Quantum Computation: Overview **45**
- 2.1 Single-Qubit Gates . . . 46
  - 2.1.1 Pauli Gates . . . 46
  - 2.1.2 Hadamard Gate . . . 50
  - 2.1.3 Rotations . . . 54
- 2.2 Two-Qubit Gates . . . 57
  - 2.2.1 CNOT, CZ, and SWAP . . . 57
  - 2.2.2 Controlled-Unitary Gates . . . 68
  - 2.2.3 General Unitary Gate . . . 74
- 2.3 Multi-Control Unitary Gates . . . 81
  - 2.3.1 Gray Code . . . 82
  - 2.3.2 Multi-Control NOT Gate . . . 84
- 2.4 Universal Quantum Computation . . . 90
- 2.5 Measurements . . . 92

3 Realizations of Quantum Computers **101**
- 3.1 Quantum Bits . . . 102
- 3.2 Dynamical Scheme . . . 104
  - 3.2.1 Implementation of Single-Qubit Gates . . . 105
  - 3.2.2 Implementation of CNOT . . . 111
- 3.3 Geometric/Topological Scheme . . . 114
  - 3.3.1 A Toy Model . . . 115

3.3.2 Geometric Phase . . . 121
3.4 Measurement-Based Scheme . . . 124
3.4.1 Single-Qubit Rotations . . . 128
3.4.2 CNOT Gate . . . 131
3.4.3 Graph States . . . 133

4 Quantum Algorithms 139
4.1 Quantum Teleportation . . . 140
4.1.1 Nonlocality in Entanglement . . . 141
4.1.2 Implementation of Quantum Teleportation . . . 144
4.2 Deutsch-Jozsa Algorithm & Variants . . . 148
4.2.1 Quantum Oracle . . . 148
4.2.2 Deutsch-Jozsa Algorithm . . . 154
4.2.3 Bernstein-Vazirani Algorithm . . . 156
4.2.4 Simon's Algorithm . . . 158
4.3 Quantum Fourier Transform (QFT) . . . 162
4.3.1 Definition and Physical Meaning . . . 163
4.3.2 Quantum Implementation . . . 164
4.3.3 Semiclassical Implementation . . . 168
4.4 Quantum Phase Estimation (QPE) . . . 172
4.4.1 Definition . . . 173
4.4.2 Implementation . . . 174
4.4.3 Accuracy . . . 177
4.4.4 Simulation of the von Neumann Measurement . . . 178
4.5 Applications . . . 180
4.5.1 The Period-Finding Algorithm . . . 180
4.5.2 The Order-Finding Algorithm . . . 187
4.5.3 Quantum Factorization Algorithm . . . 189
4.5.4 Quantum Search Algorithm . . . 190

5 Quantum Decoherence 201
5.1 How Does Decoherence Occur? . . . 202
5.2 Quantum Operations . . . 208
5.2.1 Kraus Representation . . . 210
5.2.2 Choi Isomorphism . . . 218
5.2.3 Unitary Representation . . . 222
5.2.4 Examples . . . 222
5.3 Measurements as Quantum Operations . . . 227
5.4 Quantum Master Equation . . . 228
5.4.1 Derivation . . . 230
5.4.2 Examples . . . 231
5.4.3 Solution Methods . . . 234
5.4.4 Examples Revisited . . . 241
5.5 Distance between Quantum States . . . 245

A draft provided with the perimission of Springer

5.5.1 Norms and Distances . . . 246
5.5.2 Hilbert-Schmidt and Trace Norms . . . 247
5.5.3 Hilbert-Schmidt and Trace Distances . . . 252
5.5.4 Fidelity . . . 257

6 Quantum Error-Correction Codes 267
6.1 Elementary Examples: Nine-Qubit Code . . . 268
6.1.1 Bit-Flip Errors . . . 268
6.1.2 Phase-Flip Error . . . 271
6.1.3 Shor's Nine-Qubit Code . . . 273
6.2 Quantum Error Correction . . . 277
6.2.1 Quantum Error-Correction Conditions . . . 278
6.2.2 Discretization of errors . . . 280
6.3 Stabilizer Formalism . . . 280
6.3.1 Pauli Group . . . 283
6.3.2 Properties of the Stabilizers . . . 289
6.3.3 Unitary Gates in Stabilizer Formalism . . . 291
6.3.4 Clifford Group . . . 292
6.3.5 Measurements in Stabilizer Formalism . . . 299
6.3.6 Examples . . . 301
6.4 Stabilizer Codes . . . 307
6.4.1 Bit-Flip Code . . . 309
6.4.2 Phase-Flip Code . . . 310
6.4.3 Nine-Qubit Code . . . 312
6.4.4 Five-Qubit Code . . . 314
6.5 Surface Codes . . . 318
6.5.1 Toric Codes . . . 318
6.5.2 Planar Codes . . . 324
6.5.3 Recovery Procedure . . . 326

7 Quantum Information Theory 333
7.1 Shannon Entropy . . . 334
7.1.1 Definition . . . 334
7.1.2 Relative Entropy . . . 335
7.1.3 Mutual Information . . . 337
7.1.4 Data Compression . . . 340
7.2 Von Neumann Entropy . . . 341
7.2.1 Definition . . . 341
7.2.2 Relative Entropy . . . 344
7.2.3 Quantum Mutual Information . . . 346
7.3 Entanglement and Entropy . . . 348
7.3.1 What is Entanglement? . . . 348
7.3.2 Separability Tests . . . 349
7.3.3 Entanglement Distillation . . . 352

A draft provided with the perimission of Springer

7.3.4 Entanglement Measures 354

A Linear Algebra **359**
A.1 Vectors 359
A.1.1 Vector Space 359
A.1.2 Hermitian Product 361
A.1.3 Basis 362
A.1.4 Representations 363
A.2 Linear Operators 365
A.2.1 Linear Maps 365
A.2.2 Representations 366
A.2.3 Hermitian Conjugate of Operators 367
A.3 Dirac's Bra-Ket Notation 369
A.4 Spectral Theorems 372
A.4.1 Spectral Decomposition 372
A.4.2 Functions of Operators 375
A.5 Factorization of Operators 376
A.6 Tensor-Product Spaces 378
A.6.1 Vectors in a Product Space 379
A.6.2 Operators on a Product Space 380

B Superoperators **383**
B.1 Operators as Vectors 383
B.2 Superoperators 389
B.2.1 Matrix Representation 390
B.2.2 Operator-Sum Representation 391
B.2.3 Choi Isomorphism 396
B.3 Partial Trace 399
B.4 Partial Transposition 401

C Group Theory **405**
C.1 The Concept 405
C.2 Classes 409
C.3 Invariant Subgroups 410
C.4 Cosets and Quotient Groups 411
C.5 Product Groups 413

D Mathematica Application Q3 **415**
D.1 Installation 415
D.2 Quick Start 416

E Integrated Compilation of Demonstrations **417**
E.1 Installation 417
E.2 Quick Start 418

A draft provided with the perimission of Springer

F Solutions to Select Problems **419**
F.1 The Postulates of Quantum Mechanics 419
F.2 Quantum Computation: Overview 419
F.3 Quantum Computers 422
F.4 Quantum Algorithms 424
F.5 Decoherence 425
F.6 Quantum Error-Correction Codes 429
F.7 Quantum Information Theory 433

Bibliography **435**

Index **444**

A draft provided with the perimission of Springer

A draft provided with the perimission of Springer