

Michael Brooks (Ed.)

.....

QUANTUM COMPUTING AND COMMUNICATIONS

**No in-depth knowledge of
quantum mechanics needed**

**all you need to know
about the core technology**

**Includes contributions from researchers at: the
Los Alamos National Laboratory, the Jet Propulsion
Laboratory, IBM, Hewlett-Packard, and more.**



Springer

Michael Brooks (Ed.)

Quantum Computing and Communications

TP38
B873



Springer

Michael Brooks, DPhil, BSc (Hons)

ISBN 1-85233-091-0 Springer-Verlag London Berlin Heidelberg

British Library Cataloguing in Publication Data

Quantum computing and communications

1. Quantum computers 2. Telecommunication – Technological innovations

I. Brooks, Michael

621.3'9'81

ISBN 1852330910

Library of Congress Cataloging-in-Publication Data

Brooks, Michael, 1970-

Quantum computing and communications / Michael Brooks.

p. cm.

ISBN 1-85233-091-0 (alk. paper)

1. Quantum computers. 2. Optical communications. I. Title.

QA76.889.B76 1999

99-19975

004.1-dc21

CIP

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

© Springer-Verlag London Limited 1999

Printed in Great Britain

The use of registered names, trademarks etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Typesetting: Camera ready by editor

Printed and bound by the Athenæum Press Ltd., Gateshead, Tyne & Wear

34/3830-543210 Printed on acid-free paper

Quantum Computing and Communications

Springer

London

Berlin

Heidelberg

New York

Barcelona

Hong Kong

Milan

Paris

Santa Clara

Singapore

Tokyo

Preface

We have, in the last few years, radically improved our grasp of the quantum world. Not just intellectually, either: our ability to manipulate real quantum systems has grown in equal measure with our understanding of their fundamental behavior. These two shoots - the intellectual and the practical harnessing of the quantum world - have sprung up at a time when a third shoot - information processing - has also been experiencing explosive growth. These three shoots are now becoming intertwined. Twisted together, our understanding of information processing, quantum theory and practical quantum control make for a strong new growth with enormous potential.

One must always be careful about using the word 'revolutionary' too readily. It is, however, difficult to find another word to describe the developments that have been taking place during the second half of the 1990s. In 1986 Richard Feynman, the visionary professor of physics, made a very interesting remark:

"...we are going to be even more ridiculous later and consider bits written on one atom instead of the present 1011 atoms. Such nonsense is very entertaining to professors like me."

It is exceptionally unfortunate that Feynman did not live to see this 'nonsense' fully transformed into reality. He, more than anybody, would enjoy the fact that it is now possible to write information onto an atom, or indeed an ion or a photon. Furthermore, theorists and experimentalists have shown that this information can be processed and transmitted in ways that allow a seemingly absurd degree of power and control over the information. It is now possible to use one quantum particle to influence another particle that it has never met. It is possible to transmit information encoded in a single photon through the air and, on detection, to verify whether that information has been read by anyone else. Experiments are just beginning to string together quantum bits of information that promise massively parallel computing power, far beyond anything that classical machines can manage. In short, we are on the verge of the quantum information revolution.

There could have been no better time for the European Commission to fund a Pathfinder Project in Quantum Computing and Communications* to look into this subject. This Project, which was carried out with the financial support of the Commission, within the frame of the Esprit LTR Working Group 27126 QCEPP, facilitated the gathering and organization of a large amount of useful material about the field; I have freely and extensively used this material in this book. It is reproduced here with the kind permission of the Commission, but it does not necessarily reflect the views of the Commission.

It has been a great privilege for me to spend the last year being so closely involved with the Pathfinder Project. Some of the members of the Project's Working Group have laid the theoretical or experimental foundations in important areas of this field; I have taken great pleasure in working alongside them, and am grateful for all their assistance in drafting parts of this volume. As a journalist I often have to skim the surface of a subject, taking in its essence, but with little time to consider its implications or to examine its fundamental basis. My involvement with the Pathfinder Project has enabled me to investigate this fascinating area to my heart's content, often learning directly from those who have originated the concepts. I am grateful to the European Commission, and to all of the Working Group for their input and advice. However, I take full responsibility for any errors or omissions that have crept into this volume.

Finally, I would like to acknowledge the important role played by Brian Oakley, Chairman of the Pathfinder Project, and Charles Ross, its Honorary Secretary. Without their seemingly boundless energy and enthusiasm, it is likely that little of this material would ever have been gathered.

Michael Brooks, January 1999

* The term 'Quantum Information Processing' (QIP) is also used to describe Quantum Computing and Communications throughout this book.

Contents

Section I	A Wide Perspective	
Chapter 1	Introduction	
	<i>Michael Brooks</i>	3
	1.1 Exploiting the Quantum World	3
	1.2 Historical Background	5
	1.3 Worldwide Efforts in QCC	6
Chapter 2	The Fundamentals of Quantum Information	
	<i>Michael Brooks</i>	9
Chapter 3	Quantum Computer Science	
	<i>Michael Brooks</i>	17
	3.1 Introduction	17
	3.2 Algorithms and the Complexity Problem	18
	3.3 The Quantum Computation Answer	19
	3.4 Quantum Algorithms	20
	3.5 Quantum Logic Gates and Networks	21
	3.6 Obstacles	23
	3.7 A Workable Solution: Quantum Error Correction	23
	3.8 Conclusions	24
Chapter 4	Experimental Realizations	
	<i>Michael Brooks</i>	27
	4.1 Introduction	27
	4.2 Trapped Ions	27
	4.3 Nuclear Magnetic Resonance	29
	4.4 Cavity Quantum Electrodynamics	30
	4.5 Quantum Dots	31
Chapter 5	Optical Technologies for Quantum Computing and Communications	
	<i>Michael Brooks</i>	33
	5.1 Introduction	33
	5.2 Using the Quantum Nature of Light	34
	5.2.1 Potential	34
	5.2.2 Problems	34

5.3	Quantum Noise in Optical Communications	35
5.4	Generic Technologies in Quantum Communications	35
5.4.1	Nonlinear Optics	36
5.4.2	Cavity Quantum Electrodynamics	36
5.5	Operations Performed on Optical Signals	37
5.5.1	Signal Generation	37
5.5.2	Detection	38
5.5.3	Attenuation	38
5.5.4	Distribution	39
5.5.5	Amplification	39
5.6	Conclusions: Towards the Second Generation	40
Chapter 6	Applications	
	<i>Michael Brooks</i>	43
6.1	Introduction	43
6.2	Emerging Technologies	44
6.2.1	Quantum Cryptography	44
6.2.2	Quantum Repeaters	44
6.2.3	Quantum Simulators	45
6.2.4	Metrology and Few Photon Applications	46
6.3	Conclusions: Measuring Progress	47
Chapter 7	A Note on the Question of Scaling: Decoherence and Error Correction	
	<i>Michael Brooks</i>	49
Section II	Personal Perspectives	
Chapter 8	Solid State Quantum Computation: Prospects, Proposals, and Prejudices	
	<i>Bruce Kane, University of New South Wales, Sydney, Australia</i>	53
Chapter 9	Information is Physical, But Slippery	
	<i>Rolf Landauer, IBM, Yorktown Heights</i>	59
Chapter 10	Nanocircuitry, Defect Tolerance and Quantum Computing: Architectural and Manufacturing Considerations	
	<i>R. Stanley Williams, Quantum Structures Research Initiative, Hewlett-Packard Laboratories</i>	63
Chapter 11	Quantum Computing and NMR	
	<i>Jonathan A. Jones, University of Oxford</i>	71
Chapter 12	Quantum Networks and Quantum Algorithms	
	<i>Vlatko Vedral, University of Oxford</i>	79

Chapter 13	Quantum Cryptography <i>Richard Hughes, Physics Division, Los Alamos National Laboratory</i>	87
Section III	A Perspective for the Future	
Chapter 14	Realizing the Potential of Quantum Information Processing <i>Michael Brooks</i>	97
	14.1 Prospects for Quantum Computing	97
	14.2 Prospects for Special Applications	98
	14.2.1 Quantum Simulation.....	98
	14.2.2 Limited Qubit and Reduced-Noise High Precision Applications	98
	14.2.3 Secure Communications	99
	14.3 Meeting The Needs of the QIP Field.....	99
	14.3.1 The Need for Academic Focus	100
	14.3.2 The Need for Industrial Focus	100
	14.3.3 The Need for Awareness	101
Chapter 15	The Role of Europe <i>Michael Brooks</i>	103
	15.1 The Pioneering Stage.....	103
	15.2 Today.....	104
	15.2.1 Multi-Disciplinary or Trans-Disciplinary Nature of the Community	104
	15.2.2 The Numbers Involved	104
	15.2.3 The Geographical Spread	105
	15.2.4 The Industrial Scene	105
	15.2.5 Summary of the European Scene.....	106
Chapter 16	Quantum Computing and Communications: A View from the USA <i>Colin P. Williams, Jet Propulsion Laboratory, California Institute of Technology</i>	107
	16.1 Introduction	107
	16.2 What Works Well	108
	16.3 What Does Not Work So Well	108
	16.4 NASA/JPL.....	109
	16.5 Lessons Learned from Experience with NASA.....	111
	16.6 Opportunities for Europe.....	111
	16.7 Commercialization.....	112
	16.8 Recommendations	113
	16.8.1 Programmatic Recommendations.....	113
	16.8.2 Technology Solutions.....	113
	16.8.3 Quantum Computer Science	113
	16.8.4 Education and Training	114

Section IV Reference materials

Chapter 17 Quantum Information Processing:

A Brief Overview of Recent Advances

<i>Antonella Karlson, StarLab, Riverland nv</i>	119
17.1 Introduction	119
17.2 The Underlying Physical System.....	120
17.2.1 Quantum Bits and Quantum Superpositions.....	120
17.2.2 Quantum Gates	120
17.2.3 Quantum Parallelism	121
17.3 Fundamentals of Quantum Information	121
17.3.1 Entanglement.....	121
17.3.2 Quantum Dense Coding.....	122
17.3.3 Quantum Teleportation.....	123
17.4 Quantum Cryptography.....	123
17.4.1 Standard Cryptosystems	123
17.4.2 Quantum Key Distribution	124
17.5 Quantum Computing	125
17.5.1 Quantum Algorithms	125
17.5.2 Grover's Search Algorithm.....	126
17.5.3 Period Finding and Shor's Factorization Algorithm	127
17.5.4 Minimum Requirements for any Quantum System to Be a Quantum Computer	128
17.5.5 Simulation of Other Quantum Systems	128
17.6 Quantum Decoherence	129
17.6.1 What is Decoherence?	129
17.6.2 Quantum Error Correction.....	130
17.7 Experimental Realizations	131
17.7.1 Systems with Few Degrees of Freedom	131
17.7.2 Macroscopic Systems	132
17.8 Conclusions	132

Chapter 18 Categories and Definitions 137

18.1 Definitions and Glossary of Terms.....	137
18.1.1 Definition of Quantum Computing and Communications	137
18.1.2 Sub-Sector Definitions	138
18.1.3 Some Relevant Terms.....	140
18.2 The Disciplines that Contribute to Quantum Information Processing.....	142

Appendix A The Pathfinder Project 145

A.1 Pathfinder Activities.....	145
A.1.1 Newsletters	145
A.1.2 Database of Active Individuals and Organizations.....	146
A.1.3 Taxonomy of the Subject.....	146
A.1.4 Helsinki Conference	146

A.1.5	QIP Report.....	147
A.2	Pathfinder Project Partners	147
Appendix B	A Preliminary QIP Roadmap	149
Index	151

Section I

A Wide Perspective

An examination of the whole field of Quantum Computing and Communications requires some decisions to be taken about where to draw divisions between the various subject areas; the placement of these divisions is a subject that could sustain infinite debate. For the purposes of this volume, the field has been split into four main fields, each covered by a chapter in this section. These four chapters are preceded by an introduction to the subject of quantum information, and are followed by a note on the problems of decoherence.

Chapter 1

Introduction

Michael Brooks

1.1 Exploiting the Quantum World

Civilization has always advanced as people discovered new ways of exploiting various physical resources, such as materials, forces and energies. In the twentieth century, information was added to the list when the invention of computers allowed complex information processing to be performed outside human brains. The history of information technology has involved a sequence of changes from one type of physical realization to another; from gears to relays to valves to transistors to integrated circuits and so on. Now, developments of quantum information processing have reached the stage where one bit of information can be encoded in quantum systems, for example using two different polarizations of light, or two different electronic states of an atom. Matter on this scale obeys the laws of quantum mechanics, which are quite different from the classical laws followed by 'conventional' technologies. If an atom is used as a physical bit then quantum mechanics shows that apart from the two distinct electronic states the atom can be also prepared in a coherent superposition of the two states. This means that the atom is both in state 0 *and* state 1. In general, a quantum two-state system, called a quantum bit or a qubit, can be prepared in a superposition of its two logical states 0 and 1. Thus one qubit can encode at a given moment of time both 0 and 1. Strings of qubits in superposition states can be 'entangled' together to simultaneously encode, in principle at least, vast amounts of information.

Entanglement is one of the distinct properties of quantum systems (together with quantum superposition and probabilistic measurement among others) that makes quantum information processing so different from classical information technology. This phenomenon refers to the joint state of two or more quantum systems and describes correlations between them that are much stronger than any classical correlations. Entangled states offer the possibility to encode information in a completely new way. Let us assume we have two qubits and we

want to encode two bits of information. The straightforward approach is to encode one bit of information onto each qubit separately. But using entangled states it is possible to do it in such a way that neither of the two qubits carries any well defined information on its own: all the information is encoded in their joint properties. Entanglement makes possible quantum teleportation, quantum error correction, quantum dense coding, etc. It is closely linked to the issue of non-locality in quantum theory.

This means that quantum technology, potentially, can offer much more than cramming more and more bits on to silicon and multiplying the clock-speed of microprocessors. It can support entirely new kinds of computation with qualitatively new algorithms based on quantum principles. It also offers very significant improvements - in speed, security and quality - in the technologies of information transfer.

Considering quantum computation first, it has been shown that quantum effects could allow the creation of a register of qubits. Such a register composed of three qubits, for example, can simultaneously represent the numbers from binary 000 to binary 111 - i.e. the decimal numbers 0 to 7. Computations performed on these entangled qubits thus have the potential to process simultaneously, offering new and exciting possibilities in information processing.

Algorithms have now been developed which show how quantum computation could lead to enormous advantages over classical computation, accomplishing tasks that are impossible, or impossibly time-consuming, to any classical computer - no matter what its clock speed or processing power. That list of tasks includes code-breaking factorization operations, which makes the development of quantum computation a matter of great importance to any institutions involved with matters of national or financial security. Practical implementation of these ideas is not without its very considerable difficulties and there can be no certainty that it will ever prove possible to build a useful quantum computer. But solutions to existing problems are continually being discovered and analyzed. Whatever the end result, the journey towards the implementation of quantum computation is already yielding valuable spin-off technologies and applications in fields such as communication security.

Entangled qubits are also at the heart of quantum communications, a field whose development is of fundamental interest to financial institutions and national security agencies. Research has demonstrated that measuring the properties of one of a pair of entangled photons would lead to an instantaneous change in the properties of the other half of the entangled pair, however far it was from the measured photon. Development of this work has taken entirely secure communications, using information encoded in entangled photon pairs, to a near-marketable development stage. The use of quantum effects are enabling new and extremely useful techniques to be discovered and implemented.

1.2 Historical Background

The subject of Quantum Information Processing is not new. In one sense the work stems from the recognition of the quantum nature of radiation by Max Planck in 1900, and the equation derived by Erwin Schrödinger in 1926 which provided a mathematical basis for quantum mechanics. This showed that if a quantum system was to operate as a computer it had to be capable of operating reversibly. The history of twentieth century computing, stemming from Turing's work in 1936, is based on a model of a computer that is not reversible. The super-computer of today is essentially of the same nature of machine as the early computers of the 1940s, as is the PC; they differ in memory and operating speed but not in fundamental operations. It has been recognized for many years that they have some practical limitations; for example in not being able to generate a truly random set of numbers; and not being able to perform certain calculations such as those that can be solved for smaller numbers, but at some point become too lengthy for any current or conceivable computer operating on the current classical principals. As the semiconductor switches, on which modern computers are based, have become smaller and smaller, it has become apparent that at some stage, probably within the next 10 to 20 years, the number of atoms in the structures will become so small that the classical laws will have to be replaced by the laws of quantum physics if their behavior is to be understood and predicted.

Perhaps the key breakthrough in quantum computation came in 1973 when Charles Bennett (IBM, Yorktown Heights) showed that a reversible Turing machine was a theoretical possibility. Then, in 1980, Paul Benioff (at that time at Argonne National Laboratory) formulated a reversible Turing machine, which could read, write and shift using quantum mechanical interactions. In 1982, Richard Feynman suggested that a quantum computer could simulate a quantum system efficiently, in a way that no classical computer could. And then, in 1985, David Deutsch (Oxford University) described how the quantum Turing machine might be built, in principle, and how the 'superposition' of 0s and 1s simultaneously led to quantum parallelism. During the 1980s, work was developing on ways of constructing the necessary quantum gates, and then experimental work on a variety of approaches to handling a limited number of quantum bits started in the 1990s. The problem of decoherence seemed to create a practical limitation on the use of quantum information processing, but work at various centers in the 1990s has shown how this might be overcome by error correction techniques. A very considerable boost to the practical interest in the subject came in 1994 when Peter Shor (then at Bell Labs) demonstrated an algorithm which showed how the superpolynomial time process for factorizing a large number on a classical computer could be reduced to an efficient polynomial time process on a quantum computer, a result of considerable interest to the cryptography community.

And amongst the algorithms for quantum computers that followed this breakthrough, Lov Grover developed in 1996 an algorithm that would reduce the time required to find a single item in an unsorted list in the square root of the time