Eleanor Rieffel and Wolfgang Polak

Quantum Computing

A Gentle Introduction

QUANTUM COMPUTING

A Gentle Introduction

Eleanor Rieffel and Wolfgang Polak

The MIT Press
Cambridge, Massachusetts
London, England

This book was set in Syntax and Times Roman by Westchester Book Group. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data
Rieffel, Eleanor, 1965–
Quantum computing : a gentle introduction / Eleanor Rieffel and Wolfgang Polak.
p. cm.—(Scientific and engineering computation)
Includes bibliographical references and index.
ISBN 978-0-262-01506-6 (hardcover : alk. paper) 1. Quantum computers. 2. Quantum theory. I. Polak, Wolfgang, 1950– II. Title.
QA76.889.R54 2011
004.1—dc22

2010022682

10 9 8 7 6 5 4 3 2 1

Contents

out of introductory books, and discusses bipartite entanglement. Discussions of multipartite entanglement require examples, which made it natural to include a section on cluster states, the fundamental entanglement resource used for cluster state, or one-way, quantum computation. Cluster state quantum computation and adiabatic quantum computation, two alternatives to the standard circuit model, are briefly introduced and their strengths and applications discussed.

As a final example, while the conversion between general classical circuits and reversible classical circuits is a purely classical topic, it is the heart of the proof that anything a classical computer can do, a quantum computers can do with comparable efficiency. For this reason, the book includes a detailed account of this piece of classical, but nonstandard, computer science.

This is not a book about quantum mechanics. We treat quantum mechanics as an abstract mathematical theory and consider the physical aspects only to elucidate theoretical concepts. We do not discuss issues of interpretation of quantum mechanics; the occasional use of terms such as *quantum parallelism*, for example, is not to be construed as an endorsement of one or another particular interpretation.

Acknowledgments

We are enormously indebted to Michael B. Heaney and Paul McEvoy, both of whom read multiple versions of many of the chapters and provided valuable comments each time. It is largely due to their steadfast belief in this project that the book reached completion. The FXPAL/PARC reading group enabled us to discover which expository approaches worked and which did not. The group's comments, struggles, and insights spurred substantial improvements in the book. We are grateful to all of the members of that group, particularly Dirk Balfanz, Stephen Jackson, and Michael Plass. Many thanks to Tad Hogg and Marc Rieffel for their feedback on some of the most technical and notationally heavy sections. Thanks also go to Gene Golovchinsky for suggestions that clarified and streamlined the writing of an early draft, to Livia Polanyi for suggestions that positively impacted the flow and emphasis, to Garth Dales for comments on an early draft that improved our wording and use of notation, and to Denise Greaves for extensive editorial assistance. Many people provided valuable comments on drafts of the tutorial[3] that was the starting point for this book. Their comments improved this book as well as the tutorial. We gratefully acknowledge the support of FXPAL for part of this work. We are grateful to our friends, to our family, and especially to our spouses for their support throughout the years it took us to write this book.

Notes

1. FX Palo Alto Laboratory.
2. Palo Alto Research Center.
3. E. G. Rieffel and W. Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32(3):300–335, 2000.

1 Introduction

In the last decades of the twentieth century, scientists sought to combine two of the century's most influential and revolutionary theories: information theory and quantum mechanics. Their success gave rise to a new view of computation and information. This new view, quantum information theory, changed forever how computation, information, and their connections with physics are thought about, and it inspired novel applications, including some wildly different algorithms and protocols. This view and the applications it spawned are the subject of this book.

Information theory, which includes the foundations of both computer science and communications, abstracted away the physical world so effectively that it became possible to talk about the major issues within computer science and communications, such as the efficiency of an algorithm or the robustness of a communication protocol, without understanding details of the physical devices used for the computation or the communication. This ability to ignore the underlying physics proved extremely powerful, and its success can be seen in the ubiquity of the computing and communications devices around us. The abstraction away from the physical had become such a part of the intellectual landscape that the assumptions behind it were almost forgotten. At its heart, until recently, information sciences have been firmly rooted in classical mechanics. For example, the Turing machine is a classical mechanical model that behaves according to purely classical mechanical principles.

Quantum mechanics has played an ever-increasing role in the development of new and more efficient computing devices. Quantum mechanics underlies the working of traditional, classical computers and communication devices, from the transistor through the laser to the latest hardware advances that increase the speed and power and decrease the size of computer and communications components. Until recently, the influence of quantum mechanics remained confined to the low-level implementation realm; it had no effect on how computation or communication was thought of or studied.

In the early 1980s, a few researchers realized that quantum mechanics had unanticipated implications for information processing. Charles Bennett and Gilles Brassard, building on ideas of Stephen Wiesner, showed how nonclassical properties of quantum measurement provided a provably secure mechanism for establishing a cryptographic key. Richard Feynman, Yuri Manin, and others recognized that certain quantum phenomena—phenomena associated with so-called

entangled particles—could not be simulated efficiently by a Turing machine. This observation led to speculation that perhaps these quantum phenomena could be used to speed up computation in general. Such a program required rethinking the information theoretic model underlying computation, taking it out of the purely classical realm.

Quantum information processing, a field that includes quantum computing, quantum cryptography, quantum communications, and quantum games, explores the implications of using quantum mechanics instead of classical mechanics to model information and its processing. Quantum computing is not about changing the physical substrate on which computation is done from classical to quantum, but rather changing the notion of computation itself. The change starts at the most basic level: the fundamental unit of computation is no longer the bit, but rather the quantum bit or qubit. Placing computation on a quantum mechanical foundation led to the discovery of faster algorithms, novel cryptographic mechanisms, and improved communication protocols.

The phrase *quantum computing* does not parallel the phrases *DNA computing* or *optical computing*: these describe the substrate on which computation is done without changing the notion of computation. *Classical computers*, the ones we all have on our desks, make use of quantum mechanics, but they compute using bits, not qubits. For this reason, they are not considered quantum computers. A quantum or classical computer may or may not be an optical computer, depending on whether optical devices are used to carry out the computation. Whether the computer is quantum or classical depends on whether the information is represented and manipulated in a quantum or classical way. The phrase *quantum computing* is closer in character to *analog computing* because the computational model for analog computing differs from that of standard computing: a continuum of values, rather than only a discrete set, is allowed. While the phrases are parallel, the two models differ greatly in that analog computation does not support entanglement, a key resource for quantum computation, and measurements of a quantum computer's registers can yield only a small, discrete set of values. Furthermore, while a qubit can take on a continuum of values, in many ways a qubit resembles a bit, with its two discrete values, more than it does analog computation. For example, as we will see in section 4.3.1, only one bit's worth of information can be extracted from a qubit by measurement.

The field of quantum information processing developed slowly in the 1980s and early 1990s as a small group of researchers worked out a theory of quantum information and quantum information processing. David Deutsch developed a notion of a quantum mechanical Turing machine. Daniel Bernstein, Vijay Vazirani, and Andrew Yao improved upon his model and showed that a quantum Turing machine could simulate a classical Turing machine, and hence any classical computation, with at most a polynomial time slowdown. The standard quantum circuit model was then defined, which led to an understanding of quantum complexity in terms of a set of basic quantum transformations called quantum gates. These gates are theoretical constructs that may or may not have direct analogs in the physical components of an actual quantum computer.

In the early 1990s, researchers developed the first truly quantum algorithms. In spite of the probabilistic nature of quantum mechanics, the first quantum algorithms, for which superiority

over classical algorithms could be proved, give the correct answer with certainty. They improve upon classical algorithms by solving in polynomial time with certainty a problem that can be solved in polynomial time only with high probability using classical techniques. Such a result is of no direct practical interest, since the impossibility of building a perfect machine reduces any practical machine running any algorithm to solving a problem only with high probability. But such results were of high theoretical interest, since they showed for the first time that quantum computation is theoretically more powerful than classical computation for certain computational problems.

These results caught the interest of various researchers, including Peter Shor, who in 1994 surprised the world with his polynomial-time quantum algorithm for factoring integers. This result provided a solution to a well-studied problem of practical interest. A classical polynomial-time solution had long been sought, to the point where the world felt sufficiently confident that no such solution existed that many security protocols, including the widely used RSA algorithm, base their security entirely on the computational difficulty of this problem. It is unknown whether an efficient classical solution exists, so Shor's result does not prove that quantum computers can solve a problem more efficiently than a classical computer. But even in the unlikely event that a polynomial-time classical algorithm is found for this problem, it would be an indication of the elegance and effectiveness of the quantum information theory point of view that a quantum algorithm, in spite of all the unintuitive aspects of quantum mechanics, was easier to find.

While Shor's result sparked a lot of interest in the field, doubts as to its practical significance remained. Quantum systems are notoriously fragile. Key properties, such as quantum entanglement, are easily disturbed by environmental influences that cause the quantum states to *decohere*. Properties of quantum mechanics, such as the impossibility of reliably copying an unknown quantum state, made it look unlikely that effective error-correction techniques for quantum computation could ever be found. For these reasons, it seemed unlikely that reliable quantum computers could be built.

Luckily, in spite of serious and widespread doubts as to whether quantum information processing could ever be practical, the theory itself proved so tantalizing that researchers continued to explore it. As a result, in 1996 Shor and Robert Calderbank, and independently Andrew Steane, saw a way to finesse the seemingly show-stopping problems of quantum mechanics to develop quantum error correction techniques. Today, quantum error correction is arguably the most mature area of quantum information processing.

How practical quantum computing and quantum information will turn out is still unknown. No fundamental physical principles are known that prohibit the building of large-scale and reliable quantum computers. Engineering issues, however, remain. As of this writing, laboratory experiments have demonstrated quantum computations with several quantum bits performing dozens of quantum operations. Myriad promising approaches are being explored by theorists and experimentalists around the world, but much uncertainty remains as to how, when, or even whether, a quantum computer capable of carrying out general quantum computations on hundreds of qubits will be built.

QUANTUM BUILDING BLOCKS

Quantum mechanics, that mysterious, confusing discipline, which none of us really understands, but which we know how to use.
—*Murray Gell-Mann* [126]

2 Single-Qubit Quantum Systems

Quantum bits are the fundamental units of information in quantum information processing in much the same way that bits are the fundamental units of information for classical processing. Just as there are many ways to realize classical bits physically (two voltage levels, lights on or off in an array, positions of toggle switches), there are many ways to realize quantum bits physically. As is done in classical computer science, we will concern ourselves only rarely with how the quantum bits are realized. For the sake of concretely illustrating quantum bits and their properties, however, section 2.1 looks at the behavior of polarized photons, one of many possible realizations of quantum bits.

Section 2.2 abstracts key properties from the polarized photon example of section 2.1 to give a precise definition of a quantum bit, or qubit, and a description of the behavior of quantum bits under measurement. Dirac's bra/ket notation, the standard notation used throughout quantum information processing as well as quantum mechanics, is introduced in this section. Section 2.4 describes the first application of quantum information processing: quantum key distribution. The chapter concludes with a detailed discussion of the state space of a single-qubit system.

2.1 The Quantum Mechanics of Photon Polarization

A simple experiment illustrates some of the nonintuitive behavior of quantum systems, behavior that is exploited to good effect in quantum algorithms and protocols. This experiment can be performed by the reader using only minimal equipment: a laser pointer and three polaroids (polarization filters), readily available from any camera supply store. The formalisms of quantum mechanics that describe this simple experiment lead directly to a description of the quantum bit, the fundamental unit of quantum information on which quantum information processing is done. The experiment not only gives a concrete realization of a quantum bit, but it also illustrates key properties of quantum measurement. We encourage you to obtain the equipment and perform the experiment yourself.

2.1.1 A Simple Experiment

Shine a beam of light on a projection screen. When polaroid A is placed between the light source and the screen, the intensity of the light reaching the screen is reduced. Let us suppose that the polarization of polaroid A is horizontal (figure 2.1).

Next, place polaroid C between polaroid A and the projection screen. If polaroid C is rotated so that its polarization is orthogonal (vertical) to the polarization of A, no light reaches the screen (figure 2.2).

Figure 2.1
Single polaroid attenuates unpolarized light by 50 percent.

Figure 2.2
Two orthogonal polaroids block all photons.

Any photon that passes through polaroid A becomes horizontally polarized, so the amplitude of any such photon's state $|\rightarrow\rangle$ in the direction $|\nearrow\rangle$ is $\frac{1}{\sqrt{2}}$. Applying the quantum theory we just learned tells us that a horizontally polarized photon will pass through polaroid B with probability $\frac{1}{2} = |\frac{1}{\sqrt{2}}|^2$. Any photons that have passed through polaroid B now have polarization $|\nearrow\rangle$. When these photons hit polaroid C, they do have amplitude in the vertical direction, so some of them (half) will pass thorough polaroid C and hit the screen (see figure 2.3). In this way, quantum mechanics explains how more light can reach the screen when the third polaroid is added, and it provides a means to compute how much light will reach the screen.

In summary, the polarization state of a photon is modeled as a unit vector. Its interaction with a polaroid is probabilistic and depends on the amplitude of the photon's polarization in the direction of the polaroid's preferred axis. Either the photon will be absorbed or the photon will leave the polaroid with its polarization aligned with the polaroid's preferred axis.

2.2 Single Quantum Bits

The space of possible polarization states of a photon is an example of a *quantum bit*, or *qubit*. A qubit has a continuum of possible values: any state represented by a unit vector $a|\uparrow\rangle + b|\rightarrow\rangle$ is a legitimate qubit value. The amplitudes a and b can be complex numbers, even though complex amplitudes were not needed for the explanation of the experiment. (In the photon polarization case, the imaginary coefficients correspond to *circular polarization*.)

In general, the set of all possible states of a physical system is called the *state space* of the system. Any quantum mechanical system that can be modeled by a two-dimensional complex vector space can be viewed as a qubit. (There is redundancy in this representation in that any vector multiplied by a modulus one [unit length] complex number represents the same quantum state. We discuss this redundancy carefully in sections 2.5 and 3.1.) Such systems, called *two-state quantum systems*, include photon polarization, electron spin, and the ground state together with an excited state of an atom. The *two-state* label for these systems does not mean that the state space has only two states—it has infinitely many—but rather that all possible states can be represented as a linear combination, or superposition, of just two states. For a two-dimensional complex vector space to be viewed as a qubit, two linearly independent states, labeled $|0\rangle$ and $|1\rangle$, must be distinguished. For the theory of quantum information processing, all two-state systems, whether they be electron spin or energy levels of an atom, are equally good. From a practical point of view, it is as yet unclear which two-state systems will be most suitable for physical realizations of quantum information processing devices such as quantum computers; it is likely that a variety of physical representation of qubits will be used.

Dirac's bra / ket notation is used throughout quantum physics to represent quantum states and their transformations. In this section we introduce the part of Dirac's notation that is used for quantum states. Section 4.1 introduces Dirac's notation for quantum transformations. Familiarity and fluency with this notation will help greatly in understanding all subsequent material; we strongly encourage readers to work the exercises at the end of this chapter.

In Dirac's notation, a *ket* such as $|x\rangle$, where x is an arbitrary label, refers to a vector representing a state of a quantum system. A vector $|v\rangle$ is a *linear combination* of vectors $|s_1\rangle, |s_2\rangle, \ldots, |s_n\rangle$ if there exist complex numbers a_i such that $|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \cdots + a_n|s_n\rangle$.

A set of vectors S *generates* a complex vector space V if every element $|v\rangle$ of V can be written as a complex linear combination of vectors in the set: every $|v\rangle \in V$ can be written as $|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \cdots + a_n|s_n\rangle$ for some elements $|s_i\rangle \in S$ and complex numbers a_i. Given a set of vectors S, the subspace of all linear combinations of vectors in S is called the *span* of S and is denoted span(S). A set of vectors B for which every element of V can be written *uniquely* as a linear combination of vectors in B is called a *basis* for V. In a two-dimensional vector space, any two vectors that are not multiples of each other form a basis. In quantum mechanics, bases are usually required to be *orthonormal*, a property we explain shortly. The two distinguished states, $|0\rangle$ and $|1\rangle$, are also required to be orthonormal.

An *inner product* $\langle v_2|v_1\rangle$, or *dot product*, on a complex vector space V is a complex function defined on pairs of vectors $|v_1\rangle$ and $|v_2\rangle$ in V, satisfying

- $\langle v|v\rangle$ is non-negative real,
- $\langle v_2|v_1\rangle = \overline{\langle v_1|v_2\rangle}$, and
- $(a\langle v_2| + b\langle v_3|)|v_1\rangle = a\langle v_2|v_1\rangle + b\langle v_3|v_1\rangle$,

where $\overline{z}$ is the complex conjugate $\overline{z} = a - \mathbf{i}b$ of $z = a + \mathbf{i}b$.

Two vectors $|v_1\rangle$ and $|v_2\rangle$ are said to be *orthogonal* if $\langle v_1|v_2\rangle = 0$. A set of vectors is orthogonal if all of its members are orthogonal to each other. The *length*, or norm, of a vector $|v\rangle$ is $\big||v\rangle\big| = \sqrt{\langle v|v\rangle}$. Since all vectors $|x\rangle$ representing quantum states are of unit length, $\langle x|x\rangle = 1$ for any state vector $|x\rangle$. A set of vectors is said to be *orthonormal* if all of its elements are of length one and orthogonal to each other: a set of vectors $B = \{|\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_n\rangle\}$ is orthonormal if $\langle\beta_i|\beta_j\rangle = \delta_{ij}$ for all i, j, where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

In quantum mechanics we are mainly concerned with bases that are orthonormal, so whenever we say *basis* we mean *orthonormal basis* unless we say otherwise.

For the state space of a two-state system to represent a quantum bit, two orthonormal distinguished states, labeled $|0\rangle$ and $|1\rangle$, must be specified. Apart from the requirement that $|0\rangle$ and $|1\rangle$ be orthonormal, the states may be chosen arbitrarily. For instance, in the case of photon polarization, we may choose $|0\rangle$ and $|1\rangle$ to correspond to the states $|\uparrow\rangle$ and $|\rightarrow\rangle$, or to $|\nearrow\rangle$ and $|\nwarrow\rangle$. We follow the convention that $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\rightarrow\rangle$, which implies that $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. In the case of electron spin, $|0\rangle$ and $|1\rangle$ could correspond to the spin-up and spin-down states, or spin-left and spin-right. When talking about qubits, and quantum information processing in general, a *standard basis* $\{|0\rangle, |1\rangle\}$ with respect to which all statements are made must be chosen in advance and remain fixed throughout the discussion. In quantum information

processing, classical bit values of 0 and 1 will be encoded in the distinguished states $|0\rangle$ and $|1\rangle$. This encoding enables a direct comparison between bits and qubits: bits can take on only two values, 0 and 1, while qubits can take on not only the values $|0\rangle$ and $|1\rangle$ but also any superposition of these values, $a|0\rangle + b|1\rangle$, where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$.

Vectors and linear transformations can be written using matrix notation once a basis has been specified. That is, if basis $\{|\beta_1\rangle, |\beta_2\rangle\}$ is specified, a ket $|v\rangle = a|\beta_1\rangle + b|\beta_2\rangle$ can be written $\begin{pmatrix} a \\ b \end{pmatrix}$; a ket $|v\rangle$ corresponds to a column vector v, where v is simply a label, a name for this vector. The conjugate transpose $v^\dagger$ of a vector

$$v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \text{is} \quad v^\dagger = (\overline{a_1}, \ldots, \overline{a_n}) \ .$$

In Dirac's notation, the conjugate transpose of a ket $|v\rangle$ is called a *bra* and is written $\langle v|$, so

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \text{and} \quad \langle v| = (\overline{a_1}, \ldots, \overline{a_n}) \ .$$

A bra $\langle v|$ corresponds to a row vector $v^\dagger$.

Given two complex vectors

$$|a\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \text{and} \quad |b\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \ ,$$

the standard *inner product* $\langle a|b\rangle$ is defined to be the scalar obtained by multiplying the conjugate transpose $\langle a| = (\overline{a_1}, \ldots, \overline{a_n})$ with $|b\rangle$:

$$\langle a|b\rangle = \langle a||b\rangle = (\overline{a_1}, \ldots, \overline{a_n}) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} \overline{a_i} b_i .$$

When $\vec{a} = |a\rangle$ and $\vec{b} = |b\rangle$ are real vectors, this inner product is the same as the standard dot product on the n dimensional real vector space $\mathbf{R}^n$: $\langle a|b\rangle = a_1 b_1 + \cdots + a_n b_n = \vec{a} \cdot \vec{b}$. Dirac's choice of *bra* and *ket* arose as a play on words: an inner product $\langle a|b\rangle$ of a bra $\langle a|$ and a ket $|b\rangle$ is sometimes called a *bracket*. The following relations hold, where $v = a|0\rangle + b|1\rangle$: $\langle 0|0\rangle = 1$, $\langle 1|1\rangle = 1$, $\langle 1|0\rangle = \langle 0|1\rangle = 0$, $\langle 0|v\rangle = a$, and $\langle 1|v\rangle = b$.

In the standard basis, with ordering $\{|0\rangle, |1\rangle\}$, the basis elements $|0\rangle$ and $|1\rangle$ can be expressed as $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, and a complex linear combination $|v\rangle = a|0\rangle + b|1\rangle$ can be written $\begin{pmatrix} a \\ b \end{pmatrix}$.

This choice of basis and order of the basis vectors are mere convention. Representing $|0\rangle$ as $\begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle$ as $\begin{pmatrix}0\\1\end{pmatrix}$ or representing $|0\rangle$ as $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ and $|1\rangle$ as $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ would be equally good as long as it is done consistently. Unless otherwise specified, all vectors and matrices in this book will be written with respect to the standard basis $\{|0\rangle, |1\rangle\}$ in this order.

A quantum state $|v\rangle$ is a *superposition* of basis elements $\{|\beta_1\rangle, |\beta_2\rangle\}$ if it is a nontrivial linear combination of $|\beta_1\rangle$ and $|\beta_2\rangle$, if $|v\rangle = a_1|\beta_1\rangle + a_2|\beta_2\rangle$ where a_1 and a_2 are non-zero. For the term *superposition* to be meaningful, a basis must be specified. In this book, if we say "superpostion" without explicitly specifying the basis, we implicitly mean with respect to the standard basis.

Initially the vector/matrix notation will be easier for many readers to use because it is familiar. Sometimes matrix notation is convenient for performing calculations, but it always requires the choice of a basis and an ordering of that basis. The bra/ket notation has the advantage of being independent of basis and the order of the basis elements. It is also more compact and suggests correct relationships, as we saw for the inner product, so once it becomes familiar, it is easier to read and faster to use.

Instead of qubits, physical systems with states modeled by three- or n-dimensional vector spaces could be used as fundamental units of computation. Three-valued units are called *qutrits*, and n-valued units are called *qudits*. Since qudits can be modeled using multiple qubits, a model of quantum information based on qudits has the same computational power as one based on qubits. For this reason we do not consider qudits further, just as in the classical case most people use a bit-based model of information.

We now have a mathematical model with which to describe quantum bits. In addition, we need a mathematical model for measuring devices and their interaction with quantum bits.

2.3 Single-Qubit Measurement

The interaction of a polaroid with a photon illustrates key properties of any interaction between a measuring device and a quantum system. The mathematical description of the experiment can be used to model all measurements of single qubits, whatever their physical instantiation. The measurement of more complicated systems retains many of the features of single-qubit measurement: the probabilistic outcomes and the effect measurement has on the state of the system. This section considers only measurements of single-qubit systems. Chapter 4 discusses measurements of more general quantum systems.

Quantum theory postulates that any device that measures a two-state quantum system must have two preferred states whose representative vectors, $\{|u\rangle, |u^{\perp}\rangle\}$, form an orthonormal basis for the associated vector space. Measurement of a state transforms the state into one of the measuring device's associated basis vectors $|u\rangle$ or $|u^{\perp}\rangle$. The probability that the state is measured as basis vector $|u\rangle$ is the square of the magnitude of the amplitude of the component of the state in the direction of the basis vector $|u\rangle$. For example, given a device for measuring the polarization of

photons with associated basis $\{|u\rangle, |u^\perp\rangle\}$, the state $|v\rangle = a|u\rangle + b|u^\perp\rangle$ is measured as $|u\rangle$ with probability $|a|^2$ and as $|u^\perp\rangle$ with probability $|b|^2$.

This behavior of measurement is an axiom of quantum mechanics. It is not derivable from other physical principles; rather, it is derived from the empirical observation of experiments with measuring devices. If quantum mechanics is correct, all devices that measure single qubits must behave in this way; all have associated bases, and the measurement outcome is always one of the two basis vectors. For this reason, whenever anyone says "measure a qubit," they must specify with respect to which basis the measurement takes place. Throughout the book, if we say "measure a qubit" without further elaboration, we mean that the measurement is with respect to the standard basis $\{|0\rangle, |1\rangle\}$.

Measurement of a quantum state changes the state. If a state $|v\rangle = a|u\rangle + b|u^\perp\rangle$ is measured as $|u\rangle$, then the state $|v\rangle$ changes to $|u\rangle$. A second measurement with respect to the same basis will return $|u\rangle$ with probability 1. Thus, unless the original state happens to be one of the basis states, a single measurement will change that state, making it impossible to determine the original state from any sequence of measurements.

While the mathematics of measuring a qubit in the superposition state $a|0\rangle + b|1\rangle$ with respect to the standard basis is clear, measurement brings up questions as to the meaning of a superposition. To begin with, the notion of superposition is basis-dependent; all states are superpositions with respect to some bases and not with respect to others. For instance, $a|0\rangle + b|1\rangle$ is a superposition with respect to the basis $\{|0\rangle, |1\rangle\}$ but not with respect to $\{a|0\rangle + b|1\rangle, \overline{b}|0\rangle - \overline{a}|1\rangle\}$.

Also, because the result of measuring a superposition is probabilistic, some people are tempted to think of the state $|v\rangle = a|0\rangle + b|1\rangle$ as a probabilistic mixture of $|0\rangle$ and $|1\rangle$. It is not. In particular, it is not true that the state is really either $|0\rangle$ or $|1\rangle$ and that we just do not happen to know which. Rather, $|v\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results: a photon with polarization $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$ behaves deterministically when measured with respect to the Hadamard basis $\{|\nearrow\rangle, |\nwarrow\rangle\}$, but it gives random results when measured with respect to the standard basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$. It is okay to think of a superposition $|v\rangle = a|0\rangle + b|1\rangle$ as in some sense being in both state $|0\rangle$ and state $|1\rangle$ at the same time, as long as that statement is not taken too literally: states that are combinations of $|0\rangle$ and $|1\rangle$ in similar proportions but with different amplitudes, such as $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$, represent distinct states that behave differently in many situations.

Given that qubits can take on any one of infinitely many states, one might hope that a single qubit could store lots of classical information. However, the properties of quantum measurement severely restrict the amount of information that can be extracted from a qubit. Information about a quantum bit can be obtained only by measurement, and any measurement results in one of only two states, the two basis states associated with the measuring device; thus, a single measurement yields at most a single classical bit of information. Because measurement changes the state, one cannot make two measurements on the original state of a qubit. Furthermore, section 5.1.1 shows that an unknown quantum state cannot be cloned, which means it is not possible to measure a qubit's state in two ways, even indirectly by copying the qubit's state and measuring the copy.

assurance they require, Alice and Bob compare a certain number of bit values to check that no eavesdropping has occurred. These bits will also be discarded, and only the remaining bits will be used as their private key.

We describe one sort of attack that Eve can make and how quantum aspects of this protocol guard against it. On the classical channel, Alice and Bob discuss only the choice of bases and not the bit values themselves, so Eve cannot gain any information about the key from listening to the classical channel alone. To gain information, Eve must intercept the photons transmitted by Alice through the quantum channel. Eve must send photons to Bob before knowing the choice of bases made by Alice and Bob, because they compare bases only after Bob has confirmed receipt of the photons. If she sends different photons to Bob, Alice and Bob will detect that something is wrong when they compare bit values, but if she sends the original photons to Bob without doing anything, she gains no information.

To gain information, Eve makes a measurement before sending the photons to Bob. Instead of using a polaroid to measure, she can use a calcite crystal and a photon detector; a beam of light passing through a calcite crystal is split into two spatially separated beams, one polarized in the direction of the crystal's optic axis and the other polarized in the direction perpendicular to the optic axis. A photon detector placed in one of the beams performs a quantum measurement: the probability with which a photon ends up in one of the beams can be calculated just as described in section 2.3.

Since Alice has not yet told Bob her sequence of bases, Eve does not know in which basis to measure each bit. If she randomly measures the bits, she will measure using the wrong basis approximately half of the time. (Exercise 2.10 examines the case in which Eve does not even know which two bases to choose from.) When she uses the wrong basis to measure, the measurement changes the polarization of the photon before it is resent to Bob. This change in the polarization means that, even if Bob measures the photon in the same basis as Alice used to encode the bit, he will get the correct bit value only half the time.

Overall, for each of the qubits Alice and Bob retain, if the qubit was measured by Eve before she sent it to Bob, there will be a 25 percent chance that Bob measures a different bit value than the one Alice sent. Thus, this attack on the quantum channel is bound to introduce a high error rate that Alice and Bob detect by comparing a sufficient number of bits over the classical channel. If these bits agree, they can confidently use the remaining bits as their private key. So, not only is it likely that 25 percent of Eve's version of the key is incorrect, but the fact that someone is eavesdropping can be detected by Alice and Bob. Thus Alice and Bob run little risk of establishing a compromised key; either they succeed in creating a private key or they detect that eavesdropping has taken place.

Eve does not know in which basis to measure the qubits, a property crucial to the security of this protocol, because Alice and Bob share information about which bases they used only after Bob has received the photons; if Eve knew in which basis to measure the photons, her measurements would not change the state, and she could obtain the bit values without Bob and Alice noticing anything suspicious. A seemingly easy way for Eve to overcome this obstacle is for her to copy the qubit, keeping a copy for herself while sending the original on to Bob. Then she can measure her copy

later after learning the correct basis from listening in on the classical channel. Such a protocol is defeated by an important property of quantum information. As we will show in section 5.1.1, the no-cloning principle of quantum mechanics means that it is impossible to reliably copy quantum information unless a basis in which it is encoded is known; all quantum copying machines are basis dependent. Copying with the wrong machine not only does not produce an accurate copy, but it also changes the original in much the same way measuring in the wrong basis does. So Bob and Alice would detect attempts to copy with high probability.

The security of this protocol, like other pure key distribution protocols such as Diffie-Hellman, is vulnerable to a *man-in-the-middle attack* in which Eve impersonates Bob to Alice and impersonates Alice to Bob. To guard against such an attack, Alice and Bob need to combine it with an authentication protocol, be it recognizing each other's voices or a more mathematical authentication protocol.

More sophisticated versions of this protocol exist that support quantum key distribution through noisy channels and stronger guarantees about the amount of information Eve can gain. In the noisy case, Eve is able to gain some information initially, but techniques of quantum error correction and privacy amplification can reduce the amount of information Eve gains to arbitrarily low levels as well as compensate for the noise in the channels.

2.5 The State Space of a Single-Qubit System

The *state space* of a classical or quantum physical system is the set of all possible states of the system. Depending on which properties of the system are under consideration, a state of the system consists of any combination of the positions, momenta, polarizations, spins, energy, and so on of the particles in the system. When we are considering only polarization states of a single photon, the state space is all possible polarizations. More generally, the state space for a single qubit, no matter how it is realized, is the set of possible qubit values,

$$\{a|0\rangle + b|1\rangle\},$$

where $|a|^2 + |b|^2 = 1$ and $a|0\rangle + b|1\rangle$ and $a'|0\rangle + b'|1\rangle$ are considered the same qubit value if $a|0\rangle + b|1\rangle = c(a'|0\rangle + b'|1\rangle)$ for some modulus one complex number c.

2.5.1 Relative Phases versus Global Phases

That the same quantum state is represented by more than one vector means that there is a critical distinction between the complex vector space in which we write our qubit values and the quantum state space itself. We have reduced the ambiguity by requiring that vectors representing quantum states be unit vectors, but some ambiguity remains: unit vectors equivalent up to multiplication by a complex number of modulus one represent the same state. The multiple by which two vectors representing the same quantum state differ is called the *global phase* and has no physical meaning. We use the equivalence relation $|v\rangle \sim |v'\rangle$ to indicate that $|v\rangle = c|v'\rangle$ for some complex global phase $c = e^{i\phi}$. The space in which two two-dimensional complex vectors are considered equivalent if they are multiples of each other is called *complex projective space* of dimension one.

This *quotient space*, a space obtained by identifying sets of equivalent vectors with a single point in the space, is expressed with the compact notation used for quotient spaces:

$$\mathbf{CP}^1 = \{a|0\rangle + b|1\rangle\}/\sim .$$

So the quantum state space for a single-qubit system is in one-to-one correspondence with the points of the complex projective space $\mathbf{CP}^1$. We will make no further use of $\mathbf{CP}^1$ in this book, but it is used in the quantum information processing literature.

Because the linearity of vector spaces makes them easier to work with than projective spaces (we know how to add vectors and there is no corresponding way of adding points in projective spaces), we generally perform all calculations in the vector space corresponding to the quantum state space. The multiplicity of representations of a single quantum state in this vector space representation, however, is a common source of confusion for newcomers to the field.

A physically important quantity is the *relative phase* of a single-qubit state $a|0\rangle + b|1\rangle$. The relative phase (in the standard basis) of a superposition $a|0\rangle + b|1\rangle$ is a measure of the angle in the complex plane between the two complex numbers a and b. More precisely, the relative phase is the modulus one complex number $e^{\mathbf{i}\phi}$ satisfying $a/b = e^{\mathbf{i}\phi}|a|/|b|$. Two superpositions $a|0\rangle + b|1\rangle$ and $a'|0\rangle + b'|1\rangle$ whose amplitudes have the same magnitudes but that differ in a relative phase represent different states.

The physically meaningful relative phase and the physically meaningless global phase should not be confused. While multiplication with a unit constant does not change a quantum state vector, relative phases in a superposition do represent distinct quantum states: even though $|v_1\rangle \sim e^{\mathbf{i}\phi}|v_1\rangle$, the vectors $\frac{1}{\sqrt{2}}(e^{\mathbf{i}\phi}|v_1\rangle + |v_2\rangle)$ and $\frac{1}{\sqrt{2}}(|v_1\rangle + |v_2\rangle)$ do *not* represent the same state. We must always be cognizant of the $\sim$ equivalence when we interpret the results of our computations as quantum states.

A few single-qubit states will be referred to often enough that we give them special labels:

$$|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle) \tag{2.1}$$

$$|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle) \tag{2.2}$$

$$|\mathbf{i}\rangle = 1/\sqrt{2}(|0\rangle + \mathbf{i}|1\rangle) \tag{2.3}$$

$$|-\mathbf{i}\rangle = 1/\sqrt{2}(|0\rangle - \mathbf{i}|1\rangle). \tag{2.4}$$

The basis $\{|+\rangle, |-\rangle\}$ is referred to as the Hadamard basis. We sometimes use the notation $\{|\nwarrow\rangle, |\nearrow\rangle\}$ for the Hadamard basis when discussing photon polarization.

Some authors omit normalization factors, allowing vectors of any length to represent a state where two vectors represent the same state if they differ by any complex factor. We will explicitly write the normalizations factors, both because then the amplitudes have a more direct relation to the measurement probabilities and because keeping track of the normalization factor provides a check that helps avoid errors.

2.5.2 Geometric Views of the State Space of a Single Qubit

While we primarily use vectors to represent quantum states, it is helpful to have models of the single-qubit state space in which there is a one-to-one correspondence between states and points in the space. We give two related but different geometric models with this property. The second of these, the Bloch sphere model, will be used in section 5.4.1 to illustrate single-qubit quantum transformations, and in chapter 10 it will be generalized to aid in the discussion of single-qubit subsystems. These models are just different ways of looking at complex projective space of dimension 1. As we will see, complex projective space of dimension 1 can be viewed as a sphere. First we show that it can be viewed as the extended complex plane, the complex plane $\mathbf{C}$ together with an additional point traditionally labeled ∞.

Extended Complex Plane $\mathbf{C} \cup \{\infty\}$ A correspondence between the set of all complex numbers and single-qubit states is given by

$$a|0\rangle + b|1\rangle \mapsto b/a = \alpha$$

and its inverse

$$\alpha \mapsto \frac{1}{\sqrt{1+|\alpha|^2}}|0\rangle + \frac{\alpha}{\sqrt{1+|\alpha|^2}}|1\rangle.$$

The preceding mapping is not defined for the state with $a = 0$ and $b = 1$. To make this correspondence one-to-one we need to add a single point, which we label ∞, to the complex plane and define $\infty \leftrightarrow |1\rangle$. For example, we have

$$|0\rangle \mapsto 0$$

$$|1\rangle \mapsto \infty$$

$$|+\rangle \mapsto +1$$

$$|-\rangle \mapsto -1$$

$$|\mathbf{i}\rangle \mapsto \mathbf{i}$$

$$|-\mathbf{i}\rangle \mapsto -\mathbf{i}.$$

We now describe another useful model, related to but different from the previous one.

Bloch Sphere Starting with the previous representation, we can map each state, represented by the complex number $\alpha = s + \mathbf{i}t$, onto the unit sphere in three real dimensions, the points $(x, y, z) \in \mathbf{C}$ satisfying $|x|^2 + |y|^2 + |z|^2 = 1$, via the standard *stereographic projection*

$$(s, t) \mapsto \left(\frac{2s}{|\alpha|^2+1}, \frac{2t}{|\alpha|^2+1}, \frac{1-|\alpha|^2}{|\alpha|^2+1} \right),$$

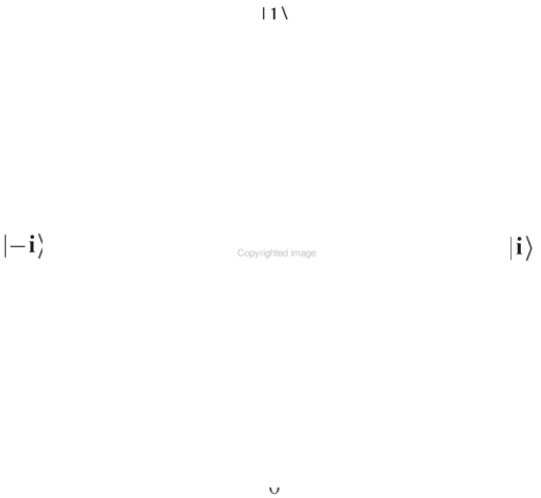

Figure 2.6
Location of certain single-qubit states on the surface of the Bloch sphere.

further requiring that $\infty \mapsto (0, 0, -1)$. Figure 2.6 illustrates the following correspondences:

$|0\rangle \mapsto (0, 0, 1)$

$|1\rangle \mapsto (0, 0, -1)$

$|+\rangle \mapsto (1, 0, 0)$

$|-\rangle \mapsto (-1, 0, 0)$

$|\mathbf{i}\rangle \mapsto (0, 1, 0)$

$|-\mathbf{i}\rangle \mapsto (0, -1, 0)$.

We have given three representations of the quantum state space for a single-qubit system.

1. Vectors written in ket notation: $a|0\rangle + b|1\rangle$ with complex coefficients a and b, subject to $|a|^2 + |b|^2 = 1$, where a and b are unique up to a unit complex factor. Because of this factor, the global phase, this representation is not one-to-one.

2. Extended complex plane: a single complex number $\alpha \in \mathbf{C}$ or ∞. This representation is one-to-one.

3. Bloch sphere: points (x, y, z) on the unit sphere. This representation is also one-to-one.

As we will see in section 10.1, the points in the interior of the sphere also have meaning for quantum information processing. For historical reasons, the entire ball, including the interior, is called the Bloch sphere, instead of just the states on the surface, which truly form a sphere. For

c. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(-|0\rangle + \mathbf{i}|1\rangle)$

d. $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

e. $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and $\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$

f. $\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$ and $\frac{1}{\sqrt{2}}(\mathbf{i}|1\rangle - |0\rangle)$

g. $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|0\rangle$

h. $\frac{1}{\sqrt{2}}(|\mathbf{i}\rangle - |-\mathbf{i}\rangle)$ and $|1\rangle$

i. $\frac{1}{\sqrt{2}}(|\mathbf{i}\rangle + |-\mathbf{i}\rangle)$ and $\frac{1}{\sqrt{2}}(|-\rangle + |+\rangle)$

j. $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\mathbf{i}\pi/4}|1\rangle\right)$ and $\frac{1}{\sqrt{2}}\left(e^{-\mathbf{i}\pi/4}|0\rangle + |1\rangle\right)$

Exercise 2.3. Which states are superpositions with respect to the standard basis, and which are not? For each state that is a superposition, give a basis with respect to which it is not a superposition.

a. $|+\rangle$

b. $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$

c. $\frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

d. $\frac{\sqrt{3}}{2}|+\rangle - \frac{1}{2}|-\rangle)$

e. $\frac{1}{\sqrt{2}}(|\mathbf{i}\rangle - |-\mathbf{i}\rangle)$

f. $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Exercise 2.4. Which of the states in 2.3 are superpositions with respect to the Hadamard basis, and which are not?

Exercise 2.5. Give the set of all values of θ for which the following pairs of states are equivalent.

a. $|1\rangle$ and $\frac{1}{\sqrt{2}}\left(|+\rangle + e^{\mathbf{i}\theta}|-\rangle\right)$

b. $\frac{1}{\sqrt{2}}\left(|\mathbf{i}\rangle + e^{\mathbf{i}\theta}|-\mathbf{i}\rangle\right)$ and $\frac{1}{\sqrt{2}}\left(|-\mathbf{i}\rangle + e^{-\mathbf{i}\theta}|\mathbf{i}\rangle\right)$

c. $\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ and $e^{\mathbf{i}\theta}\left(\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle\right)$

Exercise 2.6. For each pair consisting of a state and a measurement basis, describe the possible measurement outcomes and give the probability for each outcome.

a. $\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle, \{|0\rangle, |1\rangle\}$

b. $\frac{\sqrt{3}}{2}|1\rangle - \frac{1}{2}|0\rangle, \{|0\rangle, |1\rangle\}$

c. $|-\mathbf{i}\rangle, \{|0\rangle, |1\rangle\}$

d. $|0\rangle, \{|+\rangle, |-\rangle\}$

e. $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \{|\mathbf{i}\rangle, |-\mathbf{i}\rangle\}$

f. $|1\rangle, \{|\mathbf{i}\rangle, |-\mathbf{i}\rangle\}$

g. $|+\rangle, \{\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle, \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\}$

Exercise 2.7. For each of the following states, describe all orthonormal bases that include that state.

a. $\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$

b. $\frac{1+\mathbf{i}}{2}|0\rangle - \frac{1-\mathbf{i}}{2}|1\rangle$

c. $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{\mathbf{i}\pi/6}|1\rangle\right)$

d. $\frac{1}{2}|+\rangle - \frac{\mathbf{i}\sqrt{3}}{2}|-\rangle$

Exercise 2.8. Alice is confused. She understands that $|1\rangle$ and $-|1\rangle$ represent the same state. But she does not understand why that does not imply that $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ would be the same state. Can you help her out?

Exercise 2.9. In the BB84 protocol, how many bits do Alice and Bob need to compare to have a 90 percent chance of detecting Eve's presence?

Exercise 2.10. Analyze Eve's success in eavesdropping on the BB84 protocol if she does not even know which two bases to choose from and so chooses a basis at random at each step.

a. On average, what percentage of bit values of the final key will Eve know for sure after listening to Alice and Bob's conversation on the public channel?

b. On average, what percentage of bits in her string are correct?

c. How many bits do Alice and Bob need to compare to have a 90 percent chance of detecting Eve's presence?

Exercise 2.11. *B92 quantum key distribution protocol.* In 1992 Bennett proposed the following quantum key distribution protocol. Instead of encoding each bit in either the standard basis or the Hadamard basis as is done in the BB84 protocol, Alice encodes her random string x as follows

$$0 \mapsto |0\rangle$$
$$1 \mapsto |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and sends them to Bob. Bob generates a random bit string y. If $y_i = 0$ he measures the i th qubit in the Hadamard basis $\{|+\rangle, |-\rangle\}$, if $y_i = 1$ he measures in the standard basis $\{|0\rangle, |1\rangle\}$. In this protocol, instead of telling Alice over the public classical channel which basis he used to measure

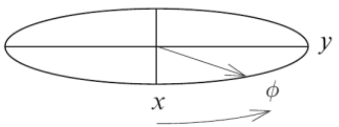

Figure 2.7
Bloch sphere representation of single-qubit quantum states.

each qubit, he tells her the results of his measurements. If his measurement resulted in $|+\rangle$ or $|0\rangle$ Bob sends 0; if his measurement indicates the state is $|1\rangle$ or $|-\rangle$, he sends 1. Alice and Bob discard all bits from strings x and y for which Bob's bit value from measurement yielded 0, obtaining strings x' and y'. Alice uses x' as the secret key and Bob uses y'. Then, depending on the security level they desire, they compare a number of bits to detect tampering. They discard these check bits from their key.

a. Show that if Bob receives exactly the states Alice sends, then the strings x' and y' are identical strings.

b. Why didn't Alice and Bob decide to keep the bits of x and y for which Bob's bit value from measurement was 0?

c. What if an eavesdropper Eve measures each bit in either the standard basis or the Hadamard basis to obtain a bit string z and forwards the measured qubits to Bob? On average, how many bits of Alice and Bob's key does she know for sure after listening in on the public classical? If Alice and Bob compare s bit values of their strings x' and y', how likely are they to detect Eve's presence?

Exercise 2.12. *Bloch Sphere: Spherical coordinates:*

a. Show that the surface of the Bloch sphere can be parametrized in terms of two real-valued parameters, the angles θ and ϕ illustrated in figure 2.7. Make sure your parametrization is in one-to-one correspondence with points on the sphere, and therefore single-qubit quantum states, in the range $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$ except for the points corresponding to $|0\rangle$ and $|1\rangle$.

b. What are θ and ϕ for each of the states $|+\rangle$, $|-\rangle$, $|\mathbf{i}\rangle$, and $|-\mathbf{i}\rangle$?

Exercise 2.13. Relate the four parametrizations of the state space of a single qubit to each other: Give formulas for

a. vectors in ket notation

b. elements of the extended complex plane

c. spherical coordinates for the Bloch sphere (see exercise 2.12)

in terms of the x, y, and z coordinates of the Bloch sphere.

Exercise 2.14.

a. Show that antipodal points on the surface of the Block sphere represent orthogonal states.

b. Show that any two orthogonal states correspond to antipodal points.

3 Multiple-Qubit Systems

The first glimpse into why encoding information in quantum states might support more efficient computation comes when examining systems of more than one qubit. Unlike classical systems, the state space of a quantum system grows exponentially with the number of particles. Thus, when we encode computational information in quantum states of a system of n particles, there are vastly more possible computation states available than when classical states are used to encode the information. The extent to which these large state spaces corresponding to small amounts of physical space can be used to speed up computation will be the subject of much of the rest of this book.

The enormous difference in dimension between classical and quantum state spaces is due to a difference in the way the spaces combine. Imagine a macroscopic physical system consisting of several components. The state of this classical system can be completely characterized by describing the state of each of its component pieces separately. A surprising and unintuitive aspect of quantum systems is that often the state of a system cannot be described in terms of the states of its component pieces. States that cannot be so described are called *entangled states*. Entangled states are a critical ingredient of quantum computation.

Entangled states are a uniquely quantum phenomenon; they have no classical counterpart. Most states in a multiple-qubit system are entangled states; they are what fills the vast quantum state spaces. The impossibility of efficiently simulating the behavior of entangled states on classical computers suggested to Feynman, Manin, and others that it might be possible to use these quantum behaviors to compute more efficiently, leading to the development of the field of quantum computation.

The first few sections of this chapter will be fairly abstract as we develop the mathematical formalism to discuss multiple-qubit systems. We will try to make this material more concrete by including many examples. Section 3.1 formally describes the difference between the way quantum and classical state spaces combine, the difference between the *direct sum* of two or more vector spaces and the *tensor product* of a set of vector spaces. Section 3.1 then explores some of the implications of this difference, including the exponential increase in the dimension of a quantum state space with the number of particles. Section 3.2 formally defines entangled states and begins to describe their uniquely quantum behavior. As a first illustration of the usefulness of this behavior, section 3.4 discusses a second quantum key distribution scheme.

If V and W are inner product spaces, then $V \otimes W$ can be given an inner product by taking the product of the inner products on V and W; the inner product of $|v_1\rangle \otimes |w_1\rangle$ and $|v_2\rangle \otimes |w_2\rangle$ is given by

$$(\langle v_2| \otimes \langle w_2|) \cdot (|v_1\rangle \otimes |w_1\rangle) = \langle v_2|v_1\rangle\langle w_2|w_1\rangle,$$

The tensor product of two unit vectors is a unit vector, and given orthonormal bases $\{|\alpha_i\rangle\}$ for V and $\{|\beta_i\rangle\}$ for W, the basis $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ for $V \otimes W$ is also orthonormal. The tensor product $V \otimes W$ has dimension $\dim(V) \times \dim(W)$, so the tensor product of n two-dimensional vector spaces has 2^n dimensions.

Most elements $|w\rangle \in V \otimes W$ cannot be written as the tensor product of a vector in V and a vector in W (though they are all linear combinations of such elements). This observation is of crucial importance to quantum computation. States of $V \otimes W$ that cannot be written as the tensor product of a vector in V and a vector in W are called *entangled* states. As we will see, for most quantum states of an n-qubit system, in particular for all entangled states, it is not meaningful to talk about the state of a single qubit of the system.

A tensor product structure also underlies probability theory. While the tensor product structure there is rarely mentioned, a common source of confusion is a tendency to try to impose a direct sum structure on what is actually a tensor product structure. Readers may find it useful to read section A.1, which discusses the tensor product structure inherent in probability theory, which illustrates the use of tensor product in another, more familiar, context. Readers may also wish to do exercises A.1 through A.4.

3.1.3 The State Space of an n-Qubit System

Given two quantum systems with states represented by unit vectors in V and W respectively, the possible states of the joint quantum system are represented by unit vectors in the vector space $V \otimes W$. For $0 \leq i < n$, let V_i be the vector space, with basis $\{|0\rangle_i, |1\rangle_i\}$, corresponding to a single qubit. The standard basis for the vector space $V_{n-1} \otimes \cdots \otimes V_1 \otimes V_0$ for an n-qubit system consists of the 2^n vectors

$$\{|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |0\rangle_0,$$

$$|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |1\rangle_0,$$

$$|0\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |0\rangle_0,$$

$$\vdots,$$

$$|1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |1\rangle_0\}.$$

The subscripts are often dropped, since the corresponding qubit is clear from position. The convention that adjacency of kets means the tensor product enables us to write this basis more compactly:

$$\{|0\rangle \cdots |0\rangle|0\rangle,$$

$$|0\rangle \cdots |0\rangle|1\rangle,$$

$$|0\rangle \cdots |1\rangle|0\rangle,$$

$$\vdots,$$

$$|1\rangle \cdots |1\rangle|1\rangle\}.$$

Since the tensor product space corresponding to an n-qubit system occurs so frequently throughout quantum information processing, an even more compact and readable notation uses $|b_{n-1} \ldots b_0\rangle$ to represent $|b_{n-1}\rangle \otimes \cdots \otimes |b_0\rangle$. In this notation the standard basis for an n-qubit system can be written

$$\{|0 \cdots 00\rangle, |0 \cdots 01\rangle, |0 \cdots 10\rangle, \ldots, |1 \cdots 11\rangle\}.$$

Finally, since decimal notation is more compact than binary notation, we will represent the state $|b_{n-1} \ldots b_0\rangle$ more compactly as $|x\rangle$, where b_i are the digits of the binary representation for the decimal number x. In this notation, the standard basis for an n-qubit system is written

$$\{|0\rangle, |1\rangle, |2\rangle, \ldots, |2^n - 1\rangle\}.$$

The standard basis for a two-qubit system can be written as

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\},$$

and the standard basis for a three-qubit system can be written as

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

$$= \{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle\}.$$

Since the notation $|3\rangle$ corresponds to two different quantum states in these two bases, one a two-qubit state, the other a three-qubit state, in order for such notation to be unambiguous, the number of qubits must be clear from context.

We often revert to a less compact notation when we wish to set apart certain sets of qubits, to indicate separate registers of a quantum computer, or to indicate qubits controlled by different people. If Alice controls the first two qubits and Bob the last three, we may write a state as $\frac{1}{\sqrt{2}}(|00\rangle|101\rangle + |10\rangle|011\rangle)$, or even as $\frac{1}{\sqrt{2}}(|00\rangle_A|101\rangle_B + |10\rangle_A|011\rangle_B)$, where the subscripts indicate which qubits Alice controls and which qubits Bob controls.

Example 3.1.3 The superpositions

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|7\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$$

and

$$\frac{1}{2}(|1\rangle + |2\rangle + |4\rangle + |7\rangle) = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$$

represent possible states of a three-qubit system.

To use matrix notation for state vectors of an n-qubit system, the order of basis vectors must be established. Unless specified otherwise, basis vectors labeled with numbers are assumed to be sorted numerically. Using this convention, the two qubit state

$$\frac{1}{2}|00\rangle + \frac{\mathbf{i}}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{2}|0\rangle + \frac{\mathbf{i}}{2}|1\rangle + \frac{1}{\sqrt{2}}|3\rangle$$

will have matrix representation

$$\begin{pmatrix} \frac{1}{2} \\ \frac{\mathbf{i}}{2} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}.$$

We use the standard basis predominantly, but we use other bases from time to time. For example, the following basis, the Bell basis for a two-qubit system, $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, where

$$\begin{aligned} |\Phi^+\rangle &= 1/\sqrt{2}(|00\rangle + |11\rangle \\ |\Phi^-\rangle &= 1/\sqrt{2}(|00\rangle - |11\rangle \\ |\Psi^+\rangle &= 1/\sqrt{2}(|01\rangle + |10\rangle \\ |\Psi^-\rangle &= 1/\sqrt{2}(|01\rangle - |10\rangle, \end{aligned} \tag{3.1}$$

is important for various applications of quantum information processing including quantum teleportation. As in the single-qubit case, a state $|v\rangle$ is a superposition with respect to a set of orthonormal states $\{|\beta_1\rangle, \ldots, |\beta_i\rangle\}$ if it is a linear combination of these states, $|v\rangle = a_1|\beta_1\rangle + \cdots + a_i|\beta_i\rangle$, and at least two of the a_i are non-zero. When no set of orthonormal states is specified, we will mean that the superposition is with respect to the standard basis.

Any unit vector of the 2^n-dimensional state space represents a possible state of an n-qubit system, but just as in the single-qubit case there is redundancy. In the multiple-qubit case, not only do vectors that are multiples of each other refer to the same quantum state, but properties of the tensor product also mean that phase factors distribute over tensor products; the same phase factor in different qubits of a tensor product represent the same state:

$$|v\rangle \otimes (e^{\mathbf{i}\phi}|w\rangle) = e^{\mathbf{i}\phi}(|v\rangle \otimes |w\rangle) = (e^{\mathbf{i}\phi}|v\rangle) \otimes |w\rangle.$$

Phase factors in individual qubits of a single term of a superposition can always be factored out into a single coefficient for that term.

Example 3.1.4 $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Example 3.1.5 $(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{\mathbf{i}}{\sqrt{2}}|1\rangle) = \frac{1}{2\sqrt{2}}|00\rangle + \frac{\mathbf{i}}{2\sqrt{2}}|01\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|10\rangle + \frac{\mathbf{i}\sqrt{3}}{2\sqrt{2}}|11\rangle)$

Just as in the single-qubit case, vectors that differ only in a global phase represent the same quantum state. If we write every quantum state as

$$a_0|0\ldots00\rangle + a_1|0\ldots01\rangle + \cdots + a_{2^n-1}|1\ldots11\rangle$$

and require the first non-zero a_i to be real and non-negative, then every quantum state has a unique representation. Since this representation uniquely represents quantum states, the quantum state space of an n-qubit system has $2^n - 1$ complex dimensions. For any complex vector space of dimension N, the space in which vectors that are multiples of each other are considered equivalent is called *complex projective space* of dimension $N - 1$. So the space of distinct quantum states of an n-qubit system is a complex projective space of dimension $2^n - 1$.

Just as in the single-qubit case, we must be careful not to confuse the vector space in which we write our computations with the quantum state space itself. Again, we must be careful to avoid confusion between the relative phases between terms in the superposition, of critical importance in quantum mechanics, and the global phase which has no physical meaning. Using the notation of section 2.5.1, we write $|v\rangle \sim |w\rangle$ when two vectors $|v\rangle$ and $|w\rangle$ differ only by a global phase and thus represent the same quantum state. For example, even though $|00\rangle \sim e^{\mathbf{i}\phi}|00\rangle$, the vectors $|v\rangle = \frac{1}{\sqrt{2}}(e^{\mathbf{i}\phi}|00\rangle + |11\rangle)$ and $|w\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ represent different quantum states, which behave differently in many situations:

$$\frac{1}{\sqrt{2}}(e^{\mathbf{i}\phi}|00\rangle + |11\rangle) \not\sim \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

However,

$$\frac{1}{\sqrt{2}}(e^{\mathbf{i}\phi}|00\rangle + e^{\mathbf{i}\phi}|11\rangle) \sim \frac{e^{\mathbf{i}\phi}}{\sqrt{2}}(|00\rangle + |11\rangle) \sim \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Quantum mechanical calculations are usually performed in the vector space rather than in the projective space because linearity makes vector spaces easier to work with. But we must always be aware of the $\sim$ equivalence when we interpret the results of our calculations as quantum states. Further confusions arise when states are written in different bases. Recall from section 2.5.1 that $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The expression $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ is a different way of writing $|0\rangle$, and $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and $\frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)$ are simply different expressions for the same vector.

Fluency with properties of tensor products, and with the notation just presented, will be crucial for understanding the rest of the book. The reader is strongly encouraged to work exercises 3.1 through 3.9 at this point to begin to develop that fluency.

3.2 Entangled States

As we saw in section 2.5.2, a single-qubit state can be specified by a single complex number so any tensor product of n individual single-qubit states can be specified by n complex numbers. But in the last section, we saw that it takes $2^n - 1$ complex numbers to describe states of an n-qubit system. Since $2^n \gg n$, the vast majority of n-qubit states cannot be described in terms of the state of n separate single-qubit systems. States that cannot be written as the tensor product of n single-qubit states are called *entangled* states. Thus the vast majority of quantum states are entangled.

Example 3.2.1 The elements of the Bell basis (Equation 3.1) are entangled. For instance, the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be described in terms of the state of each of its component qubits separately. This state cannot be decomposed, because it is impossible to find a_1, a_2, b_1, b_2 such that

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

since

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

and $a_1b_2 = 0$ implies that either $a_1a_2 = 0$ or $b_1b_2 = 0$. Two particles in the Bell state $|\Phi^+\rangle$ are called an EPR pair for reasons that will become apparent in section 4.4.

Example 3.2.2 Other examples of two-qubit entangled states include

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$\frac{1}{\sqrt{2}}(|00\rangle - i|11\rangle),$$

$$\frac{i}{10}|00\rangle + \frac{\sqrt{99}}{10}|11\rangle),$$

and

$$\frac{7}{10}|00\rangle + \frac{1}{10}|01\rangle + \frac{1}{10}|10\rangle + \frac{7}{10}|11\rangle).$$

---

when such states are considered in different bases. Nevertheless, as long as one is aware that this description should not be taken too literally, it can be helpful at first to think of superpositions as being in multiple states at once. Over the course of this chapter and the next, you will begin to develop more of a feel for the workings of these states.

Not only is entanglement between qubits key to the exponential size of quantum state spaces of multiple-qubit systems, but, as we will see in sections 3.4, 5.3.1, and 5.3.2, particles in an entangled state can also be used to aid communication of both classical and quantum information. Furthermore, the quantum algorithms of part II exploit entanglement to speed up computation. The way entangled states behave when measured is one of the central mysteries of quantum mechanics, as well as a source of power for quantum information processing. Entanglement and quantum measurement are two of the uniquely quantum properties that are exploited in quantum information processing.

3.3 Basics of Multi-Qubit Measurement

The experiment of section 2.1.2 illustrates how measurement of a single qubit is probabilistic and transforms the quantum state into a state compatible with the measuring device. A similar statement is true for measurements of multiple-qubit systems, except that the set of possible measurements and measurement outcomes is significantly richer than in the single-qubit case. The next paragraph develops some mathematical formalism to handle the general case.

Let V be the $N = 2^n$ dimensional vector space associated with an n-qubit system. Any device that measures this system has an associated direct sum decomposition into orthogonal subspaces

$$V = S_1 \oplus \cdots \oplus S_k$$

for some $k \leq N$. The number k corresponds to the maximum number of possible measurement outcomes for a state measured with that particular device. This number varies from device to device, even between devices measuring the same system. That any device has an associated direct sum decomposition is a direct generalization of the single-qubit case. Every device measuring a single-qubit system has an associated orthonormal basis $\{|v_1\rangle, |v_2\rangle\}$ for the vector space V associated with the single-qubit system; the vectors $|v_i\rangle$ each generate a one-dimensional subspace S_i (consisting of all multiples $a|v_i\rangle$ where a is a complex number), and $V = S_1 \oplus S_2$. Furthermore, the only nontrivial decompositions of the vector space V are into two one-dimensional subspaces, and any choice of unit length vectors, one from each of the subspaces, yields an orthonormal basis.

When a measuring device with associated direct sum decomposition $V = S_1 \oplus \cdots \oplus S_k$ interacts with an n-qubit system in state $|\psi\rangle$, the interaction changes the state to one entirely contained within one of the subspaces, and chooses the subspace with probability equal to the square of the absolute value of the amplitude of the component of $|\psi\rangle$ in that subspace. More formally, the state $|\psi\rangle$ has a unique direct sum decomposition $|\psi\rangle = a_1|\psi_1\rangle \oplus \cdots \oplus a_k|\psi_k\rangle$, where $|\psi_i\rangle$ is a unit vector in S_i and a_i is real and non-negative. When $|\psi\rangle$ is measured, the state $|\psi_i\rangle$ is obtained

with probability $|a_i|^2$. That any measuring device has an associated direct sum decomposition, and that the interaction can be modeled in this way, is an axiom of quantum mechanics. It is not possible to prove that every device behaves in this way, but so far it has provided an excellent model that predicts the outcome of experiments with high accuracy.

Example 3.3.1 *Single-qubit measurement in the standard basis.* Let V be the vector space associated with a single-qubit system. A device that measures a qubit in the standard basis has, by definition, the associated direct sum decomposition $V = S_1 \oplus S_2$, where S_1 is generated by $|0\rangle$ and S_2 is generated by $|1\rangle$. An arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle$ measured by such a device will be $|0\rangle$ with probability $|a|^2$, the amplitude of $|\psi\rangle$ in the subspace S_1, and $|1\rangle$ with probability $|b|^2$.

Example 3.3.2 *Single-qubit measurement in the Hadamard basis.* A device that measures a single qubit in the Hadamard basis

$$\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

has associated subspace decomposition $V = S_+ \oplus S_-$, where S_+ is generated by $|+\rangle$ and S_- is generated by $|-\rangle$. A state $|\psi\rangle = a|0\rangle + b|1\rangle$ can be rewritten as $|\psi\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle$, so the probability that $|\psi\rangle$ is measured as $|+\rangle$ will be $\left|\frac{a+b}{\sqrt{2}}\right|^2$ and $|-\rangle$ will be $\left|\frac{a-b}{\sqrt{2}}\right|^2$.

The next two examples describe measurements of two-qubit states that are used in the entanglement-based quantum key distribution protocol described in section 3.4. Chapter 4 explores measurement of multiple-qubit systems in more detail and builds up the standard notational shorthand for describing quantum measurements.

Example 3.3.3 *Measurement of the first qubit of a two-qubit state in the standard basis.* Let V be the vector space associated with a two-qubit system. A device that measures the first qubit in the standard basis has associated subspace decomposition $V = S_1 \oplus S_2$ where $S_1 = |0\rangle \otimes V_2$, the two-dimensional subspace spanned by $\{|00\rangle, |01\rangle\}$, and $S_2 = |1\rangle \otimes V_2$, which is spanned by $\{|10\rangle, |11\rangle\}$. To see what happens when such a device measures an arbitrary two-qubit state $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$, we write $|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle$ where $|\psi_1\rangle = 1/c_1(a_{00}|00\rangle + a_{01}|01\rangle) \in S_1$ and $|\psi_2\rangle = 1/c_2(a_{10}|10\rangle + a_{11}|11\rangle) \in S_2$, with $c_1 = \sqrt{|a_{00}|^2 + |a_{01}|^2}$ and $c_2 = \sqrt{|a_{10}|^2 + |a_{11}|^2}$ as the normalization factors. Measurement of $|\psi\rangle$ with this device results in the state $|\psi_1\rangle$ with probability $|c_1|^2 = |a_{00}|^2 + |a_{01}|^2$ and the state $|\psi_2\rangle$ with probability $|c_2|^2 = |a_{10}|^2 + |a_{11}|^2$. In particular, when the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is measured, we obtain $|00\rangle$ and $|11\rangle$ with equal probability.

Example 3.3.4 *Measurement of the first qubit of a two-qubit state in the Hadamard basis.* A device that measures the first qubit of a two-qubit system with respect to the Hadamard basis $\{|+\rangle, |-\rangle\}$ has an associated direct sum decomposition $V = S_1' \oplus S_2'$, where $S_1' = |+\rangle \otimes V_2$, the two-dimensional subspace spanned by $\{|+\rangle|0\rangle, |+\rangle|1\rangle\}$, and $S_2' = |-\rangle \otimes V_2$. We write $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ as $|\psi\rangle = a_1'|\psi_1'\rangle + a_2'|\psi_2'\rangle$, where

$$|\psi_1'\rangle = c_1' \left(\frac{a_{00} + a_{10}}{\sqrt{2}} |+\rangle|0\rangle + \frac{a_{01} + a_{11}}{\sqrt{2}} |+\rangle|1\rangle \right)$$

and

$$|\psi_2'\rangle = c_2' \left(\frac{a_{00} - a_{10}}{\sqrt{2}} |-\rangle|0\rangle + \frac{a_{01} - a_{11}}{\sqrt{2}} |-\rangle|1\rangle \right).$$

We leave it to the reader to calculate c_1' and c_2' and the probabilities for the two outcomes, and to show that such a measurement on the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$ yields $|+\rangle|+\rangle$ and $|-\rangle|-\rangle$ with equal probability.

3.4 Quantum Key Distribution Using Entangled States

In 1991, Artur Ekert developed a quantum key distribution scheme that makes use of special properties of entangled states. The Ekert 91 protocol resembles the BB84 protocol of section 2.4 in some ways. In his protocol, Alice and Bob establish a shared key by separately performing random measurements on their halves of an EPR pair and then comparing which bases they used over a classical channel.

Because Alice and Bob do not exchange quantum states during the protocol, and an eavesdropper Eve cannot learn anything useful by listening in on the classical exchange alone, Eve's only chance to obtain information about the key is for her to interact with the purported EPR pair as it is being created or transmitted in the setup for the protocol. For this reason it is easier to prove the security of protocols based on entangled states. Such proofs have then been modified to prove the security of other QKD protocols like BB84. As with BB84, we describe only the protocol; tools developed in later chapters are needed to describe many of Eve's possible attacks and to give a proof of security. Exercise 3.15 analyzes the limited effectiveness of some simple attacks Eve could make.

The protocol begins with the creation of a sequence of pairs of qubits, all in the entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$. Alice receives the first qubit of each pair, while Bob receives the second. When they wish to create a secret key, for each qubit they both independently and randomly choose either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$ in which to measure, just as in the BB84 protocol. After they have made their measurements, they compare bases and discard those bits for which their bases differ.

If Alice measures the first qubit in the standard basis and obtains $|0\rangle$, then the entire state becomes $|00\rangle$. If Bob now measures in the standard basis, he obtains the result $|0\rangle$ with certainty. If instead he measures in the Hadamard basis $\{|+\rangle, |-\rangle\}$, he obtains $|+\rangle$ and $|-\rangle$ with equal probability, since $|00\rangle = |0\rangle(\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle))$. Just as in the BB84 protocol, he interprets the states $|+\rangle$ and $|-\rangle$ as corresponding to the classical bit values 0 and 1 respectively; thus when he measures in the basis $\{|+\rangle|-\rangle\}$ and Alice measures in the standard basis, he obtains the same bit value as Alice only half the time. The behavior is similar when Alice's measurement indicates her qubit is in state $|1\rangle$. If instead Alice measures in the Hadamard basis and obtains the result that her qubit is in the state $|+\rangle$, the whole state becomes $|+\rangle|+\rangle$. If Bob now measures in the Hadamard basis, he obtains $|+\rangle$ with certainty, whereas if he measures in the standard basis he obtains $|0\rangle$ and $|1\rangle$ with equal probability. Since they always get the same bit value if they measure in the same basis, the protocol results in a shared random key, as long as the initial pairs were EPR pairs. The security of the scheme relies on adding steps to the protocol we have just described that enable Alice and Bob to test the fidelity of their EPR pairs. We are not yet in a position to describe such tests. The tests Ekert suggested are based on Bell's inequalities (section 4.4.3). Other, more efficient tests have been devised.

This protocol has the intriguing property that in theory Alice and Bob can prepare shared keys as they need them, never needing to store keys for any length of time. In practice, to prepare keys on an as-needed basis in this way, Alice and Bob would need to be able to store their EPR pairs so that they are not corrupted during that time. The capability of long-term reliable storage of entangled states does not exist at present.

3.5 References

In the early 1980s, Richard Feynman and Yuri Manin separately recognized that certain quantum phenomena associated with entangled particles could not be simulated efficiently on standard computers. Turning this observation around caused them to speculate whether these quantum phenomena could be used to speed up computation in general. Their early musings on quantum computation can be found in [121], [150], [202], and [203].

More extensive treatments of the tensor product can be found in Arno Bohm's *Quantum Mechanics* [53], Paul Bamberg and Shlomo Sternberg's *A Course in Mathematics for Students of Physics* [30], and Thomas Hungerford's *Algebra* [158].

Ekert's key distribution protocol based on EPR pairs, originally proposed in [111], has been demonstrated in the laboratory [163, 294]. Gisin et al. [130] provide a detailed survey of work on quantum key distribution including Ekert's algorithm.

3.6 Exercises

Exercise 3.1. Let V be a vector space with basis $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. Give two different bases for $V \otimes V$.