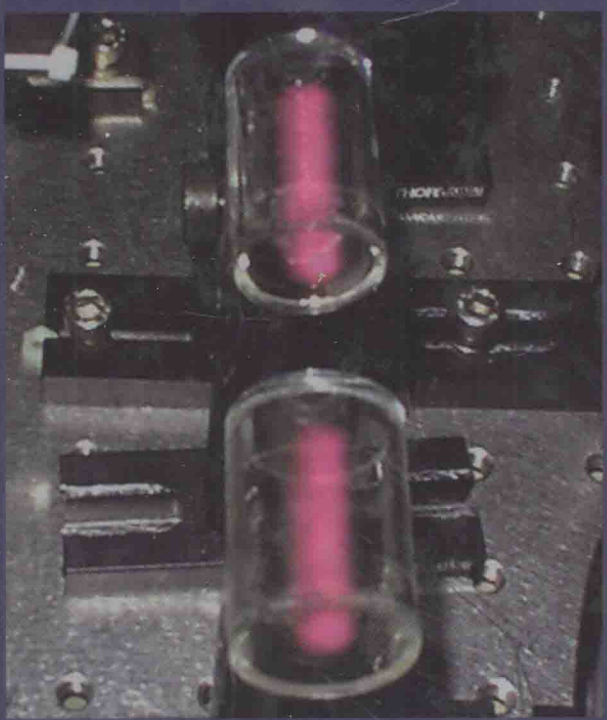
Quantum Information with Continuous Variables

Edited by

Samuel L. Braunstein and Arun K. Pati



Kluwer Academic Publishers

Quantum Information with Continuous Variables

Edited by

SAMUEL L. BRAUNSTEIN
School of Informatics,
University of Wales, Bangor, United Kingdom

and

ARUN K. PATI
Institute of Physics, Orissa, India
and
Theoretical Physics Division,
BARC, Mumbai, India

KLUWER ACADEMIC PUBLISHERS
DORDRECHT / BOSTON / LONDON

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN 1-4020-1195-4

Published by Kluwer Academic Publishers,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

Sold and distributed in North, Central and South America
by Kluwer Academic Publishers,
101 Philip Drive, Norwell, MA 02061, U.S.A.

In all other countries, sold and distributed
by Kluwer Academic Publishers,
P.O. Box 322, 3300 AH Dordrecht, The Netherlands.

Printed on acid-free paper

Cover illustration:
reprinted with permission from Nature [Nature 413, 400–403 (2001)]
Copyright (2001) Macmillan Publishers Ltd.

Printed in the Netherlands.

QUANTUM INFORMATION WITH CONTINUOUS VARIABLES

Dedicated to
Netta, Rashmi
and our parents

Preface

Quantum information has become a flagship of interdisciplinary research in recent years, sweeping physicists from a variety of disciplines, as well as computer scientists and mathematicians. It all started with the realization that the principles of quantum theory open new avenues of information processing capabilities which are unavailable in the classical world. Primarily, the discovery that quantum entanglement can be put to use has led to a watershed of activity towards the eventual implementation of quantum computation and quantum cryptography. This was naturally accompanied by efforts to place fundamental quantum limits on information processing. Today, real-world applications of quantum-information technologies seem closer and more tangible than ever.

The field of quantum information has typically concerned itself with the manipulation of discrete systems such as quantum bits, or "qubits." However, many quantum variables, such as position, momentum or the quadrature amplitudes of electromagnetic fields, are continuous. Quantum information processing with continuous variables is the subject of this volume.

Initially, quantum information processing with continuous variables seemed daunting at best, ill-defined at worst. The first real success came with the experimental realization of quantum teleportation for optical fields. This was soon followed by a flood of activity, to understand the strengths and weaknesses of this type of quantum information and how it may be processed. The next major breakthrough was the successful definition of a notion of universal quantum computation over continuous variables, suggesting that such variables are as powerful as conventional qubits for any class of computation.

In some ways continuous-variable computation may not be so different than qubit-based computation. In particular, limitations due to finite precision make quantum floating-point operations, like their classical counterparts, effectively discrete. Thus we might expect a continuous-variable quantum computer to perform no better than a discrete quantum computer. However, for some tasks continuous-variable quantum computers are nonetheless more efficient. Indeed,

in many protocols, especially those relating to communication, they only require *linear* operations together with classical feed-forward and detection. This together with the large bandwidths naturally available to continuous (optical) variables appears to give them the potential for a significant advantage.

Noise is the Achilles' heel of quantum computation, and continuous variables are even more susceptible to noise than discrete variables. Since an uncountably infinite number of things can go wrong with a continuous variable, error correction protocols might be expected to require infinite redundancy. Fortunately, continuous-variable error correction routines exist and require no greater redundancy than protocols for discrete variables. With the problem of noise potentially reduced to manageable proportions, many other hurdles persist, and many more exciting questions remain open. Quantum information with continuous variables continues to be a dynamic and exciting field of ongoing research and development.

In this volume we present important developments in the area of quantum information theory for continuous-variable systems from various leading researchers in the field. Several introductory chapters lay out some of the basics of quantum information theory in terms of the more usual qubits. Each introduction is followed by generalizations to continuous variables. In addition to chapters on quantum computation and quantum teleportation, we have included work on quantum dense coding, quantum error correction, some simple attempts at generalizing quantum algorithms and technologically promising work on quantum cryptography and quantum memory. These results apply to any collection of continuous variables, including phonons, photons, Josephson Junction circuits, Bose-Einstein condensates, etc. Finally, the underlying nature of continuous quantum information is investigated in chapters on quantum cloning and quantum entanglement.

At this juncture, we express our gratitude to Kluwer Academic for allowing us to bring this work to light. We hope that this book offers the reader a rigorous introduction to continuous-variable quantum information and some thought-provoking snapshots of recent developments. We sincerely thank all the authors for their contributions. A.K.P. would especially like to express his thanks to Prof. R. K. Choudhury, Director of the Institute of Physics, in Orissa, India, for his encouragement. Finally, both authors appreciate the support provided by the University of Wales, Bangor, throughout this endeavor.

SAMUEL L. BRAUNSTEIN

ARUN K. PATI

About the Editors

Samuel L. Braunstein is a Professor at the University of Wales, Bangor, where he has taught since 1997. He is a recipient of the prestigious Royal Society-Wolfson Research Merit Award and was awarded the honorary title of 2001 Lord Kelvin Lecturer. Before joining the University of Wales, he held a German Humboldt Fellowship (spent at the University of Ulm). He is editor of two books *Quantum Computing* and *Scalable Quantum Computing* and serves on the editorial board of the journal *Fortschritte der Physik*. He has initiated and is a Founding Managing Editor of *Quantum Information and Computation* – the first journal dedicated specifically to this field.

Arun K. Pati is a Visiting Scientist in the Institute of Physics, Bhubaneswar, Orissa, India since 2001. He has been a Scientific Officer in the Theoretical Physics Division, BARC, Mumbai since 1989. His research interests include Quantum Theory, Foundations, and Quantum Information and Computation. He is a recipient of the Indian Physics Association NSS Memorial Award for the year 2000 and the Indian Physical Society Award for Young Physicists for the year 1996. He was an Associate of the Indian Academy of Science, Bangalore from 1998-2001. Presently he is an Associate at the Center for Philosophy and Foundation Science, New Delhi and an Honorary Research Fellow at the University of Wales, Bangor, United Kingdom.

Contents

I
QUANTUM COMPUTING

Chapter 1

QUANTUM COMPUTING WITH QUBITS

Samuel L. Braunstein
Informatics, Bangor University, Bangor LL57 1UT, United Kingdom
schmuel@sees.bangor.ac.uk

Arun K. Pati
Institute of Physics, Bhubaneswar-751005, Orissa, INDIA
Theoretical Physics Division, BARC, Mumbai, INDIA
akpati@iopb.res.in

Abstract We briefly give an introduction to quantum computing with qubits.

This book will introduce the reader to the area of quantum information processing with continuous variables. However, to put it into some context with the "conventional" approach to quantum computing with qubits we shall give a brief introduction to its basic principles skipping all details. Briefly, we will touch on notions of bits, qubits, quantum parallelism, and quantum algorithms such as the Deutsch-Jozsa, the Shor factoring problem, and the Grover quantum search.

Quantum information theory is a marriage between two scientific pillars of modern science, namely, quantum theory and classical information theory. Quantum theory as developed by Planck, Einstein, Schrödinger, Dirac, Heisenberg and many others in the early part of the last century is one of the finest theories that explains phenomena ranging from molecules to electrons, protons, neutrons and other microscopic particles. The mathematical theory of classical information was put forth by Shannon in the mid part of the last century. Whatever revolution in information technology we see at present is partly due to the ground breaking work by Shannon, Turing, Church and others.

When the ideas from information theory are carried over to quantum theory there emerges a revolution in our ability to process information. Ultimately, the basic ways of expressing and manipulating information require physical states

S.L. Braunstein and A.K. Pati (eds.), Quantum Information with Continuous Variables, 3–8.

and processes. In quantum theory we know that physical processes are fundamentally different than those of classical physics. Therefore manipulation of information based on quantum physical processes has also to be fundamentally different than their classical counterparts. It was first realised by Feynman that simulating quantum systems on a classical computer would be very inefficient [1]. However, if one utilizes quantum systems than one can do much more. For this reason, quantum information is distinguished from conventional classical information.

1. QUANTUM COMPUTATION

The physics of information and computation are intimately related. Information is encoded in the state of a physical system, whereas computation involves the processing of this information through actions on the physical system. This processing must obey physical law. Therefore, the study of information and computation are linked through the study of underlying physical processes. If the physical processes obey the rules of classical physics, the corresponding computation is dubbed "classical." If on the other hand, the underlying processes are subjected to quantum mechanical rules, the resulting computation will be called "quantum computation." The logic that lies at the heart of conventional computers and quantum computers is therefore fundamentally different. Quantum computation is a particular way of processing information which utilizes the principles of the linearity of quantum mechanics, out of which comes quantum superposition, quantum entanglement and quantum parallelism. This was first suggested by Deutsch [2].

In a conventional computer information is stored as binary digits (bits) usually (logically) labeled 0 and 1. To represent a bit, one may use any physical system that one likes provided it allows two distinct states. Two bits of information can be stored in any system allowing $2^2 = 4$ possible distinct states. Similarly, n bits of information may be represented in any system capable of providing 2^n distinct states. In each case, there is only *one* configuration at a time of the logical bits (e.g., 110 for 3 bits). Information stored in these binary digits can be manipulated using elementary logic gates that obey Boolean algebra. For example, in a conventional classical computer one can manipulate information using sequence of logical operations such as AND, OR, NOT, and XOR gates. These gates may be built into circuits constructing any possible Boolean functions [3].

1.1 QUBITS

Let us represent a bit, 0 or 1, by saying that the spin of a neutron is up or down, or we could say an atom is in ground or in an excited state, or a photon is horizontally or vertically polarized. All these systems are examples

of two-state quantum systems because the two states are orthogonal and hence logically distinct from each other. When a quantum system is in a given basis state it may be said to carry classical information. However, quantum theory also allows states which are in linear superpositions of these basis states. If we use the logical label for each of the basis states then the most general pure quantum state for a "two-state" system is given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ , \tag{1.1}$$

for some complex numbers α and β which satisfy $|\alpha|^2 + |\beta|^2 = 1$. According to Dirac a quantum state ψ is denoted by a "ket" $|\psi\rangle \in \mathcal{H} = \mathbb{C}^2$ (a two-dimensional Hilbert space). Such a system contains a quantum bit or "qubit" of information [4].

A single qubit allows two inputs to be stored (and possibly processed) simultaneously. As we add more qubits the number of simultaneous possibilities grows very quickly. For example, for two qubits, which have logically distinct states labeled by $00, 01, 10$ and 11 the most general state may be written as a superposition of these four possibilities

$$\alpha|00\rangle + \beta|01 + \delta|10\rangle + \gamma|11\rangle \in \mathcal{H} = \mathbb{C}^4 \ . \tag{1.2}$$

For n qubits with 2^n possible distinct logical basis states the most general pure state will take the form of a simultaneous superposition of this exponential number of possibilities, such as

$$\sum_{x=0}^{2^n-1} c_x|x\rangle \ . \tag{1.3}$$

This ability for quantum states to simultaneously represent (and process) an exponential number of "logical states" demonstrates the fundamental difference between classical and quantum computers.

In the case of a composite system of two or more qubits (or any kind of subsystems) as seen in Eq, (1.3), the result of this superposition can give rise to *quantum entanglement* (inter-twinedness). If a pure composite state cannot be written as a product of individual states for each subsystem then it is an entangled state. The word entanglement neatly encapsulates the novel non-classical correlations accessible to quantum systems, yet which cannot be described within any local realistic model since they allow for the violation of Bell inequalitiesinequality,Bell [5]. What this means is that one cannot attribute definite properties to the individual subsystems of an entangled state. Charlie Bennett's metaphor for a pair of entangled particles is that they are to be likened to a pair of lovers. If a pair of particles are entangled, then a measurement of one, will, in some sense, instantaneously affect the other no matter how far apart they lie.

2. QUANTUM PARALLELISM AND ALGORITHMS

It is possible to design new types of logic gates, generalizing those that work for classical bits, that act on qubits. These quantum gates may also be combined into circuits in such a way as to allow the most general (unitary) transformations between quantum states. We may think of these circuits as performing particular quantum algorithms for a given input. Because more general transformations than simple Boolean functions are available, quantum superpositions may be created using these quantum circuits. This allows for the ability of quantum computers to perform many computational tasks in parallel. Further, because the potential amount of parallelism grows exponentially with the number of qubits, this feature cannot be efficiently simulated in any conventional computer, no matter how parallel its architecture.

To illustrate quantum parallelism, imagine that we had access to a black box that computes a given function $f(x)$ from an input x of n qubits ($x = 0, 1, \ldots, 2^n$). Quantum mechanically because one can create a superposition of all inputs, one could perform all $N = 2^n$ function evaluations in a single go. Classically, this would require the N separate function evaluations. In particular, one can start by preparing a "register" of n qubits in an equal superposition of all possible bit strings given by

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \ . \tag{1.4}$$

Further, we suppose that the function f is evaluated by some unitary operation U_f acting via [2]

$$U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle \ , \tag{1.5}$$

on any given input x, with the input located in the first register and the output stored in a second register. Then by the linearity of quantum mechanics, the action of U_f on the equal superposition of the input register plus an extra output register will produce

$$U_f : \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \ . \tag{1.6}$$

That is, all possible function evaluations have been done in a single step. This massive parallelism comes for free if one could ever build a quantum computer.

Unfortunately, we are unable to extract all this information in a single observation of the resulting quantum state. Instead, we will only be able to *probabilistically* extract the information encoded in a single "branch" or term in this superposition. Naively then the quantum parallelism is all lost at the