QUANTUM APPROACH TO INFORMATICS

Stig Stenholm
KTH, Stockholm, Sweden
and HUT, Espoo, Finland

Kalle-Antti Suominen
University of Turku, Finland
QUANTUM APPROACH TO INFORMATICS
Motto

Whatever is investigated by human reason commonly also contains falsehood, and this derives partly from the weak judgement of our intellect and partly from the admixtures of pictures. Consequently many, who remain unaware of the power of visualization, will doubt such things that have been most truly demonstrated. This is the case especially because each one having a reputation as a wise man teaches his own version of the creed. In addition, many truths that are taken to be demonstrated also encompass something false, something which has not been truly demonstrated but rather is claimed on the basis of some probable or contrived argument, which is nevertheless taken to be a valid demonstration.

Thomas of Aquinas
1224–1274
QUANTUM APPROACH TO INFORMATICS

Stig Stenholm
KTH, Stockholm, Sweden
and HUT, Espoo, Finland

Kalle-Antti Suominen
University of Turku, Finland
CONTENTS

PREFACE ix

1 INTRODUCTION 1

1.1 Background / 1
1.2 Quantum Information Unit / 3
1.3 Representation of the Qubit / 9
  1.3.1 Bloch Sphere / 9
  1.3.2 Poincaré Sphere / 11
1.4 The Appetizer: Secure Communication / 16
1.5 References / 18

2 QUANTUM THEORY 20

2.1 Quantum Mechanics / 20
  2.1.1 Structure of Quantum Theory / 20
  2.1.2 Quantum Ensembles / 29
2.2 Nonlocality of Quantum Mechanics / 38
  2.2.1 Nonsignaling by Quantum Observations / 38
  2.2.2 No Cloning of Quantum States / 39
  2.2.3 Teleportation / 42
  2.2.4 Bell Inequalities / 46
  2.2.5 GHZ States and Reality / 49
2.3 The Process of Measurement / 54
  2.3.1 Introducing the Meter / 54
  2.3.2 Measurement Transformation / 56
  2.3.3 Observation on Nonorthogonal States / 56
  2.3.4 Special Cases / 59
2.4 Introduction of Irreversibility / 61
  2.4.1 Master Equation / 61
  2.4.2 Unraveling the Master Equation / 66
  2.4.3 Continuous Measurements / 68
  2.4.4 Completely Positive Maps / 69
2.5 References / 74

3 QUANTUM COMMUNICATION AND INFORMATION 76

3.1 Classical Communication / 76
  3.1.1 Information Theory / 76
  3.1.2 Coding Theory / 86
3.2 Quantum Communication / 98
  3.2.1 Quantum Information / 98
  3.2.2 Quantum Channel / 103
  3.2.3 Use of Generalized Measurements / 108
  3.2.4 Neumark Extension / 119
3.3 Distance Between States / 121
  3.3.1 Trace Distance / 121
  3.3.2 Fidelity / 124
  3.3.3 Relative Entropy / 126
3.4 References / 129

4 QUANTUM COMPUTING 130

4.1 Logic Operations / 130
  4.1.1 Classical Logic Operations / 130
  4.1.2 Quantum Logic Functions / 133
  4.1.3 Simple Quantum Operations / 136
  4.1.4 The Deutsch Problem / 139
4.2 The Computer / 141
  4.2.1 Classical Universal Computer / 141
  4.2.2 Computational Complexity / 144
  4.2.3 Quantum Computer / 145
  4.2.4 Quantum Computing Circuits / 146
4.2.5 Universal Quantum Gates / 154
4.2.6 Quantum Measurement Circuit / 154
4.2.7 Quantum Fourier Transform / 157
4.3 Quantum Algorithms / 160
  4.3.1 Public Key Code / 161
  4.3.2 Quantum Factoring Algorithm / 163
  4.3.3 Quantum Algorithms / 167
4.4 Errors in Quantum Computing / 175
  4.4.1 Types of Errors in Quantum States / 175
  4.4.2 Quantum Error Correction / 180
4.5 Energetics of Quantum Computations / 183
  4.5.1 Energy Used by a Classical Computer / 183
  4.5.2 Resetting Energy / 186
4.6 References / 190

5 PHYSICAL REALIZATION OF QUANTUM INFORMATION PROCESSING

5.1 General Considerations / 192
5.2 Requirements for Quantum Computers / 194
5.3 Logic in Electromagnetic Cavities / 197
  5.3.1 Cavity Quantum Electrodynamics / 197
  5.3.2 Conditional Logic / 203
  5.3.3 Dissipative Processes in Cavity QED / 206
5.4 Logic with Ions in Traps / 208
  5.4.1 Trapping Cool Ions / 208
  5.4.2 Quantum Logic in an Ion Trap / 212
  5.4.3 Computing with Hot Ions / 216
5.5 Solid-State Systems / 217
  5.5.1 General Considerations / 217
  5.5.2 Special Examples / 218
5.6 Macromolecules and Optical Lattices / 222
  5.6.1 Nuclear Spin in Molecules / 222
  5.6.2 Optical Lattices / 226
5.7 Conclusions / 226
5.8 References / 227

REFERENCES 229

INDEX 235
To see the world as a web of information is a recent view. Humanity has contemplated the source and character of our knowledge since the dawn of time, but the present technologically oriented civilization demands a more concrete concept. Knowledge has been replaced by information. The information has to be carried by physical objects, and these are described by the theories of physics. Thus, we have to develop a theory for information coded in physical objects.

Long ago, scientists developed formal descriptions of classical information transfer and its manipulation. Only recently, however, have we encountered the information capacity carried by quantum entities. The quantum theory of information, communication, and computing is rather recent. It has grown and matured at a surprising speed. Many discussions of physical observations and quantum measurements are today phrased in terms of information-theoretic concepts. Thus, there is a need to educate students in this thinking but also a need for established researchers to get acquainted with the new way of thinking provoked by the informational aspects of physics. The present book is written to fulfill this need. We consider our readership to be mainly physicists who want to absorb the basics of quantum information within the quantum mechanical framework with which they are familiar. For people who wish to work seriously on the topic or who have a nonphysicist background, many alternative sources are already available.

We regard this book as a contribution to the theory and applications of quantum physics. However, most scientists working with applied quantum theory lack knowledge of classical information theory. Consequently, we introduce the basic ideas from information theory on which the quantum developments are to be built. On the other hand, standard courses in quantum mechanics do not necessarily
cover those aspects most significant for the processing of quantum information. Thus, we present the fundamentals of quantum theory as an introduction to the information discussion. Here we need to explore the actual process of quantum observations in more detail than is usually contained in standard textbooks. The material is not really new, but it acquires novel significance in the present context. Armed with this knowledge, we are prepared to develop the theory of information processing and computing in the quantum domain.

We present the basic ideas of quantum information through an introduction to its basic concepts and methods. It should be useful as the material for a one-semester course of quantum information. The book requires some prior knowledge of quantum theory; thus, it is a text aimed primarily at physicists. This prerequisite should not exceed that given in the standard courses at most universities. The book may, however, be used to indicate to information theorists which parts of quantum theory they need to learn in order to work in this new field; to them the task may not be too arduous. It is our hope that we may introduce the field to a broad range of readers. These may be approaching the text either out of curiosity or in order to be able to proceed to more advanced material.

The presentation aims at neither completeness nor formal rigor. We present the necessary quantum concepts in their simplest forms and introduce ideas by concrete examples. These are presented in such detail that the reader should be able to work through all exercises. Thus, we teach general principles by example rather than by formal demonstrations and general theorems. Many aspects of information theory, classical as well as quantum, can be the subject of formal proofs. For these we refer the reader to the literature.

The references we give are only a small part of the rapidly growing literature in this field. We offer primarily reviews or monographs to set the stage of the action. In addition, we give specific references to particular results treated in the text. The development of the field is too rapid for the reference list to be complete and up to date. We do believe, however, that having mastered the material in this book, the reader can utilize the literature to penetrate any chosen aspect further. In addition, there are comprehensive monographs covering the scope of the field much more completely than we do.

After a brief introduction to set the scene, in Chapter 2 we present the formalism and structure of quantum theory in a form needed for the rest of the book. In addition to a summary of the theory, we introduce some concepts and methods that emerge from this approach. Many of these aspects are treated in further detail in other works, to which we refer. This chapter is central to an understanding of later applications; the basic theme of the book is methods and meanings of quantum manipulations.

Chapter 3 covers the application of information concepts to quantum physics. We summarize briefly the results of information theory and then implement them on quantum systems. No prior knowledge of information theory is assumed. The many quantum results presented in the literature are elucidated by a few central examples. Of particular interest is the possibility to detect and identify
information coded in quantum states. The special character of quantum uncertainties makes this problem different from the corresponding classical problem in noisy transmission channels.

In Chapter 4 we take up the highly topical field of quantum information processing and computing. Most of the material in this chapter is independent of Chapter 3 and can be approached directly after Chapter 2. We do not assume any prior knowledge of computer science; however, those who want to pursue such problems further need more classical background material than we can present here. The text first summarizes the classical approach to data processing and the abstract concept of classical computation. The results are then implemented on quantum systems, and the concept of a quantum computing element, a gate, is introduced. The treatment indicates how quantum gates can be utilized to realize quantum algorithms by combining gates into circuits. As an application, the by-now canonical integer factoring problem is discussed in some detail. We review its origin in methods of classical secret communication and briefly present the method to speed up the factoring on a quantum computer. This solution initiated the present lively interest in quantum computing. We also briefly introduce the sources and character of computing errors and the possibilities for correcting them by quantum means. To conclude the chapter, the energy aspects of quantum computing are briefly introduced.

Finally, in Chapter 5 we present some aspects of the physical realizations of quantum computing circuits. This chapter is rather sketchy, for two reasons: The material covers a broad range of physical phenomena and we can treat their necessary background only briefly. Second, the field is evolving rapidly, so whatever we write here is going to be obsolete in a very brief time. Thus, we begin the chapter by summarizing general considerations concerning possible realizations. We subsequently present the physics behind the most promising systems at the time of writing. The technical details and up-to-date achievements must be learned from more complete presentations than the present one.

We have not inserted detailed references into the text of the book. This would only interrupt the flow of the argument and be useless at a first reading. Instead, we have collected all references into a section at the end of each chapter. In this way we can comment briefly on the contents and significance of the various sources. This is intended to help the reader find a reference dealing with just the specific problem for which he or she requires additional information. We also give the necessary credits to material taken directly from specific publications.

**Acknowledgments**

We are very grateful to Rainer Blatt and Anton Zeilinger for permission to present images obtained by their experimental research groups. We have, over the years, benefited from discussions with too many persons to mention them all here. A selected list is, however, as follows: Erika Andersson, Adriano Barenco, Steve Barnett, Ingemar Bengtsson, Rainer Blatt, Sam Braunstein, Časlav Brukner, Dagmar Bruss, Vladimír Bužek, John Calsamiglia, Ignacio Cirac, David DiVincenzo,
Joe Eberly, Göran Einarsson, Artur Ekert, Barry Garraway, Florian Haug, David Haviland, Peter Knight, Pekka Lahti, Maciej Lewenstein, Göran Lindblad, Norbert Lütkenhaus, Chiara Macchiavello, Harri Mäkelä, Klaus Mølmer, Massimo Palma, Sorin Paraoanu, Jukka Pekola, Jyrki Piilo, Martin Plenio, Anna Sanpera, Päivi Törmä, Vlatko Vedral, Martin Wilkens, Anton Zeilinger, and Peter Zoller.

Stig Stenholm
Kalle-Antti Suominen

Stockholm, Sweden
Turku, Finland
December 2004
CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Quantum mechanics arose from the need to understand the thermal properties of radiation and the discrete spectral features of atoms. From this developed the present understanding of the nonclassical behavior of the fundamental units of matter and radiation. Quantum theory has turned out to be the most universally successful theory of physics. From its start in atomic spectroscopy, it has developed to predict structures of molecules, nuclei, and even the large-scale structures of the universe.

Much of our electronics industry today utilizes quantum phenomena in an essential manner. Without the understanding offered by quantum theory, our ability to build integrated circuits and communication devices would not have emerged. In these areas the basic theoretical progress took place in the middle of the twentieth century; the engineers who plan electronics devices need hardly worry about the problems still lingering on our interpretation of quantum theory.

Despite all its successes, quantum theory is more a set of recipes than a well-formed theory. Even if we master quantum theory in practical applications, we do not really comprehend its basic structure as a probabilistic theory with its associated highly nonclassical and nonlocal correlations. The rather strange role of an observer and the very act of measurements give an uneasy feeling that the theory is not closed. Over the decades, this feeling was put forward by many eminent physicists, including some of the very founders of the theory.