Mathematical Foundations of Quantum Computation

Lectures Notes for MA591 at NCSU

Moody T. Chu

Department of Mathematics
North Carolina State University

November 11, 2020

Preface

Quantum computing and quantum information science are emerging disciplines in which the principles of quantum physics are employed to store and process information. Quantum technologies are pushing forward the frontiers of the future. At the time when quantum computation is fully developed, many salient applications will stand to benefit from this fast, concurrent, and secure information processing ability — we will be able to handle some of the most pressing problems the world faces as well as leap to discoveries not yet known. As such, students should be curious and find it both beneficial and of vital importance that they are exposed to this subject as early as possible. A solid grasp and holistic treatment of this subject will require disciplines across multiple academic fields, which is hard to come by. This course intends to serve as a stepping stone by introducing this subject from the mathematical perspective. Mathematical and computational foundations useful for deciphering the rich structure within a quantum system and the quantum computation will be discussed.

This course is developed with the aim at exposing students via the mathematical vista how the quantum computation can be understood and formulated. Its goal is to build basic, and somewhat in-depth, mathematical knowledge needed for more advanced quantum computation.

I shall assume that students are familiar with linear algebra, e.g., inner product spaces, unitary transformations, and so on. Some familiarity with basic logic gates for Boolean functions, e.g., AND, XOR, and truth table, will be useful.

The notes are prepared in the form of itemized list, which highlights the basic but important concepts. More meat will be put on the bones during the class hours. I code some texts with colors for the following purposes:

1. Blue color means a suggested problem that readers are encouraged to work out the details.

2. Red color means some additional thoughts that readers are encouraged to ponder and perhaps some deeper investigations.

Contents

1 Tensor Product Space **1**

1.1 Hilbert Space . . . 2
- Inner Product . . . 3
- Orthogonal Complements . . . 5
- Gram-Schmidt Orthogalization Process . . . 6

1.2 Representation Theory . . . 8
- Approximation . . . 9
- Projection Theorem . . . 10
- Schauder Basis versus Hamel Basis . . . 12
- Fourier Series . . . 13

1.3 Tensor Algebra . . . 15
- Tensor Product . . . 16
- Linear Operators . . . 18
- Tensor Product versus Kronecker Product . . . 20

1.4 Schmidt Decomposition and Singular Value Decomposition . . . 27
- Singular Value Decomposition . . . 28
- Schmidt Decomposition . . . 31

2 Basic Principles in Quantum Mechanics **33**

2.1 Copenhagen Interpretation . . . 34
- Postulate 1 – Pure and Mixed States . . . 35
- Postulate 2 – Observables . . . 36
- Postulate 3 – Schröndinger Equation . . . 37

2.2 Density Matrix and Its Statistical Meaning . . . 38
- Convex Hull of Pure States . . . 39
- Bloch Sphere . . . 40
- Statistical Ensembles . . . 42

2.3 Entanglement . . . 43
- Composite Systems . . . 44
- Bipartite Density Matrices . . . 46
- Separability . . . 49

2.4 Purification . . . 56
- Partial Traces . . . 57
- Purifying a Mixed State . . . 59

3 Quantum Computing Tools **61**
3.1 Quantum Computer . . . 62
Bits versus Qubits . . . 63
Representing an n-Qubit . . . 64
Multistate Systems . . . 66
3.2 Reversible Operations . . . 67
Some Irreversible Operators . . . 68
Some Reversible Operations . . . 69
Why Is Reversibility Necessary? . . . 70
3.3 Logic Gates vs. Quantum Gates . . . 72
cNOT Gate . . . 73
Z Gate . . . 74
Hadamard Gate **H** . . . 76
Toffoli Gate **T** . . . 79
AND and **NAND** Gates . . . 80
OR Gate . . . 81
3.4 Circuits . . . 82
Registers . . . 83
Quantum Parallelism and Weirdness . . . 84
Non-Cloning Theorem . . . 85
3.5 Applications of Entanglement . . . 87
Dense Coding . . . 88
Teleportation . . . 90

4 Computational Examples **93**
4.1 Deutsch Problem . . . 94
Problem Statement . . . 95
Deutsch Algorithm . . . 97
Deutsch-Jozsa algorithm . . . 98
4.2 Bernstein-Vazirani Problem . . . 100
Problem Statement . . . 101
Algorithm . . . 102
4.3 Simon Problem . . . 103
Problem Statement . . . 104
Conventional Search . . . 105
Algorithm . . . 106
4.4 Unstructured Search Problem . . . 108
Problem Statement . . . 109
Grover Iterate . . . 110
Grover Algorithm . . . 111
4.5 Constructing the Toffoli gate . . . 114

5 Applications **115**
5.1 RSA Encryption . . . 116
Fermat Little Theorem . . . 117
Communication between Alice and Bob . . . 119
Decoding by Eve . . . 120
5.2 Quantum Fourier Transform . . . 121
Quick Recap of Classical DFT . . . 122
n-qubit QFT . . . 123
Using QFT for Period Finding . . . 125
5.3 Shor Factorization . . . 132
Basic Idea . . . 133
Order Finding . . . 135
Continued Fraction . . . 136
5.4 Solving Linear Algebra Problems . . . 137
Eigenvalue Problem . . . 138
Quantum Phase Estimation . . . 141
System of Linear Equations . . . 146
5.5 Differential Equations . . . 150
Classical ODE Methods . . . 151
Quantum Formulation . . . 158