CRC Press
Taylor & Francis Group
A TAYLOR & FRANCIS BOOK

QUANTUM COMPUTING

From Linear Algebra to Physical Realizations

Mikio Nakahara and Tetsuo Ohmi

Contents

I From Linear Algebra to Quantum Computing 1

1 Basics of Vectors and Matrices 3
1.1 Vector Spaces 4
1.2 Linear Dependence and Independence of Vectors 5
1.3 Dual Vector Spaces 6
1.4 Basis, Projection Operator and Completeness Relation 8
1.4.1 Orthonormal Basis and Completeness Relation 8
1.4.2 Projection Operators 9
1.4.3 Gram-Schmidt Orthonormalization 10
1.5 Linear Operators and Matrices 11
1.5.1 Hermitian Conjugate, Hermitian and Unitary Matrices 12
1.6 Eigenvalue Problems 13
1.6.1 Eigenvalue Problems of Hermitian and Normal Matrices 14
1.7 Pauli Matrices 18
1.8 Spectral Decomposition 19
1.9 Singular Value Decomposition (SVD) 23
1.10 Tensor Product (Kronecker Product) 26

2 Framework of Quantum Mechanics 29
2.1 Fundamental Postulates 29
2.2 Some Examples 32
2.3 Multipartite System, Tensor Product and Entangled State . . 36
2.4 Mixed States and Density Matrices 38
2.4.1 Negativity 42
2.4.2 Partial Trace and Purification 45
2.4.3 Fidelity 47

3 Qubits and Quantum Key Distribution 51
3.1 Qubits 51
3.1.1 One Qubit 51
3.1.2 Bloch Sphere 53
3.1.3 Multi-Qubit Systems and Entangled States 54
3.1.4 Measurements 56

3.1.5 Einstein-Podolsky-Rosen (EPR) Paradox 59
3.2 Quantum Key Distribution (BB84 Protocol) 60

4 Quantum Gates, Quantum Circuit and Quantum Computation 65
4.1 Introduction 65
4.2 Quantum Gates 66
4.2.1 Simple Quantum Gates 66
4.2.2 Walsh-Hadamard Transformation 69
4.2.3 SWAP Gate and Fredkin Gate 70
4.3 Correspondence with Classical Logic Gates 71
4.3.1 NOT Gate 72
4.3.2 XOR Gate 72
4.3.3 AND Gate 73
4.3.4 OR Gate 73
4.4 No-Cloning Theorem 75
4.5 Dense Coding and Quantum Teleportation 76
4.5.1 Dense Coding 77
4.5.2 Quantum Teleportation 79
4.6 Universal Quantum Gates 82
4.7 Quantum Parallelism and Entanglement 95

5 Simple Quantum Algorithms 99
5.1 Deutsch Algorithm 99
5.2 Deutsch-Jozsa Algorithm and Bernstein-Vazirani Algorithm . 101
5.3 Simon's Algorithm 105

6 Quantum Integral Transforms 109
6.1 Quantum Integral Transforms 109
6.2 Quantum Fourier Transform (QFT) 111
6.3 Application of QFT: Period-Finding 113
6.4 Implementation of QFT 116
6.5 Walsh-Hadamard Transform 122
6.6 Selective Phase Rotation Transform 123

7 Grover's Search Algorithm 125
7.1 Searching for a Single File 125
7.2 Searching for *d* Files 133

8 Shor's Factorization Algorithm 137
8.1 The RSA Cryptosystem 137
8.2 Factorization Algorithm 140
8.3 Quantum Part of Shor's Algorithm 141
8.3.1 Settings for STEP 2 141
8.3.2 STEP 2 143