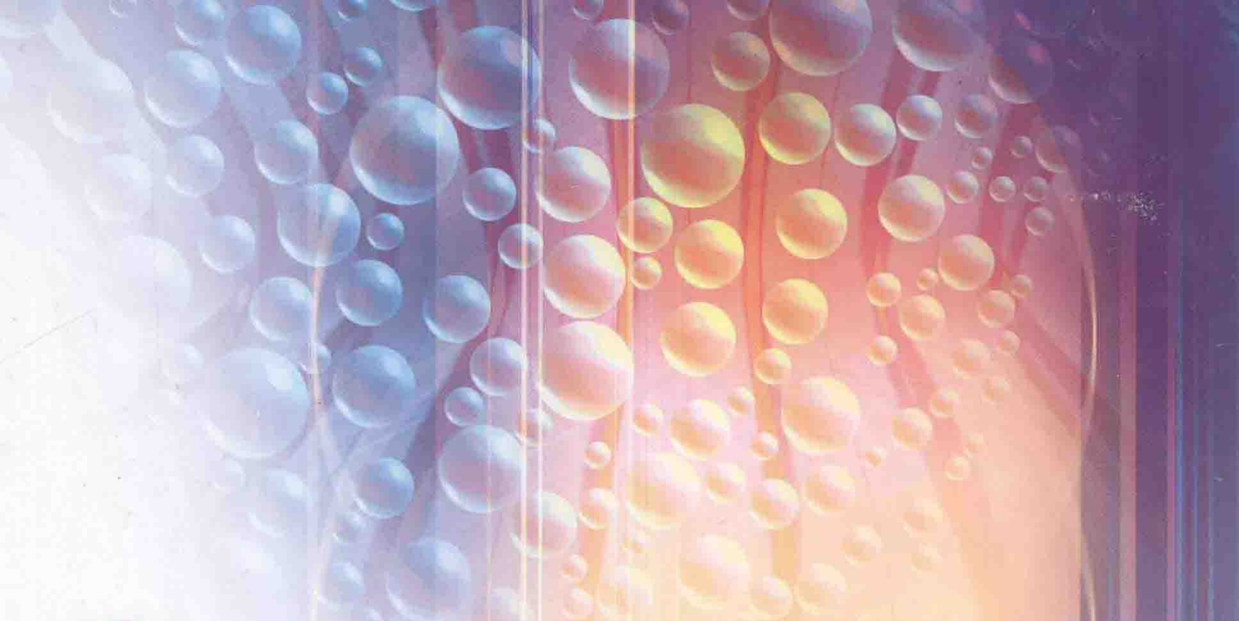

Quantum Computing and Communications

An Engineering Approach

Sándor Imre
Ferenc Balázs

WILEY

Quantum Computing and Communications

An Engineering Approach

Sándor Imre and Ferenc Balázs

Both of
Budapest University of Technology and Economics, Hungary

John Wiley & Sons, Ltd

Copyright © 2005 John Wiley & Sons Ltd,
The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk

Visit our Home Page on www.wileyeurope.com or www.wiley.com

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada M9W 1L1

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0-470-86902-X

Typeset in LaTeX from author-supplied files.
Printed and bound in Germany.
This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

Quantum Computing and Communications

An Engineering Approach

To my father who taught me the way of thinking and to my mother who showed me how to endure to the end.

Sándor Imre

P.S. and of course to my children Sanyus, Marci, Orsi, Andris and their mother Adel.

Preface

Quantum computing and communications is one of the promising new fields of the new millennium. This emerging topic has reached the age when not only physicists and mathematicians but also engineers are becoming more and more interested in it. This book is based on the first semester of a two-semester subject dedicated to Ph.D. students and undergraduates in electrical engineering and computer sciences at Budapest University of Technology and Economics. This first semester covers a thorough basic introduction to the quantum computing world and discusses *quantum-assisted* computing and communications where we use the new paradigm to improve (assist) the performance of classical systems (e.g. searching in an unsorted database or strengthening communication security). In addition the second semester deals with *quantum-based* communications or more precisely with quantum information theory (e.g. channel capacity, error correction). After six semesters of experience we decided to prepare a book which can be used both as lecture notes and as a standalone learning aid for colleagues with engineering practice.

Although there are several good books on the market none of them has been written by engineers to engineers. The so-called 'engineering' approach has minor and major differences compared to materials authored by experts of physics, despite the fact that they cover more or less the same topic. As a simple example for the former category let us mention that engineers use j rather than i to denote the imaginary part of a complex number. However, it is not only conventions that make the discussion different. A presented sophisticated solution of a certain problem and the proof of its correctness do no satisfy an engineer. She/he always wants to know the way leading from the definition of the problem via system model construction and a logical chain of thoughts before reaching an answer to the original problem. If this 'special' viewpoint is omitted, which happens often when the authors are not familiar with engineers' everyday lives, then it always leaves behind a lack of completeness.

Another important aspect for engineers can be summarized as the 'need for practical applications'. A new theory or even an algorithm in itself has limited value. One has to prove and show that their implementation constraints, such as computational complexity, required memory, etc., can be fulfilled in the case of certain practical applications. Furthermore an unambiguous mapping of theoretical and real-life parameters has to be provided.

Finally, working as an engineer means the permanent study of the science of making compromises. The outcome of a design process must be precise enough *and* cheap enough *and* manageable enough *and* etc. and not the most precise *or* the cheapest *or* the most manageable *or* etc. Hence error analysis must always be kept at the focus of investigations.

All these endeavors are motivated by the fact that engineers should learn how to *design* new practical solutions. We always have this philosophy in sight when addressing various topics of quantum computing and communications. Of course we do not want to rank the engineering approach above those of physicists and mathematicians, we simply state that they are different (and not better or worse) in some sense. Due to this fact learning and understanding are much easier if explanations follow the way we are used to.

From a background mathematics' point of view we assumed a typical curriculum of engineers and computer scientists, however, the required math has been summarized in the appendix.

Because of the limited size of this book there are some aspects that are not discussed in detail. We did not devote an individual chapter to the implementation questions of quantum computers. Instead at the end of each chapter in the *Further Reading* we give a state-of-the-art survey of the current status of implementation and provide up-to-date references for interested readers. Philosophical questions and answers are also beyond the scope of this book but we suggest reading e.g. [84, 145] if the reader has time and would like to widen his/her knowledge.

Now we invite the reader to join us on the journey which is going to pass sometimes interesting, sometimes strange and sometimes challenging lands of the quantum world. Do not hesitate, the new world is waiting for you...

The Authors

How to use this book

According to ancient legend, one day Alexander the Great, conqueror of the 'that time known world' (Greece, Egypt, Persia), asked Menaikhmos the famous mathematician to teach him geometry in an easier and faster way. Menaikhmos smiled at this wish and answered: '*Oh king, you ordered your engineers to build distinct roads for citizens and for messengers and the army of the king all around your empire, but there is only one road for all in geometry!*'[1]

Basically we agree with Menaikhmos: learning and understanding quantum computing and communications need time and effort from the reader. However, we are convinced that if the way the knowledge is served is chosen carefully and fits more or less to previous studies of the reader, then high spirits can be maintained at hard portions of the topic. Before starting the voyage we would like to provide some useful hints and tools similarly to seamen who check their maps and compasses before sailing out to sea.

This book can be divided logically into three well-defined parts. Part I explains the basics of quantum computing and communications. As the next level Part II introduces well-known quantum algorithms while advanced readers can find several quantum assisted solutions for state-of-the-art infocom problems in Part III. The book has been equipped with several special features intended to help the reader.

- A dedicated web site can be found at **www.mcl.hu/qcc** containing useful information related to this book.

[1] The same story is known with Euclid and King Ptolemy.

- All the used notations, acronyms and abbreviations are summarized at the beginning of this book so that the reader can turn to this list at any time.

- We prepared plenty of exercises from easy to hard-to-answer types, which allow the reader to test whether his/her understanding is appropriate. The solutions of exercises can be downloaded from the web site of this book or a hard copy can be obtained from the publisher. We do not claim, however, that the proposed solutions are the simplest and shortest ones. Therefore we encourage diligent readers to find more attractive solutions and send them to the authors (imre@hit.bme.hu) in latex format. Appropriate alternatives will be included with the names of their solver into the solutions file.

- As a life belt the reader may find a summary of corresponding mathematical background in the appendices.

- In order to allow the reader to widen his/her knowledge beyond the scope and size of this book a carefully selected large list of references has been attached. We took special care to choose – if possible – such publications that can be accessed electronically on the Internet so that the reader may save time (and money).

- The book is amended with a list containing links to the web pages of the most important leading institutes and laboratories where additional information can be found or even current activities can be followed.

- Obviously the probability of writing a book without any error is fairly low. Therefore we ask the reader to address any comments or found errata to the authors (imre@hit.bme.hu). A regularly updated and downloadable list of errata is maintained on the book's web site.

Acknowledgments

The authors gratefully acknowledge the comments and helpful advice of Prof. Katalin Friedl from the Computer and Automation Research Institute of the Hungarian Academy of Sciences. Pressure from and interest of students attending the corresponding courses were the most motivating issues that helped us keep the deadlines. We thank our boss Prof. Laszló Pap for the permanent encouragement and allowing us enough free time to complete the work.

Certain results introduced in this book were prepared in the frames of OTKA F042590, COST 289.

Acronyms

BER	Bit Error Ratio
BPSK	Binary Phase Shift Keying
CAC	Call Admission Control
CDMA	Code Division Multiple Access
DES	Data Encryption Standard
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DNS	Domain Name Server
DS-CDMA	Direct Sequence-Code Division Multiple Access
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
HLR	Home Location Register
GSM	Global System for Mobile communications
GUT	Great Unified Theory
IETF	Internet Engineering Task Force
IP	Internet Protocol

LSB	Least Significant Bit
MSB	Most Significant Bit
pdf	probability density function
MAC	Medium Access Control
MAP	Maximum *A Posteriori*
ML	Maximum Likelihood
MLS	Maximum Likelihood Sequence
MUD	Multiuser Detection
NMR	Nuclear Magnetic Resonance
PG	Processing Gain
QC	Quantum Computation/Quantum Computing
QFT	Quantum Fourier Transform
QMUD	Quantum-based Multiuser Detection
SDM	Space Division Multiplexing
SDMA	Space Division Multiple Access
SIM	Subscriber Identity Module
SRM	Square-Root Measurement
SS	Spread Spectrum
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
UMTS	Universal Mobile Telecommunication System
URL	Uniform Resource Locator
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
WWW	World Wide Web
$\tilde{a}$	Measured/estimated value of variable a
$\breve{a}$	Technical constraint/demand for variable a, e.g. a must be less than $\breve{a}$
$\forall$	for all
j	$\sqrt{-1}$
$\vert\cdot\rangle$	Vector representing a quantum state, its coordinates are probability amplitudes
$\mathbf{x}$	Traditional vector, e.g. $\mathbf{x} \in \{0, 1\}^n$ refers to the vector representation of n-bit binary numbers

$\lvert\cdot\rangle_N$	State of an N-dimensional quantum register, i.e. the qregister contains $n = \mathrm{ld}(N)$ qbits
$\lvert\mathbf{0}\rangle$	Special notion for the more than one-qbit zero computational basis vector to distinguish it from the single qbit $\lvert 0\rangle$
U	Operator
$U^{\otimes n}$	n-qbit (2^n-dimensional) operator
$\mathbf{U}$	Matrix of operator U
$P(\alpha)$	Phase gate with matrix $\begin{bmatrix} 1 & 0 \\ 1 & e^{j\alpha} \end{bmatrix}$
H	Hadamard gate with matrix $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
X	Pauli-X (bit-flip) gate with matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Y	Pauli-Y gate with matrix $\begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}$
Z	Pauli-Z (phase-flip) gate with matrix $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
$\otimes$	Tensor product; this notation is often omitted, it is used only if the tensor product operation has to be emphasized
$\oplus$	Modulo 2 addition
$(\cdot)^*$	Complex conjugate
$\langle\cdot\vert\cdot\rangle$	Inner product
$\lvert\cdot\rangle\langle\cdot\rvert$	Outer product
$\dagger$	Adjoint
$(\cdot)^T$	Transpose
$*$	Convolution
$\triangleq$	Definition
$\equiv$	Equivalence
$\wedge$	Logical AND operator
$\vee$	Logical OR operator
$\vert$	Logical IF operator
$\mathbb{Z}$	Set of integer numbers

$\mathbb{Z}_2 \equiv \{0,1\}$	Set of binary numbers
$(\mathbb{Z}_2)^n \equiv \{0,1\}^n \equiv \{0,1\}^n$	Set of n-bit binary numbers
$\mathbb{Z}_N \equiv \{0,1,\ldots,N{-}1\}$	Set of positive integer numbers between 0 and $(N-1)$, i.e. set belonging to the modulo N additive group
$\mathbb{Z}^+$	Set of natural numbers, i.e. positive integer numbers
$\mathbb{Z}^-$	Set of negative integer numbers
$\mathbb{Z}_p^*$	Set of positive integers belonging to the modulo N multiplicative group
$\mathbb{C}$	Set of complex numbers
$\mathrm{ld}(\cdot)$	*Logarithmus dualis*, $\log_2(\cdot)$
$\lceil \cdot \rceil$	Smallest integer greater than or equal to a number
$\lfloor \cdot \rfloor$	Greatest integer less than or equal to a number
$\lfloor \cdot \rceil$	Rounds to the nearest integer
$\gcd(a,b)$	Greatest common divisor of a and b
$\delta(x-x_0)$	Dirac function, it is 1 if its argument equals zero i.e. $x = x_0$ else it is zero everywhere
$\mathbb{E}(x)$	Expected value of random variable x
$f(x)$	Function continuous in x
$f[x]$	Function discrete in x
$\Re(x)$	Real part of complex number x
$\Im(x)$	Imaginary part of complex number x
$\#(\cdot)$	Number of, counts the occurrence of its argument
Thin line	Quantum channel
Thick line	Classical channel

Part I

Introduction to Quantum Computing

Contents

Part I Introduction to Quantum Computing