

Quantum Science and Technology

Renato Portugal

Quantum Walks and Search Algorithms

Second Edition

 Springer

Quantum Science and Technology

Series editors

Raymond Laflamme, Waterloo, Canada

Gaby Lenhart, Sophia Antipolis, France

Daniel Lidar, Los Angeles, USA

Arno Rauschenbeutel, Vienna, Austria

Renato Renner, Zürich, Switzerland

Maximilian Schlosshauer, Portland, USA

Yaakov S. Weinstein, Princeton, USA

H. M. Wiseman, Brisbane, Australia

Aims and Scope

The book series Quantum Science and Technology is dedicated to one of today's most active and rapidly expanding fields of research and development. In particular, the series will be a showcase for the growing number of experimental implementations and practical applications of quantum systems. These will include, but are not restricted to: quantum information processing, quantum computing, and quantum simulation; quantum communication and quantum cryptography; entanglement and other quantum resources; quantum interfaces and hybrid quantum systems; quantum memories and quantum repeaters; measurement-based quantum control and quantum feedback; quantum nanomechanics, quantum optomechanics and quantum transducers; quantum sensing and quantum metrology; as well as quantum effects in biology. Last but not least, the series will include books on the theoretical and mathematical questions relevant to designing and understanding these systems and devices, as well as foundational issues concerning the quantum phenomena themselves. Written and edited by leading experts, the treatments will be designed for graduate students and other researchers already working in, or intending to enter the field of quantum science and technology.

More information about this series at <http://www.springer.com/series/10039>

Renato Portugal

Quantum Walks and Search Algorithms

Second Edition

 Springer

Renato Portugal
National Laboratory of Scientific
Computing (LNCC)
Petrópolis, Brazil

ISSN 2364-9054 ISSN 2364-9062 (electronic)
Quantum Science and Technology
ISBN 978-3-319-97812-3 ISBN 978-3-319-97813-0 (eBook)
<https://doi.org/10.1007/978-3-319-97813-0>

Library of Congress Control Number: 2018950813

1st edition: © Springer Science+Business Media New York 2013

2nd edition: © Springer Nature Switzerland AG 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To my father (in memoriam)

Preface

This is a textbook about *quantum walks* and *quantum search algorithms*. The readers will take advantage of the pedagogical aspects and learn the topics faster and make less effort than reading the original research papers, often too convoluted. The exercises and references allow the readers to deepen their knowledge on specific issues. Guidelines to use or to develop computer programs for simulating the evolution of quantum walks are also available.

Almost nothing can be extracted from this book if the reader is unfamiliar with the postulates of quantum mechanics, described in the second chapter, and the material on linear algebra described in Appendix A. Some extra bases are required: It is desirable that the reader has (1) notions of quantum computing, including the circuit model, references of which are provided at the end of Appendix A, (2) notions of graph theory, references of which are provided at the end of Appendix B, and (3) notions of classical algorithms and computational complexity. Any undergraduate or graduate student with this background can read this book. Some topics addressed in this second edition are currently active research areas with impact on the development of new quantum algorithms. Because of that, researchers working with quantum computing may find this book useful.

The second edition brings at least three main novelties: (1) a new chapter on the staggered quantum walk model—Chap. 8, (2) a new chapter on the element distinctness problem—Chap. 10, and (3) a new appendix on graph theory—Appendix B. Besides, the chapter on quantum-walk-based search algorithm—Chap. 9—was rewritten, the presentation has been simplified, and new material has been included.

Corrections, suggestions, and comments are welcome, which can be sent through Web page (qubit.lncc.br) or directly to the author by email (portugal@lncc.br).

Petrópolis, RJ, Brazil

Renato Portugal

Acknowledgements

I am grateful to many people, including colleagues, graduate students, and the group of quantum computing of LNCC, friends and coauthors in research papers, projects, and conference organization. I am also grateful to many researchers for exchanging ideas in conferences and in collaborations. Some of them helped by reviewing, giving essential suggestions, and spending time on this project, in special, Drs. Stefan Boettcher, Norio Konno, Raqueline Santos, and Etsuo Segawa.

In January and February 2018, I gave a short course on quantum-walk-based search algorithms at the Tohoku University under the invitation of Dr. Etsuo Segawa. I thank the students and researchers that attended the course, who raised interesting discussion topics, helping to improve some chapters of the new edition of this book.

I thank Tom Spicer and Cindy Zitter from Springer for encouraging me to write the second edition, which turned out to be an opportunity for fixing many problems of the first edition and improving the book by adding new material. I hope to have introduced fewer problems this time.

I thank the support of the National Laboratory of Scientific Computing (LNCC), the funding agencies CNPq, CAPES, and FAPERJ, and the scientific societies SBMAC and SBC.

Last but not least, from the bottom of my heart, I thank my family, wife and sons, for giving support and amplifying my inner motivation.

Contents

1	Introduction	1
2	The Postulates of Quantum Mechanics	5
2.1	State Space	5
2.1.1	State Space Postulate	7
2.2	Unitary Evolution	8
2.2.1	Evolution Postulate	8
2.3	Composite Systems	11
2.4	Measurement Process	12
2.4.1	Measurement Postulate	12
2.4.2	Measurement in the Computational Basis	14
2.4.3	Partial Measurement in the Computational Basis	16
3	Introduction to Quantum Walks	19
3.1	Classical Random Walk on the Line	19
3.2	Classical Discrete-Time Markov Chains	23
3.3	Coined Quantum Walks	25
3.3.1	Coined Walk on the Line	26
3.4	Classical Continuous-Time Markov Chains	33
3.5	Continuous-Time Quantum Walks	35
3.5.1	Continuous-Time Walk on the Line	35
3.5.2	Why Must Time be Continuous?	38
4	Grover's Algorithm and Its Generalization	41
4.1	Grover's Algorithm	42
4.2	Quantum Circuit of Grover's Algorithm	44
4.3	Analysis of the Algorithm Using Reflection Operators	45
4.4	Analysis Using the Two-Dimensional Real Space	50
4.5	Analysis Using the Spectral Decomposition	52
4.6	Optimality of Grover's Algorithm	53
4.7	Search with Repeated Elements	59

4.7.1	Analysis Using Reflection Operators	60
4.7.2	Analysis Using the Reduced Space	62
4.8	Amplitude Amplification	63
4.8.1	The Technique	64
5	Coined Walks on Infinite Lattices	69
5.1	Hadamard Walk on the Line	69
5.1.1	Fourier Transform	71
5.1.2	Analytic Solution	75
5.1.3	Other Coins	78
5.2	Two-Dimensional Lattice	79
5.2.1	The Hadamard Coin	81
5.2.2	The Fourier Coin	82
5.2.3	The Grover Coin	83
5.2.4	Standard Deviation	84
5.3	Quantum Walk Packages	85
6	Coined Walks with Cyclic Boundary Conditions	89
6.1	Cycles	89
6.1.1	Fourier Transform	91
6.1.2	Analytic Solutions	94
6.1.3	Periodic Solutions	97
6.2	Finite Two-Dimensional Lattices	98
6.2.1	Fourier Transform	100
6.2.2	Analytic Solutions	104
6.3	Hypercubes	106
6.3.1	Fourier Transform	108
6.3.2	Analytic Solutions	114
6.3.3	Reducing a Hypercube to a Line Segment	115
7	Coined Quantum Walks on Graphs	125
7.1	Quantum Walks on Class-1 Regular Graphs	126
7.2	Coined Quantum Walks on Arbitrary Graphs	127
7.2.1	Locality	129
7.2.2	Grover Quantum Walk	130
7.2.3	Coined Walks on Cayley Graphs	131
7.2.4	Coined Walks on Multigraphs	132
7.3	Dynamics and Quasi-periodicity	132
7.4	Perfect State Transfer and Fractional Revival	137
7.5	Limiting Probability Distribution	139
7.5.1	Limiting Distribution Using the Fourier Basis	142
7.5.2	Limiting Distribution of QWs on Cycles	143
7.5.3	Limiting Distribution of QWs on Hypercubes	147
7.5.4	Limiting Distribution of QWs on Finite Lattices	150

7.6	Distance Between Distributions	152
7.7	Mixing Time	155
7.7.1	Instantaneous Uniform Mixing (IUM)	156
8	Staggered Model	159
8.1	Graph Tessellation Cover	159
8.2	The Evolution Operator	161
8.3	Staggered Walk on the Line	163
8.3.1	Fourier Analysis	167
8.3.2	Standard Deviation	169
9	Spatial Search Algorithms	175
9.1	Quantum-Walk-Based Search Algorithms	176
9.2	Analysis of the Time Complexity	178
9.2.1	Case $B = 0$	182
9.2.2	Tulsi's Modification	183
9.3	Finite Two-Dimensional Lattices	186
9.3.1	Tulsi's Modification of the Two-Dimensional Lattice	191
9.4	Hypercubes	192
9.5	Grover's Algorithm as Spatial Search on Graphs	195
9.5.1	Grover's Algorithm in terms of the Coined Model	195
9.5.2	Grover's Algorithm in terms of the Staggered Model	197
9.5.3	Complexity Analysis of Grover's Algorithm	198
10	Element Distinctness	201
10.1	Classical Algorithms	202
10.2	Naïve Quantum Algorithms	202
10.3	The Optimal Quantum Algorithm	203
10.3.1	Analysis of the Algorithm	207
10.3.2	Number of Queries	216
10.3.3	Example	218
11	Szegedy's Quantum Walk	223
11.1	Discrete-Time Markov Chains	223
11.2	Markov Chain-Based Quantum Walk	224
11.3	Evolution Operator	227
11.4	Singular Values and Vectors of the Discriminant	228
11.5	Eigenvalues and Eigenvectors of the Evolution Operator	230
11.6	Quantum Hitting Time	234
11.7	Searching Instead of Detecting	237
11.8	Example: Complete Graphs	237
11.8.1	Probability of Finding a Marked Element	242

Appendix A: Linear Algebra for Quantum Computation	247
Appendix B: Graph Theory for Quantum Walks.	271
Appendix C: Classical Hitting Time	281
References	289
Index	303

Chapter 1

Introduction



Quantum mechanics has changed the way we understand the physical world and has introduced new ideas that are difficult to accept, not because they are complex, but because they are different from what we are used to in our everyday lives. Those new ideas can be collected in four postulates or laws. It is hard to believe that Nature works according to those laws, and the difficulty starts with the notion of the superposition of contradictory possibilities. Do you accept the idea that a billiard ball could rotate around its axis in both directions at the same time?

Quantum computation was born from this kind of idea. We know that digital classical computers work with zeroes and ones and that the value of the bit cannot be zero and one at the same time. The classical algorithms must obey Boolean logic. So, if the coexistence of bit-0 and bit-1 is possible, which logic should the algorithms obey?

Quantum computation was born from a paradigm change. Information storage, processing, and transmission obeying quantum mechanical laws allowed the development of new algorithms, faster than the classical analogues, which can be implemented in physics laboratories. Nowadays, quantum computation is a well-established area with important theoretical results within the context of the theory of computing, as well as in terms of physics, and has raised huge engineering challenges to the construction of the quantum hardware.

The majority of people, who are not familiar with the area and talk about quantum computers, expect that the hardware development would obey the famous Moore's law, valid for classical computer development for fifty years. Many of those people are disappointed to learn about the enormous theoretical and technological difficulties to be overcome to harness and control quantum systems whose tendency is to behave classically. On the one hand, the quantum CPU must be large enough and must stay coherent long enough to allow at least thousands of steps in order to produce a nontrivial output.

The processing of classical computers is very stable. Depending on the calculation, an inversion of a single bit could invalidate the entire process. But we know that long computations, which require inversion of billions of bits, are performed without problems. Classical computers are unerring because its basic components

are stable. Consider, for example, a mechanical computer. It would be very unusual for a mechanical device to change its position, especially if we put a spring to keep it stable in the desired position. The same is true for electronic devices, which remain in their states until an electrical pulse of sufficient power changes this. Electronic devices are built to operate at a power level well above the noise, and this noise is kept low by dissipating heat into the environment.

The laws of quantum mechanics require that the physical device must be isolated from the environment; otherwise the superposition vanishes, at least partially. It is too difficult a task to isolate macroscopic physical systems from their environment. Ultra-relativistic particles and gravitational waves pass through any blockade, penetrate into the most guarded places, obtain information, and convey it out of the system. This process is equivalent to a measurement of a quantum observable, which often collapses the superposition and slows down the quantum computer, making it almost, or entirely, equivalent to the classical one. Theoretical results show that there are no fundamental issues against the possibility of building quantum hardware. It is a matter of technological difficulty.

There is no point in building quantum computers if we are going to use them in the same way we use classical computers. Algorithms must be rewritten, and new techniques for simulating physical systems must be developed. The task is more difficult than for classical computers. So far, we do not have a quantum programming language. Also, quantum algorithms must be developed using concepts of linear algebra. Quantum computers with a large enough number of qubits are not available, as yet, slowing down the development of simulations. At the moment that the second edition of this book is to be released, Google and IBM and Intel have built universal quantum computers with 72 and 50 and 49 qubits, respectively, using superconducting electronic circuits which need temperatures as low as one-tenth of one Kelvin or around one-thirtieth of the temperature in deep space. Despite those impressive achievements, the coherence time announced by IBM is around 90 ms, not enough yet.

The quantum walk (QW) is a powerful technique for building quantum algorithms and for simulating complex quantum systems. Quantum walks were developed in the beginning as the quantum version of the classical random walk, which requires the tossing of a coin to determine the direction of the next step. The laws of quantum mechanics state that the evolution of an isolated quantum system is deterministic. Randomness shows up only when the system is measured and classical information is obtained. This explains why the name “quantum random walk” is seldom used. The coined model evolves at discrete time steps on a discrete space, which is modeled by a graph. The coined model is not the only discrete-time version of quantum walks. In fact, there is a coinless version called staggered model, which uses an evolution operator defined by partitioning the vertex set. Besides, there is a continuous-time version, which has been extensively studied.

The richness of the area has attracted the attention of the scientific community, and the interest has increased significantly in the last years. Good parameters to test this statement are shown in Fig. 1.1, which depicts the number of paper with the tag “quantum walk” either in the title or in the topics returned after querying the

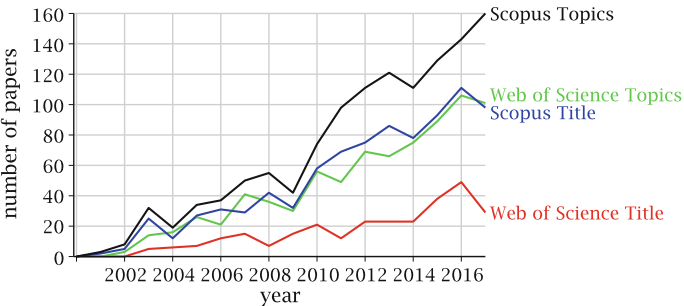


Fig. 1.1 Number of papers with the tag “quantum walk” in the title and in the topics returned by Scopus and Web of Science from 2000 to 2017

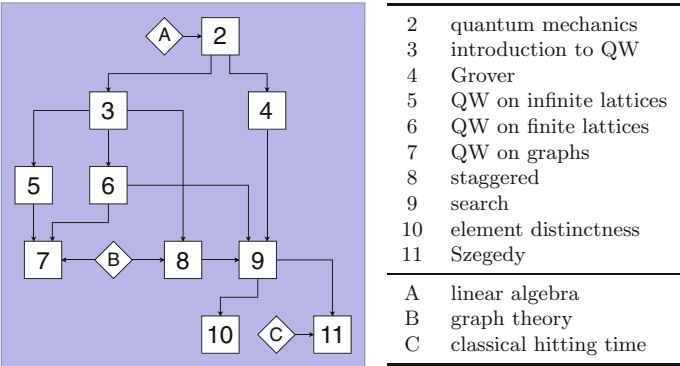


Fig. 1.2 Flowchart of the chapter dependencies

databases Scopus and Web of Science. It is easy to see that the number of papers is increasing as a superlinear function.

This book starts by describing in Chap. 2 the set of postulates of quantum mechanics, which is one of the pillars of quantum computation. Chapter 2 is a gentle introduction to quantum walks with the goal of describing how the coined and the continuous-time models can be obtained by quantizing classical random walks and classical continuous-time Markov chains, respectively. Chapter 4 describes the Grover algorithm, its generalization when there is more than one marked element, and its optimality. At the heart of the Grover algorithm lies the amplitude amplification technique, which is addressed at the end of the chapter. Chapters 5 and 6 are devoted to the coined model on lattices and hypercubes. Quantum walks on infinite lattices and lattices with cyclic boundary conditions with one and two dimensions are analyzed in detail using the Fourier transform. Chapter 7 defines coined quantum walks on arbitrary graphs and analyzes the limiting probability distribution and mixing time. Chapter 8 is new to the second edition of this book and describes the staggered quantum walk model and the analytic calculation of the position standard deviation of a staggered walk

on the line. Chapter 9 describes quantum-walk-based spatial search algorithms and has been remodeled in this edition. Readers will benefit from the efficacious presentation. Chapter 10 is also new to this edition and describes the optimal algorithm that solves the element distinctness problem. Finally, Chap. 11 describes Szegedy's quantum walk model and the definition of quantum hitting time. The flowchart of Fig. 1.2 shows the chapter dependencies.

There are three appendices. Appendix A compiles the main definitions of linear algebra used in this book. Appendix B compiles the main definitions of graph theory used in the area of quantum walks. Appendix C addresses the classical hitting time, which is useful to the definition of Szegedy's model. The dependencies on the appendices are also shown in Fig. 1.2

Chapter 2

The Postulates of Quantum Mechanics



It is impossible to present quantum mechanics in few pages. Since the goal of this book is to describe quantum algorithms, we limit ourselves to the *principles* of quantum mechanics and describe them as “game rules.” Suppose you have played checkers for many years and know several strategies, but you really do not know chess. Suppose now that someone describes the chess rules. Soon you will be playing a new game. Certainly, you will not master many chess strategies, but you will be able to play. This chapter has a similar goal. The postulates of a theory are its game rules. If you break the rules, you will be out of the game.

At best, we can focus on four postulates. The first describes the arena where the game goes on. The second describes the dynamics of the process. The third describes how we adjoin various systems. The fourth describes the process of physical measurement. All these postulates are described in terms of linear algebra. It is essential to have a solid understanding of the basic results in this area. Moreover, the postulate of composite systems uses the concept of tensor product, which is a method of combining two vector spaces to build a larger one. This concept must be mastered.

2.1 State Space

The *state* of a physical system describes its physical characteristics at a given time. Usually, we describe some possible features that the system can have because, otherwise, the physical problems would be too complex. For example, the spin state of a billiard ball can be characterized by a vector in $\mathbb{R}^3$. In this example, we disregard the linear velocity of the billiard ball, its color or any other characteristics that are not directly related to its rotation. The spin state is completely characterized by the axis direction, the rotation direction, and rotation intensity. The spin state can be described by three real numbers that are the entries of a vector, whose direction

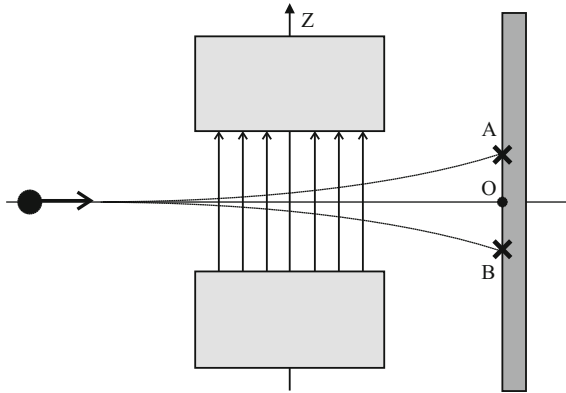


Fig. 2.1 Scheme of an experimental device to measure the spin state of an electron. The electron passes through a nonuniform magnetic field in the vertical direction. It hits *A* or *B* depending on the rotation direction. The distance of the points *A* and *B* from point *O* depends on the rotation speed. The results of this experiment are quite different from what we expect classically

characterizes the rotation axis, whose sign describes to which side of the billiard ball is spinning, and whose length characterizes the speed of rotation. In classical physics, the direction of the rotation axis can vary continuously, as well as the rotation intensity.

Does an *electron*, which is considered an elementary particle, i.e., not composed of other smaller particles, rotates like a billiard ball? The best way to answer this is by experimenting in real settings to check whether the electron in fact rotates and whether it obeys the laws of classical physics. Since the electron has charge, its rotation would produce magnetic fields that could be measured. Experiments of this kind were performed at the beginning of quantum mechanics, with beams of silver atoms, later on with beams of hydrogen atoms, and today they are performed with individual particles (instead of beams), such as electrons or photons. The results are different from what is expected by the laws of the classical physics.

We can send the electron through a magnetic field in the vertical direction (direction *z*), according to the scheme of Fig. 2.1. The possible results are shown. Either the electron hits the screen at the point *A* or point *B*. One never finds the electron at point *O*, which means no rotation. This experiment shows that the *spin* of the electron only admits two values: *spin up* and *spin down* both with the same intensity of “rotation.” This result is quite different from what is expected classically since the direction of the rotation axis is quantized, admitting only two values. The rotation intensity is also quantized.

Quantum mechanics describes the electron spin as a unit vector in the Hilbert space $\mathbb{C}^2$. The *spin up* is described by the vector

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and the *spin down* by the vector

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

This seems a paradox because vectors $|0\rangle$ and $|1\rangle$ are orthogonal. Why use orthogonal vectors to describe *spin up* and *spin down*? In $\mathbb{R}^3$, if we add *spin up* and *spin down*, we obtain a rotationless particle because the sum of two opposite vectors of equal length gives the zero vector, which describes the absence of rotation. In the classical world, we cannot rotate a billiard ball to both sides at the same time. We have two mutually excluded situations, and we apply the law of excluded middle. The notions of spin up and spin down of billiard balls refer to $\mathbb{R}^3$, whereas quantum mechanics describes the behavior of the electron before the observation, that is, before entering the magnetic field, which aims to determine its state of rotation.

If the electron has not entered the magnetic field and if it is somehow isolated from the macroscopic environment, its spin state is described by a linear combination of vectors $|0\rangle$ and $|1\rangle$

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \quad (2.1)$$

where the coefficients a_0 and a_1 are complex numbers that satisfy the constraint

$$|a_0|^2 + |a_1|^2 = 1. \quad (2.2)$$

Since vectors $|0\rangle$ and $|1\rangle$ are orthogonal, the sum does not result in the zero vector. Excluded situations in classical physics can coexist in quantum mechanics. This coexistence is destroyed when we try to observe it using the device shown in Fig. 2.1. In the classical case, the spin state of an object is independent of the choice of the measuring apparatus and, in principle, has not changed after the measurement. In the quantum case, the spin state of the particle is a mathematical idealization which depends on the choice of the measuring apparatus to have a physical interpretation and, in principle, suffers irreversible changes after the measurement. The quantities $|a_0|^2$ and $|a_1|^2$ are interpreted as the probability of detection of spin up or down, respectively.

2.1.1 State Space Postulate

An *isolated physical system* has an associated Hilbert space, called the *state space*. The state of the system is fully described by a unit vector, called the *state vector* in that Hilbert space.

Notes

1. The postulate does not tell us the Hilbert space we should use for a given physical system. In general, it is not easy to determine the dimension of the Hilbert space of the system. In the case of electron spin, we use the Hilbert space of dimension 2

because there are only two possible results when we perform an experiment to determine the vertical electron spin. More complex physical systems admit more possibilities, which can be an infinite number.

2. A system is isolated or *closed* if it does not influence and is not influenced by the outside. In principle, the system need not be small, but it is easier to isolate small systems with few atoms. In practice, we can only deal with approximate isolated systems, so the state space postulate is an idealization.

The state space postulate is impressive, on the one hand, but deceiving, on the other hand. The postulate admits that classically incompatible states coexist in superposition, such as rotating to both sides simultaneously, but this occurs only in isolated systems, that is, we cannot see this phenomenon, as we are on the outside of the insulation (let us assume that we are not *Schrödinger's cat*). A second restriction demanded by the postulate is that quantum states must have unit norm. The postulate constraints show that the quantum superposition is not absolute, i.e., is not the way we understand the classical superposition. If quantum systems admit a kind of superposition that could be followed classically, the quantum computer would have available an exponential amount of parallel processors with enough computing power to solve the problems in *class NP-complete*.¹ It is believed that the quantum computer is exponentially faster than the classical computer only in a restricted class of problems.

2.2 Unitary Evolution

The goal of physics is not simply to describe the state of a physical system at a present time; rather the main objective is to determine the state of this system at future times. A theory makes predictions that can be verified or falsified by physical experiments. This is equivalent to determining the dynamical laws the system obeys. Usually, these laws are described by differential equations, which govern the time evolution of the system.

2.2.1 Evolution Postulate

The *time evolution* of an isolated quantum system is described by a *unitary transformation*. If the state of the quantum system at time t_1 is described by vector $|\psi_1\rangle$, the system state $|\psi_2\rangle$ at time t_2 is obtained from $|\psi_1\rangle$ by a unitary transformation U , which depends only on t_1 and t_2 , as follows:

¹The class NP-complete consists of the most difficult problems in the class NP (*nondeterministic polynomial*). The class NP is defined as the class of computational problems that have solutions whose correctness can be “quickly” verified.

$$|\psi_2\rangle = U|\psi_1\rangle. \quad (2.3)$$

Notes

1. The action of a unitary operator on a vector preserves its norm. Thus, if $|\psi\rangle$ is a unit vector, $U|\psi\rangle$ is also a unit vector.
2. A *quantum algorithm* is a prescription of a sequence of unitary operators applied to an initial state takes the form

$$|\psi_n\rangle = U_n \cdots U_1 |\psi_1\rangle.$$

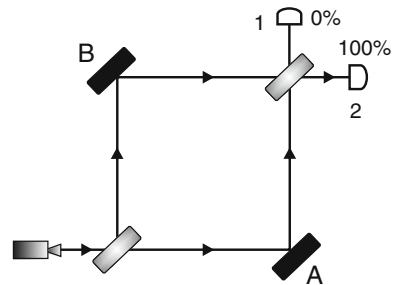
The qubits in state $|\psi_n\rangle$ are measured, returning the result of the algorithm. Before measurement, we can obtain the initial state from the final state because unitary operators are invertible.

3. The evolution postulate is to be written in the form of a differential equation, called *Schrödinger equation*. This equation provides a method to obtain operator U once given the physical context. Since the goal of physics is to describe the dynamics of physical systems, the Schrödinger equation plays a fundamental role. The goal of computer science is to analyze and implement algorithms, so the computer scientist wants to know if it is possible to implement some form of a unitary operator previously chosen. Equation (2.3) is useful for the area of quantum algorithms.

Let us analyze a second experimental device. It will help to clarify the role of unitary operators in quantum systems. This device uses *half-silvered mirrors* with 45° incident light, which transmit 50% of incident light and reflect 50%. If a single photon hits the mirror at 45° , with probability $1/2$, it keeps the direction unchanged, and with probability $1/2$, it is reflected. These half-silvered mirrors have a layer of glass that can change the phase of the wave by $1/2$ wavelength. The complete device consists of a source that can emit one photon at a time, two half-silvered mirrors, two fully reflective mirrors, and two photon detectors, as shown in Fig. 2.2. By tuning the device, the result of the experiment shows that 100% of the light reaches detector 2.

There is no problem explaining the result using the interference of electromagnetic waves in the context of the *classical physics* because there is a phase change in the

Fig. 2.2 Schematic drawing of an experimental device, which consists of a light source, two half-silvered mirrors, fully reflective mirrors A and B, detectors 1 and 2. The interference produced by the last half-silvered mirror makes all light to go to the detector 2



light beam that goes through one of the paths producing a destructive interference with the beam going to the detector 1 and constructive interference with the beam going to the detector 2. However, if the light intensity emitted by the source is decreased such that one photon is emitted at a time, this explanation fails. If we insist on using classical physics in this situation, we predict that 50% of the photons would be detected by detector 1 and 50% by detector 2 because the photon either goes through the mirror A or goes through B, and it is not possible to interfere since it is a single photon.

In *quantum mechanics*, if the set of mirrors is isolated from the environment, the two possible paths are represented by two orthonormal vectors $|0\rangle$ and $|1\rangle$, which generate the state space that describes the possible paths to reach the photon detector. Therefore, a photon can be in the superposition of “*path A*,” described by $|0\rangle$, and “*path B*,” described by $|1\rangle$. This is the application of the first postulate. The next step is to describe the dynamics of the process. How is this done and what are the unitary operators in the process? In this experiment, the dynamics are produced by the half-silvered mirrors, since they generate the paths. The action of the half-silvered mirrors on the photon must be described by a unitary operator U . This operator must be chosen so that the two possible paths are created in a balanced way, i.e.,

$$U|0\rangle = \frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}. \quad (2.4)$$

This is the most general case where paths A and B have the same probability to be followed because the coefficients have the same modulus. To complete the definition of operator U , we need to know its action on state $|1\rangle$. There are many possibilities, but the most natural choice that reflects the experimental device is $\phi = \pi/2$ and

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}. \quad (2.5)$$

The state of the photon after passing through the second half-silvered mirror is

$$\begin{aligned} U(U|0\rangle) &= \frac{(|0\rangle + i|1\rangle) + i(i|0\rangle + |1\rangle)}{2} \\ &= i|1\rangle. \end{aligned} \quad (2.6)$$

The intermediate step of the calculation was displayed on purpose. We can see that the paths described by $|0\rangle$ algebraically cancel, which can be interpreted as a destructive interference, while the $|1\rangle$ -paths interfere constructively. The final result shows that the photon that took path B remains, going directly to the detector 2. Therefore, quantum mechanics predicts that 100% of the photons will be detected by detector 2.

2.3 Composite Systems

The *postulate of composite systems* states that the state space of a *composite system* is the *tensor product* of the state space of the components. If $|\psi_1\rangle, \dots, |\psi_n\rangle$ describe the states of n isolated quantum systems, the state of the composite system is $|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$.

An example of a composite system is the memory of a n -qubit quantum computer. Usually, the memory is divided into sets of qubits, called *registers*. The state space of the computer memory is the tensor product of the state space of the registers, which is obtained by the repeated tensor product of the Hilbert space $\mathbb{C}^2$ of each *qubit*.

The state space of the memory of a 2-qubit quantum computer is $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$. Therefore, any unit vector in $\mathbb{C}^4$ represents the quantum state of two qubits. For example, the vector

$$|0, 0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad (2.7)$$

which can be written as $|0\rangle \otimes |0\rangle$, represents the state of two electrons both with spin up. Analogous interpretation applies to $|0, 1\rangle$, $|1, 0\rangle$, and $|1, 1\rangle$. Consider now the unit vector in $\mathbb{C}^4$ given by

$$|\psi\rangle = \frac{|0, 0\rangle + |1, 1\rangle}{\sqrt{2}}. \quad (2.8)$$

What is the spin state of each electron in this case? To answer this question, we have to factor $|\psi\rangle$ as follows:

$$\frac{|0, 0\rangle + |1, 1\rangle}{\sqrt{2}} = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle). \quad (2.9)$$

We can expand the right-hand side and match the coefficients setting up a system of equations to find a, b, c , and d . The state of the first qubit would be $a|0\rangle + b|1\rangle$ and second would be $c|0\rangle + d|1\rangle$. But there is a big problem: The system of equations has no solution, that is, there are no coefficients a, b, c , and d satisfying (2.9). Every state of a composite system that cannot be factored is called *entangled*. The quantum state is well-defined when we look at the composite system as a whole, but we cannot attribute the states to the parts.

A single qubit can be in a superposed state, but it cannot be entangled because its state is not composed of subsystems. The qubit should not be taken as a synonym of a particle because it is confusing. The state of a single particle can be entangled when we are analyzing more than a physical quantity related to it. For example, we may describe both the position and the rotation state. The position state may be entangled with the rotation state.

Exercise 2.1. Consider the states

$$|\psi_1\rangle = \frac{1}{2}(|0, 0\rangle - |0, 1\rangle + |1, 0\rangle - |1, 1\rangle),$$

$$|\psi_2\rangle = \frac{1}{2}(|0, 0\rangle + |0, 1\rangle + |1, 0\rangle - |1, 1\rangle).$$

Show that $|\psi_1\rangle$ is not entangled and $|\psi_2\rangle$ is entangled.

Exercise 2.2. Show that if $|\psi\rangle$ is an entangled state of two qubits, then the application of a unitary operator of the form $U_1 \otimes U_2$ necessarily generates an entangled state.

2.4 Measurement Process

In general, measuring a quantum system that is in the state $|\psi\rangle$ seeks to obtain classical information about this state. In practice, measurements are performed in laboratories using devices such as lasers, magnets, scales, and chronometers. In theory, we describe the process mathematically in a way that is consistent with what occurs in practice. Measuring a physical system that is in an unknown state, in general, disturbs this state irreversibly. In those cases, there is no way to know or recover the state before the measurement. If the state was not disturbed, no new information about it is obtained. Mathematically, the disturbance is described by an *orthogonal projector*.

If the projector is over a one-dimensional space, it is said that the quantum state *collapsed* and is now described by the unit vector belonging to the one-dimensional space. In the general case, the projection is over a vector space of dimension greater than 1, and it is said that the collapse is partial or, in extreme cases, there is no change at all in the quantum state of the system.

The measurement requires the interaction between the quantum system with a macroscopic device, which violates the *state space postulate* because the quantum system is not isolated at this moment. We do not expect the evolution of the quantum state during the measurement process to be described by a unitary operator.

2.4.1 Measurement Postulate

A *projective measurement* is described by a Hermitian operator O , called *observable*, which acts on the state space of the system being measured. The observable O has a *diagonal representation*

$$O = \sum_{\lambda} \lambda P_{\lambda}, \quad (2.10)$$

where P_λ is the projector on the eigenspace of O associated with the eigenvalue λ . The possible results of the measurement of the observable O are the eigenvalues λ . If the system state at the time of measurement is $|\psi\rangle$, the probability of obtaining the result λ will be $\|P_\lambda|\psi\rangle\|^2$ or, equivalently,

$$p_\lambda = \langle\psi|P_\lambda|\psi\rangle. \quad (2.11)$$

If the result of the measurement is λ , the state of the quantum system immediately after the measurement is

$$\frac{1}{\sqrt{p_\lambda}} P_\lambda|\psi\rangle. \quad (2.12)$$

Notes

1. There is a correspondence between the physical layout of the devices in a physics lab and the observable O . When an experimental physicist measures a quantum system, he or she gets real numbers as result. Those numbers correspond to the eigenvalues λ of the Hermitian operator O .
2. The states $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ have the same *probability distribution* p_λ when one measures the same observable O . The states after the measurement differ by the same factor $e^{i\phi}$. The term $e^{i\phi}$ multiplying a quantum state is called *global phase factor*, whereas a term $e^{i\phi}$ multiplying a vector of a sum of vectors, such as $|0\rangle + e^{i\phi}|1\rangle$, is called *relative phase factor*. The real number ϕ is called *phase*.

Since the possible outcomes of a measurement of observable O obey a probability distribution, we can define the *expected value* of a measurement as

$$\langle O \rangle = \sum_{\lambda} p_\lambda \lambda, \quad (2.13)$$

and the *standard deviation* as

$$\Delta O = \sqrt{\langle O^2 \rangle - \langle O \rangle^2}. \quad (2.14)$$

It is important to remember that the mean and standard deviation of an observable depend on the state that the physical system was in just before the measurement.

Exercise 2.3. Show that $\langle O \rangle = \langle\psi|O|\psi\rangle$.

Exercise 2.4. Show that if the physical system is in a state $|\psi\rangle$ that is an eigenvector of O , then $\Delta O = 0$, that is, there is no uncertainty about the result of the measurement of the observable O . What is the result of the measurement?

Exercise 2.5. Show that $\sum_{\lambda} p_\lambda = 1$ for any observable O and any state $|\psi\rangle$.

Exercise 2.6. Suppose that the physical system is in an arbitrary state $|\psi\rangle$. Show that $\sum_{\lambda} p_\lambda^2 = 1$ to an observable O if and only if $\Delta O = 0$.

2.4.2 Measurement in the Computational Basis

The *computational basis* of space $\mathbb{C}^2$ is the set $\{|0\rangle, |1\rangle\}$. For one qubit, the observable of the *measurement in the computational basis* is the Pauli matrix Z , whose spectral decomposition is

$$Z = (+1)P_{+1} + (-1)P_{-1}, \quad (2.15)$$

where $P_{+1} = |0\rangle\langle 0|$ and $P_{-1} = |1\rangle\langle 1|$. The possible results of the measurement are ± 1 . If the state of the qubit is given by (2.1), the probabilities associated with possible outcomes are

$$p_{+1} = |a_0|^2, \quad (2.16)$$

$$p_{-1} = |a_1|^2, \quad (2.17)$$

whereas the states immediately after the measurement are $|0\rangle$ and $|1\rangle$, respectively. In fact, each of these states has a global phase that can be discarded. Note that

$$p_{+1} + p_{-1} = 1,$$

because state $|\psi\rangle$ has unit norm.

Before generalizing to n qubits, it is interesting to reexamine the process of measurement of a qubit with another observable given by

$$O = \sum_{k=0}^1 k|k\rangle\langle k|. \quad (2.18)$$

Since the eigenvalues of O are 0 and 1, the above analysis holds if we replace $+1$ by 0 and -1 by 1. With this new observable, there is a one-to-one correspondence in the nomenclature of the measurement result and the final state. If the result is 0, the state after the measurement is $|0\rangle$. If the result is 1, the state after the measurement is $|1\rangle$.

The *computational basis* of the Hilbert space of n qubits in decimal notation is the set $\{|0\rangle, \dots, |2^n - 1\rangle\}$. The *measurement in the computational basis* is associated with observable

$$O = \sum_{k=0}^{2^n-1} k P_k, \quad (2.19)$$

where $P_k = |k\rangle\langle k|$. An arbitrary state of n qubits is given by

$$|\psi\rangle = \sum_{k=0}^{2^n-1} a_k |k\rangle, \quad (2.20)$$

where amplitudes a_k satisfying the constraint

$$\sum_k |a_k|^2 = 1. \quad (2.21)$$

The measurement result is an integer k in the range $0 \leq k \leq 2^n - 1$ with a probability distribution given by

$$\begin{aligned} p_k &= \langle \psi | P_k | \psi \rangle \\ &= |\langle k | \psi \rangle|^2 \\ &= |a_k|^2. \end{aligned} \quad (2.22)$$

Equation (2.21) ensures that the sum of the probabilities is 1. The n -qubit state immediately after the measurement is

$$\frac{P_k |\psi\rangle}{\sqrt{p_k}} \simeq |k\rangle. \quad (2.23)$$

For example, suppose that the state of two qubits is given by

$$|\psi\rangle = \frac{1}{\sqrt{3}} (|0, 0\rangle - i |0, 1\rangle + |1, 1\rangle). \quad (2.24)$$

The probability that the result is 00, 01, or 11 in binary notation is 1/3. Result 10 is never obtained because the associated probability is 0. If the measurement result is 00, the system state immediately after will be $|0, 0\rangle$, similarly for 01 and 11. For the measurement in the computational basis, it makes sense to say that the result is *state* $|0, 0\rangle$ because there is a one-to-one correspondence between eigenvalues and states of the computational basis.

The result of the measurement specifies on which vector of the computational basis state $|\psi\rangle$ is projected. The result does not provide the value of coefficient a_k , that is, none of the 2^n amplitudes a_k describing state $|\psi\rangle$ are revealed. Suppose we want to find number k as a result of an algorithm. This result should be encoded as one of the vectors of the computational basis, which spans the vector space to which state $|\psi\rangle$ belongs. It is undesirable, in principle, that the result itself is associated with one of the amplitudes. If the desired result is a noninteger real number, then the k most significant digits should be coded as a vector of the computational basis. After a measurement, we have a chance to get closer to k . A technique used in quantum algorithms is to amplify the value of a_k making it as close as possible to 1. A measurement at this point will return k with high probability. Therefore, the number that specifies a *ket*, for example, number k of $|k\rangle$ is a possible outcome of the algorithm, while the amplitudes of the quantum state are associated with the probability of obtaining a result.

The description of the measurement process of observable (2.19) is equivalent to simultaneous measurements or in a cascade of observables Z , that is, one observable Z for each qubit. The possible results of measuring Z are ± 1 . Simultaneous measurements, or in a cascade of n qubits, result in a sequence of values ± 1 . The relationship between a result of this kind and the one described before is obtained by replacing $+1$ by 0 and -1 by 1. We will have a binary number that can be converted into a decimal number which is one of the values k of (2.19).

For example, for three qubits the result may be $(-1, +1, +1)$, which is equivalent to $(1, 0, 0)$. Converting to base-10, the result is number 4. The state after the measurement is obtained using the projector

$$\begin{aligned} P_{-1,+1,+1} &= |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\ &= |1, 0, 0\rangle\langle 1, 0, 0| \end{aligned} \quad (2.25)$$

over the state system of the three qubits followed by *renormalization*. The renormalization in this case replaces the coefficient by 1. The state after the measurement is $|1, 0, 0\rangle$. When using the computational basis, for both observables (2.19) and Z 's, it makes sense to say that the result is $|1, 0, 0\rangle$ because we automatically know that the eigenvalues of Z in question are $(-1, +1, +1)$ and the number k is 4.

A simultaneous measurement of n observables Z is not equivalent to measure observable $Z \otimes \cdots \otimes Z$. The latter observable returns a single value, which can be $+1$ or -1 , whereas measuring n observables Z , simultaneously or not, we obtain n values ± 1 . Measurements on a cascade are performed with observable $Z \otimes I \otimes \cdots \otimes I$, $I \otimes Z \otimes \cdots \otimes I$, and so on. They can also be performed simultaneously. Usually, we use a more compact notation, Z_1, Z_2 , successively, where Z_1 means that observable Z was used for the first qubit and the identity operator for the remaining ones. Since these observables commute, the order is irrelevant and the limitations imposed by the *uncertainty principle* do not apply. Measurement of observables of this kind is called *partial measurement* in the computational basis.

Exercise 2.7. Suppose that the state of a qubit is $|1\rangle$.

1. What are the mean value and standard deviation of the measurement of observable X ?
2. What are the mean value and standard deviation of the measurement of observable Z ? Compare with Exercise 2.4.

2.4.3 Partial Measurement in the Computational Basis

The term *measurement in the computational basis* of n qubits implies a measurement of all n qubits. However, it is possible to perform a *partial measurement*—to measure some qubits. The result in this case is not necessarily a state of the computational

basis. For example, we can measure the first qubit of a system described by the state $|\psi\rangle$ of (2.24). It is convenient to rewrite that state as follows:

$$|\psi\rangle = \sqrt{\frac{2}{3}}|0\rangle \otimes \frac{|0\rangle - i|1\rangle}{\sqrt{2}} + \frac{1}{\sqrt{3}}|1\rangle \otimes |1\rangle. \quad (2.26)$$

We can see that the measurement result is either 0 or 1. The probability of obtaining 1 is $1/3$ because the only way to get 1 for a measurement of the first qubit is to obtain 1 as well, for the second qubit. Therefore, the probability of obtaining 0 is $2/3$, and the state immediately after the measurement in this case is

$$|0\rangle \otimes \frac{|0\rangle - i|1\rangle}{\sqrt{2}}.$$

Only the qubits involved in the measurement are projected on the computational basis. The state of the remaining qubits is in superposition in general. In this example, when the result is 0, the state of the second qubit is a superposition, and when the result is 1, the state of the second qubit is $|1\rangle$.

If we have a system composed of subsystems A and B , a partial measurement of subsystem A is a measurement of the observable $O_A \otimes I_B$, where O_A is an observable of system A and I_B is the identity operator of system B . Physically, this means that the measuring apparatus interacted only with the subsystem A . Equivalently, a partial measurement interacting only with subsystem B is a measurement of the observable $I_A \otimes O_B$.

If we have a register of m qubits together with a register of n qubits, we can represent the computational basis in a compact form $\{|i, j\rangle : 0 \leq i \leq 2^m - 1, 0 \leq j \leq 2^n - 1\}$, where i and j are both represented in base-10. An arbitrary state is represented by

$$|\psi\rangle = \sum_{i=0}^{2^m-1} \sum_{j=0}^{2^n-1} a_{ij} |i, j\rangle. \quad (2.27)$$

Suppose we measure all qubits of the first register in the computational basis, that is, we measure observable $O_A \otimes I_B$, where

$$O_A = \sum_{k=0}^{2^m-1} k P_k. \quad (2.28)$$

The probability of obtaining k so that $0 \leq k \leq 2^m - 1$ is

$$\begin{aligned} p_k &= \langle \psi | (P_k \otimes I) | \psi \rangle \\ &= \sum_{j=0}^{2^n-1} |a_{kj}|^2. \end{aligned} \quad (2.29)$$

The set $\{p_0, \dots, p_{2^m-1}\}$ is a probability distribution and therefore satisfies

$$\sum_{k=0}^{2^m-1} p_k = 1. \quad (2.30)$$

If the measurement result is k , the state immediately after the measurement will be

$$\frac{1}{\sqrt{p_k}} (P_k \otimes I) |\psi\rangle = \frac{1}{\sqrt{p_k}} |k\rangle \left(\sum_{j=0}^{2^n-1} a_{kj} |j\rangle \right). \quad (2.31)$$

Note that the state after the measurement is a superposition of the second register. A measurement of observable (2.28) is equivalent to measure observables $Z_1, \dots, Z_m$.

Exercise 2.8. Suppose that the state of two qubits is given by

$$|\psi\rangle = \frac{3}{5\sqrt{2}}|0, 0\rangle - \frac{3i}{5\sqrt{2}}|0, 1\rangle + \frac{2\sqrt{2}}{5}|1, 0\rangle - \frac{2\sqrt{2}i}{5}|1, 1\rangle. \quad (2.32)$$

1. Describe completely the measurement process of observable Z_1 , that is, obtain the probability of each outcome and the corresponding states after the measurement. Suppose that, after measuring Z_1 , we measure Z_2 . Describe all resulting cases.
2. Now invert the order of the observables and describe the whole process.
3. If the intermediate quantum states are disregarded, is there a difference when we invert the order of the observable? Note that the measurement of Z_1 and Z_2 may be performed simultaneously. One can move the qubits without changing the quantum state, which may be entangled or not, and put each of them into a measuring device, both adjusted to measure observable Z , as in Fig. 2.1.
4. For two qubits, the state after the measurement of the first qubit in the computational basis can be either $|0\rangle|\alpha\rangle$ or $|1\rangle|\beta\rangle$, where $|\alpha\rangle$ and $|\beta\rangle$ are states of the second qubit. In general, we have $|\alpha\rangle \neq |\beta\rangle$. Why is this not the case in the previous items?

Further Reading

The amount of good books about quantum mechanics is very large. For the first contact, we suggest [126, 257, 287]. Reference [287] uses the *Dirac notation* since the beginning, which is welcome in the context of *quantum computation*. For a more complete approach, we suggest [84]. For a more conceptual approach, we suggest [96, 252]. For those who are only interested in the application of quantum mechanics to quantum computation, we suggest [170, 234, 248, 272, 276].