

Mahn-Soo Choi (Korea University)

A Quantum Computation Workbook

February 4, 2022

For students

Notice

N.B. This book will be published with Springer on February 1, 2022. 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>

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

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	32
1.3.1	Projection Measurements	33
1.3.2	Generalized Measurements	37
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	53
2.2	Two-Qubit Gates	57
2.2.1	CNOT, CZ, and SWAP	57
2.2.2	Controlled-Unitary Gates	67
2.2.3	General Unitary Gates	73
2.3	Multi-Control Unitary Gates	80
2.3.1	Gray-Code Method	81
2.3.2	Multi-Control NOT Gate	83
2.4	Universal Quantum Computation	88
2.5	Measurements	93
3	Realizations of Quantum Computers	103
3.1	Quantum Bits	104
3.2	Dynamical Scheme	106
3.2.1	Implementation of Single-Qubit Gates	107
3.2.2	Implementation of CNOT	113
3.3	Geometric/Topological Scheme	116
3.3.1	A Toy Model	117

3.3.2	Geometric Phase	122
3.4	Measurement-Based Scheme	125
3.4.1	Single-Qubit Rotations	129
3.4.2	CNOT Gate	132
3.4.3	Graph States	135
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	157
4.3	Quantum Fourier Transform	161
4.3.1	Definition and Physical Meaning	162
4.3.2	Quantum Implementation	163
4.3.3	Semiclassical Implementation	167
4.4	Quantum Phase Estimation	171
4.4.1	Definition	171
4.4.2	Implementation	173
4.4.3	Accuracy	175
4.4.4	Simulation of the von Neumann Measurement	176
4.5	Applications	178
4.5.1	The Period-Finding Algorithm	178
4.5.2	The Order-Finding Algorithm	185
4.5.3	Quantum Factorization Algorithm	187
4.5.4	Quantum Search Algorithm	188
5	Quantum Decoherence	199
5.1	How Does Decoherence Occur?	200
5.2	Quantum Operations	206
5.2.1	Kraus Representation	208
5.2.2	Choi Isomorphism	216
5.2.3	Unitary Representation	219
5.2.4	Examples	220
5.3	Measurements as Quantum Operations	225
5.4	Quantum Master Equation	226
5.4.1	Derivation	228
5.4.2	Examples	229
5.4.3	Solution Methods	232
5.4.4	Examples Revisited	238
5.5	Distance between Quantum States	243

5.5.1	Norms and Distances	243
5.5.2	Hilbert-Schmidt and Trace Norms	244
5.5.3	Hilbert-Schmidt and Trace Distances	250
5.5.4	Fidelity	254
6	Quantum Error-Correction Codes	265
6.1	Elementary Examples: Nine-Qubit Code	266
6.1.1	Bit-Flip Errors	266
6.1.2	Phase-Flip Errors	269
6.1.3	Arbitrary Errors	271
6.2	Quantum Error-Correction Theorems	276
6.2.1	Quantum Error-Correction Conditions	276
6.2.2	Discretization of Errors	279
6.3	Stabilizer Formalism	279
6.3.1	Pauli Group	282
6.3.2	Properties of the Stabilizers	287
6.3.3	Unitary Gates in Stabilizer Formalism	290
6.3.4	Clifford Group	291
6.3.5	Measurements in Stabilizer Formalism	297
6.3.6	Examples	299
6.4	Stabilizer Codes	305
6.4.1	Bit-Flip Code	307
6.4.2	Phase-Flip Code	308
6.4.3	Nine-Qubit Code	310
6.4.4	Five-Qubit Code	312
6.5	Surface Codes	316
6.5.1	Toric Codes	316
6.5.2	Planar Codes	322
6.5.3	Recovery Procedure	324
7	Quantum Information Theory	331
7.1	Shannon Entropy	332
7.1.1	Definition	332
7.1.2	Relative Entropy	333
7.1.3	Mutual Information	335
7.1.4	Data Compression	338
7.2	Von Neumann Entropy	339
7.2.1	Definition	339
7.2.2	Relative Entropy	342
7.2.3	Quantum Mutual Information	344
7.3	Entanglement and Entropy	346
7.3.1	What is Entanglement?	346
7.3.2	Separability Tests	347
7.3.3	Entanglement Distillation	350

7.3.4	Entanglement Measures	352
A	Linear Algebra	357
A.1	Vectors	357
A.1.1	Vector Space	357
A.1.2	Hermitian Product	359
A.1.3	Basis	360
A.1.4	Representations	361
A.2	Linear Operators	363
A.2.1	Linear Maps	363
A.2.2	Representations	364
A.2.3	Hermitian Conjugate of Operators	365
A.3	Dirac's Bra-Ket Notation	367
A.4	Spectral Theorems	370
A.4.1	Spectral Decomposition	370
A.4.2	Functions of Operators	372
A.5	Factorization of Operators	374
A.6	Tensor-Product Spaces	376
A.6.1	Vectors in a Product Space	376
A.6.2	Operators on a Product Space	378
B	Superoperators	381
B.1	Operators as Vectors	381
B.2	Superoperators	387
B.2.1	Matrix Representation	387
B.2.2	Operator-Sum Representation	389
B.2.3	Choi Isomorphism	394
B.3	Partial Trace	396
B.4	Partial Transposition	398
C	Group Theory	403
C.1	The Concept	403
C.2	Classes	407
C.3	Invariant Subgroups	408
C.4	Cosets and Quotient Groups	409
C.5	Product Groups	411
D	Mathematica Application Q3	413
D.1	Installation	413
D.2	Quick Start	414
E	Integrated Compilation of Demonstrations	415
E.1	Installation	415
E.2	Quick Start	416

CONTENTS

11

F

Solutions to Select Problems

417

F.1

The Postulates of Quantum Mechanics

417

F.2

Quantum Computation: Overview

417

F.3

Quantum Computers

420

F.4

Quantum Algorithms

422

F.5

Decoherence

423

F.6

Quantum Error-Correction Codes

427

F.7

Quantum Information Theory

431

Bibliography

433

Index

442

