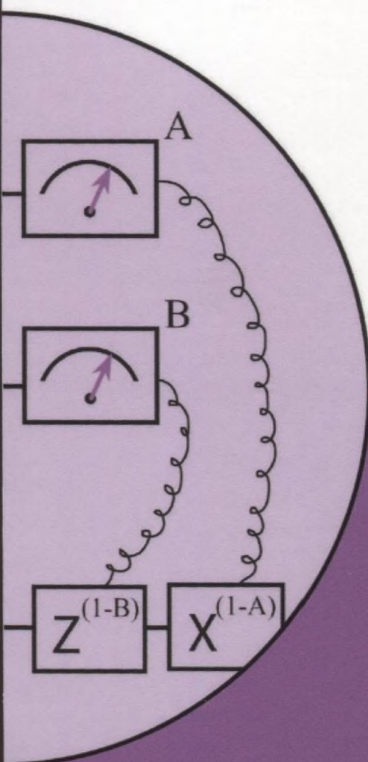


OXFORD MASTER SERIES IN ATOMIC, OPTICAL, AND LASER PHYSICS

Books in this series are written at the final year undergraduate and beginning graduate level, and provide straightforward introductions to key topics in physics today. Background material and applications as well as pointers to more advanced work are included, along with ample tutorial material, examples, illustrations, chapter summaries, and graded problem sets (with some answers and hints).

Quantum information—the subject—is a new and exciting area of science, which brings together physics, information theory, computer science, and mathematics. *Quantum Information*—the book—is based on two successful lecture courses given to advanced undergraduate and beginning graduate students in physics. The intention is to introduce readers at this level to the fundamental, but often rather simple, ideas behind ground-breaking developments including quantum cryptography, teleportation, and quantum computing. The text is necessarily rather mathematical in style, but the mathematics are nowhere allowed priority over the key physical ideas. The aim throughout is to be complete and self-contained but to avoid, as far as possible, lengthy and formal mathematical proofs. Each of the eight chapters is followed by about forty exercise problems with which the reader can test their understanding and hone their skills. These will also provide a valuable resource to tutors and lecturers.

Stephen M. Barnett is Professor of Quantum Optics in the Department of Physics at the University of Strathclyde, Glasgow.



Cover image: A quantum circuit for teleportation (cf. Fig. 6.24)

IN THE SAME SERIES ATOMIC, OPTICAL, AND LASER PHYSICS

Atomic physics

C.J. Foot

Modern classical optics

G.A. Brooker

Laser physics

S.M. Hooker, C.E. Webb

Quantum optics: an introduction

A.M. Fox

STATISTICAL, COMPUTATIONAL, AND THEORETICAL PHYSICS

Statistical mechanics:

algorithms and computations

W. Krauth

Statistical mechanics: entropy, order parameters, and complexity

J.P. Sethna

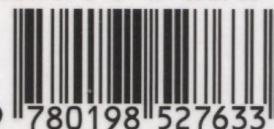
A modern introduction to quantum field theory

M. Maggiore

OXFORD
UNIVERSITY PRESS

www.oup.com

ISBN 978-0-19-852763-3



9 780198 527633

Contents

1	Probability and information	1
1.1	Introduction	1
1.2	Conditional probabilities	2
1.3	Entropy and information	7
1.4	Communications theory	17
	Suggestions for further reading	26
	Exercises	27
2	Elements of quantum theory	31
2.1	Basic principles	31
2.2	Mixed states	37
2.3	Unitary operators	43
2.4	Qubits	45
2.5	Entangled states	49
	Suggestions for further reading	54
	Exercises	55
3	Quantum cryptography	59
3.1	Information security	59
3.2	Quantum communications	66
3.3	Optical polarization	70
3.4	Quantum key distribution	76
	Suggestions for further reading	83
	Exercises	84
4	Generalized measurements	89
4.1	Ideal von Neumann measurements	89
4.2	Non-ideal measurements	92
4.3	Probability operator measures	93
4.4	Optimized measurements	98
4.5	Operations	106
	Suggestions for further reading	111
	Exercises	112
5	Entanglement	115
5.1	Non-locality	115
5.2	Indirect measurements	121
5.3	Ebits and shared entanglement	125
5.4	Quantum dense coding	127

5.5	Teleportation	129
	Suggestions for further reading	136
	Exercises	136
6	Quantum information processing	141
6.1	Digital electronics	141
6.2	Quantum gates	144
6.3	Quantum circuits	148
6.4	Quantum error correction	153
6.5	Cluster states	158
	Suggestions for further reading	160
	Exercises	161
7	Quantum computation	165
7.1	Elements of computer science	165
7.2	Principles of quantum computation	169
7.3	The quantum Fourier transform	175
7.4	Shor's factoring algorithm	181
7.5	Grover's search algorithm	185
7.6	Physical requirements	189
	Suggestions for further reading	191
	Exercises	192
8	Quantum information theory	197
8.1	The von Neumann entropy	197
8.2	Composite systems	202
8.3	Quantitative state comparison	205
8.4	Measures of entanglement	211
8.5	Quantum communications theory	214
	Suggestions for further reading	227
	Exercises	227
A	The equivalence of information and entropy	231
B	Lagrange multipliers	235
C	Stirling's approximation	239
D	The Schmidt decomposition	241
E	Number theory for cryptography	243
E.1	Division properties	243
E.2	Least common multiple and greatest common divisor	243
E.3	Prime numbers	244
E.4	Relatively prime integers and Euler's φ -function	245
E.5	Congruences	245
E.6	Primitive root modulo p	245
E.7	Diffie–Hellman cryptosystem	246
E.8	RSA cryptosystem	246

F Quantum copying	249
G Quantized field modes	253
H Position and momentum eigenstates	257
I Necessary conditions for a minimum-error POM	261
J Complete positivity	263
K Hardy's theorem	269
L Universal gates	271
M Nine- and five-qubit quantum codewords	275
N Computational complexity	277
O The Bernstein–Vazirani algorithm	279
P Discrete Fourier transforms	283
Q An entropy inequality	285
R Quantum relative entropy	287
S The Araki–Lieb inequality	289
T Fidelity for mixed states	291
U Entanglement of formation for two qubits	295
Index	297