QUANTUM APPROACH TO INFORMATICS

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

Kalle-Antti Suominen
University of Turku, Finland

A JOHN WILEY & SONS, INC., PUBLICATION

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

A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Stenholm, Stig.
Quantum approach to informatics / Stig Stenholm, Kalle-Antti Suominen.
p. cm.
Includes bibliographical references and index.
ISBN-13 978-0-471-73610-3
ISBN-10 0-471-73610-4
1. Quantum theory—Mathematics. 2. Computer science—Mathematics. 3. Quantum computers. I. Suominen, Kalle-Antti, 1964–II. Title.
QC174.17.M35S74 2005
530.12—dc22

2005042842

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

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 Knowledge has been replaced by information.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.

Quantum Approach to Informatics, by Stig Stenholm and Kalle-Antti Suominen

Quantum measurements have always been concerned with information transfer; the object under investigation is supposed to give up knowledge about some of its properties to a measuring device that is eventually read by an observer. Thus, even the very act of physical measurement can be regarded as an information transfer between nature and the scientist. The transmitting method is the totality of our laws of physics, with quantum theory being one eminent member.

But humans want to perform many other information-processing operations than observations. We want to communicate at arbitrary distances and process data to analyze them or obtain answers to well-posed mathematical queries. In some investigations in theoretical physics, we want to use computing devices to simulate natural phenomena. All this has to take place in media consisting of physical objects. These thus have to carry the necessary information, manipulate it, and inform the operator about the outcome. All information processing is to take place in a material medium.

The question arises: How does quantum mechanics affect all this? Richard Feynman was a pioneer in suggesting that the optimal way to model a quantum process would be to simulate it with an appropriate other quantum process. But quantum components are widely different from classical ones, and thus the understanding of their operation becomes an investigation into the scope and limit of quantum mechanics as we know it.

Quantum systems carry a character of wholeness, which is lacking in classical systems. If we interfere with one part of a system, this may have important consequences for the other parts. Thus, one cannot do onto quantum systems all one can do onto classical ones. This has been utilized in communication with quantum systems; if a photon is absorbed by a receiver, it is not available for any intruder.

On the other hand, quantum systems can do more things simultaneously than classical objects can. The well-known two-slit experiment shows interference between particle paths going different ways to their ultimate absorption; no classical particle can do that. This offers a possibility to let quantum systems perform all desired calculations in parallel, which has been found to speed up certain algorithmic processes beyond what classical computers can achieve. Thus, the idea of a quantum computer was born.

Over all such new applications falls the shadow of quantum measurements. The proper introduction of an observer and the processes he or she is able to effect play an important role in all quantum information-processing methods. Thus, we need to understand the fundamental structure of quantum theory at its deepest level. We must realize all the possibilities that the theory offers, but also be aware of the limitations imposed by quantum measurements. Recent developments in quantum information research can be seen as a thorough exploration of our basic understanding of the quantum theory of physical systems. Even if nothing else useful ever emerges from the effort, we may hope that it will result in a broader and deeper understanding of the theory.

Quantum technology is very much alive today. This is an interesting development, because there are no practically useful realizations available in the

laboratories. All experimental setups are primitive and explorative. All practical rewards are far in the future. However, long before that, the field has reached a certain maturity. We are exploring the possible uses of generic quantum systems, which still are very far from practical materialization. This is new in quantum physics; so far it has been used primarily to analyze observed phenomena. Now we have reached the age of synthesis. Devices are planned and explored which today are far beyond our technical abilities. As to their eventual materialization, only the future can tell.

The popularity of the concept of information has inspired some researchers to claim that all our best descriptions of nature are based only on information retrieved from the observations; information theory lies behind all understanding. Sometimes an even wilder claim is made: The universe as we experience it is only a set of information carriers; its very existence is as information and nothing else. This is highly speculative; there is no empirical basis for such a claim. In fact, taken at face value, one may find it difficult to actually understand what this claim means. As physicists we believe in an independent reality, but quantum theory tells us that this is, in fact, weirder than we can imagine.

In this work we approach information transfer and manipulation as a branch of quantum physics. The basic facts of the fundamental theory are put forward in a form conducive to this end. We do not try to cover all the aspects of this rapidly developing field, but we present selected applications to illustrate how quantum mechanics is used in information physics. To make the presentation self-contained, we present such facts from classical information theory which are needed to comprehend the quantum application. The basic outlook is, however, that we are dealing with a branch of quantum physics. Thus, the progress in insight and understanding gained may turn out useful even if a technically successful quantum information machine is never to be built.

1.2 QUANTUM INFORMATION UNIT

Classical information is carried by numerical variables, which are in practice often reduced to the binary representation $\{0, 1\}$. A sequence *abcd* of these correspond to the number

$$abcd \Leftrightarrow a \times 2^3 + b \times 2^2 + c \times 2 + d. \tag{1.1}$$

Each binary variable carries an amount of information called a *bit*; the number above thus carries 4 bits of information. This is a measure of the length of the string carrying the information, whereas the string can actually be used to name $2^4 = 16$ different numbers. From the point of view of information, the length of the string is interesting; it tells us how much space is required to hold the number. Hence the measure of information is often taken to be the length of this: in this case,

$$4 = \log_2 16 = \frac{\log 16}{\log 2}, \tag{1.2}$$

where "log" denotes the ordinary natural logarithm, based on Euler's number e. Using the logarithmic definition of information, we see that a single bit carries $\log_2 2 = 1$ (i.e., 1 bit of information).

In quantum mechanics, the simple two-level system based on the state space spanned by the basis vectors $\{|0\rangle, |1\rangle\}$ replaces the classical bit. Throughout this book we take Dirac's notation of bras and kets for granted. The basis states are assumed to be normalized and orthogonal with respect to the scalar product in the space

$$\langle k|n\rangle = \delta_{kn}. \tag{1.3}$$

We can represent a general state in this basis as

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle. \tag{1.4}$$

An alternative notation is the vector form

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \Leftrightarrow \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}. \tag{1.5}$$

For large state spaces the vector form (and the accompanying matrix notation for operators) becomes cumbersome, but for quantum information systems it provides a useful alternative to Dirac's notation.

The norm of the general state of a two-level system is given by

$$||\,|\psi\rangle||^2 \equiv \langle\psi|\psi\rangle = |c_0|^2 + |c_1|^2 = 1. \tag{1.6}$$

The two complex numbers $\{c_0, c_1\}$ have four real parameters; one of these is fixed by the normalization condition. We can write the state as

$$|\psi\rangle = e^{i\eta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right). \tag{1.7}$$

Usually, the overall (global) phase η lacks significance, and the state is thus determined by the two parameters $\{\theta, \varphi\}$. One should note, however, that when considering a larger system that consists of many such two-level systems, the phase relations between the two-level systems (given by η) are relevant.

The vector describing the state of a two-level quantum system carries the quantum analog of a bit; this is called a *qubit*. The qubit is a more general information carrier than the bit. Its use derives from a combination of quantum physics with ideas from classical information processing. The storing and processing of quantum information offers many exciting and novel features. Its practical utility and general properties are still only incompletely known.

If we choose to code some information in the coefficients $\{c_0, c_1\}$, we call this basis the *computational basis*. Choosing this, we have given up the well-known freedom to use an arbitrary basis in quantum mechanical calculations; the information is specifically carried in one basis only. We are, of course, free to

redefine our computational basis at any time. Another very useful complementary basis is given by the states

$$|\psi_{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right). \tag{1.8}$$

These are easily seen to be orthogonal, and in terms of the original basis states, we have

$$|\langle 0|\psi_{\pm}\rangle|^2 = |\langle 1|\psi_{\pm}\rangle|^2 = \frac{1}{2}. \tag{1.9}$$

Quantum mechanically, this tells us that when the system is in the states $|\psi_{\pm}\rangle$, there are equal probabilities that it will be found in any of the original basis states. The new states consequently carry no information about the occurrence of the original states. Performing a measurement, we will find that they occur with equal random probabilities.

In quantum physics a central role is played by linear transformations of the state vectors. These are given by the operators M, which appear as matrices if we use the vector notation for the amplitudes:

$$M|\psi\rangle \Leftrightarrow \begin{bmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}. \tag{1.10}$$

The matrix in Eq. (1.10) can be written in the form

$$\begin{aligned} M = {} & \frac{m_{00}+m_{11}}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \frac{m_{01}+m_{10}}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ & + i\frac{m_{01}-m_{10}}{2}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} + \frac{m_{00}-m_{11}}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned} \tag{1.11}$$

Here we have introduced the Pauli matrices

$$\begin{aligned} \sigma_1 &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_2 &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \\ \sigma_3 &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned} \tag{1.12}$$

They are normally used to describe spin variables in quantum physics, but here we regard them as simple basis matrices for 2×2 matrix transformations. They obey the simple relations

$$\sigma_1\sigma_2 - \sigma_2\sigma_1 = 2i\sigma_3 \tag{1.13}$$

with cyclic permutations $1 \to 2 \to 3 \to 1$. We also have for any pair

$$\mathrm{Tr}(\sigma_i \sigma_j) = 2\delta_{ij}, \tag{1.14}$$

where the notation $\mathrm{Tr}(M)$ means the sum of the diagonal elements of a matrix M (i.e., its trace). Using these, we can write any matrix in the form

$$M = \frac{1}{2}\left(\mathrm{Tr}(M) + \sum_{i=1}^{3} M_i \sigma_i\right), \tag{1.15}$$

with

$$M_i = \mathrm{Tr}(\sigma_i M). \tag{1.16}$$

Note: In the quantum information literature, one often encounters the notation

$$\begin{aligned} \sigma_1 &= X, \\ \sigma_2 &= Y, \\ \sigma_3 &= Z. \end{aligned} \tag{1.17}$$

In this book we prefer, however, the Pauli notation, which is standard in quantum mechanics literature.

In telecommunications, light has a special role. Photons are natural carriers of quantum information. The orthogonal polarization states of a photon form a quantum mechanical two-level system, although technologically it is not necessarily the best option (e.g., in optical fibers, polarization states are extremely fragile). Another possibility is to consider the existence of the photon itself if we know that the photons are arriving at regular intervals. Recently, the orbital angular momentum carried by laser beams has emerged as yet another available degree of freedom at the level of single photons.

A photon is the bosonic quantum of the electromagnetic field. Its description follows from the fact that the theory of electromagnetic radiation can be cast in the form of an assembly of independent harmonic oscillators. The quantum theory of this system is well presented in most texts on quantum theory; here we refresh the reader's memory by summarizing the main parts of the argument. We return to this topic again in Sec. 5.3.1, where we consider field quantization in a cavity.

In suitably chosen units the Hamiltonian of one harmonic mode is given by

$$H = \frac{P^2}{2} + \frac{1}{2}\omega^2 Q^2, \tag{1.18}$$

where ω is the angular frequency of the mode. As P and Q are canonical variables, we perform the quantization by setting

$$[Q, P] \equiv QP - PQ = i\hbar. \tag{1.19}$$

If we define the operators

$$\begin{aligned} a &= \sqrt{\frac{\omega}{2\hbar}}\left(Q + \frac{iP}{\omega}\right), \\ a^\dagger &= \sqrt{\frac{\omega}{2\hbar}}\left(Q - \frac{iP}{\omega}\right), \end{aligned} \tag{1.20}$$

we can then directly calculate

$$\left[a, a^\dagger\right] = aa^\dagger - a^\dagger a = 1. \tag{1.21}$$

This shows that the operators characterize bosons. We also obtain

$$aa^\dagger + a^\dagger a = \frac{2H}{\hbar\omega}, \tag{1.22}$$

giving

$$H = \frac{\hbar\omega}{2}\left(aa^\dagger + a^\dagger a\right) = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right). \tag{1.23}$$

We can now define the eigenstates $|n\rangle$ of the operator $N = a^\dagger a$, by requiring that

$$N|n\rangle = n|n\rangle. \tag{1.24}$$

Assuming the existence of a vacuum state $|0\rangle$ such that

$$a|0\rangle = 0, \tag{1.25}$$

we find that the eigenstates n have to be integers $\{0, 1, 2, \ldots\}$. These are taken to count the number of photons in the mode. From (1.21) we can prove that

$$\begin{aligned} a|n\rangle &= \sqrt{n}|n-1\rangle, \\ a^\dagger|n\rangle &= \sqrt{(n+1)}|n+1\rangle. \end{aligned} \tag{1.26}$$

This justifies calling a and $a^\dagger$ photon annihilation and creation operators, respectively. From (1.26) it follows that the eigenstates can be written as

$$|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle, \tag{1.27}$$

where the denominator is chosen to give normalized states. They are also easily seen to be orthogonal for different quantum numbers.

In optical physics there is one set of operators for each type of photon. Thus, the electromagnetic field is replaced by a set of boson excitation modes. This representation is particularly useful in the quantum mechanical description of optical devices.

Application: Beamsplitter A beamsplitter is an optical element with two inputs and two outputs (Fig. 1.1). We assume that the incoming signals are split equally between the outputs. If the state amplitudes coming in are a_1 and a_2, respectively, and the outputs are b_1 and b_2, respectively, the transformation between the inputs and the outputs can be written as

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}. \tag{1.28}$$

This transformation is unitary, and we have the inverse transformation

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}. \tag{1.29}$$

This guarantees that the state amplitude is conserved:

$$|b_1|^2 + |b_2|^2 = |a_1|^2 + |a_2|^2. \tag{1.30}$$

Classically, the same relation guarantees that the outgoing energy is equal to the incoming energy.

We have defined the beamsplitter transformation in a symmetric way. We can move the phases around by redefining the relative phase of incoming and/or outgoing state amplitudes, but for most applications the symmetric form is most advantageous.

The beamsplitter transformation (1.28) has been defined in terms of classical amplitudes impinging on the device. As this is a linear transformation of the signals, we may directly replace the amplitudes by the corresponding quantum operators. The symbols $\{a^\dagger, b^\dagger\}$ then become photon creation operators, and the

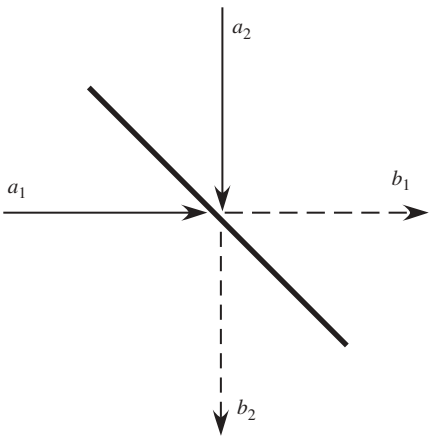

Figure 1.1 Beamsplitter with input amplitudes a_1, a_2 and output amplitudes b_1, b_2.

relations describe how incoming photons are transmitted into outgoing ones. This gives a convenient way to treat the properties of the device.

As an exercise, we calculate the output if one photon is impinging on the beamsplitter at each input port. Conveniently, we can replace the amplitudes in our description with the photon creation operators. Note that generally the photon vacuum is denoted with $|0\rangle$, which is not related to the quantum bit state $|0\rangle$ (unless we assign 0 to the detection of no photons). We have the input operators in terms of the output operators as

$$\begin{aligned} a_1^\dagger &= \frac{1}{\sqrt{2}}\left(b_1^\dagger + i b_2^\dagger\right), \\ a_2^\dagger &= \frac{1}{\sqrt{2}}\left(i b_1^\dagger + b_2^\dagger\right). \end{aligned} \tag{1.31}$$

The input state is now given by

$$\begin{aligned} |\psi_{\text{in}}\rangle &= a_1^\dagger a_2^\dagger |0\rangle \\ &= \frac{i}{2}\left(b_1^{\dagger 2} + b_2^{\dagger 2}\right)|0\rangle \\ &= \frac{i}{\sqrt{2}}\left(|n_1 = 2, n_2 = 0\rangle + |n_1 = 0, n_2 = 2\rangle\right). \end{aligned} \tag{1.32}$$

We thus find that both photons exit at the same output, and no coincidences can be observed between detectors in the two outputs. This is a manifestation of the bosonic character of the photons. Note that the original phase relation of the two photons plays no role; the incoming channels do not share the same state space (nor do the two output channels).

1.3 REPRESENTATION OF THE QUBIT

1.3.1 Bloch Sphere

From the representation (1.7) of the general quantum state $|\psi\rangle$ we define the quantities

$$\begin{aligned} u &\equiv \langle\psi|\sigma_1|\psi\rangle = c_0^* c_1 + c_0 c_1^* = \sin\theta\cos\varphi, \\ v &\equiv \langle\psi|\sigma_2|\psi\rangle = i\left(c_0 c_1^* - c_1 c_0^*\right) = \sin\theta\sin\varphi, \\ w &\equiv \langle\psi|\sigma_3|\psi\rangle = c_0 c_0^* - c_1 c_1^* = \cos\theta. \end{aligned} \tag{1.33}$$

From this we see that the real vector

$$\vec{R} = \begin{bmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{bmatrix} \tag{1.34}$$

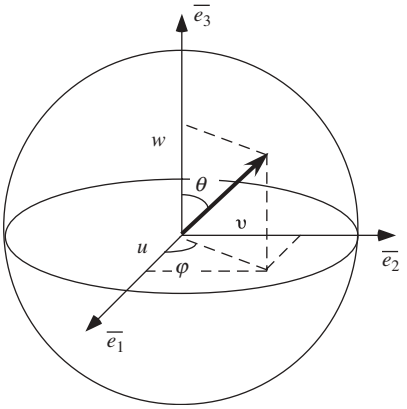

Figure 1.2 Bloch vector in the Bloch sphere and its parametrization with angles θ and φ.

is of unit length

$$\vec{R} \cdot \vec{R} = u^2 + v^2 + w^2 = 1. \tag{1.35}$$

It is a representation of the quantum state in a fictitious three-dimensional space, where u, v, and w are the coordinates along three axes represented by orthogonal unit vectors $\vec{e}_1$, $\vec{e}_2$, and $\vec{e}_3$ (Fig. 1.2). This is the Bloch vector. In fact, since $|\vec{R}| = 1$, the representation is reduced to defining a point on the surface of a unit sphere with angular coordinates (θ, φ). This unit sphere is called the *Bloch sphere*. The origin of the term is in nuclear magnetism, where by defining the quantum mechanical spin in this manner, one can identify the fictitious three-dimensional space with the actual three-dimensional space. This allows a simple description of the spin dynamics due to the coupling of the spin to the magnetic field (which is an object of the actual three-dimensional space).

For a given state, the vector $\vec{R}$ has the right number of real parameters to specify the state uniquely. The state $[1, 0]^{\mathrm{T}}$ is given by the "north pole," $w = 1$ $(\theta = 0)$, and the state $[0, 1]^{\mathrm{T}}$ by the "south pole," $w = -1$ $(\theta = \pi)$. States of the type

$$|\varphi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\varphi} |1\rangle \right) \tag{1.36}$$

lie along the "equator" [i.e., $\theta = \pi/2$, with φ as the angle in the $\vec{e}_1, \vec{e}_2$-plane, measured counterclockwise from the $\vec{e}_1$-axis (Fig. 1.2)]. In open quantum systems, probabilities are not necessarily normalized to unity, and the length of the Bloch vector becomes another variable, and the description of the two-level system is no longer limited to the surface of the Bloch sphere.

If we introduce the Pauli vector by setting

$$\vec{\sigma} = \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{bmatrix}, \tag{1.37}$$

the quantum object called the *density matrix* can be written as

$$\rho \equiv \begin{bmatrix} c_0 c_0^* & c_0 c_1^* \\ c_1 c_0^* & c_1 c_1^* \end{bmatrix} = \frac{1}{2}\left(1 + \vec{R}\cdot\vec{\sigma}\right), \tag{1.38}$$

which is easily verified directly. The density matrix is going to play an essential role in our discussions.

1.3.2 Poincaré Sphere

There exists an alternative way to arrive at the representation of a quantum state as a sphere. We start from the state

$$|\psi\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0 \begin{bmatrix} 1 \\ z \end{bmatrix}, \tag{1.39}$$

where the complex number

$$z = \frac{c_1}{c_0} = e^{i\varphi} \tan\frac{\theta}{2} \tag{1.40}$$

can take any value in the complex plane. We then insert a three-dimensional sphere of unit radius centered at the origin in the plane. The axis orthogonal to the complex plane is designated the 3-axis, and the real and imaginary axes of the complex plane give the 1- and 2-axes, respectively (here we do not use unit vectors because they allude to a three-dimensional vector space).

We next perform a stereoscopic projection from the point z in the plane to the south pole of the sphere (Fig. 1.3). The point where the ray penetrates the sphere

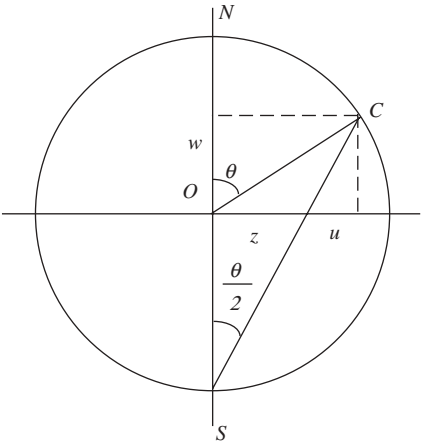

Figure 1.3 Poincaré sphere and its parametrization.

is taken to represent the state. It is obvious that this is a one-to-one mapping of the complex plane, and hence it represents all possible quantum states of a two-level system. The state $[1, 0]^{\mathrm{T}}$ is given by the north pole ($|z| = 0$), and the state $[0, 1]^{\mathrm{T}}$ by the south pole ($|z| = \infty$); this agrees with the situation for the Bloch sphere. Physicists use this sphere, called the *Poincaré sphere*, to describe the polarization states of light, but in mathematics it is known as the *Riemann sphere* and is used in complex analysis to map the surroundings of infinity into the surroundings of zero.

The Poincaré sphere turns out to be fully equivalent with the Bloch sphere of Sec. 1.3.1. To see this, we set $\varphi = 0$. From (1.40) this only rotates the complex plane; it contains no new information. From Fig. 1.3 we can see how the identification works: From the construction it follows that lengths OS and OC are equal to unity (i.e., of equal length), so $\measuredangle SC$ must be equal to $\pi - \theta$, and thus $\measuredangle NC$ is equal to θ. Therefore, the coordinates of point C must be $\sin\theta$ and $\cos\theta$ (i.e., the coordinates u and w of the corresponding point on the Bloch sphere). As we have $v = 0$, we see that this agrees with the result in (1.33).

The representation of a state on the Poincaré sphere is thus identical with the representation on the Bloch sphere. However, in addition, we have obtained the representation by z in the complex plane. Note that we have taken the south pole as a special point, whereas for the Riemann sphere one often uses the north pole and then defines $z = e^{i\varphi}\tan(\pi/4 + \theta/2)$, which is quite equivalent to our choice, Eq. (1.40).

Application: Photon Polarization A quantum of the electromagnetic field, a photon, can have only two polarization states. This makes it an ideal object to use as a genuine two-state system. If we choose to describe the polarization state in the orthogonal basis formed by linear polarization states in the horizontal and vertical directions, we can set

$$|\updownarrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}; \quad |\leftrightarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{1.41}$$

We can also introduce orthogonal polarization states turned by an angle of $\pi/4$ in real space. These states are given by

$$\begin{aligned} |\nearrow\rangle &= \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle + |\leftrightarrow\rangle\right), \\ |\nwarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle - |\leftrightarrow\rangle\right). \end{aligned} \tag{1.42}$$

On the Bloch sphere these basis states are at an angle with respect to each other, which is given by

$$\cos\frac{\alpha}{2} = \langle\updownarrow \mid \nearrow\rangle = \frac{1}{\sqrt{2}}. \tag{1.43}$$