

# QUANTUM COMPUTING

*From Linear Algebra  
to Physical Realizations*

Mikio Nakahara

*Department of Physics*

*Kinki University, Higashi-Osaka, Japan*

Tetsuo Ohmi

*Interdisciplinary Graduate School of Science and Engineering*

*Kinki University, Higashi-Osaka, Japan*



**CRC Press**

Taylor & Francis Group

Boca Raton London New York

---

CRC Press is an imprint of the  
Taylor & Francis Group, an **informa** business

A TAYLOR & FRANCIS BOOK

---

# Contents

<b>I</b>	<b>From Linear Algebra to Quantum Computing</b>	<b>1</b>
<b>1</b>	<b>Basics of Vectors and Matrices</b>	<b>3</b>
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
<b>2</b>	<b>Framework of Quantum Mechanics</b>	<b>29</b>
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
<b>3</b>	<b>Qubits and Quantum Key Distribution</b>	<b>51</b>
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
<b>4</b>	<b>Quantum Gates, Quantum Circuit and Quantum Computation</b>	<b>65</b>
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
<b>5</b>	<b>Simple Quantum Algorithms</b>	<b>99</b>
5.1	Deutsch Algorithm . . . . .	99
5.2	Deutsch-Jozsa Algorithm and Bernstein-Vazirani Algorithm .	101
5.3	Simon's Algorithm . . . . .	105
<b>6</b>	<b>Quantum Integral Transforms</b>	<b>109</b>
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
<b>7</b>	<b>Grover's Search Algorithm</b>	<b>125</b>
7.1	Searching for a Single File . . . . .	125
7.2	Searching for $d$ Files . . . . .	133
<b>8</b>	<b>Shor's Factorization Algorithm</b>	<b>137</b>
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

8.4	Probability Distribution . . . . .	144
8.5	Continued Fractions and Order Finding . . . . .	151
8.6	Modular Exponential Function . . . . .	156
8.6.1	Adder . . . . .	157
8.6.2	Modular Adder . . . . .	161
8.6.3	Modular Multiplexer . . . . .	166
8.6.4	Modular Exponential Function . . . . .	168
8.6.5	Computational Complexity of Modular Exponential Circuit . . . . .	170
<b>9</b>	<b>Decoherence</b> . . . . .	<b>173</b>
9.1	Open Quantum System . . . . .	173
9.1.1	Quantum Operations and Kraus Operators . . . . .	174
9.1.2	Operator-Sum Representation and Noisy Quantum Channel . . . . .	177
9.1.3	Completely Positive Maps . . . . .	178
9.2	Measurements as Quantum Operations . . . . .	179
9.2.1	Projective Measurements . . . . .	179
9.2.2	POVM . . . . .	180
9.3	Examples . . . . .	181
9.3.1	Bit-Flip Channel . . . . .	181
9.3.2	Phase-Flip Channel . . . . .	183
9.3.3	Depolarizing Channel . . . . .	185
9.3.4	Amplitude-Damping Channel . . . . .	187
9.4	Lindblad Equation . . . . .	188
9.4.1	Quantum Dynamical Semigroup . . . . .	189
9.4.2	Lindblad Equation . . . . .	189
9.4.3	Examples . . . . .	192
<b>10</b>	<b>Quantum Error Correcting Codes</b> . . . . .	<b>195</b>
10.1	Introduction . . . . .	195
10.2	Three-Qubit Bit-Flip Code and Phase-Flip Code . . . . .	196
10.2.1	Bit-Flip QECC . . . . .	196
10.2.2	Phase-Flip QECC . . . . .	202
10.3	Shor's Nine-Qubit Code . . . . .	203
10.3.1	Encoding . . . . .	204
10.3.2	Transmission . . . . .	205
10.3.3	Error Syndrome Detection and Correction . . . . .	205
10.3.4	Decoding . . . . .	208
10.4	Seven-Qubit QECC . . . . .	209
10.4.1	Classical Theory of Error Correcting Codes . . . . .	209
10.4.2	Seven-Qubit QECC . . . . .	213
10.4.3	Gate Operations for Seven-Qubit QECC . . . . .	220
10.5	Five-Qubit QECC . . . . .	224
10.5.1	Encoding . . . . .	224

10.5.2	Error Syndrome Detection . . . . .	227
<b>II</b>	<b>Physical Realizations of Quantum Computing</b>	<b>231</b>
<b>11</b>	<b>DiVincenzo Criteria</b>	<b>233</b>
11.1	Introduction . . . . .	233
11.2	DiVincenzo Criteria . . . . .	234
11.3	Physical Realizations . . . . .	239
<b>12</b>	<b>NMR Quantum Computer</b>	<b>241</b>
12.1	Introduction . . . . .	241
12.2	NMR Spectrometer . . . . .	241
12.2.1	Molecules . . . . .	242
12.2.2	NMR Spectrometer . . . . .	242
12.3	Hamiltonian . . . . .	245
12.3.1	Single-Spin Hamiltonian . . . . .	245
12.3.2	Multi-Spin Hamiltonian . . . . .	248
12.4	Implementation of Gates and Algorithms . . . . .	252
12.4.1	One-Qubit Gates in One-Qubit Molecule . . . . .	252
12.4.2	One-Qubit Operation in Two-Qubit Molecule: Bloch-Siegert Effect . . . . .	256
12.4.3	Two-Qubit Gates . . . . .	257
12.4.4	Multi-Qubit Gates . . . . .	259
12.5	Time-Optimal Control of NMR Quantum Computer . . . . .	262
12.5.1	A Brief Introduction to Lie Algebras and Lie Groups . . . . .	262
12.5.2	Cartan Decomposition and Optimal Implementation of Two-Qubit Gates . . . . .	264
12.6	Measurements . . . . .	268
12.6.1	Introduction and Preliminary . . . . .	268
12.6.2	One-Qubit Quantum State Tomography . . . . .	269
12.6.3	Free Induction Decay (FID) . . . . .	270
12.6.4	Two-Qubit Tomography . . . . .	271
12.7	Preparation of Pseudopure State . . . . .	274
12.7.1	Temporal Averaging . . . . .	276
12.7.2	Spatial Averaging . . . . .	277
12.8	DiVincenzo Criteria . . . . .	281
<b>13</b>	<b>Trapped Ions</b>	<b>285</b>
13.1	Introduction . . . . .	285
13.2	Electronic States of Ions as Qubits . . . . .	287
13.3	Ions in Paul Trap . . . . .	289
13.3.1	Trapping Potential . . . . .	289
13.3.2	Lattice Formation . . . . .	294
13.3.3	Normal Modes . . . . .	296
13.4	Ion Qubit . . . . .	298

13.4.1	One-Spin Hamiltonian . . . . .	298
13.4.2	Sideband Cooling . . . . .	301
13.5	Quantum Gates . . . . .	302
13.5.1	One-Qubit Gates . . . . .	302
13.5.2	CNOT Gate . . . . .	304
13.6	Readout . . . . .	306
13.7	DiVincenzo Criteria . . . . .	307
<b>14</b>	<b>Quantum Computing with Neutral Atoms</b>	<b>311</b>
14.1	Introduction . . . . .	311
14.2	Trapping Neutral Atoms . . . . .	311
14.2.1	Alkali Metal Atoms . . . . .	311
14.2.2	Magneto-Optical Trap (MOT) . . . . .	312
14.2.3	Optical Dipole Trap . . . . .	314
14.2.4	Optical Lattice . . . . .	316
14.2.5	Spin-Dependent Optical Potential . . . . .	317
14.3	One-Qubit Gates . . . . .	319
14.4	Quantum State Engineering of Neutral Atoms . . . . .	321
14.4.1	Trapping of a Single Atom . . . . .	321
14.4.2	Rabi Oscillation . . . . .	321
14.4.3	Neutral Atom Quantum Register . . . . .	323
14.5	Preparation of Entangled Neutral Atoms . . . . .	324
14.6	DiVincenzo Criteria . . . . .	327
<b>15</b>	<b>Josephson Junction Qubits</b>	<b>329</b>
15.1	Introduction . . . . .	329
15.2	Nanoscale Josephson Junctions and SQUIDS . . . . .	330
15.2.1	Josephson Junctions . . . . .	330
15.2.2	SQUIDS . . . . .	333
15.3	Charge Qubit . . . . .	337
15.3.1	Simple Cooper Pair Box . . . . .	337
15.3.2	Split Cooper Pair Box . . . . .	341
15.4	Flux Qubit . . . . .	342
15.4.1	Simplest Flux Qubit . . . . .	342
15.4.2	Three-Junction Flux Qubit . . . . .	345
15.5	Quantronium . . . . .	347
15.6	Current-Biased Qubit (Phase Qubit) . . . . .	348
15.7	Readout . . . . .	352
15.7.1	Charge Qubit . . . . .	352
15.7.2	Readout of Quantronium . . . . .	355
15.7.3	Switching Current Readout of Flux Qubits . . . . .	357
15.8	Coupled Qubits . . . . .	358
15.8.1	Capacitively Coupled Charge Qubits . . . . .	359
15.8.2	Inductive Coupling of Charge Qubits . . . . .	362
15.8.3	Tunable Coupling between Flux Qubits . . . . .	366

15.8.4	Coupling Flux Qubits with an LC Resonator . . . . .	369
15.9	DiVincenzo Criteria . . . . .	374
<b>16</b>	<b>Quantum Computing with Quantum Dots</b>	<b>377</b>
16.1	Introduction . . . . .	377
16.2	Mesoscopic Semiconductors . . . . .	377
16.2.1	Two-Dimensional Electron Gas in Inversion Layer . . . . .	377
16.2.2	Coulomb Blockade . . . . .	378
16.3	Electron Charge Qubit . . . . .	383
16.3.1	Electron Charge Qubit . . . . .	384
16.3.2	Rabi Oscillation . . . . .	385
16.4	Electron Spin Qubit . . . . .	386
16.4.1	Electron Spin Qubit . . . . .	386
16.4.2	Single-Qubit Operations . . . . .	387
16.4.3	Coherence Time . . . . .	390
16.5	DiVincenzo Criteria . . . . .	396
16.5.1	Charge Qubits . . . . .	396
16.5.2	Spin Qubits . . . . .	397
<b>A</b>	<b>Solutions to Selected Exercises</b>	<b>399</b>
	<b>Index</b>	<b>417</b>