



Hands-on Quantum Communications and Networking

Michel BARBEAU, PhD

Edition: March 24, 2017

Copyright © 2017 Michel Barbeau
All Rights Reserved

Copyright © 2017 Michel Barbeau
All Rights Reserved

Cover

The circuit pictured on the cover page was produced using the Web interface to the five-qubit quantum computer IBM Q5, see The IBM Quantum Experience.

This is a draft text book.

Please send comments and feedback to Michel Barbeau.

Draft

Contents

1	Introduction	1
1.1	Further Reading	2
2	Quantum Computing	3
2.1	Quantum Model of Information	3
2.1.1	Qubit	3
2.1.2	Quregister	8
2.2	Products of Qubits	9
2.2.1	Inner Product	10
2.2.2	Tensor Product	11
2.2.3	Outer Product	12
2.2.4	Mixed State	13
2.3	Gates	13
2.4	Quantum Circuit	14
2.5	Pauli Gates	15
2.5.1	Identity Gate	16
2.5.2	X Gate	16
2.5.3	Y Gate	16
2.5.4	Z Gate	16
2.5.5	Pauli Matrices	18
2.5.6	Pauli Group	19
2.6	Superposition Generation Gates	19
2.6.1	Hadamard Gate	19
2.6.2	S Gate	22
2.7	Multiple Qubit Gates	23
2.7.1	CNOT Gate	23
2.7.2	Swap Gate	24
2.7.3	Clifford Group	25
2.8	Projection Operator	29
2.9	Quantum Measurement	29
2.9.1	Other Forms of Measurement	32
2.10	Conditional Gate	33
2.11	Circuit Simulation	33
2.12	Entanglement	35

2.12.1	Bell-EPR Pairs	37
2.12.2	Bell-EPR Pair Production	37
2.12.3	Bell-EPR Measurement Preparation Circuit	38
2.12.4	W State	39
2.13	Further Reading	40
2.14	On the Net	40
3	Quantum Algorithms	41
3.1	Quantum Oracle	41
3.2	Deutsch's Algorithm	43
3.3	Bernstein-Vazirani Problem	47
4	Teleportation	51
4.1	Teleportation Programming	54
4.2	Further Reading	58
5	Quantum Communications	59
5.1	Quantum Encoding	59
5.1.1	Polarization Encoding	59
5.1.2	Phase Encoding	63
5.2	Quantum Key Distribution	63
5.3	Software-Defined Quantum Communication	71
5.3.1	Stream-cipher Example	72
5.3.2	Class <code>encoder</code>	73
5.3.3	Class <code>decoder</code>	77
5.3.4	Class <code>channel_ii</code>	80
5.3.5	Test Script	81
5.4	Quantum Optical Communications	82
5.5	Free Space Loss	84
5.6	Noise	84
5.7	Practical QKD	85
5.7.1	Weak Coherent Laser Pulses	85
5.7.2	Photon Number Splitting Attack	85
5.7.3	Decoy State Protocol	86
5.8	Coherent State Quantum Communication	88
5.8.1	Coherent State	89
5.8.2	Binary Communication System	90
5.9	Super Dense Coding	91
5.10	Spontaneous Parametric Down-Conversion	92
5.11	Further Reading	92
5.12	On the Net	93

6 Quantum Data Link	105
6.1 Medium Access Control by Quantum Methods	105
6.2 Qubit Distribution Protocol	106
6.3 Transmit First Election Protocol	111
6.4 Further Reading	112
7 Quantum Networking	113
7.1 Purification	114
7.2 Quantum Relay	116
7.3 Quantum Repeater	117
7.4 Entanglement Swapping	118
7.5 Error Detection and Correction	119
7.5.1 Repetition Code	119
7.6 Further Reading	120
8 Quantum Cryptography	121
8.1 Clifford Code-based Quantum Message Authentication	121
8.1.1 Authentication	121
8.2 Symmetric-key Quantum Encryption	122
8.3 Asymmetric-key Quantum Encryption	123
8.4 Further Reading	124
Answers to Exercises	125
A Class helper	129
B Introduction to MATLAB/Python Algebra	131
B.1 Complex Number	131
B.2 Inner Product	132
B.3 Tensor Product	133
B.4 Outer Product	135
B.5 Matrix Multiplication	136
C Constructing the GNU Radio SDQC Example	137
C.1 Creation of the Module Framework	137
C.2 Test Case	138
C.3 Building and Running	138
C.4 On the Net	139
D Clifford Group Element Selection	141
E Quantum Communication Lab	149
E.1 Sender	149
E.2 Receiver	150
F Decoy State Protocol Simulation	153

Bibliography	155
Glossary	158
Index	159

Draft