Graduate Texts in Physics

Masahito Hayashi
Satoshi Ishizaka
Akinori Kawachi
Gen Kimura
Tomohiro Ogawa

Introduction to Quantum Information Science

Springer

Graduate Texts in Physics

For further volumes:
http://www.springer.com/series/8431

Graduate Texts in Physics

Graduate Texts in Physics publishes core learning/teaching material for graduate- and advanced-level undergraduate courses on topics of current and emerging fields within physics, both pure and applied. These textbooks serve students at the MS- or PhD-level and their instructors as comprehensive sources of principles, definitions, derivations, experiments and applications (as relevant) for their mastery and teaching, respectively. International in scope and relevance, the textbooks correspond to course syllabi sufficiently to serve as required reading. Their didactic style, comprehensiveness and coverage of fundamental material also make them suitable as introductions or references for scientists entering, or requiring timely knowledge of, a research field.

Masahito Hayashi · Satoshi Ishizaka
Akinori Kawachi · Gen Kimura
Tomohiro Ogawa

Introduction to Quantum Information Science

Springer

Masahito Hayashi
Graduate School of Mathematics
Nagoya University
Nagoya
Japan

Satoshi Ishizaka
Graduate School of Integrated Arts
and Sciences
Hiroshima University
Higashi-Hiroshima
Japan

Akinori Kawachi
Department of Mathematical
and Computing Sciences
Tokyo Institute of Technology
Tokyo
Japan

Gen Kimura
College of Systems Engineering
and Science
Shibaura Institute of Technology
Saitama
Japan

Tomohiro Ogawa
Graduate School of Information Systems
University of Electro-Communications
Tokyo
Japan

License for English edition only!

ISSN 1868-4513 ISSN 1868-4521 (electronic)
ISBN 978-3-662-43501-4 ISBN 978-3-662-43502-1 (eBook)
DOI 10.1007/978-3-662-43502-1
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014942016

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Original Japanese edition published by
Kyoritsu shuppan, Tokyo, 2012

Preface

Have you heard of quantum teleportation, quantum cryptography, or quantum computation? These seem science fiction, but are truly most-advanced scientific topics that are growing involving physics, information science, and mathematics. This area, called quantum information science, is information science based on "quantum theory," which is a fundamental theory of physics in the microscopic world.

This area has the potential to produce fascinating technology for teleportation, unconditionally secure cryptography, and ultrahigh-speed computer. Unfortunately, although this is an emerging area, non-experts, especially undergraduate students, have no sufficient opportunities to glance at this topic.

Considering this circumstance, professors in quantum information science have brought out this textbook, which explains the fundamentals of quantum information science. This book requires only first-year calculus, first-year linear algebra, and elementary probability theory as background knowledge, and does not require any knowledge of quantum theory and information science so that undergraduate students can read this textbook independently. Before the publication of the original Japanese version, confronted with the problem that there is no undergraduate course for quantum information science in Japan, the authors organized Winter School of Quantum Information Science in the seminar house in Tohoku University in Japan in 2009, 2010, and 2011. The authors published the following original Japanese version based on the lecture materials and the participants' responses in the above winter school.

Title: Introduction to Quantum Information Science
Japanese title: ryoushi jouhou kagaku nyuumon
Publisher: Kyoritsu shuppan
Year: May, 2012
Number of pages: 377

Precise description of quantum information science requires various background knowledge of the related fields. Fortunately, since the five authors of this book are from different backgrounds, this requirement is satisfied. After finishing the first manuscript, the authors adjusted the relation between chapters. Finally, Hayashi coordinated the whole organization.

The organization of this book and the responsible persons for the respective chapters are given as follows. First, in Chap. 1, Hayashi introduces an overview of quantum information science and describes the details of this textbook as its coordinator. Please read Sect. 1.5 “Organization of this book” before reading the contents of this book. Next, in Chap. 2, using vectors and matrices, Kimura explains the simplified formulation of quantum theory as an expert on foundation of quantum theory so that a beginner can easily understand it. In Chap. 3, Kawachi describes the foundations of quantum computation and quantum circuit as an expert of quantum computation. In Chap. 4, Kawachi treats quantum algorithms, which are algorithms for quantum computer. For example, Shor’s algorithm is treated as a quantum algorithm that solves factorization problem by using quantum computer. In Chap. 5, Kimura explains the advanced structure of quantum theory, which is necessary to learn quantum information science. In Chap. 6, Ogawa introduces various information quantities for quantum system as an expert on quantum information theory. In Chap. 7, Ishizaka treats quantum entanglement as an expert on quantum entanglement and statistical physics. In Chap. 8, Ogawa explains quantum channel coding. In Chap. 9, Hayashi treats quantum error correcting code and quantum cryptography as an expert on quantum information theory and quantum cryptography. This book is organized so that Chaps. 2–4 can be read with elementary calculus for matrices and inner products of complex vectors. The latter chapters require advanced knowledge for linear algebra, which are summarized in Appendix A by Kimura, Hayashi, and Ogawa.

Since this book covers various fields in quantum information, it can be used as a text for a lecture course or a seminar. Especially, since it contains many exercises with solutions in Appendix B, it also can be used for an exercise course. Further, it also treats a recent development in quantum information science. Hence, the reader can investigate more advanced topics by using the references after finishing this book. The authors hope that readers develop interest in quantum information science.

Finally, the authors express their gratitude to Graduate School of Information Sciences, Tohoku University, Grant-in-Aid for Scientific Research on Priority Area ‘Deepening and Expansion of Statistical Mechanical Informatics (DEX-SMI)’, Global COE: Computationism as a Foundation for the Sciences (CompView in short) of Tokyo Inst. of Tech., and the organizing committee members of Winter School of Quantum Information Science for supporting the organization of Winter

School of Quantum Information Science. The authors are also grateful to Mr. Hideaki Hosaka, Dr. Shojun Nakayama, Mr. Yueri Wakakuwa in Tokyo University, Mr. Ryota Nakayama in Tohoku University, Dr. Yutaka Shikano in Institute for Molecular Science, Dr. Masakazu Yoshida in Doshisya University, and Mr. Seiji Mizukami, Mr. Yohei Kawaguchi, Mr. Ryo Yaguchi, Dr. Wataru Kumagai in Nagoya University for making valuable comments for this book. The authors are thankful for Mr. Hideo Kotobuki and Ms Yoko Nakagawa for the publication of the original Japanese version. Finally, the authors express their appreciation to Dr. Claus E. Ascheron of Springer Science+Business Media for his encouragement and patience during the preparation of the manuscript.

Masahito Hayashi
Satoshi Ishizaka
Akinori Kawachi
Gen Kimura
Tomohiro Ogawa

Contents

Chapter 1
Invitation to Quantum Information Science

1.1 From Classical Information Science to Quantum Information Science

All of information processing has been realized by the combination of physical devices, e.g., semiconductor devices and optical fibers. The current information-communication and information processing on the computer are designed with the combination of these devices. Electrons in semiconductors and photons of optical fiber ultimately obey not the classical mechanics, but the quantum mechanics. Further, many information processing devices realizing brilliant performance use the quantum effects inside of the devices, e.g., superconducting Josephson device and Esaki diode. However, it is implicitly required as a basic requirement of current information device that the device has no quantum effect in the input and output systems. Hence, the device engineers have been required to design the information device so that no quantum effect directly appears in the input and the output.

What is the quantum effect in the input and the output? In the traditional information sciences, each of the input and the output is required to have a certain fixed value at a moment although it is allowed to change in time and/or behave stochastically. However, when the device is too miniaturized, the device comes to behave as a quantum system. Then, the input and the output do not take fixed values and take quantum superposition states. In the framework of the traditional information sciences, the engineers adopt the strategy to avoid such quantum input and output by limiting the quantum effects inside the device. However, when the miniaturization of the device has been advanced, the above-mentioned strategy does not necessarily realize the optimal performance of the total system. In order to improve the total performance, it is better to admit devices with quantum input and output. Hence, it is required to study information science based on the framework of quantum theory, and such a research area is called Quantum Information Science. On the other hand, the research area that does not take into account the quantum input and output in each device at all is called Classical Information Science.

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_1,

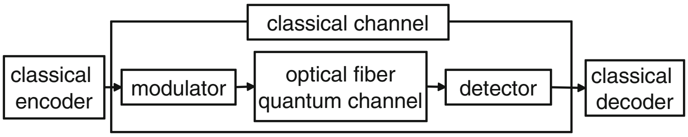


Fig. 1.1 Classical treatment of the optical communication

In fact, thanks to research achievement up to now, it has been clarified that the potential of information science and technology could be expanded very much if we are allowed to use the devices with quantum input and output. It could even say that the traditional strategy that avoids the quantum input and output works against further improvement for the total performance of information system. Indeed, although device engineers are familiar with the quantum effects and even utilize it, information scientists have required so that no quantum effect appears in the input and output due to the convenience. In future, quantum information science will become more popular, and it will be allowed to use devices with quantum input and output, which we expect leads to much progress of information science.

In the following, we call an information processing device a classical device when it does not deal with quantum input and output. Otherwise, it is called a quantum device. Then, the research area with respect to the computation with classical/quantum devices is called quantum computation/classical computation. Similarly, the research area with respect to the communication with classical/quantum devices is called quantum communication/classical communication. In quantum communication/classical communication, a communication channel is treated as quantum channel/classical channel.

In the following, we explain the relation between the quantum channel and the classical channel by taking for example a communication via an optical fiber (the optical communication). In the case of long-distance communication via an optical fiber, the signal is so weak that it behaves as a quantum particle. However, the traditional information science treats the optical communication in the classical way based on the framework given in Fig. 1.1 as follows: The hardware engineers take care of the design and implementation of all optical fiber, modulator, and photon detector, in which modulator converts the input information (the input alphabet) to the input photon, and the photon detector converts the output photon to the output information (the output alphabet). It is usual that the output alphabet behaves stochastically and, when the characteristics of the hardware (fiber, modulator and detector) are fixed, the probability distribution is decided depending on the input alphabet only. In this way, in the classical communication, the optical fiber, modulator and photon detector are encapsulated like in a single device, a classical channel, which is characterized by a probability distribution of the output alphabet as a function of the input alphabet. Then, information scientists do not deal with the internal physical structure of the channel, such as a state of a photon, at all. They employ classical mechanical description of the channel, and as a result, they design an encoder and decoder as a classical device that converts between messages and alphabets.

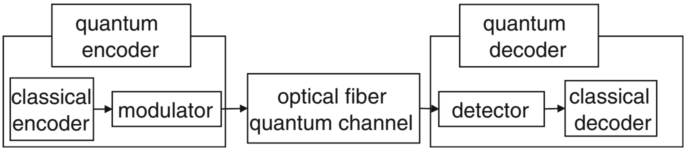


Fig. 1.2 Optical communication as quantum channel

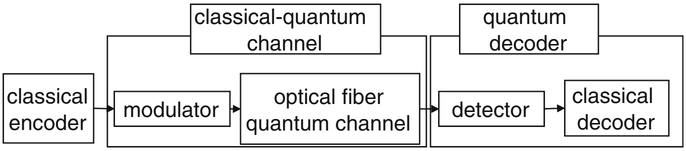


Fig. 1.3 Optical communication as classical-quantum channel

Fig. 1.4 Current hierarchical structure of information processing (Computer and communication)

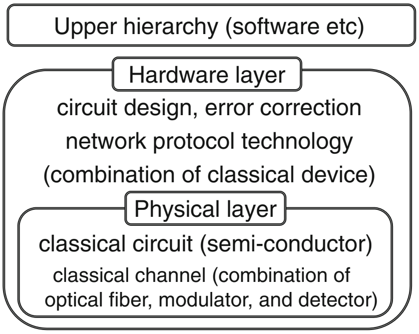
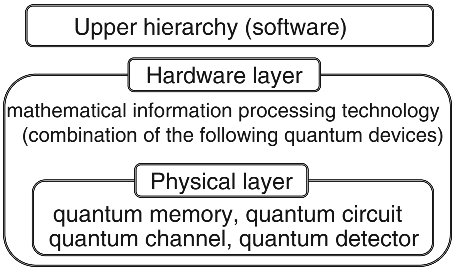

Upper hierarchy (software etc)
Hardware layer
circuit design, error correction
network protocol technology
(combination of classical device)
Physical layer
classical circuit (semi-conductor)
classical channel (combination of
optical fiber, modulator, and detector)

Fig. 1.5 Future hierarchical structure of information processing (Computer and communication)


Upper hierarchy (software)
Hardware layer
mathematical information processing technology
(combination of the following quantum devices)
Physical layer
quantum memory, quantum circuit
quantum channel, quantum detector

Under the framework of quantum information science, we do not encapsulate modulator, optical fiber and detector; instead we regard the encoder and modulator as a single device as shown in Fig. 1.2. The single device directly converts the message to the photon inputted to the fiber that is called a quantum encoder. Similarly, we regard the photo detector and the decoder as a single device directly converting the output photon to the message, which is called a quantum decoder. Hence, we can extract the maximal performance of the optical fiber. As a variant, we can formulate the optical communication like Fig. 1.3. In this formulation, the photon detector and the classical decoder are encapsulated to the quantum decoder. Similarly, the modulator and the quantum channel are encapsulated to the classical-quantum channel. Even in this framework, we need to take into account the non-commutativity caused by quantum property of the output signal so that quantum treatment is essentially required.

In both formulations, information scientists have to design quantum devices as explained in Fig. 1.5. Comparing Fig. 1.5 with Fig. 1.4, it is clear that they have to cover a wider field including physical layer. In quantum information science, we consider the information processing based on a hierarchical structure different from traditional hierarchical structure.

Here, we should remark that there are two types of tasks in quantum channel coding as follows. The purpose of one task is to transmit classical messages, and the other is to transmit quantum states. While the above discussion considers the transmission of the classical messages, it is possible to transmit a quantum state via a nosiy quantum channel. The latter is often called quantum error correction, and cannot be described by Fig. 1.2. The classical–quantum channel can realize only the task of transmitting the classical message, but the quantum channel can realize both tasks, i.e., transmitting the classical message and transmitting the quantum state. Chapter 8 discusses the coding for the classical-quantum channel, which gives a foundation of transmission of the classical message via the quantum channel.[1]

1.2 Further Expansion of Quantum Information Science

Quantum information science is different from the traditional information science not only in the framework of the information process, but also in the possibility of a new task that is impossible in the traditional method.

The quantum computation and quantum cryptography fall in this category. Quantum cryptography can guarantee the information theoretical security by assuming only physical laws as assumption. On the other hand, the security of the current cryptography is based on the calculation time. That is, in the latter cryptography, although the cipher text (the encrypted text) by itself contains all information to recover the plain text (the original text to be sent) in principle, they consider that the cryptography is secure because the relation between the cipher text and the plain text is so complicated that there is no effective algorithm to recover the plain text from the cipher text.[2] The security based on the calculation time is called computational

[1] As is mentioned here, even though the formulation in the classical setting is uniquely determined, its quantum extension often has plural formulations. That is, one classical formulation might correspond to plural quantum formulations, in general. When a beginner of quantum information science considers a quantum version of a given problem in the classical information science, he often discuss it with believing that there uniquely exists the quantum extension. Hence, if another person considers a different quantum extension, their argument mismatches each other.

[2] In this case, it is required that it is easy only to convert the cipher text from the plain text, and it is not easy to convert the plain text from the cipher text. Furthermore, in order that only the authorized receiver can decrypt the cipher text, it is also required that an additional information kept only by the authorized receiver enables to convert the plain text from the cipher text.

security. Hence, if a new algorithm for effective decryption or a speed up of calculation time is available, the security is threatened. On the other hand, the information theoretic security is guaranteed under the assumption that any information of the plain text cannot be leaked to an eavesdropper, even from the cipher text. Needless to say, the information theoretical security is better than the computational security. There are several types of information theoretic security, one of which is guaranteed under the assumption that the property of the physical device partially restricts the eavesdropper to access the information. In the case of quantum cryptography, the security is guaranteed by the physical law of quantum physics that inevitably restricts the eavesdropper to access the information. Currently, except for quantum cryptography, there exists no cryptography system that guarantees the information theoretical security without any assumption for the eavesdropper.

On the other hand, introducing algorithm utilizing quantum effects, quantum computation can drastically improve the calculation time for several problems whose effective algorithm is not given in the current technology, e.g., factorization problem. No known algorithm can efficiently solve the factorization problem in the framework of the traditional computer science. However, Shor's algorithm can efficiently solve the factorization problem by using quantum computer. The difficulty of the factorization problem is used as the assumption guaranteeing the computational security of the RSA protocol, which is one of the most popular cryptography protocols. Hence, Shor's algorithm gave a strong impact because realization of quantum computer enables to decrypt the RSA protocol. The power of quantum computer is often considered to originate from its capability of parallelism. In fact, a quantum computer can execute a vast number of calculation processes in parallel by superposing the calculation processes as a quantum superposition state. However, if we measure the superposition state wishing to obtain all the final results of the calculation processes, we can only obtain a single result of a randomly selected process. The capability of quantum parallelism only usually does not provide any benefit for us. In order to utilize an advantage of a quantum computer, it is necessary to extract a process whose result just matches a condition to solve the problem. So, in addition to employ the quantum parallelism, an efficient quantum algorithm employs a quantum interference effect and amplifies a state among the superposed states such that the result corresponding to the amplified state matches the condition. For example, Grover's algorithm explained in Sect. 4.3 directly amplifies the state corresponding the correct solution.

In order to realize quantum information processing, we need to experimentally implement all components as quantum devices as well as to propose quantum protocols, e.g., the above mentioned quantum algorithms and quantum cryptography protocol. Hence, quantum information science can be mainly divided into two areas: the first area theoretically explores the possibility of quantum information protocol, and the other area experimentally implements the quantum devices realizing the quantum information processing. The former targets to find and analyze quantum protocols. The latter studies various technologies of condensed matter physics and various materials for realizing quantum device experimentally. As an intermediate area, they often study to find candidates of the materials realizing the quantum device

This book mainly covers the theoretical part, which has two main sub-areas. One is the quantum computer area to study quantum algorithms and their possibility, and the other is the quantum communication area treating quantum communication and its possibility. The quantum cryptography can be regarded to belong to the latter area. There are also two sub-areas: “foundation of quantum theory” to study the formulation of quantum theory from the viewpoint of quantum information, and “quantum entanglement” to study the entanglement of quantum system. There is a further sub-area: “quantum statistical inference” to study statistical inference of quantum state or channel. Note that there is also a sub-area “quantum non-locality” but is not covered by this book. Quantum information science contains not only quantum computation and quantum communication, but also various areas related to their foundations. In the following, we describe the relation more deeply.

1.3 Feedback from Quantum Information Science to Physics

When we revisit quantum theory from the viewpoint of information science, we find various aspects of quantum theory, which cannot be found from the traditional viewpoint. Many standard textbooks for quantum theory introduce the formulation of quantum theory via canonical quantization after explanation of analytical mechanics over the phase space due to the historical reason. However, since this type explanation uses analogy with classical mechanics over the phase space, there exist readers who have an unnecessary picture related to the classical phase space for the quantum system. Such a picture often inhibits a proper understanding of the quantum theory. In order to avoid such a negative effect, it is better to explain only the formulation of the quantum theory itself. But, it might be difficult for the reader to master such an abstract framework for quantum theory due to the abstractness. Fortunately, since quantum information science has a concrete purpose to design information processing on quantum systems, the reader can understand the theoretical formulation of quantum theory via several concrete examples by excluding an unnecessary picture. When the reader is interested only in the information scientific aspect of quantum theory, he/she needs only the theoretical framework of quantum theory.

Quantum information science regards a quantum system as an information processing component that has inputs and outputs with proper relations. For this purpose, we need a minimum description for the probabilistic relation between inputs and outputs. In fact, usual textbooks of quantum mechanics do not have such a minimum description. Chapters 2 and 5 give such a desired description for quantum system, which is a product from quantum information science and has never been obtained from the traditional context of physics. These chapters treat the theoretical framework of quantum theory based on “operations” e.g., state preparation and measurement. Thanks to the treatment, the reader can understand what quantum theory can predict and how to apply quantum theory. Hence, the reader can grasp the operational framework of quantum theory based on operations implemented by experimentalists rather than the interpretation problem of quantum theory, e.g., Copenhagen interpretation. Unfortunately, the traditional physics does not have the key concept to grasp the quantum theory from the operational viewpoint excluding the historical factors. Fortunately, quantum information science has the purpose for performing information process in the quantum system, which works as a key concept to perform the above description for quantum theory. This type of understanding of quantum theory is not sufficient for realization of quantum information processing in actual systems. When the reader investigates actual quantum information processing, he/she needs to study the usual formulation, e.g, canonical quantization, and concrete descriptions for atoms, molecules and condensed matters, separately. Even for such an investigation, the study of the above theoretical framework of quantum theory is helpful for precise use of quantum theory.

In particular, our description for quantum dynamics is quite different from that of traditional textbooks of quantum theory. Traditional textbooks of quantum theory describe quantum dynamics as a form of differential equations. The methods were suitable to deal with the determination of whether the state is stable or unstable, but did not provide the simple relation between the input and output states under the quantum dynamical system, e.g., optical communication system.[3] On the other hand, quantum information science emphasizes the relation between the input and output states rather than the stability of states. This treatment enables us to treat the quantum communication according to the formulation of information science.

The formulation for the quantum system given by quantum information science yields the great contribution for entanglement theory, one area of modern physics, as well as for quantum computation and quantum communication. Heretofore, entanglement has been studied in the relation with the non-locality by Schrödinger and negation of the local realism by Bell among researchers of foundation of quantum theory. Most of them are speculative and are not quantitative. Hence, most of physicists have heard the name of entanglement but have not payed deep attention to it. Even more, they have no idea for quantifying the amount of entanglement. Quantum information science introduces the concept of "local operations and classical communications (LOCC)" as a foundation for quantifying the amount of entanglement. The concept is essentially based on the description of quantum theory that is established in the context of quantum information science. Combining the idea of coding and information quantity, e.g., entropy given in Chap. 6 to the concept of LOCC, we can formulate the quantification of amount of entanglement as in Chap. 7. Similarly, the development of the description for measuring process also greatly contributes the foundation of quantum theory. This progress enables us to describe measuring process that cannot be written as unitary dynamics, and produces the progress of the measuring technology.

Since quantum information science has greatly contributed internal problems of physics, it can be expected that the viewpoint of quantum information science

[3] A mathematical foundation of statistical mechanics has a similar mathematical formulation. This direction has generated an important area of mathematics "operator algebra" and has contributed many results useful for quantum information science. However, statistical mechanics is different from quantum information science in that statistical mechanics uses a density operator as an ensemble of many particles while quantum information science uses it as a state of one particle.

plays an important role for development of physics. For example, quantum error correction given in Chap. 9 can be regarded as one approach to decoherence, which has been discussed in physics for a long time. Generally, interaction between the given quantum system and the environment generates decoherence, and demolishes the coherence of the state when the state is a superposition among basis states. Quantum information process, in particular quantum computation, desires a technology that preserves the coherence of the quantum state. Quantum error correction treats the dissipation process of coherence by decoherence as state transmission via a quantum channel so that we can protect the quantum state by the proper combination of the encoding and the decoding. The framework of quantum information science is essential for producing these ideas.

1.4 Toward Realization of Quantum Information Processing

Decoherence caused by the noise appears in quantum cryptography. In the quantum communication, it is possible to use the bit-basis states and the phase-basis states, which is an advantage of quantum communication. Consider the case when the messages to be sent are converted only to the bit-basis states in spite of the above advantage. Although the message can be correctly transmitted even with decoherence, the information for the message might be leaked behind decoherence. In fact, when the message is transmitted via the bit basis, the amount of leaked information can be evaluated by the amount of decoherence with respect to the bit basis, i.e., the amount of breaking the superposition with respect to the bit basis. Hence, avoiding decoherence is an essential problem for realizing secure quantum cryptography. The amount of decoherence can be expressed by the error probability in the phase basis, which is the dual basis of the bit basis. Indeed, if we perform the encoding and the decoding for quantum error correction before or after the quantum communication channel, the error probability in the phase basis becomes sufficiently small. So, this method can guarantee the security for the quantum cryptography even when there exists decoherence in the quantum channel. However, it is not so easy to realize the encoding and the decoding for quantum error correction with the current technology. Hence, it had been thought that it is difficult to realize quantum cryptography. Since the final purpose of quantum cryptography is secure transmission of classical message, we might expect that the encoding and the decoding for quantum error correction can be replaced by classical information processes. In fact, this expectation is correct. That is, in the case of quantum cryptography, these processes can be replaced by the classical error correction and the privacy amplification. The classical error correction corresponds to the error correction for the bit basis, and the privacy amplification realizes the error correction for the phase basis by sacrificing the bit-length. Hence, the privacy amplification is directly linked to the disablement of leaked information. Since it is theoretically guaranteed that quantum cryptography can be implemented by the combination of existing technologies, many people believe that it is mostly close to practical use among quantum information technologies. In this scenario, the communication with the phase basis enables us to estimate the amount of the phase error in the original quantum channel. This information can decide how many bits should be sacrificed in the privacy amplification.

Currently, the National Institute of Information and Communication Technology (NICT) in Japan organizes a large project for realization of quantum key distribution, and it succeeded in demonstrating a secure TV conference with an installed fiber over a distance of 45 km by using a commercial QKD product for long-term stable operation [1]. Similar demonstration has been done in Switzerland [2]. We can expect its practical use. For its further transmission, we need quantum repeater that relays more than two quantum channels with keeping the coherence of the input state. Quantum computation is the quantum information technology that is next close to practical use. Unfortunately, its practical use has serious difficulty because it requires keeping the coherence for quantum memory. It can be expected that quantum computation becomes practical use when quantum memory is established according to the demand by quantum repeater technology.

The target of the practical use of quantum information science gave experimental physics a large effect. Traditional experimental physics emphasizes the treatment of the ground state. However, quantum information science requires to implement a given unitary operation, e.g., CNOT-gate. Such a request has never been required among traditional experimental physics. Several new technologies have been developed as a result for experimentalist's answer for such a harder request. Hence, we can expect developments of new technologies under the direction of quantum information science. Since quantum information science has provided a new viewpoint, new problems, and new targets, it has activated related research fields. This trend will continue future.

1.5 Organization of This Book

First, for accessibility for beginners, Chap. 2 treats the simplified formulation of quantum theory based on vectors and matrices. While a standard lecture of quantum theory in department of physics often starts with its history and the relation with analytical mechanics, this book daringly omits these topics, which are not necessarily needed for quantum information science. It starts with basic concepts of physical system, state, and observable. Then, it gives a formulation of quantum theory only for the two-level quantum system, which is called the qubit. As the first step, it deals with a measurement for the qubit system, a time evolution corresponding to a quantum computing process, a composite system that is required for simultaneous treatment of plural qubit systems. The reader can understand the contents of Chaps. 3 and 4 based only on these basic knowledges.

Chapter 3 devotes foundation of quantum computation and quantum circuits. This chapter, firstly, describes the foundation of computer science, and explains quantum circuits based on the relation with classical logic operation. It is recommended to read this part even for the readers who are not interested in quantum computation because this part will be used in the latter chapters. Chapter 4 discusses quantum computation more deeply. This chapter explains three typical quantum algorithms for quantum computer. The first is Deutsch-Jozsa's algorithm, the second is Grover's algorithm for a search problem, and the third is Shor's algorithm for prime factorization.

Chapter 5 discusses two different types of topics. The first half of this chapter devotes the traditional formulation of quantum theory based on the postulates. The formulation given in Chap. 2 is more precisely described here. However, this traditional formulation is not sufficient for studying the topics in quantum information science except for quantum computation. In order to resolve this problem, the latter half of this chapter devotes a more advanced structure of quantum theory. The preceding chapters describe quantum information processes without any noise, but the latter chapters describe quantum information processes containing noise. For this purpose, we need to introduce the concept of mixed state, which describes a noisy quantum state. In quantum theory, a noisy quantum state and a noisy time evolution cannot be described by simple stochastic mixtures of the noiseless cases. The latter half of this chapter introduces the framework of quantum theory for the description of a noisy quantum state and a noisy time evolution. A noiseless state given in the first half is called a pure state, and a noisy state given in the latter half is called a mixed state. The latter half also discusses the description of measurement deeply. It formulates the concepts of state, measurement, and time evolution in the optimum way for studying quantum information science, which are essential for latter chapters.

Chapter 6 deals with various information quantities in quantum systems. The concept of entropy plays a central role in quantum information science like in classical information science. This chapter explains these information quantities and their mathematical properties, which will be used in the latter chapters.

Chapter 7 addresses entanglement in a quantum system, and explains its related topics, quantum teleportation, dense coding, and quantum data compression. Next, it discusses the key concept of quantum information science, local operations and classical communications (LOCC), and discusses the convertibility of entanglement based on LOCC. The amount of entanglement is quantified based on the convertibility. The above mentioned theory has been established in the bipartite pure states case, but the bipartite mixed states case requires more difficult treatment. The end of this chapter makes mention of the bipartite mixed states case.

Chapter 8 addresses the quantum channel coding, which discusses the transmission of the classical message via a quantum channel. In fact, Nagaoka proposed the conjecture "Many things can be understood with the hypothesis testing via the information spectrum".[4] Chapter 8 is organized according to this conjecture. That is, we firstly treat the quantum hypothesis testing. Then, we explain the relation between

[4] The information spectrum is a unified method in information theory proposed by Han-Verdú in 1993 [3], in which, the asymptotic optimal performance can be characterized by the likelihood ratio. This conjecture has been proposed by Nagaoka [4] in 1999, and is called Nagaoka's dream. After his proposal, many topics has been characterized in the relation with the hypothesis testing, e.g., quantum channel coding, quantum source coding, entanglement concentration, entanglement dilution, channel resolvability, wire-tap channel coding, and reverse Shannon theorem.

the channel coding and the hypothesis testing. Based on the relation, we treat the quantum channel coding, and show the quantum channel coding theorem for the transmission of the classical message, which gives the limit of transmission rate.

Chapter 9 deals with the quantum error correction and quantum cryptography. The quantum error correction discusses the transmission of the quantum state via a noisy quantum channel, which is different from the problem discussed in Chap. 8. The beginning part discusses the classical error correction based on an algebraic method. Using the knowledge of the classical error correction, the second part treats the quantum error correction. Then, using the property of the quantum error correction, we treat the secure communication of the classical message via a quantum channel. Based on quantum error correction, the final part discusses the quantum cryptography. It is possible to consider the channel coding theorem for the transmission of the quantum state, which gives the limit of transmission rate. However, this book does not deal with the optimal transmission rate and explains only the rate based on the algebraic construction. This is because the algebraic construction is closely related to the quantum cryptography.

A common distinction among Chaps. 7, 8, and 9 is the characterization of the (optimal) rates of respective information protocols by the respective information quantities such as entropy. Such a characteristic is a common property among information theory, entanglement theory, and statistical mechanics, which reflects a common structure of large size many-body system.

This book is organized so that Chaps. 2, 3, and 4 can be understood with elementary calculations for matrices, vector spaces, and probabilities. Chapter 5 and the latter chapters require knowledges of (coordinate-free) linear algebra, which is summarized in Appendix A. Since Chap. 9 treats an algebraic treatment, it additionally requires knowledges of linear algebra over a finite filed, which is also summarized in Appendix A. In Appendix A, mathematical basic knowledges to study quantum information theory are summarized in a self-contained form so that it can be read as an independent chapter.

The description of Chaps. 2, 3, and 4 are different from that of the latter chapters. The reason is the following. In quantum mechanics, an observable (a physical quantity) is an operator, which can be represented by a matrix. However, the matrix representation has an ambiguity such that the representation depends on the choice of a coordinate (or a basis), and hence it is not a convenient way in most fields of quantum information science. In the field of quantum computation, however, there is no such ambiguity because the computational basis can be widely and naturally used for the representation basis. From the above reasons, Chap. 2 adopts the matrix representation from the beginning, which is beneficial to make the introduction easier. Originally, however, an observable should be precisely dealt with an operator, and we adopt the precise description from Chap. 5.

References

1. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.F. Dynes, A.R. Dixon, A.W. Sharpe, Z.L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev and A. Zeilinger, Field test of quantum key distribution in the Tokyo QKD Network. Opt. Express **19**, 10387 (2011)
2. D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta and H. Zbinden, Long-term performance of the Swiss Quantum quantum key distribution network in a field environment. New J. Phys. **13**, 123001 (2011)
3. T.S. Han, S. Verdú, IEEE Trans. Inf. Theor. **39**, 752 (1993)
4. H. Nagaoka, On The Information-Spectrum Method : Its role in classical and quantum information theory. IEICE Technical report IT **100**(332), 7–12 (2000). (in Japanese)

Chapter 2
Quantum Mechanics for Qubit Systems

2.1 Preliminary

Quantum mechanics (QM) is a physical theory to explain the microscopical world (typically of atomic scales) with extraordinary high accuracy. In QM, we encounter several "weird" phenomena, such as the superposition of states, the uncertainty principle, and an entanglement (a "stronger" correlation than classical one). Quantum information science is a recently developing field of information science which turns these "weirdness" of quantum phenomena to the marvelous applications of information processings, such as a super-fast computation (Chap. 4), a teleportation of a state (Chap. 7), and an unconditionally secure cryptography (Chap. 9).

While learning QM is a must for quantum information science, it is not indispensable to start from traditional textbooks of QM. Required ability is rather to understand the basic concepts and the theoretical structure of QM, especially to grasp the range (the set) of quantum states, measurements, time evolutions, etc., for the possible applications to information processings.

With this in mind, we introduce the theoretical framework of QM as a theory of probability[1] from operational point of view. Indeed, an outcome of each measurement of physical quantity is typically random in quantum systems, and QM is a theory to predict its probability (see Fig. 2.1). More precisely, the basic proposition QM predicts is

$$\begin{aligned}&\textit{what is the probability to observe a certain}\\&\textit{measurement outcome under a given state}.\end{aligned}\tag{2.1}$$

With this proposition at the core, we need to learn the description of quantum states and measurements, in addition to the laws of time evolution and composite systems of QM.

[1] This idea is based on the **Copenhagen interpretation**, one of the most famous interpretations of QM, and is widely accepted at least for the usage of QM.

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_2,

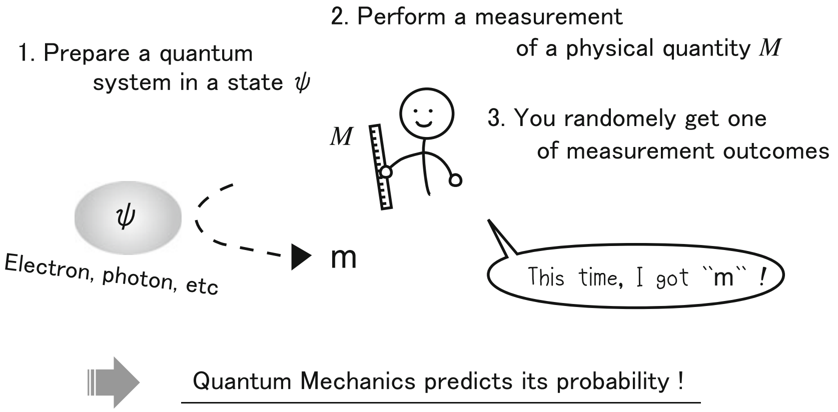

1. Prepare a quantum system in a state ψ
2. Perform a measurement of a physical quantity M
3. You randomely get one of measurement outcomes
ψ
Electron, photon, etc
M
m
This time, I got "m" !
Quantum Mechanics predicts its probability !

Fig. 2.1 An illustration of a state-preparation and a measurement in quantum system

In this chapter, we explain QM through a **qubit** system (2-level quantum system), which is the most elementary quantum system with only two orthogonal states. The purpose is to survey the world of QM in order to get familiar with physical concepts and mathematical tools of QM at a cost of generality. Moreover, a composition of qubit systems provides a platform for the realization of several quantum information processings. Indeed, in quantum information science, a qubit system plays a role of the unit of information as a generalization of a bit in classical information science. After reading this chapter, the reader will be able to understand most applications in quantum information sciences. (The general theory of QM is explained in Chap. 5 in detail.) The background knowledge required for this chapter is an elementary probability theory with finite outcomes and a simple linear algebra on the complex Euclidean space $\mathbb{C}^d$.[2]

Finally, let us give a few remarks for those who study QM for the first time.[3] In any physical theory, we use a mathematics as a reliable and useful language mainly to logically, quantitatively and universally describe our nature. However, the way to use a mathematics in QM is quite different from that in classical physics. As we shall see soon, we use mathematical tools such as vectors and matrices (linear operators) for the description of QM. However each mathematics by itself does not *directly* correspond to any physical statement, but only after combining (and calculating) them, we get a physical statement typically of the probability law (2.1) which is testable in experiments. On this point, it always happens for the beginner of QM to feel a sense of discomfort.[4] We just advice here; don't bother with this

[2] The only difficulty would be the tensor product for the description of composite systems. However, this is also explained in this chapter and Appendix A.5 in detail.

[3] We recommend to read this part again after studying this chapter.

[4] For instance, physical quantities of QM will be represented by complex matrices which are generally non-commutative to each other (see Sect. 5.2.1). Many beginners naturally wonder why physical quantities are non-commutative.

matter for the present. Indeed, such mathematical representations in QM are given a priori without any convictive physical reasoning, and the validity for the usage is only established by the fact that the predictions of QM perfectly coincide with all quantum phenomena observed in experiments.[5] On the other hand, the reader should recognize that QM can still be interpreted—at least from the viewpoint of positivism—as an operationally well-defined probabilistic theory. Indeed, after fixing a state and a measurement of QM, the probability can be treated just as the same in classical probability theory [9]: As normal, the probability in QM can be interpreted as the (convergent) frequency with a large number of trials. Therefore, the general property of probability (the positivity and the normalization of a probability, the addition law for exclusive events, etc.) and any derived notions of probability (an expectation value, a standard deviation, the conditional probability, etc.) are completely the same as those of classical probability theory.

2.2 Preparation

We begin with a brief introduction of physical concepts required not only for QM but also for any physics. The Dirac notation, a peculiar notation of a vector, in QM is also explained here.

2.2.1 Conceptual Preparation: Physical System, State, Measurement of Physical Quantity

One of the main purposes of physics is to understand and predict natural phenomena with scientific methods. To do this, it is convenient first to restrict the range of the "object" in which we are interested; otherwise, we always have to treat a whole universe. In other words, we have to identify what **physical system** we are dealing with. In particular, a **quantum (mechanical) system** is a physical system typically at atomic scale where quantum mechanical effects appear. The typical examples would be physical systems of atoms, electrons, photons, etc., but also could be a partial system by focusing on a particular freedom of a particle like a spin of an electron and a polarization of a photon. Moreover, to describe the relation between physical systems, e.g., their interaction and correlations, we need to treat the physical systems as a whole. A physical system composed of multiple physical systems is called a **composite system**.

The characteristics of a physical system are determined by **physical quantities**. The typical examples of the physical quantities include position, momentum, energy, (spin) angular momentum of a particle, polarization of a photon, etc. Needless to say,

[5] For those who are interested in the fundamental aspects of QM, see e.g. [1, 2] for the possible interpretations of QM; [3, 4] for the profound fact on the reality related to the entanglement; [5–8], and references therein for the recent attempts to derive QM from purely physical principles.

physical quantities should be able to be measured in experiments. In this context, they are often called **observables**.

Depending on a way of preparation, a physical system can be in a variety of different **state**s. The reader may image a "state" as the same notion used in a daily life. However in physics, a state is an important technical nomenclature with a clear scientific definition. Operationally, a state is responsible for how a physical system responses to measurements of physical quantities. Therefore, it can be formally defined as the "list" of physical responses to measurements of all physical quantities (see also Sect. 5.1.1). As the responses in QM are observed a probabilistic process, a state of QM can be formally defined as a function from physical quantities to the probabilities of each response. In the standard description of QM, however, we mathematically represent each of a state and a physical quantity separately, and give a rule to combine them to calculate the probability (see Sect. 2.3).

2.2.2 Notational Preparation: Dirac Notation

In QM, we usually use a peculiar notation for the description of vectors which is not used in mathematics community. The notation is called a **Dirac notation** introduced by the famous physicist Dirac [10] and is quite useful and reasonable to describe the theory of QM. As we also use this notation throughout this book, we explain it here by restricting to the complex Euclidean space $\mathbb{C}^d$. (For the general case, see Sect. 5.1.3.)

In the following, a, b, c (also $a_1, a_2 \ldots$, etc.) are complex numbers, while d represents the dimension of a vector space. The capital letters A, B, C represent $d \times d$ complex matrices. We consider a vector in $\mathbb{C}^d$ as a column vector, e.g., $\begin{pmatrix} 2+i \\ -5+6i \end{pmatrix} \in \mathbb{C}^2$, which is sometimes abbreviated as $(2+i, -5+6i)^T$ with the transposition symbol ^{T} to save a space.

[A] $|\psi\rangle$ denotes a (Column) Vector

In Dirac notation, a column vector of $\mathbb{C}^d$ is denoted with the **ket** symbol[6] $|\ \rangle$ such as

$$|\psi\rangle = \begin{pmatrix} 1 \\ 2+i \end{pmatrix}, |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2, |\phi\rangle = \begin{pmatrix} 3+i \\ 2 \\ -4i \end{pmatrix} \in \mathbb{C}^3, \text{ etc.} \tag{2.2}$$

[6] The symbol $|\ \rangle$ is called a "ket" as it represents the right half of the "bracket" $\langle\ ,\ \rangle$.

One of the roles to introduce the ket symbol is to make one possible to recognize that the object is a (column) vector.[7] In Dirac notation, a column vector is sometimes called a **ket vector**. Inside the ket symbol, any symbol can be used, which identifies the specific vector. In QM, we usually use a Greek character like $|\psi\rangle$, $|\phi\rangle$, $|\xi\rangle$, etc., while in quantum information science, we often use a bit sequence like $|0\rangle$, $|1\rangle$, $|0100\rangle$, etc., with an encode of information to a quantum state in mind. However, the zero vector $(0, \ldots, 0)^T$ is exceptionally denoted simply by 0, without the ket symbol. (The reader should judge whether 0 represents a zero as a number or the zero vector by the context.) Notice that the symbol $|0\rangle$ does not represent the zero vector as in (2.2). We sometimes use an abbreviation for a linear combination of vectors: a vector $a|\psi\rangle + b|\phi\rangle$ can be denoted by $|a\psi + b\phi\rangle$.

The reader might think that the use of the ket symbol is redundant especially if you are familiar with a notational convention in mathematics, where a vector is simply denoted like ψ. However, there are many advantages to use Dirac notation, which will be explained later. Here, we just point out one advantage which is particularly important in quantum information science. For the physical realization of information processing, we often need to encode a bit sequence (classical information) to a physical state. As we shall see soon, a quantum state is represented by a vector, and by introducing the ket symbol, one can clearly distinguish between a bit sequence (e.g. 0100101) and the encoded state (e.g. $|0100101\rangle$). On the other hand, if the conventional notation in mathematics is used, the encoded state would be denoted like $\psi_{0100101}$ and the important information of the bit sequence is degraded to just a subscript [11].

[B] $\langle\psi|$ denotes the Conjugate Transpose of $|\psi\rangle$

In Dirac notation, the conjugate transpose of a column vector $|\psi\rangle$, i.e., the row vector with the complex conjugation, is denoted by $\langle\psi|$. Namely, for $|\psi\rangle = (a_1, a_2, \ldots, a_d)^T$, we have

$$\langle\psi| := (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_d}). \tag{2.3}$$

For instance, we have $\langle\psi| = (1, 2-i)$, $\langle 0| = (1, 0)$, $\langle 1| = (0, 1)$, $\langle\phi| = (3-i, 2, 4i)$ for vectors in (2.2). The symbol $\langle\ |$ is called a **bra**[8] and $\langle\psi|$ is sometimes called a **bra vector**. Remind that both a column vector and a row vector with dimension d can be considered as a $d \times 1$ matrix and a $1 \times d$ matrix, respectively. With this in mind, a bra vector $\langle\psi|$ is just an adjoint matrix[9] of $|\psi\rangle$:

[7] In the elementary textbook of mathematics, the symbol $\vec{\ }$ is sometimes used to represent vectors like $\vec{a} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$. One can simply replace $\vec{\ }$ to $|\ \rangle$ in Dirac notation.

[8] This is because $\langle\ |$ represents the left half of the "bracket" $\langle\ ,\ \rangle$.

[9] The adjoint matrix (the conjugate transpose) of a $d_1 \times d_2$ matrix $A = (a_{ij})$ is defined as the $d_2 \times d_1$ matrix $(\overline{a_{ji}})$, and is denoted by $A^\dagger$. For instance,

$$\langle\psi| = |\psi\rangle^{\dagger}.$$

Next, we consider the combinations of ket and bra vectors.

[C] $\langle\psi|\phi\rangle$ represents the Inner Product

First, we consider the matrix product of a bra vector, $1 \times d$ matrix, from the left and a ket vector, $d \times 1$ matrix, from the right. Then, the obtained matrix is 1×1 matrix, or equivalently just a scalar (a complex number): For column vectors $|\psi\rangle = (a_1, \ldots, a_d)^T$ and $|\phi\rangle = (b_1, \ldots, b_d)^T \in \mathbb{C}^d$, we have

$$\langle\psi|\,|\phi\rangle = (\overline{a_1}, \ldots, \overline{a_d}) \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} = \sum_{i=1}^{d} \overline{a_i} b_i \in \mathbb{C}\,. \tag{2.4}$$

Notice that the result coincides with the complex **Euclid inner product** between two vectors $|\psi\rangle = (a_1, \ldots, a_d)^T$ and $|\phi\rangle = (b_1, \ldots, b_d)^T \in \mathbb{C}^d$ in this order. For the consistency of the notation, in Dirac notation, we denote the inner product by

$$\langle\psi|\phi\rangle := \sum_{i=1}^{d} \overline{a_i} b_i\,. \tag{2.5}$$

Namely we have

$$\langle\psi|\,|\phi\rangle = \langle\psi|\phi\rangle. \tag{2.6}$$

With this notation, $\langle\psi|\phi\rangle$ has the two meanings, “the matrix product of a bra vector and a ket vector” or “the inner product of two ket vectors $|\psi\rangle$ and $|\phi\rangle$” , and we can utilize both their properties. For instance, it is often useful to use the associative law of a matrix product (of bra and ket) in calculation, while the general property of an inner product[10] is quite useful to formalize the theory of QM. We denote the **Euclid norm** of a vector $|\psi\rangle$ simply by $||\psi||$ without a ket symbol:

$$||\psi|| := \sqrt{\langle\psi|\psi\rangle} = \sqrt{\sum_i |a_i|^2}.$$

(Footnote 9 continued)

$$A = \begin{pmatrix} 2-3i & 1-6i \\ -1+5i & 4+7i \end{pmatrix} \Rightarrow A^{\dagger} = \begin{pmatrix} 2+3i & -1-5i \\ 1+6i & 4-7i \end{pmatrix}.$$

[10] The essential properties of an inner product are (p1) the positivity with non-degeneracy, (p2) the (conjugate) symmetry, and (p3) the linearity in the second argument (see Appendix A.2.2 in detail). Namely, (p1) $\langle\psi|\psi\rangle \geq 0$ for any $|\psi\rangle \in \mathbb{C}^d$, while the equality holds if and only if $|\psi\rangle = 0$, (p2) $\overline{\langle\phi|\psi\rangle} = \langle\psi|\phi\rangle$, (p3) $\langle\psi|a\phi_1 + b\phi_2\rangle = a\langle\psi|\phi_1\rangle + b\langle\psi|\phi_2\rangle$. The reader should check these properties for Euclid inner product by the definition (2.5).

As an example of the Dirac notation, the condition that the set of vectors $\{|\psi_i\rangle\}_{i=1}^{m}$ is an orthonormal system[11] can be written by $\langle\psi_i|\psi_j\rangle = \delta_{ij}$ $(i, j = 1, \ldots, m)$ with the Kronecker delta symbol.[12]

Excercise 2.1 Calculate $\langle\psi|\phi\rangle$ for $|\psi\rangle = (1 + 2i, 2 - i, 3)^T$ and $|\phi\rangle = (-5 - 3i, 4, 2 + i)^T$.

[D] $|\psi\rangle\langle\phi|$ is a Matrix

Next, we consider another matrix product by swapping the order of a ket and a bra. A product of a ket vector, $d \times 1$ matrix, and a bra vector, $1 \times d$ matrix in this order, is a $d \times d$ matrix. For $|\phi\rangle = (b_1, \ldots, b_d)^T$ and $|\psi\rangle = (a_1, \ldots, a_d)^T \in \mathbb{C}^d$, we have

$$|\phi\rangle\langle\psi| = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} (\overline{a_1}, \ldots, \overline{a_d}) = \begin{pmatrix} b_1\overline{a_1} & \cdots & b_1\overline{a_d} \\ \vdots & \vdots & \vdots \\ b_d\overline{a_1} & \cdots & b_d\overline{a_d} \end{pmatrix}. \tag{2.7}$$

The symbols for the inner product $\langle\psi|\phi\rangle$ and the matrix $|\psi\rangle\langle\phi|$ might look similar but are completely different; the former is a scalar and the latter is a matrix!

Now observe a matrix product of $|\psi\rangle\langle\phi|$ to a vector $|\xi\rangle = (c_1, \ldots, c_d)^T$:

$$|\phi\rangle\langle\psi||\xi\rangle = \begin{pmatrix} b_1\overline{a_1} & \cdots & b_1\overline{a_d} \\ \vdots & \vdots & \vdots \\ b_d\overline{a_1} & \cdots & b_d\overline{a_d} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_d \end{pmatrix} = \begin{pmatrix} (\sum_i \overline{a_i}c_i)b_1 \\ \vdots \\ (\sum_i \overline{a_i}c_i)b_d \end{pmatrix} = \langle\psi|\xi\rangle|\phi\rangle. \tag{2.8}$$

In general argument, it is sometimes preferable to recognize the definition of $|\phi\rangle\langle\psi|$ not by the matrix elements of (2.7) but by its effect of the multiplication to an arbitrary vector $|\xi\rangle$:

$$|\phi\rangle\langle\psi||\xi\rangle = \langle\psi|\xi\rangle|\phi\rangle. \tag{2.9}$$

(See also [D′] in Sect. 5.1.3.)

One of the advantages to use Dirac notation is to make a calculation easy. The point is to first calculate a combination of bra and ket in this order as it becomes just a scalar. For instance, the result (2.9) is trivial if one computes the pair of $\langle\psi|$ and $|\xi\rangle$ first. Also, we trivially have

$$|\psi\rangle\langle\phi||\xi\rangle\langle\eta||\chi\rangle\langle\mu| = \langle\phi|\xi\rangle\langle\eta|\chi\rangle|\psi\rangle\langle\mu|, \text{ etc.}$$

[11] The set of vectors is called an orthonormal system if the vectors are mutually orthogonal (i.e., the inner product is zero) and the norms of all the vectors are 1.

[12] $\delta_{ij} := \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$

The reason why these computations are possible is due to the associative law of matrix multiplication.[13] From this property, as long as we keep the order of matrices, we can freely choose the combination of adjacent matrices to compute their multiplication first. Moreover, as the matrix product also satisfies the linearity,[14] we don't have to much care for the order of a summation, either.

The reader will gradually get used to and benefit from Dirac notation through the examples from the next section.

Excercise 2.2 Let $|\phi\rangle = (2i, 3)^T$, $|\psi\rangle = (1, i)^T$, $|\xi\rangle = (1+i, 2)^T$, $|\chi\rangle = (3, -i)^T$. Calculate $\langle\xi|(|\phi\rangle\langle\psi|)|\chi\rangle$ in the following two ways: (i) First, calculate the matrix $A := |\phi\rangle\langle\psi|$ and the vector $|\chi\rangle' := A|\chi\rangle$, and finally the inner product between $|\xi\rangle$ and $|\chi\rangle'$. (ii) Considering $\langle\xi|(|\phi\rangle\langle\psi|)|\chi\rangle$ as products of bra $\langle\xi|$, ket $|\phi\rangle$, bra $\langle\psi|$, and ket $|\chi\rangle$, and calculate first $\langle\xi|\phi\rangle$ and $\langle\psi|\chi\rangle$, and finally multiply them.

2.3 Qubit Systems

In this section, we survey the theory of quantum mechanics through the **qubit** system,[15] the simplest example of a quantum system. (See Chap. 5 for the general theory of QM.)

Roughly speaking, a qubit system is a quantum system where two outcomes are randomly obtained under the typical measurements.[16] Indeed, a qubit system is a quantum version (the quantization) of a classical bit system with two **root events** such as a system of a coin toss.

Theoretically, a qubit system is a quantum system described by a vector space $\mathbb{C}^2$. As we explain below, states, measurements, time evolutions of a qubit system are represented by vectors of $\mathbb{C}^2$ and 2×2 complex matrices. Although the way to predict a probability with these mathematics seems to be kind of strange, the important thing to remember is that the result perfectly coincides with what is happening in the microscopic world. Indeed, a qubit system is physically realized by the spin of an electron and the polarization of a photon, etc.

[13] For matrices A, B, C, we have $A(BC) = (AB)C$.

[14] For matrices A, B, C, it follows $(A + B)C = AC + BC$ and $C(A + B) = CA + CB$.

[15] A qubit system is sometimes abbreviated simply as a qubit, which is used as an information unit of a quantum information science, the quantum analogue of the classical bit.

[16] [Advanced Remark] One can consider a measurement with more than or less than two outcomes even in a qubit system. For instance, the measurement of observables with degenerate eigenvalues have only one outcome (Sect. 5.2.1). Moreover, POVM measurement can have more than and equal to three outcomes (Sect. 5.3.2). With this point of view, a qubit system can be operationally defined as a quantum system where the maximum number of the distinguishable states is two.

2.3.1 A Qubit System

The rules of measurement in a qubit system are summed up as follows:

(R1) A state is represented by a unit vector[17] $|\psi\rangle$ in $\mathbb{C}^2$.
(R2) A measurement is represented by an orthonormal basis (ONB) $\{|\phi_0\rangle, |\phi_1\rangle\}$ of $\mathbb{C}^2$.
(R3) When we perform a measurement $\{|\phi_0\rangle, |\phi_1\rangle\}$ under a state $|\psi\rangle$, we get an outcome $i = 0$ or 1 randomly with the probability

$$|\langle\phi_i|\psi\rangle|^2 \ (i = 0, 1).$$

The following example shows how these rules are used.

Example 2.1 (R1) Let the qubit system be in a state $|\psi\rangle = (\frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}})^T \in \mathbb{C}^2$ and (R2) perform the measurement of an ONB $\{|0\rangle, |1\rangle\}$ where $|0\rangle = (1, 0)^T$ and $|1\rangle = (0, 1)^T$. (R3) Then we get outcome 0 with probability $|\langle 0|\psi\rangle|^2 = |1 \times \frac{1}{\sqrt{5}} + 0 \times \frac{2}{\sqrt{5}}|^2 = |\frac{1}{\sqrt{5}}|^2 = \frac{1}{5}$, or outcome 1 with probability $|\langle 1|\psi\rangle|^2 = |\frac{2}{\sqrt{5}}|^2 = \frac{4}{5}$.

In the following, rules (R1)–(R3) are explained in detail one by one.

(R1): A state of a qubit system is mathematically represented by a unit vector of $\mathbb{C}^2$. The typical examples of states are

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.10}$$

From the information-theoretical point of view, these states may correspond to a classical bit 0 and 1. Namely, we can encode a classical bit, 0 and 1, to a quantum state $|0\rangle$ and $|1\rangle$, respectively.

Different from a classical bit system, where there are only two distinct states,[18] a qubit system has infinitely many states of arbitrary unit vectors in $\mathbb{C}^2$:

$$|\psi\rangle = (a, b)^T = a|0\rangle + b|1\rangle \tag{2.11}$$

with the normalization condition

$$|a|^2 + |b|^2 = 1. \tag{2.12}$$

[17] A vector with norm 1 is called a unit vector: For $|\psi\rangle = (a, b)^T$, a unit vector satisfies $||\psi|| = \sqrt{|a|^2 + |b|^2} = 1$.

[18] [Advanced Remark] The reader might think that even in a classical bit system there are more than two states by introducing a probability measure on $\{0, 1\}$. However, these states are mixed states, and there are only two pure states, 0 and 1. On the other hand, in a qubit system, there are infinitely many pure states (2.11). (See Sect. 5.3.1).

The state in Example 2.1 is one with $a = \frac{1}{\sqrt{5}}, b = \frac{2}{\sqrt{5}}$. Notice that a and b in (2.11) are written as $a = \langle 0|\psi\rangle, b = \langle 1|\psi\rangle$.[19] Thus, (2.11) is rewritten by

$$|\psi\rangle = \langle 0|\psi\rangle|0\rangle + \langle 1|\psi\rangle|1\rangle = \sum_{i=0,1} \langle i|\psi\rangle|i\rangle. \tag{2.13}$$

Note that this formula follows for any ONB $\{|\psi_i\rangle\}_{i=1}^d$ of $\mathbb{C}^d$:

$$\forall|\psi\rangle \in \mathbb{C}^d, \quad |\psi\rangle = \sum_{i=1}^{d} \langle\psi_i|\psi\rangle|\psi_i\rangle, \tag{2.14}$$

which will be frequently used below (see Exercise A.5).

The fact that a quantum state is represented by a vector implies that we can mathematically add two states as vectors to make a new quantum state. This is called the **superposition principle** and the added state is called a **superposition state**.

Note, however, that a state and a unit vector is not one-to-one. Different unit vectors parallel to each other corresponds to the same state. For instance, $|\psi\rangle = (1, 0)^T$ and $|\psi'\rangle = (i, 0)^T$ are different vectors, but as they satisfy $|\psi'\rangle = i|\psi\rangle$, they correspond to the same quantum state. More generally, if unit vectors $|\psi\rangle$ and $|\psi'\rangle$ are related as $|\psi'\rangle = c|\psi\rangle$ with a complex number c with magnitude 1, they represent the same quantum state. This is called an **indefiniteness of phase** as c is written by $c = e^{i\phi}$ where $\phi \in \mathbb{R}$ is called a **phase**.

In a qubit system, we sometimes use another state representation, which is mathematically equivalent to the unit vector representation of $\mathbb{C}^2$. (The reader can skip this part until necessary.) A qubit state can be represented by a three-dimensional real vector, called the **Bloch vector**. Different from the unit vector in $\mathbb{C}^2$, the Bloch vector enables us to geometrically grasp the properties of the states because the Bloch vector lives in $\mathbb{R}^3$. Moreover, the Bloch vector incorporates the indefiniteness of phase into the definition, and thus there is a one-to-one correspondence between a qubit state and the Bloch vector.

To introduce the Bloch vector, notice that any qubit state is written as

$$|\psi\rangle = \cos(\theta/2)|0\rangle + \mathrm{e}^{i\varphi}\sin(\theta/2)|1\rangle \tag{2.15}$$

with two real parameters θ, φ. In particular, their ranges are chosen to $0 \le \theta \le \pi, 0 \le \varphi < 2\pi$ for the one-to-one correspondence to a unit vector of $\mathbb{C}^2$ up to the phase indefiniteness.[20] Note that the ranges of θ, φ are exactly the same as those of

[19] By taking an inner product between $|0\rangle$ and (2.11), the left hand side is $\langle 0|\psi\rangle$, while the right hand side is $a\langle 0|0\rangle + b\langle 0|1\rangle = a$. Similarly, we get $b = \langle 1|\psi\rangle$.

[20] Write an arbitrary state in the form (2.11). Noting the normalization condition $|a|^2 + |b|^2 = 1$, there exists a real parameter θ' such that $|a| = \cos\theta'$, $|b| = \sin\theta'$ where the range of θ' is enough to be $0 \le \theta' \le \frac{\pi}{2}$ due to the positivity of the absolute value. Let φ_1 and φ_2 $(0 \le \varphi_1, \varphi_2 < 2\pi)$

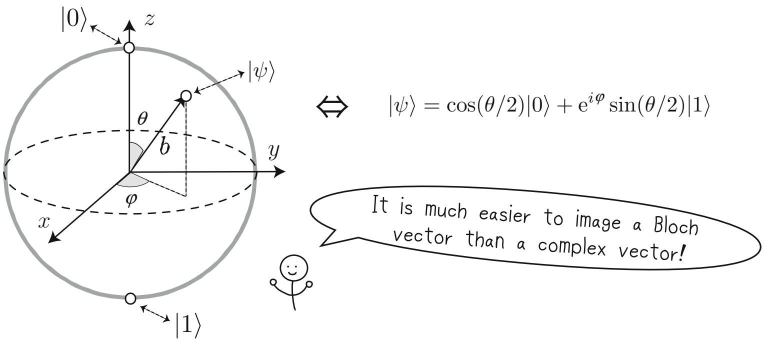

$|0\rangle$
z
$|\psi\rangle$
θ
b
y
φ
x
$|1\rangle$
$\Leftrightarrow$
$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$
It is much easier to image a Bloch vector than a complex vector!

Fig. 2.2 The Bloch vector and the Bloch sphere

angular parameters (the angle θ from the z axis and the angle φ between the x axis and the projection to xy plane) of the polar coordinate for the unit sphere in $\mathbb{R}^3$. Therefore, we have the one-to-one correspondence between a qubit state $|\psi\rangle \in \mathbb{C}^2$ and a three-dimensional vector $\boldsymbol{b} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)^T \in \mathbb{R}^3$ on the unit sphere through the relation (2.15). The correspondence is illustrated in Fig. 2.2. The unit sphere is called the **Bloch sphere**, and the three-dimensional vector on the sphere is called the Bloch vector. For instance, the states $|0\rangle$ and $|1\rangle$ correspond to the north and south poles of the Bloch sphere, respectively. Compared to the unit vector of $\mathbb{C}^2$, it is easy to imagine the Bloch vector helping us to geometrically grasp states. Moreover, as we explain in Sect. 5.3.1, the Bloch vector is redefined as a vector whose components are expectation values of some physical quantities, thus we can directly have a physical intuition from the Bloch vector representation.

(R2): To obtain an information from a physical system, we need to make a **measurement** (of a physical quantity). The typical measurement in a qubit system is a **basis measurement**.[21] A basis measurement has two distinct outcomes, and is mathematically represented by an ONB of $\mathbb{C}^2$. For instance, two unit vectors in (2.10) form an ONB $\{|0\rangle, |1\rangle\}$, which provides a typical example of a basis measurement.[22] In the field of quantum computation, this is called the **computational basis**. Example 2.1 uses a measurement of the computational basis. Of course, there are infinitely many ONBs, e.g.,

(Footnote 20 continued)
be arguments of a and b, respectively. Then, (2.11) can be written as $|\psi\rangle = e^{i\varphi_1}\cos\theta'|0\rangle + e^{i\varphi_2}\sin\theta'|1\rangle$. Due to the phase indefiniteness of a state, this state is physically equivalent to $|\psi'\rangle = \cos\theta'|0\rangle + e^{i(\varphi_2-\varphi_1)}\sin\theta'|1\rangle$. ($|\psi\rangle = e^{i\varphi_1}|\psi'\rangle$.) Therefore, we get (2.15) and its parameter range by putting $\varphi := \varphi_1 - \varphi_2$ $(0 \leq \phi < 2\pi)$, $\theta := 2\theta'$ $(0 \leq \theta \leq \pi)$. (See Sect. 5.3.1 for more general argument.)

[21] We will see more general measurements in Secs. 5.2 and 5.3.2.

[22] Notice that each unit vector in (2.10) can be a physical state. However, as an ONB, they can also represent a basis measurement.

$$|\xi_0\rangle := \frac{1}{\sqrt{2}}(1,1)^T, |\xi_1\rangle := \frac{1}{\sqrt{2}}(1,-1)^T \tag{2.16}$$

and

$$|\eta_0\rangle := \frac{1}{\sqrt{2}}(1,i)^T, |\eta_1\rangle := \frac{1}{\sqrt{2}}(1,-i)^T, \tag{2.17}$$

each corresponds to a basis measurement. In fact, as we explain later, each basis corresponds to a physical quantity. (See Sect. 5.2.1.)

Concerning the measurement outcome, we always label the two-valued outcomes by 0 and 1 in this chapter. In physics, we usually use a real number to represent an outcome with an appropriate unit system. On the other hand, in quantum information theory, the value of the outcome itself is generally not essential. Important things are to distinguish different outcomes to encode each information and to describe their probabilities for the occurrence.

(R3): Although we have the mathematical representations of states and measurements, at this stage, we don't get any physical information. We need the fundamental law for the proposition (2.1).

In a qubit system, the law is given as follows: if performing a basis measurement $\{|\phi_0\rangle, |\phi_1\rangle\}$ under a state $|\psi\rangle$, we randomly get an outcome $i = 0$ or 1 with the probabilities

$$|\langle\phi_i|\psi\rangle|^2 \ (i = 0, 1). \tag{2.18}$$

This is the simplest example of the proposition (2.1) of QM.

Excercise 2.3 Under a state $|\psi\rangle = (\frac{i}{\sqrt{3}}, \sqrt{\frac{2}{3}})^T$, let perform a basis measurement of (2.16). Calculate the probability to obtain each outcome. How about the case for the basis measurement of (2.17) under the same state?

Excercise 2.4 Make up a state and a basis measurement in a qubit system as you like, and calculate the probability for each outcome of the measurement under the state.

2.3.2 Time Evolution in Qubit System

A state can change as the time passes. In a qubit system, there are two kinds of time evolution:

(R4) Unitary time evolution: $|\psi\rangle \mapsto U|\psi\rangle$ with a unitary operator U.

(R5) State-change after a measurement: $|\psi\rangle \overset{\text{outcome } i}{\longmapsto} |\phi_i\rangle$ $(i = 0, 1)$ for a basis measurement $\{|\phi_i\rangle\}_{i=0,1}$.

(R4): The basic law of a time evolution in a qubit system is the **unitary evolution**: An initial state $|\psi\rangle \in \mathbb{C}^2$ and the final state $|\psi'\rangle \in \mathbb{C}^2$ are connected by a 2×2 unitary matrix[23] U such that

$$|\psi'\rangle = U|\psi\rangle. \tag{2.19}$$

U is called a **time evolution matrix**, or a unitary **transformation**, which characterizes the way how the quantum state evolves in time. (In Chap. 5, we see that the unitary evolution is based on the famous Schrödinger equation.)

The following example shows how (R4) is used.

Example 2.2 Consider a basis measurement of (2.16) after the time evolution with a time evolution matrix $U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ from an initial state $|0\rangle$. From (2.19), the final state is $|\psi'\rangle = U|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\xi_0\rangle$. From (2.18), the probabilities to obtain outcomes 0 and 1 are $|\langle\xi_0|\psi'\rangle|^2 = 1$ and $|\langle\xi_1|\psi'\rangle|^2 = 0$, respectively. In other words, we obtain the outcome 0 with certainty.

Notice that if $|\psi\rangle$ is a unit vector in $\mathbb{C}^2$, then so is $|\psi'\rangle = U|\psi\rangle$, assuring that they can represent a state in any time. This can be easily seen using the formula for a $d \times d$ matrix A:

$$\langle A^\dagger \chi|\xi\rangle = \langle\chi|A\xi\rangle \tag{2.20}$$

for all $|\chi\rangle, |\xi\rangle \in \mathbb{C}^d$.[24] Using this, we observe the norm-preservation property of a unitary matrix as follows:

$$||\psi'||^2 = \langle\psi'|\psi'\rangle = \langle U\psi|U\psi\rangle = \langle U^\dagger U\psi|\psi\rangle = \langle I\,\psi|\psi\rangle = \langle\psi|\psi\rangle = ||\psi||^2. \tag{2.21}$$

Note that we have used (2.20) for $|\chi\rangle = U|\psi\rangle$, $|\xi\rangle = |\psi\rangle$ and $A = U$ in the third equality and the unitarity condition $U^\dagger U = I$ in the forth equality.

In principle, we have different time evolutions as many as unitary matrices. Thus, a choice of a unitary matrix provides us a way to control a quantum system. For instance, in quantum computation, we theoretically find a unitary matrix which is of help to a particular calculation. (See Chaps. 3 and 4 for details.)

The following are examples of 2×2 unitary matrices which are often used in quantum information science:

- Unit matrix I and **Pauli matrices** $\sigma_x, \sigma_y, \sigma_z$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.22}$$

[23] Recall that a matrix U is called a unitary matrix iff it satisfies the unitarity condition $UU^\dagger = U^\dagger U = I$ where I is the unit matrix (or the identity matrix).

[24] As $A^\dagger = (\overline{a_{ji}})$ for $A = (a_{ij})$, we have $\langle A^\dagger\chi|\xi\rangle = \sum_i \overline{(A^\dagger|\chi\rangle)_i}\, y_i = \sum_i \overline{\sum_j \overline{a_{ji}} x_j}\, y_i = \sum_j \overline{x_j}(\sum_i a_{ji} y_i) = \langle\chi|A\xi\rangle$. We strongly recommend the reader to recognize the definition of the adjoint matrix not by the matrix elements but by the formula (2.20) (see Sect. A.3.3).

Pauli matrices σ_x, σ_y, σ_y are sometimes denoted as σ_1, σ_2, σ_3 or simply as X, Y, Z, respectively.

- **Hadamard matrix** H

$$H := \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.23}$$

- Rotations (on the Bloch sphere) R_x, R_y, R_z

$$R_x(\theta) = \cos(\theta/2)I - i\sin(\theta/2)\sigma_x = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \tag{2.24}$$

$$R_y(\theta) = \cos(\theta/2)I - i\sin(\theta/2)\sigma_y = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \tag{2.25}$$

$$R_z(\theta) = \cos(\theta/2)I - i\sin(\theta/2)\sigma_z = \begin{pmatrix} \exp(-i\theta/2) & 0 \\ 0 & \exp(i\theta/2) \end{pmatrix}. \tag{2.26}$$

The time evolutions with $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$ are clear in the Bloch vector representation of states: they transform a state by rotating the corresponding Bloch vectors by angle θ about the x, y, z axes (counterclockwise as viewed from the positive directions). For instance, the state $|0\rangle$ is transformed by $R_x(\pi/2)$ as $R_x(\pi/2)|0\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$, while the corresponding Bloch vectors of $|0\rangle$ and $R_x(\pi/2)|0\rangle$ are the north pole of the Bloch sphere and the vector with $(\theta, \varphi) = (\pi/2, 3\pi/2)$ (or $(0, -1, 0)$ in the normal coordinate of $\mathbb{R}^3$.)

Excercise 2.5 Show that Pauli matrices σ_x, σ_y, σ_z, Hadamard matrix H, and rotations R_x, R_y, R_z are all unitary.

Excercise 2.6 Let $|\psi\rangle = (\frac{i}{\sqrt{5}}, \frac{2}{\sqrt{5}})^T$ be an initial state. Calculate the probabilities to obtain outcomes 0 and 1 when making a basis measurement of computational basis after the time evolution with Pauli matrix σ_x.

Excercise 2.7 Show the following properties of Pauli matrices:

$$[\sigma_x, \sigma_y] = 2i\sigma_z, [\sigma_y, \sigma_z] = 2i\sigma_x, [\sigma_z, \sigma_x] = 2i\sigma_y \tag{2.27}$$

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I, \{\sigma_x, \sigma_y\} = \{\sigma_y, \sigma_z\} = \{\sigma_z, \sigma_x\} = 0 \tag{2.28}$$

Here $[A, B]$ and $\{A, B\}$ for matrices A, B are defined by $[A, B] := AB - BA$ and $\{A, B\} := AB + BA$, which are called the **commutator** and the **anticommutator** of A, B, respectively. Observe also that (2.27) and (2.28) can be summed up as $[\sigma_j, \sigma_k] = \sum_{l=1,2,3} 2i\epsilon_{jkl}\sigma_l$[25] and $\{\sigma_j, \sigma_k\} = 2\delta_{jk} I$ $(j, k = 1, 2, 3)$ with the **Levi-Civita Symbol** ϵ_{jkl}[26] and the Kronecker delta symbol.

[25] [Remark for physicists] From (2.27), the matrices $S_i := \frac{\hbar\sigma_i}{2}$ $(i = 1, 2, 3)$ represent angular momentums (or spin 1/2) [10].

[26] $\epsilon_{jkl} = 1$ if (j, k, l) is an even permutation of $(1, 2, 3)$, $\epsilon_{jkl} = -1$ if (j, k, l) is an odd permutation of $(1, 2, 3)$, otherwise $\epsilon_{jkl} = 0$.

(R5): In a quantum system, we have another time evolution caused by a performance of a measurement. This is completely different from the unitary time evolution in the sense that the way how a state changes depends on the obtained outcome. In this book, we call the state change due to the measurement a **measurement process**. A resultant state after the measurement is called a post-measurement state.

Though there are several kinds of measurement processes, the most typical one is the **projective measurement** with respect to a basis measurement: Assume that we obtain an outcome i ($i = 0, 1$) after performing a basis measurement $\{|\phi_0\rangle, |\phi_1\rangle\}$ under the initial state $|\psi\rangle$. Then, irrespective of the initial state, it changes to the state $|\phi_i\rangle$ ($i = 0, 1$) according to the obtained outcome i:

$$|\psi\rangle \overset{\text{outcome } i}{\longmapsto} |\phi_i\rangle \ (i = 0, 1). \tag{2.29}$$

Namely, a post-measurement state is one of the vectors of the basis $\{|\phi_i\rangle\}_{i=0,1}$. The occurrence of a state change due to a measurement is one of the distinct characters from a classical physics. We explain the general theory of measurement process in Sect. 5.3.4 in details (see also Sect. 5.2.4). Here, the reader should just recognize that this state-change is inevitable to get an information from a quantum system.

Example 2.3 Perform a basis measurement of a computational basis under a state $|\psi\rangle = \sqrt{1/3}|0\rangle + \sqrt{2/3}|1\rangle$. If we get the outcome 1 (which occurs with a probability $|\sqrt{1/3}|^2 = 1/3$), the state changes to $|0\rangle$; if we get the outcome 0 (which occurs with a probability $|\sqrt{2/3}|^2 = 2/3$), the state changes to $|1\rangle$.

Here, we notice a useful fact which enables us to fix a particular basis measurement, e.g., of a computational basis, by combining a measurement and a time evolution: Any basis measurement $\{|\psi_0\rangle, |\psi_1\rangle\}$ can be realized by another basis measurement $\{|\phi_0\rangle, |\phi_1\rangle\}$ combined with a time evolution given by the unitary U which satisfies $|\phi_i\rangle = U|\psi_i\rangle$ ($i = 0, 1$) (see Exercise A.12 for the existence of such a unitary matrix). Indeed, for any state $|\psi\rangle$, the probability to get an outcome $i = 0, 1$ by the measurement $\{|\phi_0\rangle, |\phi_1\rangle\}$ under the final state $|\psi'\rangle = U|\psi\rangle$ is given by

$$|\langle\phi_i|\psi'\rangle|^2 = |\langle\phi_i|U\psi\rangle|^2 = |\langle U^\dagger\phi_i|\psi\rangle|^2 = |\langle\psi_i|\psi\rangle|^2,$$

which coincides with the probability to get an outcome $i = 0, 1$ of the measurement $\{|\psi_0\rangle, |\psi_1\rangle\}$ under the initial state $|\psi\rangle$. Hence, these two operations are statistically equivalent for an arbitrary state $|\psi\rangle$.[27] Based on this fact, we sometimes (especially in the field of quantum computation) consider only the measurements of the computational basis.

[27] If one also wants to coincide the post-measurement states, then just apply $U^\dagger$ in the final step.

2.3.3 *Composition of Qubit Systems: n-Qubit Systems*

As the conclusion of this chapter, we explain the description of a composite system of a multiple qubit system. If we are interested in n qubit systems together e.g., considering their collisions, we need to describe their composite system. We call the composite system of n qubit systems an **n-qubit system**, or simply, a **multi-qubit system**. While the vector space $\mathbb{C}^2$ describes each qubit system, the vector space to describe an n-qubit system is the 2^n-dimensional Euclidean space $\mathbb{C}^{2^n} \simeq (\mathbb{C}^2)^{\otimes n} := \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ as the n-fold tensor product space.[28] Then, the descriptions of a state, a measurement, and a time evolution of an n-qubit system are given by simple generalizations of the ones in a qubit system:

(R1′) A state is represented by a unit vector $|\psi\rangle$ in $\mathbb{C}^{2^n}$.

(R2′) A measurement is represented by an ONB $\{|\phi_i\rangle\}_{i=1,\ldots,2^n}$ of $\mathbb{C}^{2^n}$.

(R3′) When we perform a measurement $\{|\phi_i\rangle\}_{i=1,\ldots,2^n}$ under a state $|\psi\rangle$, we get an outcome, labeled by e.g., $i = 1, \ldots, 2^n$, randomly with the probability

$$|\langle\phi_i|\psi\rangle|^2 \quad (i = 1, \ldots, 2^n). \tag{2.30}$$

(R4′) Unitary time evolution: $|\psi\rangle \mapsto U|\psi\rangle$ with a unitary operator U.

(R5′) State-change after a measurement: $|\psi\rangle \overset{\text{outcome } i}{\longmapsto} |\phi_i\rangle$ $(i = 1, \ldots, 2^n)$ for a basis measurement $\{|\phi_i\rangle\}_{i=1,\ldots,2^n}$.

However, to describe a composite system, it is important to specify the relations between each subsystem and the total system about states, measurements, and time evolutions. It is on this point that the tensor product structure plays an essential role.

We first explain the case of 2-qubit system in detail. Then, the generalization to the case of n-qubit system is straightforward.

First, consider the situation that two qubit systems are independently prepared in states $|\psi\rangle = (a_0, a_1)^T \in \mathbb{C}^2$ and $|\phi\rangle = (b_0, b_1)^T \in \mathbb{C}^2$, respectively. Then, the total state of the composite system is described by a unit vector in $\mathbb{C}^4$ characterized by the tensor product of $|\psi\rangle$ and $|\phi\rangle$:

$$|\psi\rangle \otimes |\phi\rangle := \begin{pmatrix} a_0|\phi\rangle \\ a_1|\phi\rangle \end{pmatrix} = \begin{pmatrix} a_0b_0 \\ a_0b_1 \\ a_1b_0 \\ a_1b_1 \end{pmatrix} \in \mathbb{C}^4 . \tag{2.31}$$

Example 2.4 Assume that two qubit systems are in a state $|\psi\rangle = \frac{1}{\sqrt{3}}(i, \sqrt{2})^T$ and $|\phi\rangle = \frac{1}{\sqrt{5}}(2, 1)^T$, respectively. From (2.31), the composite state is $|\psi\rangle \otimes |\phi\rangle = (\frac{i}{\sqrt{3}}|\phi\rangle, \frac{\sqrt{2}}{\sqrt{3}}|\phi\rangle)^T = \frac{1}{\sqrt{15}}(2i, i, 2\sqrt{2}, \sqrt{2})^T$.

[28] In this subsection, we briefly explain the necessary mathematics of the tensor product of $\mathbb{C}^2$ for qubit systems. For the details, see Appendix A.5.1.

It is noteworthy to observe here that the essential properties of the tensor product are the bilinearity[29] and the inner-product rule:

(Bilinearity) For any $|\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$, $|\phi\rangle, |\phi_1\rangle, |\phi_2\rangle \in \mathbb{C}^2$ and $a \in \mathbb{C}$,

(a) $(|\psi_1\rangle + |\psi_2\rangle) \otimes |\phi\rangle = |\psi_1\rangle \otimes |\phi\rangle + |\psi_2\rangle \otimes |\phi\rangle$,
(b) $|\psi\rangle \otimes (|\phi_1\rangle + |\phi_2\rangle) = |\psi\rangle \otimes |\phi_1\rangle + |\psi\rangle \otimes |\phi_2\rangle$,
(c) $a(|\psi\rangle \otimes |\phi\rangle) = (a|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (a|\phi\rangle)$.

(Inner product) For any $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$, $|\phi_1\rangle, |\phi_2\rangle \in \mathbb{C}^2$,

$$\langle \psi_1 \otimes \phi_1 | \psi_2 \otimes \phi_2 \rangle = \langle \psi_1 | \psi_2 \rangle \langle \phi_1 | \phi_2 \rangle, \tag{2.32}$$

where we use an abbreviated notation $|\psi \otimes \phi\rangle := |\psi\rangle \otimes |\phi\rangle$.

In a general argument, it is convenient to use these properties rather than going back to the vector components (2.31).

Excercise 2.8 By the direct use of (2.31), show the biniliarity (a), (b), (c) and the inner product rule (2.32).

A striking fact is that a state in a 2-qubit system is not always written in the product form (2.31). Due to the **superposition principle**, there exists a state composed of a superposition of states (2.31), and such superposition states generally cannot be written in the product form (2.31).

Example 2.5 A superposition state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(1, 0, 0, 1)^T \tag{2.33}$$

is a unit vector of $\mathbb{C}^4$ which cannot be written as the product form (2.31).[30]

A state with the form (2.31) is called a **product state**, while a state which cannot be written in the product form is called an **entangled state**. It is known that entangled states have a stronger correlation than classical ones.[31] As we will see in Chap. 7, entangled states play an important role for many applications to quantum information processings.

In a composite system, it is possible to perform a joint measurement of local measurements on each subsystem (see Fig. 2.3). In a 2-qubit system, we have a joint measurement of an ONB $\{|\psi_i\rangle\}_{i=0,1}$ of one qubit system and an ONB $\{|\phi_i\rangle\}_{i=0,1}$ of another qubit system together. Note that, as we have two outcomes 0, 1 in each

[29] See also (A.32) and footnote 27 in Appendix A.5.1.

[30] Assume on the contrary that (2.33) can be written in the product form $|\psi\rangle = |\phi\rangle \otimes |\xi\rangle$. Then, from (2.31), there exist complex numbers $a_0, a_1, b_0, b_1 \in \mathbb{C}$ such that $\frac{1}{\sqrt{2}}(1, 0, 0, 1)^T = (a_0 b_0, a_0 b_1, a_1 b_0, a_1 b_1)^T$. From the second element, we have $a_0 = 0$ or $b_1 = 0$. However, the former case contradicts the first element, and the latter case contradicts the forth element.

[31] Precisely speaking, an entangled state has a correlation which cannot be explained by any local realistic model [3].

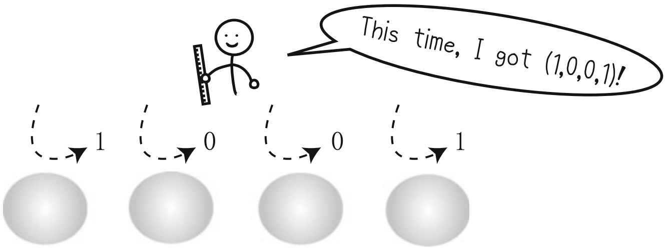


Fig. 2.3 An illustration of a joint measurement on a multiple qubit system

qubit system, a measurement outcome of a 2-qubit system is a pair of measurement outcomes (i, j) $(i, j = 0, 1)$. The joint measurement is then described by an ONB $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i,j=0,1}$ on $\mathbb{C}^4$, such that the joint probability to get an outcome (i, j) under a composite state $|\psi\rangle \in \mathbb{C}^2$ is given by

$$|\langle\psi_i \otimes \psi_j|\psi\rangle|^2 \ (i, j = 0, 1), \tag{2.34}$$

which is in accordance with (2.30): Note that $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i,j=0,1}$ forms an ONB of $\mathbb{C}^4$ since the orthonormality condition $(\langle\psi_i \otimes \phi_j|\psi_k \otimes \phi_l\rangle = \delta_{ik}\delta_{jl})$ follows by (2.32) and the dimension of $\mathbb{C}^4$ is 4 (see also Proposition A.13). If the measurement is the projective measurement, the post-measurement state is one of $|\psi_i\rangle \otimes |\phi_j\rangle$ depending on the outcome (i, j) (see (R5′)). A typical joint measurement is given by each computational basis. The corresponding ONB $\{|i\rangle \otimes |j\rangle\}_{i,j=0,1}$[32] of $\mathbb{C}^4$ is called the **computational basis** of a 2-qubit system. In the following, we use a further abbreviation $|ij\rangle := |i\rangle \otimes |j\rangle$ for the computational basis.

Example 2.6 Let the composite state $|\psi\rangle$ of a 2-qubit system be the entangled state (2.33) and consider the joint measurement of the computational basis $\{|ij\rangle\}_{i,j=0,1}$. Then, the joint probabilities to get outcomes (0, 0), (0, 1), (1, 0), and (1, 1) are given by $|\langle 00|\psi\rangle|^2 = |(1, 0, 0, 0)\frac{1}{\sqrt{2}}(1, 0, 0, 1)^T|^2 = 1/2$, $|\langle 01|\psi\rangle|^2 = |(0, 1, 0, 0)\frac{1}{\sqrt{2}}(1, 0, 0, 1)^T|^2 = 0$, $|\langle 10|\psi\rangle|^2 = |(0, 0, 1, 0)\frac{1}{\sqrt{2}}(1, 0, 0, 1)^T|^2 = 0$, and $|\langle 00|\psi\rangle|^2 = |(0, 0, 0, 1)\frac{1}{\sqrt{2}}(1, 0, 0, 1)^T|^2 = 1/2$, respectively. Therefore, the probability to get the same outcomes (i.e., (0, 0) or (1, 1)) is 1. (Note that we observe here a perfect correlation in the entangled state (2.33)).

In a joint measurement of a multi-qubit system, it is not necessarily to perform measurements on all qubit systems. It is possible to perform a local measurement of a subsystem of a multi-qubit system, for which we need to add a new measurement rule. In the case of a 2-qubit system, we can perform a local measurement of an ONB $\{|\psi_i\rangle\}_{i=0,1}$ of one qubit system only. To describe the measurement rule, it is convenient first to introduce an "inner product" between vectors living in different vector spaces. We define an "inner product" between a vector $|\chi\rangle \in \mathbb{C}^2$ of the left

[32] By using (2.31), check that $\{|i\rangle \otimes |j\rangle\}_{i,j=0,1}$ forms the standard bases $\{(1, 0, 0, 0)^T, (0, 1, 0, 0)^T, (0, 0, 1, 0)^T, (0, 0, 0, 1)^T\}$ of $\mathbb{C}^4$.

qubit and $|\psi\rangle := \sum_k |\xi_k\rangle \otimes |\eta_k\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$[33] by

$$\langle\chi|\psi\rangle := \sum_k \langle\chi|\xi_k\rangle|\eta_k\rangle \in \mathbb{C}^2 .$$

Similarly, one can define an "inner product" between a vector of the right qubit and a vector of the composite system. Roughly speaking, an "inner product" is to take the usual inner product between vectors belonging to the same vector space in the tensor product space, the left $\mathbb{C}^2$ in the above case. Notice, however, that the result of an "inner product" is not a scalar but a vector.

As an example, for the entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$ in (2.33), we have

$$\begin{aligned}\langle 0|\psi\rangle &= \frac{1}{\sqrt{2}}(\langle 0|0\rangle|0\rangle + \langle 0|1\rangle|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle\\ \langle 1|\psi\rangle &= \frac{1}{\sqrt{2}}(\langle 1|0\rangle|0\rangle + \langle 1|1\rangle|1\rangle) = \frac{1}{\sqrt{2}}|1\rangle.\end{aligned} \tag{2.35}$$

Now we are ready to describe the rule for a measurement in a subsystem: Under a composite state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ of a 2-qubit system, if we perform a basis measurement of an ONB $\{|\psi_i\rangle\}_{i=0,1}$ of one qubit system only (without loss of generality, let the qubit be the left part of $\mathbb{C}^2 \otimes \mathbb{C}^2$), then we get an outcome $i = 0, 1$ with the probabilities

$$||\langle\psi_i|\psi\rangle||^2 \quad (i = 0, 1). \tag{2.36}$$

This is a generalization of the rule (2.33). The projective measurement for this measurement is characterized by

$$|\psi\rangle \overset{\text{outcome } i}{\longmapsto} |\psi_i\rangle \otimes \langle\psi_i|\psi\rangle/||\langle\psi_i|\psi\rangle|| \quad (i = 0, 1). \tag{2.37}$$

The division by the norm in the last expression is simply for the normalization of the vector $\langle\psi_i|\psi\rangle$. Therefore, the state-change due to the projective measurement is essentially $|\psi\rangle \mapsto |\psi_i\rangle \otimes \langle\psi_i|\psi\rangle$: Namely, the state of the measured qubit changes to $|\psi_i\rangle$, as the usual projective measurement, while the state of the untouched qubit changes to $\langle\psi_i|\psi\rangle$ up to normalization.

Example 2.7 Under the entangled state (2.33) of a 2-qubit system, let perform a local measurement of the computational basis $\{|i\rangle\}_{i=0,1}$ on the left qubit. Then, from (2.35) and (2.36), the probabilities to get an outcome $i = 0, 1$ are $||\langle i|\psi\rangle||^2 = ||\frac{1}{\sqrt{2}}|i\rangle||^2 = \frac{1}{2}$. From (2.37), the post-measurement state with an outcome $i = 0, 1$

[33] Notice here that any vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$ can be written in the form $|\psi\rangle := \sum_k |\xi_k\rangle \otimes |\eta_k\rangle$: Letting $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i,j=0,1}$ be an ONB of $\mathbb{C}^2 \otimes \mathbb{C}^2$, any vector $|\psi\rangle$ can be written as $|\psi\rangle = \sum_{k,j} x_{kj}|\psi_k\rangle \otimes |\phi_j\rangle$ with complex coefficients $x_{kj} \in \mathbb{C}$. Using the bilinearity, we have $|\psi\rangle = \sum_k |\psi_k\rangle \otimes (\sum_j x_{kj}|\phi_j\rangle) =: \sum_k |\psi_k\rangle \otimes |\eta_k\rangle$.

is

$$|i\rangle \otimes \langle i|\psi\rangle / ||\langle i|\psi\rangle|| = |i\rangle \otimes |i\rangle. \tag{2.38}$$

Alternatively, if we start from the expression of the state:

$$|\psi\rangle = \sum_k |\psi_k\rangle \otimes |\eta_k\rangle, \tag{2.39}$$

then we have $\langle\psi_i|\psi\rangle = |\eta_i\rangle$ by using the orthonormality condition of $|\psi_i\rangle$. Therefore, one can immediately recognize that the probability to obtain an outcome i and the post-measurement state are

$$||\eta_i||^2 \text{ and } |\psi_i\rangle \otimes |\eta_i\rangle / ||\eta_i|| \quad (i = 0, 1), \tag{2.40}$$

directly from the expression (2.39).

Excercise 2.9 Consider a local measurement of the basis (2.16) on the right part of 2-qubit under the composite state $|\psi\rangle = \frac{1}{\sqrt{15}}(|00\rangle + 3|01\rangle - |10\rangle + 2|11\rangle)$ Calculate the probability to obtain an outcome i and the post-measurement state.

Finally, we explain the description of the local time evolution. In a 2-qubit system, each qubit system can independently evolves in time by the unitary time evolutions U and V, respectively. The total effect of the time evolution is given by the tensor product of the unitary matrices: $U \otimes V$ defined by the following action on $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$(U \otimes V)|\psi\rangle \otimes |\phi\rangle := U|\psi\rangle \otimes V|\phi\rangle.$$

From (2.31), $U \otimes V$ can be represented by a 4×4 complex matrix as follows: For $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$, $V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}$,

$$U \otimes V = \begin{pmatrix} u_{11}V & u_{12}V \\ u_{21}V & u_{22}V \end{pmatrix} = \begin{pmatrix} u_{11}v_{11} & u_{11}v_{12} & u_{12}v_{11} & u_{12}v_{12} \\ u_{11}v_{21} & u_{11}v_{22} & u_{12}v_{21} & u_{12}v_{22} \\ u_{21}v_{11} & u_{21}v_{12} & u_{22}v_{11} & u_{22}v_{12} \\ u_{21}v_{21} & u_{21}v_{22} & u_{22}v_{21} & u_{22}v_{22} \end{pmatrix}.$$

For example, the tensor product of two Hadamard transforms is given as

$$H \otimes H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Notice however, a general unitary matrix on $\mathbb{C}^4$ cannot be written in the product form $U \otimes V$.[34] Physically speaking, the time evolution matrix is in general not of the product form if there exists an interaction between qubit systems.

Although we have focused on the description of a 2-qubit system so far, the generalization to the composition of n-qubit systems is straightforward. The vector space is an n-fold tensor product of $\mathbb{C}^2$ which can be defined inductively as $(\mathbb{C}^2)^{\otimes n} := \mathbb{C}^2 \otimes (\mathbb{C}^2)^{\otimes n-1}$ $(n = 2, 3, \ldots)$. For instance, in a 3-qubit system, the composite state where the first qubit is in a state $|\psi\rangle = (a_0, a_1)^T \in \mathbb{C}^2$, the second qubit is in a state $|\phi\rangle = (b_0, b_1)^T \in \mathbb{C}^2$, and the third qubit is in a state $|\xi\rangle = (c_0, c_1)^T \in \mathbb{C}^2$, is described by

$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle \otimes |\xi\rangle &:= \begin{pmatrix} a_0 |\phi\rangle \otimes |\xi\rangle \\ a_1 |\phi\rangle \otimes |\xi\rangle \end{pmatrix} \\ &= (a_0b_0c_0, a_0b_0c_1, a_0b_1c_0, a_0b_1c_1, a_1b_0c_0, a_1b_0c_1, a_1b_1c_0, a_1b_1c_1)^T \in \mathbb{C}^8 . \end{aligned} \tag{2.41}$$

An ONB $\{|i_1\rangle \otimes |i_2\rangle \otimes \cdots |i_n\rangle\}_{i_1,\ldots,i_n=0,1}$ in $(\mathbb{C}^2)^{\otimes n}$[35] is again called the **computational basis** of n-qubit system. We use an abbreviation such as $|i_1\rangle \otimes |i_2\rangle \otimes \cdots |i_n\rangle = |i_1 i_2 \cdots i_n\rangle$ to avoid a lengthy notation. In the following, let us consider the joint measurement of the computational basis.[36]

A measurement of the computational basis on a composite system is physically realized by performing measurement of computational bases in each qubit system together. As we get two outcomes 0, 1 in each qubit system, the measurement outcome in the computational basis of an n-qubit system is given as an n-tuple of respective measurement outcomes $(i_1, i_2, \ldots, i_n)$ $(i_1, \ldots, i_n = 0, 1)$. (See Fig. 2.3). Thus, there are 2^n measurement outcomes, from $(0, \ldots, 0)$ to $(1, \ldots, 1)$.

First, consider a measurement of the computational basis $|i_1 i_2 \cdots i_n\rangle$ on an n-qubit system. Then, the probability to get an outcome $(i_1, \ldots, i_n)$ under a state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is given by

$$|\langle i_1 i_2 \cdots i_n | \psi\rangle|^2, \tag{2.42}$$

and the post-measurement state is one of $|i_1, \ldots, i_n\rangle$ depending on the outcome $(i_1, \ldots, i_n)$.

Next, consider a local measurement of the computational basis of an m-qubit $(m \leq n)$ system on an n-qubit system. For the simplicity of description, we focus

[34] For instance, the CNOT gate (3.10) in Chap. 3 is such an example.

[35] Check that $\{|i\rangle \otimes |j\rangle \otimes |k\rangle\}_{i,j,k=0,1}$ forms the standard basis $\{(1, 0, 0, 0, 0, 0, 0, 0)^T, (0, 1, 0, 0, 0, 0, 0, 0)^T, \ldots, (0, 0, 0, 0, 0, 0, 0, 1)^T\}$ of $\mathbb{C}^8$, by using (2.41).

[36] For an arbitrary choice of an ONB of each qubit, just replace the computational basis to the basis to obtain the general measurement rule. However, remind that the arbitrary basis measurement can be realized by the measurement of the computational basis with a suitable (locally) unitary transformation (see the end of Sect. 2.3.2). Hence, we don't lose any generality by restricting the measurement to the computational basis. Indeed, this is often done especially in the context of quantum computation.

on m-qubit system that consists of the m qubit systems from the left in $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$. By performing this measurement under a general state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, the probability to obtain an m-tuple of outcomes $(i_1, \ldots, i_m)$ is given by

$$||\langle i_1 \cdots i_m|\psi\rangle||^2, \tag{2.43}$$

where $\langle i_1 \cdots i_m|\psi\rangle$ is an "inner product" between a vector in $(\mathbb{C}^2)^{\otimes m}$ and a vector in $(\mathbb{C}^2)^{\otimes n}$: For a vector $|\chi\rangle \in (\mathbb{C}^2)^{\otimes m}$ and $|\psi\rangle = \sum_k |\xi_k\rangle \otimes |\eta_k\rangle \in (\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes n-m}$,

$$\langle \chi|\psi\rangle := \sum_k \langle \chi|\xi_k\rangle |\eta_k\rangle \in (\mathbb{C}^2)^{\otimes n-m}. \tag{2.44}$$

The post-measurement state with the measurement outcome $(i_1, \ldots, i_m)$ is given by

$$|\psi\rangle \overset{\text{outcome } (i_1,\ldots,i_m)}{\longmapsto} |i_1 \cdots i_m\rangle \otimes \langle i_1 \cdots i_m|\psi\rangle / ||\langle i_1 \cdots i_m|\psi\rangle||. \tag{2.45}$$

The division by the norm in the last expression is again for the normalization of the vector. Therefore, the state-change due to the projective measurement is essentially $|\psi\rangle \mapsto |i_1 \cdots i_m\rangle \otimes \langle i_1 \cdots i_m|\psi\rangle$.

Example 2.8 Consider a measurement of the computational basis of 2 left qubits on a 3-qubit system which is in a state $|\psi\rangle = \frac{1}{2}(|000\rangle + |001\rangle + |101\rangle + |111\rangle)$. Observing that $|\psi_{00}\rangle := \langle 00|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$, $|\psi_{01}\rangle := \langle 01|\psi\rangle = 0$, $|\psi_{10}\rangle := \langle 10|\psi\rangle = \frac{1}{2}|1\rangle$, $|\psi_{11}\rangle := \langle 11|\psi\rangle = \frac{1}{2}|1\rangle$ and using (2.43), the probabilities to get outcomes $(0, 0), (0, 1), (1, 0), (1, 1)$ are $||\psi_{00}||^2 = 1/2$, $||\psi_{01}||^2 = 0$, $||\psi_{10}||^2 = 1/4$, $||\psi_{11}||^2 = 1/4$, respectively. By (2.45), the post-measurement states with outcomes $(0, 0), (1, 0), (1, 1)$ are $|00\rangle \otimes |\psi_{00}\rangle/(||\psi_{00}||) = \frac{1}{\sqrt{2}}(|000\rangle + |001\rangle)$, $|10\rangle \otimes |\psi_{10}\rangle/||\psi_{10}|| = |101\rangle$, $|11\rangle \otimes |\psi_{11}\rangle/||\psi_{11}|| = |111\rangle$, respectively. Note that, there is no need to consider a post-measurement state for the outcome $(0, 1)$ as the probability to get it is zero.

References

1. B. d'Espagnat, *Conceptual Foundations of Quantum Mechanics*, 2nd edn. (Addison-Wesley, Reading, 1976)
2. Stanford Encyclopedia, http://plato.stanford.edu/
3. J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, New York, 1988)
4. A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1998)
5. C. A. Fuchs, quant-ph/0205039 (2002)
6. G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. A **84**, 012311 (2011)
7. G. Kimura, K. Nuida, H. Imai, arXiv:1012.5361v2 (2010)
8. G. Kimura, K. Nuida, J. Geom. Phys. **86**, 1–18. arXiv:1012.535v3 (2014)
9. A.N. Kolmogorov, *Foundations of the Theory of Probability*, 2nd edn. (Chelsea, New York, 1996) (Originally published in German in 1933)

10. P.A.M. Dirac, *The Principles of Quantum Mechanics*. (Oxford University Press, Oxford, 1958)
11. N.D. Mermin, *Quantum Computer Science: An Introduction*. (Cambridge University Press, Cambridge, 2007)

Chapter 3
Foundations on Quantum Computing

3.1 What is Computation?

The *computation* is an important concept to base a wide range of science and technology such as mathematics, and hence, you may be able to come up with a number of examples of the computation for specific problems. We now would like to discuss the concept of computation in mathematical manners. It is the theoretical computer science that the field offers the manner that formalizes the computation mathematically and discusses its (im)possibility.

Abstractly, computation is a procedure that transforms input information to the output result by a sequence of simple elementary operations. Let us consider a problem that decides if a given number x is a prime or not. This problem can be solved in hand by testing whether x is divisible by every number more than 1. If no number less than x divides x, then we decide x is a prime, and otherwise, it is a composite number. It is obvious for this procedure to provide a correct answer for every number x from the definition of primes. We can explicitly write down this procedure as follows. This procedure takes a number x we want to decide its primality as an input and then it automatically carries on steps shown in (i)–(iv). Finally, it outputs the result that is whether x is a prime or not.

```
Primality Test
       Input:  a number $x \in \mathbb{N}$
      Output:  1 if $x$ is a prime, and 0 if $x$ is a composite number

  (i) Set $y = 2$.
 (ii) If the remainder obtained by dividing $x$ by $y$ is equal to 0, output 0 and halt
      this procedure. Otherwise, go to (iii).
(iii) Increment $y$ by 1.
 (iv) If $y = x$, output 1 and halt this procedure. Otherwise, go back to (ii).
```

For example, let us take an input $x = 3$. At step (i), the value of y becomes 2. At step (ii), dividing 3 by 2, the remainder is 1. Hence, it does not halt and move to

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_3,

step (iii), and the value of y is incremented from 2 to 3. Then, $y = x$ holds at step (iv), and thus, this procedure outputs 1, that is, decides that the input 3 is a prime, and halts.

If you have learned any programming language, you can easily implement this procedure on your computer by a sequence of simple operations such as conditional branches and arithmetic operations. This procedure indeed consists only of simple operations, but we can obtain the correct answer for any number x by it. Such a procedure, a sequence of simple operations defined in advance, is usually called an **algorithm**. In order to formalize the algorithm mathematically, the above description is inadequate; we actually need to strictly define a mathematical model of a computer with its elementary operations. As one of specific models of a computer, we will briefly study the *circuit* model in Sect. 3.3.

In the field of the theoretical computer science, it is important not only if we can construct an algorithm that solves a given problem, but also how efficiently the algorithm solves the problem. It is because the field is also motivated by an engineering perspective that we wish to solve large-scale problems much faster when the algorithm is implemented on computers.

We usually measure the efficiency by **complexity**. In order to define the concept strictly, we need to define a mathematical model of algorithms, but we can roughly define the complexity of some problem as sufficient and necessary numbers of elementary operations for solving the problem. Since this concept is directly connected to computation time for solving the problem, it is also called time complexity. (If simply saying ‘complexity’, it usually indicates the time complexity, but note that the term ‘complexity’ covers a wide range of concepts of efficiency, for example, the space complexity of some problem is defined as sufficient and necessary amount of memory for solving the problem.) Precisely, the time complexity is one of complexity measures defined over a specific computational model called the Turing machine, and thus, for the circuit model to be discussed, we require another measure based on its elementary operations than the time complexity. In any case, the number of elementary operations is an important measure for the efficiency.

In particular, we are interested in roughly how long computation time we require, or how many elementary operations we require, to solve an input instance of a problem with respect to length of the input represented in binary digits. Since the computation time is realistically critical to handle huge inputs in computers, it is significant to roughly estimate the computation time with respect to very long instances in binary digits. Moreover, it is more reasonable to consider that the complexity of asymptotically long instances represents essential hardness of the problem. Therefore, we investigate an order of computation time on input length n (in binary digits), and estimate it using the order notation. For some constant C independent of input length n, if a function $t(n)$ which denotes the computation time satisfies $t(n) \leq C \cdot f(n)$ for all sufficiently large n, we write $t(n) = O(f(n))$, and say $t(n)$ is of order $f(n)$. Then, we consider $t(n)$ is smaller than $f(n)$ roughly. (See Definition 3.1 in Sect. 3.2 for the formal definition.)

Let us investigate computation time of the above algorithm for primality test. This algorithm uses several elementary operations, but we now only count the number of division for simplification. Let n be the binary length of a natural number x. (Note that n digits in binary can represent natural numbers from 0 to $2^n - 1$, and thus, we can identify $x \in \{0, 1\}^n$ as $x \in \{0, ..., 2^n - 1\}$.) If x is a prime, starting with $y = 2$, the algorithm repeats steps (i), (ii), and (iii) until $y = x$. Thus, the number of division in this case is at most $2^n - 2$. If x is a composite number, the algorithm halts before y arrives at x, and thus, the number of division is at most $2^n - 2$.

Is this algorithm the most efficient? Surely, it is quite significant to improve the efficiency of algorithms. Checking this algorithm carefully, we can notice that it wastes computation time. If x is a composite number, any factor of x must appear at less than or equal to $\lfloor \sqrt{x} \rfloor$. Thus, it is enough to check if x is divisible by all the natural numbers less than $\lfloor \sqrt{x} \rfloor$ for testing primality of x, where $\lfloor \sqrt{x} \rfloor$ denotes the maximum integer that does not exceed $\sqrt{x}$. (We summarize mathematical notation like $\lfloor \cdot \rfloor$ in Sect. 3.2.) Hence, we can significantly reduce the number of division by replacing step (iv) to the following step (iv$'$):

(iv$'$) If $y > \sqrt{x}$, output 1 and halt this procedure. Otherwise, go back to (ii).

It is easy to see that the number of division becomes $O(2^{n/2})$ by this replacement.

For the primality test, it is known that there is a polynomial-time algorithm (namely, an algorithm whose computation time is at most n^c for some constant c independent of input length n), which is called the Agrawal-Kayal-Saxena primality test [1]. Can we further improve the algorithm? Where is the limit of the improvements?, that is, how long computation time we require for primality test at least? In the field of the theoretical computer science, it is one of important research issues to prove lower bounds of time complexity of problems, namely, statements how long computation time any algorithm requires to solve the problem. Proving lower bounds of time complexity is often quite difficult for explicit problems. For example, the best known lower bound of time complexity of the primality test is n [2], and thus, it is unknown whether the currently best algorithm which takes roughly $O(n^6)$ time [3] is optimal or not.

So far, we only discussed *classical computation* implemented on conventional computers. *Quantum computation* is a new computational model that incorporates elementary operations given from principles of quantum physics, and it has been known that it has great advantages over classical computation for several computational tasks, as described below. In Sect. 3.2, we summarize basic notation generally required for discussions on information science throughout this book. We briefly review the classical circuit model as one of the models for classical computation in Sect. 3.3, and we introduce the quantum circuit model which deals with qubits as media of quantum information in Sect. 3.4.

In any computational model, we take an input (e.g., a natural number) encoded by a sequence of bits $\{0, 1\}$, apply an algorithm that consists of a sequence of elementary operations to the input, and then, output the result encoded by a sequence of bits $\{0, 1\}$ like the input. In the classical circuit model, we implement a classical algorithm by combining small predetermined functions (2-bit input 1-bit output functions defined in Table 3.1). In the quantum circuit model, we implement a quantum algorithm by applying a sequence of small predetermined unitary transforms (e.g., the Hadamard transformation (2.23)) to qubits generated from the input, and output a sequence of bits $\{0, 1\}$ that encodes the result obtained by measurement.

3.2 Mathematical Notation for Information Science

Let us summarize mathematical notation, including those used in the previous section, for information science in general.

We first introduce the floor and ceiling functions that associate reals with integers. The **floor function** maps a real x to the maximum integer less than or equal to x as $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$. The **ceiling function** maps a real x to the minimum integer more than or equal to x as $\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$.

In information science, the logarithm log plays an important role, and so does it in this book. It depends on contexts which base of logarithms we assume. In this book, all the logarithms are assumed to have base 2 unless it is explicitly stated otherwise, and we omit it. For a logarithm $\log_a x$ of x to base $a > 0$, since we have $\log_a x = \frac{1}{\log_b a} \log_b x$, we can see that the difference of bases only causes a gap of a constant factor, and it is easy to convert it to other bases. In information science, the logarithm is commonly assumed to have base 2, and then, a logarithm of a number expresses bits of the number. (When we express a natural number n in binary, the number of binary digits is $\lceil \log_2 n \rceil$.) In theories that deal with differentiation, it is usually assumed to have base of the natural logarithm e. Also, we write $\log^n x$ as $(\log x)^n$.

Next, let us define the **order notation** for asymptotic evaluation of functions.

Definition 3.1 Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions. If there exist a positive real C and $N_0 \in \mathbb{N}$ such that for every $n > N_0$ we have $f(n) \leq Cg(n)$, namely,

$$\overline{\lim_{n\to\infty}} \frac{f(n)}{g(n)} \leq C, \tag{3.1}$$

we write $f(n) \in O(g(n))$, or $f(n) = O(g(n))$. Also, there exist a positive real D and $N_0 \in \mathbb{N}$ such that for every $n > N_0$ we have $f(n) \geq Dg(n)$, namely,

$$\underline{\lim_{n\to\infty}} \frac{f(n)}{g(n)} \geq D, \tag{3.2}$$

we write $f(n) \in \Omega(g(n))$, or $f(n) = \Omega(g(n))$.

Note that the O notation and Ω notation give asymptotic upper and lower bounds, respectively. For example, For $f(n) = 2n^2 + 3n + 1$, we have $f(n) = O(n^2)$ and $f(n) = \Omega(n^2)$, and for $f(n) = n + \log^2 n$, $f(n) = O(n)$ and $f(n) = \Omega(n)$. Also, for $f(n) = 2^{3n} + 4n^{23}$, we have $f(n) = O(2^{3n})$ and $f(n) = \Omega(2^{3n})$.

Excercise 3.1 Let $f(n) = n^2 + \log^{\log n} n$. $f(n) = O(n^2)$?

We sometimes use the following asymptotic notions to express a function that asymptotically diminishes or dominates.

Definition 3.2 Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions. If, for every positive real c, there exists an $N_0 \in \mathbb{N}$ such that $f(n) \leq cg(n)$ for every $n > N_0$, namely,

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0, \tag{3.3}$$

we write $f(n) \in o(g(n))$, or $f(n) = o(g(n))$. Also, if for every positive real d there exists an $N_0 \in \mathbb{N}$ such that $f(n) \geq dg(n)$ for every $n > N_0$, namely,

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty, \tag{3.4}$$

we write $f(n) \in \omega(g(n))$, or $f(n) = \omega(g(n))$.

For example, if $f(n) = o(1)$, $f(n)$ approaches to 0 as n increases, and if $f(n) = \omega(n)$, $f(n)/n$ diverges to infinity.

The number of elements in a set we discuss, i.e., the **size of a set**, often is of significance in information science. We denote by $|\mathcal{X}|$ the size of a set $\mathcal{X}$ in this book.

3.3 Classical Circuit Model

We overview algorithms and complexity in Sect. 3.1. As mentioned there, we need to define a computational model to mathematically deal with algorithms. The best-known computational model is the Turing machine in the field of theoretical computer science, which performs computation in a manner close to programs on practical computers. However, since the definition of the Turing machine is somewhat complicated and it is tangled to handle the Turing machine in theory, we study another famous computational model called **classical circuit** model in this section. Note that the term "classical circuit" means a non-quantum circuit from the viewpoint of quantum computing, it is called a logical circuit model in the field of conventional (or, classical) computing.

The classical circuit consists of elementary gates of few predetermined types. Here we use $\wedge$ gate (AND gate), $\vee$ gate (OR gate), and $\neg$ gate (NOT gate). Each of gates implements a function of a fixed number of inputs and 1-bit output. The $\wedge$ and $\vee$ gates are 2-input and 1-output, and the $\neg$ gate is 1-input and 1-output. They implement functions as given in Table 3.1.

Conventionally, $\wedge$, $\vee$ and $\neg$ are treated as (unary and binary) operators. So, $\wedge(x_1, x_2)$ is usually denoted by $x_1 \wedge x_2$. In the classical circuit model, we construct a complicated circuit by combining these gates.

Table 3.1 Elementary gates of classical circuits

$\wedge$ gate		$\vee$ gate		$\neg$ gate	
Input	Output	Input	Output	Input	Output
00	0	00	0	0	1
01	0	01	1	1	0
10	0	10	1		
11	1	11	1		

A function is called a **Boolean function** if it maps a sequence of n bits to 1 bit, and a classical circuit computes this function. For a given Boolean function $f : \{0, 1\}^n \to \{0, 1\}$, a circuit computing f is not unique in general. Then, we wish to choose a way to save a computational resource, i.e., a way of low complexity from a viewpoint of theoretical computer science. In circuit models, elementary gates correspond elementary operations in algorithms, and thus, the number of the gates used in the circuit is typically adopted as a measure of efficiency.

Definition 3.3 The **circuit complexity** $\mathcal{C}(f)$ of a Boolean function $f : \{0, 1\}^n \to \{0, 1\}$ is defined by the number of gates used in the minimum circuit that correctly computes f. Namely, denoting by $|C|$ the number of gates in a circuit C, we have $\mathcal{C}(f) := \min\{|C| : \forall x \in \{0, 1\}^n,\ C(x) = f(x)\}$.

The circuit complexity is closely related to computation time of algorithms (i.e., time complexity of Turing machines), but we omit the details here (see, for example, [4] for the details). In this book, it is enough to just recognize that we have an efficient algorithm that computes f if we have a small circuit for f. (This is the same as the relation between quantum algorithms and quantum circuits.)

As an example, let us consider the following simple problem called the parity problem. Given an n-bit sequence x, we decide whether the number of 1's in x is odd or even. We construct a classical circuit computing a function $\mathrm{PARITY} : \{0, 1\}^n \to \{0, 1\}$ which correctly decides the parity function (i.e., $\mathrm{PARITY}(x) = 1$ if it is odd and $\mathrm{PARITY}(x) = 0$ if it is even). In the case where $n = 2$, namely, $x = x_1 x_2$ ($x_1, x_2 \in \{0, 1\}$), we can implement the exclusive OR[1] of 2 inputs, i.e., the addition over a finite field $\mathbb{F}_2$ ($0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$), by using 5 elementary gates as shown in the following Fig. 3.1.

$$x_1 \oplus x_2 = \oplus(x_1, x_2) = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2).$$

For general n inputs, i.e., $x = x_1 \cdots x_n$ ($x_1, \ldots, x_n \in \{0, 1\}$), we have $\mathrm{PARITY}(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n = (x_1 \oplus \cdots \oplus x_{n/2}) \oplus (x_{n/2+1} \oplus \cdots \oplus x_n)$ if n is even, and $\mathrm{PARITY}(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n = (x_1 \oplus \cdots \oplus x_{(n-1)/2}) \oplus (x_{(n-1)/2+1} \oplus \cdots \oplus x_n)$ if

[1] We use the symbol $\oplus$ to denote the exclusive OR in accord with convention of theoretical computer science, but note that the symbol $\oplus$ is also used to denote the direct sum of linear spaces and matrices in this book.

$\oplus$ gate

input	output
00	0
01	1
10	1
11	0

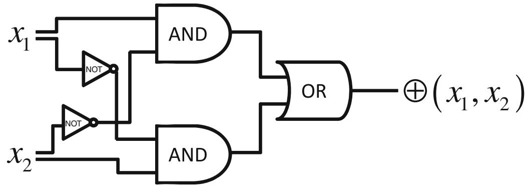


Fig. 3.1 Exclusive OR $\oplus$

n is odd. Therefore, an n-input PARITY can be recursively constructed from at most two $\lceil n/2 \rceil$-input PARITYs and one 2-input PARITY (where $\lceil n/2 \rceil$ is the minimum integer larger than or equal to $n/2$). By a simple calculation, we can figure out that the number of gates is $O(n)$ in this circuit.

By constructing an explicit circuit that computes the function, we can prove an upper bound of circuit complexity of the function. For example, the above circuit construction shows that $\mathcal{C}(\text{PARITY}) = O(n)$.

Then, can we compute any function by combining elementary gates? If possible, what is an upper bound of circuit complexity of the function? The following theorem answers these questions:

Theorem 3.1 *For any $n \in \mathbb{N}$ and any Boolean function $f : \{0, 1\}^n \to \{0, 1\}$ of n-bit input and* 1*-bit output, the circuit complexity of f is at most* $5 \cdot 2^{n-1} - 4$.

Proof By induction. Boolean functions of 1-bit input and 1-bit output are $f(x) = c$ $(c \in \{0, 1\})$, $f(x) = x$, and $f(x) = \neg x$, and hence, the number of gates is at most 1. (We need one $\neg$ gate in the case $f(x) = \neg x$.) Assume that any Boolean function of $(n-1)$-bit input and 1-bit output can be constructed from $5 \cdot 2^{n-2} - 4$ elementary gates. Note that the following equality holds:

$$f(x_1, \ldots, x_{n-1}, x_n) = (\neg x_n \wedge f(x_1, ..., x_{n-1}, 0)) \vee (x_n \wedge f(x_1, ..., x_{n-1}, 1)), \tag{3.5}$$

where x_i is a variable over $\{0, 1\}$. (Check the value of the righthand side by substituting 0 and 1 into x_n in the lefthand side.) By the assumption for induction, $5 \cdot 2^{n-2} - 4$ gates suffice to compute each of two functions $f(x_1, ..., x_{n-1}, 0)$, $f(x_1, ..., x_{n-1}, 1)$ of $(n-1)$-bit input. By the above equality, a circuit computing the function $f(x_1, ..., x_n)$ of n-bit input and 1-bit output can be constructed from two $\wedge$ gates, one $\vee$ gate, one $\neg$ gate, and circuits of $f(x_1, ..., x_{n-1}, 0)$ and $f(x_1, ..., x_{n-1}, 1)$. Thus, any Boolean function of n-bit input and 1-bit output can be computed with at most $2 \cdot (5 \cdot 2^{n-2} - 4) + 4 = 5 \cdot 2^{n-1} - 4$ gates. □

Now, what can we prove for lower bounds of circuit complexity? It is quite difficult to prove lower bounds of explicit functions because we need to prove that any small circuit cannot compute the explicit function. However, we can show the existence of a hard function that no small circuit computes as follows. (We generally say a function is hard if it is impossible to compute with small amounts of computational resources like the number of gates.)

Theorem 3.2 *For any $n \in \mathbb{N}$, there exists some Boolean function of n-bit input and* 1*-bit output $f : \{0, 1\}^n \to \{0, 1\}$ such that circuit complexity of f is at least $2^n/2n$.*

Proof We first count up the number of functions of n-bit input and 1-bit output, and then we bound the number of circuits constructed from less than s gates from above. For some appropriate s, we can show that the number of the functions (of n-bit input and 1-bit output) is larger than the number of the circuits, and hence, there exists a function that no small circuit computes. This is called counting argument, often used in complexity theory.

Any function of n-bit input and 1-bit output has one-to-one correspondence with a list of 2^n-bit output values $f(0\cdots0), \ldots, f(1\cdots1)$. Since the number of such lists is 2^{2^n}, the total number of the functions is 2^{2^n}.

On the other hand, an upper bound of the number of Boolean functions that have less than s gates can be evaluated as follows: First, we count the number of ways to connect each of gates to the others. Each gate has at most two input wires, and each input wire connects to output wire of one of other $s - 1$ gates. Thus, the number of ways to connect every gate to the others is at most $\binom{s-1}{2}$ at each of gates. Since this is counted up at each of gates, the total number of ways of the connection is at most $\binom{s-1}{2}^s$. Also, every gate should be assigned to one of $\wedge$, $\vee$, $\neg$ and the identity gate doing nothing of 1-bit input and 1-bit output, and then, the number of ways of the assignment is 4^s. Therefore, the total number of circuits constructed from at most s gates is $\binom{s-1}{2}^s \cdot 4^s = (2(s-1)(s-2))^s$. If $s \le 2^n/2n$, this value is less than 2^{2^n}, and thus, there exists a function that no circuit constructed from at most $2^n/2n$ gates compute. □

Since we took easier proofs for circuit complexity of general functions here, we have some gap between upper and lower bounds. In fact, we can improve the upper bound by a more complicated proof, and we can show any function is computable by a circuit of $O(2^n/n)$ gates [4]. Therefore, the sufficient and necessary number of the gates to compute any Boolean function of n-bit input and 1-bit output is $2^n/n$ if constant factors are ignored.

We can prove not only a hard function exists but also almost all the functions are in fact hard by the same counting argument.

Theorem 3.3 *For any $n \in \mathbb{N}$, among all the 2^{2^n} Boolean functions of n-bit input and* 1*-bit output, the circuit complexity of more than $(1 - 2^{-(\log n/n)2^n})2^{2^n}$ functions is at least $2^n/2n$. Namely, we have*

$$\Pr\left\{\mathcal{C}(f) \ge \frac{2^n}{2n}\right\} \ge 1 - 2^{-(\log n/n)2^n},$$

where f is chosen uniformly at random from all the Boolean functions of n-bit input and 1*-bit output and $\mathcal{C}(f)$ denotes the circuit complexity of f.*

Therefore, for sufficiently large n, a fraction of functions of high circuit complexity (approximately $2^n/n$) becomes almost one.

Excercise 3.2 Prove Theorem 3.3.

As this theorem shows, almost all the Boolean functions have very high circuit complexity. However, it is extremely difficult to show such high circuit complexity of explicit problems like the primality test. Generally in complexity theory, proving lower bounds of explicit problems is quite difficult and important as in the circuit model. In fact, the outstanding NP $\neq$ P conjecture [5, 6], which is offered a reward of 1 million dollars for the resolution as well as the Riemann hypothesis and other famous conjectures, is the problem proving lower bounds of time complexity for some sort of problems.

Remark 3.1 As mentioned above, we focus on how computation proceeds at large parameters in the field of theoretical computer science. For example, while we gave estimations of circuit complexity which holds for any n in Theorem 3.3 and others, it is sufficient to observe if the theorems hold for any sufficiently large n in order to overview behaviours of computation. Also, it is possible to improve the bounds by more detailed calculations, but such improvements are not so significant to understand the nature of computation. (Surely, a significant improvement from a new perspective is quite important since it would provide a way approaching to nature of the complexity.)

Remark 3.2 As stated above, we focus on time complexity of an algorithm in theoretical computer science. In particular, if upper bounds of the time complexity is a polynomial in n, we say the algorithm runs in polynomial time, and we often regard it is efficient. Realistically, $O(n)$, $O(n \log n)$ and $O(n^2)$-time algorithms are commonly used as efficient ones, and hence, it is important to design such algorithms of low complexity for practical use. Obviously, we cannot say n^{100}-time algorithm is efficient in practice, which indeed runs in polynomial time in n. However, for sake of theoretical usefulness and beauty, the notion of polynomial time is taken as a representative criteria of the 'efficiency'.

3.4 Quantum Circuit Model

In the classical circuit model which is one of the models that perform classical computation, a circuit performs computation by operating a sequence of bits $\{0, 1\}^n$. Quantum computation can perform stronger computation by extending the classical circuit model to the model over quantum mechanics. In this section, we study the *quantum circuit model*, which is one of the models that perform quantum computation. (Besides the quantum circuit model, there is also the model called the quantum Turing machines as a generalization of the Turing machines.)

The **qubit** was introduced as information media by generalizing the classical bit in Sect. 2.3. However, we cannot perform information processing only by media.

Hence, we need to introduce a model of circuits that operate qubits like the model of classical circuits that operate classical bits in classical computation. There are a lot of theoretical models that operate qubits, but in this book, we focus only on the **quantum circuit** model which is simple and widely used.

Computation in the classical world is transformation from classical bits to classical bits. Quantum computation, which is an extension of the classical computation, provides transformation from qubits to (classical) bits or qubits. The basic operations that quantum algorithms can perform are measurements and unitary transformations. Since quantum algorithms basically perform the basis measurement in the computational basis, if we simply say 'measurement', it means "basis measurement in the computational basis". Recall that an $N \times N$ unitary matrix $U \in \mathbb{C}^{N \times N}$ is a square matrix that satisfies $UU^\dagger = U^\dagger U = I$, where † denotes the complex conjugate transpose and I denotes the identity matrix. We generally suppose $N := 2^n$ in the context of quantum computation, where n dentoes length of qubit sequences to which we apply the unitary matrix, since the n-qubit sequence is a 2^n-dimensional vector. Recall that the Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ are defined as the following unitary matrices by (2.22) in Sect. 2.3

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.6}$$

Since the Pauli matrix σ_x performs $\sigma_x|0\rangle = |1\rangle, \sigma_x|1\rangle = |0\rangle$, it achieves the **bit flip**, which is the same as the $\neg$ gate in the classical circuit model. The Pauli matrix σ_z performs $\sigma_z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$, which is called the **phase flip**.

Recall that the **Hadamard transform** H is defined as the following 2×2 matrix by (2.23) in Sect. 2.3.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.7}$$

Applying this to qubits $|0\rangle, |1\rangle$, we have

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \\ H|1\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \end{aligned}$$

The Hadamard transform H is used frequently in quantum computation. Like the Hadamard transform, when a unitary matrix has fixed small input and output lengths, it is called a **quantum gate**. We also include an operation of the 1-qubit measurement (in the computational basis), which is not unitary, into the set of quantum gates.

We usually illustrate a quantum circuit with quantum gates by diagrams like Fig. 3.2. This figure shows the following procedure: One qubit comes from left of the input wire. The qubit is applied a transformation by a quantum gate (the Hadamard

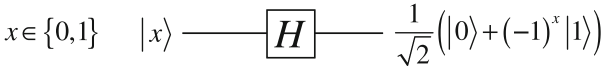


Fig. 3.2 Hadamard transform

transform in this case) at the center box, and then the gate sends it to right of the output wire.

Remark 3.3 Note that unitary matrices transform othorgonal vectors to othorgonal vectors as preserving the **Euclid distance** ($d(|\phi\rangle, |\psi\rangle) := \sqrt{\langle \phi - \psi, \phi - \psi \rangle}$). Also, unitary matrices are invertible. Thus, any computation process without measurements has its inverse of the process. (The measurements are irreversible.)

Recall that an n-qubit sequence $|\phi\rangle$ and an m-qubit sequence $|\psi\rangle$ can be concatenated to an $n+m$-qubit sequence $|\phi, \psi\rangle = |\phi\rangle \otimes |\psi\rangle$. Applying a $2^n \times 2^n$ unitary matrix U and a $2^m \times 2^m$ unitary matrix V to $|\phi\rangle$ and $|\psi\rangle$ respectively, we obtain $U|\phi\rangle \otimes V|\psi\rangle$. This operation is also represented as

$$(U \otimes V)|\phi, \psi\rangle := (U \otimes V)|\phi\rangle \otimes |\psi\rangle = U|\phi\rangle \otimes V|\psi\rangle \tag{3.8}$$

by a **tensor product** of matrices. The tensor product of two matrices U and V is defined as follows. We denote by $M = [m_{i,j}]_{i,j \in \{1,\dots,d\}}$ a $d \times d$ matrix having an element $m_{i,j}$ at (i, j) entry. For $U = [u_{i,j}]_{i,j \in \{1,\dots,2^n\}}$, we have

$$U \otimes V = \begin{pmatrix} u_{1,1}V & u_{1,2}V & \cdots & u_{1,2^n}V \\ u_{2,1}V & \ddots & & \\ \cdots & & & \\ u_{2^n,1}V & u_{2^n,2}V & \cdots & u_{2^n,2^n}V \end{pmatrix}. \tag{3.9}$$

The Hadamard transform is a 2×2 unitary matrix, namely, an operation acting on 1 qubit. We also have several important operations acting on (more than) 2 qubits. Among 2-qubit operations, the following operation is primalily important, and is called the **controlled NOT gate**. which is abbreviated to **CNOT gate** and whose unitary is written as CNOT (Fig. 3.3a).

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.10}$$

CNOT was originally invented at the area called "reversible computation", which is one of the areas in classical computation. The reason why this is called controlled NOT is that the first input bit plays a role of a controller for an operation on the second input bit, and if the first bit is 1 the second bit is flipped as the ¬ gate is applied to, and otherwise, the second bit does not change. In both cases, the first bit

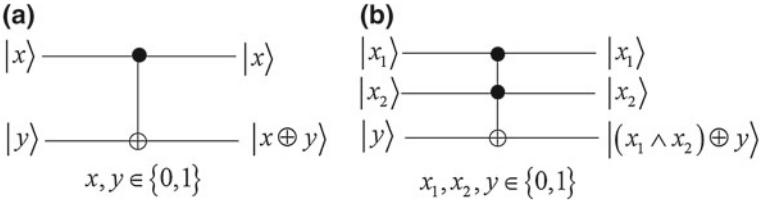


Fig. 3.3 **a** Controlled NOT gate. **b** Toffoli gate

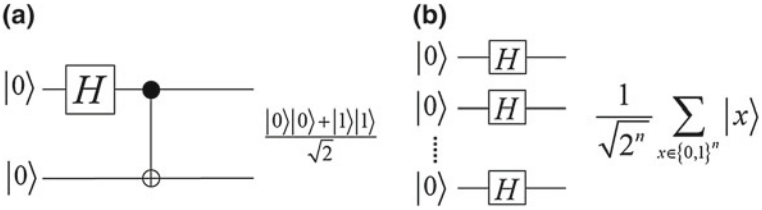

(a)
$|0\rangle$
H
$|0\rangle$
$\frac{|0\rangle|0\rangle+|1\rangle|1\rangle}{\sqrt{2}}$
(b)
$|0\rangle$
H
$|0\rangle$
H
$|0\rangle$
H
$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

Fig. 3.4 **a** Hadamard gates + CNOT. **b** Parallel application of Hadamard gates

is output as it is. This gate works similarily in the quantum case. For example, if we input $|01\rangle = |0\rangle \otimes |1\rangle = |0\rangle|1\rangle$ and $|10\rangle = |1\rangle \otimes |0\rangle = |1\rangle|0\rangle$ to CNOT, we have

$$\mathrm{CNOT}|01\rangle = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |01\rangle,$$

$$\mathrm{CNOT}|10\rangle = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |11\rangle,$$

respectively. We can easily see that we cannot decompose CNOT into a tensor product of any two unitary matrices on 1 qubit since the second output bit depends on the first input bit.

A generalization of the controlled NOT gate is also often considered. The generalized controlled NOT gate of $k + 1$-bit input and $k + 1$-bit output takes k bits as the controller. If they all are 1, the $(k + 1)$-th input bit is flipped, and otherwise, the $(k + 1)$-th bit does not change. Namely, we have

$$\mathrm{GCNOT}|x_1, ..., x_k, y\rangle = |x_1, ..., x_k, y \oplus (x_1 \wedge \cdots \wedge x_k)\rangle. \tag{3.11}$$

If $k = 1$ it is obviously equivalent with CNOT, and if $k = 2$ it is called the **Toffoli gate** (Fig. 3.3b), or controlled-controlled NOT gate CCNOT, which is also an important gate often discussed in areas of the reversible computation and quantum computation.

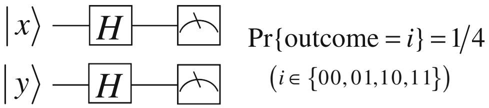

$|x\rangle$
H
$|y\rangle$
H
$\Pr\{\text{outcome} = i\} = 1/4$
$(i \in \{00, 01, 10, 11\})$

Fig. 3.5 Hadamard gates + measurements

Let us see examples of quantum circuits in Fig. 3.4. In the quantum circuit given in Fig. 3.4a, we first apply the Hadamard transform to the first qubit, and then apply CNOT gate to the result. Let us consider a case that we input $|00\rangle = |0^2\rangle$ to this circuit. We first apply the Hadamard transform to the first qubit and nothing, i.e., the identity matrix I to the second qubit, namely, we have

$$\begin{aligned}|00\rangle \overset{H \otimes I}{\longmapsto} (H \otimes I)|00\rangle = (H|0\rangle) \otimes (I\,|0\rangle) &= \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}\,(|00\rangle + |10\rangle)\,.\end{aligned}$$

We next apply the CNOT gate to the resultant sequence of qubits $(|00\rangle + |10\rangle)/\sqrt{2}$. Then, we have

$$\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{\text{CNOT}}{\longmapsto} \frac{1}{\sqrt{2}}(\text{CNOT}|00\rangle + \text{CNOT}|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

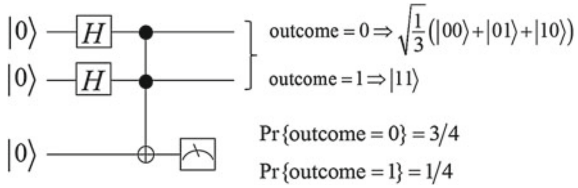
The quantum circuit given in Fig. 3.4b uses n Hadamard transforms. If we input $|0\cdots0\rangle = |0^n\rangle$ to this circuit as an initial qubit sequence, each of n qubits is transformed as $|0\rangle \overset{H}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ from the definition of the Hadamard transform. Viewing this as an n-qubit sequence, we have

$$\begin{aligned}|0^n\rangle \overset{H^{\otimes n}}{\longmapsto} H|0\rangle \otimes \cdots \otimes H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle,\end{aligned}$$

namely, we obtain a qubit sequence that superposes the 2^n bases from $|0\cdots0\rangle$ up to $|1\cdots1\rangle$ with the equal amplitude $1/\sqrt{2^n}$. This operation generating the superposition of the equal amplitude is used frequently for design of quantum algorithms. (See Sects. 4.2 and 4.3.)

We also see examples of quantum circuits with measurements. The first example is given in Fig. 3.5. In this diagram, the quantum circuit first applies Hadamard transforms $H \otimes H$ to two qubits $|x, y\rangle$ for $x, y \in \{0, 1\}$, and then, it performs 1-qubit measurements on the resultant qubits. After the application of the Hadamard transforms to the initial qubits $|x, y\rangle$ we have:

Fig. 3.6 Toffoli gates + measurements


$|0\rangle$
$|0\rangle$
$|0\rangle$
H
H
$\text{outcome} = 0 \Rightarrow \sqrt{\frac{1}{3}}(|00\rangle + |01\rangle + |10\rangle)$
$\text{outcome} = 1 \Rightarrow |11\rangle$
$\Pr\{\text{outcome} = 0\} = 3/4$
$\Pr\{\text{outcome} = 1\} = 1/4$

$$\begin{aligned} H \otimes H|x, y\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle + (-1)^x|1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + (-1)^y|1\rangle\big) \\ &= \frac{1}{2}\big(|00\rangle + (-1)^y|01\rangle + (-1)^x|10\rangle + (-1)^{x+y}|11\rangle\big). \end{aligned}$$

Then, the measurement operations on these two qubits provide outcome one of 00, 01, 10, 11 with equal probability independently of x and y from the definition of the basis measurement in the computational basis.

The second example is given in Fig. 3.6. In this diagram, the quantum circuit first applies the Hadamard transforms to the first two qubits, and then, it applies the Toffoli gates to all the three qubits. Giving the initial qubits $|000\rangle$ to this quantum circuit, we have after the Hadamard transforms to the first two qubits:

$$(H \otimes H \otimes I)|000\rangle = \frac{1}{2}\sum_{x\in\{0,1\}^2} |x\rangle|0\rangle.$$

Next, we have after the Toffoli gate:

$$\begin{aligned} \text{CCNOT}\left(\frac{1}{2}\sum_{x\in\{0,1\}^2} |x\rangle|0\rangle\right) &= \frac{1}{2}\sum_{x\in\{0,1\}^2} \text{CCNOT}|x\rangle|0\rangle \\ &= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle\right)|0\rangle + \frac{1}{2}|11\rangle|1\rangle. \end{aligned}$$

Recall that CCNOT negates the third bit if and only if the first and second bits are given ones.

Performing the measurement only on the third bit, we have an outcome 0 with probability $3/4$ and an outcome 1 with probability $1/4$. When the outcome is 0, the first and second qubits are given $\sqrt{\frac{1}{3}}\,(|00\rangle + |01\rangle + |10\rangle)$. When the outcome is 1, they are given $|11\rangle$.

Excercise 3.3 Verify the outputs of the above two quantum circuits from the definition of the measurement. (See Sect. 2.3.3.)

As mentioned before, classical circuits can compute any Boolean function by combining the predetermined elementary gates. Also in the quantum circuit model, we can implement any unitary matrix as a quantum circuit by combining some elementary quantum gates of predetermined low-dimensional unitary matrices.

We now move to more details of fundamental issues on quantum circuits, but readers who are interested in quantum algorithms rather than quantum circuits can skip to the next chapter "Quantum Algorithms" only with the knowledge of quantum circuits so far.

First, we consider a systematic way to implement an arbitrary unitary matrix on 1 qubit by combining elementary quantum gates. Recall that any qubit can be represented by the Bloch ball. (See Sect. 2.3.2.) In fact, as the following theorem shows, any 2×2 unitary matrix U can be represented by using R_y and R_z that represent clockwise rotations in the positive y-axis and z-axis on the Bloch ball, repectively. (See Sect. 2.3.2 (2.24).)

Theorem 3.4 (Z–Y Decomposition) *For any* 2×2 *unitary matrix* U*, there exist* $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ *such that* $U = \mathrm{e}^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

Since we can ignore the scalar transformation $\mathrm{e}^{i\alpha}$ on the global phase for operations on 1 qubit, any 1-qubit gate has the form of $R_z(\beta) R_y(\gamma) R_z(\delta)$.

Proof Since U is unitary, all the row (column) vectors are othonormal to each other. Therefore, we have for some $\alpha, \beta, \delta, \gamma \in \mathbb{R}$

$$U = \begin{pmatrix} \mathrm{e}^{i(\alpha-\beta/2-\delta/2)} \cos(\gamma/2) & -\mathrm{e}^{i(\alpha-\beta+\delta/2)} \sin(\gamma/2) \\ \mathrm{e}^{i(\alpha+\beta/2-\delta/2)} \sin(\gamma/2) & \mathrm{e}^{i(\alpha+\beta/2+\delta/2)} \cos(\gamma/2) \end{pmatrix}.$$

From the definitions of R_y, R_z, it immediately follows that $U = \mathrm{e}^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$. □

We can prove a similar theorem with R_x, R_y instead of using R_y, R_z.

Excercise 3.4 Show the X–Y decomposition of by replacing R_z to R_x.

Since the global phase $\mathrm{e}^{i\alpha}$ can be ignored, we can construct an arbitrary quantum circuit acting on 1 qubit by combining the gates that implement the rotations R_y and R_z.

How can we construct a quantum circuit that implements a unitary matrix on a longer sequence of qubits? It is in fact known that we can implement any quantum circuit from 1-qubit quantum gates and the CNOT gate.

Theorem 3.5 *For any* $n \in \mathbb{N}$*, we can construct any quantum circuit that acts on* n*-qubit sequence by using quantum gates on* 1 *qubit and the* CNOT *gate. The total number of the gates used in the circuit is at most* $O(n^2 2^{2n})$ [7, 8].

Therefore, we can implement any unitary matrix only with the rotation gates and the CNOT gate. We call a set of quantum gates, like these rotations and CNOT, **universal gates**. The universality of sets of quantum gates has been deeply investigated further.

As studied above, a quantum circuit implements a huge unitary matrix and measurement in the computational basis. Since unitary matrices must be reversible and measurements are just an operation that probabilistically extracts classical bits from quantum states, quantum circuits seem to be more restricted than classical ones in some sense. Can quantum circuits compute any Boolean function $f : \{0,1\}^n \to \{0,1\}$ that classical ones can compute?

In fact, due to studies in reversible computation, they can compute any Boolean function $f : \{0,1\}^n \to \{0,1\}$ using the Toffoli (controlled-controlled NOT) gates CCNOT if they are given fixed inputs of 0, 1 and auxiliary qubits that store a history of computation. This is because we can simulate each of $\neg, \wedge, \vee$ gates by feeding appropriate fixed inputs to CCNOT. (Recall that we can compute any Boolean function f only by combining $\neg, \wedge, \vee$ gates.)

Now, let us see how to simulate them briefly. Note that CCNOT implements a map $\mathrm{CCNOT}(x_1, x_2, x_3) = (x_1, x_2, (x_1 \wedge x_2) \oplus x_3)$ for inputs $x_1, x_2, x_3 \in \{0,1\}$. For example, setting 1 to the two control bits x_1 and x_2, we have $\mathrm{CCNOT}(1, 1, x_3) = (1, 1, \neg x_3)$. Hence, we can perform the operation of the $\neg$ gate on the third input/output. Also, setting 0 to the third bit x_3, we have $\mathrm{CCNOT}(x_1, x_2, 0) = (x_1, x_2, x_1 \wedge x_2)$. Then, we can perform the operation of the $\wedge$ gate on the first and second inputs and the third output. Since we have $x_1 \vee x_2 = \neg((\neg x_1) \wedge (\neg x_2))$ by de Morgan's law, we can also simulate the operation of the $\vee$ gate using the simulations of the $\wedge$ and $\neg$ gates. We obtain the following theorem by this simulation technique.

Theorem 3.6 *Let $f : \{0,1\}^n \to \{0,1\}$ be any Boolean function that a circuit of size $s(n)$ can compute. Then, there exists a quantum circuit U_f such that U_f is constructed only from the* CCNOT *gates and it satisfies*

$$U_f |x\rangle|0\rangle|011\rangle|0^{\ell(n)}\rangle = |x\rangle|f(x)\rangle|011\rangle|G(x)\rangle, \tag{3.12}$$

where $0^{\ell(n)}$ denotes an all-zero sequence of length $\ell(n)$, and $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$, $\ell(n) = O(s(n) + n)$.

Remark 3.4 $G(x)$ is a sequence of $\ell(n)$ bits, which is called a garbage information. The fixed input bits 011 is utilized for the simulations of $\neg, \wedge, \vee$ gates.

Therefore, since we can obtain the value $f(x)$ we should compute by using U_f, even quantum circuits can compute any Boolean function in this sense.

We often compute a Boolean function in the execution process of quantum algorithms. If we apply the technique of Theorem 3.6, we need to store the gabage information for the reversibility of computation. There is no point in occupying quantum memory with the garbage information that is not necessary as a result of the computation, and furthermore, it prevents some effects of quantum computation, as we will demonstrated later. So, we initialize the garbage information without violating the reversibility by a simple technique shown in the following corollary.

Corollary 3.1 Let U_f be a quantum circuit satisfying (3.12) in Theorem 3.6. Then, there exists a quantum circuit U'_f using two gates of U_f and one CNOT such that for any $x \in \{0,1\}^n$

$$U'_f|x\rangle|0\rangle|0\rangle|011\rangle|0^{\ell(n)}\rangle = |x\rangle|f(x)\rangle|0\rangle|011\rangle|0^{\ell(n)}\rangle \tag{3.13}$$

Proof We construct the circuit U'_f as follows. First, we apply U_f to an input $|x\rangle|0\rangle|0\rangle|011\rangle|0^{\ell(n)}\rangle$ of five sequences except for the second sequence. We then have $|x\rangle|0\rangle|f(x)\rangle|011\rangle|G(x)\rangle$. Next, applying CNOT to the second and third sequences by taking the third as the controller, we have $|x\rangle|f(x)\rangle|f(x)\rangle|011\rangle|G(x)\rangle$. Finally, we apply a quantum circuit U_f^{-1}, which reverses input and output in U_f, except for the second sequence. Then, we can obtain $|x\rangle|f(x)\rangle|0\rangle|011\rangle|0^{\ell(n)}\rangle$. □

As (3.13) shows, the auxiliary sequence does not change the value in input and output. This fact is significant especially in quantum computing. For example, let us consider a situation that we compute a Boolean function f on input $(|x\rangle|0\rangle+|y\rangle|0\rangle)/\sqrt{2}$. Applying the technique of Theorem 3.6, we obtain $(|x\rangle|f(x)\rangle|011\rangle|G(x)\rangle + |y\rangle|f(y)\rangle|011\rangle|G(y)\rangle)/\sqrt{2}$ by adding auxiliary sequences $|011\rangle|0\cdots0\rangle$. In this case, the garbage information $|G(x)\rangle$, $|G(y)\rangle$ is not separable from the other parts. (We say two qubit sequences are separable if they are not entangled. See Sect. 2.3.3 and Chap. 7.) In contrast, if we choose the technique of Corollary 3.1, we obtain $(|x\rangle|f(x)\rangle|011\rangle|0\cdots0\rangle+|y\rangle|f(y)\rangle|011\rangle|0\cdots0\rangle)/\sqrt{2} = ((|x\rangle|f(x)\rangle+|y\rangle|f(y)\rangle)/\sqrt{2})\otimes|011\rangle|0\cdots0\rangle$. Since the auxiliary sequences are separable from the sequences of input and result in this case, we can ignore the existence of the auxiliary sequences henceforth. Therefore, we can consider that this technique achieves an operation $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ by cutting off the auxiliary sequences.

References

1. M. Agrawal, N. Kayal, N. Saxena, Ann. Math. **160**, 781–793 (2004)
2. T. Tao, J. Aust. Math. Soc. to appear (arXiv:0802.3361)
3. H.W. Lenstra Jr., C. Pomerance, Primality testing with Gaussian periods, preprint (2005)
4. H. Vollmer, *Introduction to Circuit Complexity: A Uniform Approach* (Springer, Berlin, 1999)
5. Clay Mathematics Institute, Millennium Prize Problems: NP versus P Problem, http://www.claymath.org/millennium/P_vs_NP/
6. J. Carlson, A. Jaffe, A. Wiles, *The Millennium Prize Problems* (AMS, Cambridge, 2006)
7. A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, Phys. Rev. A **52**, 3457–3467 (1995)
8. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)

Chapter 4
Quantum Algorithms

4.1 Introduction

Quantum computing has deep potentials to construct much faster algorithms for hard problems than classical ones. In this chapter, we will study several famous quantum algorithms that have significant advantages over classical ones.

We will first study the Deutsch-Jozsa algorithm in Sect. 4.2. This algorithm solves some artificial problem which would not be useful in practice, but it is quite simple to demonstrate the potential of quantum computing. If you learn quantum circuits at Chap. 3 for the first time, this algorithm is highly recommended to understand the power of quantum computing. (We will deal with an improved version given in [1] as the Deutsch-Jozsa algorithm in this section.)

Next in Sect. 4.3, we will study a fast quantum algorithm called Grover's algorithm [2] that searches solutions of problems. More specifically, for a given $f : \{0, 1\}^n \rightarrow \{0, 1\}$, it can find an $x_0 \in \{0, 1\}^n$ satisfying $f(x_0) = 1$ fast. This quantum algorithm is quite versatile since it assumes no structure on the given function f.

Following Grover's algorithm, we will study an overview of Shor's algorithm [3] in Sect. 4.4. Shor's algorithm is able to efficiently solve the factorization and discrete logarithm problems, which are believed to be hard against classical computers. The hardness of these problems provides a security basis of cryptographic protocols used widely in the Internet and others such as the RSA and elliptic curve cryptosystems. This fact implies that we can easily attack cryptographic protocols based on the hardness of these problems if we can build practical quantum computers of the same scale with the classical ones. The discovery of Shor's algorithm was a big breakthrough in the area of quantum computing, and that was one of the main reasons why this area attracted remarkable attention.

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_4,

4.2 Deutsch-Jozsa Algorithm

The **Deutsch-Jozsa algorithm** solves a problem of deciding whether a given function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is constant or balanced only from queries $x \in \{0, 1\}^n$ and their answers $f(x) \in \{0, 1\}$. We say f is a **constant function** if $f(x) = 0$ for all $x \in \{0, 1\}^n$, or $f(x) = 1$ for all $x \in \{0, 1\}^n$ and f is a **balanced function** if $f(x) = 0$ for a half of $x \in \{0, 1\}^n$ and $f(x) = 1$ for the other half of x, namely, $|\{x \in \{0, 1\}^n : f(x) = 0\}| = 2^n/2$.

Decision problem of constant/balanced functions
Input: a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$
Output: 0 if f is constant, and 1 if f is balanced

The function f is given as a black box. Namely, we are given no information on description of f, for example, f can be described as $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$, and we can learn only relationships between inputs and outputs by queries $x = (x_1, x_2, x_3)$ and their answers $f(x)$. Such a function given as a black box is often called an **oracle**. In computation with an oracle, we discuss the sufficient and necessary number of queries to the oracle as a measure of computational resource, which is called **query complexity**.[1] In this section and the next section, we analyze the number of queries to oracles.

In classical computation, how many queries to f do we need to solve this problem correctly? It is easy to see that the deterministic computation, that is, the classical computation which uniquely determines an output value from an input value, requires $2^{n-1}+1$ queries to some f. Even in the randomized computation, that is, the classical computation which determines an output value from an input and random values, requires exponentially many queries to f to solve this problem with probability 1. Nonetheless, the Deutsch-Jozsa algorithm allows us to solve this problem with only 1 query to f and probability 1 using power of the quantum computation.

Remark 4.1 Since the quantum computation extracts classical information from qubits through measurement, we need to analyze probability that a quantum algorithm outputs a correct value. Fortunately, the Deutsch-Jozsa algorithm outputs a correct value with probability 1, but quantum algorithms we will discuss later such as Grover's algorithm and Shor's algorithm have possibility that they provide wrong outputs. However, we can analyze that such a probability is sufficiently small, and further, we can efficiently verify if the outputs are correct or not in the problems treated by these algorithms. So, it is not a serious problem for these algorithms to have a small error probability.

Let us check the details of the Deutsch-Jozsa algorithm. Since we are given f as an oracle, the oracle itself should be instantiated by a quantum circuit in order to make a

[1] The query complexity takes care in the number of queries and it ignores the complexity of the other quantum operations. Therefore, in discussions of query complexity, we are able to perform any phisically implementable operation.

query to the oracle from a quantum circuit. We suppose that the oracle is instantiated by a quantum circuit U_f that acts on n-qubit and 1-qubit sequences as follows:

$$U_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle, \tag{4.1}$$

where $x \in \{0,1\}^n$, $b \in \{0,1\}$ and $\oplus$ is the exclusive OR. (Recall that any Boolean function can be represented by a unitary matrix as shown in Corollary 3.1.)

It is easy to see that this operation is a unitary matrix. We can interpret a single use of U_f as a single call to the oracle f.

We show the Deutsch-Jozsa algorithm below. This algorithm is given an initial qubit sequence $|0^{n+1}\rangle = |0^n\rangle|0\rangle$ as an input and obtains information of U_f by measuring the final qubit sequence, where 0^n is a concatenation of n zeros.

Deutsch-Jozsa Algorithm

(i) Apply the Pauli matrix σ_x to the $(n+1)$th bit.
(ii) Apply the Hadamard transform H to all the $n+1$ bits.
(iii) Apply U_f to all the $n+1$ bits.
(iv) Apply the Hadamard transform H to the first n bits.
(v) Measure the first n bits in the computational basis. If the obtained classical n-bit sequence is $0\cdots0$, output 0, i.e., decide f is constant. Otherwise, output 1, i.e., decide f is balanced.

Obviously, this algorithm uses only one U_f. As mentioned above, this circuit can correctly decide if f is constant or balanced with probability 1. We now analyze this below.

After (i), the initial qubit sequence $|0^n\rangle|0\rangle$ is transformed to $|0^n\rangle|1\rangle$ by the Pauli matrix σ_x. (Recall that σ_x acts as the bit flip. See Sect. 3.4.) In (ii), it is further transformed to the following sequence. Let $N := 2^n$.

$$|0^n\rangle|1\rangle \overset{(ii)}{\longmapsto} \frac{1}{\sqrt{2N}} \sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle).$$

The transformation of the first n-qubit sequence is the same one as Fig. 3.6 in Sect. 3.4. In (iii), applying U_f to the $(n+1)$-qubit sequence, we obtain

$$\begin{aligned}
&\frac{1}{\sqrt{2N}} \sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle) \\
&\quad \overset{(iii)}{\longmapsto} \frac{1}{\sqrt{2N}} \sum_{x\in\{0,1\}^n} |x\rangle(|f(x)\oplus 0\rangle - |f(x)\oplus 1\rangle) \\
&\quad = \frac{1}{\sqrt{2N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle).
\end{aligned} \tag{4.2}$$

Namely, this step does not change the amplitude in basis vectors $|x\rangle$ satisfying $f(x) = 0$ but flip the sign of the amplitude in basis vectors $|x\rangle$ satisfying $f(x) = 1$.

Finally in (iv), what happens by applying $H^{\otimes n}$ to the first n-qubit sequence again? Since the first n-qubit sequence is separable from the last 1 qubit and $H^{\otimes n}(\sum_{x\in\{0,1\}^n}|x\rangle/\sqrt{N}) = \sum_{x\in\{0,1\}^n}(H^{\otimes n}|x\rangle)/\sqrt{N}$ by the linearity of unitary matrices, let us check how $H^{\otimes n}|x\rangle$ changes for each of $|x\rangle$. It is easy to prove the following lemma.

Lemma 4.1 *For every* $x \in \{0,1\}^n$,

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{\langle x,y\rangle}|y\rangle, \tag{4.3}$$

where $\langle x, y\rangle := \sum_{i=1}^n x_i y_i \bmod 2$ *for the* i*-th bits* x_i, y_i *in* x, y.

Exercise 4.1 Prove this lemma. (Hint: $H|x\rangle = (|0\rangle + (-1)^x|1\rangle)/\sqrt{2}$ in the 1-bit case.)

By this lemma, the first n-qubit sequence is

$$\frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \overset{(iv)}{\longmapsto} \frac{1}{N} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)}(-1)^{\langle x,y\rangle}|y\rangle.$$

We measure this state in (v). Then, from the amplitude in $|0^n\rangle$,

$$\Pr\left\{\text{we obtain } 0^n \text{ by the measurement in (v)}\right\} = \left|\frac{1}{N}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right|^2.$$

If f is constant, it is obvious that this probability is 1. Otherwise if f is balanced, since $\sum_{x\in\{0,1\}^n}(-1)^{f(x)} = 0$, this probability is 0, namely, we always obtain 0^n in the measurement of (v) if f is constant, and something other than 0^n if f is balanced.

From the above discussion, we can see that the Deutsch-Jozsa algorithm solves the decision problem of constant/balanced functions with probability 1 by a single use of U_f.

Why can we achieve such a surprising task by quantum computing? In what follows, we will observe the heart of the algorithm. The key is the state given in (4.2) after the step (iii). Since the last 1 qubit is separable from the first n-qubit sequence in this state and independent of f, we focus only on the first n-qubit sequence and define

$$|\phi_f\rangle := \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle.$$

If f is constant, $|\phi_f\rangle = \sum_x |x\rangle/\sqrt{N}$, and if f is balanced, $|\phi_f\rangle$ is the state that that an exact half of basis vectors have different signs from the others. ($|\phi_f\rangle$ and $-|\phi_f\rangle$ are identified). It should be noted that for a constant function f and a balanced function g, the corresponding states $|\phi_f\rangle$ and $|\phi_g\rangle$ are orthogonal:

$$\langle \phi_f | \phi_g \rangle = \frac{1}{N} \sum_{x,y} (-1)^{f(x)+g(y)} \langle x | y \rangle = \frac{1}{N} \sum_{x} (-1)^{f(x)+g(x)} = 0.$$

Since a unitary matrix is an invertible transformation that maps an orthonormal basis to another orthonormal basis, the vectors $(H^{\otimes n})^{-1}|\phi_f\rangle = |0\cdots 0\rangle$ and $(H^{\otimes n})^{-1}|\phi_g\rangle$ are orthogonal again. Therefore, while $(H^{\otimes n})^{-1}|\phi_f\rangle = |0\cdots 0\rangle$, $(H^{\otimes n})^{-1}|\phi_g\rangle$ is in the subspace spanned by basis vectors except for $|0\cdots 0\rangle$, namely, $\langle 0\cdots 0|((H^{\otimes n})^{-1}|\phi_g\rangle) = 0$. Since $H = H^{-1}$, we never obtain $0\cdots 0$ from $H^{\otimes n}|\phi_g\rangle$ by the measurement in (v). As discussed above, we reduce the decision problem of given functions to the discrimination problem of given quantum states, called **quantum state discrimination**. If we interpret the Deutsch-Jozsa algorithm in the context of the quantum state discrimination, we are given one of the two states $\{|\phi_f\rangle, |\phi_g\rangle\}$ (precisely, there are many states as $|\phi_f\rangle$, $|\phi_g\rangle$, but we simplify the discussion), and we can then discriminate them by the measurement used by the Deutsch-Jozsa algorithm. In addition, it is known that we can discriminate candidate quantum states with probability 1 if they are orthogonal. (See Proposition 5.4 in Sect. 5.2.)

In the interpretation of quantum algorithms as quantum state discrimination, the following two points are important:

1. It is possible to construct an efficient quantum circuit that generates (nearly) orthogonal states from given inputs.
2. It is possible to construct an efficient quantum circuit that provides the measurement which discriminates the generated states.

Indeed, there are several quantum algorithms that reduce the target problems to the quantum state discrimination, and thus, the reduction is a useful technique to design quantum algorithms. In fact, the quantum state discrimination plays an essential role in Shor's algorithm, we will study that later in Sect. 4.4.

4.3 Grover's Algorithm

We next study **Grover's algorithm** in this section.

4.3.1 Construction of Grover's Algorithm

Grover's algorithm is applicable to a general search problem, which we call **Grover's search problem**, in which we find a satisfying assignment x_0 (we call a solution simply below) for a given function $f : \{0,1\}^n \to \{0,1\}$, i.e., $f(x_0) = 1$.

Grover's search problem
Input: A function $f : \{0,1\}^n \to \{0,1\}$, where it has a unique solution $x_0 \in \{0,1\}^n$ of $f(x_0) = 1$.
Output: the unique solution $x_0 \in \{0,1\}^n$ satisfying the above equation.

Similarly to the previous section, the function f is given as an oracle, i.e., a black box to be applied, and it answers a value $f(x)$ for a query x. We are able to learn f only through this oracle. We will analyze the number of queries in Grover's algorithm as in the Deutsch-Jozsa algorithm.

Let $N := 2^n$. Then, every deterministic algorithm (i.e., classical algorithm that uses no random numbers) requires $N - 1$ queries to output the solution x_0 of $f(x_0) = 1$ correctly for every f. If a deterministic algorithm A makes at most $N - 2$ queries, thereare two distinct x_0' and x_0'' such that A cannot distinguish the cases that $f(x_0') = 1$ and $f(x_0'') = 1$. Therefore, A must fail on one of these two cases. Also, by the proof technique called Yao's principle [4] used for lower bounds of query complexity, we can prove that every randomized algorithm using random numbers requires $\Omega(N)$ queries to solve this problem with a constant probability (say, 0.8) that is independent of n.

On the other hand, Grover's algorithm can correctly output x_0 with at least probability $1 - 1/N$ (note that this probability approaches to 1 as N grows larger) only by making at most $O(\sqrt{N})$ queries to f. Therefore, it is possible to save the number of queries significantly in Grover's algorithm for this general search problem, compared with classical algorithms.

Now, let us study the details of Grover's algorithm. Since a function f is an oracle, we suppose it is given as a quantum gate $U_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$ as in Equality (4.1) of the previous section.

Before studying the details, we will first observe the intuitions behind Grover's algorithm. Our goal is to construct a quantum circuit that outputs quantum states which provide a solution x_0 with high probability by the measurement from input $|0^n\rangle|0\rangle$.

We consider the following quantum circuit: (1) Apply the Hadamard transform H to the first n bits. (2) Apply U_f to all the $n + 1$ bits. This transformation is described as follows:

$$\begin{aligned}|0^n\rangle|0\rangle &\xmapsto{(1)} \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes n} \otimes |0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle \\ &\xmapsto{(2)} \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle.\end{aligned}$$

Measuring the output, we obtain a pair $(x, f(x))$ randomly. Since the amplitude in $|x\rangle|f(x)\rangle$ is $1/\sqrt{N}$ for every x, the success probability, i.e., the probability that we obtain the pair $(x_0, 1)$, is $1/N$. This is the same as the probability that we luckily obtain the solution by choosing x uniformly at random from $\{0, 1\}^n$, and hence, we have no advantage of quantum computing at this point.

Next, we consider the following quantum circuit. (1) Apply the Pauli matrix σ_x only to $(n + 1)$th qubit. (2) Apply the Hadamard transform to all the $n + 1$ qubits. (3) Apply U_f to whole of the $n + 1$ qubits. (4) Apply the **diffusion matrix**, which is defined as follows, to the first n qubits.

$$D_N := \begin{pmatrix} -1+\frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} & \frac{2}{N} \\ \frac{2}{N} & -1+\frac{2}{N} & \cdots & \frac{2}{N} & \frac{2}{N} \\ \vdots & & \vdots & & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} & -1+\frac{2}{N} \end{pmatrix}. \tag{4.4}$$

It is easy to see that D_N is an $N \times N$ unitary matrix of $[D_N]_{i,i} = -1 + 2/N$ and $[D_N]_{i,j} = 2/N(i \neq j)$. The transformation of the qubit sequence is described as follows:

$$\begin{aligned} |0^n\rangle|0\rangle &\overset{(1)}{\longmapsto} |0^n\rangle|1\rangle \overset{(2)}{\longmapsto} \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\overset{(3)}{\longmapsto} \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{N}} \left(-|x_0\rangle + \sum_{x\neq x_0} |x\rangle \right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &\overset{(4)}{\longmapsto} \left(\frac{3-(4/N)}{\sqrt{N}}|x_0\rangle + \sum_{x\neq x_0} \frac{1-(2/N)}{\sqrt{N}}|x\rangle \right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

Looking at the first n qubits after the step (3), we have $\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle/\sqrt{N}$. Namely, the sign of amplitudes in x that $f(x) = 1$ is flipped to minus. Applying the diffusion matrix to this state and then measuring the result, we obtain x_0 with probability $(3 - (4/N))^2/N$, as seen from the above transformation. This success probability is approximately 9 times higher than that in the first quantum circuit. In both of these quantum circuits, we only used one U_f, i.e., we make a query to f only once. Nonetheless, we can amplify the success probability by adding these magical transformations with the same single query. We will study why these transformations amplify the success probability in the next subsection.

Grover's algorithm iterates the operation which amplifies the success probability. For simplicity, we set the initial qubit sequence to $|0^n\rangle|1\rangle$, and let θ be the value satisfying $\sin\theta = \sqrt{1/N}$.

Grover's algorithm

(i) Apply the Hadamard transform H to the $n + 1$ qubits.
(ii) Iterate the steps (iii) and (iv) $\lfloor \pi/(4\theta) \rfloor$ times.
(iii) Apply U_f to whole of the $n + 1$ qubits.
(iv) Apply the diffusion matrix D_N to the first n qubits.
(v) Output classical n bits obtained by measuring the first n qubits.

Below, we denote the steps (iii) and (iv) by a **Grover iteration**, or simply, an iteration.

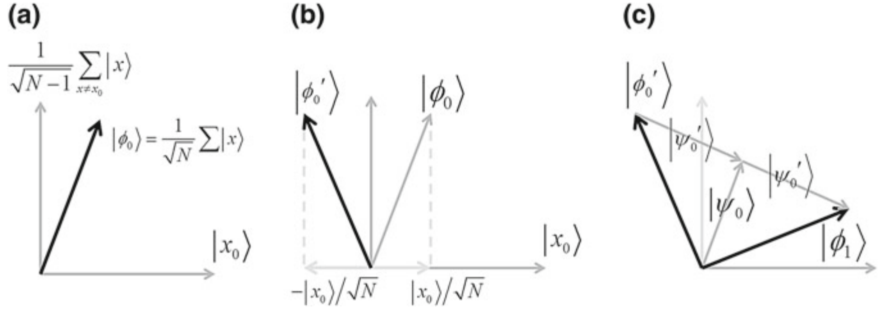


Fig. 4.1 **a** Step (i). **b** Step (iii). **c** Step (iv)

The following theorem shows the performance of Grover's algorithm:

Theorem 4.1 *Grover's algorithm outputs* x_0 *satisfying* $f(x_0) = 1$ *with probability at least* $1 - 1/N$ *by using* U_f $\lfloor(\pi/4)\sqrt{N}\rfloor$ *times.*

The number of U_f the algorithm uses is $\lfloor\pi/(4\theta)\rfloor$ from the construction, and its upper bound is $\lfloor\pi/(4\theta)\rfloor \leq \lfloor(\pi/4)\sqrt{N}\rfloor$ since $\sin\theta \leq \theta$. In the next subsection, we will analyze the success probability.

4.3.2 Analysis of Success Probability

Let us recall that Grover's algorithm amplifies the success probability with several magical operations. Now, we precisely observe what these operations mean. This algorithm runs on two sequences of n qubits and 1 qubit, and since these two sequences are separable in each of Grover iterations, we look only at the first n-qubit sequence.

The basic idea is that the n-qubit sequence used by this algorithm can be represented as a linear combination of bases of "solution" $|x_0\rangle$ and "non-solution" $\sum_{x\neq x_0}|x\rangle$ and the algorithm amplifies the amplitude in the basis $|x_0\rangle$ by the Grover iterations.

We consider the first Grover iteration. By the application of the Hadamard transforms in (ii), the n-qubit sequence is changed to

$$|\phi_0\rangle = H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}|x_0{}^{\perp}\rangle,$$

where $|x_0{}^{\perp}\rangle = \sum_{x\neq x_0}|x\rangle/\sqrt{N-1}$ is a vector of norm 1 in the orthogonal complement of the span$\{|x_0\rangle\}$ (see Fig. 4.1a). As mentioned above, the probability that we obtain x_0 is $1/N$ if we measure the state at this point. In (iii), we apply U_f to whole of the $n+1$ qubits. This corresponds to the operation that flips only the sign of the amplitude in $|x_0\rangle$ on the first n qubits, which is equivalent to the operation $V_f = I - 2|x_0\rangle\langle x_0|$ (see Fig. 4.1b). Namely, we have

$$|\phi_0'\rangle = V_f|\phi_0\rangle = -\frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}|x_0{}^{\perp}\rangle.$$

As Fig. 4.1b illustrates, V_f maps a vector to an axisymmetric one with respect to $|x_0^{\perp}\rangle$. Finally in (iv), we apply the diffusion matrix D_N to the first n qubits. In fact, the matrix D_N is decomposable as follows:

$$D_N = H^{\otimes n}\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -1 \end{pmatrix} H^{\otimes n} = -I + 2H^{\otimes n}|0^n\rangle\langle 0^n|H^{\otimes n} = -I + 2|\phi_0\rangle\langle\phi_0|.$$

(Note that the Hadamard transform H is unitary and Hermite $H = H^{\dagger}$ and hence the inverse of H is H itself.)

Exercise 4.2 Prove that we can decompose D_N as $D_N = -I + 2|\phi_0\rangle\langle\phi_0|$.

Denote by $|\phi_1\rangle$ the resultant state when we apply D_N to $|\phi_0'\rangle$. Then, we have

$$|\phi_1\rangle = D_N|\phi_0'\rangle = (-I + 2|\phi_0\rangle\langle\phi_0|)|\phi_0'\rangle = -|\phi_0'\rangle + 2\langle\phi_0|\phi_0'\rangle|\phi_0\rangle.$$

As Fig. 4.1c illustrates, $|\phi_1\rangle$ is actually the axisymmetric vector of $|\phi_0'\rangle$ with respect to $|\phi_0\rangle$. Since the vector $|\psi_0\rangle$ in Fig. 4.1c is a projection of $|\phi_0'\rangle$ onto the one-dimensional space spanned by $|\phi_0\rangle$, we have $|\psi_0\rangle = |\phi_0\rangle\langle\phi_0| \cdot |\phi_0'\rangle$, and since $|\psi_0'\rangle = -|\phi_0'\rangle + |\phi_0\rangle\langle\phi_0| \cdot |\phi_0'\rangle$, we have $|\phi_1\rangle = |\phi_0'\rangle + 2|\psi_0'\rangle = -|\phi_0'\rangle + 2\langle\phi_0|\phi_0'\rangle|\phi_0\rangle$. It easily follows from the above discusssion that $D_N = -I + 2|\phi_0\rangle\langle\phi_0|$ is the transformation that maps a vector to the axisymmetric one with respect to $|\phi_0\rangle$.

Therefore, V_f maps a vector to the axisymmetric one with respect to $|x_0^{\perp}\rangle$ and then D_N maps a vector to the axisymmetric one with respect to $|\phi_0\rangle$ in the iterations of Grover's algorithm. By these operations, the qubit sequence originally close to $|x_0^{\perp}\rangle$ gradually approaches to $|x_0\rangle$. Since $\langle\phi_0|x_0^{\perp}\rangle = \sqrt{N-1/N} = \cos\theta$, the angle formed by $|\phi_0\rangle$ and $|x_0^{\perp}\rangle$ is θ. From the geometric intuition we mentioned above, the angle formed by $|\phi_1\rangle$ and $|x_0^{\perp}\rangle$ is 3θ, and each of iterations increases the angle by 2θ.

The change of the state in iterations is given by the following lemma.

Lemma 4.2 *Let $|\phi_k\rangle$ be the first n-qubit sequence after the k-th Grover iteration. Then, we have $|\phi_k\rangle = \alpha_k|x_0\rangle + \beta_k|x_x^{\perp}\rangle$, where $\alpha_k = \sin((2k+1)\theta)$, $\beta_k = \cos((2k+1)\theta)$ and $|\langle\phi_0|x_0^{\perp}\rangle| = \cos\theta$.*

Proof By induction. The case $k = 0$ is immediate since we have $|\phi_0\rangle = (1/\sqrt{N})|x_0\rangle + (\sqrt{N-1/N})|x_0^{\perp}\rangle$ and thus $\alpha_0 = 1/\sqrt{N}$, $\beta_0 = \sqrt{N-1/N}$.

We assume that the statement holds on k. Applying V_f to $|\phi_k\rangle = \alpha_k|x_0\rangle + \beta_k|x_0^{\perp}\rangle$, we obtain $|\phi_k'\rangle = -\alpha_k|x_0\rangle + \beta_k|x_0^{\perp}\rangle$. Then applying $D_N = -I + 2|\phi_0\rangle\langle\phi_0|$, (note $|\phi_0\rangle = \alpha_0|x_0\rangle + \beta_0|x_0^{\perp}\rangle$) we have by the trigonometric identities

$$\begin{aligned}|\phi_{k+1}\rangle &= D_N|\phi_k'\rangle\\ &= \left(\alpha_k(1-2\alpha_0^2) + 2\beta_k\beta_0\alpha_0\right)|x_0\rangle + \left(\beta_k(-1+2\beta_0^2) - 2\alpha_k\beta_0\alpha_0\right)|x_0^{\perp}\rangle\\ &= \sin((2k+1)\theta + 2\theta)|x_0\rangle + \cos((2k+1)\theta + 2\theta)|x_0^{\perp}\rangle.\end{aligned}$$

Therefore, it follows that $\alpha_{k+1} = \sin((2k+3)\theta)$ and $\beta_{k+1} = \cos((2k+3)\theta)$. □

By Lemma 4.2, we immediately obtain the proof of Theorem 4.1, which shows the performance of Grover's algorithm.

Proof of Theorem 4.1 By Lemma 4.2, performing the measurement after the k iterations, we obtain the outcome x_0 with probability $\sin^2((2k+1)\theta) = 1 - \cos^2((2k+1)\theta)$. Setting $k = \lfloor \pi/(4\theta) \rfloor = (\pi/(4\theta)) - \delta$ for some $0 < \delta < 1$, we have $\cos^2((2k+1)\theta) = \cos^2((\pi/2) + (-2\delta+1)\theta) = \sin^2((-2\delta+1)\theta) \leq \sin^2(\theta) \leq 1/N$. Therefore the success probability is $1 - \cos^2((2k+1)\theta) \geq 1 - 1/N$. □

It is obvious from this analysis that the success probability $\sin^2((2k+1)\theta)$ with k iterations becomes smaller if k is too large. Therefore, it is important to set the number k of the iterations appropriately.

4.3.3 Generalization: Multiple Solutions

In the previous subsection, we assumed that the blackbox function $f : \{0,1\}^n \to \{0,1\}$ had a unique solution x_0 satisfying $f(x_0) = 1$. It is more natural that the blackbox function has multiple solutions and the algorithm tries to find one of them. Now, we assume f has t solutions.

If we pick up an element $x \in \{0,1\}^n$ uniformly at random from $N := 2^n$ candidates, x satisfies $f(x) = 1$ with probability t/N. Thus, picking up k elements uniformly at random, none of them satisfies $f(x) = 1$ with probability $(1 - t/N)^k \leq 1 - kt/N + (k(k-1)/2)(t/N)^2$. Setting $k := N/t$, this probability is at least $1/2$ and hence we can obtain one of solutions by N/t queries with a constant probability in classical computation.

In quantum computation, we can still apply Grover's algorithm to the case of multiple solutions. Recall that we set the parameter θ to the integer satisfying $\sin\theta = \sqrt{1/N}$ and $k = \lfloor \pi/(4\theta) \rfloor$ of the Grover iterations in Grover's algorithm for a unique solution.

If there are t solutions, we define another parameter θ_t as the value satisfying $\sin\theta_t = \sqrt{t/N}$, and we set the number of the Grover iterations to $R_t := \lfloor \pi/(4\theta_t) \rfloor = O(\sqrt{N/t})$. Then, Grover's algorithm with R_t iterations can find one of solutions with high probability. Note that the algorithm *knows the number t of solutions*.

More specifically, the following lemma gives the success probability of Grover's algorithm with k iterations in the case of t solutions.

Lemma 4.3 *If there are t solutions x_0 such that $f(x_0) = 1$, Grover's algorithm with k iterations can find one of x_0's with probability $\sin^2((2k+1)\theta_t)$, where θ_t is the value which satisfies $\sin\theta_t = \sqrt{t/N}$.*

Exercise 4.3 Prove Lemma 4.3.

We can immediately obtain the following theorem.

Theorem 4.2 *If there are t solutions x_0 such that $f(x_0) = 1$, Grover's algorithm with $\lfloor \pi/(4\theta_t) \rfloor$ iterations can find one of x_0's by using U_f $\lfloor \pi/(4\theta_t) \rfloor = O(\sqrt{N/t})$ times with probability at least $1 - t/N$.*

As in the case of a unique solution, we can easily see from Lemma 4.3 that the success probability can be small if the number of the Grover iterations is too large. The appropriate number of the Grover iterations is $R_t := \lfloor \pi/(4\theta_t) \rfloor = O(\sqrt{N/t})$, which should be determined by the number t of the solutions.

However, it is a strong assumption that the algorithm knows the number of the solutions in advance. For example, the simple algorithm that just picks up candidates uniformly at random does not need to learn the number of the solutions.

In fact, we can obtain one of the solutions with low query complexity by a simple idea of classical computation even if we do not know the number of the solutions. The trick is to exponentially increase the number of the Grover iterations in Grover's algorithm. Namely, we sequentially run Grover's algorithm with 1 iteration, 2 iterations, 4 iterations, and so on.

At some stage, we can eventually run Grover's algorithm that approximately has an appropriate number R_t of the Grover iterations, and then, it obtains the solution with a constant probability. We need to use U_f more times with this idea. However, since we just need to use U_f $1 + 2 + 4 + \cdots + R_t \approx 2R_t$ times, the total number of the Grover iterations is approximately twice that of Grover's algorithm when the number of the solutions is known.

We describe Grover's algorithm in the case that the number of the solutions is unknown below.

Grover's algorithm (for unknown number of the solutions)

(i) Set $r := 1$ as the initial value.

(ii) Run Grover's algorithm with r iterations. If it obtains a solution, output the solution and halt.

(iii) Double r and go back to (ii).

We can show the following theorem for this algorithm:

Theorem 4.3 *Suppose that a given function f has t solutions. Grover's algorithm for unknown number of the solutions can find one of the solutions by using U_f $2\sqrt{N/t}$ times with probability at least $1/2$.*

Proof Let θ_t be the value satisfying $\sin\theta_t = \sqrt{t/N}$, and let ℓ be the integer satisfying $\pi/(8\theta_t) \leq 2^\ell \leq \pi/(4\theta_t)$. We consider the probability that the algorithm cannot find a solution when $r < 2^\ell$, but it finds a solution when $r = 2^\ell$. By Lemma 4.3, Grover's algorithm with 2^ℓ iterations finds a solution with probability $\sin^2((2\cdot 2^\ell + 1)\theta_t) \geq \sin^2(\pi/4+\theta_t) = 1-\cos^2(\pi/4+\theta_t)$. Since $\cos^2(\pi/4+\theta_t) = (1-2\cos\theta_t\sin\theta_t)/2 \leq 1/2$, the algorithm finds a solution with probability at least $1/2$. Until the algorithm finds a solution at $r = 2^\ell$, it uses U_f at most $1+2+4+\cdots+2^\ell = 2^{\ell+1}-1 < \pi/(2\theta_t) < 2\sqrt{N/t}$ times. □

Exercise 4.4 Design a quantum algorithm with $O(\sqrt{N})$ queries (recall $N := 2^n$) that decides if a given function $f : \{0,1\}^n \to \{0,1\}$ satisfies the following (1) or (2) with high probability.

(1) There exists the unique solution x_0 such that $f(x_0) = 1$.
(2) For every $x \in \{0,1\}^n$, $f(x) = 0$, namely, f is the constant function that always outputs 0.

4.4 Shor's Algorithm

In this section, we first study a quantum algorithm for the problem named period-finding problem to understand the heart of **Shor's algorithm**, and then, we consider how to apply the algorithm to the integer factorization and discrete logarithm problems. We will not move into details of Shor's algorithm in this section. See [3] for the details.

4.4.1 Quantum Algorithm for Period Finding

The central idea of Shor's algorithm stems from the quantum algorithm for the following period-finding problem. For $N \in \mathbb{N}$, define $\mathbb{Z}_N := \{0, \ldots, N-1\}$.

> Period-finding problem
> Input: An oracle f on $\mathbb{Z}_N$, where some $s \in \mathbb{N}$ divides $N \in \mathbb{N}$ and it holds that $f(a) = f(a+s \bmod N) = f(a+2s \bmod N) = f(a+3s \bmod N) = \cdots$.
> Output: The number s hidden in f.

For example, defining $N := 16$ and $f(a) := a \bmod 4$, it is immediately seen that $f(a)$ has the hidden period $s = 4$. The most simple classical algorithm is to just enumerate $f(0), f(1), f(2), \ldots$ sequentially and find s such that $f(0) = f(s)$. However, this algorithm needs to compute f $N/2$ times in the worst case. Our goal is to efficiently find such an s only by computing f polynomially many times in $n := \lceil \log N \rceil$ which is the length of N represented in binary.

The following is an overview of the quantum algorithm for this problem. In this section, algorithms store natural numbers rather than bits into qubit sequences. We then suppose that these natural numbers are represented as binary numbers in the qubit sequences. For example, $(|1\rangle + |3\rangle)/\sqrt{2}$ means $(|01\rangle + |11\rangle)/\sqrt{2}$.

Quantum algorithm for period-finding problem

(i) Generate the following state in the initial qubit sequences:

$$\frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} |a\rangle|0\rangle.$$

(ii) Compute $f(a)$ for an input a in the first qubit sequence and store it into the second sequence:

$$\frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} |a\rangle|f(a)\rangle.$$

(iii) Measure the second sequence. If some value z is measured, then we have

$$\frac{1}{\sqrt{N/s}} \sum_{a: f(a)=z} |a\rangle|z\rangle.$$

(Note that the summation is taken only over the values a so that $f(a) = z$.)

(iv) Apply the **quantum Fourier transform** to the first sequence, and measure the resultant sequence. Then, we can obtain a multiple of N/s by this measurement.

(v) Repeating (i)–(iv) appropriately, recover s from the obtained multiples of N/s.

The step (i) can be done by the same method used in Deutsch-Jozsa and Grover's algorithms with the Hadamard transform. More specifically, the following procedure achieves (i):

(1) Generate $2^{-n/2} \sum_{a \in \{0,1\}^n} |a\rangle|0\rangle$. (Since the bit length of N is n, note that $2^{n-1} \leq N < 2^n$.)

(2) Interpreting a as a binary number, compute a function t defined as $t(a) := 1$ if $a < N$ and $t(a) := 0$ otherwise, and store $t(a)$ into the last qubit.

(3) Measure only the last qubit. If 0 is obtained, go back to (1) since the procedure fails. Otherwise, the whole state is $N^{-1/2} \sum_{a:t(a)=1} |a\rangle|1\rangle = N^{-1/2} \sum_{a=0}^{N-1} |a\rangle|1\rangle$ and thus, the first qubit sequence gives the desired state.

(4) Repeat (1)–(3) n times.

The probability that the procedure fails at (3) is at most $1/2$. Hence, repeating these steps n times, we obtain the desired state with probability at least $1 - 1/2^n$.

The quantum Fourier transform used at (iv) plays important roles not only in Shor's algorithm but also in many other quantum algorithms. For example, it is exploited in a quantum algorithm for phase estimation of unitary transforms [5].[2] For more details, we observe a concrete example below.

[2] The phase estimation is also studied deeply based on the Fourier analysis from viewpoints of quantum statistical estimation [6].

Let us consider a function $f(a) = a \bmod 4$ which we picked up in the above example. The state generated in (i) with this function is $(|0\rangle + |1\rangle + \cdots + |14\rangle + |15\rangle)|0\rangle/\sqrt{16}$, and the state generated in (ii) is

$$\begin{aligned}&\frac{1}{\sqrt{16}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle + |3\rangle|3\rangle + |4\rangle|0\rangle + |5\rangle|1\rangle + |6\rangle|2\rangle + |7\rangle|3\rangle + \cdots\right)\\ &= \frac{1}{\sqrt{16}}\left((|0\rangle + |4\rangle + |8\rangle + |12\rangle)|0\rangle + (|1\rangle + |5\rangle + |9\rangle + |11\rangle)|1\rangle + \cdots\right).\end{aligned}$$

Assume the outcome of the measurement is 1 in (iii). In this case, the resultant state changes to

$$\frac{1}{4}\left(|1\rangle + |5\rangle + |9\rangle + |11\rangle\right)|1\rangle.$$

We now apply the quantum Fourier transform F over $\mathbb{Z}_{16}$ to the first qubit sequence in this state $(|1\rangle + |5\rangle + |9\rangle + |11\rangle)/\sqrt{4}$. In general, the quantum Fourier transform over $\mathbb{Z}_N$ is defined as

$$F|a\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{ak}|k\rangle \tag{4.5}$$

for every $a \in \mathbb{Z}_N$, where $\omega_N := \exp(2\pi i/N)$.

Exercise 4.5 Show that the quantum Fourier transform over $\mathbb{Z}_N$ can be represented as a unitary matrix.

Applying the quantum Fourier transform F over $\mathbb{Z}_{16}$ to the first qubit sequence, we obtain

$$\begin{aligned}F\frac{1}{\sqrt{4}}\left(|1\rangle + |5\rangle + |9\rangle + |13\rangle\right) &= \frac{1}{\sqrt{4}}\sum_{k=0}^{15}\frac{1}{\sqrt{16}}\left(\omega_{16}^{1\cdot k} + \omega_{16}^{5\cdot k} + \omega_{16}^{9\cdot k} + \omega_{16}^{13\cdot k}\right)|k\rangle\\ &= \frac{1}{\sqrt{4}}\sum_{k=0}^{15}\frac{1}{\sqrt{16}}\omega_{16}^{k}\sum_{\ell=0}^{3}\omega_4^{\ell k}|k\rangle.\end{aligned}$$

We then note the value of $S_4(k) := \sum_{\ell=0}^{3}\omega_4^{\ell k}$. For example, setting $k = 0$, we have $S_4(0) = 4$, and setting $k = 1$, we have $S_4(1) = \omega_4^0 + \omega_4^1 + \omega_4^2 + \omega_4^3 = 0$.

Exercise 4.6 For every $N, k \in \mathbb{N}$, let $S_N(k) := \sum_{\ell=0}^{N-1}\omega_N^{\ell k}$. Show that $S_N(k) = N$ if k is a multiple of N and $S_N(k) = 0$ otherwise. (Hint: Calculate $(\omega_N^k - 1)(\omega_N^{k(N-1)} + \omega_N^{k(N-2)} + \cdots + \omega_N^k + \omega_N^0)$).

Immediately from this exercise, we have $S_4(k) = 4$ when $k = 0, 4, 8, 12$ and $S_4(k) = 0$ for the other ks. Therefore, the state obtained by the quantum Fourier transform is

$$F\left(\frac{1}{\sqrt{4}}(|1\rangle+|5\rangle+|9\rangle+|13\rangle)\right)=\frac{1}{\sqrt{4}}\sum_{k=0}^{15}\frac{1}{\sqrt{16}}\omega_{16}^{k}\sum_{\ell=0}^{3}\omega_4^{\ell k}|k\rangle$$
$$=\frac{1}{2}\left(\omega_{16}^{0}|0\rangle+\omega_{16}^{4}|4\rangle+\omega_{16}^{8}|8\rangle+\omega_{16}^{12}|12\rangle\right).$$

Measuring this state, we obtain one of 0, 4, 8 and 12 with probability $1/4$ respectively (independently of the phase $\omega_{16}^0, \omega_{16}^4, \ldots$ of the amplitudes).

More generally, when we obtain the outcome $f(a)$ at (iii) via the measurement in the second qubit sequence, the resultant state is $(|a\rangle+|a+4\rangle+|a+8\rangle+|a+12\rangle)|f(a)\rangle/\sqrt{4}$. Then, applying the quantum Fourier transform to the first qubit sequence, we obtain the state

$$F\left(\frac{1}{\sqrt{4}}(|a\rangle+|a+4\rangle+|a+8\rangle+|a+12\rangle)\right)$$
$$=\frac{1}{2}\left(\omega_{16}^{a}|0\rangle+\omega_{16}^{4a}|4\rangle+\omega_{16}^{8a}|8\rangle+\omega_{16}^{12a}|12\rangle\right),$$

independently of the outcome at (iii). So, the value obtained at (iv) is one of 0, 4, 8 and 12 with probability $1/4$ respectively. To wrap up, we obtain a multiple of $s=4$ by the procedure from (i) to (iv). As done in (v), we can find $s=4$ from non-zero multiples by repeating this procedure appropriately.

In the above discussion, we only consider a special case ($N=16$, $f(a)=a \bmod 4$), but the general case is analyzed similarly. Assuming that we obtain $z=f(a_0)=f(a_0+s)=f(a_0+2s)=\cdots$ in the measurement of (ii), we have the following by applying the quantum Fourier transform F over $\mathbb{Z}_N$ to the resultant state at (iii).

$$F\left(\frac{1}{\sqrt{N/s}}\sum_{f(a)=z}|a\rangle\right)=\frac{1}{\sqrt{N/s}}\sum_{f(a)=z}\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{ak}|k\rangle$$
$$=\frac{\sqrt{s}}{N}\sum_{k=0}^{N-1}\left(\omega_N^{a_0k}+\omega_N^{(a_0+s)k}+\cdots+\omega_N^{(a_0+((N/s)-1)s)k}\right)|k\rangle$$
$$=\frac{\sqrt{s}}{N}\sum_{k=0}^{N-1}\omega_N^{a_0k}\sum_{\ell=0}^{(N/s)-1}\omega_{N/s}^{\ell k}|k\rangle$$
$$=\frac{\sqrt{s}}{N}\sum_{k=0}^{N-1}\omega_N^{a_0k}S_{N/s}(k)|k\rangle=\frac{1}{\sqrt{s}}\sum_{j=0}^{s-1}\omega_N^{a_0j(N/s)}|j(N/s)\rangle.$$

In the last equality, we used the fact that $S_{N/s}(k)=N/s$ if k is a multiple of N/s and $S_{N/s}(k)=0$ otherwise. Measuring the qubit sequence obtained by the quantum Fourier transform, multiples of (N/s), i.e., $0, (N/s), 2(N/s), \ldots, (s-1)(N/s)$, outcome at (iv) with probability $1/s$, respectively.

Now suppose that $m_1 = k_1 N/s$ and $m_2 = k_2 N/s$ outcome from two samples (where $k_1, k_2 \in \{0, \ldots, s-1\}$). The values m_1, m_2 and N are known but s and k_1, k_2 are unknown. If k_1 is a coprime to k_2, the greatest common divisor of m_1 and m_2 is N/s, and hence, we can then obtain s from m_1, m_2 and N by using the Euclidean algorithm.

The probability that k_1 is not coprime to k_2 is bounded by

$$\begin{aligned}
&\Pr\{\cup_{p:\text{prime}}\ k_1 \text{ and } k_2 \text{ are multiples of } p\} \\
&\le \sum_{p:\text{prime}} \Pr\{k_1 \text{ and } k_2 \text{ are multiples of } p\} \\
&\le \sum_{p:\text{prime}} \frac{1}{p^2} < \sum_{n \ge 2} \frac{1}{n^2} < 0.65,
\end{aligned}$$

where the last inequality is derived from $\sum_{n\in\mathbb{N}} n^{-2} = \pi^2/6$. From, say, $2n$ samples, we can hence obtain s with probability at least $1 - 0.65^n$.

Although we omit the details of the complexity analysis, if we can implement f by $n^{O(1)}$ gates, i.e., polynomially many gates in n, this quantum algorithm finds the period s with high probability by $n^{O(1)}$ gates.

This quantum algorithm is a sort of the quantum state discrimination similarly to the Deutsch-Jozsa algorithm. Indeed, the (probabilistic mixture of) quantum states in (iii) are determined by the period s, and therefore, it suffices that we can discriminate which period s the quantum states have. In the case of this discrimination, we can implement an efficient discriminator by using the quantum Fourier transform.

4.4.2 Quantum Algorithm for Factorization

Let us construct the quantum algorithm for factorization from the period-finding algorithm. First, we define the **factorization problem**.

Factorization problem
Input: a natural number N of bit length n, where $N = pq$ for two primes p and q.
Output: the two primes p, q.

Since it is trivial if N is even, we consider only the case that N is odd (and thus p, q are odd primes). The natural number N of bit length n is less than 2^n. Therefore, if we look for the primes by brute-force search, we require exponentially high computational complexity in n. There are much faster classical algorithms than brute-force search for the factorization (see, e.g., [7]). However, they still require exponentially high computational complexity, and it is open to construct a polynomial-time algorithm for the factorization.

How can we reduce the factorization to the period-finding problem? We can efficiently solve the factorization problem (even by classical algorithms) if we can find the minimum r which satisfies $x^r \equiv 1 \mod N$ for any integer x coprime to N. The part we need the power of quantum computation is to find the minimum r. The heart of Shor's algorithm is to show how to efficiently solve the problem of finding this r by quantum computation.

We overview the classical part of the reduction. This part mainly requires the number theory and classical algorithms for it. Let $\mathrm{GCD}(a, b)$ denote the greatest common divisor of two integers a, b.

First, we choose x from $\{1, \ldots, N-1\}$ uniformly at random. If x is not coprime to N, i.e., $\mathrm{GCD}(x, N) \neq 1$, $\mathrm{GCD}(x, N)$ divides N. Since this $\mathrm{GCD}(x, N)$ is efficiently computable by the Euclidean algorithm, we can factor N efficiently in this case.

So, suppose that $\mathrm{GCD}(x, N) = 1$. The value of r is determined by the choice of x. If r is even, it holds $(x^{r/2} + 1)(x^{r/2} - 1) \equiv 0 \mod N$. Further, if $x^{r/2} \not\equiv -1 \mod N$, either $\mathrm{GCD}(x^{r/2} + 1, N)$ or $\mathrm{GCD}(x^{r/2} - 1, N)$ is a nontrivial factor of N (i.e., p or q). Then, we can show that r is even and $x^{r/2} \not\equiv -1 \mod N$ with probability at least $1/2$ for a random x. Therefore, our task is reduced to find the r that satisfies $x^r \equiv 1 \mod N$ since we can easily compute $\mathrm{GCD}(x^{r/2} + 1, N)$ and $\mathrm{GCD}(x^{r/2} - 1, N)$ from r and we can verify if they divide N.

To wrap up, the overview of Shor's algorithm for the factorization is as follows.

Shor's algorithm

(i) Choose $x \in \{1, \ldots, N - 1\}$ uniformly at random.
(ii) Compute $\mathrm{GCD}(x, N)$. If it is not 1, output $\mathrm{GCD}(x, N)$ and halt.
(iii) Find the minimum r that satisfies $x^r \equiv 1 \bmod N$. (We discuss this quantum part later.)
(iv) If r is even and $x^{r/2} \not\equiv -1 \mod N$, verify if $\mathrm{GCD}(x^{r/2}+1, N)$ or $\mathrm{GCD}(x^{r/2} - 1, N)$ divide N. If so, output it and halt. Otherwise, go back to (i).

Next, we study the quantum part that computes r. This part is implemented by reducing the problem of finding r to the period-finding problem. Define $f(a) := x^a \bmod N$. In fact, this function has a period s so that $f(a) = f(a + s) = f(a + 2s) = \cdots$. For example, consider that $N = 15 = 3 \cdot 5, x = 2$. Then, we have $f(0) = f(4) = f(8) = \cdots = 1$, $f(1) = f(5) = f(9) = \cdots = 2$, $f(2) = f(6) = f(8) = \cdots = 4$, and $f(3) = f(7) = f(11) = \cdots = 8$. Therefore, we can find the period s using the technique of the period-finding algorithm. Since $f(0) = f(s) = f(2s) = \cdots = 1$, this period s is the value r we want to compute.

The original algorithm of Shor did not use the quantum Fourier transform over $\mathbb{Z}_N$, but it used another one which was efficiently implemented since it was not known how to implement the quantum Fourier transform over $\mathbb{Z}_N$ at the time of the discovery of Shor's algorithm. Later, the efficient implementation was found (e.g., [8]) and thus we can efficiently and directly solve the factorization problem using the quantum transform over $\mathbb{Z}_N$.

Although we supposed the case N consists of two primes in this subsection, this algorithm can be generalized to the case that N consists of more than two primes.

4.4.3 Quantum Algorithm for Discrete Logarithm

Shor also applied the idea of the period finding to the **discrete logarithm problem**. First, we define the discrete logarithm problem as follows. (The original problem is defined in a more general form with terms of finite cyclic groups, but we consider a special case for simplicity).

> Discrete logarithm problem
> Input: a prime p of bit length n, natural numbers g coprime to $p-1$ (that is, $\mathrm{GCD}(p-1, g) = 1$) and y with $0 < y < p$.
> Output: a natural number x such that $y \equiv g^x \bmod p$ and $0 < x < p$.

For example, if the input is $p = 5, y = 2, g = 3$, the output should be $x = 3$ since $3^3 = 27 = 5^2 + 2$.

Since the bit length of p is n, brute-force search for x requires to check $O(2^n)$ candidates in the worst case. There are several classical algorithms much faster than brute-force search for the discrete logarithm problem (see, e.g., [7]), but they still require exponentially high computational complexity. In contrast, Shor's algorithm can solve this problem only using polynomially many gates.

Consider the function $f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ defined as follows.

$$f(a, b) = g^a \cdot (y^{-1})^b \bmod p = g^{a-bx} \bmod p, \tag{4.6}$$

where $\mathbb{Z}_{p-1} := \{0, \ldots, p-1\}$ and $\mathbb{Z}_p^* := \{y \in \mathbb{Z}_p : \mathrm{GCD}(y, p) = 1\}$. In particular, since p is a prime, $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

y^{-1} denotes the element that satisfies $y \cdot y^{-1} \equiv 1 \bmod p$. This function f is efficiently computable from the given p, y, g.

This function f has an interesting property: $(a, b) \in \{(0, 0), (x \bmod p-1, 1 \bmod p-1), (2x \bmod p-1, 2 \bmod p-1), \ldots\}$ if and only if $f(a, b) = 1$. More generally, $(a, b) \in \{(v, w), (x + v, 1 + w), (2x + v, 2 + w), \ldots\}$ if and only if $f(a, b) = g^{v-wx}$. From a viewpoint of finite groups, f takes a constant value on each coset of a subgroup $\langle(x, 1)\rangle$ of an additive group $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$.

In the same example $p = 5, y = 2, g = 3$ as above, since $2 \cdot 3 = 6 \equiv 1$ mod 5 and hence $y^{-1} = 3$, we have $f(a, b) = 3^a 3^b \bmod 5$. Indeed, $f(0, 0) = 1$ and $f(3, 1) = 3^3 3^1 \bmod 5 = 81 \bmod 5 = 1$. The following is the values of $f(a, b)$ in this example.

$$\begin{aligned}
f(0,0) &= f(3,1) = f(2,2) = f(1,3) = 1,\\
f(1,0) &= f(4,1) = f(3,2) = f(2,3) = 3,\\
f(2,0) &= f(1,1) = f(0,2) = f(3,3) = 4,\\
f(3,0) &= f(2,1) = f(1,2) = f(0,3) = 2.
\end{aligned}$$

From these values, f satisfies $f(a, b) = f(a + 3 \bmod 4, b + 1 \bmod 4)$, and it has a hidden period $(x, 1)$.

The original period-finding problem is to find a one-dimensional period, but we can generalize it to a problem of finding a two-dimensional period. For solving this generalized problem, we use the following quantum Fourier transform over $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, defined as follows, rather than over $\mathbb{Z}_N$.

$$F|a\rangle|b\rangle = \frac{1}{\sqrt{(p-1)^2}} \sum_{k,\ell \in \mathbb{Z}_{p-1}} \omega_{p-1}^{ak+b\ell} |k\rangle|\ell\rangle \tag{4.7}$$

Using this quantum Fourier transform, we can construct an efficient quantum algorithm that finds the period $(x, 1)$, which contains the solution we want to find in the discrete logarithm problem.

4.5 Other Quantum Algorithms

We briefly studied only famous quantum algorithms in this chapter. In the recent progress of quantum algorithms, there are novel techniques to design quantum algorithms not included in the algorithms we studied here. For example, the quantum walk is a quantum analogue of the random walk, which is one of important tools for classical algorithms. The quantum walk has remarkably different properties from the classical one, and these properties have been actively used to design new quantum algorithms in recent years [9, 10]. If readers are interested in the recent progress including the technique of the quantum walk, see the survey article [11].

References

1. R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, Proc. R. Soc. Lond. A **454**, 339–354 (1998)
2. L.K. Grover, in Proceedings of the 28th ACM Symposium on Theory of Computing, (ACM Press, Philadelphia, 1996) pp. 212–218.
3. P.W. Shor, SIAM J. Comput. **26**, 1484–1509 (1997)
4. A.C.-C. Yao, in Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science (IEEE Computer Society Press, Los Alamitos, 1977), pp. 222–227.
5. G. Brassard, P. Høyer, M. Mosca, A. Tapp, in Quantum Computation and Information, Contemporary Mathematics, ed. by S.J. Lomonaco, Jr., H.E. Brandt, AMS (2002) pp. 30553–30574.
6. H. Imai, M. Hayashi, New J. Phys. **11**, 043034 (2009)
7. R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd edn. (Springer, New York, 2005)
8. L. Hales, S. Hallgren, in Proceedings of the 41st IEEE Conference on Foundations of Computer Science (2000) pp. 515–525.
9. A. Ambainis, SIAM J. Comput. **37**, 210–239 (2007)
10. A.M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, D.A. Spielman, in Proceedings of the 35th Annual ACM Symposium on Theory of Computing (ACM Press, New York, 2003) pp. 59–68.
11. D. Bacon, W. van Dam, Commun. ACM **53**, 84–93 (2010)

Chapter 5
Foundations of Quantum Mechanics and Quantum Information Theory

5.1 Introduction

In Chap. 2, we have explored the world of quantum mechanics (QM) through the qubit systems. It is not much difficult to generalize the laws for qubits to those for general quantum systems. In this chapter, we give two formulations of general quantum mechanics.[1] The first one is based on *postulates* of QM which directly bridges the gap between qubit systems and general quantum systems (Sect. 5.2). The postulates of QM provide the ground for all the quantum phenomena. However, it is not clever to always go back to postulates from the applicational point of view. In particular, when we focus on a particular quantum system, the presence of an interaction with other physical systems brings a variety of phenomena to the system of interest. At times such an other system acts as an environment which causes an undesirable noise, and at other times as a measurement device which extracts an information of the system of interest. Although these phenomena can be explained based on postulates of QM by referring the other systems, e.g., the environment system, as well as the system of interest, it would be convenient if we have a formulation of QM which preliminarily incorporates them directly without referring other systems. The second formulation of QM given in this chapter is formulated in this line of philosophy. Specifically, the formulation gives the most general descriptions for states (Sect. 5.3.1), measurements (Sect. 5.3.2), time evolutions (Sect. 5.3.3), and measurement-processes (Sect. 5.3.4) in a fixed quantum system under the possible presence of other quantum systems (see e.g. [3–7]). Since the second formulation of QM clarifies the border between realizable and unrealizable phenomena and operations in a fixed quantum system without referring the other systems, the second formulation is often useful as the theoretical ground of quantum information science.

[1] For the mathematical simplicity, we restrict ourselves to the cases where the associated Hilbert spaces are finite-dimensional. However, a formal generalization to the infinite-dimensional cases follows in the parallel manner [1] subject to the careful treatments of topological issues and domains of operators [2].

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_5,

Before proceeding to the formulations, let us give a few remarks about the nomenclatures and notations.

5.1.1 Postulates and Preconditions

Although the two formulations of QM are basically equivalent up to trivial things, some of their mathematical descriptions are quite different. This apparent difference could be an obstacle in communication among researchers with different backgrounds. To avoid it, we carefully explain the physical connections between two formulations. In particular, the second formulation is deduced from the first one based on postulates in detail.

In the following discussion, we distinguish two nomenclatures, *postulates* and *preconditions* as follows. We use *postulates* for the assumptions which characterize quantum mechanics, while we reserve *preconditions* for natural assumptions which hold not only in QM but also in any operationally valid physical theories (including a classical physics). Indeed, in many textbooks, many of *preconditions* are not explicitly specified but implicitly assumed. Although it is not our intention to logically mention all these conditions, in the following we would like to point out some of important preconditions as much as possible.

To see the nature of preconditions, we shall start by some of the examples here. Remind that the fundamental prediction of QM is about the outcome-probability in a measurement as is described in (1). Here, we are implicitly assuming the following:

$$\textit{In each measurement}, \ \textit{we get an outcome}, \tag{5.1}$$

which could be our first *precondition*. Some of the readers might think that Precondition (5.1) is too natural to be explicitly described. However, in QM, this assumption itself is sometimes questioned if we include an observer (of the measurement) as a part of physical system. Precondition (5.1) shows our standpoint of positivism: In this book, we don't treat such a meta-physical problem and we start from our discussion after admitting that we objectively get an outcome in each measurement. In the probabilistic theories like QM, we are also assuming:

$$\begin{aligned} &\textit{The probability to get an outcome is determined} \\ &\qquad\qquad \textit{dependently on the state of the system}. \end{aligned} \tag{5.2}$$

We denote, by $\Pr(M = m \mid s)$, the probability to get an outcome m by a measurement M under a state s.[2] In this book, for the mathematical simplicity, we only consider a measurement with finite numbers of outcomes $m \in \mathcal{M} = \{m_1, \ldots, m_n\}$.[3]

Another example of preconditions lies in the identification of states. To understand the precondition, remind that a state is completely characterized by the physical responses to any possible measurement (see Sect. 2.2.1). This characterization indicates that we can distinguish states s_1 and s_2 if and only if there exists a measurement with which we observe different responses under s_1 and s_2. In probabilistic theories like QM, we assume the following precondition:

$$\begin{aligned}&\textit{We identify states } s_1 \textit{ and } s_2 \textit{ if they predict the same}\\&\textit{probability distributions in all possible measurements.}\end{aligned} \tag{5.3}$$

Notice that this identification should be required even if s_1 and s_2 are prepared by completely different methods. In this case, we sometimes say that s_1 and s_2 are **statistically equivalent**.

Similarly, we assume the following precondition for the identification of measurements:

$$\begin{aligned}&\textit{We identify measurements } M_1 \textit{ and } M_2 \textit{ if}\\&(i) \textit{ they have the same set of measurement-outcomes and}\\&(ii) \textit{ they predict the same probability distributions under all states.}\end{aligned} \tag{5.4}$$

This precondition is also natural from the operational point of view. For instance, using both a ruler and a tape-measure, one can measure the same physical quantity, a position of a particle. Notice, however, an outcome itself is usually not important in the application of information processings being just labeled by proper symbols (such as 0 and 1). In that case, the condition (i) in (5.4) is relaxed to the condition $(i)'$ to have the same number of measurement outcomes (see also the footnote 3).

5.1.2 Hilbert Space and Linear Operators

Until Chap. 4, we have explained qubit systems with a complex Euclidean space $\mathbb{C}^d$ and a $d \times d$ matrix. To deal with QM in general, we need a **Hilbert space** and a **linear operator** on the space. A Hilbert space is a vector space equipped

[2] The symbol "|" with "s" implies that the probability is considered as the conditional probability conditioned that the state is s. (see the footnote 18 for the conditional probability). Precisely speaking, we are identifying the random variable and the measurement and use the same symbol M.

[3] Using a measure theoretical languages, one can formulate the general measurement theory in a parallel manner including continuous outcomes (see e.g. [8]).

with an inner product, i.e., an inner product space, with the completeness condition (Appendix A.2.2). As we will explain from the next subsection, many notions of QM such as physical quantities will be represented by linear maps on a Hilbert space $\mathcal{H}$. In QM, we call them linear operators on $\mathcal{H}$ instead of "maps". Following this convention, a linear map on the set $\mathcal{L}(\mathcal{H})$ of linear operators on $\mathcal{H}$ is sometimes called a **super-operator**. However, in this book, we just call it a linear map following the convention of the field of quantum information science.

Throughout this book, we restrict ourselves to quantum systems associated with Hilbert spaces of finite dimension. This is because we think primarily of the applications to the quantum information science, and in that case, it is usually enough to treat finite-dimensional spaces. It is well known that the completeness condition of a Hilbert space of finite dimension is automatically satisfied. Therefore, the reader may think a Hilbert space just as an inner product space in the following. Moreover, any finite-dimensional Hilbert space $\mathcal{H}$ is represented by $\mathbb{C}^d$ (Proposition A.2) such that the inner product is given by (2.5). On this representation, any linear operator on $\mathcal{H}$ is also represented by a $d \times d$ complex matrix (Appendix A.3.1). Therefore, the reader who is unfamiliar with the abstract treatment of vector spaces may always consider a Hilbert space and a linear operator just as $\mathbb{C}^d$ and a $d \times d$ complex matrix, respectively. However, noting that these representations depend on a particular basis, it is necessary to understand mathematical ingredients independent from the basis for the deep comprehension of the theoretical structure of QM and its applications to quantum information processings. Therefore, we recommend the reader to read the Appendix A whenever he/she finds the unfamiliar mathematics below.

5.1.3 Dirac Notation II

In this subsection, we explain again the for a general Hilbert space $\mathcal{H}$. While the notation has been already explained in Sect. 2.2.2 for $\mathbb{C}^d$ based on [**A**]–[**D**], we formulate it slightly in a different manner by [**A**′], [**C**′] and [**D**′]. In this subsection, a, b (including $a_1, a_2 \cdots$) are complex numbers and A is a linear operator on $\mathcal{H}$.

[A′] $|\psi\rangle$ denotes a Vector

In Dirac notation, we denote an element (a vector) of $\mathcal{H}$ with symbols $|$ and $\rangle$, the same as in [**A**] in Sect. 2.2.2. Note that an addition of vectors and a scalar multiplication, say $|\psi\rangle + |\phi\rangle$ and $a|\psi\rangle$, are sometimes abbreviated simply to $|\psi + \phi\rangle$ and $|a\psi\rangle$. Similarly, the action of a linear operator A to a vector $|\psi\rangle$ is denoted by $A|\psi\rangle$, or abbreviated to $|A\psi\rangle$. For instance, the linearity of A can be expressed not only by $A(a|\psi\rangle + b|\phi\rangle) = aA|\psi\rangle + bA|\phi\rangle$, but also by $A|a\psi + b\phi\rangle = a|A\psi\rangle + b|A\phi\rangle$. A vector of $\mathcal{H}$ with this notation is sometimes called a **ket** vector.

[C′] $\langle\psi|\phi\rangle$ denotes the Inner Product

In Dirac notation, the inner product between vectors $|\psi\rangle$ and $|\phi\rangle$ in $\mathcal{H}$ is denoted by $\langle\psi|\phi\rangle$ (see Appendix A.2.2 for the definition and general properties of the inner product). Following the convention in quantum physics, let the linearity of the inner product hold in the right element: $\langle\psi|a\phi_1 + b\phi_2\rangle = a\langle\psi|\phi_1\rangle + b\langle\psi|\phi_2\rangle$. By the symmetry $\overline{\langle\psi|\phi\rangle} = \langle\phi|\psi\rangle$, the anti-linearity holds in the left element: $\langle a\phi_1 + b\phi_2|\psi\rangle = \overline{a}\langle\phi_1|\psi\rangle + \overline{b}\langle\phi_2|\psi\rangle$. The norm of a vector $|\psi\rangle$ is defined by $\sqrt{\langle\psi|\psi\rangle}$, which will be simply denoted by $||\psi||$. We sometimes abbreviate the inner product between vectors $|\psi\rangle$ and $A|\phi\rangle$ as $\langle\psi|A\phi\rangle$. For instance, the adjoint operator $A^\dagger$ of A satisfies $\langle\psi|A\phi\rangle = \langle A^\dagger\psi|\phi\rangle$.

[D′] $|\psi\rangle\langle\phi|$ denotes a Linear Operator

With two vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}$, the symbol $|\phi\rangle\langle\psi|$ is the linear operator on $\mathcal{H}$ whose action to vectors is defined by

$$|\xi\rangle \in \mathcal{H} \to |\phi\rangle\langle\psi|\ |\xi\rangle := \langle\psi|\xi\rangle|\phi\rangle \in \mathcal{H}\,. \tag{5.5}$$

One can memorize this action formally by recombining $\langle\psi|$ and $|\xi\rangle$ to make it an inner product $\langle\psi|\xi\rangle$ based on the notation [**C**′]. The linearity of $|\phi\rangle\langle\psi|$ immediately follows from the linearity of the inner product.

In Sect. 2.2.2, we have introduced $|\phi\rangle\langle\psi|$ by the matrix (2.7). One can easily check that this matrix corresponds to a matrix representation of the linear operator (5.5).[4]

The typical use of (5.5) is for the one-dimensional projection operator: With a unit vector $|\psi\rangle \in \mathcal{H}$, the linear operator $|\psi\rangle\langle\psi|$ is the projection operator onto the subspace spanned by the vector $|\psi\rangle$. More generally, the projection operator P_W onto the subspace W of $\mathcal{H}$ can be written by $P_W = \sum_{i=1}^n |\psi_i\rangle\langle\psi_i|$ with an ONB $\{|\psi_i\rangle\}_{i=1}^n$ of W. (see Appendix A.3.5.)

Exercise 5.1 For vectors $|\psi\rangle, |\psi'\rangle, |\phi\rangle, |\phi'\rangle \in \mathcal{H}$, show the following formulae:

$$\langle\phi'|(|\phi\rangle\langle\psi|)\psi'\rangle = \langle\phi'|\phi\rangle\langle\psi|\psi'\rangle, \tag{5.6}$$

$$|\psi\rangle\langle\phi||\psi'\rangle\langle\phi'| = \langle\phi|\psi'\rangle|\psi\rangle\langle\phi'|, \tag{5.7}$$

The above conditions [**A**′], [**C**′], [**D**′] are minimally required characters of the Dirac notation to describe the theory of QM and quantum information theory. However, Dirac notation also provides another notation for a linear functional on $\mathcal{H}$.[5] An

[4] With an ONB $\{|\psi_i\rangle\}_{i=1}^d$ of $\mathcal{H}$, let $(a_1, \ldots, a_d)^T := (\langle\psi_1|\psi\rangle, \ldots, \langle\psi_d|\psi\rangle)$, $(b_1, \ldots, b_d)^T := (\langle\psi_1|\phi\rangle, \ldots, \langle\psi_d|\phi\rangle) \in \mathbb{C}^d$ be representations (A.4) of vectors $|\psi\rangle$ and $|\phi\rangle$. Then, the matrix representation of $A := |\phi\rangle\langle\psi|$ with the same ONB reads $a_{ij} := \langle\psi_i|A\psi_j\rangle = \langle\psi_i|\phi\rangle\langle\psi|\psi_j\rangle = b_i\overline{a_j}$ (see (5.6) in Exercise 5.1).

[5] A linear map from $\mathcal{H}$ to $\mathbb{C}$ (or $\mathbb{R}$) is called a linear functional on $\mathcal{H}$.

introduction of this notation would make calculations easy and formal. However, this is not indispensable to describe the theory below, so it is the reader's option to read the rest of this subsection.

[B′] $\langle\psi|$ denotes a Linear Functional

For each ket vector $|\psi\rangle \in \mathcal{H}$, the symbol $\langle\psi|$ is defined by the linear functional on $\mathcal{H}$ such that

$$\forall|\xi\rangle \in \mathcal{H} \to \langle\psi|\,|\xi\rangle := \langle\psi|\xi\rangle \in \mathbb{C}\,. \tag{5.8}$$

The linearity of this map immediately follows from the linearity of the inner product. In Sect. 2.2.2, we have introduced this notation $\langle\psi|$ by (2.3), the conjugate transpose of the corresponding column vector $|\psi\rangle$. One can easily check that this is a matrix (a row vector) representation of a linear functional (5.8).

The set $\mathcal{H}^*$ of all (bounded) linear functionals on $\mathcal{H}$ is called the **dual space**. It is easy to see that $\mathcal{H}^*$ is a vector space. As a vector in $\mathcal{H}^*$, $\langle\psi|$ is called the **bra** vector corresponding to the ket vector $|\psi\rangle$. It is known that any element of $\mathcal{H}^*$ can be represented as a bra vector (Riesz's representation theorem [2]). Thus, the set of all bras equals $\mathcal{H}^*$.

5.2 Postulates for Quantum Mechanics

In this section, we formulate QM based on postulates and explain the general properties of QM. The postulates we adopt are based on those introduced by Dirac [9] and mathematically formulated by von Neumann [1], with which most physicists would be familiar. Specifically, we explain QM by three Postulates; Postulate 1 for the representations of a quantum state and a physical quantity including the measurement rule, Postulate 2 for the rule of a time evolution, and Postulate 3 for the description of a composite quantum system. Notice, however, that we don't include the so-called projection postulate for measurement processes, since they are operationally explained by combining other postulates and natural preconditions[6] (see Sect. 5.3.4 for the details).

In the following, let $\mathcal{H} \simeq \mathbb{C}^d$ and $\mathcal{L}(\mathcal{H})$ be a finite-dimensional Hilbert space and the set of linear operators on $\mathcal{H}$, respectively. Unless is noted, d is always used for the dimension of $\mathcal{H}$. Hermitian operators are denoted by A, B, C, projection operators by P, Q, and the identity operator by I. The set of eigenvalues of $A \in \mathcal{L}(\mathcal{H})$ is denoted by $\sigma(A)$.

[6] This idea is mainly credited to Ozawa. See [7, 10–12], and references therein for the detail.

5.2.1 Quantum States, and Measurements of Physical Quantities

The first postulate of QM describes the mathematical representations of quantum states, physical quantities (observables), and the probabilistic rule for the measurement.

> [Postulate 1] For any quantum system, there is an associated Hilbert space $\mathcal{H}$ in a way that a state is represented by a unit vector of $\mathcal{H}$. A physical quantity is represented by a Hermitian operator on $\mathcal{H}$ where the measurement outcome is one of the eigenvalues. If we measure a physical quantity $A \in \mathcal{L}(\mathcal{H})$ under a state $|\psi\rangle \in \mathcal{H}$, then the probability to observe an outcome $a \in \sigma(A)$ is given by
>
> $$\Pr(A = a \,||\psi\rangle) = \langle\psi|P_a\psi\rangle. \tag{5.9}$$
>
> Here, P_a is the eigen-projection belonging to the eigenvalue a of A.

For each quantum system, e.g. of an electron, a photon, and a carbon dioxide (in principle even for a macroscopic system such as a tennis ball and a star), we theoretically assume that there is an associated Hilbert space with which all the physics on the system are described. For instance, the Hilbert space for the qubit system was $\mathbb{C}^2$ as seen in Chap. 2. In general, the dimension of a Hilbert space for quantum mechanical system could be (countably) infinite. However, in quantum information science, it is enough to use a finite-dimensional Hilbert space, mainly for encoding a classical information on a finite set to a quantum state. A quantum system where the associated Hilbert space is of finite-dimensional is called a **finite level (quantum) system**. Alternatively, it is called a d-level (quantum) system when the dimension is d.

A quantum state and a physical quantity are represented by a unit vector of $\mathcal{H}$ and a Hermitian operator on $\mathcal{H}$, respectively. The description of a state is the same as in Chap. 2, but a representation of a physical quantity by a Hermitian operator is more general than that by an orthonormal basis (a basis measurement). We will see below that a basis measurement corresponds to a measurement of a non-degenerate physical quantity. Notice that a measurement outcome of a physical quantity $A \in \mathcal{L}(\mathcal{H})$ is always one of the eigenvalues of the operator A. The mathematical fact that an eigenvalue of any Hermitian operator is a real number guarantees that a measurement outcome is also a real number so that it is gauged with respect to a fixed physical unit. The probability law (2.1) in QM is given by (5.9), which is called the **Born rule**. Notice that the mathematical consistency holds for the description of a probability which is positive with the normalization condition (Exercise 5.2):

Exercise 5.2 Show that the right hand side of (5.9) is a probability distribution.

As is noticed in Chap. 2, the correspondence between a unit vector and a quantum state is not one-to-one. If two unit vectors $|\phi\rangle$ and $|\psi\rangle$ are related by $|\psi\rangle = e^{i\theta}|\phi\rangle$ with some **phase** $\theta \in \mathbb{R}$, they are considered to represent the same physical state. This is called the **indefiniteness of phase**. This identification can be naturally explained by Precondition (5.3): By (5.9), it is easy to see that states $|\phi\rangle$ and $|\psi\rangle = e^{i\theta}|\phi\rangle$ predict the same probability distribution for any measurement of physical quantities.[7]

Note that Postulate 1 does not necessarily require that all unit vectors correspond to physical states; conversely it only requires that any physical state corresponds to some unit vector. However, in this book (and usually in the field of quantum information science), we assume the stronger condition that (i) **there exists a physical state corresponding to any unit vector**. In the same way, we assume the stronger condition also for physical quantities: (ii) **There exists a physical quantity corresponding to any Hermitian operator**. In the following, we identify a quantum state and a unit vector, a physical quantity and a Hermitian operator, respectively.

The mathematical representation of physical states by means of vectors implies that the addition of states (as vectors) makes another state. This fact is called the **superposition principle** and the resultant state is called the **superposition state**. One might wonder how to interpret the superposition state of $|\psi\rangle$ and $|\phi\rangle$, e.g., $\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$, especially the physical relation between the superposition state and the superposed states $|\psi\rangle$, $|\phi\rangle$. In particular, it is quite difficult to imagine the superposition state of classically exclusive states of e.g. "switch ON" and "switch OFF". We should notice here that an **interpretation** of QM is still controversial and there are many explanations, including non-scientific one, also for the interpretation of superposition states.[8] However, from the operational point of view, one does not have to be troubled over this problem since even a superposed state is just a physical state from which one can get an measurement outcome with the probability following the Born rule (5.9). We only notice here that interpreting a superposition state just as a probabilistic mixture of superposed states is a typical misinterpretation. For instance, a state $\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$ cannot be interpreted by a preparation of $|\psi\rangle$ or $|\phi\rangle$ with probability $1/2$. In Sect. 5.3.1, we will see that a probabilistic mixture of states yields the so-called mixed state.

A physical quantity $A \in \mathcal{L}(\mathcal{H})$ is called **degenerate** (or **non-degenerate**) if it has (or do not have) a multiplicity of eigenvalues. If an eigenvalue a of a Hermitian operator has a multiplicity of length l, then the dimension corresponding to the eigenspace E_a is also l. Therefore, we can write the eigen-projection by $P_a = \sum_{i=1}^{l} |\phi_{a,i}\rangle\langle\phi_{a,i}|$ with an orthonormal basis $\{|\phi_{a,i}\rangle\}_{i=1}^{l}$ of E_a. Using this representation, the Born rule (5.9) reads

$$\Pr(A = a||\psi\rangle) = \langle\psi|P_a\psi\rangle = \sum_{i=1}^{l} |\langle\phi_{a,i}|\psi\rangle|^2. \tag{5.10}$$

For a non-degenerate physical quantity A, we have $P_a = |\phi_a\rangle\langle\phi_a|$ where $|\phi_a\rangle$ is the uniquely determined unit eigenvector of A (up to an arbitrary phase) belonging to

[7] By the Born rule (5.9), we have $\Pr(A = a \mid |\psi\rangle) = \langle e^{i\theta}\phi|P_a e^{i\theta}\phi\rangle = e^{-i\theta}e^{i\theta}\langle\phi|P_a\phi\rangle = \Pr(A = a \mid |\phi\rangle)$ for any physical quantity A.

[8] For those who are interested in this problem, we recommend to read [13].

an eigenvalue a. Therefore, we have

$$\Pr(A = a||\psi\rangle) = \langle\psi|(|\phi_a\rangle\langle\phi_a|)\psi\rangle = |\langle\phi_a|\psi\rangle|^2. \tag{5.11}$$

Noting that $\{|\phi_a\rangle\}_{a\in\sigma(A)}$ forms an orthonormal basis of the whole space $\mathcal{H}$ due to the completeness of a Hermitian operator, a measurement of a non-degenerate physical quantity corresponds to a basis measurement explained in Chap. 2 (see (2.18)). Therefore, the formulation of a measurement in this chapter is essentially the same as that in Chap. 2 except for the following points: (i) we will treat a general physical quantity including a degenerate one in this chapter, and (ii) the measurement outcome of a physical quantity is automatically gauged by eigenvalues of a Hermitian operator with a fixed physical unit, while in Chap. 2 we have labeled a measurement outcome by proper symbols, e.g. 0 and 1.

In the following, we denote the spectrum decomposition of a linear operator A by

$$A = \sum_{a\in\sigma(A)} aP_a \tag{5.12}$$

where a is an eigenvalue of A with the eigen-projection P_a and $\sigma(A)$ denotes the set of all eigenvalues of A. We usually abbreviate the summation simply to $\sum_a$. To distinguish the spectrum decomposition and an eigenvalue decomposition (see Appendix A.3.6), an eigenvalue decomposition of A is denoted by

$$A = \sum_{i=1}^{d} a_i|\phi_i\rangle\langle\phi_i| \tag{5.13}$$

where $a_i\,(i = 1, \ldots, d)$ represents the d eigenvalues of A (including the multiplicity) and $|\phi_i\rangle$ represents the eigenvector belonging to the eigenvalue a_i. (See the footnote 9 in Example 5.1 and the footnote 10 in Example 5.2.)

Example 5.1 Consider a qubit system with an associated Hilbert space $\mathbb{C}^2$. Notice that Pauli matrices (2.22) represent physical quantities as they are (not only unitary but also) Hermitian. For instance, σ_x is a non-degenerate observable with two eigenvalues ± 1 with the corresponding eigenvectors $|\phi^x_\pm\rangle := \frac{1}{\sqrt{2}}(1, \pm 1)^T = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ (One should check here an eigenvalue decomposition of σ_x: $\sigma_x = |\phi^x_+\rangle\langle\phi^x_+| + (-1)|\phi^x_-\rangle\langle\phi^x_-|$[9]). The measurement in the former part of Exercise 2.3 in Chap. 2 can be considered as the measurement of σ_x subject to the relabeling of the outcomes to 1 and -1 from 0 and 1, respectively. Similarly, Hermitian operators σ_y and σ_z have eigenvalues ± 1 with the corresponding eigenvectors $|\phi^y_\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)^T$ (an ONB in (2.7)) and $|\phi^z_+\rangle := |0\rangle, |\phi^z_-\rangle := |1\rangle$ (an ONB in (2.10)). Thus, the

[9] Using (2.7), we have $|\phi^x_+\rangle\langle\phi^x_+| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $|\phi^x_-\rangle\langle\phi^x_-| = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$, from which we obtain $|\phi^x_+\rangle\langle\phi^x_+| - |\phi^x_-\rangle\langle\phi^x_-| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$.

measurement in the latter part of Exercise 2.3 can be considered as the measurement of σ_y, and the basis measurement with respect to the computational basis can be considered as the measurement of σ_z.

Exercise 5.3 Check that the eigenvalues and eigenvectors of Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ are given by those in Example 5.1. Show also the relations: $|\langle\phi^x_\pm|\phi^y_\pm\rangle|^2 = |\langle\phi^y_\pm|\phi^z_\pm\rangle|^2 = |\langle\phi^z_\pm|\phi^x_\pm\rangle|^2 = \frac{1}{2}$.

Example 5.2 Consider a 3-level quantum system associated by the Hilbert space $\mathbb{C}^3$. If we perform a measurement of a physical quantity $A = \begin{pmatrix} 5 & 1 & 2 \\ 1 & 5 & -2 \\ 2 & -2 & 2 \end{pmatrix}$ under a state $|\psi\rangle = (1, 0, 0)^T \in \mathbb{C}^3$, we get one of eigenvalues of A, which are $a = 0, 6$, as the measurement outcome. Since the eigen-projections are $P_0 = \frac{1}{6}\begin{pmatrix} 1 & -1 & -2 \\ -1 & 1 & 2 \\ -2 & 2 & 4 \end{pmatrix}$ and $P_6 = \frac{1}{6}A$,[10] the probabilities to get 0 and 6 are given by $\langle\psi|P_0\psi\rangle = \frac{1}{6}$ and $\langle\psi|P_6\psi\rangle = \frac{5}{6}$, respectively.

Because the measurement outcomes of a physical quantity are real numbers, we can calculate the **expectation value** and the **variance** (or the **standard deviation**, which is the square root of the variance) of a physical quantity. Following the probability theory, the expectation value of a physical quantity A under a state $|\psi\rangle$ is defined by $\mathrm{E}_\psi[A] := \sum_a a\Pr(A = a||\psi\rangle)$. Combining with the Born rule (5.9), we get $\mathrm{E}_\psi[A] = \sum_a a\langle\psi|P_a\psi\rangle = \langle\psi|(\sum_a aP_a)\psi\rangle = \langle\psi|A\psi\rangle$ where we have used the spectral decomposition of $A = \sum_a aP_a$. This gives the formula of expectation value in QM:

$$\mathrm{E}_\psi[A] = \langle\psi|A\psi\rangle. \tag{5.14}$$

Similarly, the variance with the same context is defined by $\mathrm{V}_\psi[A] := \sum_a(a - \mathrm{E}_\psi[A])^2\Pr(A = a||\psi\rangle)$. Using the Born rule (5.9) again, we get the formula of the variance in QM:

$$\mathrm{V}_\psi[A] = \langle\psi|A^2\psi\rangle - \langle\psi|A\psi\rangle^2 = \langle\psi|(A - \mathrm{E}_\psi[A]\,I)^2\psi\rangle. \tag{5.15}$$

Therefore, we can directly use a Hermitian operator A in (5.14) and (5.15) to obtain the expectation value and the variance, while we have to solve the eigenvalue-problem and calculate an eigen-projection of A in order to obtain the probability (5.9).

[10] Notice that the multiplicities of eigenvalues 0 and 6 are 1 and 2, respectively. A unit eigenvector belonging to the eigenvalue 0 is $|\xi_0\rangle = \frac{1}{\sqrt{6}}(1, -1, -2)^T$, and thus one can compute $P_0 = |\xi_0\rangle\langle\xi_0|$ by using (2.7). On the other hand, the eigenvalue 6 has a multiplicity 2, where one can find two orthogonal unit eigenvectors, e.g., $|\xi_6\rangle := \frac{1}{\sqrt{2}}(1, 1, 0)^T$ and $|\xi_6'\rangle := \frac{1}{\sqrt{3}}(1, -1, 1)$. From these eigenvectors, we obtain $P_6 = |\xi_6\rangle\langle\xi_6| + |\xi_6'\rangle\langle\xi_6'| = \frac{1}{6}A$. Observe here the difference between an eigenvalue decomposition $A = 0|\xi_0\rangle\langle\xi_0| + 6|\xi_6\rangle\langle\xi_6| + 6|\xi_6'\rangle\langle\xi_6'| = \sum_{i=1}^3 a_i|\phi_i\rangle\langle\phi_i|$ where $a_1 = 0, a_2 = a_3 = 6$, $|\phi_1\rangle := |\xi_0\rangle, |\phi_2\rangle := |\xi_6\rangle, |\phi_3\rangle := |\xi_6'\rangle$ and the spectral decomposition $A = 0P_0 + 6P_6 = \sum_{a=0,6} aP_a$.

A quantum state which is represented by one of unit eigenvectors of A is called an **eigenstate** of A. An eigenstate is a deterministic state with respect to A in the sense that the probability to obtain the corresponding eigenvalue in a measurement of A is 1. Indeed, if a state $|\psi\rangle$ is an eigenstate corresponding to an eigenvalue a, i.e., $A|\psi\rangle = a|\psi\rangle$ and thus $P_a|\psi\rangle = |\psi\rangle$, then by the Born rule (5.9), the probability to obtain a is $\langle\psi|P_a\psi\rangle = \langle\psi|\psi\rangle = 1$. Conversely, a deterministic state with respect to A is always one of eigenstates of A. To show this, let $|\psi\rangle$ be a deterministic state such that one gets a measurement outcome $a \in \sigma(A)$ with probability 1. By (5.9), we have $1 = \langle\psi|P_a\psi\rangle$. Letting $Q_a := I - P_a$ be the orthogonal projection to P_a,[11] we have $1 = ||\psi||^2 = ||P_a\psi + Q_a\psi||^2 = ||P_a\psi||^2 + ||Q_a\psi||^2$ by Pythagorean theorem (Theorem A.1). On the other hand, we have $1 = \langle\psi|P_a\psi\rangle = \langle\psi|P_a^2\psi\rangle = \langle P_a\psi|P_a\psi\rangle = ||P_a\psi||^2$. Hence, we obtain $||Q_a\psi||^2 = 0$. Therefore, we have $Q_a|\psi\rangle = |\psi\rangle - P_a|\psi\rangle = 0$, which implies that $|\psi\rangle = P_a|\psi\rangle$ is an eigenvector belonging to the eigenvalue a. To summarize, we have obtained the following proposition:

Proposition 5.1 *A deterministic state with respect to a physical quantity A is one of eigenstates of A, and vice versa.*

As one of the peculiar properties of QM, a deterministic state with respect to one physical quantity is not necessarily deterministic with respect to another physical quantity. A simple example can be seen using Pauli matrices. From Proposition 5.1, a deterministic state with respect to σ_x is one of its eigenstates, $|\phi^x_+\rangle$ or $|\phi^x_-\rangle$ (see Example 5.1). However, under either case $|\psi\rangle = |\phi^x_\pm\rangle$, the probability to obtain ± 1 in the measurement of σ_z is $\Pr(\sigma_z = \pm||\psi\rangle) = |\langle\phi^z_\pm|\psi\rangle|^2 = \frac{1}{2}$ by the results in Exercise 5.3. This implies that a deterministic state with respect to σ_x is not deterministic with respect to σ_z. On the contrary, it is the most random state for σ_z in the sense that the probability distribution is the uniform distribution. Similarly, one can show that a deterministic state with respect to σ_z is the most random state for σ_x. The pair of physical quantities is called **complementary** (or **mutually unbiased**) if a deterministic state to one of the physical quantity is the most random state for another physical quantity, and vice versa.[12] σ_x and σ_z are the typical examples of a complementary physical quantities. Moreover, by Exercise 5.3, all the pairs from $\sigma_x, \sigma_y, \sigma_z$ are mutually unbiased.

An **uncertainty relation** provides a quantitative description of the above peculiar features of QM. Though it has several different formulations, let us introduce here the most famous one. Before explain the formulation, notice first that one can naturally represent an uncertainty of a physical quantity by the standard deviation, which is the square of the variance. In particular, a state is deterministic if and only if a standard deviation is zero. The following relation gives the tradeoff between standard deviations of two physical quantities:

Theorem 5.1 (Heisenberg-Robertson uncertainty relation) *For any physical quantities A and B and any quantum state $|\psi\rangle$, we have*

[11] Note that $P_aQ_a = P_a(1 - P_a) = P_a - P_a^2 = 0$. Check also that $Q_a = Q_a^2 = Q_a^\dagger$.

[12] A pair of a position and a momentum is another typical example of the complementary pair of physical quantities, although we need an infinite-dimensional Hilbert space to describe them.

$$\Delta_\psi[A]\Delta_\psi[B] \geq \frac{1}{2}|\langle\psi|[A, B]\psi\rangle|, \tag{5.16}$$

where $\Delta_\psi[A] := \sqrt{\mathrm{V}_\psi[A]}$ *and* $\Delta_\psi[B] := \sqrt{\mathrm{V}_\psi[B]}$ *are standard deviations of A and B under the state $|\psi\rangle$, and $[A, B] := AB - BA$ is the commutator between A and B.*

Proof First, we show the case where expectation values of A and B are both zero: $\mathrm{E}_\psi[A] = \mathrm{E}_\psi[B] = 0$. In this case, we have $\Delta_\psi^2[A] = \langle\psi|A^2\psi\rangle = ||A\psi||^2$ as $A = A^\dagger$. Similarly, we have $\Delta_\psi^2[B] = ||B\psi||^2$. By using the Schwarz inequality (Theorem A.2), we have $|\langle\psi|AB\psi\rangle|^2 = |\langle A\psi|B\psi\rangle|^2 \leq ||A\psi||^2||B\psi||^2$. Therefore,

$$\Delta_\psi^2[A]\Delta_\psi^2[B] \geq |\langle\psi|AB\psi\rangle|^2. \tag{5.17}$$

Observe that $AB = \frac{\{A,B\}}{2} + i\frac{[A,B]}{2i}$ where $\{A, B\} := AB + BA$ be the anticommutator of A and B. Since both $\frac{\{A,B\}}{2}$ and $\frac{[A,B]}{2i}$ are Hermitian,[13] we have $|\langle\psi|AB\psi\rangle|^2 = |\langle\psi|\frac{\{A,B\}}{2}\psi\rangle + i\langle\psi|\frac{[A,B]}{2i}\psi\rangle|^2 = |\langle\psi|\frac{\{A,B\}}{2}\psi\rangle|^2 + |\langle\psi|\frac{[A,B]}{2i}\psi\rangle|^2 \geq \frac{1}{4}|\langle\psi|[A, B]\psi\rangle|^2$. Applying this inequality to (5.17), we obtain the uncertainty relation (5.16).

In the general case where $\mathrm{E}_\psi[A]$ and $\mathrm{E}_\psi[B]$ are not zero, one can follow the above proof just by replacing A and B by $\tilde{A} := A - \mathrm{E}_\psi[A]\,I$ and $\tilde{B} := B - \mathrm{E}_\psi[B]\,I$ which have zero expectation values. By noting $\Delta_\psi^2[A] = \Delta_\psi^2[\tilde{A}]$, $\Delta_\psi^2[B] = \Delta_\psi^2[\tilde{B}]$, and $[\tilde{A}, \tilde{B}] = [A, B]$, one obtains the uncertainty relation (5.16).

The uncertainty relation (5.16) implies that there is a tradeoff between uncertainties (here measured by the standard deviations) of two non-commutative physical quantities A and B ($[A, B] \neq 0$). Indeed, if the right hand side of (5.16) is positive definite, then making the uncertainty of A smaller forces the uncertainty of B larger, and vice versa. Moreover, this relation also indicates the impossibility of the simultaneously measurement of non-commutative physical quantities. This rough intuition is indeed correct in some sense, as we will see later in Sect. 5.3.1. These features are quite peculiar to QM not seen in any classical physics and sometimes called **uncertainty principle**.

Here, we only show the converse, i.e., the simultaneous measurability for commutative physical quantities. To make the statement clear, we start by the exact meaning of the **simultaneous measurability**. In this book, we say that two physical quantities A and B are simultaneously measurable if there exists a measurement which outputs a pair of measurement outcomes (a, b) for A and B such that the joint probability distribution $\Pr(A = a, B = b||\psi\rangle)$ under any state $|\psi\rangle$ correctly predicts the marginal probability distributions[14] of both A and B according to the Born rule:

[13] The second equality follows since $\langle\psi|C\psi\rangle$ is real for any Hermitian operator C (see Proposition A.5).

[14] The **marginal (probability) distribution** gives the local probability distribution of a subset of random variables (physical quantities) without reference to other random variables. For instance, with the joint probability distribution $\Pr(A = a, B = b)$ of A and B, the marginal distribution

$$\sum_b \Pr(A = a, B = b||\psi\rangle) = \langle\psi|P_a\psi\rangle, \sum_a \Pr(A = a, B = b||\psi\rangle) = \langle\psi|Q_b\psi\rangle, \tag{5.18}$$

where P_a and Q_b are eigen-projections of A and B belonging to eigenvalues a and b, respectively. Notice that the simultaneous measurement does not necessarily mean the measurement with a temporal simultaneity.

As the following proposition shows, two commutative physical quantities are simultaneously measurable in the sense described above:

Proposition 5.2 *Commutative physical quantities A and B can be simultaneously measurable such that the joint probability distribution under a state $|\psi\rangle$ is given by*

$$\Pr(A = a, B = b||\psi\rangle) = \langle\psi|P_a Q_b\psi\rangle, \tag{5.19}$$

where P_a and Q_b are eigen-projections of A and B belonging to eigenvalues a and b, respectively.

Before giving the proof, we first see a simple fact about the measurement of a function of a physical quantity, which is implied by Precondition (5.4) (see Appendix A.3.7 for the function of operators):

Proposition 5.3 *For any physical quantity A and any real function f (provided that the range includes $\sigma(A)$), the measurement of $f(A)$ can be performed by the measurement of A by outputting $f(a)$ if the measurement outcome of A is a.*

For example, one can measure $f(A) = A^2$ by measuring A and square the outcome as its output.

Proof Fix an arbitrary state $|\psi\rangle$ and let $A = \sum_a aP_a$ be the spectral decomposition of A. Noting that $f(A) = \sum_a f(a)P_a$, eigenvalues of $f(A)$ are given by $\{b := f(a)\}_{a\in\sigma(A)}$ with the corresponding eigen-projections $Q_b = \sum_{a;\, f(a)=b} P_a$.[15] By the Born rule, we have $\Pr(f(A) = b \mid |\psi\rangle) = \langle\psi|Q_b\psi\rangle = \sum_{a;\, f(a)=b}\langle\psi|P_a\psi\rangle$. However, this is nothing but the probability given by the measurement of A which outputs $b = f(a)$. Since $|\psi\rangle$ is arbitrary, the measurement of $f(A)$ and the latter measurement are identified by Precondition (5.4). □

Based on this fact, we show Proposition 5.2 by constructing a simultaneous measurement satisfying (5.18).

Proof of Proposition 5.2 Since Hermitian operators A and B are commutative, there exist a Hermitian operator C and real functions f and g such that $A = f(C)$

(Footnote 14 continued)
of A is calculated as $\sum_b \Pr(A = a, B = b)$ by the **sum rule** of the probability for mutually exclusive events: If events E_1 and E_2 are mutually exclusive, i.e., if one of the occurrence implies non-occurrence of other events, then the probability $\Pr(E_1 \cup E_2)$ for the sum event $E_1 \cup E_2$ is the sum of the probabilities $\Pr(E_1)$ and $\Pr(E_2)$.

[15] Note that we have to collect up all the eigenvalues a satisfying $b = f(a)$ for the case where f is not injective.

and $B = g(C)$.[16] From Proposition 5.3, the measurements of A and B can be simultaneously performed by measuring C and outputting $f(c)$ and $g(c)$, respectively.

By means of this measurement, the joint probability is given by $\Pr(A = a, B = b||\psi\rangle) = \sum_{c;a=f(c),b=g(c)} \Pr(C = c||\psi\rangle)$. Let $C = \sum_c cR_c$ be the spectral decomposition of C. Noting that $P_a = \sum_{c;a=f(c)} R_c$, $Q_b = \sum_{c;b=g(c)} R_c$ and orthonormal condition $R_c R_{c'} = \delta_{cc'} R_c$, we obtain $\sum_{c;a=f(c),b=g(c)} \Pr(C = c||\psi\rangle) = \sum_{c;a=f(c),b=g(c)} \langle\psi|R_c\psi\rangle = \sum_{c;a=f(c)} \sum_{c';b=g(c')} \langle\psi|R_c R_{c'}\psi\rangle = \langle\psi|P_a Q_b\psi\rangle$. Notice finally that this equation satisfies condition (5.18) by the completeness conditions $\sum_a P_a = \sum_b Q_b = I$. □

We will come back to the general problem on the simultaneous measurability in Sect. 5.3.1. It will be shown that the converse of Proposition 5.2 is also true, i.e., non-commutative physical quantities cannot be simultaneously measured. Moreover, the joint probability of any simultaneous measurement of commutative physical quantities A and B is given by (5.19).

In the field of quantum information, the problem to distinguish (unknown) states is often discussed in several contexts such as quantum cryptography. The following proposition provides the basis for the general problem:

Proposition 5.4 *Unknown orthogonal states* $|\psi_i\rangle$ $(i = 1, \ldots, n)$ *are distinguishable with probability* 1 *in one-time measurement* (*a single-shot measurement*).

Proof Let $\mathcal{H}$ be an associated Hilbert space with dimension d. Since $\{|\psi_j\rangle\}_{j=1}^{n}$ forms an orthonormal system, one can supplement appropriate additional orthonormal system $\{|\psi_j\rangle\}_{j=n+1}^{d}$ to form an orthonormal basis together (see Exercise A.6). Then, a basis measurement of $\{|\psi_j\rangle\}_{j=1}^{d}$, i.e., a measurement of a non-degenerate physical quantity with these eigenvectors, clearly distinguishes states $|\psi_i\rangle$ $(i = 1, \ldots, n)$. Indeed, the probability to get the jth output of this measurement under a state $|\psi_i\rangle$ is $|\langle\psi_j|\psi_i\rangle|^2 = \delta_{ij}$. Therefore, in the situation where the unknown state is one of $|\psi_i\rangle$ $(i = 1, \ldots, n)$, we can correctly judge that the state was $|\psi_j\rangle$ where j is the measurement outcome. □

In Sects. 5.3.1 and 8.2, we will again discuss the general problem on the states-distinguishability.

5.2.2 *Time Evolution*

The second postulate of QM is about the time evolution in quantum systems.

[16] By Proposition A.8, there exists an ONB $\{|\phi_i\rangle\}$ which simultaneously diagonalizes A and B: $A = \sum_{i=1}^{d} a_i |\phi_i\rangle\langle\phi_i|$, $B = \sum_{j=1}^{d} b_j |\phi_j\rangle\langle\phi_j|$. Letting c_i $(i = 1, \ldots, d)$ be all distinct real numbers, define a Hermitian operator C by $C := \sum_i c_i |\phi_i\rangle\langle\phi_i|$. By choosing real functions f and g such that $a_i = f(c_i), b_i = f(c_i)$ $(i = 1, \ldots, d)$, we have $A = f(C)$ and $B = g(C)$.

[Postulate 2] A time evolution in an isolated quantum system is governed by the **Schrödinger equation**:

$$i\hbar \frac{d}{dt}|\psi_t\rangle = H|\psi_t\rangle, \tag{5.20}$$

where $|\psi_t\rangle$ is a quantum state at time $t \in \mathbb{R}$, H is the Hamiltonian, and $\hbar$ is the reduced Planck constant.

A Hermitian operator H in (5.20) is called the **Hamiltonian** (operator) which represents the energy of the quantum system. The reduced **Planck constant** $\hbar \simeq 1.054 \times 10^{-34}$ [Js] is the physical constant which determines the typical scale where quantum mechanical effects appear. However, as it does not play a proactive role in the theoretical structure of QM, we will not explicitly write $\hbar$ by adopting a physical unit such that $\hbar = 1$ in the following.

With the **time evolution operator** $U_t := \exp(-iHt)$, we have the formal solution of Schrödinger equation:

$$|\psi_t\rangle = U_t|\psi_0\rangle. \tag{5.21}$$

One can easily check that (5.21) satisfies (5.20) by differentiating $|\psi_t\rangle := \exp(-iHt)$ $|\psi_0\rangle$ with respect to t and using $\frac{d}{dt}\exp(-iHt) = -iH\exp(-iHt)$. Letting $H = \sum_h hP_h$ be the spectral decomposition of H, we have $U_t = \exp(-iHt) = \sum_h \exp(-iht)P_h$. By this expression, it is easy to show the unitarity conditions $U_tU_t^\dagger = U_t^\dagger U_t = \sum_h P_h = I$. Therefore, the time evolution operator U_t is always a unitary operator.

In quantum information science, we are often interested in the discrete time evolution describing the state change from the initial time to the final time. In that case, it is preferable to deal with the time evolution by the time-evolution map

$$|\psi_0\rangle \mapsto |\psi_t\rangle = U_t|\psi_0\rangle, \tag{5.22}$$

which maps an initial state $|\psi_0\rangle$ to the final state $|\psi_t\rangle$. This is nothing but the **unitary evolution** explained in Chap. 2.

Postulate 2 does not necessarily require that all unitary evolutions correspond to physically realizable time evolutions. However, in this book (and usually in the field of quantum information science), we also assume that for any unitary operator the time evolution (5.22) is physically realizable.

5.2.3 Composite Systems

The final postulate of QM describes the way to composite quantum systems. According to postulate 1, any quantum system is associated with an intrinsic Hilbert space to theoretically describe the physics. Thus, the composite quantum system should also have its own Hilbert space. Postulate 3 describes the way to construct the Hilbert space for the composite system from Hilbert spaces associated with the subsystems.

> [Postulate 3] Let S_{12} be the composite system of quantum systems S_1 and S_2 with Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, the associated Hilbert space of S_{12} is the **tensor product** Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$. A physical quantity of S_1 represented by a Hermitian operator A_1 on $\mathcal{H}_1$ is identified with the physical quantity of S_{12} represented by $A_1 \otimes I_2$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$, where I_2 is the identity operator on $\mathcal{H}_2$. The same identification follows for A_2 of S_2 and $I_1 \otimes A_2$ of S_{12}.

Based on Postulate 3, all the physics on the composite quantum systems are described with Postulates 1 and 2 on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. For instance, a composite state is represented by a unit vector on $\mathcal{H}_1 \otimes \mathcal{H}_2$ and a physical quantity is represented by a Hermitian operator on $\mathcal{H}_1 \otimes \mathcal{H}_2$ with the Born rule. In addition to these representations, it is important to recognize the physical relations between the composite system and subsystems. In particular, a local physical quantity A_1 of $\mathcal{H}_1$ (resp. A_2 of $\mathcal{H}_2$) is identified with physical quantity the $A_1 \otimes I_2$ (resp. $I_1 \otimes A_2$) on $\mathcal{H}_1 \otimes \mathcal{H}_2$. By using this, the composite state

$$|\psi \otimes \phi\rangle := |\psi\rangle \otimes |\phi\rangle \tag{5.23}$$

with states $|\psi\rangle$ and $|\phi\rangle$ of S_1 and S_2 is naturally interpreted as a state where the local states of S_1 and S_2 are $|\psi\rangle$ and $|\phi\rangle$, respectively. To see this, let us consider an arbitrary local measurement of a physical quantity $A_1 = \sum_a a P_a$ of S_1 under the composite state (5.23). As A_1 is represented by $A_1 \otimes I_2$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ with the spectral decomposition $\sum_a a(P_a \otimes I_2)$, the probability to obtain an outcome a is $\Pr(A_1 \otimes I_2 = a \| \psi\rangle \otimes |\phi\rangle) = \langle \psi \otimes \phi | (P_a \otimes I_2) \psi \otimes \phi \rangle$ by the Born rule on the composite system. However, by $\langle \phi | \phi \rangle = 1$, this probability coincides with $\langle \psi | P_a \psi \rangle$, which is the probability distribution of the measurement of A_1 under the state $|\psi\rangle$. As A_1 is arbitrary, the state (5.23) is locally in the state $|\psi\rangle$ of S_1. Similarly, one can show that the state is locally in $|\phi\rangle$ of S_2.

A composite state of the form (5.23) is called a **product state**. In general, however, there exists a composite state which cannot be written in this form (see Example 2.5). A quantum state which cannot be written in the form (5.23) is called an. It turns out that an entangled state has a stronger correlation among subsystems than any correlation appearing in classical physics (see the footnote 31 in Sect. 2.3.3). For this strong correlation, an entangled state plays a crucial role in quantum information processings which go beyond the classical information processings. The general properties and applications of an entangled state will be explained in Chap. 6 in detail.

Notice that local operators A of S_1 and B of S_2 correspond to $A \otimes I_2$ and $I_1 \otimes B$ on the composite system and thus are commutative. Consequently, by Proposition 5.2, we can simultaneously measure A and B such that the joint probability under a state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is given by

$$\Pr(A = a, B = b||\psi\rangle) = \langle\psi|(P_a \otimes I_2)(I_1 \otimes Q_b)\psi\rangle = \langle\psi|P_a \otimes Q_b\psi\rangle, \tag{5.24}$$

where P_a and Q_b are eigen-projections of A and B. We naturally assume the following precondition:

$$\begin{aligned}&\textit{In composite system of } S_1 \textit{ and } S_2, \textit{ a simultaneous measurement}\\ &\textit{of } A \textit{ of } S_1 \textit{ and } B \textit{ of } S_2 \textit{ can be performed by locally measuring them.}\\ &\textit{The time ordering of the local measurements does not affect}\\ &\textit{the joint probability distribution.}\end{aligned} \tag{5.25}$$

5.2.4 *Comment on the Measurement Process: State-Changes due to Measurements*

As we have seen in Sect. 2.3.2, a measurement on a quantum system generally causes a state-change, and we have called it a **measurement process**. Although in many text books this measurement effect is assumed as one of the Postulates of QM, we do not include any kind of postulates for a measurement process. Indeed, the post-measurement states are naturally explained from Postulates 1–3 combined with some natural preconditions (see the footnote 6). As the rule of the measurement process will be derived from other Postulates in Sect. 5.3.4, we rather discuss here a plausible interpretation which attributes this measurement effect to the acquisition of information, and show that it is difficult to adopt such idea.

A typical measurement process is the projective measurement: If we measure a non-degenerate physical quantity A under a state $|\psi\rangle$ and get an outcome a, then the post-measurement state becomes the eigenstate $|\phi_a\rangle$ belonging to the eigenvalue a:

$$|\psi\rangle \overset{\text{got } a}{\longmapsto} |\phi_a\rangle. \tag{5.26}$$

The measurement of a non-degenerate physical quantity accompanied by the measurement process (5.26) is called the **von Neumann's projective measurement**. The natural generalization to include a degenerate physical quantity is given by the so-called **Lüders' rule**:

$$|\psi\rangle \overset{\text{got } a}{\longmapsto} P_a|\psi\rangle/||P_a|\psi\rangle||, \tag{5.27}$$

where P_a is the eigen-projection belonging to the eigenvalue a.

What is the cause for the state-change of the measurement? A seemingly appealing idea to interpret the cause is to attribute the state-change to the acquisition of information. Indeed, such a state-change happens even in the classical probability theory. For instance, suppose that we have a dice (of the form of a regular hexahedron) inside a closed black box. Before opening the box, we may describe the state of the dice by the probability distribution $\mathbf{p} = (1/6, 1/6, 1/6, 1/6, 1/6, 1/6)$ for each spots 1–6 of the dice. However, after opening the box and observing that the dice has a spot 1, we redescribe the state of the dice by the probability distribution $\boldsymbol{p}'_1 = (1, 0, 0, 0, 0, 0)$, since we have confirmed that the spot 1 is certainly pointing upward. This "measurement process" of the dice can be formalized by

$$\boldsymbol{p} \overset{\text{got spot } i}{\longmapsto} \boldsymbol{p}'_i,$$

where $\boldsymbol{p}'_i$ is the probability distribution with probability 1 for ith spot. This fact indicates the idea that a state-change in probabilistic theories is naturally explained by the acquisition of information, provided that the state is dependent on the knowledge of observers. One might be interested in interpreting measurement processes of QM in the same way.

To proceed this idea in QM, consider a measurement of a physical quantity A in a quantum system. In the same manner as in the discussion of a dice, the post-measurement state after observing a measurement outcome a should be a state such that a physical quantity "have" the value a with certainty. From the operational point of view, it is a state which predicts the outcome a with probability 1 if the same measurement of A is performed. This is nothing but a deterministic state discussed in Sect. 5.2.1, which is an eigenstate of A belonging to the eigenvalue a by Proposition 5.1. Consequently, the post-measurement state is an eigenstate of A, which is consistent with the projective measurement.

So far the same as in the state change of dices. However, we have to recognize that it becomes quite weird if we also consider measurements of other physical quantities as well. To understand this, remind that a deterministic state for one physical quantity is not necessarily deterministic for another physical quantity (see Sect. 5.2.1). There even exist complementary physical quantities A and B, each of deterministic state is most random state to each other. Therefore, a measurement of A with which the state changes to the deterministic state of A causes an inevitable disturbance for another physical quantity B. What is peculiar to QM, not seen in classical physics, lies in this point. This property makes it difficult to attribute the cause of state-change in quantum systems just to the acquisition of information.

Notice, however, that in the above discussion, we have implicitly assumed the following:

If we measure a physical quantity A and get an outcome a,
and if we measure the same A immediately after the first measurement,
we will get the same outcome a with probability 1. (5.28)

This assumption is sometimes called the **repeatability hypothesis**, which is often assumed for granted in physics community (see e.g. [9]). It should be emphasized here that there exists measurement processes which do not satisfy the repeatability hypothesis but still physically realizable (see Sect. 5.3.4).

Important thing here is that such a hypothesis can determine the characteristic of the measurement processes from the operational point of view. For instance, by assuming the repeatability hypothesis for the measurement of a non-degenerate physical quantity, the post-measurement state is uniquely determined to the eigenstate by Proposition 5.1. Namely, von Neumann's projective measurement is operationally derived from the repeatability hypothesis.

5.3 Reformulation of Quantum Mechanics

In this section, we introduce the second formulation of QM explained in the beginning of this chapter. Through the reformulation, we will clarify the most general states (Sect. 5.3.1), measurements (Sect. 5.3.2), time evolutions (Sect. 5.3.3), and measurement-processes (Sect. 5.3.4) in a fixed quantum system under the presence of other quantum systems. These will be summarized as Formulations 1–4 comparing Postulates 1–3.

5.3.1 General Class of Quantum States

According to Postulate 1, a quantum state is represented by a unit vector of the associated Hilbert space with the quantum system. However, this does not mean that a physically realizable state is limited to a state described by a unit vector if we consider possible operations in the preparation of the state. These operations include the probabilistic mixture of states and also the restriction of our interest to a particular physical subsystem. In this subsection, we show that such operations broaden the set of quantum states to the set strictly wider than the set of states described by unit vectors. After clarifying the most general class of quantum states, we introduce the useful mathematical representation of quantum states by means of density operators.

5.3.1.1 Probabilistic Mixture of States

In a stage of a state-preparation, it is operationally legitimate to *probabilistically* prepare a state from some sets of states. We should be able to describe this situation by a particular state with which the statistics of any measurement under the situation can be predicted (Remind the operational definition of a state in Sect. 2.2.1). Such a probabilistic method is called a **probabilistic mixture** of states. The resultant state generally cannot be described by any unit vector of the associated Hilbert space. Namely, the probabilistic mixture of states broadens the set of possible quantum states based on Postulate 1. To see this, let us begin with some example in a qubit system.

To realize a simple probabilistic mixture of states, we shall use a fair coin with probability 1/2 for both tail and head.[17] By tossing the coin, if we get a tail then we prepare the state $|0\rangle = (1, 0)^T$, while if we get a head then we prepare the state $|1\rangle = (0, 1)^T$. Let us denote the state by s. Notice here, (and also in the following when discussing the probabilistic mixture of states), we assume an observer who knows that the state is probabilistically prepared in the above mentioned way but does not know the result of the coin tossing. In the following, we will see that the state s for the observer cannot be described by any unit vector in $\mathbb{C}^2$.

For this purpose, it is important to recognize that the probability in the Born rule can be considered as a conditional probability[18] given a state. With this view, we can rewrite the Born rule by

$$\langle\psi|P_a\psi\rangle = \Pr(A = a \mid |\psi\rangle) = \frac{\Pr(\text{“}A = a\text{”} \cap |\psi\rangle)}{\Pr(|\psi\rangle)}, \tag{5.29}$$

where $\Pr(|\psi\rangle)$ is the probability to prepare the state $|\psi\rangle$ and $\Pr(\text{“}A = a\text{”} \cap |\psi\rangle)$ is the joint probability that the measurement outcome of A is a and the state is $|\psi\rangle$.

We now consider an arbitrary basis measurement $M = \{|\phi_0\rangle, |\phi_1\rangle\}$ (a measurement of non-degenerate physical quantity) under the state s. Noting that the events to prepare the state $|0\rangle$ and the state $|1\rangle$ are mutually exclusive, we can use the sum rule (see footnote 14) as

$$\Pr(M = j|s) = \Pr(\text{“}M = j\text{”} \cap |0\rangle) + \Pr(\text{“}M = j\text{”} \cap |1\rangle). \tag{5.30}$$

Using (5.29) and the Born rule (5.11) for the basis measurement M, we have

$$\Pr(\text{“}M = j\text{”} \cap |i\rangle) = \Pr(|i\rangle)\Pr(M = j||i\rangle) = \frac{1}{2}|\langle\phi_j|i\rangle|^2 \ (i = 0, 1),$$

where we have used $\Pr(|i\rangle) = 1/2$ $(i = 0, 1)$, which are the probabilities given by the coin tossing. Therefore we obtain

$$\Pr(M = j|s) = \frac{1}{2}|\langle\phi_j|0\rangle|^2 + \frac{1}{2}|\langle\phi_j|1\rangle|^2 = \frac{1}{2}||\phi_j||^2 = \frac{1}{2} \ (j = 0, 1). \tag{5.31}$$

(The second equality follows from the completeness condition of $\{|0\rangle, |1\rangle\}$.) Since M is an arbitrary basis measurement, the state s is the one which predicts the uniform

[17] For those who are not satisfied with using classical probabilistic events in the theory of QM, just replace a coin to some qubit system in a state, say $|+\rangle = \frac{1}{\sqrt{2}}(1, 1)^T$, and measure a computational basis $\{|0\rangle, |1\rangle\}$ to get probabilities 1/2.

[18] Remind that a probability under a certain conditioning of an event is called a **conditional probability** . Under a conditioning event B with non-zero probability $\Pr(B)$, the conditional probability of A given B, denoted by $\Pr(A|B)$, is defined by $\Pr(A|B) := \frac{\Pr(A\cap B)}{\Pr(B)}$, where $\Pr(A \cap B)$ is the joint probability of A and B.

probability distribution $\{1/2, 1/2\}$ for all basis measurements. However, it is easy to show that there are no unit vectors in $\mathbb{C}^2$ to reproduce such probability distributions.[19]

The above simple example shows that the operation of probabilistic mixtures broadens the set of quantum states so that it contains states that cannot be described by Postulate 1. In the following, we call a state described by a unit vector a **pure state**, while an enlarged state, as exemplified by probabilistic mixtures, is called a **mixed state**. Alternatively, a pure state is called a **vector state** to emphasize that it is described by a vector.

Note that the probabilistic mixtures of states naturally appear in statistical physics both in classical[20] and quantum physics, especially when dealing with a physical system consisting of a vast numbers of particles. In such cases, it is practically impossible to know the pure state (even in reality the system is in a pure state), and we inevitably use the probabilistic mixture of states by putting an appropriate probability distribution on the set of pure states. A typical example of a mixed state both in classical and quantum physics is a thermal equilibrium state.

It should be noticed that the origin of a mixed state from the probabilistic mixture lies in the absence of information of the observer. Indeed, even in the above example with a coin tossing, if the observer knows the result of the coin tossing, the state is described by a unit vector, either $|0\rangle$ or $|1\rangle$. We will see, however, another origin of mixed states exists which is peculiar to quantum physics (see Sect. 5.3.1.5).

5.3.1.2 The Density Operator

In this part, we introduce the useful state-representation by means of the density operator to describe both pure and mixed quantum states. Consider a quantum state s in an arbitrary quantum system which is prepared as a probabilistic mixture by preparing a state $|\psi_i\rangle \in \mathcal{H}$ with a probability p_i $(i = 1, \ldots, n)$. Note that this situation includes a pure state in the case $n = 1$. A possible representation of such a state is to explicitly write all information of states $|\psi_i\rangle$ and the probability p_i. For instance, we can denote the state s by

$$s = \{p_i; |\psi_i\rangle\}_{i=1}^n \quad (\text{or } s = \{p_1, \ldots, p_n; |\psi_1\rangle, \ldots, |\psi_n\rangle\}). \tag{5.32}$$

However, such notation has a certain defect of the non-uniqueness in a state representation. To understand this, let us again consider the qubit system. Let s_1 be a mixed state by preparing states $|0\rangle$ or $|1\rangle$ with probabilities $1/2$, and let s_2 be a mixed state by preparing states $|+\rangle$ or $|-\rangle$ with probabilities $1/2$. (Remind that

[19] One can show this by contradiction. Suppose that s is described by some unit vector $|\xi\rangle \in \mathbb{C}^2$. Let $|\xi\rangle^\perp$ be an orthogonal vector to $|\xi\rangle$ so that $\{|\xi\rangle, |\xi\rangle^\perp\}$ forms an ONB of $\mathbb{C}^2$. Then, the basis measurement $\{|\xi\rangle, |\xi\rangle^\perp\}$ under state $|\xi\rangle$ gives a contradiction: The probability to get the outcome corresponding to $|\xi\rangle$ is $|\langle\xi|\xi\rangle|^2 = 1$, which is inconsistent with (5.31).

[20] In classical mechanics, a pure state is described by positions and momentums of the particles, namely a point in the phase space. A mixed state is described by a probability distribution on the phase space.

$|\pm\rangle := \frac{1}{\sqrt{2}}(1, \pm 1)^T = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.) If we use the notation (5.32), s_1 and s_2 are differently denoted as $s_1 = \{1/2, 1/2; |0\rangle, |1\rangle\}$ and $s_2 = \{1/2, 1/2; |+\rangle, |-\rangle\}$. However, as is easily shown, s_1 and s_2 are statistically equivalent and should be identified according to the preposition (5.3). Indeed, for the measurement of an arbitrary physical quantity $A = \sum_a aP_a$, we have $\Pr(A = a|s_2) = \frac{1}{2}\langle +|P_a|+\rangle + \frac{1}{2}\langle -|P_a|-\rangle = \frac{1}{2}\langle 0|P_a|0\rangle + \frac{1}{2}\langle 1|P_a|1\rangle = \Pr(A = a|s_1)$.[21]

In order to get rid of the non-uniqueness defect, we usually use other representation. Consider a measurement of a physical quantity $A = \sum_a aP_a$ under a state $s = \{p_i; |\psi_i\rangle\}_{i=1}^n$ in an arbitrary quantum system. Then, the probability to obtain an outcome a is given by

$$\Pr(A = a \mid s) = \sum_i p_i \Pr(A = a \mid |\psi_i\rangle) = \sum_i p_i \langle\psi_i|P_a\psi_i\rangle. \tag{5.33}$$

This follows in the same manner as in the derivation of (5.31) and using the Born rule (5.9). We now introduce the linear operator ρ defined by

$$\rho := \sum_{i=1}^n p_i |\psi_i\rangle\langle\psi_i|. \tag{5.34}$$

By using the linearity of the trace operation (see Appendix A.3.8) and Exercise 5.4 below, we have $\sum_i p_i \langle\psi_i|P_a\psi_i\rangle = \sum_i p_i \operatorname{Tr}(P_a|\psi_i\rangle\langle\psi_i|) = \operatorname{Tr}(P_a\rho)$. Therefore, (5.33) can be rewritten as

$$\Pr(A = a \mid s) = \operatorname{Tr}(P_a\rho) = \operatorname{Tr}(\rho P_a). \tag{5.35}$$

(For the final equality, remind the cyclic property of the trace operation: $\operatorname{Tr} AB = \operatorname{Tr} BA$.)

The operator (5.34) can physically represent a state $s = \{p_i; |\psi_i\rangle\}_{i=1}^n$ because it can predict the probability distribution of an arbitrary physical quantity by (5.35). The operator (5.34) is called a **density operator** (or a **density matrix**, a **statistical operator**) which represents a state $s = \{p_i; |\psi_i\rangle\}$. Important thing is that the use of density operator can resolve the non-uniqueness defect as follows: Consider two states $s = \{p_i; |\psi_i\rangle\}_{i=1}^n$ and $s' = \{p'_j; |\psi'_j\rangle\}_{j=1}^m$ with the corresponding density operators $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ and $\rho' = \sum_j p'_j|\psi'_j\rangle\langle\psi'_j|$. Let states s and s' are statistically equivalent so that an arbitrary physical quantity A satisfies $\Pr(A = a \mid s) = \Pr(A = a \mid s')$. By (5.35), it follows that $\operatorname{Tr}(P_a\rho) = \operatorname{Tr}(P_a\rho')$ for any eigen-projection P_a, and thus we obtain $\rho = \rho'$.[22] Conversely, if $\rho = \rho'$, we

[21] To obtain the second equality, one can substitute $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Alternatively, just use the arbitrariness of ONBs in the definition of the trace operation: $\operatorname{Tr} P_a = \langle 0|P_a|0\rangle + \langle 1|P_a|1\rangle = \langle +|P_a|+\rangle + \langle -|P_a|-\rangle$ (see Appendix A.3.8).

[22] By putting $A = |\psi\rangle\langle\psi|$ with an arbitrary $|\psi\rangle \in \mathcal{H}$, we have $\langle\psi|\rho\psi\rangle = \Pr(A = 1|\rho) = \Pr(A = 1|\rho') = \langle\psi|\rho'\psi\rangle$. From Proposition A.3-(ii), we have $\rho = \rho'$.

have $\Pr(A = a \mid s) = \mathrm{Tr}(P_a \rho) = \mathrm{Tr}(P_a \rho') = \Pr(A = a \mid s')$ from (5.35), and thus s and s' are statistically equivalent. (See also Exercise 5.5.)

Note that the density operator representing a pure state $s = \{1; |\psi\rangle\}$ is a one-dimensional projection operator

$$\rho = |\psi\rangle\langle\psi|. \tag{5.36}$$

Different from the state representation by a unit vector, a phase indefiniteness of a state is also resolved in the density operator representation.[23] A vector $|\psi\rangle$ to represent a pure state is sometimes called a **state vector**.

We have shown that a density operator can *uniquely* represent both pure and mixed quantum states. In the following, we use a state-representation by means of density operators. The probability rule by (5.35) is a generalization of the Born rule (5.9) and is also called the **Born rule** for density operators.

Exercise 5.4 For any $A \in \mathcal{L}(\mathcal{H})$ show that

$$\mathrm{Tr}(A|\psi\rangle\langle\phi|) = \langle\phi|A\psi\rangle \quad \forall|\psi\rangle, |\phi\rangle \in \mathcal{H}\,. \tag{5.37}$$

In particular, by putting $A = I$, we have $\mathrm{Tr}(|\psi\rangle\langle\phi|) = \langle\phi|\psi\rangle$.

Exercise 5.5 Show that the corresponding density operators for states $s_1 = \{1/2, 1/2; |0\rangle, |1\rangle\}$ and $s_2 = \{1/2, 1/2; |+\rangle, |-\rangle\}$ are both $\frac{1}{2}I$.

5.3.1.3 Properties of the Density Operator

In the preceding part, we have introduced a density operator (5.34) in a way to represent a state $s = \{p_i; |\psi_i\rangle\}_{i=1}^n$. In this part, we give the mathematical definition of a density operator by extracting the essence of the operator of the form (5.34).

For any mixed (including pure) state $\{p_i; |\psi_i\rangle\}$ prepared by probabilistic mixtures, the corresponding density operator $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ satisfies the following two properties: (i) $\rho \geq 0$ (positivity) and (ii) $\mathrm{Tr}\,\rho = 1$. (See Appendix A.3.5 for the positivity of operators.) Indeed, for an arbitrary vector $|\xi\rangle \in \mathcal{H}$, we have $\langle\xi|\rho\xi\rangle = \langle\xi|(\sum_i p_i|\psi_i\rangle\langle\psi_i|)\xi\rangle = \sum_i p_i|\langle\xi|\psi_i\rangle|^2 \geq 0$. Also, we have $\mathrm{Tr}\,\rho = \mathrm{Tr}(\sum_i p_i|\psi_i\rangle\langle\psi_i|) = \sum_i p_i\langle\psi_i|\psi_i\rangle = \sum_i p_i = 1$ by using Exercise 5.4 and the linearity of the trace operation.

Importantly, the converse is also true in the sense that any linear operator satisfying (i) and (ii) corresponds to a physically realizable density operator. To see this, let $\rho \in \mathcal{L}(\mathcal{H})$ satisfies (i) and (ii). Then, by (i), ρ is a Hermitian operator with non-negative eigenvalues $q_i \geq 0$ $(i = 1, \ldots, d)$ (see Proposition A.7), and thus have an eigenvalue decomposition $\rho = \sum_{i=1}^d q_i|\phi_i\rangle\langle\phi_i|$. On the other hand, we have $1 = \mathrm{Tr}\,\rho = \sum_i q_i$ by (ii). Noting that $\{q_i\}_{i=1}^d$ forms a probability distribution, the

[23] For unit vectors $|\psi\rangle$ and $|\phi\rangle$ such that $|\phi\rangle = e^{i\theta}|\psi\rangle$, the corresponding density operators are the same: $|\phi\rangle\langle\phi| = e^{i\theta}|\psi\rangle\langle\psi|e^{-i\theta} = |\psi\rangle\langle\psi|$.

linear operator ρ can be physically realized as the density operator representing the state $s = \{q_i; |\phi_i\rangle\}_{i=1}^{d}$.[24]

Consequently, we have obtained the mathematical definition of the **density operator** by a linear operator on a Hilbert space $\mathcal{H}$ satisfying properties (i) and (ii):

$$\rho : \text{density operator} \Leftrightarrow \text{(i) } \rho \geq 0, \ \text{(ii) } \operatorname{Tr} \rho = 1. \tag{5.38}$$

Combining with the Born rule (5.35), a density operator represents a general quantum state. Namely, by measuring a physical quantity $A = \sum_a a P_a$ under a density operator ρ, we get an outcome a such that the probability is given by $\operatorname{Tr}(\rho P_a)$.

Similarly as in the case of pure states (unit vectors), we can calculate statistical quantities such as expectation values and variances of physical quantities under general quantum states. Under a density operator ρ, the expectation value of a physical quantity $A = \sum_a a P_a$ is given by $\mathrm{E}_\rho[A] := \sum_a a \Pr(A = a|\rho) = \sum_a a \operatorname{Tr} \rho P_a = \operatorname{Tr}(\rho(\sum_a a P_a)) = \operatorname{Tr}(\rho A)$:

$$\mathrm{E}_\rho[A] = \operatorname{Tr}(\rho A) = \operatorname{Tr}(A\rho). \tag{5.39}$$

Similarly, we have the formula for the variance

$$\mathrm{V}_\rho[A] = \operatorname{Tr}(\rho A^2) - (\operatorname{Tr}(A\rho))^2 = \operatorname{Tr}(\rho(A - \mathrm{E}_\rho[A]\, I)^2). \tag{5.40}$$

Similar to the case of pure states, these quantities can be computed using only A without solving the eigenvalue problem.

Exercise 5.6 Show that $\rho = \begin{pmatrix} \frac{1}{2} & -\frac{1}{6} \\ -\frac{1}{6} & \frac{1}{2} \end{pmatrix}$ is a density operator on a qubit system. Calculate the probabilities to get ±1 when measuring σ_x under the state ρ.

In the following, we will investigate other important properties of density operators.

Proposition 5.5 *A convex combination of density operators is a density operator. Namely, for any density operators ρ_1, ρ_2 and $p \in [0, 1]$,*

$$\rho := p\rho_1 + (1 - p)\rho_2 \tag{5.41}$$

is a density operator. The density operator (5.41) *represents a state which is prepared by probabilistic mixtures $\{p, 1 - p; \rho_1, \rho_2\}$.*

Proof First, we show that the operator ρ in (5.41) satisfies the mathematical definition of a density operator, namely, (i) and (ii) in (5.38): For any vector $|\psi\rangle \in \mathcal{H}$, (i) $\langle\psi|\rho\psi\rangle = p\langle\psi|\rho_1\psi\rangle + (1 - p)\langle\psi|\rho_2\psi\rangle \geq 0$ since ρ_1 and ρ_2 are positive. Also, we

[24] Notice that this method may not be the only preparation of ρ. As is shown later, a mixed state has always non-unique (and indeed infinitely many) state-preparations, while a pure state has the unique state-preparation (see Proposition 5.7).

have (ii) $\mathrm{Tr}\,\rho = p\,\mathrm{Tr}\,\rho_1 + (1-p)\,\mathrm{Tr}\,\rho_2 = p + (1-p) = 1$ by using $\mathrm{Tr}\,\rho_1 = \mathrm{Tr}\,\rho_2 = 1$. Therefore, the convex combination of density operators is a density operator.

Next, we show that the density operator ρ represents the state $s = \{p, 1-p; \rho_1, \rho_2\}$. To show this, we consider a measurement of an arbitrary physical quantity $A = \sum_a a P_a$ under the state s. Then, in a similar way of the derivation of (5.33), we have $\Pr(A = a \mid s) = p\,\mathrm{Tr}(P_a\rho_1) + (1-p)\,\mathrm{Tr}(P_a\rho_2) = \mathrm{Tr}(P_a(p\rho_1 + (1-p)\rho_2))$. This implies that the corresponding density operator to represent s is $\rho = p\rho_1 + (1-p)\rho_2$. □

In a similar way, a convex combination $\rho := \sum_{i=1}^{n} p_i\rho_i$ of density operators ρ_i $(i = 1, \ldots, n)$ with probability distribution $\{p_i\}_{i=1}^{n}$ is shown to be a density operator corresponding the state $\{p_i; \rho_i\}$. This fact implies that the set of quantum states is not any more enlarged through probabilistic mixtures of mixed states because the set of density operators is closed under the operation of the probabilistic mixture. In other words, the density operators can represent all quantum states that reflects the operation of the probabilistic mixture.

In the following, we denote by $\mathcal{S}(\mathcal{H})$ the set of all density operators:

$$\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{L}(\mathcal{H})_h \mid \text{(i) } \rho \geq 0,\ \text{(ii) } \mathrm{Tr}\,\rho = 1\}, \tag{5.42}$$

where $\mathcal{L}(\mathcal{H})_h$ denotes the set of all the Hermitian operators on $\mathcal{H}$. We shall simply call $\mathcal{S}(\mathcal{H})$ the **state space**. Proposition 5.5 implies that the state space $\mathcal{S}(\mathcal{H})$ is a **convex (sub)set** of the real vector space $\mathcal{L}(\mathcal{H})_h$ (see Appendix A.4).

The following proposition gives some equivalent conditions to characterize a pure state:

Proposition 5.6 *For $\rho \in \mathcal{S}(\mathcal{H})$, the followings are equivalent:*

(a) *ρ is a pure state,*
(b) $\rho = \rho^2$,
(c) $\mathrm{Tr}(\rho^2) = 1$,
(d) *The eigenvalues of ρ are* $\{1, 0, \ldots, 0\}$,
(e) *ρ is an **extreme point** of $S(\mathcal{H})$* (see Appendix A.4).

Proof [(a) ⇒ (b)] Letting $|\psi\rangle$ be a state vector of ρ, we have $\rho^2 = |\psi\rangle\langle\psi||\psi\rangle\langle\psi| = ||\psi||^2|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho$. [(b) ⇒ (c)] By (ii) of (5.38), we have $\mathrm{Tr}\,\rho^2 = \mathrm{Tr}\,\rho = 1$. [(c) ⇒ (d)] Using an eigenvalue decomposition $\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i|$ $(1 \geq p_i \geq 0)$, we get $1 = \mathrm{Tr}\,\rho^2 = \mathrm{Tr}(\sum_i p_i|\phi_i\rangle\langle\phi_i|)(\sum_j p_j|\phi_j\rangle\langle\phi_j|) = \sum_{i,j} p_i p_j |\langle\phi_i|\phi_j\rangle|^2 = \sum_i p_i^2$. Assume contrary that all eigenvalues satisfy $p_i < 1$, we have the contradiction that $\sum_i p_i^2 < \sum_i p_i = 1$. Therefore, $p_{i_0} = 1$ for some $i_0 \in \{1, \ldots, d\}$. From $\sum_i p_i = 1$, the remaining eigenvalues are all 0. [(d) ⇒ (a)] An eigenvalue decomposition of ρ shows that $\rho = |\phi_{i_0}\rangle\langle\phi_{i_0}|$ where $|\phi_{i_0}\rangle$ is the eigenvector belonging to the eigenvalue 1.

[(a) ⇒ (e)] Let $\rho = |\psi\rangle\langle\psi|$ with a state vector $|\psi\rangle$. Assume that ρ is not an extreme point of $\mathcal{S}(\mathcal{H})$ so that there exist density operators $\rho_1, \rho_2 (\neq \rho) \in \mathcal{S}(\mathcal{H})$ and

$p \in (0, 1)$ such that $\rho = p\rho_1 + (1-p)\rho_2$. Taking an inner product between $|\psi\rangle$ and $\rho|\psi\rangle$, we have $1 = p\langle\psi|\rho_1\psi\rangle + (1-p)\langle\psi|\rho_2\psi\rangle$. Since $0 \le \langle\psi|\rho_i\psi\rangle \le 1$ $(i = 1, 2)$ by Exercise 5.7 and $0 < p < 1$, we obtain $\langle\psi|\rho_1\psi\rangle = 1$. Substituting an eigenvalue decomposition $\rho_1 = \sum_{i=1}^{l} q_i|\phi_i\rangle\langle\phi_i|$ ($q_i > 0$: removing zero-eigenvalues), we have $\sum_{i=1}^{l} q_i|\langle\phi_i|\psi\rangle|^2 = 1$. By the Schwarz inequality $|\langle\phi_i|\psi\rangle|^2 \le ||\phi_i||^2||\psi||^2 = 1$ and $\sum_i q_i = 1$, we have $|\langle\phi_i|\psi\rangle| = 1$ for any $i = 1, \dots, l$. Since the equality of the Schwarz inequality follows, we have $|\phi_i\rangle = |\psi\rangle$ (up to the phase indefiniteness). Hence, $\rho_1 = |\psi\rangle\langle\psi|$, but this equation contradicts $\rho \neq \rho_1$. By contradiction, we have proved that ρ is an extreme point of $\mathcal{S}(\mathcal{H})$.

Finally, we shall show [(e) ⇒ (a)] by its contraposition. Let ρ be not a pure state. Then, from (d), we can make an eigenvalue decomposition $\sum_{j=1} p_j|\psi_j\rangle\langle\psi_j|$ of ρ such that $0 < p := p_1 < 1$. Then, it is easy to see that $\rho_1 := |\psi_1\rangle\langle\psi_1|$ and $\rho_2 := \frac{1}{1-p}\sum_{j=2}^{d} p_j|\psi_j\rangle\langle\psi_j|$ are both density operators which are distinct from ρ. Moreover, we have $\rho = p\rho_1 + (1-p)\rho_2$. Therefore, ρ is not an extreme point. □

If a state ρ can be prepared by the probabilistic mixture of states $\{p, 1-p; \rho_1, \rho_2\}$ such that ρ_1, ρ_2 are distinct from ρ and $p \neq 0, 1$, we say ρ can be prepared by a **nontrivial probabilistic mixture**. By Proposition 5.5, this is equivalent to say that ρ is an extreme point of $\mathcal{S}(\mathcal{H})$. Therefore, Proposition 5.6-(e) indicates the following operational characterization of pure states:

Proposition 5.7 *A quantum state is a pure state if and only if it can be prepared by a nontrivial probabilistic mixture.*

Namely, we can redefine a pure state (resp. a mixed state) by a state which cannot (resp. can) be prepared by a nontrivial probabilistic mixture. This gives an operational definition of a pure (and mixed) state which is valid not only for QM but also for any probabilistic theories.

Exercise 5.7 Show that for any $\rho \in \mathcal{S}(\mathcal{H})$ and any unit vector $|\psi\rangle$,

$$0 \le \langle\psi|\rho\psi\rangle \le 1.$$

Exercise 5.8 Show that for any $\rho \in \mathcal{S}(\mathcal{H})$,

$$\frac{1}{d} \le \mathrm{Tr}(\rho^2) \le 1. \tag{5.43}$$

The lower bound is achieved if and only if ρ is the **completely mixed state** $\rho_{\mathrm{mix}} := \frac{1}{d}I$, while the upper bound is achieved if and only if ρ is a pure state. $\mathrm{Tr}(\rho^2)$ is called the **purity** of ρ.

5.3.1.4 Bloch Vector

In Sect. 2.3.1, we have introduced the Bloch vector representation for state vectors in a qubit system. This representation can be generalized to represent a density operator of a qubit system as follows.[25] The **Bloch vector** corresponding to the density operator ρ in a qubit system is defined by the three dimensional real vector whose components are expectation values of Pauli matrices (2.22):

$$\mathbf{b} = (b_1, b_2, b_3)^T := (\mathrm{Tr}(\rho\sigma_x), \mathrm{Tr}(\rho\sigma_y), \mathrm{Tr}(\rho\sigma_z))^T \in \mathbb{R}^3. \tag{5.44}$$

(Remind the formula (5.39) for an expectation value). It turns out that the Bloch vector provides a state-representation equivalent to that of a density operator in a way to preserve the convex structure of the state space $\mathcal{S}(\mathbb{C}^2)$. Namely, we have the one-to-one correspondence between a density operator and a Bloch vector in a qubit system such that a convex combination of density operators corresponds to the convex combination of the corresponding Bloch vectors.

We first show that the corresponding density operator to the Bloch vector is given by

$$\rho = \frac{1}{2}(I + \sum_{i=1}^{3} b_i \sigma_i). \tag{5.45}$$

To see this, we just need a simple mathematical fact that the identity matrix $\sigma_0 := I$ and Pauli matrices form an orthogonal basis of $M_2(\mathbb{C})$ (the set of 2×2 complex matrices) in terms of the Hilbert-Schmidt inner product (Appendix A.3.8). Indeed, the dimension of $M_2(\mathbb{C})$ is 4 (see Exercise A.8), and one can check the orthogonality condition

$$\mathrm{Tr}(\sigma_j \sigma_k) = 2\delta_{jk} \ (j, k = 0, 1, 2, 3) \tag{5.46}$$

by the direct computation. Therefore, any 2×2 complex matrix A has the form[26]

$$A = \frac{1}{2}\sum_{j=0}^{3} \mathrm{Tr}(A\sigma_j)\sigma_j. \tag{5.47}$$

Applying this equation to a density operator ρ and using $\mathrm{Tr}\,\rho = 1$ and $b_i = \mathrm{Tr}(\rho\sigma_i)$, we obtain (5.45). Notice that by substituting (2.15) to the corresponding density operator $\rho = |\psi\rangle\langle\psi|$, one can easily show that (5.45) gives a generalization of the Bloch vector given in Sect. 2.3.1.[27]

Equation (5.44) gives a map from a density operator to the corresponding Bloch vector, while (5.45) gives the inverse map. From (5.44) and the linearity of the trace operation, it is easy to see that a convex combination of density operators $\rho = p\rho_1 + (1-p)\rho_2$ corresponds to $\mathbf{b}(\rho) = p\mathbf{b}(\rho_1) + (1-p)\mathbf{b}(\rho_2)$. Therefore,

[25] In this book, we introduce the Bloch vector only in a qubit system. However, one can easily generalize the Bloch vector in arbitrary d-level quantum systems [14, 15].

[26] Take the inner product between σ_i $(i = 0, 1, 2, 3)$ and $A = \sum_{j=0}^{3} x_j \sigma_j$ (the expansion of A with respect to the basis) and use condition (5.46) to get $x_i = \frac{1}{2}\mathrm{Tr}(A\sigma_i)$.

[27] By putting $\rho = |\psi\rangle\langle\psi|$ with the parametrization (2.15), one can get $b_1 = \sin\theta\cos\phi$, $b_2 = \sin\theta\sin\phi$, $b_3 = \cos\theta$, which give the polar coordinates of $\mathbf{b}$.

the Bloch vector $\mathbf{b}(\rho)$ can be interpreted to be a state prepared by the probabilistic mixture $\{p, 1-p; \mathbf{b}(\rho_1), \mathbf{b}(\rho_2)\}$ as in the case of a density operator.

The set of Bloch vectors $B(\mathbb{R}^3)$, which is the image of $\mathcal{S}(\mathbb{C}^2)$ of the map (5.44), has a simple geometrical structure. First, it is a convex subset of $\mathbb{R}^3$ because $\mathcal{S}(\mathbb{C}^2)$ is a convex set and the map (5.44) preserves the convex structure. In fact, $B(\mathbb{R}^3)$ can be shown to be a unit ball in $\mathbb{R}^3$.

To show this, we need to find the condition that the operator ρ in (5.45) is a density operator (i.e., conditions (i) and (ii) in (5.38)). Since $\operatorname{Tr}\sigma_0 = 2$ and $\operatorname{Tr}\sigma_i = \operatorname{Tr}\sigma_i\sigma_0 = 0$ $(i = 1, 2, 3)$ by (5.46), one of the conditions (ii) $\operatorname{Tr}\rho = 1$ is already satisfied. Moreover, as σ_i $(i = 0, \ldots, 3)$ are all Hermitian, so is any operator ρ in (5.45) for any $\mathbf{b} \in \mathbb{R}^3$. Thus, the condition (i) reduces to the non-negativity of the eigenvalues. However, by Exercise 5.9 and $\operatorname{Tr}\rho = 1$, the non-negativity of eigenvalues is equivalent to the inequality $\operatorname{Tr}\rho^2 \leq 1$ (see also Exercise 5.8). By the direct computation using (5.45) and (5.46), we get $\operatorname{Tr}\rho^2 = \frac{1}{2}(1 + |\mathbf{b}|^2)$, and we have $\operatorname{Tr}\rho^2 \leq 1 \Leftrightarrow |\mathbf{b}| \leq 1$. Consequently, we obtain that the set of all the Bloch vectors is a unit ball $\{\mathbf{b} \in \mathbb{R}^3 \mid |\mathbf{b}| \leq 1\}$, which is called the **Bloch ball**. Notice that, as we have already seen in Sect. 2.3.1, the set of pure states corresponds to the surface of the Bloch ball (see Fig. 2.2). One can understand this fact by noting that the set of extreme points of a ball corresponds to the surface and that Bloch vector representation preserves the convex combination of the density operator. Alternatively, one can use the fact that a density operator ρ is pure if and only if $\operatorname{Tr}\rho^2 = 1$ (see Exercise 5.8) and $\operatorname{Tr}\rho^2 = 1 \Leftrightarrow |\mathbf{b}| = 1$.

One of the advantages to use the Bloch vector representation is that the components of the Bloch vector are expectation values, which can be directly determined by experiments. In particular, the Bloch vector (as experimental data) gives a way to determine an unknown quantum state through (5.45). In general, the way to determine the corresponding quantum state using experimental data (such as expectation values and probability distributions) is called the **quantum (state) statistical inference** [16] or the **quantum (state) tomography**.

Exercise 5.9 Show that all the eigenvalues of 2×2 Hermitian matrix A are non-negative if and only if $\operatorname{Tr} A \geq 0$ and $(\operatorname{Tr} A)^2 - \operatorname{Tr}(A^2) \geq 0$.

5.3.1.5 Reduced States

So far, we have treated only the operation of a probabilistic mixture of states. In this part, we introduce another important operation by simply restricting our interest from a system to its subsystem. Remarkably, this natural operation also enlarges the set of quantum states from the set of pure states. Before giving the general discussion, let us see a simple example of this fact. Let S and E be both qubit systems, and let the state of the composite system of S+E be the entangled state $|\psi\rangle$ in (2.33). To see the nature of the local state s of the subsystem S from the total state $|\psi\rangle$, consider an arbitrary basis measurement $M = \{|\phi_0\rangle, |\phi_1\rangle\}$ of S, where the corresponding physical quantity on the composite system S+E is $A \otimes I_{\mathrm{E}} = (0|\phi_0\rangle\langle\phi_0| + 1|\phi_1\rangle\langle\phi_1|) \otimes I_{\mathrm{E}}$ according to Postulate 3. By the Born rule, the probability to obtain an outcome $j = 0, 1$ is given by

$$\begin{aligned}\Pr(M = j|s) &= \Pr(A \otimes I_{\mathrm{E}} = j||\psi\rangle) = \langle\psi|(|\phi_j\rangle\langle\phi_j| \otimes I_{\mathrm{E}})\psi\rangle \\ &= \frac{1}{2}(\langle 00| + \langle 11|)(|\phi_j\rangle\langle\phi_j| \otimes I_{\mathrm{E}})(|00\rangle + |11\rangle) \\ &= \frac{1}{2}|\langle\phi_j|0\rangle|^2 + \frac{1}{2}|\langle\phi_j|1\rangle|^2 = \frac{1}{2}. \end{aligned} \tag{5.48}$$

The probability is exactly the same as in (5.31), which has been shown not to be described by any unit vector of $\mathbb{C}^2$. That is, the restriction introduces a state different from a pure state in Postulate 1. (See also Exercise 5.11 below). In the following, however, we show that any state produced by the restriction can still be described by density operators. Therefore, we can conclude that a density operator describes a general quantum state introduced by both operations of the probabilistic mixture and the restriction of our interest.

In the following, let S be a subsystem in which we are interested and let E be the remaining subsystem so that the composite system S + E composes the total system. We call S the **system of interest** and E an **environment** (system). Let $\mathcal{H}_{\mathrm{S}}, \mathcal{H}_{\mathrm{E}}$ be Hilbert spaces associated with systems S and E, respectively. Remind that the associated Hilbert space with the composite system S + E is the tensor product space $\mathcal{H}_{\mathrm{SE}} := \mathcal{H}_{\mathrm{S}} \otimes \mathcal{H}_{\mathrm{E}}$ (Postulate 3). The local state will be called the **reduced state**. From the operational point of view, the reduced state of S should be defined in a way to have the ability to predict probability distributions for the measurements of arbitrary physical quantities of S. In the theory of classical probability, the reduced state is described by the marginal probability distribution (see the footnote 14).

To describe a reduced state of a quantum system, we need to introduce the **partial trace** operation Tr_{E} over the space $\mathcal{H}_{\mathrm{E}}$ as a linear map:

$$C = \sum_j A_j \otimes B_j \in \mathcal{L}(\mathcal{H}_{\mathrm{SE}}) \to \mathrm{Tr}_{\mathrm{E}}\, C := \sum_j (\mathrm{Tr}\, B_j) A_j \in \mathcal{L}(\mathcal{H}_{\mathrm{S}}). \tag{5.49}$$

Notice here that any linear operator C on $\mathcal{H}_{\mathrm{S}} \otimes \mathcal{H}_{\mathrm{E}}$ can be written by the form $C = \sum_j A_j \otimes B_j$ with some linear operators $A_j \in \mathcal{L}(\mathcal{H}_{\mathrm{S}}), B_j \in \mathcal{L}(\mathcal{H}_{\mathrm{E}})$ (see Appendix A.5.2). Rigorously speaking, we should also show that the mapping in (5.49) does not depend of the decompositions of $C = \sum_j A_j \otimes B_j$ for the well-definedness, which will be shown in the solution of Exercise 5.10-(1).

Exercise 5.10 Show properties (1)–(4) below on the partial trace:

(1) The definition of the partial trace is equivalent to the following: For any $C \in \mathcal{L}(\mathcal{H}_{\mathrm{SE}})$, $\mathrm{Tr}_{\mathrm{E}}\, C$ is defined as the linear operator on $\mathcal{H}_{\mathrm{S}}$ which is characterized by

$$\forall|\psi\rangle, |\phi\rangle \in \mathcal{H}_{\mathrm{S}}, \quad \langle\psi|(\mathrm{Tr}_{\mathrm{E}}\, C)\phi\rangle := \sum_k \langle\psi \otimes e_k|C|\phi \otimes e_k\rangle, \tag{5.50}$$

where $\{|e_k\rangle\}_k$ is an arbitrary ONB of $\mathcal{H}_{\mathrm{E}}$.

(2) For any $A \in \mathcal{L}(\mathcal{H}_S), C \in \mathcal{L}(\mathcal{H}_{SE})$,

$$\mathrm{Tr}(A \otimes I_E\, C) = \mathrm{Tr}(A(\mathrm{Tr}_E\, C)),$$

where Tr on the left (resp. right) hand side is the trace operation on $\mathcal{H}_{SE}$ (resp. $\mathcal{H}_S$).

(3) For any positive operator $C \in \mathcal{L}(\mathcal{H}_{SE})$, $\mathrm{Tr}_E\, C \in \mathcal{L}(\mathcal{H}_S)$ is also positive.

(4) (Linearity) For any $C_1, C_2 \in \mathcal{L}(\mathcal{H}_{SE})$ and $\alpha, \beta \in \mathbb{C}$,

$$\mathrm{Tr}_E(\alpha C_1 + \beta C_2) = \alpha(\mathrm{Tr}_E\, C_1) + \beta(\mathrm{Tr}_E\, C_2).$$

In the following, in order to indicate the underlying Hilbert space of the trace operation, we often denote a usual trace with a subscript of the system. For instance, in Exercise 5.10-(2), we may denote the two trace operations in the left and right hand side by Tr_{SE} and Tr_S, respectively. One should distinguish between a usual trace and a partial trace by an operator on which the trace operation acts.[28]

Proposition 5.8 *For any density operator ρ_{SE} on $\mathcal{H}_{SE}$, the partial trace $\rho_S := \mathrm{Tr}_E\, \rho_{SE}$ is a density operator on $\mathcal{H}_S$.*

Proof The positivity of ρ_S follows from Exercise 5.10-(3). Letting $\{|\psi_i\rangle\}_i$ be an ONB of $\mathcal{H}_S$, we have $\mathrm{Tr}\, \rho_S = \sum_i \langle\psi_i|\rho_S\psi_i\rangle = \sum_{i,k}\langle\psi_i \otimes e_k|\rho_{SE}|\psi_i \otimes e_k\rangle = \mathrm{Tr}_{SE}\, \rho_{SE} = 1$ by using Exercise 5.10-(1). □

The density operator $\rho_S = \mathrm{Tr}_E\, \rho_{SE}$ made by the partial trace operation is called the **reduced density operator** of ρ_{SE}. In the following, we show that a reduced density operator describes a reduced state:

Proposition 5.9 *If a total state of* S + E *is represented by a density operator ρ_{SE}, the reduced state of* Sp *is represented by the reduced density operator $\rho_S := \mathrm{Tr}_E\, \rho_{SE}$.*

Proof Since the system of interest is S, we only have to deal with an arbitrary physical quantity $A = \sum_a a P_a$ of S to characterize the reduced state of S. Based on Postulate 3 and the Born rule (5.35) on the composite system, the probability to get an outcome a of the measurement of A under the state ρ_{SE} is given by

$$\Pr(A = a|\rho_{SE}) = \mathrm{Tr}_{SE}(P_a \otimes I_E\, \rho_{SE}) = \mathrm{Tr}_S(P_a \rho_S),$$

where the final equality follows by Exercise 5.10-(2). Therefore, by the Born rule (5.35) on the system S, the reduced state of the system S is represented by the reduced density operator ρ_S. (Notice also that we have seen that the density operator satisfies Precondition (5.3) among arbitrary physical quantities of S). □

Proposition 5.9 also shows that the set of density operators is closed under the operation by the restriction of our interest. In other words, a density operator can describe all the states produced by this operation.

[28] For instance, for $X \in \mathcal{L}(\mathcal{H}_E)$, $Y \in \mathcal{L}(\mathcal{H}_{SE})$, $\mathrm{Tr}_E\, X \in \mathbb{C}$ is a usual trace of X but $\mathrm{Tr}_E\, Y \in \mathcal{L}(\mathcal{H}_S)$ is a partial trace of Y.

Exercise 5.11 Show that the reduced density operator of S from the total state $|\psi\rangle$ in (2.33) is $\rho_{\mathrm{S}} = \frac{1}{2} I_{\mathrm{S}}$.

Next, we show an interesting fact about the reduced state of a quantum system: Any mixed state can be considered as a reduced state of a total **pure state**. Using the representation of the density operator, it can be described as follows:

Proposition 5.10 (Purification) *For any density operator ρ_{S} of a system* S*, there exist a quantum system* A *and a* **pure** *density operator $\rho_{\mathrm{SA}} = |\psi\rangle\langle\psi|$ on* S + A *such that $\rho_{\mathrm{S}} = \mathrm{Tr}_{\mathrm{A}}\, \rho_{\mathrm{SA}}$.*

Proof Let A be any quantum system (an ancilla system) represented by a Hilbert space $\mathcal{H}_{\mathrm{A}}$ that has the same dimension d as $\mathcal{H}_{\mathrm{S}}$. Let $\rho_{\mathrm{S}} = \sum_{i=1}^{d} q_i |s_i\rangle\langle s_i|$ be an eigenvalue decomposition of ρ_{S} and let $\{|a_i\rangle\}_{i=1}^{d}$ be an arbitrary ONB of $\mathcal{H}_{\mathrm{A}}$. Then, $|\psi\rangle := \sum_i \sqrt{q_i}|s_i\rangle \otimes |a_i\rangle$ is a unit vector of $\mathcal{H}_{\mathrm{SA}}$, and therefore $\rho_{\mathrm{SA}} = |\psi\rangle\langle\psi|$ represent a pure state on the total system S + A. Noting that $\mathrm{Tr}_{\mathrm{A}}\, |a_i\rangle\langle a_j| = \langle a_j|a_i\rangle = \delta_{ij}$, it follows that $\mathrm{Tr}_{\mathrm{A}}\, \rho_{\mathrm{SA}} = \sum_{ij} \sqrt{q_i}\sqrt{q_j}(\mathrm{Tr}_{\mathrm{A}}\, |a_i\rangle\langle a_j|)|s_i\rangle\langle s_j| = \sum_i q_i |s_i\rangle\langle s_i| = \rho_{\mathrm{S}}$. Therefore, we have shown that ρ_{S} is the reduced density operator of the pure density operator ρ_{SA}. □

The purification of quantum states is one of the peculiar quantum properties which cannot be observed in classical physics.[29]

Note that the purification property also implies the fact that a subsystem can be a mixed state even if the total state is a pure state (We have already seen such example in two-qubit systems at the beginning of this part). As will be shown below, the origin of mixed states lies in the **correlation** of a total state.

We say that a total state ρ_{SE} on a composite system S + E has no correlations if there are no statistical correlations between arbitrary pairs of physical quantities A and B of S and E; namely, the joint probability distribution of A and B is a product of the marginal probability distributions: $\Pr(A = a, B = b|\rho) = \Pr(A = a|\rho_{\mathrm{S}})\Pr(B = b|\rho_{\mathrm{E}})$. Otherwise, a state ρ_{SE} is said to have non-zero correlations. A typical example of a state having non-zero correlations is an entangled state.[30] By using the Born rule (5.35), it is easy to show that ρ_{SE} has no correlations if and only if it is a **product state** of reduced density operators: $\rho_{\mathrm{SE}} = \rho_{\mathrm{S}} \otimes \rho_{\mathrm{E}}$.[31]

Now we are going to show a general property about the relation between a pure state and a correlation[32]:

[29] Moreover, it has recently been shown that the purification is one of the essential properties to single out QM among all operationally valid probabilistic theories [17].

[30] Note, however, that there also exist classically correlated states (separable states) which are not entangled states but have non-zero correlations (see Chap. 7).

[31] By the same argument of the derivation of (5.24) under a density operator, we get $\Pr(A = a, B = b||\psi\rangle) = \mathrm{Tr}_{\mathrm{SE}}(P_a \otimes Q_b \rho)$, where $A = \sum_a a P_a$ and $B = \sum_b b Q_b$ are spectral decomposition of A and B. Substitute this into $\Pr(A = a, B = b|\rho) = \Pr(A = a|\rho_{\mathrm{S}})\Pr(B = b|\rho_{\mathrm{E}})$, we have $\mathrm{Tr}_{\mathrm{SE}}(P_a \otimes Q_b \rho) = (\mathrm{Tr}_{\mathrm{S}}\, P_a \rho_{\mathrm{S}})(\mathrm{Tr}_{\mathrm{E}}\, Q_b \rho_{\mathrm{E}}) = \mathrm{Tr}_{\mathrm{SE}}(P_a \otimes Q_b \rho_{\mathrm{S}} \otimes \rho_{\mathrm{E}})$. As A and B are arbitrary, we obtain $\rho = \rho_{\mathrm{S}} \otimes \rho_{\mathrm{E}}$.

[32] We refer Proposition 1 (page 52) in [13] and Lemma 4.11 (page 210) in [18] for this statement. However, it turns out that this is universally satisfied not only for QM, but also for any operationally valid probabilistic theories including classical physics (see [19] and references therein).

Proposition 5.11 *If a reduced state on S from a composite state ρ_{SE} is a pure state, then ρ_{SE} has no correlations.*

Proof From Proposition 5.10, we can assume that $\rho_{\mathrm{SE}} = |\psi\rangle\langle\psi|$ is a pure state without loss of generality. (If not, applying the purification with an ancilla system A, and redefine a system E by E + A). Substituting the $|\psi\rangle = \sum_i \sqrt{p_i}|\xi_i\rangle \otimes |\eta_i\rangle$ (see Theorem A.4) to $\rho_{\mathrm{S}} := \mathrm{Tr}_{\mathrm{E}}\, |\psi\rangle\langle\psi|$, we have $\rho_{\mathrm{S}} = \sum_i p_i |\xi_i\rangle\langle\xi_i|$, which is an eigenvalue decomposition of ρ_{S}. Since the reduced density operator is a pure state, we can put the eigenvalues as $p_1 = 1$, $p_2 = p_3 = \cdots = 0$ by Proposition 5.6-(d). Therefore, we obtain $|\psi\rangle = |\xi_1\rangle \otimes |\eta_1\rangle$, and $\rho_{\mathrm{SE}} = |\xi_1\rangle\langle\xi_1| \otimes |\eta_1\rangle\langle\eta_1|$. Hence, we have shown that the state ρ_{SE} has no correlations. □

The contraposition of this proposition implies that if there exist correlations in a composite state then the reduced state is a mixed state. In QM, there exists a pure total state with non-zero correlations, i.e., a pure entangled state, (see examples 2.5 and Chap. 7). Consequently, it can happen that the reduced state is a mixed state *even if* a total state is in a pure state. Therefore, we have another origin of mixtures of quantum states due to correlations, which is different from the one due to the absence of information. To conceptually distinguish them, the latter is sometimes called the **proper mixture** while the former is called the **improper mixture** [13]. In classical physics, an improper mixture never happens because there are no pure states with correlations.

5.3.1.6 Unitary Time Evolution of Density Operators

In this part, we explain the unitary time evolution in terms of the density operator. According to Postulate 1, the time evolution of a state vector of an isolated quantum system is governed by the Schrödinger equation, or equivalently by the unitary time evolution (5.21).

The **unitary time evolution** for a density operator with a unitary operator U is given by the map

$$\rho \to \rho' = U\rho U^\dagger, \tag{5.51}$$

where ρ and ρ' are initial and final states, respectively. One can show that this time evolution is realizable based on Postulate 1 as follows: Prepare an initial state $\rho = \sum_i q_i |\phi_i\rangle\langle\phi_i|$ by probabilistic mixtures of $s = \{q_i; |\phi_i\rangle\}$. Then, each state $|\phi_i\rangle$ can be mapped to $U|\phi_i\rangle$ by (5.21). Since the probability distribution $\{q_i\}$ preserves during the time evolution, the final state is described by a probabilistic mixture $s' = \{q_i; U|\phi_i\rangle\}$ whose corresponding density operator is $\rho' = \sum_i q_i U|\phi_i\rangle\langle\phi_i|U^\dagger = U\rho U^\dagger$.[33] The general time evolution in quantum system will be discussed in Sect. 5.3.3.

[33] Alternatively, if ρ is prepared as a reduced density operator (even with probabilistic mixtures), one can realize the map (5.51) by means of a local unitary evolution. Note that based on Postulate 2, the total unitary evolution is given by a unitary operator $U \otimes I$ on a total system.

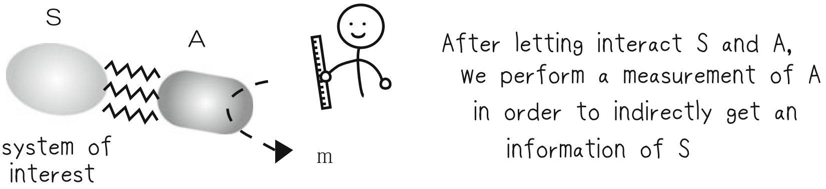

S
A
system of interest
m
After letting interact S and A, we perform a measurement of A in order to indirectly get an information of S

Fig. 5.1 Illustration of an indirect measurement

5.3.2 General Class of Measurements

A measurement we have treated so far is a direct measurement of a physical quantity represented by a Hermitian operator. However, as is the same in the case of a quantum state, the combination of possible operations introduces an alternative method to perform a measurement. In this subsection, we clarify operationally the most general class of measurements and introduce the mathematical representation by means of POVM.

Let us start by seeing how we can go beyond a measurement of a Hermitian operator. The easiest operation is to use the probabilistic mixture of measurements. For instance, performing a measurement of a physical quantity A with probability 0.2 and another physical quantity B with probability 0.8 provides a measurement which cannot be described by a single Hermitian operator. One can easily make such an example (see Exercise 5.12).

Exercise 5.12 Show that a measurement M to perform σ_x or σ_z with probabilities $1/2$ in a qubit system cannot be explained by any measurement of a single Hermitian operator.

Another operation is to use an interaction between a system of interest and another physical system (e.g., a system of a measurement device). Suppose that S is a system of interest and we want to extract a certain information on S. After the system S interacts with another system A, a measurement of a physical quantity on A will provide a certain information on S. This series of procedures can be considered as a single measurement on the system S, which is called an **indirect measurement** on S (see Fig. 5.1).

One can show that an indirect measurement generally cannot be described by a single Hermitian operator on the original system. Indeed, we will see below that a class of indirect measurements is wide enough to cover the most general class of measurements for a fixed quantum system.

5.3.2.1 General Properties of Measurements

We have seen above that a class of quantum measurements described in Postulate 1 is not enough to cover all the possible measurements in QM. In order to find the most general class of quantum measurements, it is better to start from confirming the general properties of measurements.

First, remind our operational standpoint about a measurement described in Preconditions (5.1) and (5.2). Moreover, the following precondition is naturally assumed:

$$\begin{aligned}&\textit{A probability distribution of any measurement satisfies an } \textbf{\textit{affine property}} :\\ &\Pr(M=m \mid \{p,1-p;s_1,s_2\}) = p\Pr(M=m|s_1)+(1-p)\Pr(M=m|s_2),\\ &\textit{for any probabilistic mixtures of states } s_1,\ s_2 \textit{ with a weight } p\in[0,1]\end{aligned} \tag{5.52}$$

This precondition follows by the sum rule of probability and the definition of the conditional probability.[34] In the case of QM, (5.52) can be written as

$$\Pr(M=m \mid p\rho_1+(1-p)\rho_2) = p\Pr(M=m|\rho_1)+(1-p)\Pr(M=m|\rho_2), \tag{5.53}$$

for any density operators $\rho_1, \rho_2 \in \mathcal{S}(\mathcal{H})$ and $p \in [0,1]$. In other words, a real functional $f_m(\rho) := \Pr(M=m\ |\rho)$ $(\rho \in \mathcal{S}(\mathcal{H}))$ on the state space $\mathcal{S}(\mathcal{H})$ for each outcome $m \in \mathcal{M}$ is an **affine** functional. Notice that by Exercise 5.14, any affine functional on $\mathcal{S}(\mathcal{H})$ have the unique linear extension[35] on $\mathcal{L}(\mathcal{H})$. Therefore, the reader can replace the affine property to the linearity in the following discussion.

Preconditions (5.1), (5.2), and (5.52) (or (5.53) in QM) are necessary conditions for a measurement M to be physically valid. To emphasize this fact, we sometimes call a measurement satisfying these conditions an **affine measurement**. Of course, a measurement of a physical quantity (represented by a Hermitian operator) satisfies them. In particular, Precondition (5.2) is given by the Born rule (5.35) and the affine property (5.53) holds because of the linearity of the trace. It is also easy to see that two operations given at the beginning of this section satisfy the conditions. We should notice, however, that at this stage it is far from obvious whether or not all affine measurements can be physically realizable. It turns out that the conditions are also sufficient in QM as we will see in the following. Namely, we will show that any affine measurement can be physically realizable based on Postulates 1–3. This implies that the most general class of measurements in QM is a class of affine measurements.[36]

Before explaining that, we shall start by the mathematical representation of an affine measurement in QM by means of a POVM [4]. A tuple $\{E_m \in \mathcal{L}(\mathcal{H})\}_{m\in\mathcal{M}}$ of linear operators on $\mathcal{H}$ is called a (discrete) **POVM** (**positive operator valued measure** or **probability operator valued measure**) if it satisfies

$$\text{(i) (Positivity)} E_m \geq 0,\ \text{(ii) (Normalization)} \sum_m E_m = I. \tag{5.54}$$

[34] Preparing the state by a probabilistic mixture $\{p, 1-p; s_1, s_2\}$, we have $\Pr(M=m \mid \{p, 1-p; s_1, s_2\}) = \Pr(\text{“}M=m\text{”} \cap s_1) + \Pr(\text{“}M=m\text{”} \cap s_2) = p\Pr(M=m|s_1) + (1-p)\Pr(M=m|s_2)$. (see also the derivation of (5.31)).

[35] Let f be an affine function from a convex subset W of a vector space V to a vector space V'. A linear extension $\tilde{f}$ of f is a linear map from V to V' satisfying $f(w) = \tilde{f}(w)$ for all $w \in W$.

[36] The careful and rigorous consideration was mainly given by Ozawa (see e.g. [7, 8, 10–12] and references therein).

An operator E_m is called a **POVM element**.

Exercise 5.13 Show that a tuple of operators $\{E_1 := 0.4|0\rangle\langle 0|, E_2 := 0.4|+\rangle\langle +|, E_3 := I - E_1 - E_2\}$ on $\mathbb{C}^2$ is a POVM.

We call a measurement M on a quantum system a **POVM measurement** if the measurement probability under a state ρ can be written by

$$\Pr(M = m \,|\rho) = \mathrm{Tr}(E_m \rho), \tag{5.55}$$

using a POVM $\{E_m\}_{m\in\mathcal{M}}$. Note that the right hand side of (5.55) is a probability distribution.[37] Moreover, by the linearity of the trace operation, a POVM measurement is an affine measurement.

Importantly, the converse is also true [8]:

Proposition 5.12 *Any affine measurement is described by a POVM measurement.*

Proof Let M be an arbitrary affine measurement with the set of outcomes $\mathcal{M}$. By the affine property (5.53), a functional $f_m : \mathcal{S}(\mathcal{H}) \to \mathbb{R}$ for each $m \in \mathcal{M}$ given by $f_m(\rho) := \Pr(M = m|\rho)$ is an affine functional on $\mathcal{S}(\mathcal{H})$. Using an ONB $\{|\psi_i\rangle\}_{i=1}^d$ of $\mathcal{H}$ and letting $\tilde{f}_m$ be the linear extension of f_m on $\mathcal{L}(\mathcal{H})$ (see Exercise 5.14), we can define the corresponding POVM element by $E_m := \sum_{k,l} \tilde{f}_m(|\psi_k\rangle\langle\psi_l|)|\psi_l\rangle\langle\psi_k|$. In the following, we show that $\{E_m\}$ satisfies conditions (5.54) and (5.55).

By the linearity of $\tilde{f}_m$ and the completeness condition of $\{|\psi_i\rangle\}$, we have $\mathrm{Tr}(E_m\rho) = \sum_{kl} \tilde{f}_m(|\psi_k\rangle\langle\psi_l|)\langle\psi_k|\rho\psi_l\rangle = f_m((\sum_k |\psi_k\rangle\langle\psi_k|)\rho(\sum_l |\psi_l\rangle\langle\psi_l|)) = f_m(I\rho I) = \Pr(M = m|\rho)$ for any density operator ρ. Therefore, $\{E_m\}$ satisfies (5.55). The application of a pure state $\rho = |\psi\rangle\langle\psi|$ with an arbitrary unit vector $|\psi\rangle$ reads $\langle\psi|E_m\psi\rangle = \mathrm{Tr}\, E_m|\psi\rangle\langle\psi| = \Pr(M = m||\psi\rangle\langle\psi|)$. Therefore, a positivity of a probability implies the positivity of E_m. Moreover, we have $\langle\psi|(\sum_m E_m)\psi\rangle = \sum_m\langle\psi|E_m\psi\rangle = \sum_m \Pr(M = m||\psi\rangle\langle\psi|) = 1 = \langle\psi|\,I\,\psi\rangle$, where in the third equality we have used the normalization condition of a probability. From Proposition A.3-(ii), we obtain $\sum_m E_m = I$. Hence, we have shown that $\{E_m\}$ also satisfies (5.54).

In other words, an affine measurement and a POVM measurement are mathematically equivalent through the (5.55). Therefore, a POVM measurement can represent an affine measurement of QM.

A POVM with all POVM elements being projection operators is called a **PVM** (**projection valued measure**). A measurement with a PVM is called a **PVM measurement**. Notice that a PVM measurement is equivalent to a measurement of a physical quantity (a Hermitian operator) up to measurement outcomes. Indeed, a tuple of eigen-projections $\{P_a\}_{a\in\sigma(A)}$ of a Hermitian operator A is a PVM since $P_a^2 = P_a^\dagger = P_a \geq 0$, and $\sum_a P_a = I$, and the Born rule (5.35) satisfies (5.55). Conversely, any PVM $\{P_m\}_{m\in\mathcal{M}}$ satisfies the orthogonality condition

[37] By the positivity of E_m, we have $\mathrm{Tr}(E_m\rho) = \sum_i q_i\langle\phi_i|E_m\phi_i\rangle \geq 0$, where $\rho = \sum_i q_i|\phi_i\rangle\langle\phi_i|$ is an eigenvalue decomposition of ρ. Also, by the condition $\sum_m E_m = I$, we have $\sum_m \mathrm{Tr}(E_m\rho) = \mathrm{Tr}((\sum_m E_m)\rho) = \mathrm{Tr}\,\rho = 1$.

$P_n P_m = 0$ $(n \neq m)$.[38] Therefore, $\{P_m\}_{m\in\mathcal{M}}$ forms eigen-projections of a Hermitian operator $A = \sum_m m P_m$ by labeling an outcome $m \in \mathcal{M}$ to be real numbers. A PVM measurement $\{|\phi_m\rangle\langle\phi_m|\}_{m=1}^{d}$ with an ONB $\{|\phi_m\rangle\}_{m=1}^{d}$ corresponds to a basis measurement with respect to the basis.

Exercise 5.14 Show that any affine function from the state space $\mathcal{S}(\mathcal{H}) \subset \mathcal{L}(\mathcal{H})$ to a vector space V has the unique linear extension to $\mathcal{L}(\mathcal{H})$.

5.3.2.2 Realization of POVM Measurements

Now we show that any affine measurement (equivalently any POVM measurement) is physical realizable (Theorem 5.2) by means of an indirect measurement.

We first give a mathematical formulation of an indirect measurement. Let ρ be an initial state of the system of interest S. We prepare an **ancilla** system A with the associated Hilbert space $\mathcal{H}_\mathrm{A}$ in an initial state σ so that the total system S + A is in a state $\rho \otimes \sigma$. Then, we let the total system evolve in time by a unitary evolution (5.51)

$$\rho \otimes \sigma \mapsto U(\rho \otimes \sigma)U^\dagger, \tag{5.56}$$

where U is a unitary operator on the total system. Finally, we measure a physical quantity $B = \sum_m m P_m$ on an ancilla system which shall be called a **meter observable**. Using the Born rule (5.35) and Postulate 3, the probability to get an outcome m of the measurement on B under the state (5.56) is given by $\mathrm{Tr}_{\mathrm{SA}}(I_\mathrm{S} \otimes P_m U(\rho \otimes \sigma)U^\dagger)$.

Consequently, if we consider this series of procedures as a measurement M of system S, we have

$$\Pr(M = m|\rho) = \mathrm{Tr}_{\mathrm{SA}}(I_\mathrm{S} \otimes P_m U(\rho \otimes \sigma)U^\dagger). \tag{5.57}$$

An **indirect measurement** on S is thus characterized by a quadruplet $(\mathcal{H}_\mathrm{A}, \sigma, U, B)$, where $\mathcal{H}_\mathrm{A}$ is the associated Hilbert space with an ancilla system A, σ is an initial state of A, U is a unitary time-evolution operator on the total system, and B is a meter observable on the ancilla system.

The probability (5.57) clearly satisfies the affine property (5.53). Therefore, by Proposition 5.12, an indirect measurement is represented by a suitable POVM measurement. Specifically, the POVM element corresponding to the outcome m is shown to be $E_m := \mathrm{Tr}_\mathrm{A}(I_\mathrm{S} \otimes \sigma U^\dagger\, I_\mathrm{S} \otimes P_m U)$: First, from the cyclic property of the trace and Exercise 5.10-(2), (5.57) can be rewritten as

$$\Pr(M = m|\rho) = \mathrm{Tr}_{\mathrm{SA}}((\rho \otimes I_\mathrm{A})(I_\mathrm{S} \otimes \sigma U^\dagger\, I_\mathrm{S} \otimes P_m U)) = \mathrm{Tr}_\mathrm{S}(\rho E_m). \tag{5.58}$$

[38] By $P_m = P_m^2$ and $\sum_n P_n = I$, we have $P_m = P_m I P_m = P_m(\sum_n P_n)P_m = P_m + \sum_{n\neq m} P_m P_n P_m$ for any m, thus $\sum_{n\neq m} P_m P_n P_m = 0$. As the sum of positive operators $P_m P_n P_m$ is zero, we have $P_m P_n P_m = 0$ $(n \neq m)$. Moreover, as $P_m P_n P_m = P_m P_n P_n P_m = (P_n P_m)^\dagger (P_n P_m)$, we obtain $P_n P_m = 0$ for any $n \neq m$. (Show that $A^\dagger A = 0$ implies $A = 0$.)

Next, since a unitary evolution preserves a positivity of an operator,[39] $U^\dagger(I_S \otimes P_m)U$ is positive. By Exercise 5.10-(3), E_m is a positive operator on $\mathcal{H}_S$. Finally, $\sum_m E_m = \mathrm{Tr}_A(I_S \otimes \sigma U^\dagger(I_S \otimes \sum_m P_m)U) = \mathrm{Tr}_A(I_S \otimes \sigma U^\dagger(I_S \otimes I_A)U) = \mathrm{Tr}_A(I_S \otimes \sigma) = I_S$, where we have used the linearity of the partial trace (Exercise 5.10-(4)), the completeness condition of $\{P_m\}$, the unitarity condition $U^\dagger U = I_{SA}$, and the normalization condition $\mathrm{Tr}_A\, \sigma = 1$. Therefore, $\{E_m\}$ is a POVM which represents the indirect measurement (5.57).

We can now state the main result of this part about the realizability of POVM measurements.

Theorem 5.2 *Any POVM measurement can be physically realizable by an indirect measurement.*

Proof Fix an arbitrary POVM $\{E_m\}_{m \in \mathcal{M}}$ on $\mathcal{H}_S$. For the simplicity of a notation, let the set of measurement outcomes be composed of natural numbers $\mathcal{M} = \{1, \ldots, n\}$. From (5.55) and (5.57), we show the existence of an indirect measurement characterized by a quadruplet $(\mathcal{H}_A, \sigma, U, B = \sum_{m=1}^n m P_m)$ satisfying

$$\mathrm{Tr}_S(E_m \rho) = \mathrm{Tr}_{SA}(I_S \otimes P_m(U\rho \otimes \sigma U^\dagger)) \quad \forall m = 1, \ldots, n \tag{5.59}$$

for any initial state $\rho \in \mathcal{S}(\mathcal{H}_S)$. As the equation is linear on ρ, it is enough to show (5.59) for a pure state.

To construct an indirect measurement, we can use any n-dimensional Hilbert space $\mathcal{H}_A$ for an Ancilla system A. With an arbitrary ONB $\{|\phi_j\rangle\}_{j=1}^n$ of $\mathcal{H}_A$, let $\sigma := |\phi_1\rangle\langle\phi_1|$ be an initial state of A and $B := \sum_{m=1}^n m P_m$ with $P_m := |\phi_m\rangle\langle\phi_m|$ be a meter observable on A. The unitary operator for the time evolution is constructed as follows. First, let $W := \{|\xi\rangle \in \mathcal{H}_{SA} \mid \exists |\psi\rangle \in \mathcal{H}_S\, s.t. |\xi\rangle = |\psi\rangle \otimes |\phi_1\rangle\}$ be a subspace of $\mathcal{H}_{SA} := \mathcal{H}_S \otimes \mathcal{H}_A$ and let U be a map from W to $\mathcal{H}_{SA}$ defined by[40]

$$U|\psi\rangle \otimes |\phi_1\rangle := \sum_{j=1}^n |\sqrt{E_j}\psi\rangle \otimes |\phi_j\rangle \;\; (|\psi\rangle \in \mathcal{H}_S). \tag{5.60}$$

As is easily shown,[41] U is a linear map on W preserving an inner product. By Exercise 5.15, there exists a unitary operator U on $\mathcal{H}_{SA}$ which satisfies (5.60).

With the quadruplet $(\mathcal{H}_A, \sigma, U, B = \sum_{m=1}^n m P_m)$, we can show (5.59) for any initial pure state $\rho = |\psi\rangle\langle\psi|$:

$$\mathrm{Tr}_{SA}(I_S \otimes P_m(U\rho \otimes \sigma U^\dagger)) = \mathrm{Tr}_{SA}(I_S \otimes |\phi_m\rangle\langle\phi_m| \left(U|\psi \otimes \phi_1\rangle\langle\psi \otimes \phi_1|U^\dagger\right))$$

[39] For any $A \geq 0$ and any $|\psi\rangle$, we have $\langle\psi|(U^\dagger A U)\psi\rangle = \langle(U\psi)|A(U\psi)\rangle \geq 0$.

[40] For $E \geq 0$ we can define $\sqrt{E} := \sum_e \sqrt{e} P_e$ where $E = \sum_e e P_e$ $(e \geq 0)$ is the spectral decomposition of E. Note that $(\sqrt{E})^\dagger = \sqrt{E} \geq 0$, $(\sqrt{E})^2 = E$.

[41] For any $|\psi\rangle \otimes |\phi_1\rangle, |\psi'\rangle \otimes |\phi_1\rangle \in W$, we have $\langle U(\psi \otimes \phi_1)|U(\psi' \otimes \phi_1)\rangle = \sum_{j,k=1}^n \langle\sqrt{E_j}\psi \otimes \phi_j|\sqrt{E_k}\psi' \otimes \phi_k\rangle = \sum_{j,k=1}^n \langle\psi|\sqrt{E_j}^\dagger\sqrt{E_k}\psi'\rangle\langle\phi_j|\phi_k\rangle = \sum_j \langle\psi|E_j\psi'\rangle = \langle\psi|(\sum_j E_j)\psi'\rangle = \langle\psi|\psi'\rangle$.

$$
\begin{aligned}
&= \sum_{k,l=1}^{n} \mathrm{Tr}_{\mathrm{SA}}(I_{\mathrm{S}} \otimes |\phi_m\rangle\langle\phi_m|(|\sqrt{E_k}\psi \otimes \phi_k\rangle\langle\sqrt{E_l}\psi \otimes \phi_l|)) \\
&= \sum_{k,l=1}^{n} \langle\sqrt{E_k}\psi|\sqrt{E_l}\psi\rangle\delta_{mk}\delta_{ml} = \langle\psi|E_m\psi\rangle = \mathrm{Tr}_{\mathrm{S}}(E_m\rho). \qquad (5.61)
\end{aligned}
$$

□

Exercise 5.15 Let W be a subspace of a Hilbert space $\mathcal{H}$ and let U be a linear map from W to $\mathcal{H}$ which preserves an inner product. Show that U can be linearly extended to a unitary operator on $\mathcal{H}$.

In the preceding section, we have shown that any physically valid measurement is an affine measurement, which is equivalent to a POVM measurement (Proposition 5.12). Theorem 5.2 shows that the converse is also correct. In other words, any POVM measurement can be physically realizable based on Postulates 1–3. Therefore, we conclude that the most general class of measurements of QM is the class of POVM measurement.

To summarize, the rule for the general classes of states and measurements of QM can be described as follows:

[Formulation 1] For any quantum system, there is an associated Hilbert space $\mathcal{H}$ in a way that a state is represented by a density operator and a measurement is represented by a POVM on $\mathcal{H}$. If we measure a POVM $M = \{E_m\}_{m\in\mathcal{M}}$ under a density operator ρ, the probability to observe an outcome $m \in \mathcal{M}$ is given by

$$
\Pr(M = m|\rho) = \mathrm{Tr}(\rho E_m). \qquad (5.62)
$$

The rule for composite systems (Postulate 3) may be replaced as well:

[Formulation 2] Let S_{12} be the composite system of quantum systems S_1 and S_2 with Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, the associated Hilbert space of S_{12} is the tensor product Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

A POVM measurement $\{E_m\}_{m\in\mathcal{M}}$ on S_1 (resp. S_2) is represented by $\{E_m \otimes I_2\}_{m\in\mathcal{M}}$ (resp. $\{I_1 \otimes E_m\}_{m\in\mathcal{M}}$) as a measurement on S_{12}.

5.3.2.3 Simultaneous Measurements

In this part, we investigate a simultaneous measurability of physical quantities in a general setting [6]. According to Proposition 5.2, commutative physical quantities can be simultaneously measurable. We show that the converse is also true. In other words, non-commutative physical quantities cannot be simultaneously measurable.

To see this, let us redefine a simultaneous measurability in terms of POVM measurements. We say that two POVMs $E := \{E_m\}_{m\in\mathcal{M}}$ and $F := \{F_n\}_{n\in\mathcal{N}}$ are simultaneously measurable if there exists a joint POVM $K := \{K_{mn}\}_{m\in\mathcal{M},n\in\mathcal{N}}$ such that under an arbitrary state ρ the marginal probabilities of the joint probability gives correct probabilities of both measurements E and F:

$$\mathrm{Tr}\,\rho E_m = \sum_n \mathrm{Tr}\,\rho K_{mn}, \mathrm{Tr}\,\rho F_n = \sum_m \mathrm{Tr}\,\rho K_{mn}. \tag{5.63}$$

By Proposition A.3-(ii), these conditions are equivalent to

$$E_m = \sum_n K_{mn}, F_n = \sum_m K_{mn}. \tag{5.64}$$

(See also (5.18).)

The following theorem shows the general result on the simultaneous measurability for physical quantities:

Theorem 5.3 *Physical quantities represented by Hermitian operators A and B are simultaneously measurable if and only if they are commutative. In particular, the joint probability distribution is given by*

$$\Pr(A = a, B = b|\rho) = \mathrm{Tr}(\rho P_a Q_b), \tag{5.65}$$

where P_a and Q_b are eigen-projections of A and B belonging to eigenvalues a and b, respectively.

Proof By (5.64), the necessary and sufficient condition for the simultaneous measurability of A and B is that there exists a joint POVM $K = \{K_{ab}\}$ satisfying

$$P_a = \sum_b K_{ab}, Q_b = \sum_a K_{ab}. \tag{5.66}$$

If A and B are commutative, $K_{ab} := P_a Q_b$ provides the joint POVM with which A and B are simultaneously measurable. To see this, note that $[P_a, Q_a] = 0$ for any a and b, and therefore $K_{ab} = P_a Q_b = (P_a Q_b)^\dagger (P_a Q_b)$ is positive. We have also $\sum_{a,b} K_{ab} = (\sum_a P_a)(\sum_b Q_b) = I$. Thus, the set $\{K_{ab}\}_{a,b}$ forms a POVM. The conditions in (5.66) follow as $\sum_b K_{ab} = P_a(\sum_b Q_b) = P_a$ and $\sum_a K_{ab} = (\sum_a P_a)Q_b = Q_b$.

To show the converse, let $\{K_{ab}\}_{a,b}$ be a joint POVM satisfying (5.66). Noting that $K_{ab} \leq P_a$ for any a, b, we have $P_a K_{ab} = K_{ab} P_a = K_{ab}$ by Exercise 5.16. Therefore, from the orthogonality condition $P_a P_{a'} = \delta_{aa'} P_a$, we have $P_a K_{a'b} = P_a P_{a'} K_{a'b} = \delta_{aa'} P_a K_{ab} = \delta_{aa'} K_{ab}$. Similarly, we have $K_{a'b} P_a = \delta_{aa'} K_{ab}$. By (5.66), it follows that $P_a Q_b = P_a(\sum_{a'} K_{a'b}) = (\sum_{a'} \delta_{aa'} K_{ab}) = K_{ab} = (\sum_{a'} K_{a'b}) P_a = Q_b P_a$. Hence, A and B are commutative. Moreover, the joint probability distribution is given by $\mathrm{Tr}\, \rho K_{ab} = \mathrm{Tr}(\rho P_a Q_b)$. □

Finally, we notice that local POVM measurements on different subsystems are simultaneously measurable. Specifically, the joint POVM for the two local POVMs $E = \{E_m\}$ on a system S_1 and $F = \{F_n\}$ on a system S_2 is given by$\{K_{mn} := E_m \otimes F_n\}$. (The reader should check the condition (5.64).) In particular, based on Precondition (5.25), this measurement can be realized by locally measuring E and F so that the joint probability distribution does not depend on the time order of the two measurements E and F.

Exercise 5.16 For any projection operator $P \in \mathcal{L}(\mathcal{H})$ and any positive operator $F \in \mathcal{L}(\mathcal{H})$ satisfying $F \leq P$, show that $PF = FP = F$.

5.3.2.4 State Distinguishability

In this part, we consider a general problem on the **quantum state discrimination**. We say that two states ρ and σ are distinguishable if, under the condition that the state is ρ or σ, there exists a POVM with which we can decide the state with probability 1 in one-time measurement. As shown in Proposition 5.4, orthogonal pure states can be distinguished by one-time measurement of an appropriate physical quantity. One can easily generalize this fact to the case of mixed states by replacing the orthogonality condition of vectors by that of operators. Importantly, the converse is also true:

Proposition 5.13 *Two states ρ and σ are distinguishable if and only if they are orthogonal, i.e., $\rho\sigma = 0$.*

Proof Suppose that ρ and σ are orthogonal. Let $\{P, I - P\}$ be a PVM where P is the projection operator onto the range of ρ. Then, we have $\mathrm{Tr}\, \rho P = 1$, $\mathrm{Tr}\, \sigma P = 0$ and $\mathrm{Tr}\, \rho(I - P) = 0$, $\mathrm{Tr}\, \sigma(I - P) = 1$ since the ranges of ρ and σ are orthogonal. Consequently, one can distinguish ρ and σ by the PVM measurement $\{P, I - P\}$ by guessing the state to be ρ (resp. σ) when the outcome corresponding to P (resp. $I - P$) is observed.

Suppose conversely that ρ and σ are distinguishable. Without loss of generality, we can assume that the two states ρ and σ can be distinguished by a two-valued POVM measurement $\{E_1, E_2\}$ by guessing the true state to be ρ (resp. σ) with observing the outcome 1 (resp. 2).[42] Noting that $\mathrm{Tr}\, \rho E_2 = 0$, $\mathrm{Tr}\, \sigma E_1 = 0$, we have $0 = \rho E_2 = \rho - \rho E_1$ and $0 = E_1 \sigma$ by using Proposition A.10. Therefore, we obtain $\rho\sigma = \rho E_1 \sigma = 0$. □

[42] In general, ρ and σ can be distinguished by the following procedure: First, we perform a POVM measurement $\{F_k\}_{k \in \mathcal{K}}$. Then, we decide whether the true state is ρ or σ from the obtained outcome

It is straightforward to generalize this result to the case of three or more states. One can show that states ρ_i $(i = 1, \ldots, n)$ are distinguishable if and only if they are orthogonal to each other: $\rho_i \rho_j = 0$ $(i \neq j)$.

5.3.3 General Class of Time Evolutions

In this subsection, we discuss the most general class of time evolutions on quantum system. We have already seen that a unitary evolution (5.51) of a density operator is physically realizable based on Postulate 2. However, there is a wider class of time evolutions than a class of a unitary evolution. A typical way to go beyond the unitary evolution of a system S of interest is due to an interaction with another physical system (an environment). In that case, we say that the system S is an open system.

We first discuss the general property (a necessary condition) of a time evolution, and then consider its physical realizability.

5.3.3.1 General Properties of Time Evolution

In this book, we deal with a time evolution by means of a time-evolution map which maps an initial state to a final state. Therefore, we start from a general property for a time-evolution map.

First of all, a time-evolution map should act on a state and map to a state. Mathematically speaking, a time-evolution map of a quantum system A is a map from the state space $\mathcal{S}(\mathcal{H}_{\mathrm{A}})$ to $\mathcal{S}(\mathcal{H}_{\mathrm{A}})$. Notice however that, the image of the map is not necessary the state space of the same quantum system but that of another quantum system B. For instance, consider the situation to observe an electron B by preparing a photon A and scattering with it. In such situation, we are interested in the state-change from a state of A to a state of B after their interaction. Therefore, in the following, we assume generally that a time-evolution map is a map from $\mathcal{S}(\mathcal{H}_{\mathrm{A}})$ to $\mathcal{S}(\mathcal{H}_{\mathrm{B}})$. (The discussion can be easily rephrased to the case where A and B are the same.) With the similar argument to derive (5.53), a time-evolution map Λ also should satisfy the affine property on a state:

$$\Lambda(p\rho + (1-p)\sigma) = p\Lambda(\rho) + (1-p)\Lambda(\sigma), \tag{5.67}$$

(Footnote 42 continued)
$k \in \mathcal{K}$ by using a two-valued decision function $f : \mathcal{K} \to \{1, 2\}$. (One can use a mixed strategy as well, but in this case, it is enough to use a two-valued decision function.) Under a state $\xi = \rho$ or σ, the probability to obtain the final outcome $i = 1, 2$ is given by $\sum_{k; f(k)=i} \mathrm{Tr}(\xi F_k) = \mathrm{Tr}(\xi(\sum_{k; f(k)=i} F_k))$. Therefore, by putting $E_i := \sum_{k; f(k)=1} F_k$ $(i = 1, 2)$, the above procedure can be reduced to the application of the two-valued POVM $\{E_1, E_2\}$. That is, the condition to distinguish the two states ρ and σ is the existence of a POVM $\{E_1, E_2\}$ satisfying that $\mathrm{Tr}\,\rho E_1 = 1, \mathrm{Tr}\,\sigma E_2 = 1$ $(\Leftrightarrow \mathrm{Tr}\,\rho E_2 = 0, \mathrm{Tr}\,\sigma E_1 = 0)$.

for any $\rho, \sigma \in \mathcal{S}(\mathcal{H}_{\mathrm{A}})$ and $p \in [0, 1]$.[43] Notice by Exercise 5.14 that Λ has the unique extension to the linear map Λ' from $\mathcal{L}(\mathcal{H}_{\mathrm{A}})$ to $\mathcal{L}(\mathcal{H}_{\mathrm{B}})$. A linear map $\Lambda' : \mathcal{L}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{L}(\mathcal{H}_{\mathrm{B}})$ is said to be **trace preserving** and **positive** if $\mathrm{Tr}_{\mathrm{A}}(A) = \mathrm{Tr}_{\mathrm{B}}(\Lambda'(A))$ for all $A \in \mathcal{L}(\mathcal{H}_{\mathrm{A}})$ and $\Lambda'(A) \geq 0$ for any positive operator $A \in \mathcal{L}(\mathcal{H}_{\mathrm{A}})$, respectively. Since the image of a time-evolution map Λ is included in $\mathcal{S}(\mathcal{H}_{\mathrm{B}})$, it is easy to see that the linear extension Λ' is a **trace preserving positive map**.[44] In the following, we identify the affine map Λ with its linear extension Λ' by using the same symbol Λ.

To sum up, a general class of time-evolution map of QM is described by a trace preserving positive map Λ from $\mathcal{L}(\mathcal{H}_{\mathrm{A}})$ to $\mathcal{L}(\mathcal{H}_{\mathrm{B}})$. However, by considering a consistency of the description on a composite system, a time-evolution map is shown to satisfy a stronger condition. To understand the condition, we need some mathematical preparations.

With a natural number $n \in \mathbb{N}$, a linear map $\Lambda : \mathcal{L}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{L}(\mathcal{H}_{\mathrm{B}})$ is said to be ***n*-positive** if the extended map $\Lambda \otimes \mathcal{I}_n : \mathcal{L}(\mathcal{H}_{\mathrm{A}} \otimes \mathbb{C}^n) \to \mathcal{L}(\mathcal{H}_{\mathrm{B}} \otimes \mathbb{C}^n)$ is positive where $\mathcal{I}_n$ is the identity map on $\mathcal{L}(\mathbb{C}^n)$. A linear map Λ is said to be **completely positive** if Λ is n-positive for any $n \in \mathbb{N}$. In the following, we call a (trace preserving) completely positive map a **(TP)CP map**. By the definition, a map is positive iff it is 1-positive. It is easy to show that an n-positive map is m-positive if $n \leq m$, but not vice versa. An example of a 1-positive but not 2-positive map is shown in Exercise 7.7 in Chap. 7. The following theorem gives a useful characterization of a CP map:

Theorem 5.4 *Let $\mathcal{H}_{\mathrm{A}}$ and $\mathcal{H}_{\mathrm{B}}$ be Hilbert spaces with dimensions d_{A} and d_{B}, respectively. Let Λ be a linear map from $\mathcal{L}(\mathcal{H}_{\mathrm{A}})$ to $\mathcal{L}(\mathcal{H}_{\mathrm{B}})$. The following are all equivalent:*
(i) Λ *is a CP map,*
(ii) Λ *is a d_{A}-positive map,*
(iii) $\Lambda \otimes \mathcal{I}_{d_{\mathrm{A}}}(|\psi\rangle\langle\psi|) \geq 0$ *where* $|\psi\rangle = \sum_{i=1}^{d_{\mathrm{A}}} |\xi_i\rangle \otimes |\eta_i\rangle$ *with* $\{|\xi_i\rangle\}, \{|\eta_i\rangle\}$ *being ONBs of* $\mathcal{H}_{\mathrm{A}}, \mathbb{C}^{d_{\mathrm{A}}}$,
(iv) *There exist l ($\leq d_{\mathrm{A}}d_{\mathrm{B}}$) linear operators $V_k : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}}$ ($k = 1, \ldots, l$) such that*

$$\Lambda(A) = \sum_{k=1}^{l} V_k A V_k^\dagger \quad (\forall A \in \mathcal{L}(\mathcal{H}_{\mathrm{A}})). \tag{5.68}$$

Proof Proofs for (i) ⇒ (ii) and (ii) ⇒ (iii) follow by definitions of n-positivity and the completely positivity. [(iii) ⇒ (iv)] As $\Lambda \otimes \mathcal{I}_{d_{\mathrm{A}}}(|\psi\rangle\langle\psi|) = \sum_{i,j} \Lambda(|\xi_i\rangle\langle\xi_j|) \otimes |\eta_i\rangle\langle\eta_j|$ is a positive operator on $\mathcal{H}_{\mathrm{B}} \otimes \mathbb{C}^{d_{\mathrm{A}}}$, we can rewrite it by $\sum_{k=1}^{l} |v_k\rangle\langle v_k|$ using $l(\leq d_B d_A)$ vectors $|v_k\rangle \in \mathcal{H}_{\mathrm{B}} \otimes \mathbb{C}^{d_{\mathrm{A}}}$ ($k = 1, \ldots, l$). (One can use an eigenvalue decomposition of $\Lambda \otimes \mathcal{I}_{d_{\mathrm{A}}}(|\psi\rangle\langle\psi|)$ where $|v_k\rangle$ is an eigenvector with its norm being

[43] One can consider the affine property for time-evolution map as one of the preconditions.

[44] Any operator $A \in \mathcal{L}(\mathcal{H}_{\mathrm{A}})$ can be written as $A = \sum_{k=0}^{3} i^k p_k \rho_k$ with non-negative real numbers $p_k \geq 0$ and density operators $\rho_k \in \mathcal{S}(\mathcal{H}_{\mathrm{A}})$ ($k = 0, 1, 2, 3$). (see the solution of Exercise 5.14.) By the linearity of the trace, we have $\mathrm{Tr}_{\mathrm{B}}(\Lambda'(A)) = \sum_k i^k p_k \,\mathrm{Tr}_{\mathrm{B}}(\Lambda(\rho_k)) = \sum_k i^k p_k \,\mathrm{Tr}_{\mathrm{A}}(\rho_k) = \mathrm{Tr}_{\mathrm{A}}(A)$. (Note that $\mathrm{Tr}_{\mathrm{B}}(\Lambda'(\rho_k)) = 1 = \mathrm{Tr}_{\mathrm{A}}(\rho_k)$ since ρ_k and $\Lambda(\rho_k)$ are density operators.) Since any positive operator $A \in \mathcal{L}(\mathcal{H}_{\mathrm{A}})$ can be written as $A = a\rho$ with a non-negative real number $a := \mathrm{Tr}\, A$ and a density operator $\rho := A/a$, we have $\Lambda'(A) = a\Lambda(\rho)$. As $a \geq 0$ and $\mathcal{S}(\mathcal{H}_{\mathrm{B}}) \ni \Lambda(\rho) \geq 0$, $\Lambda'(A)$ is a positive operator.

a square root of positive-definite eigenvalues.) Since $\{|\eta_i\rangle\}$ is an ONB of $\mathbb{C}^{d_\mathrm{A}}$, we can rewrite $|v_k\rangle = \sum_i |v_{ki}\rangle \otimes |\eta_i\rangle$ with some vectors $|v_{ki}\rangle \in \mathcal{H}_\mathrm{B}$. With these expressions, we have $\sum_{i,j} \Lambda(|\xi_i\rangle\langle\xi_j|) \otimes |\eta_i\rangle\langle\eta_j| = \sum_{i,j}(\sum_k |v_{ki}\rangle\langle v_{kj}|) \otimes |\eta_i\rangle\langle\eta_j|$. Since $\{|\eta_i\rangle\langle\eta_j|\}$ are linearly independent, we have $\Lambda(|\xi_i\rangle\langle\xi_j|) = \sum_k |v_{ki}\rangle\langle v_{kj}| = \sum_k V_k|\xi_i\rangle\langle\xi_j|V_k^\dagger$ for any $i, j = 1, \ldots, d_\mathrm{A}$, where $V_k : \mathcal{H}_\mathrm{A} \to \mathcal{H}_\mathrm{B}$ is a linear operator defined by $V_k|\xi_i\rangle := |v_{ki}\rangle$. Since the set $\{|\xi_i\rangle\langle\xi_j|\}$ forms a basis of $\mathcal{L}(\mathcal{H}_\mathrm{A})$, this equation also holds for any $A \in \mathcal{L}(\mathcal{H}_\mathrm{A})$. Therefore, we obtain the representation (5.68) of Λ. [(iv) ⇒ (i)] To see that $\Lambda \otimes \mathcal{I}_n$ is positive for any $n \in \mathbb{N}$ (namely, Λ is completely positive), it is enough to show $\Lambda \otimes \mathcal{I}_n(|\phi\rangle\langle\phi|) \geq 0$ for any $|\phi\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathbb{C}^n$ because of the affine property of $\Lambda \otimes \mathcal{I}_n$ and eigenvalue decompositions of positive operators. Writing $|\phi\rangle = \sum_i |x_i\rangle \otimes |\chi_i\rangle$ with an ONB $\{|\chi_i\rangle\}_{i=1}^n$ of $\mathbb{C}^n$, we have $\Lambda \otimes \mathcal{I}_n(|\phi\rangle\langle\phi|) = \sum_{i,j} \Lambda(|x_i\rangle\langle x_j|) \otimes |\chi_i\rangle\langle\chi_j| = \sum_k V_k \otimes I_n(\sum_{i,j} |x_i\rangle\langle x_j| \otimes |\chi_i\rangle\langle\chi_j|)(V_k \otimes I_n)^\dagger = \sum_k (V_k \otimes I_n)|\phi\rangle\langle\phi|(V_k \otimes I_n)^\dagger$. From the final expression, $\Lambda \otimes \mathcal{I}_n(|\phi\rangle\langle\phi|)$ is clearly a positive operator. □

From Theorem 5.4-(ii), it is enough to show that Λ is d_A-positive in order to show that it is a CP map. That is, it is not necessarily to show that Λ is n-positive for an arbitrary $n \in \mathbb{N}$. Moreover, in order to show that, it is enough to show the positivity of the output state only with the input state $|\psi\rangle\langle\psi|$ (the maximally entangled state), not necessarily with an arbitrary input state. The form (5.68) in (iv) gives a useful representation for a CP map. The TPCP map with this representation is sometimes called **Kraus representation**.

Theorem 5.5 (Kraus Representation) *A linear map* $\Lambda : \mathcal{L}(\mathcal{H}_\mathrm{A}) \to \mathcal{L}(\mathcal{H}_\mathrm{B})$ *is a TPCP map if and only if there exist linear operators* $V_k : \mathcal{H}_\mathrm{A} \to \mathcal{H}_\mathrm{B}$ $(k = 1, \ldots, l \leq d_\mathrm{A}d_\mathrm{B})$ *such that* $\sum_k V_k^\dagger V_k = I_\mathrm{A}$ *and*

$$\Lambda(A) = \sum_{k=1}^{l} V_k A V_k^\dagger \quad (\forall A \in \mathcal{L}(\mathcal{H}_\mathrm{A})). \tag{5.69}$$

Proof From Theorem 5.4-(iv), we can start from the form (5.69) for a CP map. Therefore, we just consider the trace preserving condition. However, from $\mathrm{Tr}_\mathrm{A}\, A = \mathrm{Tr}_\mathrm{B}(\Lambda(A)) = \mathrm{Tr}_\mathrm{B}(\sum_k V_k A V_k^\dagger) = \mathrm{Tr}_\mathrm{A}(\sum_k V_k^\dagger V_k)A$ for any $A \in \mathcal{L}(\mathcal{H}_\mathrm{A})$, the condition is obviously equivalent to $\sum_k V_k^\dagger V_k = I_\mathrm{A}$. □

An operator V_k in the Kraus representation (5.69) is called a **Kraus operator**.

Coming back to physics, it turns out that any time-evolution map should satisfy a completely positivity (CP) condition. One of the simple verifications of this fact comes from the consistency on a composite system as follows [20]: Notice first that in reality there may exist another physical system than the systems A and B. Letting S_n be such an n-level quantum system, a time evolution from system A to B can be also described as a time evolution from the system A + S_n to the system B + S_n. If there are no interactions with S_n, the time-evolution map on the total system is described by $\Lambda \otimes \mathcal{I}_n$. Since $\Lambda \otimes \mathcal{I}_n$ should preserve the positivity on the total system, Λ should also be an n-positive map. Since n is arbitrary, Λ is concluded to be a CP map. Another verification of the CP condition is to notice that a typical realization of a time-evolution map under the presence of an environment is directly shown to be CP (see (5.70) and the discussion below).

In the field of quantum information theory, we generally admit that the trace preserving property and the completely positivity are necessary conditions for any time-evolution map.[45] A unitary evolution (5.51) is a typical TPCP map as the form (5.51) is a Kraus representation because of the unitarity $U^\dagger U = I$.

5.3.3.2 Realization of TPCP Maps

In the preceding part, we have explained that any time-evolution map should be a TPCP map. Here, we show that the converse is also true. Namely, any TPCP map is physically realizable. The fact implies that TPCP maps represent the most general class of time-evolution maps of QM.

A typical way to realize a TPCP map from a system A to a system B is to consider the situation where A and B are not isolated but open systems. Let E be an environment such that the total composite system A + B + E is isolated. Notice that, by Postulate 2, the unitary time evolution can be applied to the total system. Let ρ be an arbitrary initial state of the system A, and let ρ_{B}, ρ_{E} be fixed initial states of the systems B and E such that there are no correlations among the systems A, B, and E. Then, a unitary evolution on the composite system A + B + E is described by

$$\rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}} \mapsto U(\rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}})U^\dagger$$

using a unitary operator U on the total system A+B+E. We are interested in a final state of B and therefore we take a partial trace over the system A + E to obtain the reduced density operator on B. This series of procedures can be interpreted as a time evolution from the initial state $\rho \in \mathcal{S}(\mathcal{H}_{\mathrm{A}})$ of A to the final state $\rho' \in \mathcal{S}(\mathcal{H}_{\mathrm{B}})$ of B, where the time evolution map is given by

$$\rho \mapsto \rho' = \Lambda(\rho) := \mathrm{Tr}_{\mathrm{AE}}\, U(\rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}})U^\dagger. \tag{5.70}$$

This map Λ is shown to be a TPCP map. Indeed, by Exercise 5.18, the map Λ is a composition of three TPCP maps, (i) $\rho \mapsto \rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}}$, (ii) $\sigma \mapsto U\sigma U^\dagger$, and (iii) $\xi \mapsto \mathrm{Tr}_{\mathrm{AE}}\, \xi$. (Notice that a composition of TPCP maps is a TPCP map.)

Based on these considerations, we can show that any TPCP map can be physically realizable:

[45] Note, however, that there is a longstanding argument for the validity of this matter. It is usually discussed with reference to the presence of initial correlations with an environment. However, the root problem includes the validity to deal with a time evolution by means of a map (see [21] and references therein).

Theorem 5.6 (Stinespring representation) *Any TPCP map from a system A to a system B can be physically realizable through* (5.70).

The proof of this theorem will be given as a simple corollary of Theorem 5.7 in Sect. 5.3.4.2 (see also the footnote 49). Note that one can also prove the same result when the systems A and B coincide with each other. In this case, we can use a unitary time evolution on $\mathrm{A}+\mathrm{E}$. By taking a partial trace over E on the final state of $\mathrm{A}+\mathrm{E}$, we get the time-evolution map on the system A described by

$$\rho \mapsto \rho' = \Lambda(\rho) := \mathrm{Tr}_{\mathrm{E}}\, U(\rho \otimes \rho_{\mathrm{E}})U^{\dagger}. \tag{5.71}$$

Then, it follows that any TPCP map $\Lambda : \mathcal{S}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{S}(\mathcal{H}_{\mathrm{A}})$ is physically realizable by a map (5.71).

We have seen that any time-evolution map of a quantum system is a TPCP map and conversely any TPCP map is physically realizable. We can conclude that a TPCP map gives the most general description of a time-evolution map in a quantum system:

[Formulation 3] The general time-evolution map from a quantum system A to a quantum system B is represented by a TPCP map $\Lambda : \mathcal{S}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{S}(\mathcal{H}_{\mathrm{B}})$.

Exercise 5.17 (i) For any $\sigma \in \mathcal{S}(\mathcal{H}_{\mathrm{B}})$, show that $\rho \in \mathcal{L}(\mathcal{H}_{\mathrm{A}}) \mapsto \Lambda(A) := A \otimes \sigma \in \mathcal{L}(\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}})$ is a TPCP map. (ii) Show also that $\rho \in \mathcal{L}(\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}) \mapsto \Lambda(A) := \mathrm{Tr}_{\mathrm{A}}\, A \in \mathcal{L}(\mathcal{H}_{\mathrm{B}})$ is a TPCP map.

5.3.4 General Class of Measurement Processes

As a conclusion of this chapter, we explain the most general description of a measurement process on quantum systems. In Sect. 5.3.2, we have seen that a POVM measurement gives the most general description of a measurement on quantum systems. However, it describes only the probability distribution of the measurement outcome. On the other hand, a **measurement process** is constructed to describe not only a probability distribution but also a state-change due to a measurement. In reading this subsection, the reader should carefully recognize that a state-change in the measurement can be operationally explained based on Postulates 1–3 with some preconditions.[46]

[46] The theory of measurement processes with operational point of view was initiated by Davies and Lewis [22], and completed by Kraus [6] and Ozawa [23] by adding the notion of complete positivity. In particular, a careful consideration of the necessary and sufficient conditions for the description of measurement processes was thoroughly given by Ozawa.

5.3.4.1 Properties of the General Measurement Processes

We start from asking in which case we need to know the post-measurement state. From the operational point of view, it is the case where we have prospects of another subsequent measurement; otherwise it has no meanings to describe the post-measurement state. This view is important to construct the theory of measurement processes. Namely, the post-measurement state is naturally constructed to be a state which can predict the probability of outcomes for the possible subsequent measurements.

Keeping this in mind, we first discuss the general property (a necessary condition) for measurement processes. As is explained in Sect. 5.3.2.1, a measurement is an operation to get an outcome m with a probability $\Pr(M = m|\rho)$ under a state ρ. In the case of measurement process, we also need to determine the post-measurement state ρ_m after getting the specific outcome m. In the same way as in the case of a time evolution, let systems A and B be initial and final systems, including the usual case where A = B. An obvious requirement for the measurement processes is that ρ_m is a quantum state for any output m, i.e., $\rho_m \in \mathcal{S}(\mathcal{H}_{\mathrm{B}})$.

Before going further, notice that there are roughly two classes of measurement processes: In general, the post-measurement state depends on the outcome of the measurement. When we know the measurement outcome m, the state-change can be described by a map

$$\rho \overset{\text{got } m}{\mapsto} \rho_m. \tag{5.72}$$

On the other hand, when we do not know the outcome m but only know the fact of the application of the measurement, the post-measurement state should be described by a probabilistic mixture $\{\Pr(M = m|\rho); \rho_m\}$ with the corresponding density operator being $\sum_{m\in\mathcal{M}} \Pr(M = m|\rho)\rho_m$. In this case, the state-change is described by a map

$$\rho \mapsto \rho' := \sum_{m\in\mathcal{M}} \Pr(M = m|\rho)\rho_m. \tag{5.73}$$

We distinguish these situations by calling the former and latter cases **selective measurement** and **non-selective measurement**, respectively.

As we have already pointed out, the post-measurement state ρ_m after a measurement M should be able to predict a probability $\Pr(N = n|\rho_m)$ for the subsequent measurement N. To know the general property of a measurement process, we focus on the joint probability for a first measurement M and a second measurement N under an initial state ρ

$$\Pr(M = m \to N = n|\rho). \tag{5.74}$$

This series of measurement is called a **successive measurement**. By the arrow → in (5.74), we may indicate that M is the first measurement and N is the subsequent measurement after M. Notice that a successive measurement is different from a simultaneous measurement. In particular, the time order of measurements could be essential in a successive measurement. Namely, $\Pr(M = m \to N = n|\rho)$ and $\Pr(N = n \to M = m|\rho)$ are in general different. Just in the similar manner as in the derivation of (5.53), the joint probability $\Pr(M = m \to N = n|\rho)$ should have the affine property:

$$\begin{aligned}&\Pr(M = m \to N = n|p\rho + (1-p)\sigma)\\ &\quad = p\Pr(M = m \to N = n|\rho) + (1-p)\Pr(M = m \to N = n|\sigma).\end{aligned} \tag{5.75}$$

Moreover, by the definition of the conditional probability, we have

$$\Pr(M = m \to N = n|\rho) = \Pr(M = m|\rho)\Pr(N = n|\rho_m). \tag{5.76}$$

Notice that the second measurement N is considered just in order to determine the post-measurement state. Therefore, we only need the probability distribution of the measurement N, which is described by a POVM measurement $\{E_n\}_{n\in\mathcal{N}}$:

$$\Pr(N = n|\rho_m) = \mathrm{Tr}(E_n\rho_m). \tag{5.77}$$

To describe a measurement process, it is convenient to introduce a map $\Lambda_m : \mathcal{S}(\mathcal{H}_\mathrm{A}) \to \mathcal{L}(\mathcal{H}_\mathrm{B})$ defined by

$$\rho \mapsto \Lambda_m(\rho) = \rho'_m, \tag{5.78}$$

where ρ'_m is an unnormalized post-measurement state:

$$\rho'_m := \Pr(M = m|\rho)\rho_m. \tag{5.79}$$

We usually use the map (5.78) instead of the map (5.72) mainly because that Λ_m has the affine property:

$$\Lambda_m(p\rho + (1-p)\sigma) = p\Lambda_m(\rho) + (1-p)\Lambda_m(\sigma)\ (\forall\rho, \sigma \in \mathcal{S}(\mathcal{H}_\mathrm{A}), p \in [0, 1]).$$

Indeed, by substituting (5.77) and (5.79) into (5.76), we have $\Pr(M = m \to N = n|\rho) = \mathrm{Tr}(E_n\rho'_m) = \mathrm{Tr}(E_n\Lambda_m(\rho))$. Since the joint probability is affine and a POVM $\{E_n\}$ is arbitrary, Λ_m is affine.

Notice that the map Λ_m includes both the information of the probability distribution of the outcomes and the post-measurement state as follows. By (5.79), (5.78) and the normalization condition $\mathrm{Tr}\,\rho_m = 1$, the probability to get an outcome m under a state ρ is given by $\Pr(M = m|\rho) = \mathrm{Tr}\,\Lambda_m(\rho)$. The post-measurement state is also given by $\rho_m = \Lambda_m(\rho)/\,\mathrm{Tr}\,\Lambda_m(\rho)$ from (5.79) and (5.78). Namely, we have

$$\Pr(M = m|\rho) = \mathrm{Tr}\,\Lambda_m(\rho), \tag{5.80a}$$

$$\rho \overset{\text{got } m}{\mapsto} \rho_m = \Lambda_m(\rho)/\,\mathrm{Tr}\,\Lambda_m(\rho). \tag{5.80b}$$

By (5.73), (5.79) and (5.78), the corresponding non-selective measurement is described by the map

$$\Lambda := \sum_{m \in \mathcal{M}} \Lambda_m. \tag{5.81}$$

Using the same argument as in Sect. 5.3.3.1, the linear extensions of the maps Λ_m and Λ to $\mathcal{L}(\mathcal{H}_\mathrm{A})$ should be completely positive. Note that Λ_m does not generally have the trace preserving property while Λ is a TPCP map because $\operatorname{Tr} \Lambda(\rho) = \sum_m \operatorname{Tr} \Lambda_m(\rho) = \sum_m \Pr(M = m|\rho) = 1 = \operatorname{Tr} \rho$.

The tuple of linear maps $\{\Lambda_m\}_{m \in \mathcal{M}}$ on $\mathcal{L}(\mathcal{H}_\mathrm{A})$ is called a **CP instrument** with a set of outcomes $\mathcal{M}$ if Λ_m are CP maps and $\Lambda := \sum_{m \in \mathcal{M}} \Lambda_m$ is a TPCP map. We have seen that any measurement processes can be described by a CP instrument by (5.80).

For any CP instrument $\{\Lambda_m\}_{m \in \mathcal{M}}$, we can apply the Kraus representation (Theorem 5.4-(iv)) to each CP map Λ_m. Let $\{V_k^{(m)}\}_{k=1}^{l_m}$ be the Kraus operators such that $\Lambda_m(A) = \sum_k V_k^{(m)} A V_k^{(m)\dagger}$ $(A \in \mathcal{L}(\mathcal{H}_\mathrm{A}))$. We have $\sum_m (\sum_k V_k^{(m)\dagger} V_k^{(m)}) = I_\mathrm{A}$ by the trace preserving property of $\Lambda = \sum_m \Lambda_m$. As a particular case, let us focus on the case when the Kraus representation of each CP map Λ_m is composed of only one operator V_m (i.e., $l_m = 1$). Then, we have

$$\Lambda_m(A) = V_m A V_m^\dagger, \tag{5.82}$$

with the normalization condition $\sum_m V_m^\dagger V_m = I$. From (5.80), the measurement process is described as

$$\Pr(M = m|\rho) = \operatorname{Tr}(V_m^\dagger V_m \rho), \;\; \rho_m = V_m \rho V_m^\dagger / \operatorname{Tr}(V_m^\dagger V_m \rho). \tag{5.83}$$

We call a tuple of operators $\{V_m\}_{m \in \mathcal{M}}$ a tuple of **measurement operators** if it satisfies $\sum_m V_m^\dagger V_m = I$. In the field of quantum information, it is often postulated that a general class of measurement process is given by measurement operators as (5.83). Indeed, when the set of outcomes is discrete, the formalism of a measurement operator is equivalent to that of a CP instrument up to the discard of a partial information.[47]

Let us introduce some examples of measurement processes. When a set of projection operators $\{P_m\}_m$ on $\mathcal{H}_\mathrm{A}$ satisfies $\sum_m P_m = I$ (i.e., a PVM), the tuple $\{P_m\}_m$ gives measurement operators which describes the measurement process by

$$\Pr(M = m|\rho) = \operatorname{Tr} P_m \rho, \;\; \rho \to \rho_m = P_m \rho P_m / \operatorname{Tr}(P_m \rho). \tag{5.84}$$

[47] Any discrete CP instrument $\{\Lambda_m\}_m$ can be described by measurement operators as follows: Let $\Lambda_m(A) = \sum_{k=1}^{l_m} V_k^{(m)} A V_k^{(m)\dagger}$ be the (Kraus) representation. By $\sum_{m,k} V_k^{(m)\dagger} V_k^{(m)} = I$, we have a tuple $\{V_k^{(m)}\}_{k,m}$ of measurement operators. By performing a non-selective measurement M' of $\{V_k^{(m)}\}_{k,m}$ and outputting only m with discarding k, we obtain (5.80).

This is a generalization of (5.27) to include mixed states, and is called the **Lüders' projective measurement**. In particular, if $P_m = |\phi_m\rangle\langle\phi_m|$ with an ONB $\{|\phi_m\rangle\}_m$ of $\mathcal{H}_\mathrm{A}$, the corresponding measurement process is a generalization of (5.26), and is called the **von Neumanns's projective measurement**.

Letting $\{E_m\}_m$ be a POVM, the tuple of $\{\sqrt{E_m}\}_m$ is that of measurement operators as $\sum_m E_m = \sum_m (\sqrt{E_m})^\dagger(\sqrt{E_m}) = I$ and the corresponding measurement processes is described by

$$\Pr(M = m|\rho) = \mathrm{Tr}\, E_m \rho,\ \ \rho \to \rho_m = \sqrt{E_m}\rho\sqrt{E_m}/\,\mathrm{Tr}(E_m\rho). \tag{5.85}$$

Although this provides a typical measurement process after the POVM measurement of $\{E_m\}_m$, one should be noticed that a post-measurement state is generally not unique. For instance, with an arbitrary unitary operator U, another tuple of $\{U\sqrt{E_m}\}_m$ is a tuple of measurement operators corresponding to the same POVM measurement.[48]

5.3.4.2 Realization of Instruments

In the preceding section, we have seen that any measurement process of a quantum system can be described by a CP instrument. Here, we show that the converse is also true. That is, any CP instrument can be physically realizable as a measurement process. Consequently, we conclude that a CP instrument represent the most general class of measurement processes in a quantum system.

We start from noting that local POVM measurements $E := \{E_m\}_m$ and $F := \{F_n\}_n$ on systems A and B are simultaneously measurable by using the POVM $\{E_n \otimes F_m\}_{n,m}$ on A + B such that the joint probability distribution under a state ρ is given by

$$\Pr(E = m, F = n \mid \rho) = \mathrm{Tr}(\rho E_m \otimes F_n). \tag{5.86}$$

One can easily check the condition (5.64). In particular, the distribution (5.86) is independent of the time order of measurements E and F by Preconditions (5.25). Namely, we have

$$\Pr(E = m, F = n \mid \rho) = \Pr(E = m \to F = n \mid \rho) = \Pr(F = n \to E = m \mid \rho). \tag{5.87}$$

Using the above argument, we can show that the post-measurement state of one subsystem is uniquely determined after the local POVM measurement on another subsystem. This is one of the important tricks why we can describe measurement processes without assuming any postulate:

Proposition 5.14 *On a composite system* A + B, *if we get an outcome n by the local POVM measurement* $F = \{F_n\}_n$ *on the system* B, *the post-measurement (reduced) state of the system* A *is given by* $\rho_n = \mathrm{Tr}_\mathrm{B}(I_\mathrm{A} \otimes F_n\rho)/\,\mathrm{Tr}_\mathrm{AB}(I_\mathrm{A} \otimes F_n\rho)$.

[48] One can construct any CP instrument based on (5.85) assisted by a certain time evolution [24].

Proof In order to determine the post-measurement state of the system A, we consider an arbitrary POVM measurement $E = \{E_m\}_m$ on A under the post-measurement state ρ_n. By the definition of the conditional probability, we have $\Pr(F = n \to E = m|\rho) = \Pr(F = n|\rho)\Pr(E = m|\rho_n) = \mathrm{Tr}_{\mathrm{A}}\left(E_m\rho'_n\right)$ where $\rho'_n := \Pr(F = n|\rho)\rho_n$. On the other hand, by (5.86) and (5.87), we have $\Pr(F = n \to E = m|\rho) = \mathrm{Tr}_{\mathrm{AB}}(E_m \otimes F_n\rho) = \mathrm{Tr}_{\mathrm{A}}\{E_m(\mathrm{Tr}_{\mathrm{B}}\, I_{\mathrm{A}} \otimes F_n\rho)\}$. As POVM $E = \{E_m\}_m$ is arbitrary, we have $\rho'_n = \Pr(F = n|\rho)\rho_n = \mathrm{Tr}_{\mathrm{B}}(I_{\mathrm{A}} \otimes F_n\rho)$. Taking the trace over A gives $\Pr(F = n|\rho) = \mathrm{Tr}_{\mathrm{AB}}(I_{\mathrm{A}} \otimes F_n\rho)$. Thus we obtain $\rho_n = \mathrm{Tr}_{\mathrm{B}}(I_{\mathrm{A}} \otimes F_n\rho)/\,\mathrm{Tr}_{\mathrm{AB}}(I_{\mathrm{A}} \otimes F_n\rho)$.

In order to show the physical realizability of any TPCP map, we consider a measurement process from a system A to another system B in an **indirect measurement** (see Sect. 5.3.2.2). Let E be an ancilla system and let $\rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}}$ be an initial state of the composite system $\mathrm{A} + B + \mathrm{E}$. After letting a unitary time evolution as $\rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}} \to U(\rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}})U^\dagger$, we perform a measurement of a meter observable $X = \sum_m mP_m$ on the system E. From Proposition 5.14, the post-measurement state ρ_m of the system B subject to the measurement outcome m is given by

$$\rho_m = \mathrm{Tr}_{\mathrm{AE}}\{(I_{\mathrm{A}} \otimes I_{\mathrm{B}} \otimes P_m)(U\rho \otimes \rho_{\mathrm{B}} \otimes \rho_{\mathrm{E}}U^\dagger)\}/\,\mathrm{Tr}_{\mathrm{ABE}}\{\cdots\}. \tag{5.88}$$

("$\cdots$" abbreviates the inside of the trace in the numerator.) In the case of A = B, we have

$$\rho_m = \mathrm{Tr}_{\mathrm{E}}\{(I_{\mathrm{A}} \otimes P_m)(U\rho \otimes \rho_{\mathrm{E}}U^\dagger)\}/\,\mathrm{Tr}_{\mathrm{AE}}\{\cdots\}. \tag{5.89}$$

The following theorem gives a physical realization of any CP instrument:

Theorem 5.7 *A measurement process with any CP instrument can be physically realizable by an indirect measurement.*

Proof Let A and B be the initial and final quantum systems with associated Hilbert spaces $\mathcal{H}_{\mathrm{A}}, \mathcal{H}_{\mathrm{B}}$. As any CP instrument can be realized by a tuple of measurement operators with discarding a partial information (see footnote 47), it is enough to show that any measurement process with measurement operators $\{V_m\colon \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}}\}_{m=1}^n$ can be physically realizable by an indirect measurement. For the notational simplicity, we put $\mathcal{M} = \{1, \ldots, n\}$.

We can use an arbitrary n-dimensional system E as an ancilla system. For any ONB $\{|i\rangle\}_{i=1}^n$ of $\mathcal{H}_{\mathrm{E}}$ and unit vectors $|\xi\rangle \in \mathcal{H}_{\mathrm{A}}, |\eta\rangle \in \mathcal{H}_{\mathrm{B}}$, there exists a unitary operator U on $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{E}}$ such that

$$U|\psi\rangle \otimes |\eta\rangle \otimes |1\rangle = \sum_{k=1}^n |\xi\rangle \otimes V_k|\psi\rangle \otimes |k\rangle \ (\forall|\psi\rangle \in \mathcal{H}_{\mathrm{A}}). \tag{5.90}$$

(One can show the existence of such a unitary operator U by using $\sum_m V_m^\dagger V_m = I_{\mathrm{A}}$ and Exercise 5.15).

Using these ingredients, we construct the indirect measurement as follows: Let ρ be an arbitrary initial state of A and let $|\eta\rangle\langle\eta|, |1\rangle\langle 1|$ be the fixed initial states of B and E, respectively. After the unitary time evolution by the unitary operator (5.90), we perform a PVM measurement $\{|m\rangle\langle m|\}_m$ on E. Then, by using (5.88), the post-measurement state of B with the pure input state $\rho = |\psi\rangle\langle\psi| \in \mathcal{S}(\mathcal{H}_{\mathrm{A}})$ is given by

$$\begin{aligned}
&\mathrm{Tr}_{\mathrm{AE}}\{(I_{\mathrm{A}} \otimes I_{\mathrm{B}} \otimes |m\rangle\langle m|)(U|\psi\rangle \otimes |\eta\rangle \otimes |1\rangle\langle\psi| \otimes \langle\eta| \otimes \langle 1|U^\dagger)\} \\
&= \sum_{k,l} \mathrm{Tr}_{\mathrm{AE}}(I_{\mathrm{A}} \otimes I_{\mathrm{B}} \otimes |m\rangle\langle m|)(|\xi\rangle\langle\xi| \otimes V_k|\psi\rangle\langle\psi|V_l^\dagger \otimes |k\rangle\langle l|) \\
&= \sum_{k,l} \langle\xi|\xi\rangle\langle m|k\rangle\langle l|m\rangle V_k|\psi\rangle\langle\psi|V_l^\dagger = V_m|\psi\rangle\langle\psi|V_m^\dagger = \Lambda_m(\rho). \qquad (5.91)
\end{aligned}$$

By the affine property of Λ_m, (5.91) holds for any state $\rho \in \mathcal{S}(\mathcal{H}_{\mathrm{A}})$. We have thus proved that a measurement process by arbitrary measurement operators $\{V_m\}_m$ is realizable by an indirect measurement.[49]

We conclude this chapter by adding the general description of measurement processes to our formulations:

[Formulation 4] A general measurement process of a quantum system is described by a CP-instrument $\{\Lambda_m\}_{m\in\mathcal{M}}$ such that the probability to get an outcome m is given by

$$\Pr(M = m|\rho) = \mathrm{Tr}\,\Lambda_m(\rho), \qquad (5.92)$$

while the post-measurement state is given by

$$\rho \overset{\text{got } m}{\mapsto} \rho_m = \Lambda_m(\rho)/\,\mathrm{Tr}\,\Lambda_m(\rho). \qquad (5.93)$$

References

1. J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932)
2. M. Reed, B. Simon, *Methods of Modern Mathematical Physics I: Functional Analysis* (Academic Press, New York, 1980)
3. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000)
4. C.W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976)

[49] One can use the same proof for Theorem 5.6 by letting a TPCP map represented by $\Lambda(X) = \sum_m V_m X V_m^\dagger$ (Kraus representation). Only the difference is that we don't perform the final measurement $|m\rangle\langle m|$.

5. A.S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982)
6. K. Kraus, *States, Effects, and Operations* (Springer, Berlin, 1983)
7. M. Ozawa, Ann. Phys. **311**, 350–416 (2004)
8. M. Ozawa, Rep. Math. Phys. **18**, 11–28 (1980)
9. P.A.M. Dirac, *The Principles of Quantum Mechanics* (Oxford, New York, 1958)
10. M. Ozawa, in *Quantum Communication, Computing, and Measurement*, ed. by P. Tombesi, O. Hirota (Kluwer, New York, 1997), pp. 233–241
11. M. Ozawa, Ann. Phys. (N.Y.) *259*, 121–137 (1997)
12. M. Ozawa, Fortschr. Phys. *46*, 615–625 (1998)
13. B. d'Espagnat, *Conceptual Foundations of Quantum Mechanics*, 2nd ed., (Addison-Wesley, Boston, 1976)
14. G. Kimura, Phys. Lett. A **314**, 339–349 (2003)
15. G. Kimura, A. Kossakowski, Open Sys. Inf. Dyn. **12**, 207–229 (2005)
16. M. Hayashi ed., *Asymptotic Theory in Quantum Statistical Inference: Selected Papers* (World Scientific, New York, 2005)
17. G. Chiribella, G.M. D'Ariano, P. Perinotti, Phys. Rev. A **84**, 012311 (2011)
18. M. Takesaki, *Theory of Operator Algebra I* (Springer, Berlin, 1979)
19. G. Kimura, S. Tasaki, Bussei Kenkyu **97**, 421–428 (2012)
20. G. Lindblad, Commun. Math. Phys. **40**, 147–151 (1975)
21. G. Kimura, in *Decoherence Suppression in Quantum Systems 2008*, ed. by M. Nakahara, R. Rahimi, A. SaiToh (2008), pp. 1–51
22. E.B. Davies, J.T. Lewis, Comm. Math. Phys. **17**, 239–260 (1970)
23. M. Ozawa, J. Math. Phys. **25**, 79–87 (1984)
24. M. Hayashi, *Quantum Information: An Introduction* (Springer, Berlin, 2006) Originally published in Japanese in 2004

Chapter 6
Information Quantities in Quantum Systems

6.1 Introduction

In this chapter, we introduce several information quantities such as the von Neumann entropy, the quantum relative entropy, the quantum mutual information, and the fidelity, which are utilized in the analysis of quantum information processing. Since it is better to understand classical and quantum information quantities at the same time, the first part of this chapter is devoted to corresponding quantities in classical information theory. We concentrate on various mathematical properties of these quantities in detail before studying quantum information processing treated in the subsequent chapters. Readers who might not feel interested could skip the details of this chapter and come back again according to need. If we understand some fundamental properties of the entropy, typical sequences, and the von Neumann entropy, we can proceed to the next chapter (Chap. 7). In Chap. 8, we utilize some properties of the quantum relative entropy and the Holevo mutual information. In Chap. 9, the trace distance and the entanglement fidelity are used effectively.

Classical information quantities such as the entropy and the mutual information are formulated by Shannon [1, 2]. He gave these quantities a definite and operational meaning by establishing the source coding theorem and the channel coding theorem, which characterize, respectively, the optimal compression rate of data and the optimal transmission rate of message over noisy channels.

Later from 1960s to 1970s, several researchers studied message transmission using carriers obeying the quantum mechanics, because weak power lasers have indispensable quantum mechanical effects and we can not apply the original information theory by Shannon directly. Significant studies in these ages include quantum hypothesis testing (Helstrom [3], Holevo [4], Yuen [5, 6]), quantum estimation theory (Holevo [7], Yuen [5, 6]), and quantum channel coding (Holevo [8, 9]), which laid the foundation of quantum information theory today.

As in the classical case, in quantum information theory it is possible to formulate information processing under quantum mechanics by introducing information quantities appropriately. At the same time, mathematical properties of some infor-

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_6,

mation quantities enable us to study efficiency and possibility (or impossibility) of quantum information processing. It has been made clear by subsequent studies after 1990s what kinds of information quantities are useful. All of quantities introduced in this chapter are standard and known as useful from operational studies in quantum information theory.

For further studies we introduce some textbooks, which were referred to in writing this chapter. As a reference of classical information theory, [10] is known as a standard textbook. We also refereed to [11] for typical sequences. As a textbook of quantum information theory, [12] has an established reputation. The textbook [13] treats various contents from an introduction to advanced topics, and it is useful for the readers of this book to study further developments. Also [14, 15] are known as textbooks which treat quantum information quantities and processing in geometrical view points.

6.2 Information Quantities in Classical Systems

6.2.1 Shannon Entropy

When we throw a dice, we observe the values $X = 1, 2, \ldots, 6$ with probability $1/6$. As in this example, a variable X is called the random variable if it is combined with its probability. Hereafter the range of X, i.e., the set of **root events**, is denoted by $\mathcal{X}$. In the example of a dice, we have $\mathcal{X} = \{1, 2, \ldots, 6\}$. For simplicity $\mathcal{X}$ is supposed to be finite. In the case of discrete random variables, we can identify a random variable X with a probability distribution (or probability mass function) $P : x \in \mathcal{X} \mapsto P(x) \in [0, 1]$ which satisfies the regularity condition $\sum_{x\in\mathcal{X}} P(x) = 1$.

To make the correspondence between random variables and their probability distributions clear, the probability distribution of X is denoted by $P_X(x)$ or $\Pr\{X = x\}$, which is the probability that the random variable X takes a realization x. For another random variable Y, we make difference of probability distributions by the subscript as $P_Y(y) = \Pr\{Y = y\}$. It should be noted that the notation $P_Y(x) = \Pr\{Y = x\}$ $(x \in \mathcal{X})$ is valid if a random variable Y ranges the identical set $\mathcal{X}$ with X. However, it is sometimes useful and simple to distinguish the probability distributions by different characters $P(x)$ and $Q(x)$ in this case. We will use both notations interchangably. Using the subscript notation is useful when many random variables appear.

The joint probability of X and Y is written as $P_{XY}(x, y) = \Pr\{X = x, Y = y\}$. Then the marginal probability distributions are calculated by $P_X(x) = \sum_{y\in\mathcal{Y}} P_{XY}(x, y)$ and $P_Y(y) = \sum_{x\in\mathcal{X}} P_{XY}(x, y)$, respectively.

The **Shannon entropy** is known as the amount of uncertainty of a random variable X, and it quantifies how much knowledge is obtained after the actual value of X is observed. Such meaning has been established rigorously through the source coding theorem by Shannon, as the number of required bits to represent X in a binary

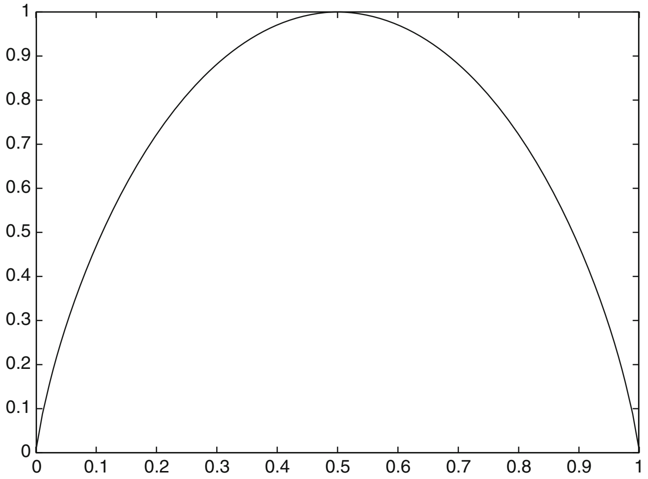


Fig. 6.1 The graph of the binary entropy $h(p)$

sequence. The Shannon entropy of a random variable X on a set $\mathcal{X}$ is defined by

$$H(X) := -\sum_{x\in\mathcal{X}} P_X(x)\log P_X(x). \tag{6.1}$$

Here and hereafter we regard $0\log 0$ as 0 when $P_X(x) = 0$ for some x, since we have $\lim_{t\to 0} t\log t = 0$. Note that $H(X)$ is a functional of the probability distribution P_X, and hence, it is sometimes denote by $H(P_X)$. The Shannon entropy is called the entropy if no confusion with the von Neumann entropy is likely to arise.

If a random variable takes its value in an alternative choice $\mathcal{X} = \{x_1, x_2\}$, then the probability distribution is given by $P_X(x_0) = p$, $P_X(x_1) = 1 - p$, where p is a real number satisfying $0 \le p \le 1$. The entropy in this case is called the **binary entropy** and written as

$$h(p) := -p\log p - (1-p)\log(1-p) \quad (0 \le p \le 1). \tag{6.2}$$

The graph of the binary entropy is shown in Fig. 6.1.

For example, let us imagine the situation in which we want to tell the outcome of coin tossing to people in a distant place. For the coin with the probability $p = 1/2$, we need to send 1 bit of information; 1 for ‘head’ and 0 for ‘tail’. Thus we can say that the random variable of coin tossing has $h(1/2) = 1$ bit of information or uncertainty.

On the other hand in the case $p = 1$, since it is clear that the actual result must be ‘head,’ we do not need to send any information. In other words, the amount of information we should send is $h(1) = 0$ bit. In the same way, in the case $p = 0$, the amount of information is $h(0) = 0$ bit.

In the intermediate case $0 < p < 1$, the entropy takes the value $0 < h(p) < 1$, which quantifies the uncertainty of coin tossing. The meaning of the entropy in this case is explained in the next subsection.

Exercise 6.1 Calculating derivatives $h'(p)$, $h''(p)$, show that $h(p)$ $(0 \leq p \leq 1)$ is a **concave function** (see Sect. A.4) and verify the shape of Fig. 6.1.

Exercise 6.2 Calculate the entropy $H(P)$ for the probability distribution $P(a) = 1/2$, $P(b) = 1/4$, $P(c) = 1/8$, $P(d) = 1/8$.

Let us verify that the entropy $H(X)$ is non-negative in general. Given a random variable X and a real valued function $f : \mathcal{X} \to \mathbb{R}$, since the function $f(X)$ also takes values randomly depending on X, $f(X)$ is considered to be a random variable.[1] In this case, the expectation of $f(X)$ is given by $E[f(X)] = \sum_{x \in \mathcal{X}} P_X(x) f(x)$. Considering the function $f(x) = -\log P_X(x)$, the entropy is expressed in the form of the expectation, i.e., $H(X) = \sum_{x \in \mathcal{X}} P_X(x)\{-\log P_X(x)\}$. Thus it is easy to see that the entropy is non-negative because $f(x)$ is non-negative for $0 \leq P_X(x) \leq 1$.

Further we show the necessary and sufficient condition for $H(X) = 0$. Note that $H(X)$ is obtained by summing non-negative values $P_X(x)\{-\log P_X(x)\}$ over $x \in \mathcal{X}$. Hence $H(X) = 0$ holds if and only if $P_X(x)\{-\log P_X(x)\} = 0$ for all $x \in \mathcal{X}$, which is equivalent to $P_X(x) = 0$ or $P_X(x) = 1$. From the regularity condition of the probability, this condition is equivalent to the existence of $x_0 \in \mathcal{X}$ such that $P_X(x_0) = 1$. These discussions are summarized as the following lemma.

Lemma 6.1 (non-negativity of the entropy) $H(X) \geq 0$ *and the equality holds if and only if there exists* $x_0 \in \mathcal{X}$ *such that* $P_X(x_0) = 1$. *In other words the equality holds if and only if the random variable* X *is deterministic.*

In Sect. 6.2.8, we show that the range of the entropy is $0 \leq H(X) \leq \log |\mathcal{X}|$, and it takes the maximum $H(X) = \log \mathcal{X}$ if and only if $P_X(x) = \frac{1}{|\mathcal{X}|}$ (the uniform distribution on $\mathcal{X}$).

Exercise 6.3 There are 2^n elements of n-bit binary sequences $x_1, x_2, \ldots, x_n$. Conversely how many bits are required to represent all elements of the set $\mathcal{X} = \{1, 2, \ldots, M\}$ in binary sequences?

6.2.2 Entropy and Typical Sequence

In this subsection, to make the meaning of the entropy clear, we introduce the **typical sequence**. For example let us consider coin tossing with the probability p for 'head' and $1 - p$ for 'tail'. Suppose that identical and independent trials for coin tossing are made n times. As for the number of trials n, we imagine a large number such as

[1] Strictly speaking, given a probability space $(\Omega, \mathcal{F}, P)$, a random variable is a function from the sample space Ω to a set $\mathcal{X}$. $f(X)$ is considered to be the composite function $f \circ X$.

$n = 100$ or $n = 1000$. Let 1 and 0 denote 'head' and 'tail' of the coin, respectively. First, we consider the case $p = \frac{2}{3}$ and $n = 12$ for simplicity. Then which sequence is likely to arise among the following?

(1) 111111111111 (2) 101110011101 (3) 000000000000

The probabilities that these sequences arise are, respectively, given by (1) $(2/3)^{12}$, (2) $(2/3)^8(1/3)^4$, (3) $(1/3)^{12}$. Apparently the sequence (1) with all bits 1 has the largest probability. However it should be noted that the expectation of the coin tossing is $1 \times 2/3 + 0 \times 1/3 = 2/3$. If we do not distinguish the order of 1 and 0, it is the most likely to observe "sequences like (2)" that has the frequency of 1 and 0 close to the probability p and $1 - p$. Note that (1) is the only sequence with all bits 1, while the number of "sequences like (2)" is the combination ${}_{12}C_8$, that is, sequences which include 8 bits of '1' and 4 bits of '0.' Summing over the probabilities of these sequences, we have ${}_{12}C_8(2/3)^8(1/3)^4 = 0.23845$, which is much larger than the probability of (1), $(2/3)^{12} = 0.0077073$. Furthermore if the length of the sequence is large enough as $n = 100$ or $n = 1000$, it is shown from **the law of large numbers** that "sequences like (2)" arise almost with probability 1.

Hereafter, following the notation in information theory, we use subscripts to indicate the place in a sequence of random variables $X_1, X_2, \ldots, X_n$ and their actual values $x_1, x_2, \ldots, x_n \in \mathcal{X}$, while we use superscripts to show the combined vectors $X^n = (X_1, X_2, \ldots, X_n)$ and $x^n = (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n$. If $X_1, X_2, \ldots, X_n$ are drawn independently and identically according to a probability distribution P, the joint probability distribution is given by $P_{X^n}(x^n) = P(x_1)P(x_2)\cdots P(x_n)$. In this case, we say that $X^n = (X_1, X_2, \ldots, X_n)$ are **independent and identically distributed** (i.i.d.) subject to P.

For a sequence of real random variables $X^n = (X_1, X_2, \ldots, X_n)$, $S_n := \frac{1}{n}\sum_{i=1}^n X_i$ is called the arithmetic mean. Note that S_n is also a random variable as it is a function of the random variable X^n, and S_n takes its value with probabilistic fluctuations. However, if X^n are drawn independently and identically and the number of trials n is large enough, it is expected that the arithmetic mean S_n takes the value close enough to the expectation $\mu = E[X_1] = E[X_2] = \cdots = E[X_n]$. This fact is stated rigorously as the law of large numbers.

Theorem 6.1 (The weak law of large numbers) *Let $X_1, X_2, \ldots, X_n$ be i.i.d. random variables subject to P. If the variance $V[X_1]$ is finite, it holds that for any $\epsilon > 0$,*

$$\lim_{n\to\infty} \Pr\left\{\left|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu\right| > \epsilon\right\} = 0,$$

where $\mu = E[X_1] = E[X_2] = \cdots = E[X_n]$ is the expectation.

The proof of the theorem is left as an exercise for readers.

Exercise 6.4 Prove the law of large numbers in the following steps.

(1) (**Markov's inequality**) For any non-negative random variable Z and any real number $a > 0$, we have $\Pr\{Z > a\} \leq \frac{E[Z]}{a}$.

(2) (**Chebyshev's inequality**) Let $\mu = E[X]$ be the expectation of a random variable X, and $V[X] = E[(X - \mu)^2]$ be the variance. For any $\epsilon > 0$, we have $\Pr\{|X - \mu| > \epsilon\} \leq \frac{V[X]}{\epsilon^2}$.

(3) For i.i.d. random variables $X_1, X_2, \ldots, X_n$, complete the proof of the law of large numbers by showing that the variance of the arithmetic mean $S_n = \frac{1}{n}\sum_{i=1}^{n} X_i$ is given by $V[S_n] = \frac{V[X_1]}{n}$.

Let us discuss several properties of typical sequences using the law of large numbers. In the example above, it is likely to observe $x^n = (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n$ that has the frequency close to the probability $P(a)$ for any character $a \in \mathcal{X}$, when the sequence of random variable is drawn i.i.d. from P. Here let $\delta_a(x)$ be the function (Kronecker's delta) which takes the value 1 for $x = a$ and 0 otherwise. Then we can calculate the frequency of the character a in a sequence x^n by $P_{x^n}(a) := \frac{1}{n}\sum_{i=1}^{n} \delta_a(x_i)$. The frequency $P_{x^n}(a)$ is called the empirical distribution in statistics and the type in information theory. Note that $P_{X^n}(x^n)$ and $P_{x^n}(a)$ have different meanings; $P_{X^n}(x^n)$ is the probability that the sequence x^n arises while $P_{x^n}(a)$ is the empirical distribution for a single character a in the sequence x^n.

A sequence $x^n \in \mathcal{X}^n$ is called strong typical if the empirical distribution $P_{x^n}(a)$ and the probability $P(a)$ are close enough for any character $a \in \mathcal{X}$. Precisely speaking, for any fixed $\epsilon > 0$, the set of strong typical sequences is defined by

$$B_{n,\epsilon} := \left\{x^n \in \mathcal{X}^n | \forall a \in \mathcal{X},\ |P_{x^n}(a) - P(a)| \leq \epsilon P(a)\right\}.$$

Noting that $P(a) = 0 \Rightarrow P_{x^n}(a) = 0$ if $x^n \in B_{n,\epsilon}$, we can see that the character a with $P(a) = 0$ never appears in the sequence $x^n = (x_1, x_2, \ldots, x_n) \in B_{n,\epsilon}$. Since $E[\delta_a(X_i)] = P(a)$ $(i = 1, 2, \ldots, n)$, we can show from the law of large numbers that the event $B_{n,\epsilon}$ happens almost with probability 1 for sufficiently large n.

$$\begin{aligned}\Pr\{B_{n,\epsilon}^c\} &= \Pr\left\{\exists a \in \mathcal{X},\ \left|\frac{1}{n}\sum_{i=1}^{n}\delta_a(X_i) - P(a)\right| > \epsilon P(a)\right\} \\ &\leq \sum_{a\in\mathcal{X}} \Pr\left\{\left|\frac{1}{n}\sum_{i=1}^{n}\delta_a(X_i) - P(a)\right| > \epsilon P(a)\right\} \xrightarrow{(n\to\infty)} 0,\end{aligned} \tag{6.3}$$

where we have used the fact that the finite sum and the limit can be exchanged, the weak law of large numbers,[2] and

$$\Pr\left\{\left|\frac{1}{n}\sum_{i=1}^{n}\delta_a(X_i) - P(a)\right| > \epsilon P(a)\right\} = \Pr\left\{\frac{1}{n}\sum_{i=1}^{n}\delta_a(X_i) > 0\right\} = 0$$

when $P(a) = 0$.

[2] Note that $V[\delta_a(X_i)] = P(a)\{1 - P(a)\} < \infty$.

In elementary discussions in classical and quantum information theory, we often use a rather weak form of the definition for typical sequences. Let $X^n = (X_1, X_2, \ldots, X_n)$ be independently and identically distributed according to P. Then $-\log P(X_i)$ $(i = 1, 2, \ldots, n)$ is also i.i.d. random variables with the expectation $E[-\log P(X_i)] = H(P)$. Let us define a subset of $\mathcal{X}^n$ for a fixed $\epsilon > 0$ by

$$A_{n,\epsilon} = \left\{ x^n \in \mathcal{X}^n \,\middle|\, \left| -\frac{1}{n} \log P_{X^n}(x^n) - H(P) \right| \leq \epsilon \right\}. \tag{6.4}$$

Since we have $-\frac{1}{n} \log P_{X^n}(x^n) = -\frac{1}{n} \sum_{i=1}^{n} \log P(x_i)$, the weak law of large numbers yields $\Pr\{A_{n,\epsilon}\} \xrightarrow{n\to\infty} 1$. An element of $A_{n,\epsilon}$ is called a weak typical sequence with respect to P. We often call weak typical sequences as typical sequences when no confusion is likely to arise.

Exercise 6.5 Show that a strong typical sequence is a weak typical sequence by the following steps.

(1) For a sequence $x^n \in B_{n,\epsilon}$, we have

$$-\frac{1}{n} \sum_{i=1}^{n} \log P(x_i) = -\sum_{a \in \mathcal{X}} P_{x^n}(a) \log P(a).$$

(2) Show that $x^n \in B_{n,\epsilon} \Rightarrow x^n \in A_{n,\epsilon'}$, where we put

$$M := \max_{a : P(a) \neq 0} \{-\log P(a)\}, \quad \epsilon' := M\epsilon.$$

Theorem 6.2 *We have the following properties for the* ***typical sequence****.*
(i) For any $\epsilon > 0$*, we have* $\lim_{n\to\infty} \Pr\{A_{n,\epsilon}\} = 1$
(ii) $x^n \in A_{n,\epsilon} \Leftrightarrow 2^{-n(H(X)+\epsilon)} \leq P_{X^n}(x^n) \leq 2^{-n(H(X)-\epsilon)}$
(iii) $|A_{n,\epsilon}| \leq 2^{n(H(X)+\epsilon)}$
(iv) For any $\epsilon > 0$ *and any* $\delta > 0$*, we have* $(1-\delta)2^{n(H(X)-\epsilon)} \leq |A_{n,\epsilon}|$ *for any sufficiently large* n*.*

The property (i) states that the typical set has the probability 1, which was already shown as a result of the law of large numbers. The property (ii) is just an equivalent modification of the definition of the weak typicality, and (ii) states that each element in the typical set is equally probable and $P_{X^n}(x^n) \simeq 2^{-n(H(X)\pm\epsilon)}$.[3] Combining (iii) and (iv), we can see that $|A_{n,\epsilon}| \simeq 2^{n(H(X)\pm\epsilon)}$ for the number of elements of the typical set. These properties show that, in the asymptotic regime $n \to \infty$, equally probable elements with the probability almost $2^{-nH(X)}$ is combined together to be the probability 1, which is called the **asymptotic equipartition property, AEP**.

[3] It should be noted that sequences in $A_{n,\epsilon}$ have considerably different probabilities with different exponents within $\pm\epsilon$. The statement means just the expression for the exponents.

For the proof of the theorem, it is enough to show (iii) and (iv). Since the probability of the subset $A_{n,\epsilon}$ is always less than 1, it holds from (ii) that $1 \geq \sum_{x^n \in A_{n,\epsilon}} P^n(x^n) \geq |A_{n,\epsilon}| \cdot 2^{-n(H(X)+\epsilon)}$. Multiplying the both sides by $2^{n(H(X)+\epsilon)}$, we obtain (iii). From (i), for any $\delta > 0$ and for any sufficiently large n, we have $\Pr\{A_{n,\epsilon}\} \geq 1 - \delta$. Hence using (ii), we obtain $1 - \delta \leq \sum_{x^n \in A_{n,\epsilon}} P^n(x^n) \leq |A_{n,\epsilon}| \cdot 2^{-n(H(X)-\epsilon)}$. Multiplying the both sides by $2^{n(H(X)-\epsilon)}$ leads to (iv).

Example 6.1 Let us consider coin tossing treated in the previous subsection, in which the probability of the head is given by $0 \leq p \leq 1$. If we toss the identical coin n times, how many binary bits are required to send the outcome to people in a distant place with almost zero error probability. If n is large enough, an element in the typical set $A_{n,\epsilon}$ arises with equal probability. Since $|A_{n,\epsilon}| \simeq 2^{nh(p)}$, by encoding each element of the typical set in $\log |A_{n,\epsilon}| \simeq nh(p)$ bits, we can tell the result with almost zero error. By this encoding scheme, we can send the outcome using $nh(p)$ bits, which is $h(p)$ bits per one coin, while just sending the outcome requires n bits.

6.2.3 Joint Entropy and Conditional Entropy

For a pair of random variable (X, Y) on the product set $\mathcal{X} \times \mathcal{Y}$, the **joint entropy** is given by

$$H(X, Y) = -\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P_{X,Y}(x, y) \log P_{X,Y}(x, y), \tag{6.5}$$

which is obtained by applying the definition of the entropy to the **joint distribution** $P_{XY}(x, y)$. Given the joint distribution $P_{XY}(x, y)$, we can calculate the **marginal distribution** $P_X(x) = \sum_{y\in\mathcal{Y}} P_{XY}(x, y)$ and the **conditional probability distribution** $P_{Y|X}(y|x) = P_{XY}(x, y)/P_X(x)$ (see the footnote 18, page 94). In the following, $P_{Y|X}(y|x)$ is written as $P(y|x)$ if no confusion is likely to arise from the context.

For a fixed x, we can calculate the entropy of $P(\cdot|x)$ corresponding to Y, which is denoted by $H(Y|x) := H(P(\cdot|x))$. Then the **conditional entropy** is defined as the expectation of $H(Y|x)$ by $P_X(x)$:

$$H(Y|X) := \sum_{x\in\mathcal{X}} P_X(x) H(Y|x). \tag{6.6}$$

The following lemma would be obvious from the definition above and non-negativity of the entropy (Lemma 6.1).

Lemma 6.2 (non-negativity of the conditional entropy) $H(Y|X) \geq 0$ *and equality holds if and only if, for any x with $P_X(x) > 0$, Y can be decided deterministically depending on x. That is to say, Y is a function of X.*

As a relation between the entropy and the conditional entropy, the **chain rule** holds:

$$H(X, Y) = H(X) + H(Y|X). \tag{6.7}$$

The proof of the chain rule is left as an exercise for readers.

Exercise 6.6 Show the chain rule in the following steps.

(1) Show that the conditional entropy is written as an expectation in the following form.

$$H(Y|X) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{XY}(x, y)\log P_{Y|X}(y|x).$$

(2) From $P_{XY}(x, y) = P_X(x)P_{Y|X}(y|x)$, we have

$$-\log P_{XY}(x, y) = -\log P_X(x) - \log P_{Y|X}(y|x).$$

Show the chain rule by taking the expectation under the distribution $P_{XY}(x, y)$ in the both sides.

6.2.4 Conditional Probability and Classical Channel

In this subsection, we introduce the concept of **classical channel** by which a noise or data processing is represented. Then in the next subsection, we study the monotonicity of the divergence with respect to classical channels. If no confusion is likely to arise, the classical channel is merely called the channel in this chapter. In Sect. 5.3.3, we have studied that the **TPCP map** is the concept representing a quantum mechanical noise or information processing to change quantum states. Therefore a TPCP map is sometimes called a **quantum channel** or a **quantum operation**. A classical channel is considered as a restriction of a TPCP map to the classical system.

A **conditional probability distribution** $W(y|x)$ ($x \in \mathcal{X}$, $y \in \mathcal{Y}$) from the set $\mathcal{X}$ to the set $\mathcal{Y}$ is defined by a function satisfying $0 \le W(y|x) \le 1$ ($\forall y \in \mathcal{Y}$) and $\sum_{y\in\mathcal{Y}} W(y|x) = 1$ for all $x \in \mathcal{X}$. In other words, it is a probability distribution depending on each $x \in \mathcal{X}$. A conditional probability $W(y|x)$ is called a channel, since it represents the probabilistic input/output relation that the output character $y \in \mathcal{Y}$ is obtained with probability $W(y|x)$ depending on the input $x \in \mathcal{X}$.

If the probability distribution $P(x)$ and the channel $W(y|x)$ are given, we can define the joint probability by $P_{XY}(x, y) = P(x)W(y|x)$, and the marginal probability is calculated as $P_Y(y) = \sum_{x\in\mathcal{X}} P(x)W(y|x)$. Since it is determined depending on $P(x)$, we denote this probability distribution by $\Lambda(P)(y) := \sum_{x\in\mathcal{X}} P(x)W(y|x)$. Thus using the channel W, we can define the map:

$$\Lambda : P \in \mathcal{P}(\mathcal{X}) \mapsto \Lambda(P) = \sum_{x\in\mathcal{X}} P(x)W(\cdot|x) \in \mathcal{P}(\mathcal{Y}), \tag{6.8}$$

where $\mathcal{P}(\mathcal{X})$ and $\mathcal{P}(\mathcal{Y})$ are the sets of probability distributions on $\mathcal{X}$ and $\mathcal{Y}$, respectively. It is easy to see that the map is positive (1-positive) and **affine**, i.e., $\Lambda(tP_1+(1-t)P_2)=t\Lambda(P_1)+(1-t)\Lambda(P_2),\ 0\le t\le 1$. Conversely, an affine and positive map Γ from $\mathcal{P}(\mathcal{X})$ to $\mathcal{P}(\mathcal{Y})$ is considered to be a channel. Indeed, let $\delta_a(x)$ be a probability distribution taking the value 1 on $x=a$ (i.e., Kronecker's delta). Then we can see that $W(y|a)=\Gamma(\delta_a)(y)$ is a conditional probability. Therefore we can identify the conditional probability $W(y|x)$ with the map (6.8) that is affine, positive, and probability preserving (corresponding to trace preserving). In the following, both concepts are called the channel. Especially, Λ is called **Markov map**, and it is sometimes written as Λ_W to show the explicit relation with $W(y|x)$.

As a special case, a map $f:\mathcal{X}\to\mathcal{Y}$ is regarded as a deterministic channel $W_f(y|x):=\delta_{f(x)}(y)$ (Kronecker's delta), which outputs $f(x)\in\mathcal{Y}$ deterministically depending on the input $x\in\mathcal{X}$. For a probability distribution P on $\mathcal{X}$, we have

$$\Lambda_{W_f}(P)(y)=\sum_{x\in\mathcal{X}}P(x)W_f(y|x)=\sum_{x:\,y=f(x)}P(x). \tag{6.9}$$

Hence the channel W_f acts as a coarse graining if the map $f:\mathcal{X}\to\mathcal{Y}$ is not injective.

It is also shown that the operation to derive the marginal distribution from a joint distribution $P(x,y)$ is a channel. Indeed, let us consider the map $f:(x,y)\longmapsto x$, which takes only x from the pair (x,y). Then we have the corresponding conditional probability $W_f(x'|x,y):=\delta_{f(x,y)}(x')$. Using (6.9) we obtain

$$\Lambda_{W_f}(P)(x')=\sum_{(x,y)}P(x,y)W_f(x'|x,y)=\sum_{(x,y)}P(x,y)\delta_x(x')=\sum_{y}P(x',y),$$

from which we can see that the channel W_f derives the marginal distribution.

Finally we will show that the operation to give a probabilistic combination is again a channel. Let $P_1(x),P_2(x),\dots,P_N(x)$ $(x\in\mathcal{X})$ be probability distributions on $\mathcal{X}$. Given a probability distribution $\pi=(\pi_1,\pi_2,\dots,\pi_N)$ on the indices $i=1,2,\dots,N$, we can define the joint distribution $P(i,x):=\pi_iP_i(x)$ for the pair (i,x). Then the marginal distribution for x, $\sum_{i=1}^N P(i,x)=\sum_{i=1}^N\pi_iP_i(x)=:P_\pi(x)$, is a probability distribution on $\mathcal{X}$. We write the probability distribution as $P_\pi=\sum_{i=1}^N\pi_iP_i$, which is called the probabilistic combination of P_i by π. The probabilistic combination gives the marginal distribution for $x\in\mathcal{X}$ when we can not obtain the information about the index $i=1,2,\dots,N$.

6.2.5 Divergence

We sometimes use the phrase that two data are similar or distant. In mathematical treatment in information theory, we suppose that there are underlying probability distributions from which these data are drawn. The **divergence** is a measure of distance between two probability distributions. For probability distributions $P(x)$, $Q(x)$, the divergence is defined by

$$D(P||Q) := \sum_{x\in\mathcal{X}} P(x)\log\frac{P(x)}{Q(x)}. \tag{6.10}$$

Remark 6.1 We make the following agreement to treat 0 in the function $s\log\frac{s}{t}$. This remark may be skipped over at the first time of reading.

(a) If $t > 0$, $0\log\frac{0}{t} = \lim_{s\to 0} s\log\frac{s}{t} = 0$. (b) If $s > 0$, $s\log\frac{s}{0} = \lim_{t\to 0} s\log\frac{s}{t} = +\infty$. (c) When $(s,t) \to (0,0)$, the limit of $s\log\frac{s}{t}$ can not be decided. In this case, we treat the element x satisfying $P(x) = Q(x) = 0$ as excluded from $\mathcal{X}$ and make the agreement that $0\log\frac{0}{0} = 0$.

Note that, when $Q(x) = 0$ for some x, the divergence is finite if and only if $P(x) = 0$. Thus we have $D(P||Q) < \infty \Leftrightarrow \text{supp}\, P \subset \text{supp}\, Q$, where for a function $f(x)$, $\text{supp}\, f$ is the **support** of f and defined by $\text{supp}\, f := \{x \in \mathcal{X} \mid f(x) \neq 0\}$.

The divergence is not a genuine distance satisfying the axiom of distance given in Definition A.2, because it is an asymmetric functional of probability distributions. However it is useful to regard the divergence as a kind of distance in information theory and statistics. We can give the divergence an operational meaning as a measure of distinguishability through the theory of hypothesis testing. Also it is possible to understand many properties of the entropy and the mutual information as those of the divergence. As the name divergence is commonly used in information theory, it is called the relative entropy in statistical mechanics, and Kulback-Leibler information in mathematical statistics, respectively. The divergence has the following properties.

Lemma 6.3 (properties of the divergence)
(i) ***non-negativity****:* $D(P||Q) \geq 0$ *(equality holds if and only if* $P = Q$*)*
(ii) ***monotonicity****: For any channel* Λ*, it holds that*

$$D(P||Q) \geq D(\Lambda(P)||\Lambda(Q)), \tag{6.11}$$

where the equality holds if and only if there exists a channel Γ *such that* $\Gamma(\Lambda(P)) = P$, $\Gamma(\Lambda(Q)) = Q$.
(iii) ***joint convexity****: For any probability distributions* P_1, P_2, Q_1, Q_2 *and any real number* $0 \leq t \leq 1$*, we have*

$$t\,D(P_1||Q_1) + (1-t)D(P_2||Q_2) \geq D\left(tP_1 + (1-t)P_2||t\,Q_1 + (1-t)\,Q_2\right). \tag{6.12}$$

(iv) ***additivity****: If* $P_{X_1Y_1}(x,y) = P_{X_1}(x)P_{Y_1}(y)$ *and* $P_{X_2Y_2}(x,y) = P_{X_2}(x)P_{Y_2}(y)$*, then*

$$D(P_{X_1Y_1}||P_{X_2Y_2}) = D(P_{X_1}||P_{X_2}) + D(P_{Y_1}||P_{Y_2}). \tag{6.13}$$

The additivity (iv) is easily shown by a direct calculation. The proofs of the other properties are given as those of the f-divergence in the next subsection. The property (ii) is called the **monotonicity** with respect to channels, and a similar inequality also holds for the mutual information (Sect. 6.2.7). The divergence and the mutual information have rigorous and operational meanings, that is, the divergence represents distinguishability, and the mutual information represents the message transmission rate. It is natural that under noise or data processing these operational quantities never get better but get worse in general, which is the meaning of the monotonicity inequality. From these reasons, the monotonicity is also called the **data processing inequality**. Also in quantum systems, various information quantities satisfy the monotonicity with respect to the **quantum channel** (TPCP map).

Exercise 6.7 Show the additivity of the divergence (iv).

6.2.6 f-Divergence

For each **convex function** f, we can define an information quantity so called the f-**divergence** [16], which constitutes a family of information quantities including the divergence and other important quantities. Various properties of the divergence presented in the previous subsection are proved here as those of the f-divergences.

For a **convex function** $f : J \subset \mathbb{R} \to \mathbb{R}$ (see Appendix A.4) the f-divergence is defined by

$$D_f(P||Q) := \sum_{x\in\mathcal{X}} P(x) f\left(\frac{Q(x)}{P(x)}\right), \tag{6.14}$$

where we treat 0 which occurs in $P(x)$ or $Q(x)$ in the same way as Remark 6.1. For example, if $f(t) = -\log t$, we have

$$D_f(P||Q) = -\sum_{x\in\mathcal{X}} P(x)\log\frac{Q(x)}{P(x)} = \sum_{x\in\mathcal{X}} P(x)\log\frac{P(x)}{Q(x)}, \tag{6.15}$$

which is nothing but the divergence $D(P||Q)$.

Theorem 6.3 (Monotonicity of the f-divergence) *For any probability distributions $P(x)$, $Q(x)$ $(x \in \mathcal{X})$ and any channel $W(y|x)$ $(x \in \mathcal{X},\ y \in \mathcal{Y})$, we have*

$$D_f(P||Q) \geq D_f(\Lambda_W(P)||\Lambda_W(Q)). \tag{6.16}$$

In the case that f is a ***strictly convex function****, the equality holds if and only if there exists a channel $V(x|y)$ such that $\Lambda_V(\Lambda_W(P)) = P$ and $\Lambda_V(\Lambda_W(Q)) = Q$.*

Proof Define joint distributions depending on P, Q by $P_{X_1Y_1}(x, y) = P(x)W(y|x)$ and $P_{X_2Y_2}(x, y) = Q(x)W(y|x)$. Then we have

$$\begin{aligned} D_f(P_{X_1Y_1}\|P_{X_2Y_2}) &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P(x)W(y|x) f\left(\frac{Q(x)W(y|x)}{P(x)W(y|x)}\right) \\ &= \sum_{x\in\mathcal{X}} P(x) \sum_{y\in\mathcal{Y}} W(y|x) f\left(\frac{Q(x)}{P(x)}\right) = \sum_{x\in\mathcal{X}} P(x) f\left(\frac{Q(x)}{P(x)}\right) \\ &= D_f(P\|Q). \end{aligned} \tag{6.17}$$

On the other hand, we can rewrite the joint distributions using conditional probabilities in the opposite direction as $P_{X_1Y_1}(x,y) = P_{Y_1}(y)P_{X_1|Y_1}(x|y)$, $P_{X_2Y_2}(x,y) = P_{Y_2}(y)P_{X_2|Y_2}(x|y)$. Applying Jensen's inequality (A.31) to the convex function f, we obtain (6.16) as follows.

$$\begin{aligned} D_f(P\|Q) &= D_f(P_{X_1Y_1}\|P_{X_2Y_2}) \\ &= \sum_{y\in\mathcal{Y}} P_{Y_1}(y) \sum_{x\in\mathcal{X}} P_{X_1|Y_1}(x|y) f\left(\frac{P_{Y_2}(y)P_{X_2|Y_2}(x|y)}{P_{Y_1}(y)P_{X_1|Y_1}(x|y)}\right) \\ &\geq \sum_{y\in\mathcal{Y}} P_{Y_1}(y) f\left(\sum_{x\in\mathcal{X}} P_{X_1|Y_1}(x|y) \frac{P_{Y_2}(y)P_{X_2|Y_2}(x|y)}{P_{Y_1}(y)P_{X_1|Y_1}(x|y)}\right) \\ &= \sum_{y\in\mathcal{Y}} P_{Y_1}(y) f\left(\frac{\sum_{x\in\mathcal{X}} P_{Y_2}(y)P_{X_2|Y_2}(x|y)}{P_{Y_1}(y)}\right) \\ &= \sum_{y\in\mathcal{Y}} P_{Y_1}(y) f\left(\frac{P_{Y_2}(y)}{P_{Y_1}(y)}\right) = D_f(\Lambda_W(P)\|\Lambda_W(Q)). \end{aligned} \tag{6.18}$$

Next we show the condition for the equality. Suppose that there exists a channel $V(x|y)$ such that $\Lambda_V(\Lambda_W(P)) = P$, $\Lambda_V(\Lambda_W(Q)) = Q$. Applying (6.18) twice which has already been proved, we can show the equality in (6.16).

$$\begin{aligned} D_f(P\|Q) &\geq D_f(\Lambda_W(P)\|\Lambda_W(Q)) \\ &\geq D_f(\Lambda_V(\Lambda_W(P))\|\Lambda_V(\Lambda_W(Q))) = D_f(P\|Q). \end{aligned}$$

If $f(t)$ is strictly convex, the equality in (6.18) holds only if arguments of the function are the same in each inequalities for any y.[4] Thus there exists a constant $C(y)$ such that for all x

$$\frac{P_{Y_2}(y)P_{X_2|Y_2}(x|y)}{P_{Y_1}(y)P_{X_1|Y_1}(x|y)} = \frac{P_{Y_2}(y)}{P_{Y_1}(y)} = C(y) \tag{6.19}$$

holds, from which we have $\frac{P_{X_2|Y_2}(x|y)}{P_{X_1|Y_1}(x|y)} = 1$. Let $V(x|y) = P_{X_1|Y_1}(x|y) = P_{X_2|Y_2}(x|y)$, then we obtain $\Lambda_V(\Lambda_W(P)) = P$, $\Lambda_V(\Lambda_W(Q)) = Q$. □

[4] Strictly speaking, we should discuss the case, that $P_{Y_1}(y)$ or $P_{X_1|Y_1}(x|y)$ might be 0, carefully in the same way as Remark 6.1.

Corollary 6.1 (non-negativity of the f -divergence) *$D_f(P||Q) \geq f(1)$ holds. If f is a **strictly convex function**, the equality holds if and only if $P = Q$. Especially when $f(1) = 0$, we have $D_f(P||Q) \geq 0$.*

Proof As a special case of Markov map, let Λ_0 be a map which outputs a certain probability P_0 for any input distribution. Then, since $\Lambda_0(P) = \Lambda_0(Q) = P_0$, the monotonicity of the f-divergence yields

$$D_f(P||Q) \geq D_f(\Lambda_0(P)||\Lambda_0(Q)) = f(1). \tag{6.20}$$

Concerning the condition for the equality, if $P = Q$ then it clearly holds that $D_f(P||Q) = f(1)$. Conversely when f is a strictly convex function, $D_f(P||Q) = f(1)$ implies the existence of a Markov map Γ satisfying $P = \Gamma(\Lambda_0(P)) = \Gamma(P_0)$ and $Q = \Gamma(\Lambda_0(Q)) = \Gamma(P_0)$, which means $P = Q$. □

Theorem 6.4 (joint convexity of the f -divergence) *Let $P_i(x)$, $Q_i(x)$ ($i = 1, 2, \ldots, N$) be probability distributions on $\mathcal{X}$ and $\pi = (\pi_1, \pi_2, \ldots, \pi_N)$ be a probability distribution on the set of indices $\{1, 2, \ldots, N\}$. Let $\sum_{i=1}^N \pi_i P_i$ and $\sum_{i=1}^N \pi_i Q_i$ be stochastic mixtures. Then we have*

$$\sum_{i=1}^N \pi_i D_f(P_i||Q_i) \geq D_f\left(\sum_{i=1}^N \pi_i P_i \middle\| \sum_{i=1}^N \pi_i Q_i\right). \tag{6.21}$$

*Especially, the f-divergence is a **convex function** with respect to one argument when the other argument is fixed, i.e.,*

$$\sum_{i=1}^N \pi_i D_f(P_i||Q) \geq D_f\left(\sum_{i=1}^N \pi_i P_i \middle\| Q\right), \tag{6.22}$$

$$\sum_{i=1}^N \pi_i D_f(P||Q_i) \geq D_f\left(P \middle\| \sum_{i=1}^N \pi_i Q_i\right). \tag{6.23}$$

Proof As described in Sect. 6.2.4, $P(i, x) := \pi_i P_i(x)$ and $Q(i, x) := \pi_i Q_i(x)$ are joint distributions on $\{1, 2, \ldots, N\} \times \mathcal{X}$, and $P(x) = \sum_{i=1}^N \pi_i P_i(x)$ and $Q(x) = \sum_{i=1}^N \pi_i Q_i(x)$ are marginal distributions. Then the f-divergence between $P(i, x)$ and $Q(i, x)$ is calculated as follows.

$$\begin{aligned} D_f(P||Q) &= \sum_{i=1}^N \sum_{x\in\mathcal{X}} \pi_i P_i(x) f\left(\frac{\pi_i Q_i(x)}{\pi_i P_i(x)}\right) = \sum_{i=1}^N \pi_i \sum_{x\in\mathcal{X}} P_i(x) f\left(\frac{Q_i(x)}{P_i(x)}\right) \\ &= \sum_{i=1}^N \pi_i D_f(P_i||Q_i), \end{aligned} \tag{6.24}$$

which is the left hand side of (6.21). On the other hand, the right hand side of (6.21) is the f-divergence between $P(x)$ and $Q(x)$. Since the data processing to take the marginal distribution is a classical channel, the assertion follows from the monotonicity of the f-divergence. □

6.2.7 *Mutual Information*

For a pair of random variables (X, Y), the **mutual information** is defined by

$$I(X;Y) := \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_{XY}(x,y)\log\frac{P_{XY}(x,y)}{P_X(x)P_Y(y)}, \tag{6.25}$$

which is the divergence between the joint distribution $P_{XY}(x, y)$ and the product of marginal distributions $P_X(x) = \sum_{y\in\mathcal{Y}} P_{XY}(x, y)$ and $P_Y(y) = \sum_{x\in\mathcal{X}} P_{XY}(x, y)$. The mutual information is a measure of correlation between X and Y as a distance of the joint random variable from the independent case. It follows from non-negativity of the divergence that $I(X;Y) \geq 0$ and that the equality holds if and only if $P_{XY}(x, y) = P_X(x)P_Y(y)$ for $\forall x, \forall y$ (X and Y are independent random variables). Various representations for the mutual information are known as follows:

$$I(X;Y) = H(X) + H(Y) - H(X,Y), \tag{6.26}$$

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X), \tag{6.27}$$

$$I(X;Y) = \sum_{x\in\mathcal{X}} P_X(x)D(P_{Y|X}(\cdot\,|x)||P_Y). \tag{6.28}$$

From (6.27), we can say that the mutual information is a measure of the reduction in uncertainty of the random variable X by knowing the other random variable Y. In Sect. 6.3.3, we show that the expressions (6.27) and (6.28) correspond directly to those for the Holevo mutual information.

Exercise 6.8 Show (6.26) and (6.27).

We can show the representation (6.28) using $P_{XY}(x, y) = P_X(x)P_{Y|X}(y|x)$ as

$$\begin{aligned} I(X;Y) &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} P_X(x)P_{Y|X}(y|x)\log\frac{P_X(x)P_{Y|X}(y|x)}{P_X(x)P_Y(y)} \\ &= \sum_{x\in\mathcal{X}} P_X(x)D(P_{Y|X}(\cdot\,|x)||P_Y). \end{aligned} \tag{6.29}$$

In the following, we show a proof for the monotonicity of the mutual information. Among several ways to prove the monotonicity, we employ a method using the

conditional mutual information and the **chain rule** of the mutual information, which would be comprehensible for readers.

For random variables (X, Y, Z), the conditional probability $P_{XZ|Y}(x, z|y)$ gives the joint distribution of X and Z for a fixed y. Thus we can calculate the mutual information depending on each realization y.

$$I(X; Z|y) := \sum_{x \in \mathcal{X}} \sum_{z \in \mathcal{Z}} P_{XZ|Y}(x, z|y) \log \frac{P_{XZ|Y}(x, z|y)}{P_{X|Y}(x|y) P_{Z|Y}(z|y)}. \tag{6.30}$$

The conditional mutual information is defined by taking the expectation with respect to y:

$$I(X; Z|Y) := \sum_{y \in \mathcal{Y}} P_Y(y) I(X; Z|y). \tag{6.31}$$

It would be clear from non-negativity of the mutual information that $I(X; Z|Y) \geq 0$ and that the equality holds if and only if $P_{XZ|Y}(x, z|y) = P_{X|Y}(x|y) P_{Z|Y}(z|y)$ $(\forall x, \forall z)$ holds for any y satisfying $P_Y(y) > 0$. If the above equality condition holds, we say that X, Y, and Z form a **Markov chain**, which is denoted by $X \to Y \to Z$. This condition is equivalent to

$$P_{XYZ}(x, y, z) = P_Y(y) P_{XZ|Y}(x, z|y) = P_Y(y) P_{X|Y}(x|y) P_{Z|Y}(z|y). \tag{6.32}$$

Moreover noting that $P_Y(y) P_{X|Y}(x|y) = P_{XY}(x, y) = P_X(x) P_{Y|X}(y|x)$, we can obtain the following equivalent condition.

$$P_{XYZ}(x, y, z) = P_X(x) P_{Y|X}(y|x) P_{Z|Y}(z|y). \tag{6.33}$$

The last condition means that X, Y, and Z are connected in this order by Markov maps, which gives the origins of the name of "Markov chain" and the notation $X \to Y \to Z$. On the other hand, the condition (6.32) means that X and Z are independent when a realization of Y is known. Obviously this condition is symmetric for X and Z, and hence, it is sometimes denoted by $X \leftrightarrow Y \leftrightarrow Z$.

In the same way as the entropy, the **chain rule** of the mutual information holds, that is,

$$I(X; YZ) = I(X; Y) + I(X; Z|Y). \tag{6.34}$$

We show a proof of the monotonicity of the mutual information based on the chain rule.

Exercise 6.9 Show the chain rule of mutual information by (6.27).

Theorem 6.5 (Monotonicity of the mutual information) *If $X \to Y \to Z$, we have*

$$I(X; Y) \geq I(X; Z). \tag{6.35}$$

The equality holds if and only if $X \to Z \to Y$.

Proof From the assumption $X \to Y \to Z$, we have $I(X;Z|Y) = 0$. Thus from the **chain rule** of the mutual information,

$$I(X;YZ) = I(X;Y) + I(X;Z|Y) = I(X;Y) \tag{6.36}$$

holds. On the other hand, from the chain rule again and non-negativity of the conditional mutual information, we have

$$I(X;YZ) = I(X;Z) + I(X;Y|Z) \geq I(X;Z). \tag{6.37}$$

Combining (6.36) and (6.37), we obtain $I(X;Y) \geq I(X;Z)$ and the equality holds if and only if $I(X;Y|Z) = 0$, which is equivalent to the condition $X \to Z \to Y$. □

6.2.8 Concavity and Subadditivity of the Entropy

In this subsection, we derive several important properties of the entropy from those of the divergence and the mutual information. A random variable U is called the uniform random variable on a finite set $\mathcal{X}$ if the corresponding probability distribution is the uniform distribution $P_U(x) = \frac{1}{|\mathcal{X}|}$ $(x \in \mathcal{X})$. Let X be a random variable on $\mathcal{X}$. Then a direct calculation yields

$$D(P_X||P_U) = \sum_{x\in\mathcal{X}} P_X(x) \log \frac{P_X(x)}{1/|\mathcal{X}|} = \log|\mathcal{X}| - H(X) \geq 0, \tag{6.38}$$

where we used non-negativity of the divergence (Lemma 6.3 (i)). From this relation, we have $H(X) \leq \log|\mathcal{X}|$ and the equality holds if and only if X is the uniform random variable. On the other hand, using non-negativity of the mutual information and (6.26) and (6.27), we have

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y) \geq 0,$$

which leads to

$$H(X) \geq H(X|Y), \tag{6.39}$$

$$H(X) + H(Y) \geq H(X,Y). \tag{6.40}$$

The equality holds in the both inequalities if and only if $I(X;Y) = 0$, i.e., X and Y are independent. The inequality (6.40) is called subadditivity of the entropy. The inequality (6.39) means that conditioning reduces the entropy, which is natural from the meaning of the entropy, a measure of uncertainty. Rewriting (6.39) into a different notation, we can show the concavity of the entropy (see Sect. A.4):

$$H\left(\sum_{i=1}^{N}\pi_i P_i\right) \geq \sum_{i=1}^{N}\pi_i H(P_i). \tag{6.41}$$

Indeed, let us define a joint distribution by $P_{XY}(i,x) = \pi_i P_i(x)$, then the marginal distribution of X is given by $P_X(x) = \sum_i \pi_i P_i(x)$ and the conditional probability is given by $P_{X|Y}(x|i) = P_i(x)$. Applying (6.39) to this case, we obtain (6.41).

6.2.9 Fano Inequality

In this subsection, we introduce **Fano inequality**, which is utilized in Chaps. 8 and 9 related to the converse part of channel coding and the security analysis. Let us consider a typical situation that a noise changes a random variable X to another random variable Y according to the conditional probability distribution $W(y|x)$. We are interested in the problem of estimating X through Y. Let $\hat{X}$ be the estimation of X. Since $\hat{X}$ should depend only on Y, these random variables form Markov chain. Let $P_e = \Pr\{X \neq \hat{X}\}$ be the error probability of estimation. Then the error probability is related to the conditional entropy.

Theorem 6.6 (Fano inequality) *Let X and $\hat{X}$ be random variables on $\mathcal{X}$, and Y be a random variable on $\mathcal{Y}$. Suppose that these random variables form Markov chain $X \to Y \to \hat{X}$. Let $P_e = \Pr\{X \neq \hat{X}\}$, then we have*

$$h(P_e) + P_e \log|\mathcal{X}| \geq H(X|\hat{X}) \geq H(X|Y). \tag{6.42}$$

Especially if $P_e = 0$ then $H(X|Y) = 0$.

Proof Let us define a random variable E taking the value 1 if $\hat{X} = X$ (correct) and 0 if $\hat{X} \neq X$ (incorrect), namely, $E = \delta_X(\hat{X})$ (Kronecker's delta). Applying the **chain rule** to $H(E, X|\hat{X})$ in two ways, we have

$$H(E,X|\hat{X}) = H(X|\hat{X}) + H(E|\hat{X},X) = H(E|\hat{X}) + H(X|\hat{X},E). \tag{6.43}$$

By the definition of E, since X and $\hat{X}$ determine E without uncertainty, we have $H(E|\hat{X},X) = 0$. Hence using $P_e = \Pr\{E = 0\}$, we obtain

$$\begin{aligned} H(X|\hat{X}) &= H(E|\hat{X}) + H(X|\hat{X},E) \\ &= H(E|\hat{X}) + \Pr\{E=1\}H(X|\hat{X},E=1) + \Pr\{E=0\}H(X|\hat{X},E=0) \\ &\leq H(E) + (1-P_e)\cdot 0 + P_e \cdot \log|\mathcal{X}| \\ &= h(P_e) + P_e \cdot \log|\mathcal{X}|, \end{aligned} \tag{6.44}$$

which asserts the first part of (6.42). The second part $H(X|\hat{X}) \geq H(X|Y)$ follows from the monotonicity of the mutual information as

$$H(X) - H(X|Y) = I(X;Y) \geq I(X;\hat{X}) = H(X) - H(X|\hat{X}). \qquad \square$$

Exercise 6.10 Using Fano inequality (6.42), show that

$$H(X) \leq \log|\mathcal{X}|(1 - P(X = x)) + h(1 - P(X = x)) \tag{6.45}$$

for any $x \in \mathcal{X}$.

6.3 Information Quantities in Quantum Systems

6.3.1 von Neumann Entropy

We introduce the **von Neumann entropy** as a counterpart of the Shannon entropy in quantum systems. For this purpose, the function $f(A)$ of Hermitian operators A plays an important role; see Sect. A.3.7. We will also use the following identity for unitary operators U:

$$f(UAU^{\dagger}) = Uf(A)U^{\dagger}, \tag{6.46}$$

which is shown in (A.23) in Appendix A.3.7. The von Neumann entropy for a density operator ρ is defined by

$$H(\rho) := -\operatorname{Tr}\rho\log\rho. \tag{6.47}$$

Using **eigenvalue decomposition** (see Corollary A.1), the density operator ρ is written as $\rho = \sum_{k=1}^{\dim\mathcal{H}} \lambda_k |\phi_k\rangle\langle\phi_k|$, where λ_k $(k = 1, 2, \ldots, \dim\mathcal{H})$ are eigenvalues and $|\phi_k\rangle$ are corresponding eigenvectors. By the definition of the function of operators, we have

$$-\rho\log\rho = -\sum_{k=1}^{\dim\mathcal{H}} \lambda_k \log\lambda_k |\phi_k\rangle\langle\phi_k|, \tag{6.48}$$

which leads to $H(\rho) = -\sum_{k=1}^{\dim\mathcal{H}} \lambda_k \log\lambda_k$ by taking the trace of the both sides. Thus we have verified that the von Neumann entropy of a density operator ρ is nothing but the Shannon entropy of the probability distribution composed of eigenvalues of ρ. Note that, if an eigenvalue has the multiplicity, it should be listed as many times as the multiplicity in the probability distribution, so that the sum of the probability is to be 1. We show several basic properties of the von Neumann entropy.

Lemma 6.4 (properties of the von Neumann entropy)

(i) ***non-negativity****:* $H(\rho) \geq 0$ *with the equality if and only if* ρ *is a pure state.*
(ii) $H(\rho) \leq \log\dim\mathcal{H}$ *with the equality if and only if* $\rho = \frac{1}{\dim\mathcal{H}}$.
(iii) If a density operator $\rho_{\mathrm{AB}} \in \mathcal{S}(\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}})$ *in a bipartite system is a pure state, the von Neumann entropies of reduced density operators coincide, i.e., for* $\rho_{\mathrm{A}} = \operatorname{Tr}_{\mathrm{B}} \rho_{\mathrm{AB}}$ *and* $\rho_{\mathrm{B}} = \operatorname{Tr}_{\mathrm{A}} A\rho_{\mathrm{AB}}$ *we have* $H(\rho_{\mathrm{A}}) = H(\rho_{\mathrm{B}})$.

(iv) ***additivity***: $H(\rho_A \otimes \rho_B) = H(\rho_A) + H(\rho_B)$.

(v) ***unitary invariance***: *For any unitary operator* U, $H(U\rho U^\dagger) = H(\rho)$ *holds.*

Later, in Sect. 6.3.4, we will study subadditivity and **concavity** of the von Neumann entropy. Let us verify the above properties. Non-negativity (i) obviously follows from the corresponding property of the Shannon entropy. From Lemma 6.1 for the Shannon entropy, the equality holds if and only if there exists an eigenvalue 1 (consequently the other eigenvalues are 0), which means that ρ is a pure state. In the same way, (ii) easily follows from the corresponding property of the Shannon entropy. To prove (iii), we consider the **Schmidt decomposition** (Theorem A.4 in Appendix) for a pure state $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$:

$$|\psi_{AB}\rangle = \sum_k \sqrt{\lambda_k}|e_k\rangle \otimes |f_k\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \tag{6.49}$$

where $\{|e_k\rangle\}$ and $\{|f_k\rangle\}$ are orthogonal normal (orthonormal) bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. By this representation, we can calculate the partial trace of ρ_{AB} as $\rho_A = \sum_k \lambda_k|e_k\rangle\langle e_k|$ and $\rho_B = \sum_k \lambda_k|f_k\rangle\langle f_k|$, from which we can see that eigenvalues of ρ_A and ρ_B coincide. Since $H(\rho_A)$ and $H(\rho_B)$ are the Shannon entropy of the probability distribution $\{\lambda_k\}$, we have (iii). To show the additivity (iv), we will calculate $\log(\rho_A \otimes \rho_B)$. For ρ_A and ρ_B, let $\rho_A = \sum_i \lambda_{A,i} E_{A,i}$ and $\rho_B = \sum_j \lambda_{B,j} E_{B,j}$ be spectral decompositions (Theorem A.3 in Appendix), respectively. Then the spectral decomposition of $\rho_A \otimes \rho_B$ is given by $\rho_A \otimes \rho_B = \sum_i \sum_j \lambda_{A,i}\lambda_{B,j} E_{A,i} \otimes E_{B,j}$. Thus we have

$$\begin{aligned}\log(\rho_A \otimes \rho_B) &= \sum_i \sum_j \log(\lambda_{A,i}\lambda_{B,j}) E_{A,i} \otimes E_{B,j} \\ &= \sum_i \sum_j \log \lambda_{A,i} E_{A,i} \otimes E_{B,j} + \sum_i \sum_j \log \lambda_{B,j} E_{A,i} \otimes E_{B,j} \\ &= \log \rho_A \otimes I_B + I_A \otimes \log \rho_B.\end{aligned} \tag{6.50}$$

Multiplying the both sides by $-\rho_A \otimes \rho_B$ and taking the trace, we obtain (iv). As for the unitary invariance (v), applying (6.46) to the function $f(x) = -x \log x$, we have

$$H(U\rho U^\dagger) = \mathrm{Tr}\, f(U\rho U^\dagger) = \mathrm{Tr}\, Uf(\rho)U^\dagger = \mathrm{Tr}\, f(\rho)U^\dagger U = \mathrm{Tr}\, f(\rho) = H(\rho).$$

For a bipartite state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the **conditional von Neumann entropy** is defined by

$$H_{\rho_{AB}}(A|B) := H(\rho_{AB}) - H(\rho_B), \tag{6.51}$$

so that the **chain rule** holds as in the classical case. It is remarkable that the conditional entropy in quantum systems can be negative while it is always non-negative in classical systems. For example, a bipartite pure state (6.49) has the von Neumann entropy $H(\rho_{AB}) = 0$, whereas $H_{\rho_{AB}}(A|B) = -H(\rho_B) \le 0$.

6.3.2 Quantum Relative Entropy

The **quantum relative entropy** corresponds to the divergence in classical systems, and it is a measure of distinguishability or discrimination. It is sometimes called the Umegaki entropy [17]. For density operators ρ and σ, the quantum relative entropy is defined by

$$D(\rho||\sigma) := \operatorname{Tr} \rho \, (\log \rho - \log \sigma). \tag{6.52}$$

As in the classical case, since the quantum relative entropy is not symmetric with respect to ρ and σ, we can not qualify it as a mathematical distance. However, through the theory of quantum hypothesis testing (Chap. 8), we can give the quantum relative entropy a rigorous meaning as a measure of distinguishability or discrimination. Also various counterparts of the mutual information in quantum systems are regarded as special cases of the quantum relative entropy.

In quantum systems, a quantum noise or operation is represented by an input/output system described by a **TPCP map**, which we call a **quantum channel** throughout this chapter. In the same way as the divergence (Lemma 6.3 (ii)), the quantum relative entropy satisfies the monotonicity with respect to quantum channels.

Theorem 6.7 (Monotonicity of the quantum relative entropy [18, 19]) *For any density operators ρ and σ and for any quantum channel (TPCP map) Λ, we have*

$$D(\rho||\sigma) \geq D(\Lambda(\rho)||\Lambda(\sigma)). \tag{6.53}$$

The equality holds if a quantum channel Γ in the reverse direction such that $\Gamma(\Lambda(\rho)) = \rho$ and $\Gamma(\Lambda(\sigma)) = \sigma$.

We omit the proof here, because it seems beyond an introduction. Among several proofs known so far, the proof based on the quantum f-divergence (quasi-entropy) [20–22] is a quantum extension of the idea based on the classical f-divergence (see Sect. 6.2.6), which leads to the monotonicity of various information quantities in quantum systems in a unified manner. As in the classical case, various properties of the quantum relative entropy are derived from the monotonicity, including the necessary and sufficient condition for the equality. Therefore let us proceed to the following discussions first with accepting the monotonicity. The monotonicity of the quantum relative entropy includes the monotonicity related to quantum measurements as a special case. For density operators ρ, σ, and a measurement (POVM) $E = \{E_x\}$, we can define the probability distributions of the measurement outcomes $P(x) = \operatorname{Tr} \rho E_x$ and $Q(x) = \operatorname{Tr} \sigma E_x$. Then the classical divergence between them is written as $D_E(\rho||\sigma) := \sum_x P(x) \{\log P(x) - \log Q(x)\}$. Note that for a fixed measurement $E = \{E_x\}$, the map $\rho \longmapsto \{\operatorname{Tr} \rho E_x\}_x$ from a density operator to the probability distribution is a quantum channel, and hence, it follows from the monotonicity that $D(\rho||\sigma) \geq D_E(\rho||\sigma)$. Here it is known [22] that there exists a measurement which achieves the equality if and only if ρ and σ commute.

Lemma 6.5 (properties of the quantum relative entropy)

(i) ***non-negativity***: $D(\rho||\sigma) \geq 0$ *with the equality if and only if* $\rho = \sigma$.
(ii) ***unitary invariance***: *For any unitary operator* U, *it holds that* $D(U\rho U^\dagger||U\sigma U^\dagger) = D(\rho||\sigma)$.
(iii) ***additivity***: $D(\rho_\mathrm{A} \otimes \rho_\mathrm{B}||\sigma_\mathrm{A} \otimes \sigma_\mathrm{B}) = D(\rho_\mathrm{A}||\sigma_\mathrm{A}) + D(\rho_\mathrm{B}||\sigma_\mathrm{B})$
(iv) ***joint convexity***: *For any* $\rho_1, \rho_2, \sigma_1, \sigma_2 \in \mathcal{S}(\mathcal{H})$ *and any* $0 \leq t \leq 1$,
$tD(\rho_1||\sigma_1) + (1-t)D(\rho_2||\sigma_2) \geq D(t\rho_1 + (1-t)\rho_2||t\sigma_1 + (1-t)\sigma_2)$.

First we show the non-negativity (i) from the monotonicity (Theorem 6.7). Let Λ be a quantum channel that outputs a certain state ρ_0 for any input. Then from the monotonicity (6.53) we have $D(\rho||\sigma) \geq D(\Lambda(\rho)||\Lambda(\sigma)) = D(\rho_0||\rho_0) = 0$, which asserts (i). As for the condition for the equality, the relation $\rho = \sigma$ obviously implies $D(\rho||\sigma) = 0$. Conversely suppose that $D(\rho||\sigma) = 0$. From the equality condition of the monotonicity, there exists a quantum channel Γ such that $\rho = \Gamma(\Lambda(\rho)) = \Gamma(\rho_0)$ and $\sigma = \Gamma(\Lambda(\sigma)) = \Gamma(\rho_0)$, which implies $\rho = \sigma$. The unitary invariance (ii) and the additivity (iii) can be shown by using (6.46) and (6.50), respectively, in the same way as the von Neumann entropy.

Exercise 6.11 Show the unitary invariance (ii) and the additivity (iii).

Next let us prove the joint convexity (iv). For density operators $\rho_1, \rho_2, \sigma_1, \sigma_2$ and a real number $0 \leq t \leq 1$, let us define block diagonal matrices by

$$R := \begin{pmatrix} t\rho_1 & 0 \\ 0 & (1-t)\rho_2 \end{pmatrix}, \quad S := \begin{pmatrix} t\sigma_1 & 0 \\ 0 & (1-t)\sigma_2 \end{pmatrix}, \tag{6.54}$$

which turn out to be density operators. The difference of the logarithm of these operators is calculated as follows.

$$\begin{aligned} \log R - \log S &= \begin{pmatrix} \log(t\rho_1) & 0 \\ 0 & \log((1-t)\rho_2) \end{pmatrix} - \begin{pmatrix} \log(t\sigma_1) & 0 \\ 0 & \log((1-t)\sigma_2) \end{pmatrix} \\ &= \begin{pmatrix} \log\rho_1 - \log\sigma_1 & 0 \\ 0 & \log\rho_2 - \log\sigma_2 \end{pmatrix}, \end{aligned} \tag{6.55}$$

where the terms $\log t$ and $\log(1-t)$ were canceled in the last equality because $\log(t\rho_1) = (\log t)\, I + \log\rho_1$ holds from (6.50). Thus we can calculate $D(R||S)$ as follows.

$$\begin{aligned} D(R||S) &= \mathrm{Tr}\, R(\log R - \log S) \\ &= t\, \mathrm{Tr}\, \rho_1 \,(\log\rho_1 - \log\sigma_1) + (1-t)\, \mathrm{Tr}\, \rho_2 \,(\log\rho_2 - \log\sigma_2) \\ &= tD(\rho_1||\sigma_1) + (1-t)D(\rho_2||\sigma_2), \end{aligned} \tag{6.56}$$

which is the left hand side of (iv). On the other hand, taking the sum of the block diagonal parts, we can define the following map:

$$\Lambda : \begin{pmatrix} A & B \\ C & D \end{pmatrix} \longmapsto A + D, \tag{6.57}$$

which is **TPCP map** (**quantum channel**). Applying this map, we have $\Lambda(R) = t\rho_1 + (1-t)\rho_2$ and $\Lambda(S) = t\sigma_1 + (1-t)\sigma_2$, and the quantum relative entropy between them $D(\Lambda(R)||\Lambda(S))$ is the right hand side of (iv). From the monotonicity we obtain $D(R||S) \geq D(\Lambda(R)||\Lambda(S))$, which proves the joint convexity (iv).

Finally we note that the quantum relative entropy $D(\rho||\sigma)$ is finite if and only if $\operatorname{supp}\rho \subseteq \operatorname{supp}\sigma$. Here $\operatorname{supp} A$ is the **support** of the Hermitian operator A. Let $A = \sum_i a_i E_i$ be the spectral decomposition (see Theorem A.3 in Appendix). Then the support of A is defined by $\operatorname{supp} A := \sum_{i:a_i \neq 0} E_i$, which coincides with the projection onto the range of A.

6.3.3 Mutual Information in Quantum Systems

We will introduce the Holevo mutual information [8], the quantum mutual information [23], and the coherent information [24] as counterparts of the classical mutual information in quantum systems. Each of them plays an important role in various channel coding theorems in quantum systems.

First we define the Holevo mutual information. Given density operators $W_1, W_2, \dots, W_N \in \mathcal{S}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$ and a probability distribution $P(x)$ $(x = 1, 2, \dots, N)$, the **Holevo mutual information** is defined by

$$I(P; W_1, \dots, W_N) := \sum_{x=1}^{N} P(x) D(W_x||W_P), \tag{6.58}$$

where W_P is the stochastic mixture defined by $W_P = \sum_{i=1}^{N} P(x) W_x$, and $D(W_x||W_P)$ is the quantum relative entropy (6.52). For simplicity of the notation, letting $W := (W_1, W_2, \dots, W_N)$, the Holevo mutual information is denoted by $I(P; W)$. The formula in the above definition corresponds to (6.28) for the classical mutual information. On the other hand, a simple calculation yields another expression of $I(P; W)$ by the von Neumann entropy.

$$\begin{aligned} I(P; W) &= \sum_{x=1}^{N} P(x) \operatorname{Tr} W_x (\log W_x - \log W_P) \\ &= \sum_{x=1}^{N} P(x) \operatorname{Tr} W_x \log W_x - \sum_{x=1}^{N} P(x) \operatorname{Tr} W_x \log W_P \\ &= H(W_P) - \sum_{x=1}^{N} P(x) H(W_x), \end{aligned} \tag{6.59}$$

which is often taken as an equivalent definition of $I(P; W)$. Note that this expression corresponds to (6.27) in the classical mutual information:

$$I(X; Y) = H(Y) - H(Y|X) = H(Y) - \sum_{x=1}^{N} P(x)H(P_{Y|X}(\cdot|x)).$$

From the non-negativity and the monotonicity of the quantum relative entropy, we have the following properties.

Lemma 6.6 (properties of the Holevo mutual information)

(i) ***non-negativity****: $I(P; W) \geq 0$. The equality holds if and only if W_x are identical to W_P for any x with $P(x) > 0$.*

(ii) ***monotonicity****: For any* ***quantum channel (TPCP map)*** *Λ, it holds that $I(P; W_1, \dots, W_N) \geq I(P; \Lambda(W_1), \dots, \Lambda(W_N))$.*

Given a density operator ρ_{AB} on a composite system $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$ of Hilbert spaces $\mathcal{H}_{\mathrm{A}}$ and $\mathcal{H}_{\mathrm{B}}$, the **quantum mutual information** is defined by

$$I_{\rho_{\mathrm{AB}}}(\mathrm{A}; \mathrm{B}) := D(\rho_{\mathrm{AB}}||\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}}), \tag{6.60}$$

where $D(\rho_{\mathrm{AB}}||\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}})$ is the quantum relative entropy, and $\rho_{\mathrm{A}} := \mathrm{Tr}_{\mathrm{B}}[\rho_{\mathrm{AB}}]$ and $\rho_{\mathrm{B}} := \mathrm{Tr}_{\mathrm{A}}[\rho_{\mathrm{AB}}]$ are the reduced density operators. This definition corresponds to (6.25) for the classical mutual information.

It is obvious from the non-negativity of the quantum relative entropy (Lemma 6.5 (i)) that the quantum mutual information is non-negative and the necessary and sufficient condition to be 0 is $\rho_{\mathrm{AB}} = \rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}}$. From the identity $\log(\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}}) = \log \rho_{\mathrm{A}} \otimes I_{\mathrm{B}} + I_{\mathrm{A}} \otimes \log \rho_{\mathrm{B}}$, which was shown in (6.50), we obtain the expression of the quantum mutual information by the von Neumann entropy in the same way as the classical case (6.26).

$$\begin{aligned} I_{\rho_{\mathrm{AB}}}(\mathrm{A}; \mathrm{B}) &= \mathrm{Tr}\, \rho_{\mathrm{AB}} \{\log \rho_{\mathrm{AB}} - \log(\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}})\} \\ &= \mathrm{Tr}\, \rho_{\mathrm{AB}} \log \rho_{\mathrm{AB}} - \mathrm{Tr}\, \rho_{\mathrm{AB}}(\log \rho_{\mathrm{A}} \otimes I_{\mathrm{B}}) - \mathrm{Tr}\, \rho_{\mathrm{AB}}(I_{\mathrm{A}} \otimes \log \rho_{\mathrm{B}}) \\ &= \mathrm{Tr}\, \rho_{\mathrm{AB}} \log \rho_{\mathrm{AB}} - \mathrm{Tr}\, \rho_{\mathrm{A}} \log \rho_{\mathrm{A}} - \mathrm{Tr}\, \rho_{\mathrm{B}} \log \rho_{\mathrm{B}} \qquad (6.61) \\ &= H(\rho_{\mathrm{A}}) + H(\rho_{\mathrm{B}}) - H(\rho_{\mathrm{AB}}), \qquad (6.62) \end{aligned}$$

where we used the property of the partial trace, $\mathrm{Tr}\, \rho_{\mathrm{AB}}(X_{\mathrm{A}} \otimes I_{\mathrm{B}}) = \mathrm{Tr}\, \rho_{\mathrm{A}} X_{\mathrm{A}}$, in (6.61). Let us verify that the Holevo mutual information is a kind of the quantum mutual information (6.60). Let $\mathcal{H}_{\mathrm{A}}$ be a Hilbert space with the dimension $\dim \mathcal{H}_{\mathrm{A}} = N$ and $\{|x\rangle\}_{x=1}^{N}$ be an orthonormal basis for $\mathcal{H}_{\mathrm{A}}$. Let us put $\mathcal{H}_{\mathrm{B}} = \mathcal{H}$ and consider the density operator $\rho_{\mathrm{AB}} = \sum_{x=1}^{N} P(x)|x\rangle\langle x| \otimes W_x$ on the composite system $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$. Then the partial traces are given by $\rho_{\mathrm{A}} = \mathrm{Tr}_{\mathrm{B}}[\rho_{\mathrm{AB}}] = \sum_{x=1}^{N} P(x)|x\rangle\langle x|$ and $\rho_{\mathrm{B}} = \mathrm{Tr}_{\mathrm{A}}[\rho_{\mathrm{AB}}] = \sum_{x=1}^{N} P(x)W_x = W_P$, and hence, we have $\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}} = \sum_{x=1}^{N} P(x)|x\rangle\langle x| \otimes W_P$.

Regarding the tensor products as the **Kronecker products**, $|1\rangle\langle 1| \otimes W_1, \ldots, |N\rangle\langle N| \otimes W_N$ are, respectively, written as block matrices with W_1 at (1, 1) block, …, W_N at (N, N) block. Summing them up, ρ_{AB} can be represented by the following block diagonal matrix, which is also applied to $\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}}$.

$$\rho_{\mathrm{AB}} = \begin{pmatrix} P(1)\,W_1 & & & 0 \\ & P(2)\,W_2 & & \\ & & \ddots & \\ 0 & & & P(N)\,W_N \end{pmatrix} \tag{6.63}$$

$$\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}} = \begin{pmatrix} P(1)\,W_P & & & 0 \\ & P(2)\,W_P & & \\ & & \ddots & \\ 0 & & & P(N)\,W_P \end{pmatrix}. \tag{6.64}$$

Thus we can see that the quantum mutual information of ρ_{AB} is nothing but the Holevo information.

$$\begin{aligned} D(\rho_{\mathrm{AB}}||\rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}}) &= \sum_{x=1}^{N} \mathrm{Tr}(P(x)W_x)\{\log(P(x)W_x) - \log(P(x)W_P)\} \\ &= \sum_{x=1}^{N} P(x)\,\mathrm{Tr}\,W_x(\log W_x - \log W_P) \\ &= I(P; W). \end{aligned} \tag{6.65}$$

The quantum mutual information is often used related to quantum channels. Let $\Lambda : \mathcal{S}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{S}(\mathcal{H}_{\mathrm{B}})$ be a quantum channel. Given a density operator $\rho_{\mathrm{A}} \in \mathcal{S}(\mathcal{H}_{\mathrm{A}})$ on the input system, let $\rho_{\mathrm{AR}} \in \mathcal{S}(\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{R}})$ be a purification of ρ_{A} with a reference system $\mathcal{H}_{\mathrm{R}}$. Let $\rho_{\mathrm{BR}} = (\Lambda \otimes \mathcal{I}_{\mathrm{R}})(\rho_{\mathrm{AR}})$, $\rho_{\mathrm{B}} = \mathrm{Tr}_{\mathrm{R}}[\rho_{\mathrm{BR}}]$, and $\rho_{\mathrm{R}} = \mathrm{Tr}_{\mathrm{B}}[\rho_{\mathrm{BR}}]$, where $\mathcal{I}_{\mathrm{R}}$ is the identical map (identical quantum channel). Thus we can define the **quantum mutual information** depending on a quantum channel Λ and a quantum state ρ_{A} on the input system by

$$\begin{aligned} I(\rho_{\mathrm{A}}; \Lambda) &:= D(\rho_{\mathrm{BR}}||\rho_{\mathrm{B}} \otimes \rho_{\mathrm{R}}) \\ &= D((\Lambda \otimes \mathcal{I}_{\mathrm{R}})(\rho_{\mathrm{AR}})||(\Lambda \otimes \mathcal{I}_{\mathrm{R}})(\rho_{\mathrm{A}} \otimes \rho_{\mathrm{R}})). \end{aligned} \tag{6.66}$$

Here it should be noted that the above formula depends only on ρ_{A} and Λ, because the degree of freedom for purification is those of unitary transformations, under which the quantum relative entropy is invariant. The quantum mutual information $I(\rho_{\mathrm{A}}; \Lambda)$ has the meaning as the entanglement assisted capacity [25], that is, the supremum of the message transmission rate over the quantum channel Λ when usage of the prior entanglement between the sender and the receiver is allowed. We often use the formula $I(\rho_A; \Lambda) = H(\rho_B) + H(\rho_R) - H(\rho_{BR})$ which is verified above.

Similarly the **coherent information** is defined by

$$I_c(\rho_A; \Lambda) := H(\rho_B) - H(\rho_{BR}) = I(\rho_A; \Lambda) - H(\rho_R), \tag{6.67}$$

which depends only on ρ_A and Λ as the quantum mutual information. The coherent information $I_c(\rho_A; \Lambda)$ has the meaning as the channel capacity of Λ for sending quantum state [26, 27]. It follows from the monotonicity of the quantum relative entropy that $I(\rho_A; \Lambda)$ and $I_c(\rho_A; \Lambda)$ satisfy the monotonicity:

$$I(\rho_A; \mathcal{I}_A) \geq I(\rho_A; \Lambda) \geq I(\rho_A; \Gamma \circ \Lambda), \tag{6.68}$$

$$I_c(\rho_A; \mathcal{I}_A) \geq I_c(\rho_A; \Lambda) \geq I_c(\rho_A; \Gamma \circ \Lambda), \tag{6.69}$$

where $\mathcal{I}_A$ is the identity channel and Γ is another quantum channel.

6.3.4 Concavity and Subadditivity of the von Neumann Entropy

As the Shannon entropy and the divergence (Sect. 6.2.8) in the classical case, the following identity holds between the von Neumann entropy and the quantum relative entropy:

$$D(\rho||\rho_{\mathrm{mix}}) = \mathrm{Tr}\,\rho\{\log\rho - \log(\tfrac{1}{\dim\mathcal{H}} I)\} = \log\dim\mathcal{H} - H(\rho), \tag{6.70}$$

where $\rho_{\mathrm{mix}} = \frac{1}{\dim\mathcal{H}} I$ is the **completely mixed state**. It follows from the non-negativity of the quantum relative entropy (Lemma 6.5) that $H(\rho) \leq \log\dim\mathcal{H}$ and the equality holds if and only if $\rho = \rho_{\mathrm{mix}}$, which is another proof for Lemma 6.4. The properties of the quantum mutual information defined in the previous subsection lead to the following properties of the von Neumann entropy.

Lemma 6.7 (concavity and subadditivity of the von Neumann entropy)

(i) ***concavity****: For any density operators ρ_1, ρ_2 and any $0 \leq t \leq 1$,*

$$H(t\rho_1 + (1-t)\rho_2) \geq tH(\rho_1) + (1-t)H(\rho_2). \tag{6.71}$$

The equality holds if and only if $t = 0, 1$ or $\rho_1 = \rho_2$.

(ii) ***subadditivity****: For any density operator ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$,*

$$H(\rho_A) + H(\rho_B) \geq H(\rho_{AB}). \tag{6.72}$$

The equality holds if and only if $\rho_{AB} = \rho_A \otimes \rho_B$.

(iii) ***strong subadditivity***[5]*: For any density operator* ρ_{ABC} *on* $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{C}}$*,*

$$H(\rho_{\mathrm{AB}}) + H(\rho_{\mathrm{BC}}) \geq H(\rho_{\mathrm{ABC}}) + H(\rho_{\mathrm{B}}). \tag{6.73}$$

Using the **conditional von Neumann entropy** (6.51), the above inequality is written as

$$H_{\rho_{\mathrm{AB}}}(A|B) + H_{\rho_{\mathrm{BC}}}(C|B) \geq H_{\rho_{\mathrm{ABC}}}(AC|B), \tag{6.74}$$

which is an extension of the subadditivity (6.72) and the origin of the name strong subadditivity.

Proof For density operators ρ_1, ρ_2 and a probability distribution $P(1) = t$, $P(2) = 1 - t$, the expression (6.59) and the non-negativity of the Holevo mutual information (Lemma 6.6(i)) lead to

$$I(P; \rho_1, \rho_2) = H(t\rho_1 + (1-t)\rho_2) - tH(\rho_1) - (1-t)H(\rho_2) \geq 0, \tag{6.75}$$

which proves (i). In the same way, from (6.62) and the non-negativity of the quantum mutual information, we have

$$I_{\rho_{\mathrm{AB}}}(\mathrm{A}; \mathrm{B}) = H(\rho_{\mathrm{A}}) + H(\rho_{\mathrm{B}}) - H(\rho_{\mathrm{AB}}) \geq 0,$$

which shows (ii). Concerning the strong subadditivity (iii), since the partial trace operation Tr_{C} is a **quantum channel** (**TPCP map**), the monotonicity of the quantum relative entropy (Theorem 6.7) yields

$$\begin{aligned} H(\rho_{\mathrm{A}}) + H(\rho_{\mathrm{BC}}) - H(\rho_{\mathrm{ABC}}) &= D(\rho_{\mathrm{ABC}} \| \rho_{\mathrm{A}} \otimes \rho_{\mathrm{BC}}) \\ &\geq D(\rho_{\mathrm{AB}} \| \rho_{\mathrm{A}} \otimes \rho_{\mathrm{B}}) = H(\rho_{\mathrm{A}}) + H(\rho_{\mathrm{B}}) - H(\rho_{\mathrm{AB}}). \end{aligned} \tag{6.76}$$

□

Exercise 6.12

(1) Let P be a projection. Show that $H(\rho) \leq H(P\rho P + (I-P)\rho(I-P))$.
(2) For a PVM $\{E_k\}$, show that $H(\rho) \leq H(\sum_k E_k \rho E_k)$.

6.3.5 Trace Distance

We introduce the trace distance between two density operators. It is recommended to learn Appendix A.6.3 first to readers who are not familiar with the mathematical treatment of the distance and the norm. The **trace distance** between two operators

[5] Tips to remember: a real valued function $f(X)$ of sets satisfying $f(X) + f(Y) \geq f(X \cup Y) + f(X \cap Y)$ is called a sub-modular function. The von Neumann entropy is a sub-modular function.

$A, B \in \mathcal{L}(\mathcal{H})$ are defined by using the trace norm $\|\cdot\|_1$ (Appendix A.6.3) on $\mathcal{L}(\mathcal{H})$ as

$$d(A, B) := \frac{1}{2}\|A - B\|_1, \tag{6.77}$$

which satisfies the axiom of distance given in Definition A.2. Especially the above formula defines a distance on the set of Hermitian operators $\mathcal{L}_h(\mathcal{H})$.

Let X_+ and X_- be, respectively, the positive part and the negative part of a Hermitian operator X (see Appendix (A.61) and (A.62)), and $|X|$ be the absolute value (actually it is an operator). Then from the relation $\mathrm{Tr}\,|X| = \mathrm{Tr}\,X_+ + \mathrm{Tr}\,X_-$, $\mathrm{Tr}\,X = \mathrm{Tr}\,X_+ - \mathrm{Tr}\,X_-$, we have

$$\mathrm{Tr}\,X_+ = \frac{1}{2}\left\{\mathrm{Tr}\,|X| + \mathrm{Tr}\,X\right\}, \tag{6.78}$$

$$\mathrm{Tr}\,X_- = \frac{1}{2}\left\{\mathrm{Tr}\,|X| - \mathrm{Tr}\,X\right\}, \tag{6.79}$$

from which the following lemma holds.

Lemma 6.8 *Let A and B be Hermitian operators. If* $\mathrm{Tr}\,A = \mathrm{Tr}\,B$ *then we have*

$$d(A, B) = \mathrm{Tr}(A - B)_+ = \mathrm{Tr}(A - B)_- = \max_{T:0\le T\le I} \mathrm{Tr}(A - B)T.$$

Especially for density operators $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, we have

$$d(\rho, \sigma) = \mathrm{Tr}(\rho - \sigma)_+ = \mathrm{Tr}(\rho - \sigma)_- = \max_{T:0\le T\le I} \mathrm{Tr}(\rho - \sigma)T.$$

Proof Replacing X with $A - B$ in (6.78) and (6.79), $\mathrm{Tr}(A - B) = 0$ implies

$$d(A, B) = \frac{1}{2}\mathrm{Tr}\,|A - B| = \mathrm{Tr}(A - B)_+ = \mathrm{Tr}(A - B)_-. \tag{6.80}$$

From Lemma A.6 in Appendix, we can see that

$$\mathrm{Tr}(A - B)_+ = \max_{T:0\le T\le I} \mathrm{Tr}(A - B)T, \tag{6.81}$$

and the maximum is attained by $T = \{A - B > 0\}$. □

Lemma 6.9 *The trace distance has the following properties.*

(i) ***monotonicity****: For any trace preserving positive map Λ:$\mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{K})$ and any operators $A, B \in \mathcal{L}(\mathcal{H})$,*

$$d(A, B) \ge d(\Lambda(A), \Lambda(B)). \tag{6.82}$$

In this book, this inequality is used when Λ is a ***quantum channel (TPCP map)****.*

(ii) ***joint convexity****: Let* $\{p_i\}$ *be a probability distribution and* $A = \sum_i p_i A_i$ *and* $B = \sum_i p_i B_i$ *be stochastic mixtures of operators. Then we have* $d(A, B) \leq \sum_i p_i d(A_i, B_i)$.

Proof For simplicity of the discussion, we prove (i) only for Hermitian operators $A, B \in \mathcal{L}_h(\mathcal{H})$, which is enough for the later chapters. Let us define the **adjoint map** with respect to the Hilbert-Schmidt inner product as the map $\Lambda^\dagger : \mathcal{L}(\mathcal{K}) \to \mathcal{L}(\mathcal{H})$ satisfying

$$\forall A \in \mathcal{L}(\mathcal{H}),\ \forall X \in \mathcal{L}(\mathcal{K}),\ \mathrm{Tr}\, \Lambda(A) X = \mathrm{Tr}\, A\, \Lambda^\dagger(X). \tag{6.83}$$

If Λ is trace preserving, it holds for any $\rho \in \mathcal{S}(\mathcal{H})$ that

$$\mathrm{Tr}\, \rho \Lambda^\dagger(I_\mathcal{K}) = \mathrm{Tr}\, \Lambda(\rho)\, I_\mathcal{K} = 1 = \mathrm{Tr}\, \rho\, I_\mathcal{H}, \tag{6.84}$$

which means $\Lambda^\dagger(I_\mathcal{K}) = I_\mathcal{H}$. Thus $\Lambda^\dagger$ is an identity preserving map called **unital map**. It is easy to verify that if Λ is a positive map then $\Lambda^\dagger$ is also a positive map. Consequently $-I \leq X \leq I$ implies $-I \leq \Lambda^\dagger(X) \leq I$. Using (A.65) in Appendix, we can prove (i) as follows.

$$\begin{aligned} 2d(\Lambda(A), \Lambda(B)) &= \max_{-I \leq X \leq I} |\mathrm{Tr}\, X(\Lambda(A) - \Lambda(B))| \\ &= \max_{-I \leq X \leq I} |\mathrm{Tr}\, \Lambda^\dagger(X)(A - B)| \leq \max_{-I \leq Y \leq I} |\mathrm{Tr}\, Y(A - B)| \\ &= 2d(A, B). \end{aligned}$$

It is obvious that (ii) follows from the triangle inequality for norms. □

Although we have shown (i) only for Hermitian operators here, the monotonicity of the trace distance holds for any operators $A, B \in \mathcal{L}(\mathcal{H})$ and any trace preserving positive map Λ. It can be shown in the same way as the above arguments using the fact that $\|X\| \leq 1$ implies $\|\Lambda^\dagger(X)\| \leq 1$ for a unital positive map $\Lambda^\dagger$ [28, 29].

6.3.6 Fidelity and Uhlmann's Theorem

For density operators ρ and σ, the **fidelity** is defined by

$$F(\rho, \sigma) := \mathrm{Tr}\, |\sqrt{\rho}\sqrt{\sigma}|. \tag{6.85}$$

Since $\mathrm{Tr}\, |A^\dagger| = \mathrm{Tr}\, |A|$ holds (Lemma A.5 in Appendix), we have

$$F(\sigma, \rho) = \mathrm{Tr}\, |(\sqrt{\sigma}\sqrt{\rho})^\dagger| = \mathrm{Tr}\, |\sqrt{\rho}\sqrt{\sigma}| = F(\rho, \sigma), \tag{6.86}$$

which means that $F(\rho, \sigma)$ is symmetric for ρ and σ. If σ is a pure state and written as $\sigma = |\phi\rangle\langle\phi|$, we have $\sqrt{\sigma} = |\phi\rangle\langle\phi|$ and

$$F(\rho, \sigma) = \operatorname{Tr} |\sqrt{\rho}\sqrt{\sigma}| = \operatorname{Tr}(\sqrt{\sigma}\rho\sqrt{\sigma})^{1/2} = \operatorname{Tr}(\langle\phi|\rho|\phi\rangle|\phi\rangle\langle\phi|)^{1/2}$$
$$= \sqrt{\langle\phi|\rho|\phi\rangle} \operatorname{Tr} |\phi\rangle\langle\phi| = \sqrt{\langle\phi|\rho|\phi\rangle}. \tag{6.87}$$

Especially if both ρ and σ are pure states, namely $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$, we have

$$F(\rho, \sigma) = |\langle\psi|\phi\rangle|. \tag{6.88}$$

In this case, $F(\rho, \sigma)$ is the absolute value of the inner product, and it obviously holds that $0 \leq F(\rho, \sigma) \leq 1$, $F(\rho, \sigma) = 1 \Leftrightarrow \rho = \sigma$, and $F(\rho, \sigma) = 0 \Leftrightarrow |\psi\rangle \perp |\phi\rangle$. Intuitively speaking, it would be clear that $F(\rho, \sigma)$ is close to 1 if and only if $|\psi\rangle$ and $|\phi\rangle$ are close up to phase factors $e^{i\theta}$.

For general two staets ρ and σ, the fidelity has a close relation with the inner product of purifications of them as described below. Let ρ and σ be density operators on a Hilbert space $\mathcal{H}_\mathrm{A}$ and consider purifications with a reference system $\mathcal{H}_\mathrm{R}$. Let $\{|e_i\rangle\}$ and $\{|f_j\rangle\}$ be orthonormal bases for $\mathcal{H}_\mathrm{A}$ and $\mathcal{H}_\mathrm{R}$, respectively, which are fixed in the following discussions. Since $\{|e_i\rangle \otimes |f_j\rangle\}$ is an orthonormal basis for $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}$, any element in $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}$ can be uniquely represented by $\sum_i \sum_j x_{i,j} |e_i\rangle \otimes |f_j\rangle$ with coefficients $x_{i,j} \in \mathbb{C}$. Let us consider the map that changes the bra-vector $\langle f_j|$ into the ket-vector $|f_j\rangle$:

$$X := \sum_i \sum_j x_{i,j} |e_i\rangle\langle f_j| \longmapsto |\phi_X\rangle = \sum_i \sum_j x_{i,j} |e_i\rangle \otimes |f_j\rangle. \tag{6.89}$$

Let $\mathcal{L}(\mathcal{H}_\mathrm{R}, \mathcal{H}_\mathrm{A})$ denote the set of linear operators from $\mathcal{H}_\mathrm{R}$ to $\mathcal{H}_\mathrm{A}$, then $\{|e_i\rangle\langle f_j|\}$ is an orthonormal basis for the vector space $\mathcal{L}(\mathcal{H}_\mathrm{R}, \mathcal{H}_\mathrm{A})$. Thus the map (6.89) provides one-to-one correspondence (bijective) and we can identify $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}$ with $\mathcal{L}(\mathcal{H}_\mathrm{R}, \mathcal{H}_\mathrm{A})$. Let $|\Phi_\mathrm{RR}\rangle := \sum_k |f_k\rangle \otimes |f_k\rangle \in \mathcal{H}_\mathrm{R} \otimes \mathcal{H}_\mathrm{R}$, then the correspondence (6.89) is given by

$$X \in \mathcal{L}(\mathcal{H}_\mathrm{R}, \mathcal{H}_\mathrm{A}) \longmapsto |\phi_X\rangle = (X \otimes I_\mathrm{R})|\Phi_\mathrm{RR}\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}\,. \tag{6.90}$$

Then, we have the following two lemmas.

Lemma 6.10 *The bipartite vector $|\phi_X\rangle$ is a purification of $\rho \in \mathcal{S}(\mathcal{H}_\mathrm{A})$, if and only if there exists a partial isometry $V : \mathcal{H}_\mathrm{R} \to \mathcal{H}_\mathrm{A}$ such that $X = \sqrt{\rho}V$ and* $\operatorname{supp} \rho \subseteq \operatorname{supp} VV^\dagger$. *Especially if* $\dim \mathcal{H}_\mathrm{A} = \dim \mathcal{H}_\mathrm{R} < \infty$, *we can take V as a unitary transformation.*

Lemma 6.11 *Let $|\phi_X\rangle$ and $|\phi_Y\rangle$ be purifications of ρ and σ, and take partial isometries V and W such that $X = \sqrt{\rho}V$ and $Y = \sqrt{\sigma}V$ as guaranteed by Lemma 6.10. Then the inner product between $|\phi_X\rangle$ and $|\phi_Y\rangle$ is written as*

$$\langle \phi_X | \phi_Y \rangle = \operatorname{Tr} X^\dagger Y = \operatorname{Tr}(\sqrt{\rho} V)^\dagger (\sqrt{\sigma} W) = \operatorname{Tr} \sqrt{\rho}\sqrt{\sigma} W V^\dagger. \tag{6.91}$$

The proofs of the lemmas are given later. Along with the Hilbert-Schmidt inner product $\langle X|Y\rangle_{HS} = \operatorname{Tr} X^\dagger Y$ on $\mathcal{L}(\mathcal{H}_\mathrm{R}, \mathcal{H}_\mathrm{A})$, Lemma 6.11 shows that (6.90) turns out to be an isomorphism between Hilbert spaces which preserves the inner product. Since $WV^\dagger$ is a partial isometry on $\mathcal{H}_\mathrm{A}$, Lemma A.5 (i) in Appendix shows that $\max_{V,W} |\operatorname{Tr} \sqrt{\rho}\sqrt{\sigma} W V^\dagger| = \operatorname{Tr} |\sqrt{\rho}\sqrt{\sigma}| = F(\rho, \sigma)$. Hence we can regard the fidelity $F(\rho, \sigma)$ as the inner product of certain purifications of ρ and σ as follows.

Theorem 6.8 (Uhlmann's thorem [30]) *For density operators $\rho, \sigma \in \mathcal{S}(\mathcal{H}_\mathrm{A})$ on a Hilbert space $\mathcal{H}_\mathrm{A}$, we have*

$$F(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}} |\langle \psi | \phi \rangle|, \tag{6.92}$$

where $\mathcal{H}_\mathrm{R}$ is a reference system and $|\psi\rangle$ and $|\phi\rangle$ are purifications of ρ and σ, respectively. Shortly speaking, the fidelity $F(\rho, \sigma)$ is given by the maximum absolute value of the inner product $|\langle \psi | \phi \rangle|$ for possible pairs of purifications. For a fixed purification $|\phi_0\rangle$ of σ, it is also possible to obtain the fidelity $F(\rho, \sigma)$ taking the maximum absolute value of the inner product $|\langle \psi | \phi_0 \rangle|$ for various purifications $|\psi\rangle$ of ρ, and the same applies to the converse situation.

$$F(\rho, \sigma) = \max_{|\psi\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}} |\langle \psi | \phi_0 \rangle| = \max_{|\phi\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}} |\langle \psi_0 | \phi \rangle|. \tag{6.93}$$

Proof of Lemma 6.10 *Since the partial trace of $M \in \mathcal{L}(\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R})$ is calculated as $\operatorname{Tr}_\mathrm{R} M = \sum_j (I_\mathrm{A} \otimes \langle f_j |) M (I_\mathrm{A} \otimes | f_j \rangle)$, we have*

$$\begin{aligned} \operatorname{Tr}_\mathrm{R} |\phi_Y\rangle\langle\phi_X| &= \sum_j (I_\mathrm{A} \otimes \langle f_j|)(Y \otimes I)|\Phi_{\mathrm{RR}}\rangle\langle\Phi_{\mathrm{RR}}|(X^\dagger \otimes I)(I_\mathrm{A} \otimes |f_j\rangle) \\ &= Y \left\{ \sum_j (I_\mathrm{A} \otimes \langle f_j|)|\Phi_{\mathrm{RR}}\rangle\langle\Phi_{\mathrm{RR}}|(I_\mathrm{A} \otimes |f_j\rangle) \right\} X^\dagger \\ &= Y X^\dagger, \end{aligned} \tag{6.94}$$

where we used the relation:

$$\sum_j (I_\mathrm{A} \otimes \langle f_j|)|\Phi_{\mathrm{RR}}\rangle\langle\Phi_{\mathrm{RR}}|(I_\mathrm{A} \otimes |f_j\rangle) = I_\mathrm{R} \ (= \operatorname{Tr}_\mathrm{R} |\Phi_{\mathrm{RR}}\rangle\langle\Phi_{\mathrm{RR}}|). \tag{6.95}$$

Thus, if $|\phi_X\rangle$ is a purification of $\rho \in \mathcal{S}(\mathcal{H}_\mathrm{A})$,

$$\sqrt{\rho}\sqrt{\rho} = \rho = \operatorname{Tr}_\mathrm{R} |\phi_X\rangle\langle\phi_X| = X X^\dagger \tag{6.96}$$

holds from (6.94). Hence from Lemma A.3 in Appendix, there exists an isometry $\hat{V} : \operatorname{Ran} \sqrt{\rho} \to \operatorname{Ran} X^\dagger$ such that $X^\dagger = \hat{V}\sqrt{\rho}$. Note that $\hat{V}$ can be extended to *a partial isometry from $\mathcal{H}_\mathrm{A}$ to $\mathcal{H}_\mathrm{R}$ such that* $\operatorname{supp}\rho \subseteq \operatorname{supp}\hat{V}^\dagger\hat{V}$. *Taking $V = \hat{V}^\dagger$ leads to $X = \sqrt{\rho}V$ and* $\operatorname{supp}\rho \subseteq \operatorname{supp} VV^\dagger$. *Especially if* $\dim\mathcal{H}_\mathrm{A} = \dim\mathcal{H}_\mathrm{R} < \infty$, *we can extend V to be a unitary transformation. Conversely, if $X = \sqrt{\rho}V$ holds with a partial isometry V satisfying* $\operatorname{supp}\rho \subseteq \operatorname{supp} VV^\dagger$, *we obtain $XX^\dagger = \rho$ and $|\phi_X\rangle$ is a purification of ρ from* (6.96). □

Proof of Lemma 6.11 *Taking the trace of the both sides in* (6.94) *in the proof of Lemma 6.10, we obtain the relation* (6.91). □

Exercise 6.13 Show the following propositions for the partial isometry.

(1) W is a partial isometry $\Leftrightarrow$ $WW^\dagger W = W$.
(2) W is a partial isometry $\Leftrightarrow$ $W^\dagger$ is a partial isometry.
(3) W is a partial isometry $\Leftrightarrow$ W^T is a partial isometry.

6.3.7 Properties of Fidelity

First, we summarize several basic properties of the fidelity derived from Uhlmann's theorem.

Lemma 6.12 *The fidelity $F(\rho, \sigma)$ has the following properties.*

(i) $0 \le F(\rho,\sigma) \le 1$ *($F(\rho,\sigma) = 1 \Leftrightarrow \rho = \sigma$)*
(ii) $F(\rho,\sigma) = F(\sigma,\rho)$
(iii) If either of the states is a pure state, say $\sigma = |\phi\rangle\langle\phi|$, we have $F(\rho,\sigma) = \sqrt{\langle\phi|\rho|\phi\rangle}$
(iv) For any quantum channel Λ, $F(\rho,\sigma) \le F(\Lambda(\rho),\Lambda(\sigma))$ holds.
(v) For a probability distribution $\{p_i\}_{i=1}^m$, $\{q_i\}_{i=1}^m$ and density operators ρ_i, σ_i $(i = 1,\ldots,m)$, we have $F(\sum_i p_i\rho_i, \sum_i q_i\sigma_i) \ge \sum_i \sqrt{p_i q_i} F(\rho_i,\sigma_i)$

*The inequality (iv) is called the **monotonicity** of the fidelity, and (v) is called the **strong concavity*** [12].

Proof Obviously (i) follows from Uhlmann's theorem (Theorem 6.8) and general properties of the inner product. We have already shown (ii) (iii) in the first part of the previous subsection. Let us show the monotonicity (iv). For a quantum channel, there exists an environment system $\mathcal{H}_\mathrm{E}$ and an isometry $V: \mathcal{H}_\mathrm{A} \to \mathcal{H}_\mathrm{B} \otimes \mathcal{H}_\mathrm{E}$ such that $\Lambda(\rho) = \mathrm{Tr}_\mathrm{E}\, V\rho V^\dagger$ holds. Let $|\psi_\mathrm{AR}\rangle, |\phi_\mathrm{AR}\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}$ be the purifications achieving the maximum in Uhlmann's theorem (6.92), respectively. Let us define

$$|\psi_\mathrm{BER}\rangle = (V \otimes I_\mathrm{R})|\psi_\mathrm{AR}\rangle, \quad |\phi_\mathrm{BER}\rangle = (V \otimes I_\mathrm{R})|\phi_\mathrm{AR}\rangle, \tag{6.97}$$

then $\langle\psi_\mathrm{AR}|\phi_\mathrm{AR}\rangle = \langle\psi_\mathrm{BER}|\phi_\mathrm{BER}\rangle$ holds from $V^\dagger V = I_\mathrm{A}$. On the other hand, noting

$$\mathrm{Tr}_\mathrm{ER}\, |\psi_\mathrm{BER}\rangle\langle\psi_\mathrm{BER}| = \Lambda(\rho), \quad \mathrm{Tr}_\mathrm{ER}\, |\phi_\mathrm{BER}\rangle\langle\phi_\mathrm{BER}| = \Lambda(\sigma),$$

we can see that $|\psi_{\mathrm{BER}}\rangle$ and $|\phi_{\mathrm{BER}}\rangle$ are purifications of $\Lambda(\rho)$ and $\Lambda(\sigma)$, respectively. Hence we obtain

$$\begin{aligned} F(\rho,\sigma) &= |\langle\psi_{\mathrm{AR}}|\phi_{\mathrm{AR}}\rangle| = |\langle\psi_{\mathrm{BER}}|\phi_{\mathrm{BER}}\rangle| \\ &\le \max_{|\psi_{\mathrm{BR}'}\rangle,|\phi_{\mathrm{BR}'}\rangle\in\mathcal{H}_{\mathrm{B}}\otimes\mathcal{H}_{\mathrm{R}'}} |\langle\psi_{\mathrm{BR}'}|\phi_{\mathrm{BR}'}\rangle| \\ &= F(\Lambda(\rho),\Lambda(\sigma)), \end{aligned} \tag{6.98}$$

where the maximum is taken over purifications of $\Lambda(\rho)$ and $\Lambda(\sigma)$.

Next we show the strong concavity (v). For given density operators $\rho_i, \sigma_i \in \mathcal{H}_{\mathrm{A}}$, let $|\psi_i\rangle, |\phi_i\rangle \in \mathcal{H}_{\mathrm{A}}\otimes\mathcal{H}_{\mathrm{R}}$ $(i = 1,\ldots,m)$ be purifications satisfying $F(\rho_i,\sigma_i) = |\langle\psi_i|\phi_i\rangle|$ in Uhlmann's Theorem (6.92). Here we can assume $F(\rho_i,\sigma_i) = \langle\psi_i|\phi_i\rangle$ without loss of generality by adjusting phase factors $e^{i\theta_i}$ appropriately. Now let $\mathcal{H}_{\mathrm{R}'}$ be an m-dimensional Hilbert space for which $|e_1\rangle,\ldots,|e_m\rangle$ are an orthonormal basis, and let

$$|\psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle\otimes|e_i\rangle, \quad |\phi\rangle = \sum_i \sqrt{q_i}|\phi_i\rangle\otimes|e_i\rangle \tag{6.99}$$

be state vectors in $\mathcal{H}_{\mathrm{A}}\otimes\mathcal{H}_{\mathrm{R}}\otimes\mathcal{H}_{\mathrm{R}'}$. Then we have $\mathrm{Tr}_{\mathrm{RR}'}|\psi\rangle\langle\psi| = \sum_i p_i\rho_i$ and $\mathrm{Tr}_{\mathrm{RR}'}|\phi\rangle\langle\phi| = \sum_i q_i\sigma_i$, and hence, $|\psi\rangle$ and $|\phi\rangle$ are purifications of $\sum_i p_i\rho_i$ and $\sum_i q_i\sigma_i$, respectively. Thus we have

$$F\Big(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\Big) \ge |\langle\psi|\phi\rangle| = \sum_i \sqrt{p_iq_i}\langle\psi_i|\phi_i\rangle = \sum_i \sqrt{p_iq_i}F(\rho_i,\sigma_i),$$

which proves (v). □

As an application of the fidelity, we prove the **no-cloning theorem**.

Theorem 6.9 *Let $|\psi\rangle$ and $|\phi\rangle$ be nonorthogonal and nonidentical pure states up to phase factors. Then there is no quantum operation that clones $|\psi\rangle$ and $|\phi\rangle$ as*

$$\Lambda(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|\otimes|\psi\rangle\langle\psi|, \quad \Lambda(|\phi\rangle\langle\phi|) = |\phi\rangle\langle\phi|\otimes|\phi\rangle\langle\phi|. \tag{6.100}$$

Proof From the assumptions, $0 < F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle| < 1$ holds for the inner product. On the other hand, suppose that there exists a quantum operation Λ which satisfies above equations. Then it must hold that $F(\Lambda(|\psi\rangle\langle\psi|), \Lambda(|\phi\rangle\langle\phi|)) = |\langle\psi|\phi\rangle|^2 < |\langle\psi|\phi\rangle| = F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|)$, which contradicts the monotonicity of the fidelity. □

Next, we study the relation between the fidelity and the trace distance. Note that distance measures, such as the trace distance $d(\rho,\sigma) = \frac{1}{2}\mathrm{Tr}\,|\rho-\sigma|$, are decreasing as the two states are getting close, while the fidelity $F(\rho,\sigma)$ is increasing. The fidelity is closely related to Bures distance defined below. From the Hilbert-Schmidt inner product $\langle X|Y\rangle_{HS} = \mathrm{Tr}\,X^\dagger Y$, we can define the norm $\|X\|_2 := \langle X|X\rangle_{HS}^{1/2}$ on the vector space of operators $\mathcal{L}(\mathcal{H})$ (see Appendix A.3.8). Then **Bures distance** is defined by

$$B(\rho, \sigma) := \min_{V,W} \|\sqrt{\rho}V - \sqrt{\sigma}W\|_2, \tag{6.101}$$

where the minimum is taken over unitary operators V and W. Then Bures distance and the fidelity are related as

$$2\{1 - F(\rho, \sigma)\} = B(\rho, \sigma)^2, \tag{6.102}$$

which can be verified as follows.

$$\begin{aligned} \|\sqrt{\rho}V - \sqrt{\sigma}W\|_2^2 &= \mathrm{Tr}(\sqrt{\rho}V - \sqrt{\sigma}W)^\dagger(\sqrt{\rho}V - \sqrt{\sigma}W) \\ &= \mathrm{Tr}\,\rho + \mathrm{Tr}\,\sigma - \mathrm{Tr}\,\sqrt{\rho}\sqrt{\sigma}WV^\dagger - \mathrm{Tr}(\sqrt{\rho}\sqrt{\sigma}WV^\dagger)^\dagger \\ &= 2\left\{1 - \mathrm{Re}\,\mathrm{Tr}\,\sqrt{\rho}\sqrt{\sigma}WV^\dagger\right\} \geq 2\{1 - F(\rho, \sigma)\}. \end{aligned} \tag{6.103}$$

Here we used $\mathrm{Re}\,\mathrm{Tr}\,\sqrt{\rho}\sqrt{\sigma}WV^\dagger \leq |\,\mathrm{Tr}\,\sqrt{\rho}\sqrt{\sigma}WV^\dagger| \leq F(\rho, \sigma)$. The equality and the minimum in (6.101) is attained by choosing V and W such that $\sqrt{\rho}\sqrt{\sigma}WV^\dagger = |\sqrt{\rho}\sqrt{\sigma}|$.

Exercise 6.14 Show that $B(\rho, \sigma) = \min_U \|\sqrt{\rho} - \sqrt{\sigma}U\|_2$. Also verify that Bures distance (6.101) satisfies the axiom of distance given in Definition A.2.

Exercise 6.15 Show that Bures distance (6.101) is obtained by changing purifications $|\psi\rangle, |\phi\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}$ for $\rho, \sigma \in \mathcal{S}(\mathcal{H}_\mathrm{A})$, respectively, and taking the minimum:

$$B(\rho, \sigma) = \min_{|\psi\rangle, |\phi\rangle \in \mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{R}} \||\psi\rangle - |\phi\rangle\|, \tag{6.104}$$

where $\||\psi\rangle - |\phi\rangle\| = \langle\psi - \phi|\psi - \phi\rangle^{1/2}$. See Lemma 6.10 and Lemma 6.11.

The following relation between the fidelity and the trace distance holds.

Lemma 6.13 *Concerning the trace distance $d(\rho, \sigma)$ and the fidelity $F(\rho, \sigma)$, if ρ and σ are pure states, we have*

$$d(\rho, \sigma) = \sqrt{1 - F(\rho, \sigma)^2}. \tag{6.105}$$

For general two states, the inequalities

$$1 - F(\rho, \sigma) \leq d(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2} \tag{6.106}$$

hold.

Proof First, we show (6.105) when ρ and σ are pure states. Let $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$, then there is no loss of generality to suppose that $\langle\psi|\phi\rangle \geq 0$ by adjusting phase factors appropriately. Applying **Gram-Schmidt orthogonalization**, let $|0\rangle = |\psi\rangle$ and take an orthogonal and normalized vector $|0\rangle$ to $|1\rangle$, so that $|\phi\rangle = a|0\rangle + b|1\rangle$. Note that $a = \langle\psi|\phi\rangle \geq 0$ and we can assume $b \geq 0$ adjusting the phase factor of $|1\rangle$. By the normalization condition, we have $a^2 + b^2 = 1$. In the following discussion, it is enough to consider the subspace spanned by $|0\rangle$ and $|1\rangle$, and ρ and σ are represented by matrices:

$$\rho = (1\ 0)\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1&0\\0&0\end{pmatrix}, \quad \sigma = (a\ b)\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}a^2&ab\\ab&b^2\end{pmatrix}. \tag{6.107}$$

By an easy calculation, the eigenvalues of $\rho - \sigma$ are $\pm b$. Since the trace norm is the sum of the absolute values of eigenvalues, we have $\|\rho - \sigma\|_1 = 2b$. Thus $d(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1 = b$ holds. On the other hand, we have $F(\rho, \sigma) = \langle\psi|\phi\rangle = a$, which asserts the relation (6.105).

Next, we consider the general case where ρ and σ are not necessarily pure states. Let us chose a purifications $|\psi\rangle\langle\psi|$ of ρ and $|\phi\rangle\langle\phi|$ of σ so that $F(\rho, \sigma) = |\langle\psi, \phi\rangle|$ holds. Then from the monotonicity of the trace distance and (6.105) we have

$$d(\rho, \sigma) \leq d(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \sqrt{1 - F(\rho, \sigma)^2}, \tag{6.108}$$

which proves the second inequality of (6.106). We show the first inequality of (6.106). For this purpose, we show the following inequality for Hermitian operators A and B (Powers-Stormer's inequality [31]).

$$\left\|\sqrt{A} - \sqrt{B}\right\|_2^2 \leq \|A - B\|_1. \tag{6.109}$$

Let $X = \sqrt{A} + \sqrt{B}$ and $Y = \sqrt{A} - \sqrt{B}$. Then $X \geq \pm Y$ follows from $X + Y \geq 0$ and $X - Y \geq 0$. Define $T_+ := \{Y \geq 0\}$, $T_- := \{Y < 0\}$, and $T := T_+ - T_-$. Then these operators commute with Y, and $Y_+ := YT_+$ and $Y_- := -YT_-$ are the positive and negative parts of Y. Thus we have

$$|Y| = Y_+ + Y_- = YT_+ - YT_- = TY = YT, \tag{6.110}$$

$$|Y| = T_+|Y|T_+ + T_-|Y|T_-. \tag{6.111}$$

Also the inequalities $X \geq \pm Y$ yield

$$T_+XT_+ \geq T_+YT_+ = Y_+, \quad T_-XT_- \geq T_-(-Y)T_- = Y_-, \tag{6.112}$$

Using these relations and $XY + YX = 2(A - B)$, we obtain

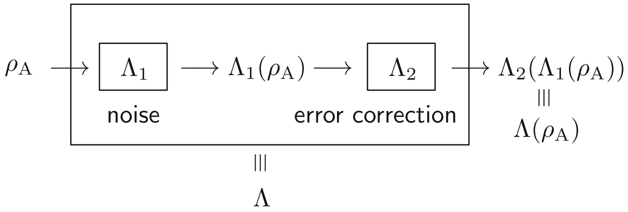

ρ_{A}
Λ_1
noise
$\Lambda_1(\rho_{\mathrm{A}})$
Λ_2
error correction
$\Lambda_2(\Lambda_1(\rho_{\mathrm{A}}))$
$\equiv$
$\Lambda(\rho_{\mathrm{A}})$
$\equiv$
Λ

Fig. 6.2 Quantum noise and error correction

$$\begin{aligned}\operatorname{Tr}|A-B| &= \max_{-I\le X\le I}\operatorname{Tr}(A-B)X \ge \operatorname{Tr}(A-B)T = \frac{1}{2}\operatorname{Tr}(XY+YX)T\\ &= \frac{1}{2}\operatorname{Tr}X(YT+TY) = \operatorname{Tr}(X|Y|) = \operatorname{Tr}X(T_+|Y|T_+ + T_-|Y|T_-)\\ &= \operatorname{Tr}(T_+XT_+ + T_-XT_-)|Y| \ge \operatorname{Tr}(Y_+ + Y_-)|Y| = \operatorname{Tr}|Y|^2, \qquad (6.113)\end{aligned}$$

which proves (6.109). Using (6.102) and (6.109), the first inequality of (6.106) is verified as follows.

$$\begin{aligned}1-F(\rho,\sigma) = \frac{1}{2}B(\rho,\sigma)^2 &= \frac{1}{2}\min_{V,W}\|\sqrt{\rho}V-\sqrt{\sigma}W\|_2^2\\ &\le \frac{1}{2}\|\sqrt{\rho}-\sqrt{\sigma}\|_2^2 \le \frac{1}{2}\|\rho-\sigma\|_1 = d(\rho,\sigma). \qquad (6.114)\end{aligned}$$

Exercise 6.16

(1) Show $1-F(\rho,\sigma)^2 \le 2(1-F(\rho,\sigma))$.
(2) Show $d(\rho,\sigma) \le B(\rho,\sigma)$.

6.3.8 Entanglement Fidelity

In this subsection, we introduce the definition of the entanglement fidelity for quantum channels and discuss its properties. The entanglement fidelity measures how much entanglement is preserved in a given channel, or how close the channel is to the ideal noiseless channel, by using the fidelity discussed in the previous subsection.

The entanglement fidelity quantifies the preservation of an initial state ρ_{A} under a noisy channel $\Lambda_1 : \mathcal{L}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{L}(\mathcal{H}_{\mathrm{B}})$, and is mostly used in the analysis in quantum error correction; see Fig. 6.2. In quantum error correction, relevant to the output $\Lambda_1(\rho_{\mathrm{A}})$, we will design a recovery operation $\Lambda_2 : \mathcal{L}(\mathcal{H}_{\mathrm{B}}) \to \mathcal{L}(\mathcal{H}_{\mathrm{A}})$ so that $\Lambda_2(\Lambda_1(\rho_{\mathrm{A}}))$ is as close to ρ_{A} as possible. Note that, however, it is useless to consider only one input, because one input ρ_{A} is recovered obviously by a quantum operation that outputs ρ_{A} for any input, that is, a quantum operation which discards its input and then generate ρ_{A}. Hence it is important to study whether more than two inputs can be

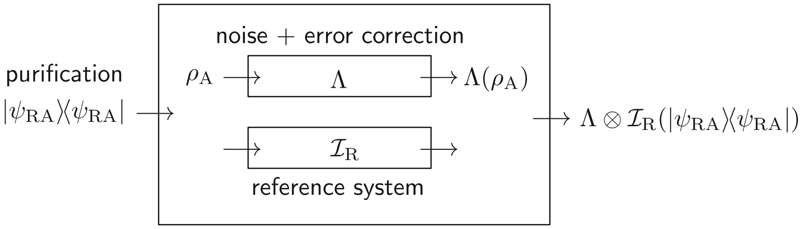

purification
$|\psi_{\mathrm{RA}}\rangle\langle\psi_{\mathrm{RA}}|$
noise + error correction
ρ_{A}
Λ
$\Lambda(\rho_{\mathrm{A}})$
$\mathcal{I}_{\mathrm{R}}$
reference system
$\Lambda\otimes\mathcal{I}_{\mathrm{R}}(|\psi_{\mathrm{RA}}\rangle\langle\psi_{\mathrm{RA}}|)$

Fig. 6.3 Entanglement fidelity

recovered or not. In quantum error correction, we try to chose an appropriate subspace $\mathcal{K}\subset\mathcal{H}_{\mathrm{A}}$ of the input system so that the effect of noise is as small as possible for $\mathcal{K}$. In the later discussions, since we want to study the performance of the composite channel $\Lambda=\Lambda_2\circ\Lambda_1$, we only treat quantum channels $\Lambda:\mathcal{L}(\mathcal{H}_{\mathrm{A}})\to\mathcal{L}(\mathcal{H}_{\mathrm{A}})$ of which the input and output systems are identical (or isomorphic).

As measures of the closeness to the noiseless channel for a given quantum channel Λ, several information quantities based on the fidelity are known so far. One is the minimum fidelity over the set of pure states on $\mathcal{K}\subset\mathcal{H}_{\mathrm{A}}$ as inputs:

$$\min_{|\psi\rangle\in\mathcal{K}} F(|\psi\rangle\langle\psi|,\Lambda(|\psi\rangle\langle\psi|))=\min_{|\psi\rangle\in\mathcal{K}}\langle\psi|\Lambda(|\psi\rangle\langle\psi|)|\psi\rangle^{1/2}. \tag{6.115}$$

Since the fidelity near 1 means similar two quantum states, we can say that when the above quantity is near 1, Λ is close to the noiseless channel with respect to the subspace $\mathcal{K}$. We often use 1 minus the square of the minimum fidelity as a measure of the error:

$$\max_{|\psi\rangle\in\mathcal{K}}\{1-F(|\psi\rangle\langle\psi|,\Lambda(|\psi\rangle\langle\psi|))^2\}. \tag{6.116}$$

On the other hand, we can study how much entanglement is preserved to measure the closeness to the noiseless channel; see Fig. 6.3. Given a density operator $\rho_{\mathrm{A}}\in\mathcal{S}(\mathcal{H}_{\mathrm{A}})$, let $|\psi_{\mathrm{AR}}\rangle\in\mathcal{H}_{\mathrm{A}}\otimes\mathcal{H}_{\mathrm{R}}$ be a purification of ρ_{A}. Then the **entanglement fidelity** is defined by

$$\begin{aligned}F_e^2(\rho_{\mathrm{A}},\Lambda)&:=F(|\psi_{\mathrm{AR}}\rangle\langle\psi_{\mathrm{AR}}|,(\Lambda\otimes\mathcal{I}_{\mathrm{R}})(|\psi_{\mathrm{AR}}\rangle\langle\psi_{\mathrm{AR}}|))^2\\&=\langle\psi_{\mathrm{AR}}|(\Lambda\otimes\mathcal{I}_{\mathrm{R}})(|\psi_{\mathrm{AR}}\rangle\langle\psi_{\mathrm{AR}}|)|\psi_{\mathrm{AR}}\rangle,\end{aligned} \tag{6.117}$$

where $\mathcal{I}_{\mathrm{R}}$ is the identity channel on the reference system. Since the entanglement fidelity is often used as the square of the fidelity, we use the superscript F_e^2 in the notation. From (6.87) the entanglement fidelity is written in the form of the inner product, as $|\psi_{\mathrm{AR}}\rangle\langle\psi_{\mathrm{AR}}|$ is a pure state. Note that the entanglement fidelity is well defined independent of purifications, because the degree of freedom for purification is those of isometries (or unitary transformations). From the properties of the fidelity, we have $0\leq F_e^2(\rho_{\mathrm{A}},\Lambda)\leq 1$.

Lemma 6.14 *The entanglement fidelity $F_e^2(\rho_A, \Lambda)$ has the following properties.*

(i) If ρ_A is a pure state $F_e^2(\rho_A, \Lambda) = F(\rho_A, \Lambda(\rho_A))^2$ holds. In general, we have $F_e^2(\rho_A, \Lambda) \le F(\rho_A, \Lambda(\rho_A))^2$.

(ii) Using the ***Kraus representation*** *$\Lambda(\rho) = \sum_k E_k \rho E_k^\dagger$ for Λ, the entanglement fidelity is represented by*

$$F_e^2(\rho_A, \Lambda) = \sum_k |\operatorname{Tr} \rho_A E_k|^2. \tag{6.118}$$

(iii) $F_e^2(\rho_A, \Lambda)$ is a ***convex function*** *with respect to ρ_A.*

(iv) $F_e^2(\rho_A, \Lambda)$ is ***affine*** *(linear) with respect to Λ.*

Proof If ρ_A is a pure state, the definition of the entanglement fidelity directly leads to (i). The general case of (i) follows from the monotonicity of the fidelity. We can verify (ii) as follows.

$$\begin{aligned} F_e^2(\rho_A, \Lambda) &= \sum_k \langle \psi_{AR}|(E_k \otimes I_R)|\psi_{AR}\rangle\langle\psi_{AR}|(E_k^\dagger \otimes I_R)|\psi_{AR}\rangle \\ &= \sum_k \{\operatorname{Tr} \rho_{AR}(E_k \otimes I_R)\}\{\operatorname{Tr} \rho_{AR}(E_k^\dagger \otimes I_R)\} \\ &= \sum_k (\operatorname{Tr} \rho_A E_k)(\operatorname{Tr} \rho_A E_k^\dagger) = \sum_k |\operatorname{Tr} \rho_A E_k|^2. \end{aligned} \tag{6.119}$$

Taking (6.118) into account, it is enough for (iii) to show that $\rho \mapsto |\operatorname{Tr} \rho E|^2$ is a convex function, that is, for any $0 \le \forall t \le 1$,

$$|\operatorname{Tr}(t\rho + (1-t)\sigma)E|^2 \le t|\operatorname{Tr} \rho E|^2 + (1-t)|\operatorname{Tr} \sigma E|^2 \tag{6.120}$$

holds. Let $a = \operatorname{Tr} \rho E$, $b = \operatorname{Tr} \sigma E$, $p = t$, and $q = 1 - t$. Then the above inequality is written as $|pa + qb|^2 \le p|a|^2 + q|b|^2$ $(a, b \in \mathbb{C})$, which is verified as follows.

$$\begin{aligned} &(p|a|^2 + q|b|^2) - |pa + qb|^2 \\ &\quad = p(1-p)|a|^2 + q(1-q)|b|^2 - 2pq\mathrm{Re}\{ab\} = pq|a-b|^2 \ge 0, \end{aligned}$$

where we used $p(1-p) = q(1-q) = pq$. Finally, (iv) is obvious from (6.117). □

The entanglement fidelity is also used in the form $1 - F_e^2(\rho_A, \Lambda)$ as a measure of the error. Let us study the relation between $1 - F_e^2(\rho_A, \Lambda)$ and (6.116). In the following, let $\mathcal{K}$ be the **support** of ρ_A. If $\rho_A = \sum_{i=1}^m p_i |\psi_i\rangle\langle\psi_i|$ is an arbitrary decomposition of ρ_A to pure states, we have $|\psi_i\rangle \in \mathcal{K}$ for any $i = 1, \ldots, m$. Corresponding to this decomposition, we can take the purification of ρ_A as $|\psi_{AR}\rangle = \sum_{i=1}^m \sqrt{p_i}|\psi_i\rangle \otimes |f_i\rangle$, where $\{f_i\}$ is an orthonormal basis for the reference system. Since $F_e^2(\rho_A, \Lambda)$ is convex for ρ_A,

$$F_e^2(\rho_{\mathrm{A}}, \Lambda) \leq \sum_{i=1}^{m} p_i F(|\psi_i\rangle\langle\psi_i|, \Lambda(|\psi_i\rangle\langle\psi_i|))^2 \tag{6.121}$$

holds. Subtracting the both sides from 1, we have

$$\sum_{i=1}^{m} p_i \{1 - F(|\psi_i\rangle\langle\psi_i|, \Lambda(|\psi_i\rangle\langle\psi_i|))^2\} \leq 1 - F_e^2(\rho_{\mathrm{A}}, \Lambda). \tag{6.122}$$

The above inequality means that if the entanglement of the purification $|\psi_{\mathrm{AR}}\rangle$ is preserved in a precision $0 \leq \epsilon \leq 1$, then the input $|\psi_i\rangle \in \mathcal{K}$ and the output $\Lambda(|\psi_i\rangle\langle\psi_i|)$ are sufficiently close in the sense of the avarage. Moreover, it is possible to turn the evaluation in the expected error into those in the worst error (6.116) by discarding the subspace that is apt to get much noise; see Exercise 8.4. Conversely, when ρ_{A} is the completely mixed state ρ_{mix}, the following inequality is known [32].

$$\{1 - F_e^2(\rho_{\mathrm{mix}}, \Lambda)\} \leq \frac{3}{2} \max_{|\psi\rangle \in \mathcal{K}} \{1 - F(|\psi\rangle\langle\psi|, \Lambda(|\psi\rangle\langle\psi|))^2\}, \tag{6.123}$$

which means that if the output $\Lambda(|\psi_i\rangle\langle\psi_i|)$ is sufficiently close to the input $|\psi_i\rangle \in \mathcal{K}$, the entanglement is also preserved with almost the same precision. Especially in the case of $\epsilon = 0$, (6.122) and (6.123) lead to

$$F_e^2(\rho_{\mathrm{mix}}, \Lambda) = 1 \Leftrightarrow \forall |\psi\rangle \in \mathcal{K},\ F(|\psi\rangle\langle\psi|, \Lambda(|\psi\rangle\langle\psi|)) = 1. \tag{6.124}$$

References

1. C.E. Shannon, Bell Syst. Tech. J. **27**(379–423), 623–656 (1948)
2. C.E. Shannon, W. Weaver, *The Mathematical Theory of Communication* (University of Illinois Press, Illinois, 1949)
3. C.W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976)
4. A.S. Holevo, J. Multivar. Anal. **3**, 337–394 (1973)
5. H.P. Yuen, Communication theory of quantum systems. MIT Res. Lab. Electron. Tech. Rep. **482** (1971)
6. H.P. Yuen, R.S. Kennedy, M. Lax, IEEE Trans. Inform. Theor. **21**, 125–134 (1975)
7. A.S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982)
8. A.S. Holevo, Probl. Inform. Transm. **9**, 177–183 (1973)
9. A.S. Holevo, Probl. Inform. Transm. **15**, 247–253 (1979)
10. T. Cover, J. Thomas, *Elements of Information Theory* (John Wiley & Sons, New York, 1991)
11. T.S. Han, K. Kobayashi, *Mathematics of Information and Coding* (American Mathematical Society, New York, 2007). (Originally published in Japanese in 1999)
12. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)
13. M. Hayashi, *Quantum Information: An Introduction* (Springer, New York, 2006) (Originally published in Japanese in 2004)
14. S. Amari, H. Nagaoka, *Methods of Information Geometry* (AMS, New York, 2001)

15. I. Bengtsson, K. Zyczkowski, *Geometry of Quantum States* (Cambridge University Press, Cambridge, 2006)
16. I. Csiszár, Stud. Sci. Math. Hung. **2**, 329–339 (1967)
17. H. Umegaki, Kōdai Math. Sem. Rep. **4**, 59–85 (1962)
18. G. Lindblad, Commun. Math. Phys. **40**, 147–151 (1975)
19. A. Uhlmann, Commun. Math. Phys. **54**, 21–32 (1977)
20. D. Petz, Rev. Math. Phys. **15**, 79–91 (2003)
21. D. Petz, *Quantum Information Theory and Quantum Statistics* (Springer, Berlin, 2008)
22. M. Ohya, D. Petz, *Quantum Entropy and Its Use* (Springer, Berlin, 1993)
23. N.J. Cerf, C. Adami, Phys. Rev. Lett. **79**, 5194–5197 (1997)
24. B. Schumacher, M.A. Nielsen, Phys. Rev. A **54**, 2629–2635 (1996)
25. C.H. Bennett, P.W. Shor, J.A. Smolin, A.V. Thapliyal, IEEE Trans. Inform. Theor. **48**, 2637–2655 (2002)
26. I. Devetak, IEEE Trans. Inform. Theor. **51**, 44–55 (2005)
27. P.W. Shor, in *MSRI Workshop on Quantum Computation*, 2002
28. B. Russo, H.A. Dye, Duke Math. J. **33**, 413–416 (1966)
29. V. Paulsen, *Completely Bounded Maps and Operator Algebras* (Cambridge University Press, Cambridge, 2002)
30. A. Uhlmann, Rep. Math. Phys. **9**, 273–279 (1976)
31. R.T. Powers, E. Stormer, Commun. Math. Phys. **16**, 1–33 (1970)
32. H. Barnum, H. Knill, M.A. Nielsen, IEEE. Trans. Inform. Theor. **46**, 1317–1329 (2000)

Chapter 7
Quantum Entanglement

7.1 Introduction

In 1935, Einstein, Podolsky and Rosen proposed a gedankenexperiment as an evidence of an incompleteness of quantum mechanics. The gedankenexperiment, known as the **EPR paradox** [1], attracted a lot of controversial studies, and it was then eventually understood that the paradox originates from a nonlocal property of quantum mechanics; two distant quantum objects, even if they are extremely far apart from each other, sometimes do not behave independently. Namely, the assumption of locality does not hold true in quantum mechanics. Such two dependent quantum objects are called *entangled*, and this phenomenon of **quantum entanglement** (entanglement in short hereafter) had been solely discussed as a fundamental problem in quantum mechanics since the EPR paradox was proposed. In 1981, however, it was confirmed experimentally that nature certainly exhibits the nonlocal property as quantum mechanics predicts [2], and then the paradigm was shifted: research of how to utilize the nonlocality of entanglement has begun.

In 1980s and 1990s, many quantum information tasks, such as quantum cryptography, quantum algorithm on quantum computers, and quantum teleportation, were proposed. Entanglement is then considered to be an important and valuable resource in quantum information processing. Since 1990s, a lot of research on entanglement has been actively carried out in the world. This is because entanglement is a striking feature of quantum mechanics (the classical counterpart does not exist), and hence clarifying its properties is crucially important for the development of quantum information technology. It is even expected that new findings in the properties of entanglement will pave a road to new quantum technologies. As a result, in recent years, the theory of entanglement has been rapidly developed along with quantum information theory.

In particular, introducing the concept of **local operations and classical communication** (**LOCC**) [3] enables us to quantify the amount of entanglement, and leads to our much better understanding of entanglement. Consider two distant parties and suppose that they cannot exchange qubits (i.e. their quantum communication is

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_7,

prohibited), but they can exchange classical information by usual telephone or Internet. What they can do is local operations (local unitary transformations, local measurements, and so on) on their own qubits and classical communication, that is LOCC. LOCC has a property such that it cannot create any entangled state from unentangled states. Therefore, if a certain quantum information task, which is impossible by LOCC alone, becomes possible by using a previously shared entangled state, we can conclude that the entangled state has a power to achieve the quantum task. In this way, the power of entanglement can be manifested by considering a restricted class of operations such as LOCC. Moreover, LOCC by itself has the usefulness as protocols in quantum information processing. Indeed, many quantum protocols that utilize quantum entanglement, including quantum teleportation [4], belong to the class of LOCC.

The quantum systems consist of more than two parties can have a variety of types of entanglement and exhibit a variety of phenomena. Moreover, in realistic systems, a pure state inevitably falls into a mixed state, and therefore it is crucial for the actual quantum information technology to clarify and understand the properties of mixed-state entanglement.

7.2 Basic Concepts of Entanglement

7.2.1 Quantum and Classical Correlation

Consider two qubits, A and B. When both A and B are in $|0\rangle$, the whole state is $|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}$. Similarly, when both are in $|1\rangle$, the whole state is $|1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}$. The superposition of the above two states

$$|\Psi\rangle = \frac{|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}}{\sqrt{2}}$$

is called an entangled state.

Suppose that we perform a basis measurement of $\{|0\rangle, |1\rangle\}$. When the outcome of the measurement on A is $|0\rangle$ (this occurs with the probability of 1/2), $|\Psi\rangle$ is changed to $|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}$, and hence the outcome of the measurement on B is also $|0\rangle$. In the same way, when the measurement outcome on A is $|1\rangle$, the measurement outcome on B is also $|1\rangle$. Even if the two qubits are far apart from each other, the two measurement outcomes on A and B always coincide. However, this phenomenon in itself is not surprising. For example, consider two boxes, each contains a paper on which “0” or “1” is written. Suppose that the same value is written on the two papers, but we do not know which value is actually written. Even in this simple setting, when we open a box and find out the paper with “0” written on it (i.e. when we obtain the outcome “0” by a measurement on the box), we always find out the paper with “0” in the other box, and two measurement outcomes always coincide regardless of the distance between the two boxes.

However, contrary to the papers in the boxes, the entangled state $|\Psi\rangle$ exhibits a much stronger correlation. Using the following orthogonal basis rotated by θ:

$$\begin{cases} |\theta\rangle \;=\; \cos\theta|0\rangle + \sin\theta|1\rangle \\ |\theta_{\perp}\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle \end{cases}$$

the state $|\Psi\rangle$ is rewritten as

$$|\Psi\rangle = \frac{|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}}{\sqrt{2}} = \frac{|\theta\rangle_{\mathrm{A}}|\theta\rangle_{\mathrm{B}} + |\theta_{\perp}\rangle_{\mathrm{A}}|\theta_{\perp}\rangle_{\mathrm{B}}}{\sqrt{2}}. \tag{7.1}$$

Therefore, even when we perform the basis measurement $\{|\theta\rangle, |\theta_{\perp}\rangle\}$ on each qubit A and B, the two measurement outcomes always coincide with each other. In this way, the measurement outcomes on an entangled state exhibit a strong correlation such that they always coincide regardless of the choice of the basis, which is called **quantum correlation**. On the other hand, the correlation of the previous example of the two papers in the two boxes is called **classical correlation**, whose corresponding state is the mixed state of $\sigma = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$ that is distinct from $|\Psi\rangle$.

7.2.2 Product State and Maximally Entangled State

Let us consider a more general pure state $|\psi\rangle$ on two d-dimensional systems A and B. By virtue of the Schmidt decomposition (see Theorem A.4), $|\psi\rangle$ is written as

$$(U \otimes V)|\psi\rangle = \sum_{i=0}^{d-1} \sqrt{p_i}|i\rangle_{\mathrm{A}}|i\rangle_{\mathrm{B}}, \tag{7.2}$$

where $(U \otimes V)$ is an appropriate local unitary transformation. We can assume that the Schmidt coefficients are aligned in decreasing order without loss of generality (by appropriately redefining the orthogonal basis sets $\{|i\rangle\}$) such that $p_0 \geq p_1 \geq p_2 \geq \cdots \geq p_{d-1}$. When $p_0 = 1$, we have $p_1 = p_2 = \cdots = p_{d-1} = 0$, and hence

$$|\psi\rangle = (U^{\dagger} \otimes V^{\dagger})(|0\rangle_{\mathrm{A}} \otimes |0\rangle_{\mathrm{B}}) = |f\rangle_{\mathrm{A}} \otimes |g\rangle_{\mathrm{B}},$$

which is written as a product of the two local states of A and B. The state in such a form is called a **product state**. The reduced density operators of a product state are pure states ($\sigma_{\mathrm{A}} = |f\rangle\langle f|$, $\sigma_{\mathrm{B}} = |g\rangle\langle g|$). On the other hand, when $p_0 < 1$, the right hand side of (7.2) becomes the sum of more than two terms, and it cannot be expressed as a product of two local states of A and B. Such a state is an **entangled state**. In particular, when all the Schmidt coefficients are equal and $p_i = 1/d$, the state $|\Psi\rangle$ is called a **maximally entangled state**, and hence the Schmidt decomposition:

$$(U \otimes V)|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_{\mathrm{A}}|i\rangle_{\mathrm{B}} \tag{7.3}$$

The reduced density operators of a maximally entangled state are $\sigma_{\mathrm{A}} = \sigma_{\mathrm{B}} = I/d$, which is a unit operator except for the normalization factor (i.e. it is a completely mixed state).

Let X be any operator (acting on A), and express it as

$$X = \sum_{kl} |k\rangle X_{kl} \langle l|.$$

Then, the following holds for a maximally entangled state $|\Psi\rangle$:

$$\begin{aligned}(X \otimes I)\,|\Psi\rangle &= \frac{1}{\sqrt{d}}\left(\sum_{kl} |k\rangle X_{kl}\langle l| \otimes I\right)\sum_{i} |i\rangle_{\mathrm{A}}|i\rangle_{\mathrm{B}} = \frac{1}{\sqrt{d}}\sum_{ki} X_{ki}|k\rangle_{\mathrm{A}}|i\rangle_{\mathrm{B}} \\ &= \frac{1}{\sqrt{d}}\left(I \otimes \sum_{il} |i\rangle X_{li}\langle l|\right)\sum_{k} |k\rangle_{\mathrm{A}}|k\rangle_{\mathrm{B}} = \left(I \otimes X^{T}\right)|\Psi\rangle, \end{aligned} \tag{7.4}$$

where T denotes a transposition. From this, when X is a real orthogonal matrix O, we have $(O \otimes O)|\Psi\rangle = (OO^{T} \otimes I)|\Psi\rangle = |\Psi\rangle$, and hence (7.1) is confirmed. Moreover, taking into account for the ambiguity of the choice of the orthogonal basis in the Schmidt decomposition (see Theorem A.4), a maximally entangled state in two d-dimensional systems has the form of $(U \otimes V)|\Psi\rangle$, which can then be rewritten as $(UV^{T} \otimes I)|\Psi\rangle = (I \otimes VU^{T})|\Psi\rangle$. Since both UV^{T} and VU^{T} are local unitary transformations, the above fact implies that all maximally entangled states are interconverted by local unitary transformations on the A's side only (or B's side only). The following four states are maximally entangled states in two qubits:

$$|\phi^{\pm}\rangle_{\mathrm{AB}} = \frac{|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} \pm |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}}{\sqrt{2}}, \quad |\psi^{\pm}\rangle_{\mathrm{AB}} = \frac{|0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}} \pm |1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}}{\sqrt{2}}. \tag{7.5}$$

All these states are all called **Bell state**, and the collection of the above four states are called a **Bell basis**, which constructs a CONS (complete orthonormal set). Since the Bell states are maximally entangled states, they are interconverted by the local unitary transformations of the Pauli matrices on A as follows:

$$\begin{aligned}|\phi^{+}\rangle_{\mathrm{AB}} &= (I \otimes I)|\phi^{+}\rangle_{\mathrm{AB}}, \\ |\psi^{+}\rangle_{\mathrm{AB}} &= (\sigma_x \otimes I)|\phi^{+}\rangle_{\mathrm{AB}}, \\ |\psi^{-}\rangle_{\mathrm{AB}} &= (i\sigma_y \otimes I)|\phi^{+}\rangle_{\mathrm{AB}}, \\ |\phi^{-}\rangle_{\mathrm{AB}} &= (\sigma_z \otimes I)|\phi^{+}\rangle_{\mathrm{AB}}. \end{aligned} \tag{7.6}$$

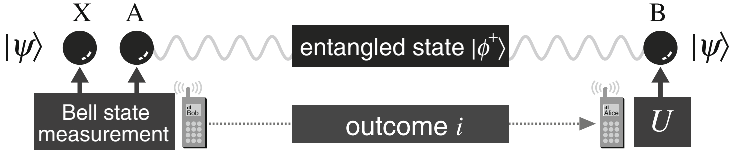


Fig. 7.1 Quantum teleportation

7.2.3 Quantum Teleportation

Quantum teleportation [4] is the most fundamental and important protocol for quantum information processing, which enables us to transfer a quantum state to a distant place utilizing an entangled state (and classical communication). Suppose that a sender and a receiver previously share the entangled state of

$$|\phi^+\rangle_{\rm AB} = \frac{|0\rangle_{\rm A}|0\rangle_{\rm B} + |1\rangle_{\rm A}|1\rangle_{\rm B}}{\sqrt{2}},$$

and they wish to teleport the state of $|\psi\rangle_{\rm X} = a|0\rangle_{\rm X} + b|1\rangle_{\rm X}$ on sender's qubit X to the receiver (Fig. 7.1). The whole state of the three qubits of X, A, and B can then be rewritten using the four Bell states (7.5) as

$$\begin{aligned}
&(a|0\rangle_{\rm X} + b|1\rangle_{\rm X}) \otimes \frac{|0\rangle_{\rm A}|0\rangle_{\rm B} + |1\rangle_{\rm A}|1\rangle_{\rm B}}{\sqrt{2}} \\
= &\frac{1}{2}\Bigg[\frac{|0\rangle_{\rm X}|0\rangle_{\rm A} + |1\rangle_{\rm X}|1\rangle_{\rm A}}{\sqrt{2}} \otimes (a|0\rangle_{\rm B} + b|1\rangle_{\rm B}) \\
&+\frac{|0\rangle_{\rm X}|0\rangle_{\rm A} - |1\rangle_{\rm X}|1\rangle_{\rm A}}{\sqrt{2}} \otimes (a|0\rangle_{\rm B} - b|1\rangle_{\rm B}) \\
&+\frac{|0\rangle_{\rm X}|1\rangle_{\rm A} + |1\rangle_{\rm X}|0\rangle_{\rm A}}{\sqrt{2}} \otimes (a|1\rangle_{\rm B} + b|0\rangle_{\rm B}) \\
&+\frac{|0\rangle_{\rm X}|1\rangle_{\rm A} - |1\rangle_{\rm X}|0\rangle_{\rm A}}{\sqrt{2}} \otimes (a|1\rangle_{\rm B} - b|0\rangle_{\rm B})\Bigg] \\
= &\frac{1}{2}\Bigg[|\phi^+\rangle_{\rm XA} \otimes (a|0\rangle_{\rm B} + b|1\rangle_{\rm B}) + |\phi^-\rangle_{\rm XA} \otimes (a|0\rangle_{\rm B} - b|1\rangle_{\rm B}) \\
&+|\psi^+\rangle_{\rm XA} \otimes (a|1\rangle_{\rm B} + b|0\rangle_{\rm B}) + |\psi^-\rangle_{\rm XA} \otimes (a|1\rangle_{\rm B} - b|0\rangle_{\rm B})\Bigg]. \qquad (7.7)
\end{aligned}$$

Here, let us suppose that the sender performs the basis measurement of the Bell basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ on the qubits X and A. This measurement on two qubits is called a **Bell state measurement**. When the sender obtains the measurement outcome of $|\phi^-\rangle$, the whole state is changed to the second term in (7.7), and hence the state of the qubit B becomes $a|0\rangle - b|1\rangle$. This state is close to $|\psi\rangle$ to be teleported, but

Table 7.1 Correcting operations in quantum teleportation

Outcome	Probability	State of B	Correcting op.	Unitary op.
$\lvert\phi^+\rangle_{\mathrm{XA}}$	1/4	$a\lvert 0\rangle_{\mathrm{B}} + b\lvert 1\rangle_{\mathrm{B}}$	nothing	I
$\lvert\phi^-\rangle_{\mathrm{XA}}$	1/4	$a\lvert 0\rangle_{\mathrm{B}} - b\lvert 1\rangle_{\mathrm{B}}$	phase flip	σ_z
$\lvert\psi^+\rangle_{\mathrm{XA}}$	1/4	$a\lvert 1\rangle_{\mathrm{B}} + b\lvert 0\rangle_{\mathrm{B}}$	bit flip	σ_x
$\lvert\psi^-\rangle_{\mathrm{XA}}$	1/4	$a\lvert 1\rangle_{\mathrm{B}} - b\lvert 0\rangle_{\mathrm{B}}$	both	$\sigma_z\sigma_x = i\sigma_y$

its phase is flipped. So, if the sender tells the receiver the measurement outcome by classical communication and the receiver applies the unitary transformation of σ_z as a correcting operation, then the state $\lvert\psi\rangle$ is reconstructed on the qubit B. This is the case for the other outcomes of the Bell state measurement. Table 7.1 summarizes the sender's outcome of the Bell state measurement, its probability, the state of the qubit B after the measurement, and the receiver's correcting operation to reconstruct $\lvert\psi\rangle$. In this way, the state of the qubit X is teleported to the qubit B, if the receiver applies one of the unitary transformations $\{I, \sigma_z, \sigma_x, \sigma_y\}$ according to the sender's measurement outcomes of $\{\lvert\phi^+\rangle, \lvert\phi^-\rangle, \lvert\psi^+\rangle, \lvert\psi^-\rangle\}$.

Note that neither the sender's operation nor the receiver's operation depends on the state $\lvert\psi\rangle$ (the operation depends neither on a nor b). This implies that they can teleport the state $\lvert\psi\rangle$ without knowing what $\lvert\psi\rangle$ is (i.e. they can teleport an unknown state). In general, if only a single copy of $\lvert\psi\rangle$ is supplied, we cannot obtain the sufficient information to determine the state $\lvert\psi\rangle$, i.e., the exact value of a and b by any measurement (to determine the values of a and b to infinite accuracy, the infinitely many identical copies of $\lvert\psi\rangle$ are necessary). Namely, it is impossible to transfer an unknown state by classical communication only. Quantum teleportation enables it by utilizing an entangled state. Moreover, if we try to directly transfer a qubit to a distant place, the state will be broken during the transmission by the effect of so-called decoherence. Quantum teleportation is beneficial in that it can transfer such a fragile quantum state by using classical communication and a previously shared entangled state, and indeed the technique of quantum teleportation enables long distance quantum cryptography through a **quantum repeater** [5].

Note further that quantum teleportation does not enable superluminal (faster than light) communication. This is because, if the receiver does not know the sender's measurement outcome, the state of the qubit B remains the reduced density operator of $\lvert\phi^+\rangle_{\mathrm{AB}}$ that is $\sigma_{\mathrm{B}} = I/2$, and hence the receiver does not obtain any information about $\lvert\psi\rangle$ from it. The receiver can get $\lvert\psi\rangle$ in her/his hand only after receiving the sender's measurement outcome via classical channel. Namely, the speed of teleporting a quantum state is constrained by the speed of classical communication.

Note finally that the schemes different from the above standard teleportation scheme have also been proposed such as continuous-variable teleportation [6, 7], where an entangled state on an infinite-adimensional Hilbert space (two-mode squeezed state) is employed, and port-based teleportation [8], where Bob has multiple output ports and can obtain the teleported state by simply selecting one of the multiple ports without any correcting operation on each port.

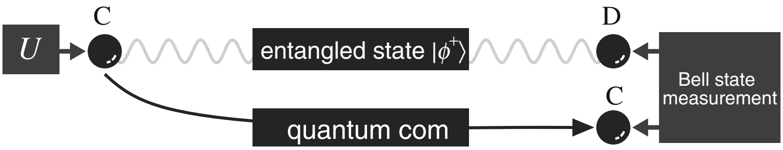


Fig. 7.2 Superdense coding

Exercise 7.1 Using the property of (7.4) for a maximally entangled state, show that quantum teleportation can also faithfully transfer a mixed state σ even if the state is entangled with another system.

7.2.4 Superdense Coding

Suppose that a single qubit is sent from a sender to a receiver. In this setting, how much classical information can be sent? If we encode the classical bit 0 (1) to the state $|0\rangle$ ($|1\rangle$) of the qubit, we can send one bit of classical information. Indeed, the maximal amount of classical information that can be sent via a single qubit is only one bit, if the qubit is not entangled with others (this is due to the fact that the upper bound of the Holevo mutual information for a single qubit is one bit (Sect. 6.3.3)). However, it becomes possible to send two bits of classical information via a single qubit if the qubit is entangled with others as shown below. This communication protocol is called **superdense coding** [9].

First, suppose that a sender and a receiver share the entangled state of (Fig. 7.2)

$$|\phi^+\rangle_{\mathrm{CD}} = \frac{|0\rangle_{\mathrm{C}}|0\rangle_{\mathrm{D}} + |1\rangle_{\mathrm{C}}|1\rangle_{\mathrm{D}}}{\sqrt{2}}.$$

The sender then applies one of the four unitary transformations $\{ I, \sigma_x, i\sigma_y, \sigma_z \}$ to the qubit C, each of which corresponds to the value of two classical bits, {00, 01, 10, 11}, the sender wishes to send. After this operation, the shared entangled state $|\phi^+\rangle_{\mathrm{CD}}$ changes to one of the four Bell states $\{|\phi^+\rangle_{\mathrm{CD}}, |\psi^+\rangle_{\mathrm{CD}}, |\psi^-\rangle_{\mathrm{CD}}, |\phi^-\rangle_{\mathrm{CD}}\}$ depending on the value of classical bits. Next, the sender sends the qubit C to the receiver. Now, since the receiver has both qubits C and D, by performing the **Bell state measurement** on them, the receiver can reliably determine which of the four Bell states $\{|\phi^+\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^-\rangle\}$, and as a result, the receiver can get two bits of classical information.

Note that, in this protocol, it appears that the sender sends only the qubit C to the receiver at first glance, but we have to take into account how they previously share the entangled state $|\phi^+\rangle_{\mathrm{CD}}$. In general, to produce an entangled state such as $|\phi^+\rangle_{\mathrm{CD}}$, the qubits must undergo some sort of interaction as will be explained in Sect. 7.3.1. Namely, in order to share $|\phi^+\rangle_{\mathrm{CD}}$, the sender needs to produce $|\phi^+\rangle_{\mathrm{CD}}$ on his/her side through the interaction between C and D, and then sends D to the receiver (it is

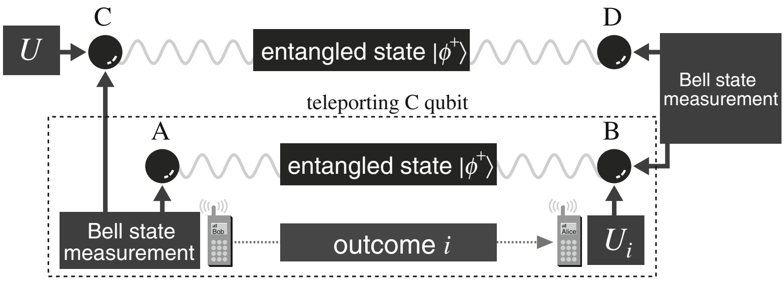


Fig. 7.3 Combining superdense coding and teleportation

of course possible that the receiver produces $|\phi^{+}\rangle_{\text{CD}}$ and sends C to the sender). In this way, taking into account the process of sharing $|\phi^{+}\rangle_{\text{CD}}$, two qubits indeed have been sent between the sender and receiver during the whole process. Superdense coding is so a protocol such that one qubit is sent previously and another is sent just when classical communication is necessary, which effectively makes classical communication twice as fast.

Here, let us consider a protocol that combines superdense coding (Fig. 7.2) and quantum teleportation (Fig. 7.1) [4] as follows: In superdense coding, the qubit C is sent from a sender to a receiver by quantum communication, but in the combined protocol, the qubit C is instead teleported as showin in Fig. 7.3 (suppose that $|\phi^{+}\rangle_{\text{AB}}$ for quantum teleportation is previously prepared in addition to $|\phi^{+}\rangle_{\text{CD}}$). Since quantum teleportation can reliably teleport a part of an entangled state such as the state of the qubit C (Exercise 7.1), the combined protocol can also transmit two bits of classical information as well as the usual superdense coding. However, in this combined protocol, no quantum communication is necessary (except for the process of sharing $|\phi^{+}\rangle_{\text{CD}}$ and $|\phi^{+}\rangle_{\text{AB}}$ for the setup). Namely, what is physically sent from the sender to the receiver is only the two classical bits, that is the outcome of the Bell state measurement in quantum teleportation. From this it is found that, in quantum teleportation, we cannot reduce the amount of classical communication from two bits at all. This is because, if the reduction would be possible, two classical bits would then be transmitted by sending less than two classical bits, which contradicts the law of physics that prohibits superluminal (faster than light) communication.

7.3 Quantifying Entanglement

7.3.1 Local Operations and Classical Communication (LOCC)

Consider a setting where any direct transmission of qubits is prohibited between two distant parties, Alice and Bob (i.e. quantum communication is prohibited). In this setting, what Alice (or Bob) can do is only to apply physical operations (measurement, unitary transformation and so on) to her (his) own qubits. These restricted operations are called **local operations** in the sense that those are applied to her (his) local qubits (on the other hand, operations applied across Alice and Bob are called **global operations**). If local operations only are allowed for Alice and Bob, they are completely isolated from each other, and hence Bob appears not to exist from Alice's point of view. So let us then consider a setting where quantum communication is still prohibited but classical communication (exchange of classical information) is allowed between Alice and Bob. Then, the following operation becomes possible: Alice measures her qubits as a local operation, she then tells the measurement outcome to Bob by classical communication, and Bob selects his subsequent local operations according to her outcomes. Such operations are called **local operations and classical communication** (**LOCC**) [3], which are quite important physical operations to understand the properties of entanglement. Quantum teleportation is considered to be a kind of LOCC (except for the process of sharing an entangled state in the setup), and many quantum protocols that utilize entanglement belong to the class of LOCC.

Here, let us consider the Kraus representation of LOCC. Suppose that Alice and Bob initially share the state denoted by the density matrix σ_{AB}. First, let Alice perform a measurement as a local operation, whose measurement operators are $\{X_i\}$ (the POVM elements are $X_i^\dagger X_i$ and $\sum_i X_i^\dagger X_i = I$). If Alice obtains the measurement outcome i_0, the state of σ_{AB} is changed to

$$\sigma_{\mathrm{AB}}^{i_0} = (X_{i_0} \otimes I)\sigma_{\mathrm{AB}}(X_{i_0} \otimes I)^\dagger.$$

Here, the normalization factor is omitted for simplicity, and note that the resultant state depends on i_0 as indicated by the suffix i_0. Next, let Alice tell the outcome i_0 to Bob by classical communication, and let Bob perform a measurement depending on i_0. Since his measurement operators depend on i_0, let us denote it by $\{Y_j^{i_0}\}$ ($\sum_j Y_j^{i_0\dagger} Y_j^{i_0} = I$). If his measurement outcome is j_0, the state is changed to

$$\sigma_{\mathrm{AB}}^{i_0 j_0} = (X_{i_0} \otimes Y_{j_0}^{i_0})\sigma_{\mathrm{AB}}(X_{i_0} \otimes Y_{j_0}^{i_0})^\dagger.$$

Moreover, let Alice perform a measurement with measurement operators $\{X_k^{i_0 j_0}\}$, which depend on i_0 and j_0, and let the outcome be k_0. The state is then changed to

$$\sigma_{\mathrm{AB}}^{i_0 j_0 k_0} = (X_{k_0}^{i_0 j_0} X_{i_0} \otimes Y_{j_0}^{i_0})\sigma_{\mathrm{AB}}(X_{k_0}^{i_0 j_0} X_{i_0} \otimes Y_{j_0}^{i_0})^\dagger. \tag{7.8}$$

By repeating this, we obtain the Kraus representation of general LOCC, but it is too complicated to write down.

However, denoting $l = (i, j, k)$, $M_l = X_k^{ij} X_i$, and $N_l = Y_j^i$, the post-measurement state in (7.8) is rewritten as $\sigma_{\mathrm{AB}}^l = (M_l \otimes N_l)\sigma_{\mathrm{AB}}(M_l \otimes N_l)^\dagger$. Namely, the measurement operators in LOCC are represented by a tensor product of Alice's and Bob's operators. Taking into account more general local operations (i.e. local CP maps) other than local measurements, general LOCC has the following form of the Kraus representation (without normalization):

$$\sigma'_{\mathrm{AB}} = \sum_l (M_l \otimes N_l)\sigma_{\mathrm{AB}}(M_l \otimes N_l)^\dagger. \tag{7.9}$$

The converse is not true in general, and indeed it has been shown that some physical operation that is described by the form of (7.9) cannot be realized by LOCC [10]. Therefore, the operations of having the form of (7.9) are a little more unrestricted than LOCC, and are called **separable operations** in the sense that the Kraus operators are described by a tensor product of Alice's and Bob's operators (and are separated). The separable operations are also important physical operations to understand the properties of entanglement.

Suppose now that Alice and Bob initially share an unentangled pure state $|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}$. The substitution of $|0\rangle\langle 0| \otimes |0\rangle\langle 0|$ into σ_{AB} in (7.9) yields the following observation: When we apply LOCC (or separable operations) to the joint system A and B with the unentangled state $|0\rangle\langle 0| \otimes |0\rangle\langle 0|$, the resultant state has the form of

$$\sigma'_{\mathrm{AB}} = \sum_l M_l|0\rangle\langle 0|M_l^\dagger \otimes N_l|0\rangle\langle 0|N_l^\dagger.$$

This state is a probabilistic mixture of unentangled pure states $M_l|0\rangle_{\mathrm{A}}N_l|0\rangle_{\mathrm{B}}$, and it is considered to be still unentangled. Namely, LOCC has the property such that it cannot produce any entangled state from unentangled states. In order to produce an entangled state of two qubits, a global operation across the two qubits such as an interaction between the qubits is indispensable, and LOCC that is mere a combination of local operations cannot newly create entanglement. This property of LOCC plays a crucial role in quantifying entanglement as shown in the following sections.

7.3.2 Basic Unit of Entanglement

For the purpose of quantifying entanglement, a basic unit to measure the amount of entanglement should be determined. It is useful to choose a maximally entangled state in two qubits as the basic unit. Since this state is also called the EPR state after the EPR paradox [1], let us denote it by $|\mathrm{EPR}\rangle$ hereafter, i.e.

$$|\mathrm{EPR}\rangle = \frac{|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}}{\sqrt{2}}.$$

This basic unit of entanglement is called an **entangled bit**, in short **ebit**. Namely, the amount of entanglement contained in $|\mathrm{EPR}\rangle$ is defined as 1 ebit.

In this choice of the basic unit, how much amount of entanglement does a maximally entangled state on two d-dimensional systems (the state of (7.3)) have? For simplicity, let us consider the case $d = 2^s$ with s being a positive integer.

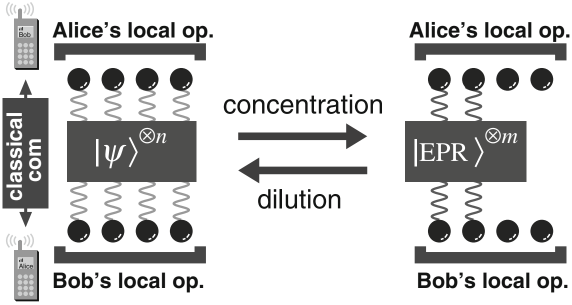


Fig. 7.4 Entanglement concentration and dilution

The state of (7.3) is a superposition of 2^s terms from $|0\rangle_\mathrm{A}|0\rangle_\mathrm{B}$ to $|2^s-1\rangle_\mathrm{A}|2^s-1\rangle_\mathrm{B}$, but let us represent each term in binary and regard 0 (1) in the binary representation as the state $|0\rangle$ ($|1\rangle$) in a qubit. Then we have

$$\begin{aligned}
|\Psi\rangle &= \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle_\mathrm{A}|i\rangle_\mathrm{B} \\
&= \frac{1}{\sqrt{2^s}}\Big(|0\rangle_\mathrm{A}|0\rangle_\mathrm{B} + |1\rangle_\mathrm{A}|1\rangle_\mathrm{B} + \cdots + |2^s-1\rangle_\mathrm{A}|2^s-1\rangle_\mathrm{B}\Big) \\
&= \frac{1}{\sqrt{2^s}}\Big(|0\cdots 00\rangle_\mathrm{A}|0\cdots 00\rangle_\mathrm{B} + |0\cdots 01\rangle_\mathrm{A}|0\cdots 01\rangle_\mathrm{B} \\
&\qquad\qquad + \cdots + |1\cdots 11\rangle_\mathrm{A}|1\cdots 11\rangle_\mathrm{B}\Big) \\
&= \Big(\frac{|0\rangle_\mathrm{A}|0\rangle_\mathrm{B}+|1\rangle_\mathrm{A}|1\rangle_\mathrm{B}}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle_\mathrm{A}|0\rangle_\mathrm{B}+|1\rangle_\mathrm{A}|1\rangle_\mathrm{B}}{\sqrt{2}}\Big) \otimes \cdots \\
&= |\mathrm{EPR}\rangle^{\otimes s},
\end{aligned} \tag{7.10}$$

which is hence equivalent to a collection of s pairs of $|\mathrm{EPR}\rangle$. Namely, the amount of entanglement of $|\Psi\rangle$ is $s = \log d$ ebits. This can be extended for general d other than $d = 2^s$ (see the subsequent sections for detail), and the amount of entanglement of a maximally entangled state, in which d terms are superposed with equal weight, is $\log d$ ebits.

7.3.3 Entanglement Concentration

As shown in Sect. 7.3.1, LOCC cannot newly create entanglement but can "concentrate" or "dilute" entanglement (Fig. 7.4). For example, suppose that there are n pairs of the following state of two qubits:

$$|\psi\rangle = \sqrt{p}|0\rangle_\mathrm{A}|0\rangle_\mathrm{B} + \sqrt{1-p}|1\rangle_\mathrm{A}|1\rangle_\mathrm{B}. \tag{7.11}$$

It is then possible to convert it and obtain m pairs of $|\mathrm{EPR}\rangle$ by LOCC. In this LOCC conversion, the most strongly entangled state $|\mathrm{EPR}\rangle$ is obtained from the weakly entangled state $|\psi\rangle$. But, in general, this conversion is possible only when $n > m$, because LOCC cannot newly create entanglement. Namely, a small number of strongly entangled states are extracted from a large number of weakly entangled states, and hence this LOCC conversion is called **entanglement concentration** [11] (the converse process is called **entanglement dilution** [11]).

Now, let us express the LOCC conversion of entanglement concentration as

$$|\psi\rangle^{\otimes n} \longrightarrow |\mathrm{EPR}\rangle^{\otimes m},$$

and let us take a concrete look at how this task is achieved by LOCC. To begin with, consider the case $n = 2$ for simplicity, where Alice and Bob each have two qubits initially. First, on the two qubits, Alice applies the measurement to determine the number of qubits (denoted by k) whose state is in $|1\rangle$. The Alice's measurement $\{\Pi_k\}_{k=0}^{2}$ is given by

$$\Pi_0 = |00\rangle\langle 00|, \quad \Pi_1 = |01\rangle\langle 01| + |10\rangle\langle 10|, \quad \Pi_2 = |11\rangle\langle 11|,$$

which can be realized by using a two-qubit quantum gate such as a CNOT gate. This is a local operation of Alice. The initial state $|\psi\rangle^{\otimes 2}$ is expanded as

$$\begin{aligned}|\psi\rangle^{\otimes 2} &= \left(\sqrt{p}|0\rangle_\mathrm{A}|0\rangle_\mathrm{B} + \sqrt{1-p}|1\rangle_\mathrm{A}|1\rangle_\mathrm{B}\right)^{\otimes 2} \\ &= p|00\rangle_\mathrm{A}|00\rangle_\mathrm{B} \\ &\quad + \sqrt{2p(1-p)}\frac{|01\rangle_\mathrm{A}|01\rangle_\mathrm{B} + |10\rangle_\mathrm{A}|10\rangle_\mathrm{B}}{\sqrt{2}} \\ &\quad + (1-p)|11\rangle_\mathrm{A}|11\rangle_\mathrm{B}.\end{aligned}$$

Therefore, when Alice obtains the outcome of $k = 0$ (or $k = 2$), $|\psi\rangle^{\otimes 2}$ is changed to the first term of $|00\rangle_\mathrm{A}|00\rangle_\mathrm{B}$ (or the third term of $|11\rangle_\mathrm{A}|11\rangle_\mathrm{B}$), but those are unentangled and hence the task of concentration fails. On the other hand, Alice can obtain the outcome of $k = 1$ with the probability of $2p(1-p)$, and $|\psi\rangle^{\otimes 2}$ is then changed to the second term, which is an entangled state. Let us denote it by $|\chi\rangle$:

$$|\chi\rangle = \frac{|01\rangle_\mathrm{A}|01\rangle_\mathrm{B} + |10\rangle_\mathrm{A}|10\rangle_\mathrm{B}}{\sqrt{2}}.$$

Note here that the local measurement of Alice must obtain the information of the number of $|1\rangle$ only; the state of each qubit must not be determined. If Alice's measurement completely determines the state of each qubit, and hence discriminates between $|01\rangle_\mathrm{A}$ and $|10\rangle_\mathrm{A}$, the entanglement of $|\chi\rangle$ is also destroyed by the measurement and the task of concentration does not work well.

When Alice obtains the measurement outcome of $k = 1$, she tells it to Bob by classical communication, and next both Alice and Bob apply the unitary transformation of exchanging $|01\rangle \leftrightarrow |00\rangle$ to her/his two qubits. By those local operations of Alice and Bob, $|\chi\rangle$ is converted to

$$|\chi\rangle \longrightarrow \frac{|00\rangle_{\mathrm{A}}|00\rangle_{\mathrm{B}} + |10\rangle_{\mathrm{A}}|10\rangle_{\mathrm{B}}}{\sqrt{2}} = |\mathrm{EPR}\rangle|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}},$$

and as a result, they can finally obtain a pair of $|\mathrm{EPR}\rangle$. To summarize, Alice and Bob succeed the task of $|\psi\rangle^{\otimes 2} \longrightarrow |\mathrm{EPR}\rangle^{\otimes 1}$ with the probability of $2p(1-p)$ by LOCC.

Let us extend the above concentration process to the case of large n. Expanding $|\psi\rangle^{\otimes n}$ and classifying the terms by the number of $|1\rangle$'s contained in each term (there are $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ states such that k qubits among the whole n qubits are in $|1\rangle$), we have

$$\begin{aligned} |\psi\rangle^{\otimes n} &= \left(\sqrt{p}|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + \sqrt{1-p}|1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}\right)^{\otimes n} \\ &= \sum_{k=0}^{n} \sqrt{p^{n-k}(1-p)^k}\Big(\underbrace{\cdots + |k\ 1\text{'s exist}\rangle_{\mathrm{A}}|k\ 1\text{'s exist}\rangle_{\mathrm{B}} + \cdots}_{\text{superposition of}\binom{n}{k}\text{terms}}\Big) \end{aligned} \tag{7.12}$$

Therefore, if Alice performs the local measurement to determine the number of $|1\rangle$'s, the probability of obtaining the outcome k is $\binom{n}{k}p^{n-k}(1-p)^k$, and the state is changed to the state in parentheses of (7.12). Since the collapsed state is a maximally entangled state, in which $d \equiv \binom{n}{k}$ terms are superposed with equal weight, the amount of entanglement is $\log d = \log\binom{n}{k}$ ebits as mentioned in Sect. 7.3.2. Indeed, as explicitly shown later, given k, Alice and Bob can extract $\log\binom{n}{k}$ pairs of $|\mathrm{EPR}\rangle$ on average by LOCC from the collapsed state.

Now, we consider the case $n \to \infty$ by using the law of large numbers. Alice has the outcome of $k = n(1-p)$ with the probability close to 1. Using Stirling's formula ($\log_e n! \approx n \log_e n - n$), the expected value of the number of $|\mathrm{EPR}\rangle$ obtained by LOCC is

$$\begin{aligned} m &= \sum_{k=0}^{n}\binom{n}{k}p^{n-k}(1-p)^k \log\binom{n}{k} \approx \sum_{k=0}^{n}\binom{n}{k}p^{n-k}(1-p)^k \log\binom{n}{n(1-p)} \\ &= \log\binom{n}{n(1-p)} \approx n\big[-p\log p - (1-p)\log(1-p)\big] = nh(p), \end{aligned} \tag{7.13}$$

where $h(p)$ is the **binary entropy**. Namely, in the limit of $n \to \infty$, the following task of concentration

$$|\psi\rangle^{\otimes n} \longrightarrow |\mathrm{EPR}\rangle^{\otimes nh(p)} \tag{7.14}$$

is possible.[1] It will be found that the above process is optimal (maximal possible number of $|\mathrm{EPR}\rangle$ is extracted) considering together with entanglement dilution explained in Sect. 7.3.5.

Finally, let us show that $\log d$ pairs of $|\mathrm{EPR}\rangle$ on average can be extracted by LOCC from a maximally entangled state consisting of d terms [$|\Psi\rangle$ in (7.3)], when

[1] Note that m was evaluated in the leading order of n in (7.13), and hence (7.14) should be precisely written as $|\psi\rangle^{\otimes n} \to |\mathrm{EPR}\rangle^{\otimes(nh(p)+o(n))}$.

sufficiently many identical copies of $|\psi\rangle$ are supplied. When d is equal to an integer power of 2 ($d = 2^s$ with s being an integer), it is obvious from (7.10) that $s = \log d$ pairs of $|\mathrm{EPR}\rangle$ can be extracted by an appropriate local unitary transformation of Alice (or Bob). For general d other than $d = 2^s$, let us consider $|\Psi\rangle^{\otimes l}$ with l being a positive integer. Since $|\Psi\rangle^{\otimes l}$ is a superposition of d^l orthogonal states, let J_0 be the integer part of $\log d^l$. Similarly, let J_1 be the integer part of $\log(d^l - 2^{J_0})$. Repeating this until the decimal part of $\log(d^l - 2^{J_0} - \cdots)$ vanishes, we have

$$\begin{aligned} \lfloor \log d^l \rfloor &= J_0 \\ \lfloor \log(d^l - 2^{J_0}) \rfloor &= J_1 \\ &\cdots \\ \log(d^l - 2^{J_0} - \cdots - 2^{J_{e-1}}) &= J_e. \end{aligned}$$

By this, we have

$$d^l = \sum_{i=0}^{e} 2^{J_i},$$

and d^l is decomposed as a sum of integer powers of 2 (this is equivalent to consider the binary representation of d^l). In the same way concerning $|\Psi\rangle^{\otimes l}$, the d^l-dimensional Hilbert space of Alice is decomposed as a sum of subspaces whose each dimension is an integer power of 2. Let Alice then perform a local measurement on $|\Psi\rangle^{\otimes l}$ to project on one of those subspaces. Since the state after the projection is a superposition of 2^{J_i} terms when the measurement outcome is i, it is possible to convert it to J_i pairs of $|\mathrm{EPR}\rangle$ by a local unitary transformation. Since the probability of projecting on 2^{J_i}-dimensional subspace is $2^{J_i}/d^l$, x pairs of $|\mathrm{EPR}\rangle$ can be extracted from $|\Psi\rangle^{\otimes l}$ on average, where x is given by

$$x = \sum_{i=0}^{e} \frac{2^{J_i}}{d^l} J_i.$$

Since $x/l \to \log d$ in the limit of $l \to \infty$, it is found that $\log d$ pairs of $|\mathrm{EPR}\rangle$ on average can be extracted per one pair of $|\Psi\rangle$.

Exercise 7.2 Show that $\displaystyle\lim_{l\to\infty} \frac{1}{l} \sum_{i=0}^{e} \frac{2^{J_i}}{d^l} J_i = \log d$.

7.3.4 Quantum Data Compression

In usual classical information processing, it is frequently performed to compress data and decompress it, in the purpose of increasing efficiency of data transmission, efficient use of memory, and so on. Quantum states can also be compressed and decompressed as shown in this section, which is necessary to understand entanglement dilution explained in the next section. The protocol is called **quantum data compression** [12].

Suppose that there are n pairs of the entangled state $|\psi\rangle$ in (7.11). The purpose here is to compress the state of Bob's n qubits, and later recover it. However, the compression and decompression must be performed so as not to destroy the entanglement with Alice's qubits. Expanding $|\psi\rangle^{\otimes n}$ into 2^n terms from $|0\cdots0\rangle_\mathrm{A}|0\cdots0\rangle_\mathrm{B}$ to $|1\cdots1\rangle_\mathrm{A}|1\cdots1\rangle_\mathrm{B}$, and denoting each term by $|x_1\cdots x_n\rangle_\mathrm{A}|x_1\cdots x_n\rangle_\mathrm{B}$, we have

$$|\psi\rangle^{\otimes n} = \sum_{x_1=0}^{1}\cdots\sum_{x_n=0}^{1}\sqrt{q(x_1)\cdots q(x_n)}|x_1\cdots x_n\rangle_\mathrm{A}|x_1\cdots x_n\rangle_\mathrm{B},$$

where $q(0)=p, q(1)=(1-p)$. If Bob measures n qubits in the basis of $\{|0\rangle,|1\rangle\}$, the state of $|x_1,\cdots,x_n\rangle_\mathrm{B}$ is obtained with the probability of $Q(x_1,\cdots,x_n)\equiv q(x_1)\cdots q(x_n)$. Since the measurement on each qubit is independent, according to the law of large numbers, there exists an integer n_0 such that for $n>n_0$

$$P\left(\left|-\frac{1}{n}\log Q(x_1,\ldots,x_n)-h(p)\right|>\delta\right)<\epsilon$$

for any $\delta,\epsilon>0$ (see Sect. 6.2.2 for detail). In other words, with the probability more than or equal to $1-\epsilon$, the sequences of $x_1,\cdots,x_n$ satisfying that

$$\left|-\frac{1}{n}\log Q(x_1,\ldots,x_n)-h(p)\right|\leq\delta \tag{7.15}$$

are obtained, but since ϵ can be arbitrary small for large n limit, the sequences satisfying (7.15) are obtained with the probability close to 1. Such a sequence is called a **typical sequence** (contrary, a sequence other than typical sequences is called an **atypical sequence**). From (7.15), the probability $Q(x_1,\ldots,x_n)$ of obtaining one of typical sequences satisfies

$$2^{-n(h(p)-\delta)}\geq Q(x_1,\ldots,x_n)\geq 2^{-n(h(p)+\delta)}.$$

Therefore, denoting the number of the typical sequences by ν, we have

$$1\geq\sum_{\text{typical}}Q(x_1,\ldots,x_n)\geq\sum_{\text{typical}}2^{-n(h(p)+\delta)}=\nu 2^{-n(h(p)+\delta)},$$

and hence ν is upper bounded by

$$\nu\leq 2^{n(h(p)+\delta)}. \tag{7.16}$$

Table 7.2 Unitary transformation for quantum data compression (in the case where the number of typical sequences ν is an integer power of 2 for simplicity)

Expanded terms $\lvert x_1, \ldots, x_n\rangle$	Number	Destination
Typical sequences		
$\lvert$1st of typical sequences$\rangle_{\mathrm{B}}$	0	$\lvert 0\cdots000\cdots00\rangle_{\mathrm{B}}$
$\lvert$2nd of typical sequences$\rangle_{\mathrm{B}}$	1	$\lvert 0\cdots000\cdots01\rangle_{\mathrm{B}}$
...	...	...
$\lvert\nu$th of typical sequences$\rangle_{\mathrm{B}}$	$\nu - 1$	$\lvert 0\cdots00\underbrace{1\cdots11}_{m}\rangle_{\mathrm{B}}$
Atypical sequences		
$\lvert$1st of atypical sequences$\rangle_{\mathrm{B}}$	ν	$\lvert 0\cdots010\cdots00\rangle_{\mathrm{B}}$
$\lvert$2nd of atypical sequences$\rangle_{\mathrm{B}}$	$\nu + 1$	$\lvert 0\cdots010\cdots01\rangle_{\mathrm{B}}$
...	...	...
$\lvert(2^n - \nu)$th of atypical sequences$\rangle_{\mathrm{B}}$	$2^n - 1$	$\lvert 1\cdots11\underbrace{1\cdots11}_{m}\rangle_{\mathrm{B}}$

With the above in mind, let us consider the following protocol of quantum data compression: First, as shown in Table 7.2, let us number the states of $\lvert x_1, \ldots, x_n\rangle$ from 0 to $\nu - 1$ in the case where $x_1, \ldots, x_n$ is a typical sequence. In the case where $x_1, \ldots, x_n$ is an atypical sequence, let us number the states from ν to $2^n - 1$. Let us then regard the binary representations of those numbers as destination states of Bob's n qubits (see the column of destination in Table 7.2). Bob then applies unitary transformation U, which maps $\lvert x_1, \ldots, x_n\rangle$ to the corresponding destination state (this transformation is unitary because it only exchanges the 2^n basis states). Now, looking at the column of destination in Table 7.2, it is found that the first part of the destination states of typical sequences is commonly $\lvert 0\cdots 0\rangle$. Since the upper bound of the number of typical sequences is given by (7.16), the states of the first $(n - m)$ qubits, at least, are all in $\lvert 0\rangle$, where

$$m \equiv \lceil n(h(p) + \delta)\rceil .$$

Next, Bob measures the first $(n - m)$ qubits and project them onto $\lvert 0\rangle$. Since this projection succeeds at least with the probability of obtaining a typical sequence, the probability of success satisfies $P_{\text{success}} \geq 1 - \epsilon$, which approaches to 1 for large n limit. Moreover, after the success of the projection, since the states of the Bob's first $(n - m)$ qubits are all in $\lvert 0\rangle$, those are unentangled with Alice's qubits and are redundant. Therefore, we can discard the first $(n - m)$ qubits, and as a result, the state of Bob's n qubits is compressed into the remaining $m = \lceil n(h(p) + \delta)\rceil$ qubits. Since δ can be arbitrary small for large n limit, the compression rate in the limit of $n \to \infty$ is

$$\frac{m}{n} = \frac{\lceil n(h(p) + \delta)\rceil}{n} \to h(p). \tag{7.17}$$

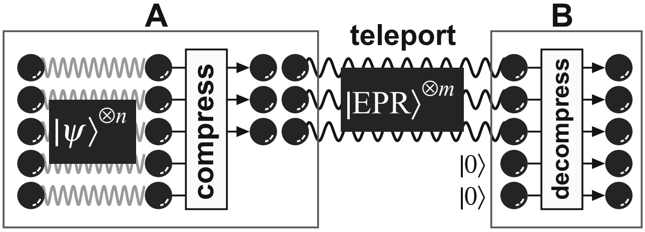

A
B
teleport
$|\psi\rangle^{\otimes n}$
compress
$|\mathrm{EPR}\rangle^{\otimes m}$
$|0\rangle$
$|0\rangle$
decompress

Fig. 7.5 Entanglement dilution

It will be found that this rate is optimal considering together with entanglement dilution explained in Sect. 7.3.5.

The state after the above compression of $|\psi\rangle^{\otimes n}$ is

$$|\mathrm{comp}\rangle = \frac{1}{\sqrt{P_{success}}}\langle\underbrace{0\cdots 00}_{n-m}|U|\psi\rangle^{\otimes n}.$$

To recover the original state, it is enough to add $(n-m)$ qubits, which are all in $|0\rangle$, to $|\mathrm{comp}\rangle$, and apply unitary transformation U^{-1} to the n qubits. The state after this recovering operation is $U^{-1}|0\cdots 00\rangle_{\mathrm{B}}|\mathrm{comp}\rangle$, and the fidelity with the original state $|\psi\rangle^{\otimes n}$ is then given by

$$\left|(\langle\psi|)^{\otimes n}U^{-1}|0\cdots 00\rangle_{\mathrm{B}}|\mathrm{comp}\rangle\right| = \sqrt{P_{\mathrm{success}}}\langle\mathrm{comp}|\mathrm{comp}\rangle \geq \sqrt{1-\epsilon},$$

which asymptotically approaches to 1 for large n limit, and hence the original state is certainly recovered. To summarize, it is possible to compress the state of n qubits of Bob into $nh(p)$ qubits and to later recover $|\psi\rangle^{\otimes n}$ without destroying the entanglement.

7.3.5 *Entanglement Dilution*

Entanglement dilution [11] is a converse process of entanglement concentration, that is the LOCC conversion of $|\mathrm{EPR}\rangle^{\otimes m} \longrightarrow |\psi\rangle^{\otimes n}$, where $|\psi\rangle$ is again given by (7.11). To achieve the task of entanglement dilution, Alice first prepares $2n$ qubits in the state of $|\psi\rangle^{\otimes n}$ (Fig. 7.5). This state preparation can be done as her local operation, because she has all $2n$ qubits in her hands. Alice then keeps a half of $2n$ qubits, namely n qubits, and compresses the other half (this half will be teleported to Bob later) by quantum data compression.

Next, the state of $nh(p)$ qubits after the compression is transfered to Bob by quantum teleportation (Fig. 7.5). To achieve the teleportation, $nh(p)$ pairs of $|\mathrm{EPR}\rangle$ are necessary (whose number is the same as the number of qubits to be teleported). The purpose of previously performing quantum data compression is to reduce the number of $|\mathrm{EPR}\rangle$ used in the teleportation as far as possible. Finally, Bob recovers the original state from the teleported state. To do this, $n - nh(p)$ qubits, which are all in $|0\rangle$, are necessary, but Bob can prepare it by his local operation, because those are unentangled with Alice.

In this way, the entangled half of $|\psi\rangle^{\otimes n}$ is compressed, teleported, recovered. Finally, Alice and Bob can share the entangled state of $|\psi\rangle^{\otimes n}$. The entanglement of $|\mathrm{EPR}\rangle$ used in the teleportation is destroyed and it is changed to an unentangled state. Instead of the state $|\mathrm{EPR}\rangle^{\otimes nh(p)}$ initially shared between Alice and Bob, they can newly share $|\psi\rangle^{\otimes n}$, and as a result, the LOCC conversion of

$$|\mathrm{EPR}\rangle^{\otimes nh(p)} \longrightarrow |\psi\rangle^{\otimes n} \tag{7.18}$$

is apparently achieved.[2]

In this protocol of entanglement dilution, one-way classical communication only from Alice to Bob arises. Such LOCC with one-way classical communication is called **1-way LOCC**, and LOCC with two-way (bi-directional) classical communication is called **2-way LOCC**. Concerning LOCC processing on bipartite pure states, for every 2-way LOCC, there always exists 1-way LOCC equivalent to it as shown below [13]. By virtue of the Schmidt decomposition (see Theorem A.4), a bipartite pure state $|\psi\rangle$ is written as

$$|\psi\rangle = (U \otimes V) \sum_i \sqrt{p_i} |i\rangle_{\mathrm{A}} |i\rangle_{\mathrm{B}},$$

where $(U \otimes V)$ is an appropriate local unitary transformation. Let Bob perform a measurement on $|\psi\rangle$, whose measurement operators are written as

$$M_i = \sum_{jk} m^i_{jk} V |j\rangle\langle k| V^\dagger,$$

where $\sum_i M_i^\dagger M_i = I$. When Bob obtains the outcome i_0, $|\psi\rangle$ is changed to

$$(I \otimes M_{i_0})|\psi\rangle = (U \otimes V) \sum_{ij} m^{i_0}_{ji} \sqrt{p_i} |i\rangle_{\mathrm{A}} |j\rangle_{\mathrm{B}} \equiv (U \otimes V)|\chi\rangle_{\mathrm{AB}}.$$

On the other hand, when Alice performs a measurement whose measurement operators are

$$M'_i = \sum_{jk} m^i_{jk} U |j\rangle\langle k| U^\dagger,$$

and when she obtains the outcome i_0, $|\psi\rangle$ is changed to

[2] The precise meaning of (7.18) is $|\mathrm{EPR}\rangle^{\otimes(nh(p)+o(n))} \rightarrow |\psi\rangle^{\otimes n}$ (see e.g. (7.17)) as in the case of entanglement concentration.

$$(M'_{i_0} \otimes I)|\psi\rangle = (U \otimes V) \sum_{ij} m^{i_0}_{ji} \sqrt{p_i} |j\rangle_{\mathrm{A}} |i\rangle_{\mathrm{B}} = (U \otimes V)|\chi\rangle_{\mathrm{BA}}.$$

Since $|\chi\rangle_{\mathrm{AB}}$ and $|\chi\rangle_{\mathrm{BA}}$ have the same Schmidt coefficients, they are related through $|\chi\rangle_{\mathrm{AB}} = (Q \otimes R)|\chi\rangle_{\mathrm{BA}}$ with $(Q \otimes R)$ being an appropriate local unitary transformation. From the above, we have

$$(I \otimes M_{i_0})|\psi\rangle = (UQU^{\dagger} \otimes VRV^{\dagger})(M'_{i_0} \otimes I)|\psi\rangle,$$

and therefore, Bob's local measurement is always replaced by Alice's local measurement and Bob's local unitary transformation. When Alice acts on behalf of Bob's measurement, classical communication from Bob to Alice becomes unnecessary. However, since R depends on the outcome i_0, classical communication from Alice to Bob is still necessary. In this way, concerning the LOCC process on bipartite pure states, it is enough to consider one-way classical communication from Alice to Bob. In the protocol of entanglement concentration in Sect. 7.3.3, if Bob also performs the same local measurements as Alice, Bob can obtain the same outcomes of Alice, and hence classical communication itself becomes unnecessary in this case. Note that, in the above discussion, it is assumed that Alice and Bob initially know what the state $|\psi\rangle$ is, and hence the above discussion cannot be applied to the case where $|\psi\rangle$ is unnkown.

7.3.6 Amount of Entanglement

Considering entanglement concentration (7.14) and dilution (7.18) together, it is found that Alice and Bob can achieve the reversible conversion of

$$|\mathrm{EPR}\rangle^{\otimes nh(p)} \longleftrightarrow |\psi\rangle^{\otimes n} \tag{7.19}$$

by LOCC (for large n limit). This reversibility plays a crucial role in quantifying entanglement. Since LOCC cannot newly create entanglement, the fact that the conversion cycle of

$$|\mathrm{EPR}\rangle^{\otimes nh(p)} \longrightarrow |\psi\rangle^{\otimes n} \longrightarrow |\mathrm{EPR}\rangle^{\otimes nh(p)} \tag{7.20}$$

is possible implies that there is no loss of entanglement during this cycle[3] (if there would be loss of entanglement, the cycle does not complete because LOCC cannot supply the loss of entanglement). Since there is no loss of entanglement, the amount of entanglement contained in $|\psi\rangle^{\otimes n}$ and $|\mathrm{EPR}\rangle^{\otimes nh(p)}$ is equal to each other, and

[3] Precisely, the exact cycle of (7.20) is impossible even in the limit $n \to \infty$. This is because the two conversion rates coincide only in the leading order of n, and moreover the final state of (7.18) is close to but not equal to the initial state of (7.14). To complete the above cycle exactly, we need to consume the excess entanglement of the amount $o(n)$ [14].

hence the amount of a pair of $|\psi\rangle$ is equal to the amount of $h(p)$ pairs of $|\mathrm{EPR}\rangle$. Namely, the amount of entanglement of $|\psi\rangle$ is determined to be $h(p)$ ebits.

Moreover, the completeness of the cycle of (7.20) implies that $h(p)$ is the optimal rate for both entanglement concentration and dilution. This is because, if entanglement concentration with a higher rate than $h(p)$ would be possible, more pairs of $|\mathrm{EPR}\rangle$ would then be obtained by LOCC than the initial $|\mathrm{EPR}\rangle^{nh(p)}$, which contradict that LOCC cannot newly create entanglement. A similar discussion can be applied to the case for entanglement dilution. Moreover, if quantum data compression with a smaller rate than $h(p)$ would be possible, entanglement dilution with the smaller rate would be possible, which causes a contradiction. Therefore, $h(p)$ is the optimal rate for quantum data compression also.

So far, the amount of entanglement for the state of (7.11) in two qubits was shown to be $h(p)$. What about the case where $|\psi\rangle$ is a general bipartite pure state (with a higher dimension). In this case, denoting the reduced density operators of $|\psi\rangle_{\mathrm{AB}}$ by $\sigma_{\mathrm{A}} = \mathrm{Tr}_{\mathrm{B}}|\psi\rangle\langle\psi|$ and $\sigma_{\mathrm{B}} = \mathrm{Tr}_{\mathrm{A}}|\psi\rangle\langle\psi|$, and replacing $h(p)$ by $H(\sigma_{\mathrm{A}})$ (or by $H(\sigma_{\mathrm{B}})$—it comes to the same thing due to the Schmidt decomposition), the same discussions hold for entanglement concentration, dilution, and quantum data compression. Here, $H(\sigma)$ is the von Neumann entropy of density operator σ. Namely, we have the following:

Theorem 7.1 *Let $|\psi\rangle$ be a bipartite pure state between Alice and Bob, and σ_{A} and σ_{B} be the reduced density operators. The amount of entanglement of $|\psi\rangle$ is then $H(\sigma_{\mathrm{A}}) = H(\sigma_{\mathrm{B}})$ ebits.*

7.4 Multipartite Entanglement

7.4.1 GHZ and W State

Let us consider the entangled state on three qubits A, B, and C:

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|0\rangle_{\mathrm{C}} + |1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}|1\rangle_{\mathrm{C}}\right).$$

This state is called the **Greenberger-Horne-Zeilinger state** (GHZ state). The reduced density operators of AB, BC, and AC are all equal to

$$\sigma_{\mathrm{AB}} = \sigma_{\mathrm{BC}} = \sigma_{\mathrm{AC}} = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|,$$

which is a probabilistic mixture of unentangled states, and hence every pair of three qubits is not entangled. However, since $|\mathrm{GHZ}\rangle$ is written as

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(\frac{|00\rangle_{\mathrm{AB}} + |11\rangle_{\mathrm{AB}}}{\sqrt{2}} \otimes \frac{|0\rangle_{\mathrm{C}} + |1\rangle_{\mathrm{C}}}{\sqrt{2}} + \frac{|00\rangle_{\mathrm{AB}} - |11\rangle_{\mathrm{AB}}}{\sqrt{2}} \otimes \frac{|0\rangle_{\mathrm{C}} - |1\rangle_{\mathrm{C}}}{\sqrt{2}}),$$

when C is measured in the basis of $(|0\rangle \pm |1\rangle)/\sqrt{2}$, the state of AB is then always converted into $|\mathrm{EPR}\rangle_{\mathrm{AB}}$, despite that the state was initially an unentangled σ_{AB}. Indeed, when the measurement outcome corresponds to $(|0\rangle - |1\rangle)/\sqrt{2}$, for example, Alice's phase-flipped operation ($|1\rangle \rightarrow -|1\rangle$) results in $|\mathrm{EPR}\rangle_{\mathrm{AB}}$. In this way, much more complicated operations are possible by LOCC in multipartite settings than in bipartite settings.

Moreover, the Schmidt decomposition cannot be applied to multipartite entangled states. This makes the properties of multipartite entanglement more complicated. For example, let us consider the following entangled state in three qubits:

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}\left(|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|1\rangle_{\mathrm{C}} + |0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}|0\rangle_{\mathrm{C}} + |1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|0\rangle_{\mathrm{C}}\right),$$

which is called **W state** [15]. Contrary to the bipartite case, this state cannot be expressed in the form of $\sqrt{p}|000\rangle + \sqrt{1-p}|111\rangle$ no matter how select the local basis of A, B, and C. As will be shown in the following sections, $|\mathrm{GHZ}\rangle$ and $|\mathrm{W}\rangle$ are entangled in completely different ways (each has a different type of entanglement).

Note that the Schmidt decomposition (see Theorem A.4) can be applied even for multipartite entangled states if the parties are grouped into two, such as A and BC, and the Schmidt decomposition can be used to judge whether the two groups are entangled or not. Let us denote, for example, the grouping by A:BC. When a multipartite pure state is given, we can judge whether the state is entangled or not by investigating the Schmidt decomposition for all possible groupings. For example, in the case of a four-partite pure state on ABCD, if and only if any of the seven groupings of A:BCD, B:ACD, C:ABD, D:ABC, AB:CD, AC:BD, AD:BC is not entangled, the state is written as a product state of $|f\rangle_{\mathrm{A}} \otimes |g\rangle_{\mathrm{B}} \otimes |h\rangle_{\mathrm{C}} \otimes |i\rangle_{D}$ and hence it is not entangled.

7.4.2 Stochastic LOCC

Suppose that a pure state $|\psi\rangle$ of three parties is converted into another pure state $|\phi\rangle$ by LOCC. As in (7.9), $|\psi\rangle$ and $|\phi\rangle$ must then be related through (except for normalization)

$$|\phi\rangle\langle\phi| = \sum_{l}(X_l \otimes Y_l \otimes Z_l)|\psi\rangle\langle\psi|(X_l \otimes Y_l \otimes Z_l)^{\dagger}.$$

Moreover, since the state on the left hand side is a pure state, every term on the right hand side must be equal to $|\phi\rangle$ (except for normalization). It is then found that the LOCC conversion of $|\psi\rangle \to |\phi\rangle$ is possible if and only if there exist operators X, Y, Z such that $|\phi\rangle = (X \otimes Y \otimes Z)|\psi\rangle$.

For example, for two bipartite pure states $|\psi\rangle = \sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$ and $|\phi\rangle = \sqrt{\frac{1}{2}}|00\rangle + \sqrt{\frac{1}{2}}|11\rangle$, if we put

$$X = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{pmatrix}, \quad Y = I,$$

we have $|\phi\rangle = \sqrt{3/2}(X \otimes Y)|\psi\rangle$ ($\sqrt{3/2}$ is a normalization factor), and hence $|\psi\rangle \to |\phi\rangle = |\mathrm{EPR}\rangle$ is possible by LOCC. Note that, since the amount of entanglement of $|\psi\rangle$ and $|\phi\rangle$ is $h(1/3) = 0.92$ ebits and 1 ebit, respectively, the amount is increased by LOCC, which seems to contradict that LOCC cannot newly create entanglement. However, this is not the case, because the above conversion only succeeds with the probability of 2/3 (see Exercise 7.3). LOCC cannot increase the *average* amount of entanglement, but can do in a probabilistic way.[4] Indeed, in the above example, the average amount after the LOCC conversion is 2/3 ebits, which is less than 0.92 ebits before the conversion. This type of operations, which succeed only stochastically, are called **stochastic LOCC** (**SLOCC**). On the other hand, since the probability of success of entanglement concentration and dilution asymptotically approaches to 1 for $n \to \infty$, such operations are called **deterministic LOCC**.

Moreover, the above stochastic LOCC is physically realized by making qubit A pass through a filter such that the transmittance of $|0\rangle$ is as two times as that of $|1\rangle$ (the conversion succeeds when the qubit passes through the filter). In this sense, stochastic LOCC is sometimes called **local filtering**.

Exercise 7.3 Show that the maximal probability of success of converting $|\psi\rangle = \sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$ to $|\phi\rangle = \sqrt{\frac{1}{2}}|00\rangle + \sqrt{\frac{1}{2}}|11\rangle$ by A's local filtering is 2/3.

7.4.3 Classification of Multipartite Entanglement

When two pure states $|\psi\rangle$ and $|\phi\rangle$ are interconverted by stochastic LOCC, namely when $|\psi\rangle \leftrightarrow |\phi\rangle$ is possible, $|\psi\rangle$ and $|\phi\rangle$ are called **comparable**. Contrary, neither the conversion of $|\psi\rangle \to |\phi\rangle$ nor $|\psi\rangle \leftarrow |\phi\rangle$ is possible, $|\psi\rangle$ and $|\phi\rangle$ are called **incomparable**. Incomparable states cannot be compared of the amount of entanglement, because they contain completely different types of entanglement.

[4] However, even in a probabilistic way, it is impossible to create any entangled state from unentangled states by LOCC.

Here, let us consider the condition that $|\psi\rangle$ and $|\phi\rangle$ are comparable [15]. The reduced density operators of $|\psi\rangle$ and $|\phi\rangle$ are denoted by like $\sigma_{\mathrm{A}}^{\psi}$ and $\sigma_{\mathrm{A}}^{\phi}$, respectively, and the rank of σ is denoted by $\mathrm{rank}(\sigma)$. If the operator X of satisfying $|\phi\rangle = (X \otimes I \otimes I)|\psi\rangle$ exists, $\mathrm{rank}(\sigma_{\mathrm{A}}^{\phi}) \leq \mathrm{rank}(\sigma_{\mathrm{A}}^{\psi})$ must hold because $\sigma_{\mathrm{A}}^{\phi} = X\sigma_{\mathrm{A}}^{\psi}X^{\dagger}$. Moreover, since $\mathrm{rank}(\sigma_{\mathrm{A}}) = \mathrm{rank}(\sigma_{\mathrm{BC}})$ holds for both pure states $|\psi\rangle$ and $|\phi\rangle$, $\mathrm{rank}(\sigma_{\mathrm{BC}}^{\phi}) \leq \mathrm{rank}(\sigma_{\mathrm{BC}}^{\psi})$ also must hold. Suppose now that the conversion of $|\psi\rangle \longrightarrow |\phi\rangle$ is possible by stochastic LOCC, and hence operators X, Y, Z such that

$$|\phi\rangle = (X \otimes Y \otimes Z)|\psi\rangle = (I \otimes Y \otimes Z)(X \otimes I \otimes I)|\psi\rangle$$

exist. It will be found by repeating the above discussion twice that $\mathrm{rank}(\sigma_{\mathrm{A}}^{\phi}) \leq \mathrm{rank}(\sigma_{\mathrm{A}}^{\psi})$ must hold. This is the case also for parties B and C. Namely, stochastic LOCC, which converts a pure state into another pure state, cannot increase the rank of the reduced density operator of any party. Since both conversions of $|\psi\rangle \rightarrow |\phi\rangle$ and $|\phi\rangle \rightarrow |\psi\rangle$ must be possible so that $|\psi\rangle$ and $|\phi\rangle$ are comparable, the two corresponding reduced density operators must have the same rank for every party.

From the above, pure states on three qubits A, B, and C are classified by the ranks of the reduced density operators as follows [5]:

(1) States with $\mathrm{rank}(\sigma_{\mathrm{A}}) = \mathrm{rank}(\sigma_{\mathrm{B}}) = \mathrm{rank}(\sigma_{\mathrm{C}}) = 1$: Completely unentangled states like $|000\rangle$ (A-B-C class).
(2) States such that $\mathrm{rank}(\sigma_{\mathrm{A}}) = 1$ but $\mathrm{rank}(\sigma_{\mathrm{B}}) = \mathrm{rank}(\sigma_{\mathrm{C}}) = 2$: Two parties among three are entangled like $|0\rangle_{\mathrm{A}}|\mathrm{EPR}\rangle_{\mathrm{BC}}$ (there are three possible classes A-BC, B-AC and C-AB depending on which pairs of parties are entangled).
(3) States with $\mathrm{rank}(\sigma_{\mathrm{A}}) = \mathrm{rank}(\sigma_{\mathrm{B}}) = \mathrm{rank}(\sigma_{\mathrm{C}}) = 2$: Three parties are genuinely entangled. $|\mathrm{GHZ}\rangle$ and $|\mathrm{W}\rangle$ belong to this class.

Exercise 7.4 For a pure state on three qubits, show that there does not exist a class such that $\mathrm{rank}(\sigma_{\mathrm{A}}) = \mathrm{rank}(\sigma_{\mathrm{B}}) = 1$ and $\mathrm{rank}(\sigma_{\mathrm{C}}) = 2$.

Moreover, stochastic LOCC on a pure state has a property such that it cannot increase the minimal number of expansion terms in product states. This is because, when $|\psi\rangle$ is expanded in product states as

$$|\psi\rangle = \sum_{i=1}^{m} \lambda_i |f_i\rangle \otimes |g_i\rangle \otimes |h_i\rangle,$$

where the number of expansion terms is m, the following

$$|\phi\rangle = (X \otimes Y \otimes Z)|\psi\rangle = \sum_{i=1}^{m} \lambda_i X|f_i\rangle \otimes Y|g_i\rangle \otimes Z|h_i\rangle$$

[5] In the case of bipartite pure states, the Schmidt decomposition is applicable and they are classified by the number of terms in the Schmidt decomposition, because it is equal to the rank of the reduced density operators.

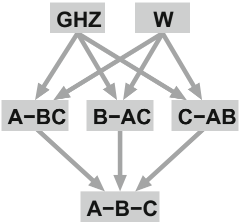


Fig. 7.6 Classification of tripartite pure states

is also an expansion in product states, and hence $|\phi\rangle$ can be necessarily expanded in less than or equal to m product states. The minimal numbers of expansion terms for $|\text{GHZ}\rangle$ and $|\text{W}\rangle$ are different, 2 and 3 respectively [15]. It is immediate from this that the conversion of $|\text{GHZ}\rangle \to |\text{W}\rangle$ is impossible. Moreover, if $|\text{W}\rangle \to |\text{GHZ}\rangle$ would be possible and hence operators X, Y, Z such that $|\text{GHZ}\rangle = (X \otimes Y \otimes Z)|\text{W}\rangle$ would exist, since the ranks of the reduced density operators of $|\text{GHZ}\rangle$ and $|\text{W}\rangle$ on all subsystems are 2 (full rank), operators X, Y, Z must be also full rank and invertible. We would then have $(X^{-1} \otimes Y^{-1} \otimes Z^{-1})|\text{GHZ}\rangle = |\text{W}\rangle$, which contradicts that $|\text{GHZ}\rangle \to |\text{W}\rangle$ is impossible. Therefore, it is concluded that $|\text{W}\rangle \to |\text{GHZ}\rangle$ is also impossible. The class of **(3)** above is then further classified into two subclasses by the minimal number of expansion terms in product states:

(3A) The minimal number of expansion terms is 2 (GHZ class).
(3B) The minimal number of expansion terms is 3 (W class).

The classification is summarized in Fig. 7.6 [15], where the conversion by stochastic LOCC is possible in the direction of arrows. It is then clear from the figure that $|\text{GHZ}\rangle$ and $|\text{W}\rangle$ are incomparable, and they have different types of entanglement. In this way, there can exist many types of entanglement in multipartite settings. Note that, even in the asymptotic settings of $n \to \infty$, the reversible conversion of $|\text{GHZ}\rangle^{\otimes n} \leftrightarrow |\text{W}\rangle^{\otimes nE}$ is also impossible by deterministic LOCC (no matter how real parameter E is chosen) [16], which is quite contrast to the bipartite case of (7.19). Moreover, more detailed classification of entanglement has been made from the view point of LOCC convertibility [17].

7.5 Mixed-State Entanglement

7.5.1 *Entanglement Criteria*

Let us consider a mixed state, where two Bell states $|\phi^+\rangle$ and $|\phi^-\rangle$ in (7.5) are mixed with equal weight in a probabilistic way. Since the density operator of this mixed state σ is rewritten as

$$\sigma = \frac{1}{2}|\phi^+\rangle\langle\phi^+| + \frac{1}{2}|\phi^-\rangle\langle\phi^-| = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|,$$

σ is equivalent to the probabilistic mixture of two unentangled pure states. As a result, the outcome of any measurement on σ can be explained by the ensemble of unentangled states, and hence σ should not be considered entangled. In this way, due to the ambiguity of the ensemble interpretation, the characteristics of entanglement of mixed states are much more complicated than pure states. The definition of entanglement including the case of mixed states is then as follows:

Definition 7.1 A state is entangled if and only if the density operator cannot be represented by a probabilistic mixture of unentangled pure states [18].

By definition, a bipartite unentangled state is written as

$$\sigma = \sum_i p_i |f_i\rangle\langle f_i| \otimes |g_i\rangle\langle g_i|, \tag{7.21}$$

where $p_i \geq 0$. Note that both $|f_i\rangle$ and $|g_i\rangle$ are not necessarily orthogonal sets. Note further that the unentangled states of (7.21) are frequently called separable states from its form.

The above definition of entanglement implies that, to judge whether a given mixed state is entangled or not, we have to investigate all possible decompositions of the density operator into pure states while searching for the form of (7.21). Contrary to the case of a bipartite pure state where its entanglement is easily judged by using the Schmidt decomposition, no universal method to judge mixed-state entanglement has been found yet. However, there have been found non-universal but simple methods as follows: The mathematical operation of transposing the basis of Alice only (or Bob only) is called **partial transposition**, which is denoted by T_A (or T_B). When density operator σ is expanded by using orthonormal sets of Alice and Bob as

$$\sigma = \sum_{ijkl} C_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l|,$$

the partially transposed operator σ^{T_A} is given by

$$\sigma^{T_\mathrm{A}} = \sum_{ijkl} C_{ijkl} |j\rangle\langle i| \otimes |k\rangle\langle l|. \tag{7.22}$$

Note that, contrary to σ, the partially transposed operator is not necessarily positive (Exercise 7.7). However, let us consider the case where σ is unentangled. Since an unentangled state is necessarily written in the form of (7.21), we have

$$\sigma^{T_\mathrm{A}} = \sum_i p_i |\bar{f}_i\rangle\langle \bar{f}_i| \otimes |g_i\rangle\langle g_i|.$$

This operator is still a positive operator ($\sigma^{T_\mathrm{A}} \geq 0$). Conversely, if the partially transposed operator of a given density operator is not a positive operator, the density operator is never written in the form of (7.21). Therefore, we have the following theorem called the **Peres criterion**:

Theorem 7.2 *A state σ, which does not satisfy $\sigma^{T_A} \geq 0$, is entangled [19].*

Exercise 7.5 Show $\mathrm{Tr} X^{T_A} = \mathrm{Tr} X, \mathrm{Tr} X^{T_A} Y^{T_A} = \mathrm{Tr} XY$ for any Hermitian operators X and Y.

Exercise 7.6 Show $\{(Y_1 \otimes Y_2) X (Y_3 \otimes Y_4)\}^{T_A} = (Y_3^T \otimes Y_2) X^{T_A} (Y_1^T \otimes Y_4)$, where Y_1, Y_2, Y_3 and Y_4 are operators on $\mathbb{C}^d$, and X is an operator on $\mathbb{C}^d \otimes \mathbb{C}^d$. Moreover, show that the eigenvalues of σ^{T_A} do not depend on the choice of the basis to which a partial transposition is applied (do not depend on the choice of the basis of $|i\rangle\langle j| \otimes |k\rangle\langle l|$ in (7.22)).

Exercise 7.7 Find the eigenvalues and eigenstates of $(|\psi\rangle\langle\psi|)^{T_A}$ for any bipartite pure state $|\psi\rangle$. Moreover, show that at least one of the eigenvalues of $(|\psi\rangle\langle\psi|)^{T_A}$ is negative when $|\psi\rangle$ is entangled.

Now, denoting the transposed operator of an operator X by X^T, we have $X^T \geq 0$ for any positive operator $X \geq 0$, and hence a partial transposition is a positive map. On the other hand, a partial transposition is nothing but transposing a part of a composite system (T_A is transposing Alice's subsystem of the composite system of Alice and Bob), and it is found from the above Exercise 7.7 that a partial transposition is not a positive map. Namely, a transposition is a positive map but is not a completely positive map. When not only a transposition but general positive map Θ is applied to Alice's part of an unentangled state (7.21), we have

$$\sum_i p_i \Theta(|f_i\rangle\langle f_i|) \otimes |g_i\rangle\langle g_i|, \tag{7.23}$$

which is a positive operator since $\Theta(|f_i\rangle\langle f_i|) \geq 0$. Conversely, if the operator, which is obtained by applying positive map Θ to Alice's part of state σ, is not a positive operator, it is concluded that the state σ is entangled. In this way, a positive map that is not completely positive provides a method to judge entanglement. A map of $X \mapsto (\mathrm{Tr} X)I - X$ is also a positive map that is not completely positive, and the operator obtained by applying this to Alice's part of state σ is given by $I_A \otimes \sigma_B - \sigma$, where $\sigma_B \equiv \mathrm{Tr}_A \sigma$. Therefore, we have the following theorem called a **reduction criterion**:

Theorem 7.3 *A state σ, which does not satisfy $I_A \otimes \sigma_B - \sigma \geq 0$, is entangled [20, 21].*

Note that, when σ is a (bipartite) pure state, the converse of Theorem 7.2 and Theorem 7.3 holds true. Namely, both σ^{T_A} and $I_A \otimes \sigma_B - \sigma$ have at least one negative eigenvalue when the pure state σ is entangled (Exercise 7.7). However, when σ is a mixed state, the converse of Theorem 7.2 and Theorem 7.3 do not hold true in general. Indeed, mixed states that is entangled despite of $\sigma^{T_A} \geq 0$ have been found.

Fortunately, however, in qubit-qubit system ($\mathbb{C}^2 \otimes \mathbb{C}^2$) and in qubit-qutrit system ($\mathbb{C}^2 \otimes \mathbb{C}^3$), Theorem 7.2 and Theorem 7.3 become equivalent,[6] and the converse also hold true.[7] Namely, in those low dimensional systems, the Peres criterion and reduction criterion become necessary and sufficient conditions to judge entanglement [20, 22].

Exercise 7.8 Let $|\Psi\rangle$ be a maximally entangled state of (7.3). Show $\langle\Psi|\sigma|\Psi\rangle \leq \frac{1}{d}$ for any unentangled state σ by using $(|\Psi\rangle\langle\Psi|)^{T_\mathrm{A}}$.

As shown above, since a transposition is not a completely positive map (i.e. it is not a TPCP map), the operation of transposing a density operator cannot be directly realized as a physical operation. The operation of partially transposing a part of a composite system cannot be directly realized also. A partial transposition is absolutely a mathematical operation. Therefore, to experimentally judge entanglement by the use of the Peres criterion, we first need to experimentally determine all elements of the density operator of the state to be judged, next mathematically construct the partially transposed operator from it, and finally evaluate the positivity of the operator numerically. However, a density operator on two d-dimensional systems contains $d^2 - 1$ independent parameters, and hence, for the determination of the density operator, we have to experimentally obtain the expected values of $d^2 - 1$ physical observables, which becomes much more difficult for large d. On the other hand, there is an efficient method to obtain the evidence of entanglement, that is called a **entanglement witness** [22, 23].

For example, let us consider the following operator on two d-dimensional systems:

$$W = \frac{1}{d}I - |\Psi\rangle\langle\Psi|, \tag{7.24}$$

where $|\Psi\rangle$ is a maximally entangled state of (7.3). The operator W is an Hermitian operator, and hence a physical observable. Let us denote the expected value of W with respect to a state σ by $\mathrm{E}_\sigma[W]$. When σ is an unentangled state, we have (see Exercise 7.8)

$$\mathrm{E}_\sigma[W] = \mathrm{Tr}\sigma(\frac{1}{d}I - |\Psi\rangle\langle\Psi|) = \frac{1}{d} - \langle\Psi|\sigma|\Psi\rangle \geq 0.$$

Namely, we have $\mathrm{E}_\sigma[W] < 0$ only when σ is entangled, and hence the fact of $\mathrm{E}_\sigma[W] < 0$ can be used as the evidence (witness) that σ is entangled. An operator of having such a property is called a witness operator. We can obtain the evidence of entanglement by only investigating the expected value of a witness operator without determining all elements of a density operator.

Note, however, that it is troublesome that an appropriate witness operator must be chosen depending on the state to obtain the evidence. For example, considering

[6] They are indeed equivalent in $\mathbb{C}^2 \otimes \mathbb{C}^n$ for $n \geq 2$.

[7] Due to the fact that any positive map $\varGamma$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ is written as $\varGamma = \varTheta_1 + \varTheta_2 \circ T$ with $\varTheta_1$ and $\varTheta_2$ being completely positive maps (T denotes transposition).

the case where $d = 2$ and $|\Psi\rangle$ is chosen to be the Bell state $|\phi^+\rangle$ given in (7.5), the witness operator in (7.24) becomes $W = \frac{1}{2}I - |\phi^+\rangle\langle\phi^+|$. When the state is $\sigma = |\phi^+\rangle\langle\phi^+|$, we have $\mathrm{E}_\sigma[W] = -1/2 < 0$, and hence we can obtain the evidence of the entanglement of σ in terms of the expected value of W. When the state is the Bell state of $\sigma = |\phi^-\rangle\langle\phi^-|$, however, we have $\mathrm{E}_\sigma[W] = 1/2 \geq 0$, and hence we cannot obtain the evidence. To obtain the evidence in this case, we have to use another witness operator such as $W = \frac{1}{2}I - |\phi^-\rangle\langle\phi^-|$.

Exercise 7.9 Let σ be an entangled state which does not satisfy $\sigma^{T_\mathrm{A}} \geq 0$ (see Theorem 7.2), $\mu < 0$ be a negative eigenvalue of σ^{T_A}, and $|\mu\rangle$ be the corresponding eigenstate. Show that $W = (|\mu\rangle\langle\mu|)^{T_\mathrm{A}}$ is an entanglement witness that can provide the evidence of the entanglement in σ. Moreover, show that $|\mu\rangle$ is entangled.

7.5.2 LOCC on Mixed States

Let us consider the LOCC conversion from a mixed state σ to $|\mathrm{EPR}\rangle$ [3] as in the case of entanglement concentration for pure states. This LOCC conversion is called **entanglement distillation**, because the situation is as if distilling pure $|\mathrm{EPR}\rangle$ from an impure mixed state. When at most $|\mathrm{EPR}\rangle^{\otimes nE_D}$ is distilled from $\sigma^{\otimes n}$, namely when the conversion of

$$\sigma^{\otimes n} \longrightarrow |\mathrm{EPR}\rangle^{\otimes nE_D} \tag{7.25}$$

is possible by LOCC for large n limit, E_D is called **distillable entanglement**. Note that this LOCC conversion is asymptotically defined in the limit of $n \to \infty$. For example, unless n is finite, the entangled mixed state $\sigma^{\otimes n}$ on two d-dimensional systems (on $\mathbb{C}^d \otimes \mathbb{C}^d$) cannot be converted exactly to $|\mathrm{EPR}\rangle^{\otimes 1}$ by LOCC, if $\mathrm{rank}(\sigma) \geq d^2 - 2$ [24, 25]. Even in such cases, however, it is frequently possible to distill a state ρ_n that asymptotically approaches $|\mathrm{EPR}\rangle^{\otimes m}$ such that

$$\sigma^{\otimes n} \longrightarrow \rho_n \quad \text{and} \quad \lim_{n\to\infty} \langle \mathrm{EPR}^{\otimes m}|\rho_n|\mathrm{EPR}^{\otimes m}\rangle = 1 \tag{7.26}$$

in the limit of $n \to \infty$. This type of conversion in $n \to \infty$ is called **asymptotic conversion** (entanglement concentration and dilution for pure states are also asymptotic conversions). To be precise, E_D is also defined as a maximal possible rate of m/n in the asymptotic conversion of (7.26).

Now, since $|\mathrm{EPR}\rangle^{\otimes m}$ in (7.26) is a maximally entangled state on $\mathbb{C}^{2^m} \otimes \mathbb{C}^{2^m}$, it is invariant under local unitary transformation $(U_\mathrm{A} \otimes \bar{U}_\mathrm{B})$ due to the property of (7.4). So, suppose that Alice and Bob randomly pick up U on $\mathbb{C}^{2^m}$ and apply $(U_\mathrm{A} \otimes \bar{U}_\mathrm{B})$ to ρ_n, but after the application, they forget which U is applied. These operations, called **twirling**, convert ρ_n to

$$\rho_n' = \frac{1}{\Omega} \int dU (U_\mathrm{A} \otimes \bar{U}_\mathrm{B}) \rho_n (U_\mathrm{A} \otimes \bar{U}_\mathrm{B})^\dagger, \tag{7.27}$$

where $\frac{1}{\Omega}\int dU \cdots$ denotes the average over all unitary operators on $\mathbb{C}^{2^m}$. In this conversion, since

$$\begin{aligned} F_n &\equiv \langle \mathrm{EPR}^{\otimes m}|\rho_n'|\mathrm{EPR}^{\otimes m}\rangle \\ &= \frac{1}{\Omega}\int dU \langle \mathrm{EPR}^{\otimes m}|(U_\mathrm{A}\otimes \bar{U}_\mathrm{B})\rho_n(U_\mathrm{A}\otimes \bar{U}_\mathrm{B})^\dagger|\mathrm{EPR}^{\otimes m}\rangle \\ &= \langle \mathrm{EPR}^{\otimes m}|\rho_n|\mathrm{EPR}^{\otimes m}\rangle, \end{aligned} \tag{7.28}$$

the fidelity with $|\mathrm{EPR}\rangle^{\otimes m}$ remains invariant. Moreover, by virtue of (7.27), ρ_n' is invariant under unitary transformation of $(U_\mathrm{A}\otimes \bar{U}_\mathrm{B})$ for any U. The states on $\mathbb{C}^{2^m}\otimes\mathbb{C}^{2^m}$ with this invariance are always written as a probabilistic mixture of $|\mathrm{EPR}\rangle^{\otimes m}$ and $(I\otimes I)/2^{2m}$ (Exercise 7.10), which is called an **isotropic state**. As a result, ρ_n' is expressed using F_n in (7.28) as

$$\rho_n' = F_n(|\mathrm{EPR}\rangle\langle\mathrm{EPR}|)^{\otimes m} + (1-F_n)\frac{(I\otimes I) - (|\mathrm{EPR}\rangle\langle\mathrm{EPR}|)^{\otimes m}}{2^{2m}-1}. \tag{7.29}$$

From the above, without loss of generality, the process of entanglement distillation can be considered as the asymptotic conversion whose final state is always an isotropic state ρ_n' such that

$$\sigma^{\otimes n} \longrightarrow \rho_n' \quad \text{and} \quad \lim_{n\to\infty} F_n = \lim_{n\to\infty}\langle \mathrm{EPR}^{\otimes m}|\rho_n'|\mathrm{EPR}^{\otimes m}\rangle = 1. \tag{7.30}$$

Exercise 7.10 Find an Hermitian operator A on $\mathbb{C}^d\otimes\mathbb{C}^d$ that is invariant under unitary transformation $(U_\mathrm{A}\otimes\bar{U}_\mathrm{B})$ for any U by the following steps [20]: (1) Represent A as $A = \sum_{mnop} a_{mnop}|mn\rangle\langle op|$ by using local bases, and consider the invariance condition for U such that $U|m_0\rangle = -|m_0\rangle$ only for a particular local basis $|m_0\rangle$. (2) Consider for U such that $U|m_0\rangle = i|m_0\rangle$. (3) Consider for U such that it exchanges two local bases of $|m_0\rangle$ and $|m_1\rangle$ $(m_0 \neq m_1)$. (4) Consider for U such that $U|m_0\rangle = (|m_0\rangle + |m_1\rangle)/\sqrt{2}$, and $U|m_0\rangle = (|m_0\rangle - |m_1\rangle)/\sqrt{2}$.

Contrary to entanglement distillation, when at least $|\mathrm{EPR}\rangle^{\otimes nE_\mathrm{C}}$ is necessary to produce $\sigma^{\otimes n}$, namely when the conversion of

$$|\mathrm{EPR}\rangle^{\otimes nE_\mathrm{C}} \longrightarrow \sigma^{\otimes n} \tag{7.31}$$

is possible by LOCC, E_C is called **entanglement cost** (which is defined through an asymptotic conversion as well as entanglement distillation). It has been shown that $E_\mathrm{C} > 0$ for any entangled state [26]. As shown in Sect. 7.3.6, when σ is a pure state, the reversible conversion is possible and hence $E_D = E_\mathrm{C} = H(\sigma_\mathrm{A})$. When σ is a mixed state, however, the conversion becomes irreversible in general and $E_D < E_\mathrm{C}$. Namely, in the conversion cycle of

$$|\mathrm{EPR}\rangle^{\otimes nE_\mathrm{C}} \longrightarrow \sigma^{\otimes n} \longrightarrow |\mathrm{EPR}\rangle^{\otimes nE_D},$$

$\mathit{\Delta} E \equiv E_\mathrm{C} - E_D$ ebits of entanglement is lost per one pair of σ. Once pure-state entanglement is converted into mixed-state entanglement, a part of it cannot be extracted as pure-state entanglement anymore. By analogy with bound energy in thermodynamics, $\mathit{\Delta} E$ is called **bound entanglement** [27].

As mentioned in Sect. 7.5.1, the converse of Theorem 7.2 does not hold true in general, and there exists an entangled mixed state σ despite $\sigma^{T_\mathrm{A}} \geq 0$. Let us consider LOCC on such states. Applying partial transposition on both sides of the Kraus representation (7.9), we have (Exercise 7.6)

$$(\sigma')^{T_\mathrm{A}} = \sum_l (\bar{M}_l \otimes N_l)\sigma^{T_\mathrm{A}}(\bar{M}_l \otimes N_l)^\dagger,$$

and hence $(\sigma')^{T_\mathrm{A}} \geq 0$ for $\sigma^{T_\mathrm{A}} \geq 0$. On the other hand, $(|\mathrm{EPR}\rangle\langle\mathrm{EPR}|)^{T_\mathrm{A}}$ is not a positive operator. Therefore, entangled σ of satisfying $\sigma^{T_\mathrm{A}} \geq 0$ cannot be converted, in any way, to $|\mathrm{EPR}\rangle$, and we have

Theorem 7.4 *Entanglement distillation is impossible ($E_D = 0$) for a state σ which satisfies $\sigma^{T_\mathrm{A}} \geq 0$ [27].*

Namely, entangled mixed state σ with $\sigma^{T_\mathrm{A}} \geq 0$ has no distillable entanglement ($E_D = 0$) though it is entangled, which implies that all entanglement in the state is bound (the state only contains bound entanglement). This state is called a **bound entangled state** [27]. In this way, strange phenomena appear by considering LOCC on entangled mixed states [27–29].

On the other hand, according to Theorem 7.3, the state σ which does not satisfy $I_\mathrm{A} \otimes \sigma_\mathrm{B} - \sigma \geq 0$ is entangled, but those entangled states can be converted to $|\mathrm{EPR}\rangle$ by applying a LOCC protocol (so-called BBPSSW protocol [30]) and local filtering, and hence the following holds:

Theorem 7.5 *Entanglement distillation is possible ($E_D > 0$) for state σ which does not satisfy $I_\mathrm{A} \otimes \sigma_\mathrm{B} - \sigma \geq 0$ [27].*

7.5.3 Entanglement Measure

As shown in Sect. 7.3.6, the amount of entanglement of a bipartite pure state σ is determined to be $H(\sigma_\mathrm{A})$ by considering entanglement concentration and dilution by LOCC. In the same manner, both E_D and E_C represent the amount of entanglement in a mixed state, but the amount in a mixed state is not unique, and as shown later, there exist other quantities than E_D and E_C. In general, a function $E(\sigma)$ that satisfies the following properties becomes a measure to quantify the amount of entanglement, called an **entanglement measure** [31–33]:

(1) Monotonicity: The average value of the function $E(\sigma)$ does not increase under LOCC. Namely, when σ_i is obtained with probability p_i by LOCC from σ (this is denoted by $\sigma \to \{p_i, \sigma_i\}$ hereafter), $E(\sigma) \geq \sum_i p_i E(\sigma_i)$.

(2) Concavity: The value of the function $E(\sigma)$ is not increased by mixing of states. Namely, $\sum_i p_i E(\sigma_i) \geq E\big(\sum_i p_i \sigma_i\big)$.

(3) When σ is unentangled, $E(\sigma) = 0$.

(4) When σ is a pure state, $E(\sigma) = H(\sigma_{\mathrm{A}}) = H(\sigma_{\mathrm{B}})$.

However, it is unclear whether E_D satisfies the concavity of (2), and the concavity is sometimes excluded from the properties that should be satisfied by entanglement measures (E_{C} satisfies all the properties of (1)–(4)). Moreover, there are some important properties related to asymptotic conversions as follows, though those are not necessarily satisfied by all entanglement measures:

(5) Weak additivity: $E(\sigma^{\otimes n}) = nE(\sigma)$ for any state σ.

(6) Asymptotic continuity for pure states: When ρ_n asymptotically approaches to $|\psi\rangle^{\otimes n}$ such that $\langle\psi^{\otimes n}|\rho_n|\psi^{\otimes n}\rangle \to 1$ for $n \to \infty$, $\frac{1}{n}|E(|\psi\rangle^{\otimes n}) - E(\rho_n)| \to 0$.

For a given entanglement measure $E(\sigma)$, the function produced from it by

$$E^{\infty}(\sigma) = \lim_{n\to\infty} \frac{E(\sigma^{\otimes n})}{n}$$

is called an **asymptotic entanglement measure**. An asymptotic entanglement measure automatically satisfies the weak additivity of the above (5) by definition.[8]

7.5.4 *Entanglement of Formation*

The function $E_F(\sigma)$ defined in the following way is an entanglement measure called **entanglement of formation** (**EoF**) [3]:

$$E_F(\sigma) = \min \sum_k \lambda_k H_{\mathrm{A}}(|\psi_k\rangle), \tag{7.32}$$

where $H_{\mathrm{A}}(|\psi\rangle) = H(\mathrm{Tr}_{\mathrm{A}}|\psi\rangle\langle\psi|)$, and minimization is performed over all possible decompositions of σ into pure states as $\sigma = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$.

Here, to understand the operational meaning of E_F, let us consider the following LOCC process: First, Alice (or Bob) produces a random value k with the probability of λ_k. Next, depending on the random value k, Alice and Bob produce $|\psi_k\rangle$ from

[8] Note that, even though E satisfies (1) and (2), E^{∞} does not necessarily satisfy them. If E also satisfies subadditivity, however, E^{∞} automatically satisfies the weak monotonicity (1′) and (2) [34].

$|\mathrm{EPR}\rangle$ by entanglement dilution shown in Sect. 7.3.5. Finally, Alice and Bob forget the information of the random value k. The sate they share then becomes the mixed state of $\sigma = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$. Since the number of $|\mathrm{EPR}\rangle$ necessary to produce $|\psi_k\rangle$ by entanglement dilution is $H_{\mathrm{A}}(|\psi_k\rangle)$, the average number of $|\mathrm{EPR}\rangle$ consumed in the above LOCC process is $\sum_k \lambda_k H_{\mathrm{A}}(|\psi_k\rangle)$. The average number depends on how to decompose σ into pure states, and the minimal value is just $E_F(\sigma)$. Namely, $E_F(\sigma)$ is the minimal number of $|\mathrm{EPR}\rangle$ necessary to produce σ by the above LOCC process.

It has been proved that entanglement cost E_{C} is the asymptotic entanglement measure of entanglement of formation E_F, namely

$$E_{\mathrm{C}}(\sigma) = \lim_{n\to\infty} \frac{E_F(\sigma^{\otimes n})}{n} \tag{7.33}$$

holds for any bipartite mixed state σ [35]. Note that the existence of the limit $\lim_{n\to\infty} \frac{E_F(\sigma^{\otimes n})}{n}$ is guaranteed by Lemma A.7 and the weak subadditivity $E_F(\sigma^{\otimes(m+n)}) \le E_F(\sigma^{\otimes m}) + E_F(\sigma^{\otimes n})$. Then, we have another expression $\lim_{n\to\infty} \frac{E_F(\sigma^{\otimes n})}{n} = \inf_{n\ge 1} \frac{E_F(\sigma^{\otimes n})}{n}$. Since E_F does not satisfy the weak additivity of the property of (5) in Sect. 7.5.3 [36], $E_F(\sigma)$ and $E_{\mathrm{C}}(\sigma)$ do not coincide with each other, and hence

$$E_{\mathrm{C}}(\sigma) \le E_F(\sigma)$$

holds in general.

It is confirmed that E_F satisfies the properties of (1)–(4) in Sect. 7.5.3 as follows: The concavity of (2) and the property of (3) are obviously satisfied by definition. Moreover, when σ is a pure state, the satisfaction of $E_F(\sigma) = H(\sigma_{\mathrm{A}})$ of the property (4) is also obvious. Concerning the monotonicity of (1), let $\sigma = \sum_k \hat{\lambda}_k |\hat{\psi}_k\rangle\langle\hat{\psi}_k|$ be an optimal decomposition that achieves the minimization, and hence $E_F(\sigma) = \sum_k \hat{\lambda}_k H_{\mathrm{A}}(|\hat{\psi}_k\rangle)$. Suppose now that Bob performs a local operation, which results in the conversion of $|\hat{\psi}_k\rangle \to \{p_{i|k}, \sigma_i^{(k)}\}$, and hence $\sigma \to \{p_i, \sigma_i = \frac{1}{p_i}\sum_k p_{i|k}\hat{\lambda}_k\sigma_i^{(k)}\}$ where $p_i = \sum_k p_{i|k}\hat{\lambda}_k$. Then, we have

$$\begin{aligned}
\sum_i p_i E_F(\sigma_i) &= \sum_i p_i E_F(\frac{1}{p_i}\sum_k p_{i|k}\hat{\lambda}_k\sigma_i^{(k)}) \overset{\text{(a)}}{\le} \sum_{ik} p_{i|k}\hat{\lambda}_k E_F(\sigma_i^{(k)}) \\
&\overset{\text{(b)}}{\le} \sum_{ik} p_{i|k}\hat{\lambda}_k H_{\mathrm{A}}(\sigma_i^{(k)}) \overset{\text{(c)}}{\le} \sum_k \hat{\lambda}_k H_{\mathrm{A}}(\sum_i p_{i|k}\sigma_i^{(k)}) \\
&\overset{\text{(d)}}{=} \sum_k \hat{\lambda}_k H_{\mathrm{A}}(|\hat{\psi}_k\rangle) = E_F(\sigma).
\end{aligned}$$

Here, we used the concavity of E_F for the inequality (a), the definition of E_F for (b), and the convexity of H_A for (c). Moreover, since the reduced density operator of Alice remains unchanged by Bob's local operation considered here, we have $\mathrm{Tr}_\mathrm{B} \sum_i p_{i|k} \sigma_i^{(k)} = \mathrm{Tr}_\mathrm{B} |\hat{\psi}_k\rangle\langle\hat{\psi}_k|$, and hence the equality (d) holds. Since $H_\mathrm{A}(|\psi\rangle) = H_\mathrm{B}(|\psi\rangle)$ for a pure state, H_A in (7.32) can be replaced by H_B. Therefore, we have the same inequality also for Alice's local operation, and after all the monotonicity under LOCC is satisfied.

In general, the calculation of entanglement of formation is a very hard task, because we must perform the minimization over all possible decompositions into pure states. For any state σ on $\mathbb{C}^2 \otimes \mathbb{C}^2$, however, the following formula for calculating $E_F(\sigma)$ has been obtained [37]: Let $\tilde{\sigma} = (\sigma_y \otimes \sigma_y)\bar{\sigma}(\sigma_y \otimes \sigma_y)$ where $\bar{\sigma}$ is the complex conjugate of σ, and let l_0, l_1, l_2, and l_3 be four eigenvalues of $\sqrt{\sqrt{\sigma}\tilde{\sigma}\sqrt{\sigma}}$ in decreasing order. According to the formula, the entanglement formation of σ is then calculated through $E_F(\sigma) = h(\frac{1}{2} + \frac{1}{2}\sqrt{1 - C^2})$, where $C = \max\{l_0 - l_1 - l_2 - l_3, 0\}$ is called **concurrence**.

Exercise 7.11 Let $|\psi\rangle$ be an entangled state on $\mathbb{C}^2 \otimes \mathbb{C}^2$, and $|\tilde{\psi}\rangle \equiv (\sigma_y \otimes \sigma_y)|\bar{\psi}\rangle$. Show that $|\langle\psi|\tilde{\psi}\rangle| = 1$ when $|\psi\rangle$ is a maximally entangled state. Moreover, show that $|\langle\psi|\tilde{\psi}\rangle| = 0$ when $|\psi\rangle$ is unentangled.

Exercise 7.12 Find the concurrence for a pure state $|\psi\rangle = \sqrt{p}|00\rangle + \sqrt{1-p}|11\rangle$, and for an isotropic state $\sigma = F|\mathrm{EPR}\rangle\langle\mathrm{EPR}| + (1-F)(I \otimes I - |\mathrm{EPR}\rangle\langle\mathrm{EPR}|)/3$.

7.5.5 Relative Entropy of Entanglement

The function $E_R(\sigma)$ defined in the following way is an entanglement measure called **relative entropy of entanglement** [31, 38]:

$$E_R(\sigma) = \min_\rho D(\sigma||\rho) = \min_\rho \left[\mathrm{Tr}\sigma \log \sigma - \mathrm{Tr}\sigma \log \rho\right], \tag{7.34}$$

where the minimization is performed over all unentangled states ρ. Since the relative entropy $D(\sigma||\rho)$ is roughly considered as a distance between states σ and ρ (to be exact, it is not a distance as shown in Sect. 6.3.2), $E_R(\sigma)$ is roughly a minimal distance from σ to the set of unentangled states. The proof is not explicitly shown here, but $E_R(\sigma)$ also satisfies the properties of (1)–(4) in Sect. 7.5.3. The monotonicity under trace-preserving LOCC (TP-LOCC) is relatively easily confirmed as follows: Denoting the map of TP-LOCC by Λ, and denoting ρ that achieves the minimization of $D(\sigma||\rho)$ by $\hat{\rho}$, we have

$$E_R(\Lambda(\sigma)) = \min_\rho D(\Lambda(\sigma)||\rho) \le D(\Lambda(\sigma)||\Lambda(\hat{\rho})) \le D(\sigma||\hat{\rho}) = E_R(\sigma),$$

by noting that $\Lambda(\hat{\rho})$ is unentangled because Λ is LOCC, and noting the monotonicity of relative entropy for a TPCP map (Theorem 6.7).

For any bipartite mixed state σ, the following inequality holds between $E_R(\sigma)$ and $E_F(\sigma)$:

$$E_R(\sigma) \leq \sum_k \hat{\lambda}_k E_R(|\hat{\psi}_k\rangle) = \sum_k \hat{\lambda}_k E_F(|\hat{\psi}_k\rangle) = E_F(\sigma),$$

where $\sigma = \sum_k \hat{\lambda}_k |\hat{\psi}\rangle\langle\hat{\psi}_k|$ is the decomposition of σ that achieves the minimization of $E_F(\sigma)$, and the concavity of E_R was used in the first inequality. Moreover, using quantum Stein's lemma (Theorem 8.1), the inequality of

$$E_D(\sigma) \leq E_R(\sigma)$$

has been proved [39, 40]. Namely, $E_R(\sigma)$ has an important role as an upper bound of $E_D(\sigma)$.

Contrary to E_F, no closed formula for the easy calculation of $E_R(\sigma)$ has been obtained even in the simplest case of $\mathbb{C}^2 \otimes \mathbb{C}^2$, but it is possible to derive σ such that $E_R(\sigma) = D(\sigma||\hat{\rho})$ for any given $\hat{\rho}$ [41].

Moreover, the definition of E_R can be easily extend to the case of multipartite settings. The multipartite E_R reflects the variety of properties of multipartite entanglement, and indeed it has been shown that it does not satisfy the weak additivity even for a pure state, and so on [16, 42].

7.5.6 Relationship among Entanglement Measures

As shown in Sect. 7.3.6, the reversible LOCC conversion of

$$|\psi\rangle^{\otimes n} \longleftrightarrow |\mathrm{EPR}\rangle^{\otimes nH(\sigma_\mathrm{A})}, \tag{7.35}$$

plays a crucial role in quantifying the amount of entanglement for a bipartite pure state $|\psi\rangle$. Let us take a look at this role from the viewpoint of entanglement measures.

Suppose that an entanglement measure E satisfies the monotonicity (1) and asymptotic continuity for pure states (6) in Sect. 7.5.3. Considering then the asymptotic conversion in the direction of $\longrightarrow$ in (7.35), we have

$$E(|\psi\rangle^{\otimes n}) \geq E(|\mathrm{EPR}\rangle^{\otimes nH(\sigma_\mathrm{A})}).$$

However, considering the asymptotic conversion in the direction of $\longleftarrow$, we also have

$$E(|\psi\rangle^{\otimes n}) \leq E(|\mathrm{EPR}\rangle^{\otimes nH(\sigma_\mathrm{A})}),$$

and after all we have $E(|\psi\rangle^{\otimes n}) = E(|\mathrm{EPR}\rangle^{\otimes nH(\sigma_{\mathrm{A}})})$. If E further satisfies the weak additivity of (5), we have $E(|\psi\rangle) = H(\sigma_{\mathrm{A}})E(|\mathrm{EPR}\rangle)$. Since $E(|\mathrm{EPR}\rangle)$ is a constant, if the entanglement measure E is normalized such as

(4′) Normalization: $E(|\mathrm{EPR}\rangle) = 1$,

we finally arrive at $E(|\psi\rangle) = H(\sigma_{\mathrm{A}})$. Namely, when an entanglement measure satisfies the monotonicity (1), normalization (4′), weak additivity (5), and asymptotic continuity for pure states (6), the measure necessarily coincides with $H(\sigma_{\mathrm{A}})$ for bipartite pure states. This fact is called the **uniqueness theorem** for entanglement measures [34].

In the case of mixed states σ, if E satisfies the concavity (2) in addition to the monotonicity (1), normalization (4′), weak additivity (5), and asymptotic continuity for pure states (6), the following inequality then holds:

$$\begin{aligned} E(\sigma) &\overset{(5)}{=} \frac{E(\sigma^{\otimes n})}{n} \overset{(2)}{\leq} \frac{\sum_k \hat{\lambda}_k E(|\hat{\psi}_k\rangle)}{n} \overset{(1),(4'),(5),(6)}{=} \frac{\sum_k \hat{\lambda}_k E_F(|\hat{\psi}_k\rangle)}{n} \\ &= \frac{E_F(\sigma^{\otimes n})}{n} = E_{\mathrm{C}}(\sigma), \end{aligned}$$

where $E(|\hat{\psi}_k\rangle) = E_F(|\hat{\psi}_k\rangle)$ due to the uniqueness theorem, $\sigma^{\otimes n} = \sum_k \hat{\lambda}_k |\hat{\psi}_k\rangle\langle\hat{\psi}_k|$ is an optimal decomposition for entanglement of formation, and (7.33) was used.

Moreover, considering the asymptotic conversion of (7.25), we have

$$E(\sigma) \overset{(5)}{=} \frac{E(\sigma^{\otimes n})}{n} \overset{(1),(6)}{\geq} \frac{E(|\mathrm{EPR}\rangle^{\otimes nE_D(\sigma)})}{n} \overset{(4'),(5)}{=} E_D(\sigma). \tag{7.36}$$

It is concluded from the above that, when an entanglement measures E satisfies the monotonicity (1), concavity (2), normalization (4′), weak additivity (5), and asymptotic continuity for pure states (6), the measure necessarily bounded as [43]

$$E_D(\sigma) \leq E(\sigma) \leq E_{\mathrm{C}}(\sigma).$$

Note that it is possible to loosen the satisfaction conditions for the inequality for E_D (7.36). Since the LOCC process of entanglement distillation is trace-preserving, the monotonicity (1) can be replaced with the weaker condition of

(1′) Weak monotonicity: $E(\sigma) \geq E(\Lambda(\sigma))$ for trace-preserving LOCC Λ.

Moreover, since the final state of entanglement distillation can be considered to be an isotropic state as (7.30) without loss of generality, the asymptotic continuity for pure states (6) can be replaced with

(6′) Continuity for isotropic states: $\lim_{F_n \to 1} E(\rho'_n) = m$ with ρ'_n being the isotropic state of (7.29).

Namely, when a function E satisfies the weak monotonicity (1′), normalization (4′), weak additivity (5), and continuity for isotropic states (6′), the function E provides an upper bound for distillable entanglement E_D [43].

7.5.7 Entanglement Monotone

The calculation of the entanglement measures shown so far, such as E_D, E_C, E_F, and E_R, is a very hard task for general mixed states. It is then convenient to introduce a function that only satisfies the most important property of the monotonicity (1), among the properties (1)–(4) in Sect. 7.5.3. This function, called an **entanglement monotone** [44], can also be used as a simpler measure to quantify the amount of entanglement. For example, the concurrence appeared in the formula for calculating E_F is an entanglement monotone, because it satisfies the properties (1), (2), and (3), while it does not satisfy the property of (4). Moreover, the following function

$$LN(\sigma) = \log \mathrm{Tr}|\sigma^{T_\mathrm{A}}|,$$

is also an entanglement monotone, called **logarithmic negativity** [45]. It is found that $LN(\sigma) = 0$ for an unentangled state, because an unentangled σ satisfies $\sigma^{T_\mathrm{A}} \geq 0$ according to the Peres criterion (Theorem 7.2), and hence $\mathrm{Tr}|\sigma^{T_\mathrm{A}}| = \mathrm{Tr}\sigma^{T_\mathrm{A}} = \mathrm{Tr}\sigma = 1$. The logarithmic negativity provides an upper bound of E_D as

$$E_D(\sigma) \leq LN(\sigma),$$

because it satisfies the weak monotonicity (1′), normalization (2′), weak additivity (5), and continuity for isotropic states (6′).

Exercise 7.13 Express the logarithmic negativity for a bipartite pure state $|\psi\rangle$ by using the Schmidt coefficients of $|\psi\rangle$. Using this result, find the logarithmic negativity for a maximally entangled state $|\Psi\rangle$ on two d-dimensional systems.

References

1. A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777–780 (1935)
2. A. Aspect, J. Dalibard, G. Roger, Phys. Rev. Lett. **49**, 1804–1807 (1982)
3. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Phys. Rev. A **54**, 3824–3851 (1996)
4. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Phys. Rev. Lett. **70**, 1895–1899 (1993)
5. H.-J. Briegel, W. Dür, J.I. Cirac, P. Zoller, Phys. Rev. Lett. **81**, 5932–5935 (1998)
6. S.L. Braunstein, H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998)
7. P. van Loock, S.L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000)
8. S. Ishizaka, T. Hiroshima, Phys. Rev. Lett. **101**, 240501 (2008)
9. C.H. Bennett, S.J. Wiesner, H.J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. Lett. **69**, 2881–2884 (1992)
10. C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, W.K. Wootters, Phys. Rev. A **59**, 1070–1091 (1999)
11. C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. A **53**, 2046–2052 (1996)
12. B. Schumacher, Phys. Rev. A **51**, 2738–2747 (1995)
13. H.K. Lo, S. Popescu, Phys. Rev. A **63**, 022301 (2001)

14. W. Kumagai, M. Hayashi, Phys. Rev. Lett. **111**, 130407 (2013)
15. W. Dür, G. Vidal, J.I. Cirac, Phys. Rev. A **62**, 062314 (2000)
16. S. Ishizaka, M.B. Plenio, Phys. Rev. A **72**, 042325 (2005)
17. L. Chen, M. Hayashi, Phys. Rev. A **83**, 022331 (2011). and references therein
18. R. Werner, Phys. Rev. A **40**, 4277–4281 (1989)
19. A. Peres, Phys. Rev. Lett. **77**, 1413–1415 (1996)
20. M. Horodecki, P. Horodecki, Phys. Rev. A **59**, 4206–4216 (1999)
21. N.J. Cerf, C. Adami, R.M. Gingrich, Phys. Rev. A **60**, 898–909 (1999)
22. M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A **223**, 1–8 (1996)
23. B.M. Terhal, Phys. Lett. A **271**, 319–326 (2000)
24. A. Kent, Phys. Rev. Lett. **81**, 2839–2841 (1998)
25. S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004)
26. D. Yang, M. Horodecki, R. Horodecki, B. Synak-Radtke, Phys. Rev. Lett. **95**, 190501 (2005)
27. M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **80**, 5239–5242 (1998)
28. R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009)
29. S. Ishizaka, M.B. Plenio, Phys. Rev. A **71**, 052303 (2005). and references therein
30. C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, A. Smolin, W.K. Wootters, Phys. Rev. Lett. **76**, 722–725 (1996)
31. V. Vedral, M.B. Plenio, Phys. Rev. A **57**, 1619–1633 (1998)
32. M. Horodecki, Quantum Inf. Comput. **1**, 3 (2001)
33. M.B. Plenio, S. Virmani, Quantum Inf. Comput. **7**, 1 (2007)
34. M.J. Donald, M. Horodecki, O. Rudolph, J. Math. Phys. **43**, 4252 (2002)
35. P.M. Hayden, M. Horodecki, B.M. Terhal, J. Phys. A: Math. Gen. **34**, 6891 (2001)
36. M.B. Hastings, Nat. Phys. **5**, 255–257 (2009)
37. W.K. Wootters, Phys. Rev. Lett. **80**, 2245–2248 (1998)
38. V. Vedral, M.B. Plenio, M.A. Rippin, P.L. Knight, Phys. Rev. Lett. **78**, 2275–2279 (1997)
39. E.M. Rains, Phys. Rev. A **60**, 179–184 (1999)
40. M. Hayashi, *Quantum Information: An Introduction* (Springer, Berlin, 2006) (Originally published in Japanese in 2004)
41. A. Miranowicz, S. Ishizaka, Phys. Rev. A **78**, 032310 (2008)
42. H. Zhu, L. Chen, M. Hayashi, New J. Phys. **12**, 083002 (2010)
43. M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **84**, 2014–2017 (2000)
44. G. Vidal, J. Mod. Opt. **47**, 355–376 (2000)
45. G. Vidal, R.F. Werner, Phys. Rev. A **65**, 032314 (2002)

Chapter 8
Classical-Quantum Channel Coding

8.1 Introduction

The transmission of messages over classical channels from a sender to a receiver is called **classical communication**. On the other hand, quantum communication has two different formulations according to what is transmitted over quantum channels. One is **classical-quantum channel coding** (cq channel coding), that is, message transmission using carriers governed by quantum mechanics, and the other is **quantum-quantum channel coding** (qq channel coding), which is faithful transmission of quantum states over noisy quantum channels.

Historically speaking, the theory of classical-quantum channel coding [1, 2] was developed partially in the studies from 1960s to 1970s, motivated by the invention of lasers in 1960. Later the classical-quantum channel coding theorem was established in the middle of 1990s by Holevo [3] and Schumacher-Westmoreland [4]. On the other hand, quantum-quantum channel coding derives from the studies of quantum error correcting codes [5, 6] in 1990s. Quantum error correction is a method to protect quantum states used in the memory of quantum computers, which are apt to be disturbed by quantum mechanical noises.

In this chapter, we study classical-quantum channel coding, while quantum-quantum channel coding will be studied in Chap. 9. In classical-quantum channel coding, the optimization of measurements is required at the receiver's side, which is the crucial difference from classical channel coding, since the receiver should perform quantum measurements on the transmitted carrier to recover the message from the sender. As is different from classical systems, the states of carriers change inevitably by measurements. Thus it is important to obtain the measurement outcome at once as effectively as possible. The essential difficulty in the detecting process is to discriminate the states received in the receiver's side. This type of discrimination problem can be essentially converted to the quantum hypothesis problem between two states in an enlarged system. From this reason, the theory of quantum hypothesis

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_8,

testing plays an important role in classical-quantum channel coding. In the following, the theory of quantum hypothesis testing is described first, and then, the classical-quantum channel coding theorem is studied.

8.2 Quantum Hypothesis Testing

8.2.1 Problem of Quantum Hypothesis Testing

Quantum hypothesis testing is a method to determine the true state based on data given by a quantum measurement when two hypotheses of quantum states are given on a Hilbert space. It is sometimes called simple quantum hypothesis testing to make difference from composite hypothesis testing where the hypothesis to be tested is composed of more than two density operators. In quantum hypothesis testing, the difficulty derived from non-commutativity in quantum information theory appears in the most simple manner, and the asymptotic theory of quantum hypothesis testing provides fundamental tools for various problems in quantum information theory.

We assume from prior knowledge that either $\rho \in \mathcal{S}(\mathcal{H})$ or $\sigma \in \mathcal{S}(\mathcal{H})$ is the true state, where $\mathcal{S}(\mathcal{H})$ is the set of density operators on a Hilbert space $\mathcal{H}$. To determine which is true, we need to obtain data from a quantum measurement on $\mathcal{H}$. Since the decision is alternative, "ρ is true" or "σ is true", the whole process can be considered as a two-valued quantum measurement (i.e., a two-valued POVM) with the form $\{T, I-T\}$ without loss of generality, where T is an operator on $\mathcal{H}$ satisfying $0 \leq T \leq I$. Since we can identify T with the two-valued POVM $\{T, I-T\}$, an operator T satisfying $0 \leq T \leq I$ is called a **test**. For a test T, there are two kinds of error probabilities; the error of accepting σ when ρ is true and the error of the converse situation, which are, respectively, written as

$$\alpha(T) := \mathrm{Tr}\rho(I-T), \quad \beta(T) := \mathrm{Tr}\sigma T. \tag{8.1}$$

As treated in Sect. 5.3.2, it is impossible to determine the true state with probability one from one trial in general, except that two states have orthogonal supports, i.e., $\rho\sigma = 0$. In the general case of two states with non-orthogonal supports, it is required to study the asymptotic theory with a large number of samples in the same way as the ordinary statistics theory. Among the asymptotic theories, the most simple setting is the i.i.d. case where either of ρ or σ is given independently and identically n times. In other words, when a certain apparatus keeps generating particles with the identical state described by ρ or σ, we want to distinguish these states, in which the apparatus is prepared, by quantum measurements on these particles.

Hereafter, the n-fold tensor product of a Hilbert space $\mathcal{H}$ is denoted by $\mathcal{H}^{\otimes n} = \underbrace{\mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n}$ in the same way as the exponential function of a scalar. Similarly

n-fold tensor products of density operators ρ and σ are, respectively, written as

$$\rho^{\otimes n} = \underbrace{\rho \otimes \rho \otimes \cdots \otimes \rho}_{n}, \quad \sigma^{\otimes n} = \underbrace{\sigma \otimes \sigma \otimes \cdots \otimes \sigma}_{n}. \tag{8.2}$$

We consider hypothesis testing of $\rho_n := \rho^{\otimes n}$ and $\sigma_n := \sigma^{\otimes n}$ on the composite system $\mathcal{H}_n := \mathcal{H}^{\otimes n}$. In the asymptotic theory of quantum hypothesis testing, it is important to optimize the measurement as a POVM on the composite system $\mathcal{H}_n$, rather than making plural measurements on $\mathcal{H}$ individually. For a test T_n $(0 \leq T_n \leq I_n)$ on $\mathcal{H}_n$, we can define two kinds of error probabilities:

$$\alpha_n(T_n) := \mathrm{Tr}\rho_n(I_n - T_n), \quad \beta_n(T_n) := \mathrm{Tr}\sigma_n T_n, \tag{8.3}$$

in the same way as the one-shot case, i.e., the case when $n = 1$. Since there is a trade-off between these error probabilities, we can not minimize these two error probabilities simultaneously. Thus we will impose the constant restriction on $\alpha_n(T_n)$ as $\alpha_n(T_n) \leq \epsilon$ $(0 < \epsilon < 1)$, and we consider the optimal error probability for $\beta_n(T_n)$:

$$\beta_n^*(\epsilon) = \min\{\beta_n(T_n) \mid T_n : \text{test}, \ \alpha_n(T_n) \leq \epsilon\}. \tag{8.4}$$

We will study the asymptotic behavior of $\beta_n^*(\epsilon)$. For the problem of the constant restriction, the following theorem holds, which is called the **quantum Stein's lemma**.

Theorem 8.1 ([7, 8]) *For any* $0 < \forall\epsilon < 1$,

$$\lim_{n\to\infty} \frac{1}{n} \log \beta_n^*(\epsilon) = -D(\rho||\sigma) \tag{8.5}$$

holds, where $D(\rho||\sigma)$ *is the quantum relative entropy.*

We can see from this theorem that the quantum relative entropy is an operational quantity for discrimination of two quantum states. The quantum Stein's lemma (Theorem 8.1) is composed of two inequalities:

$$\limsup_{n\to\infty} \frac{1}{n} \log \beta_n^*(\epsilon) \leq -D(\rho||\sigma), \tag{8.6}$$

$$\liminf_{n\to\infty} \frac{1}{n} \log \beta_n^*(\epsilon) \geq -D(\rho||\sigma). \tag{8.7}$$

In this section, we prove the former inequality [7] that is utilized in the later section.

8.2.2 Trace Inequality for Quantum Hypothesis Testing

Since quantum hypothesis testing can be considered as the problem of optimizing the trade-off between error probabilities, we often focus on the weighted sum:

$$w_1 \cdot \alpha(T) + w_2 \cdot \beta(T) = w_1 \mathrm{Tr} \rho (I - T) + w_2 \mathrm{Tr} \sigma T, \tag{8.8}$$

where w_1 and w_2 are positive real numbers. Let $A = w_1 \rho$ and $B = w_2 \sigma$. Then the solution of the minimization is characterized as follows. Hereafter, for a Hermitian operator $A - B$, let $\{A - B > 0\}$ be the projection to the positive part of $A - B$ as defined in Appendix (A.60). Similarly let $(A-B)_+$ and $(A-B)_-$ be, respectively, the positive and negative parts of $A - B$, and $|A - B|$ be the absolute value operator. It is recommended for readers who are not familiar with them to review the corresponding description in Appendix (A.6.3).

Lemma 8.1 *For any non-negative operators A and B,*

$$\max_{\substack{X \le A \\ X \le B}} \mathrm{Tr} X = \min_{0 \le T \le I} \{\mathrm{Tr} A(I - T) + \mathrm{Tr} BT\} \tag{8.9}$$

$$= \frac{1}{2} \mathrm{Tr}(A + B) - \frac{1}{2} \mathrm{Tr}|A - B| \tag{8.10}$$

holds, where the minimum in (8.9) *is attained by* $S := \{A - B > 0\}$.

Proof For any operator X satisfying $X \le A$, $X \le B$ and for any operator T satisfying $0 \le T \le I$, we have

$$\mathrm{Tr}\, X = \mathrm{Tr}\, XT + \mathrm{Tr}\, X(I - T) \le \mathrm{Tr}\, AT + \mathrm{Tr}\, B(I - T). \tag{8.11}$$

Thus, it must hold that

$$\max_{\substack{X \le A \\ X \le B}} \mathrm{Tr}\, X \le \min_{0 \le T \le I} \{\mathrm{Tr}\, A(I - T) + \mathrm{Tr}\, BT\}. \tag{8.12}$$

On the other hand, letting $S = \{A - B > 0\}$, $Y = A(I - S) + BS$, we have

$$Y = A - (A - B)S = A - (A - B)_+ \le A, \tag{8.13}$$

$$Y = B + (A - B)(I - S) = B - (A - B)_- \le B, \tag{8.14}$$

Since Y is an operator satisfying $Y \le A$, $Y \le B$ and S is an operator satisfying $0 \le S \le I$, we have

$$\begin{aligned} \max_{\substack{X \le A \\ X \le B}} \mathrm{Tr}\, X \ge \mathrm{Tr}\, Y = \mathrm{Tr}\, A(I - S) + \mathrm{Tr}\, BS& \\ \ge \min_{0 \le T \le I} \{\mathrm{Tr}\, A(I - T) + \mathrm{Tr}\, BT\}.& \end{aligned} \tag{8.15}$$

Combining (8.12) and (8.15) leads to the assertion (8.9) with the maximum in the left hand side attained by Y and the minimum in the right hand side attained by $S = \{A - B > 0\}$. Summing the both sides of the second equations in (8.13) and (8.14) leads to

$$\begin{aligned} 2\{A(I-S) + BS\} &= A + B - \{(A-B)_+ + (A-B)_-\} \\ &= A + B - |A-B|. \end{aligned} \tag{8.16}$$

Taking the trace of the both sides, we obtain (8.10). □

In the asymptotic theory of hypothesis testing, the trace inequality for operators in the following lemma takes an important role as a rigorous upper bound for (8.9).

Theorem 8.2 (Audenaert et al. [9]) *For any non-negative operators A and B, let $S = \{A - B > 0\}$ and $Y = A(I-S) + BS$. Then for* $0 \le \forall s \le 1$ *we have*

$$\begin{aligned} \operatorname{Tr} Y &= \operatorname{Tr} A(I-S) + \operatorname{Tr} BS \\ &= \frac{1}{2}\operatorname{Tr}(A+B) - \frac{1}{2}\operatorname{Tr}|A-B| \le \operatorname{Tr} A^{1-s}B^s. \end{aligned} \tag{8.17}$$

Proof The equalities have already been proved in the previous lemma. Here we show a simplified proof [10, 11] by Narutaka Ozawa for the inequality. From $A - B \le (A-B)_+$ we have $A \le B + (A-B)_+$, which leads to $A^s \le (B + (A-B)_+)^s$ because $f(x) = x^s$ is an **operator monotone function**; see Appendix A.6.4. Hence we obtain

$$\begin{aligned} \operatorname{Tr} A - \operatorname{Tr} A^{1-s}B^s &= \operatorname{Tr} A^{1-s}\{A^s - B^s\} \\ &\le \operatorname{Tr} A^{1-s}\left\{(B + (A-B)_+)^s - B^s\right\} && (8.18) \\ &\le \operatorname{Tr}(B + (A-B)_+)^{1-s}\left\{(B + (A-B)_+)^s - B^s\right\} && (8.19) \\ &= \operatorname{Tr}(B + (A-B)_+) - \operatorname{Tr}(B + (A-B)_+)^{1-s}B^s \\ &\le \operatorname{Tr}(B + (A-B)_+) - \operatorname{Tr} B^{1-s}B^s && (8.20) \\ &= \operatorname{Tr} B + \operatorname{Tr}(A-B)_+ - \operatorname{Tr} B, && (8.21) \end{aligned}$$

where (8.19) follows from $A^{1-s} \le (B + (A-B)_+)^{1-s}$ and the fact that $B + (A-B)_+ \ge B$ yields $(B + (A-B)_+)^s - B^s \ge 0$. Similary, the last inequality (8.20) follows from $(B + (A-B)_+)^{1-s} \ge B^{1-s}$. Taking (8.13) into account, we have from (8.21) that

$$\operatorname{Tr} Y = \operatorname{Tr} A(I-S) + \operatorname{Tr} BS = \operatorname{Tr} A - \operatorname{Tr}(A-B)_+ \le \operatorname{Tr} A^{1-s}B^s. \tag{8.22}$$

□

This inequality is shown easily when A and B commute each other. In this case, since $S = \{A - B > 0\}$ also commutes with A and B, we have $Y = A(I-S) + BS \ge$

0. Thus we can define Y^s $(0 \leq s \leq 1)$, which satisfies $Y^{1-s} \leq A^{1-s}$ and $Y^s \leq B^s$ from (8.13), (8.14) and the operator monotonicity of x^s $(0 \leq s \leq 1)$. Consequently we have

$$\mathrm{Tr}\, A(I-S) + \mathrm{Tr}\, BS = \mathrm{Tr}\, Y = \mathrm{Tr}\, Y^{1-s} Y^s \leq \mathrm{Tr}\, A^{1-s} Y^s \leq \mathrm{Tr}\, A^{1-s} B^s,$$

which asserts (8.17). However, in the general case, this argument is not available, since $Y \geq 0$ does not always hold when A and B are not commutative. For the original proof of the theorem, we can refer to the paper [9] and the textbook [12], in which several strong techniques for operators are developed, while the alternative proof written above is considerably simple.

Exercise 8.1 We consider the case where two pure states ρ and σ in (6.107) arise with the equal probability $\frac{1}{2}$. Let $A = \frac{1}{2}\rho$ and $B = \frac{1}{2}\sigma$. Calculate $S = \{A - B > 0\}$ specifically, where we assume $0 < a, b < 1$, $a^2 + b^2 = 1$.

Exercise 8.2 (*Continued*) Calculate $Y = A - (A - B)S$ and prove that Y is not always non-negative definite. Note that $\mathrm{Tr} Y$ is the optimal (minimum) average error probability from (8.8) and (8.9). Calculate $\mathrm{Tr} Y$ specifically.

Exercise 8.3 Give an alternative proof of (6.109) using the inequality (8.17).

8.2.3 Asymptotic Theory of Quantum Hypothesis Testing

Quantum hypothesis testing can be regarded as the problem of minimizing the weighted sum of error probabilities in (8.8). Here we consider the weights $w_1 = 1$ and $w_2 = e^{na}$ with an arbitrary real number a, so that the weighted sum is given by

$$\alpha_n(T_n) + e^{na}\beta_n(T_n) = \mathrm{Tr}\rho_n\,(I_n - T_n) + e^{na}\mathrm{Tr}\sigma_n\, T_n. \tag{8.23}$$

From Lemma 8.1, (8.23) is minimized when T_n is equal to

$$S_{n,a} := \{\rho_n - e^{na}\sigma_n > 0\}. \tag{8.24}$$

The test $S_{n,a}$ corresponds to Neyman-Pearson test in the classical hypothesis testing and is called the **quantum Neyman-Pearson test**. The quantum Neyman-Pearson test has the following properties, and it plays an important role in the theory of quantum hypothesis testing.

Lemma 8.2 *We have the following properties for the quantum Neyman-Pearson test* (8.24).

(i) For any test $0 \leq T_n \leq I_n$, *it holds that*

$$\mathrm{Tr}(\rho_n - e^{na}\sigma_n)S_{n,a} \geq \mathrm{Tr}(\rho_n - e^{na}\sigma_n)T_n. \tag{8.25}$$

(ii) We have

$$\mathrm{Tr}(\rho_n - e^{na}\sigma_n)S_{n,a} \geq 0. \tag{8.26}$$

The property (i) follows from Lemma A.6 in Appendix. Especially, taking $T_n = 0$ yields (ii). From (ii) in the above lemma,

$$\mathrm{Tr}(\rho_n - e^{na}\sigma_n)S_{n,a} = \mathrm{Tr}\rho_n S_{n,a} - e^{na}\beta(S_{n,a}) \geq 0 \tag{8.27}$$

holds. Thus for any $a \in \mathbb{R}$ we have

$$\beta_n(S_{n,a}) \leq e^{-na}\mathrm{Tr}\rho_n S_{n,a} \leq e^{-na}. \tag{8.28}$$

As an evaluation of $\alpha_n(S_{n,a})$, the following upper bound is important.

Lemma 8.3 *Let us define functions $\psi(s) = \log \mathrm{Tr}\rho^{1-s}\sigma^s$ and $g(s) = -\psi(s)$. Then for any $a \in \mathbb{R}$ and $0 \leq \forall s \leq 1$, we have*

$$\alpha_n(S_{n,a}) \leq e^{-n\{g(s)-as\}}. \tag{8.29}$$

Proof Applying the inequality (8.17) to $A = \rho_n$ and $B = e^{na}\sigma_n$, it holds for $0 \leq \forall s \leq 1$ that

$$\mathrm{Tr}\rho_n(I_n - S_{n,a}) + e^{na}\mathrm{Tr}\sigma_n S_{n,a} \leq e^{nas}\mathrm{Tr}\rho_n^{1-s}\sigma_n^s. \tag{8.30}$$

Note that the trace in the last term is written as follows:

$$\begin{aligned}\mathrm{Tr}\rho_n^{1-s}\sigma_n^s &= \mathrm{Tr}(\rho^{1-s})^{\otimes n}(\sigma^s)^{\otimes n} \\ &= \mathrm{Tr}(\rho^{1-s}\sigma^s)^{\otimes n} = \left(\mathrm{Tr}\rho^{1-s}\sigma^s\right)^n = e^{n\psi(s)}.\end{aligned} \tag{8.31}$$

Hence from $\alpha_n(S_{n,a}) = \mathrm{Tr}\rho_n(I_n - S_{n,a})$, we obtain

$$\begin{aligned}\alpha_n(S_{n,a}) &\leq \mathrm{Tr}\rho_n(I_n - S_{n,a}) + e^{na}\mathrm{Tr}\sigma_n S_{n,a} \\ &= e^{nas}e^{n\psi(s)} = e^{-n\{g(s)-as\}},\end{aligned} \tag{8.32}$$

which proves the lemma. □

To study the exponent in (8.29), let us examine the function $g(s) = -\psi(s)$. We can show the following properties for $g(s)$, and $\psi(s)$ is called the **relative Rényi entropy**, although detailed derivations are shown in the next subsection.

$$g(0) = 0, \quad g(1) = 0, \quad g(s) \geq 0 \quad (0 \leq s \leq 1), \tag{8.33}$$

$$g'(0) = D(\rho||\sigma), \quad g''(s) < 0. \tag{8.34}$$

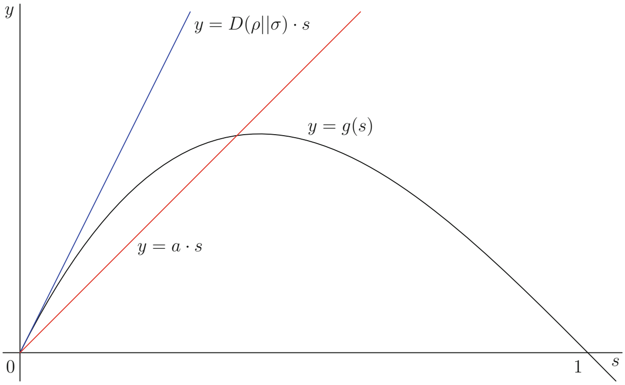


Fig. 8.1 The graph of $y = g(s)$ and $y = as$

From these properties and Proposition A.12, we can illustrate the graph of $g(s)$ as shown in Fig. 8.1, and we can see that it is a continuous and concave function. Note that the exponent in (8.29) equals the difference between the function $y = g(s)$ and the line $y = as$. Since the tangent of $y = g(s)$ at $s = 0$ is the quantum relative entropy $D(\rho||\sigma)$, there exists s such that $g(s) - as > 0$ if $a < D(\rho||\sigma)$. Thus we have the following theorem.

Theorem 8.3 *For any $a < D(\rho||\sigma)$, it holds that*

$$\begin{aligned}\alpha_n(S_{n,a}) &= \mathrm{Tr}\rho^{\otimes n}(I_n - S_{n,a})\\ &= \mathrm{Tr}\rho^{\otimes n}\{\rho^{\otimes n} - e^{na}\sigma^{\otimes n} \le 0\} \overset{n\to\infty}{\longrightarrow} 0. \qquad (8.35)\end{aligned}$$

As a consequence of the above discussions, we can show (8.6) as follows. Let $\delta > 0$ be an arbitrary (small) real number, and let $a = D(\rho||\sigma) - \delta$. Then, for any $\epsilon > 0$ and for any sufficiently large n, $\alpha_n(S_{n,a}) \le \epsilon$ follows from Theorem 8.3. Hence by the definition of $\beta_n^*(\epsilon)$, we have

$$\frac{1}{n}\log\beta_n^*(\epsilon) \le \frac{1}{n}\log\beta_n(S_{n,a}) \le -a = -D(\rho||\sigma) + \delta,$$

where the last inequality follows from (8.28). Taking lim sup of the both sides, we obtain

$$\limsup_{n\to\infty}\frac{1}{n}\log\beta_n^*(\epsilon) \le -D(\rho||\sigma) + \delta.$$

Since $\delta > 0$ can be arbitrary, we have shown (8.6).

The inequalities (8.6) and (8.7) are known to be equivalent to the limit theorem below [13].

Theorem 8.4 (Asymptotic behavior of Neyman-Pearson test [7, 8, 13])

$$\mathrm{Tr}\rho^{\otimes n}\{\rho^{\otimes n} - e^{na}\sigma^{\otimes n} > 0\} \overset{n\to\infty}{\longrightarrow} \begin{cases} 1 & a < D(\rho||\sigma), \\ 0 & a > D(\rho||\sigma). \end{cases} \tag{8.36}$$

In the theory of classical hypothesis testing with two hypotheses P and Q, the asymptotic behavior of the normalized likelihood ratio function $\frac{1}{n}\log\frac{P^{(n)}}{Q^{(n)}}$ characterizes the asymptotic optimal performance, where $P^{(n)}$ and $Q^{(n)}$ are the n-fold i.i.d. extensions of P and Q. In the i.i.d. setting, the asymptotic behavior can be obtained by the weak low of large numbers. In fact, the former characterization holds without assuming the i.i.d. setting because it can be derived from the method of information spectrum [14], which requires no assumption for the form of the distributions of hypotheses.

It can be shown by the quantum version [13] of the method of information spectrum that the asymptotic optimal performance of the quantum hypothesis testing can be characterized by the asymptotic behavior of the above probability. In the i.i.d. setting, in stead of the weak low of large numbers, the above theorem characterizes the asymptotic behavior of the above probability. That is, the above theorem can be regarded as a quantum counter part of the weak low of large numbers for the normalized likelihood ratio.

8.2.4 Properties of Relative Rényi Entropy

We will investigate the behavior of the function $\psi(s)$ used in the previous subsection as $g(s) = -\psi(s)$. In this subsection, the function is written as

$$\psi(s|\rho\|\sigma) = \log \mathrm{Tr}\rho^{1-s}\sigma^{s}, \tag{8.37}$$

by specifying the dependence on ρ and σ. This function is known as one of the quantum f**-divergence** (quasi-entropy) [15], which is a natural generalization of the classical f-divergence treated in Sect. 6.2.6. It is important to note that $\psi(s|\rho\|\sigma)$ obeys the monotonicity, i.e.,

$$\psi(s|\rho\|\sigma) \le \psi(s|\Lambda(\rho)\|\Lambda(\sigma)), \quad \forall s \in (0, 1], \tag{8.38}$$

$$\psi(s|\rho\|\sigma) \ge \psi(s|\Lambda(\rho)\|\Lambda(\sigma)), \quad \forall s \in [-1, 0) \cup (1, 2], \tag{8.39}$$

holds for any TPCP map Λ. Although the monotonicity of the quantum f-divergence plays an important role in quantum information theory, we only prove elementary properties of $\psi(s|\rho\|\sigma)$ needed in this chapter. As the monotonicity of the classical f-divergence follows from the convexity of the function, the monotonicity of the quantum f-divergence is derived [15] from the property of the **operator convex function** as well (see also [8, 12]). In Appendix A.6.4, the definition and some examples of the operator convex function are reviewed briefly.

To show several properties of $\psi(s|\rho\|\sigma)$, we introduce an argument to relate the quantum f-divergence to the classical one. Let

$$\rho = \sum_i a_i E_i, \quad \sigma = \sum_j b_j F_j \tag{8.40}$$

be the spectral decompositions (Theorem A.3) of ρ and σ, respectively. Then we can define probability distributions:

$$P(i,j) = a_i \mathrm{Tr} E_i F_j, \quad Q(i,j) = b_j \mathrm{Tr} E_i F_j, \tag{8.41}$$

since we have

$$\sum_i \sum_j P(i,j) = \mathrm{Tr}(\sum_i a_i E_i)(\sum_j F_j) = \mathrm{Tr}\rho = 1$$

and the same for $Q(i,j)$. Using $P(i,j)$ and $Q(i,j)$, we have

$$\mathrm{Tr}\rho^{1-s}\sigma^s = \sum_i \sum_j a_i^{1-s} b_j^s \mathrm{Tr} E_i F_j = \sum_i \sum_j P(i,j)^{1-s} Q(i,j)^s. \tag{8.42}$$

For simplicity of the notation, let $\mathcal{X}$ denote the range of (i,j) and write $P(i,j)$ and $Q(i,j)$ as $P(x)$ and $Q(x)$, respectively. Using this notation, we study the function $\psi(s) = \log \sum_{x\in\mathcal{X}} P(x)^{1-s} Q(x)^s$, which is called the **relative Rényi entropy** of P and Q.

First we show that $\sum_{x\in\mathcal{X}} P(x)^{1-s} Q(x)^s$ is the classical f-divergence (Sect. 6.2.6). Since $f(t) = -t^s$ is a strictly convex function for $0 \le s \le 1$, we have

$$\begin{aligned} D_f(P\|Q) &= -\sum_{x\in\mathcal{X}} P(x) \left(\frac{Q(x)}{P(x)} \right)^s \\ &= -\sum_{x\in\mathcal{X}} P(x)^{1-s} Q(x)^s \ge f(1) = -1, \end{aligned} \tag{8.43}$$

where the last inequality follows from non-negativity of the f-divergence. In the same way, since $f(t) = t^s$ a strictly convex function for $s \le 0$ or $s \ge 1$, we have

$$\begin{aligned} D_f(P\|Q) &= \sum_{x\in\mathcal{X}} P(x) \left\{ \frac{Q(x)}{P(x)} \right\}^s \\ &= \sum_{x\in\mathcal{X}} P(x)^{1-s} Q(x)^s \ge f(1) = 1. \end{aligned} \tag{8.44}$$

The relative Rényi entropy $\psi(s)$ plays an important role in both classical and quantum hypothesis testing. In the previous subsection, we used the following properties for $\psi(s)$.

Lemma 8.4 *For $\psi(s) = \log \sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s$, the following properties hold.*

(i) $\psi(0) = 0$, $\psi(1) = 0$.
(ii) $\psi(s) \le 0$ $(0 \le s \le 1)$, $\psi(s) \ge 0$ $(s \le 0, s \ge 1)$.
(iii) $\psi'(0) = -D(P||Q)$, $\psi'(1) = D(Q||P)$.
(iv) *If $P \neq Q$, then $\psi''(s) > 0$ holds, i.e., $\psi(s)$ is a* ***convex function****.*

In the following discussion, we take the base of the logarithm to e, which will make the calculation of derivatives easier, since the above properties are independent of the bases. The property (i) is easily verified by making the substitution $s = 0$ and $s = 1$, and (ii) follows from (8.43) and (8.44). Now we show (iii). By definition, $e^{\psi(s)} = \sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s$ holds. If we define

$$P_s(x) := e^{-\psi(s)} P(x)^{1-s} Q(x)^s = \frac{P(x)^{1-s} Q(x)^s}{\sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s},$$

$P_s(x)$ is a probability distribution, and $P_0(x) = P(x)$ and $P_1(x) = Q(x)$. We can calculate the derivative as follows:

$$\begin{aligned}
\psi'(s) &= \frac{\sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s \{-\log P(x) + \log Q(x)\}}{\sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s} \\
&= -e^{-\psi(s)} \sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s \{\log P(x) - \log Q(x)\} \\
&= -\sum_{x \in \mathcal{X}} P_s(x) \{\log P(x) - \log Q(x)\} \\
&= -\mathrm{E}_{P_s}\left[\log P(X) - \log Q(X)\right], \qquad (8.45)
\end{aligned}$$

where $\mathrm{E}_{P_s}[\,\cdot\,]$ denotes the expectation when X is the random variable subject to $P_s(x)$. Making substitution $s = 0$ and $s = 1$ gives (iii). Calculating the derivative further, we can show (iv) as follows:

$$\begin{aligned}
\psi''(s) &= \psi'(s) e^{-\psi(s)} \sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s \{\log P(x) - \log Q(x)\} \\
&\quad + e^{-\psi(s)} \sum_{x \in \mathcal{X}} P(x)^{1-s} Q(x)^s \{\log P(x) - \log Q(x)\}^2 \\
&= \sum_{x \in \mathcal{X}} P_s(x) \{\log P(x) - \log Q(x)\}^2 \\
&\quad + \psi'(s) \sum_{x \in \mathcal{X}} P_s(x) \{\log P(x) - \log Q(x)\}
\end{aligned}$$

$$= \mathrm{E}_{P_s}\left[\{\log P(X) - \log Q(X)\}^2\right] - \left\{\mathrm{E}_{P_s}\left[\log P(X) - \log Q(X)\right]\right\}^2$$
$$= \mathrm{V}_{P_s}\left[\log P(X) - \log Q(X)\right] > 0, \tag{8.46}$$

where $V_{P_s}[\,\cdot\,]$ means the variance of a random variable when X is the random variable subject to $P_s(x)$, and we used the fact that the variance of a random variable is positive except for the deterministic case.

8.3 Classical-Quantum Channel Coding

8.3.1 Message Transmission over Quantum Channels

In classical communication, the channel coding theorem by Shannon[1] characterizes the maximum transmission rate of channels at which reliable communications are possible. In this section, we treat the classical-quantum channel coding theorem established by Holevo [3] and Schumacher-Westmoreland [4]. Suppose that a sender wants to convey classical messages to a receiver by sending quantum mechanical carriers through a quantum channel $\Lambda : \mathcal{S}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{S}(\mathcal{H}_{\mathrm{B}})$. The sender will use input signals represented by density operators $\rho_1, \ldots, \rho_N$ to induce output states $\Lambda(\rho_1), \ldots, \Lambda(\rho_N)$. As shown in Fig. 8.2, once these density operators are fixed, we can consider the map from the input alphabet $\mathcal{X} = \{1, \ldots, N\}$ to the output states, i.e.,

$$W : x \in \mathcal{X} \longmapsto W_x := \Lambda(\rho_x), \tag{8.47}$$

which is called the **classical-quantum channel**.

For a given quantum channel Λ, the choice of input states $\{\rho_x\}_{x\in\mathcal{X}}$ should be optimized for effective transmission of messages. We assume that a sufficient variety of input states can be prepared and fixed. Indeed, it is known that $N = \dim \Lambda(\mathcal{S}(\mathcal{H}_{\mathrm{A}})) + 1$ kinds of input states are sufficient for the optimization of the channel capacity [16].

We will discuss the encoding and decoding system of message transmission and its asymptotic efficiency when the channel can be used repeatedly. For simplicity, let $\mathcal{H} = \mathcal{H}_{\mathrm{B}}$ denote the Hilbert space of the output of the quantum channel. When the same classical-quantum channel $x \in \mathcal{X} \longmapsto W_x \in \mathcal{S}(\mathcal{H})$ is used n times, we consider the extended channel:

$$W^{(n)} : x^n = x_1 x_2 \cdots x_n \in \mathcal{X}^n \mapsto W^{(n)}_{x^n} = W_{x_1} \otimes W_{x_2} \cdots \otimes W_{x_n} \in \mathcal{S}\big(\mathcal{H}^{\otimes n}\big),$$

[1] We treat the classical channel coding theorem for a class of channels with a certain symmetry in Sect. 9.2

$$x \in \mathcal{X} \longrightarrow \rho_x \longrightarrow \boxed{\Lambda} \longrightarrow W_x$$

Fig. 8.2 Classical-quantum channel

$k \in \{1, 2, \cdots, M_n\}$ message

$\Downarrow$ encoder $\phi^{(n)}$

$$\begin{array}{ccccccccc} \phi^{(n)}(k) & = & x_1(k) & , & x_2(k) & , & \cdots & , & x_n(k) \\ & & \downarrow & & \downarrow & & & & \downarrow \\ W^{(n)}_{\phi^{(n)}(k)} & = & W_{x_1(k)} & \otimes & W_{x_2(k)} & \otimes & \cdots & \otimes & W_{x_n(k)} \end{array}$$

$\Downarrow$ decoder $X^{(n)} = \{X_0^{(n)}, X_1^{(n)}, \ldots, X_{M_n}^{(n)}\}$ (POVM on $\mathcal{H}^{\otimes n}$)

$l \in \{0, 1, 2, \cdots, M_n\}$ measurement outcomes (0 indicates the failure of decoding)

Fig. 8.3 Encoding and decoding process of messages

which is called the stationary memoryless classical-quantum channel. The information to be transmitted is called a message and is randomly chosen from $\{1, 2, \ldots, M_n\}$.

The problem to send the message via the above channel is called stationary memoryless classical-quantum channel coding. Figure 8.3 describes the process of message transmission. Prior to the message transmission, each message $k \in \{1, \ldots, M_n\}$ is assigned to an input sequence $\phi^{(n)}(k) = (x_1(k), x_2(k) \ldots, x_n(k)) \in \mathcal{X}^n$, namely the **codeword**, and the sender and the receiver agree the list of these assignments, which is called the **codebook**. In the communication stage, the message $k \in \{1, \ldots, M_n\}$ is mapped to the sequence of quantum states corresponding to the codeword $\phi^{(n)}(k) = (x_1(k), x_2(k) \ldots, x_n(k)) \in \mathcal{X}^n$, where the map $\phi^{(n)}$ is called the **encoder**, and then the receiver obtains the sequence of quantum states $W^{(n)}_{\phi^{(n)}(k)} := W_{x_1(k)} \otimes \cdots \otimes W_{x_n(k)}$. The receiver will apply a quantum measurement on the system under the state $W^{(n)}_{\phi^{(n)}(k)}$ to decide which message was sent. In classical-quantum channel coding, it is important to optimize the quantum measurement over the whole composite system, rather than to make individual measurements on each system at the output. Thus the **decoder** is represented by a POVM $X^{(n)} = \{X_0^{(n)}, X_1^{(n)}, \ldots, X_{M_n}^{(n)}\}$ on the composite system $\mathcal{H}^{\otimes n}$, where the measurement outcomes $1, \ldots, M_n$ indicate decoded messages and 0 indicates the failure of decoding. A pair of the encoder and the decoder $\Phi_n := (\phi^{(n)}, X^{(n)})$ is called a **code**.

When the message k was sent, the success probability of decoding is given by $\mathrm{Tr} W^{(n)}_{\phi^{(n)}(k)} X_k^{(n)}$. Assuming that each message arises with the uniform probability, the **average error probability** of the code $\Phi_n = (\phi^{(n)}, X^{(n)})$ is defined by

$$P_e(\Phi_n) = \frac{1}{M_n} \sum_{k=1}^{M_n} \left(1 - \mathrm{Tr} W^{(n)}_{\phi^{(n)}(k)} X^{(n)}_k\right). \tag{8.48}$$

The **transmission rate** or **coding rate** is defined by $R_n := \frac{1}{n} \log M_n$, which means how many bits can be sent per one-shot usage of the channel. If the channel is used N_0 times in a second, $N_0 R_n$ is the transmission speed and has the unit bps (bit/second). For a code $\Phi_n = (\phi^{(n)}, X^{(n)})$, let $|\Phi_n|$ denote the number of messages M_n. There is a tradeoff between the error probability $P_e(\Phi_n)$ and the transmission rate R_n. Our goal is to make the transmission rate R_n as large as possible, under the condition that the error probability goes to zero asymptotically. The **channel capacity** C is defined as the supremum of such transmission rates.

Definition 8.1 (*classical-quantum channel capacity*)

$$C := \sup\left\{ R \;\middle|\; \exists \left\{\Phi_n\right\}_{n=1}^{\infty}, \lim_{n\to\infty} P_e(\Phi_n) = 0, \liminf_{n\to\infty} \frac{1}{n} \log |\Phi_n| \geq R \right\}. \tag{8.49}$$

Note that the channel capacity is defined in the operational manner. Surprisingly, the **classical-quantum channel coding theorem** states that the channel capacity is equal to the maximum of the Holevo mutual information (Sect. 6.3.3), though there seems to be no apparent relation with mathematical information quantities.

Theorem 8.5 ([1–4]) *For a classical-quantum channel $W : x \in \mathcal{X} \longmapsto W_x \in \mathcal{S}(\mathcal{H})$, it holds that*

$$C = \max_{P \in \mathcal{P}(\mathcal{X})} I(P; W), \tag{8.50}$$

where $I(P; W)$ is the Holevo mutual information and $\mathcal{P}(\mathcal{X})$ is the set of probability distributions on $\mathcal{X}$.

The classical-quantum channel coding theorem is composed of two parts:

$$C \leq \max_{P \in \mathcal{P}(\mathcal{X})} I(P; W), \tag{8.51}$$

$$C \geq \max_{P \in \mathcal{P}(\mathcal{X})} I(P; W). \tag{8.52}$$

The inequality (8.51) shows the limitation on reliable transmission rates and is called the **Holevo bound**, since it was shown by Holevo [1, 2] in 1970s. On the other hand, the inequality (8.52) means the achievability of the transmission rate, and it was proved in the middle of 1990s [3, 4]. After alternative proofs have been developed [17, 18], a transparent proof based on quantum hypothesis testing has been obtained [19, 20], which will be introduced in this section. The facts (8.51) and (8.52) are called the **converse part** and the **direct part**, respectively. In the subsequent subsections, we show the both inequalities.

8.3.2 Proof of the C-Q Channel Coding Theorem (Converse Part)

In this subsection, we prove the inequality (8.51) called the Holevo bound [1, 2], which implies the limitation on reliable transmission rates in classical-quantum channel coding. Among several proofs of the inequality known so far, we introduce the original argument by Holevo [1, 2], from which we can clearly understand the difference between the classical case and the classical-quantum case.

First we show so called the **super additivity** in classical-quantum channel coding. Consider n-fold extension of the channel, as shown in Fig. 8.3,

$$W^{(n)} : x^n = x_1 x_2 \cdots x_n \in \mathcal{X}^n \mapsto W^{(n)}_{x^n} = W_{x_1} \otimes W_{x_2} \cdots \otimes W_{x_n} \in \mathcal{S}\big(\mathcal{H}^{\otimes n}\big).$$

For an arbitrarily fixed measurement (POVM) $\big\{Y^{(n)}_k\big\}_k$ on $\mathcal{H}^{\otimes n}$, we can define the classical channel (conditional probability) by

$$V^{(n)}(k|x^n) = \operatorname{Tr} W^{(n)}_{x^n} Y^{(n)}_k. \tag{8.53}$$

For an input probability distribution $P^{(n)} = \{P^{(n)}(x^n)\}_{x^n \in \mathcal{X}^n}$ on $\mathcal{X}^n$, the classical channel $V^{(n)}$ induces the output probability distribution $Q^{(n)}$ defined by

$$Q^{(n)}(k) = \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) V^{(n)}(k|x^n) \tag{8.54}$$

$$= \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) \operatorname{Tr} W^{(n)}_{x^n} Y^{(n)}_k = \operatorname{Tr} W^{(n)}_{P^{(n)}} Y^{(n)}_k, \tag{8.55}$$

where we put $W^{(n)}_{P^{(n)}} := \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) W^{(n)}_{x^n}$. Then we can define the classical mutual information by

$$I^{(n)}_{Y^{(n)}}\big(P^{(n)}; W^{(n)}\big) := \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) D_{Y^{(n)}}\big(W^{(n)}_{x^n} \parallel W^{(n)}_{P^{(n)}}\big), \tag{8.56}$$

where $D_{Y^{(n)}}\big(W^{(n)}_{x^n} \parallel W^{(n)}_{P^{(n)}}\big)$ is the classical divergence defined by

$$D_{Y^{(n)}}\big(W^{(n)}_{x^n} \parallel W^{(n)}_{P^{(n)}}\big) = \sum_k V^{(n)}(k|x^n) \log \frac{V^{(n)}(k|x^n)}{Q^{(n)}(k)}, \tag{8.57}$$

which is the divergence between the probabilities of measurement outcomes, for density operators $W^{(n)}_{x^n}$ and $W^{(n)}_{P^{(n)}}$, when the measurement $Y^{(n)}$ is performed. We now focus on the maximization of the mutual information $I^{(n)}_{Y^{(n)}}\big(P^{(n)}; W^{(n)}\big)$ over the input probability $P^{(n)}$ and the measurement $Y^{(n)}$, i.e.,

$$C^{(n)} := \max_{P^{(n)}} \max_{Y^{(n)}} I_{Y^{(n)}}^{(n)}\big(P^{(n)}; W^{(n)}\big). \tag{8.58}$$

This quantity satisfies the **super additivity**.

Lemma 8.5 (super additivity [2])

$$C^{(m+n)} \geq C^{(n)} + C^{(m)}. \tag{8.59}$$

Proof Note that independent measurements, $Y^{(m)} = \{Y^{(m)}(k)\}_k$ on $\mathcal{H}^{\otimes m}$ and $Y^{(n)} = \{Y^{(n)}(l)\}_k$ on $\mathcal{H}^{\otimes n}$, are totally represented by

$$Y^{(m)} \otimes Y^{(n)} := \{Y^{(m)}(k) \otimes Y^{(n)}(l)\}_{k,l} \tag{8.60}$$

and that it is a special case of generalized measurements $Y^{(m+n)}$ on $\mathcal{H}^{\otimes(m+n)}$. In the same way, the product of probability distributions, $P^{(m)} = \{P^{(m)}(x^m)\}$ on $\mathcal{X}^m$ and $P^{(n)} = \{P^{(n)}(x^n)\}$ on $\mathcal{X}^n$, is defined by

$$\begin{aligned}&\big(P^{(m)} \cdot P^{(n)}\big)(x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n})\\ &= P^{(m)}(x_1, \ldots, x_n) \cdot P^{(n)}(x_{n+1}, \ldots, x_{n+m}),\end{aligned} \tag{8.61}$$

and it is a special case of probability distributions $P^{(m+n)}$ on $\mathcal{X}^{m+n}$. Taking them into account, we have

$$\begin{aligned}C^{(m+n)} &= \max_{P^{(m+n)}} \max_{Y^{(m+n)}} I_{Y^{(m+n)}}^{(m+n)}\big(P^{(m+n)}; W^{(m+n)}\big)\\ &\geq \max_{P^{(m)},P^{(n)}} \max_{Y^{(m)},Y^{(n)}} I_{Y^{(m)}\otimes Y^{(n)}}^{(m+n)}\big(P^{(m)} \cdot P^{(n)}; W^{(m+n)}\big).\end{aligned} \tag{8.62}$$

Note that from the additivity of the classical divergence we have

$$\begin{aligned}&I_{Y^{(m)}\otimes Y^{(n)}}^{(m+n)}\big(P^{(m)} \cdot P^{(n)}; W^{(m+n)}\big)\\ &\qquad = I_{Y^{(m)}}^{(m)}\big(P^{(m)}; W^{(m)}\big) + I_{Y^{(n)}}^{(n)}\big(P^{(n)}; W^{(n)}\big).\end{aligned}$$

Maximizing the both sides over measurements $Y^{(m)}, Y^{(n)}$ and the probabilities $P^{(m)}, P^{(n)}$, the left hand side yields (8.62), while the right hand side leads to $C^{(n)} + C^{(m)}$. Thus we have shown (8.59). □

The operational meaning of $C^{(n)}$ is explained as follows. If we fix a measurement $Y^{(n)}$ on the whole composite system at the output side of the extended channel $W^{(n)}$, the capacity of the total classical channel from the input to the measurement outcome, is given by $\max_{P^{(n)}} I_{Y^{(n)}}^{(n)}\big(P^{(n)}; W^{(n)}\big)$ from the channel coding theorem by Shannon [21, 22]. Then optimizing the channel capacity over the measurement $Y^{(n)}$ yields $C^{(n)}$. In other words, $C^{(n)}$ is the best achievable transmission rate of the classical-quantum channel $W^{(n)}$ when any measurements over the n-fold composite system are allowed. From the above lemma, the larger composite system we utilize for the optimization of the measurement, the better performance we obtain for the transmission rate.

In fact, **Fano inequality** (Theorem 6.6) in the classical theory leads to the following theorem.

Theorem 8.6 (Holevo [2])

$$C \leq \lim_{n\to\infty} \frac{C^{(n)}}{n} = \sup_{n\geq 1} \frac{C^{(n)}}{n}. \tag{8.63}$$

Remark 8.1 In fact, Holevo [2] showed the equality $C = \lim_{n\to\infty} \frac{C^{(n)}}{n}$. However, we only show the inequality $C \leq \lim_{n\to\infty} \frac{C^{(n)}}{n}$ here because we use only the inequality in our context.

Proof From Lemma A.7 in Appendix, we can see that $\lim_{n\to\infty} \frac{C^{(n)}}{n}$ exists and equals to $\sup_{n\geq 1} \frac{C^{(n)}}{n}$. We show the converse inequality using Fano inequality in the classical theory. Assume that $R < C$. Then, from the definition of the classical-quantum channel capacity, there exists a sequence of codes $\Phi_n = (\phi^{(n)}, X^{(n)})$ $(n = 1, 2, \ldots)$ satisfying

$$\lim_{n\to\infty} P_e(\Phi_n) = 0, \quad \liminf_{n\to\infty} \frac{1}{n} \log |\Phi_n| \geq R. \tag{8.64}$$

In the following, we fix the code $\Phi_n = (\phi^{(n)}, X^{(n)})$ and let $M_n = |\Phi_n|$ be the number of messages. Let $P^{(n)}$ be the uniform distribution $P^{(n)}(k) = \frac{1}{M_n}$ $(k = 1, 2, \ldots, M_n)$ on the messages $\{1, 2, \ldots, M_n\}$, and $V^{(n)}$ be the conditional probability defined by $V^{(n)}(l|k) = \mathrm{Tr} W^{(n)}_{\phi^{(n)}(k)} X^{(n)}_l$. If $(K^{(n)}, L^{(n)})$ is the joint random variable subject to $P^{(n)}(k)V^{(n)}(l|k)$, Fano inequality implies

$$\begin{aligned}\log 2 + P_e(\Phi^{(n)}) \log M_n \geq H(K^{(n)}|L^{(n)}) &= H(P^{(n)}) - I(P^{(n)}; V^{(n)}) \\ &\geq \log M_n - \max_{P^{(n)}} \max_{Y^{(n)}} I^{(n)}_{Y^{(n)}}(P^{(n)}; W^{(n)}),\end{aligned} \tag{8.65}$$

where we used the fact that the maximum of the binary entropy is $\log 2$, $H(P^{(n)}) = \log M_n$, and $I(P^{(n)}; V^{(n)}) = I^{(n)}_{X^{(n)}}(P^{(n)}; W^{(n)})$. Thus we have

$$\left\{1 - P_e(\Phi^{(n)})\right\} \frac{\log M_n}{n} \leq \frac{C^{(n)}}{n} + \frac{\log 2}{n}. \tag{8.66}$$

It must follow from this inequality and (8.64) that

$$R \leq \liminf_{n\to\infty} \frac{\log M_n}{n} \leq \lim_{n\to\infty} \frac{C^{(n)}}{n}, \tag{8.67}$$

since $\lim_{n\to\infty} P_e(\Phi^{(n)}) = 0$. Thus we have shown that $R < C$ implies $R \leq \lim_{n\to\infty} \frac{C^{(n)}}{n}$, which means $C \leq \lim_{n\to\infty} \frac{C^{(n)}}{n}$. □

We show a useful lemma concerning the maximization of the Holevo mutual information.

Lemma 8.6 *Given two classical-quantum channels $W^{\mathrm{A}} : x \in \mathcal{X} \mapsto W^{\mathrm{A}}_x \in \mathcal{S}(\mathcal{H}_{\mathrm{A}})$ and $W^{\mathrm{B}} : y \in \mathcal{Y} \mapsto W^{\mathrm{B}}_y \in \mathcal{S}(\mathcal{H}_{\mathrm{B}})$, let*

$$W^{\mathrm{AB}} : (x, y) \in \mathcal{X} \times \mathcal{Y} \mapsto W^{\mathrm{AB}}_{x,y} = W^{\mathrm{A}}_x \otimes W^{\mathrm{B}}_y \in \mathcal{S}(\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}})$$

be the tensor product of the channel. Then, for any joint probability $P_{XY}(x, y)$ on $\mathcal{X} \times \mathcal{Y}$, we have

$$I(P_{XY}; W^{\mathrm{AB}}) \leq I(P_X; W^{\mathrm{A}}) + I(P_Y; W^{\mathrm{B}}), \tag{8.68}$$

where $P_X(x)$ and $P_Y(y)$ are the marginal probability distributions of $P_{XY}(x, y)$. Especially, we have

$$\max_{P_{XY}} I(P_{XY}; W^{\mathrm{AB}}) = \max_{P_X} I(P_X; W^{\mathrm{A}}) + \max_{P_Y} I(P_Y; W^{\mathrm{B}}). \tag{8.69}$$

Proof From the additivity of the von Neumann entropy, we have

$$\begin{aligned} \sum_{x,y} P_{XY}(x, y) H(W^{\mathrm{AB}}_{x,y}) &= \sum_{x,y} P_{XY}(x, y) \left\{ H(W^{\mathrm{A}}_x) + H(W^{\mathrm{B}}_y) \right\} \\ &= \sum_x P_X(x) H(W^{\mathrm{A}}_x) + \sum_y P_Y(y) H(W^{\mathrm{B}}_y). \end{aligned} \tag{8.70}$$

Hence, the assertion can be shown as follows:

$$\begin{aligned} & I(P_X; W^{\mathrm{A}}) + I(P_Y; W^{\mathrm{B}}) - I(P_{XY}; W^{\mathrm{AB}}) \\ &= H(W^{\mathrm{A}}_{P_X}) - \sum_x P_X(x) H(W^{\mathrm{A}}_x) + H(W^{\mathrm{B}}_{P_Y}) - \sum_y P_Y(y) H(W^{\mathrm{B}}_y) \\ &\quad - H(W^{\mathrm{AB}}_{P_{XY}}) + \sum_{x,y} P_{XY}(x, y) H(W^{\mathrm{AB}}_{x,y}) \\ &= H(W^{\mathrm{A}}_{P_X}) + H(W^{\mathrm{B}}_{P_Y}) - H(W^{\mathrm{AB}}_{P_{XY}}) \geq 0, \end{aligned} \tag{8.71}$$

where we used $\mathrm{Tr}_{\mathrm{B}} W^{\mathrm{AB}}_{P_{XY}} = W^{\mathrm{A}}_{P_X}$, $\mathrm{Tr}_{\mathrm{A}} W^{\mathrm{AB}}_{P_{XY}} = W^{\mathrm{B}}_{P_Y}$, and the subadditivity of the von Neumann entropy (Lemma 6.7). □

Lemma 8.6 and the monotonicity of the quantum relative entropy (6.53) lead to

$$I^{(n)}_{Y^{(n)}}\big(P^{(n)}; W^{(n)}\big) \le I\big(P^{(n)}; W^{(n)}\big) \le n \max_{P \in \mathcal{P}(\mathcal{X})} I(P; W). \tag{8.72}$$

Combining Theorem 8.6 and (8.72), we can show the converse part of the classical-quantum channel coding theorem.

Theorem 8.7 (Converse Part [1, 2])

$$C \le \max_{P \in \mathcal{P}(\mathcal{X})} I(P; W). \tag{8.73}$$

Proof Since (8.72) implies that $\frac{C^{(n)}}{n} \le \max_{P \in \mathcal{P}(\mathcal{X})} I(P; W)$, Theorem 8.6 yields the desired inequality. □

8.3.3 Proof of the C-Q Channel Coding Theorem (Direct Part)

In this subsection we show the proof of the direct part (8.52), in which the existence of efficient codes to attain the channel capacity is proved. Here we follow the transparent method by Hayashi-Nagaoka [19], in which the following operator inequality plays an important role.

Lemma 8.7 (Hayashi-Nagaoka [19]) *Let S and T be Hermitian operators such that $0 \le S \le I$ and $T \ge 0$. Then we have*

$$I - \sqrt{S+T}^{-1} S \sqrt{S+T}^{-1} \le 2(I - S) + 4T, \tag{8.74}$$

where $\sqrt{S+T}^{-1}$ is defined as the operator satisfying $\mathrm{Ker}\sqrt{S+T}^{-1} = \mathrm{Ker}(S+T)$ *and* $\sqrt{S+T}\sqrt{S+T}^{-1}\sqrt{S+T} = \sqrt{S+T}$.[2]

Proof Let P be the projection to $\mathrm{Ran}(S+T)$, i.e., the support of $S+T$. Then it is clear that P commutes with S and T, and it holds that $PS = S$, $PT = T$, and $P\sqrt{S+T}^{-1} = \sqrt{S+T}^{-1}$. Similarly, let $P^{\perp} = I - P$, then $P^{\perp}$ is the projection to $\mathrm{Ker}(S+T)$. Obviously $P^{\perp}$ commutes with S and T, and we have $P^{\perp}S = 0$, $P^{\perp}T = 0$, and $P^{\perp}\sqrt{S+T}^{-1} = 0$. Thus it is enough to show the following inequalities:

$$P\left\{I - \sqrt{S+T}^{-1} S \sqrt{S+T}^{-1}\right\} \le P\{2(I - S) + 4T\}, \tag{8.75}$$

$$P^{\perp}\left\{I - \sqrt{S+T}^{-1} S \sqrt{S+T}^{-1}\right\} \le P^{\perp}\{2(I - S) + 4T\}. \tag{8.76}$$

[2] For matrices S and T, $\sqrt{S+T}^{-1}$ is called the generalized inverse.

Since it is easy to verify (8.76), we show (8.75) below. We can assume that $S+T$ has the inverse without loss of generality, by restricting the Hilbert space to $\mathrm{Ran}(S+T)$. Note that, since $(A-B)^\dagger(A-B) = A^\dagger A - A^\dagger B - B^\dagger A + B^\dagger B \geq 0$, we have $A^\dagger B + B^\dagger A \leq A^\dagger A + B^\dagger B$. Let $A = \sqrt{T}$ and $B = \sqrt{T}(\sqrt{S+T}^{-1} - I)$. Then we have

$$\begin{aligned} & T(\sqrt{S+T}^{-1} - I) + (\sqrt{S+T}^{-1} - I)T \\ & \leq T + (\sqrt{S+T}^{-1} - I)T(\sqrt{S+T}^{-1} - I), \end{aligned} \tag{8.77}$$

and hence, it holds that

$$\begin{aligned} I - \sqrt{S+T}^{-1} S \sqrt{S+T}^{-1} &= \sqrt{S+T}^{-1} T \sqrt{S+T}^{-1} \\ &= T + T(\sqrt{S+T}^{-1} - I) + (\sqrt{S+T}^{-1} - I)T \\ &\quad + (\sqrt{S+T}^{-1} - I)T(\sqrt{S+T}^{-1} - I) \\ &\overset{\text{(a)}}{\leq} 2T + 2(\sqrt{S+T}^{-1} - I)T(\sqrt{S+T}^{-1} - I) \\ &\leq 2T + 2(\sqrt{S+T}^{-1} - I)(S+T)(\sqrt{S+T}^{-1} - I) \\ &= 2T + 2(I - \sqrt{S+T})^2 \\ &= 2T + 2(S+T+I-2\sqrt{S+T}) \\ &\overset{\text{(b)}}{\leq} 2T + 2(S+T+I-2S) = 2(I-S) + 4T \end{aligned} \tag{8.78}$$

Here, the inequality (a) follows from (8.77), and the inequality (b) is derived from $\sqrt{S+T} \geq \sqrt{S} \geq S$ which follows from the fact that $\sqrt{x}$ is an **operator monotone function** (Appendix A.6.4) and $0 \leq S \leq I$. □

Lemma 8.8 (Hayashi-Nagaoka [19]) *Given n-fold extension* $W^{(n)} : x^n \in \mathcal{X}^n \longmapsto W^{(n)}_{x^n} \in \mathcal{S}(\mathcal{H}^{\otimes n})$ *of the classical quantum channel, for any probability distribution* $P^{(n)}(x)$ *on* $\mathcal{X}^n$ *and any real number* $c > 0$, *there exists a code* $\Phi_n = (\phi^{(n)}, X^{(n)})$ *such that*

$$\begin{aligned} P_e(\Phi_n) \leq 2 & \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) \mathrm{Tr} W^{(n)}_{x^n} \{W^{(n)}_{x^n} - c\, W^{(n)}_{P^{(n)}} \leq 0\} \\ & + 4M_n \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) \mathrm{Tr} W^{(n)}_{P^{(n)}} \{W^{(n)}_{x^n} - c\, W^{(n)}_{P^{(n)}} > 0\}, \end{aligned} \tag{8.79}$$

where $M_n = |\Phi_n|$ *is the number of the messages and we put* $W^{(n)}_{P^{(n)}} = \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) W^{(n)}_{x^n}$.

Proof The proof is shown using the **random coding** argument by Shannon. First, we consider an ensemble of codes $\Phi_n = (\phi^{(n)}, X^{(n)})$ and show that the expectation of the error probability with respect to the ensemble has sufficiently good performance. Then there must be, at least, a good code that has better performance than the expectation.

To make the ensemble of codes, for each message $k \in \{1, 2, \ldots, M_n\}$ let the codeword $\phi^{(n)}(k) \in \mathcal{X}^n$ be generated randomly subject to the probability distribution $P^{(n)}(x^n)$ independently. The sender and the receiver agree the codebook $\{\phi^{(n)}(k)\}_{k=1}^{M_n}$. The decoder $X^{(n)}$ is made from

$$S_{x^n} = \{W_{x^n}^{(n)} - c\, W_{P^{(n)}}^{(n)} > 0\} \quad (x^n \in \mathcal{X}^n), \tag{8.80}$$

by regularizing it to be a POVM. For each message $k = 1, 2, \ldots, M_n$, let

$$X_k^{(n)} = \left(\sum_{l=1}^{M_n} S_{\phi^{(n)}(l)}\right)^{-\frac{1}{2}} S_{\phi^{(n)}(k)} \left(\sum_{l=1}^{M_n} S_{\phi^{(n)}(l)}\right)^{-\frac{1}{2}}, \tag{8.81}$$

and $X_0^{(n)} = I - \sum_{k=1}^{M_n} X_k^{(n)}$, then these operators satisfy the condition to be a POVM. Applying Lemma 8.7 for $S = S_{\phi^{(n)}(k)}$ and $T = \sum_{l \neq k} S_{\phi^{(n)}(l)}$, we obtain

$$\begin{aligned}
P_e(\Phi_n) &= \frac{1}{M_n} \sum_{k=1}^{M_n} \mathrm{Tr} W_{\phi^{(n)}(k)}^{(n)} (I_n - X_k^{(n)}) \\
&\le \frac{2}{M_n} \sum_k \mathrm{Tr} W_{\phi^{(n)}(k)}^{(n)} (I_n - S_{\phi^{(n)}(k)}) + \frac{4}{M_n} \sum_k \sum_{l \neq k} \mathrm{Tr} W_{\phi^{(n)}(k)}^{(n)} S_{\phi^{(n)}(l)}.
\end{aligned}$$

Since $\phi^{(n)}(k)$ and $\phi^{(n)}(l)$ $(k \neq l)$ are subject to $P^{(n)}(x^n)$ independently, taking the expectation with respect to the random coding method, we have the following relations:

$$\begin{aligned}
&E\big[P_e(\Phi_n)\big] \\
&\le \frac{2}{M_n} \sum_k E\left[\mathrm{Tr} W_{\phi^{(n)}(k)}^{(n)} (I_n - S_{\phi^{(n)}(k)})\right] + \frac{4}{M_n} \sum_k \sum_{l \neq k} E\left[\mathrm{Tr} W_{\phi^{(n)}(k)}^{(n)} S_{\phi^{(n)}(l)}\right] \\
&= \frac{2}{M_n} \sum_k E_{X^n}\left[\mathrm{Tr} W_{X^n}^{(n)} (I_n - S_{X^n})\right] + \frac{4}{M_n} \sum_k \sum_{l \neq k} E_{\tilde{X}^n}\left[\mathrm{Tr} E_{X^n}\left[W_{X^n}^{(n)}\right] S_{\tilde{X}^n}\right] \\
&= 2 \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) \mathrm{Tr} W_{x^n}^{(n)} (I_n - S_{x^n}) + 4(M_n - 1) \sum_{x^n \in \mathcal{X}^n} P^{(n)}(x^n) \mathrm{Tr} W_{P^{(n)}}^{(n)} S_{x^n}.
\end{aligned}$$

Thus the expectation was evaluated, and hence, there must be a code $\Phi_n = (\phi^{(n)}, X^{(n)})$ satisfying the assertion. □

Theorem 8.8 (direct part [3, 4])

$$C \geq \max_{P \in \mathcal{P}(\mathcal{X})} I(P; W) \tag{8.82}$$

Proof We show the proof by Hayashi-Nagaoka [19]. Let us apply Lemma 8.8 to the stationary memoryless probability distribution $P^n(x^n) = P(x_1)P(x_2)\cdots P(x_n)$ on $\mathcal{X}^n$ and $c = e^{na}$ $(a \in \mathbb{R})$. Then, since we have $W^{(n)}_{P^n} = W_P^{\otimes n}$, there exists a code $\Phi_n = (\phi^{(n)}, X^{(n)})$ such that $\left|\Phi^{(n)}\right| = M_n$ and

$$\begin{aligned} P_e(\Phi^{(n)}) \leq 2 &\sum_{x^n \in \mathcal{X}^n} P^n(x^n)\,\mathrm{Tr} W^{(n)}_{x^n}\{W^{(n)}_{x^n} - e^{na} W_P^{\otimes n} \leq 0\} \\ &+ 4M_n \sum_{x^n \in \mathcal{X}^n} P^n(x^n)\,\mathrm{Tr} W_P^{\otimes n}\{W^{(n)}_{x^n} - e^{na} W_P^{\otimes n} > 0\}. \end{aligned} \tag{8.83}$$

Let us see that the right hand side is related to the error probability of quantum hypothesis testing. In the same way as the discussion in (6.63) and (6.64), let $\mathcal{H}_\mathrm{A}$ be the Hilbert space with the dimension $\dim \mathcal{H}_\mathrm{A} = |\mathcal{X}|$. Let $\{|x\rangle\}_{x \in \mathcal{X}}$ be an orthonormal basis for $\mathcal{H}_\mathrm{A}$ and put $\mathcal{H}_\mathrm{B} = \mathcal{H}$. Then we can define the density operator on $\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{B}$ by

$$\rho_{\mathrm{AB}} := \sum_{x \in \mathcal{X}} P(x)|x\rangle\langle x| \otimes W_x. \tag{8.84}$$

Since we have $\rho_\mathrm{A} = \mathrm{Tr}_\mathrm{B}[\rho_{\mathrm{AB}}] = \sum_{x \in \mathcal{X}} P(x)|x\rangle\langle x|$ and $\rho_\mathrm{B} = \mathrm{Tr}_\mathrm{A}[\rho_{\mathrm{AB}}] = \sum_{x \in \mathcal{X}} P(x) W_x = W_P$, it holds that $\rho_\mathrm{A} \otimes \rho_\mathrm{B} = \sum_{x \in \mathcal{X}} P(x)|x\rangle\langle x| \otimes W_P$. Let $\rho := \rho_{\mathrm{AB}}$ and $\sigma := \rho_\mathrm{A} \otimes \rho_\mathrm{B}$. Using the notation $|x^n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$, their n-fold tensor products are calculated as

$$\rho^{\otimes n} = \sum_{x^n \in \mathcal{X}^n} P^n(x^n)|x^n\rangle\langle x^n| \otimes W^{(n)}_{x^n}, \tag{8.85}$$

$$\sigma^{\otimes n} = \sum_{x^n \in \mathcal{X}^n} P^n(x^n)|x^n\rangle\langle x^n| \otimes W_P^{\otimes n}. \tag{8.86}$$

Consider simple quantum hypothesis testing between $\rho^{\otimes n}$ and $\sigma^{\otimes n}$. Then the Neyman-Pearson test is given by

$$\begin{aligned} S_{n,a} &:= \{\rho^{\otimes n} - e^{na}\sigma^{\otimes n} > 0\} \\ &= \sum_{x^n \in \mathcal{X}^n} |x^n\rangle\langle x^n| \otimes \{W^{(n)}_{x^n} - e^{na} W_P^{\otimes n} > 0\}. \end{aligned} \tag{8.87}$$

Thus the error probabilities of the test $S_{n,a}$ are written as follows:

$$\begin{aligned}\alpha_n(S_{n,a}) &= \mathrm{Tr}\rho^{\otimes n}(I_n - S_{n,a})\\ &= \sum_{x^n\in\mathcal{X}^n} P^n(x^n)\mathrm{Tr}W_{x^n}^{(n)}\{W_{x^n}^{(n)} - e^{na}W_P^{\otimes n} \le 0\},\end{aligned} \tag{8.88}$$

$$\begin{aligned}\beta_n(S_{n,a}) &= \mathrm{Tr}\sigma^{\otimes n}S_{n,a}\\ &= \sum_{x^n\in\mathcal{X}^n} P^n(x^n)\mathrm{Tr}W_P^{\otimes n}\{W_{x^n}^{(n)} - e^{na}W_P^{\otimes n} > 0\}.\end{aligned} \tag{8.89}$$

Consequently, (8.83) is written by using the error probabilities of quantum hypothesis testing as

$$P_e(\Phi_n) \le 2\alpha_n(S_{n,a}) + 4M_n\beta_n(S_{n,a}). \tag{8.90}$$

Here note that, from (6.65), the quantum relative entropy between ρ and σ is nothing but the Holevo mutual information $I(P;W)$. Let P be the probability distribution that attains $\max_P I(P;W)$. For any $R < I(P;W)$, we can take a real number a satisfying $R < a < I(P;W)$. It follows from Theorem 8.3 and Lemma 8.28 that

$$\lim_{n\to\infty}\alpha_n(S_{n,a}) = 0, \quad \beta_n(S_{n,a}) \le e^{-na}. \tag{8.91}$$

From (8.90), there exists a code Φ_n with $M_n = e^{nR}$ messages such that

$$\begin{aligned}P_e(\Phi_n) &\le 2\alpha_n(S_{n,a}) + 4M_n\beta_n(S_{n,a})\\ &\le 2\alpha_n(S_{n,a}) + 4e^{nR}\cdot e^{-na} \xrightarrow{(n\to\infty)} 0.\end{aligned} \tag{8.92}$$

Thus we have shown that, if $R < \max_P I(P;W)$, there exists a sequence of codes $\Phi_n = (\phi^{(n)}, X^{(n)})$ satisfying

$$\lim_{n\to\infty} P_e(\Phi_n) = 0, \quad \liminf_{n\to\infty}\frac{1}{n}\log|\Phi_n| \ge R. \tag{8.93}$$

From the definition of the classical-quantum channel capacity (8.49), we have

$$C \ge \sup\{R \mid R < \max_P I(P;W)\} = \max_P I(P;W), \tag{8.94}$$

which asserts the theorem. □

Exercise 8.4 The evaluation of the average error probability can be changed into that of the maximum error probability by discarding some bad codewords with a certain ratio (expergation technique). Suppose that a message $i = 1, 2, \dots, M$ arises with probability $P(i)$, and each message has an error probability $e_i \ge 0$. Let us rearrange the messages in ascending order of the error probability $e_i \ge 0$, and discard the bad part of the messages with the ratio $0 \le t \le 1$. That is, the set of the messages can be divided into $G = \{1, \ldots, (1-t)M\}$ and $B = \{(1-t)M + 1, \ldots, M\}$, and B is discarded. Let $m = \max_{i \in G} e_i$ be the maximum error of the remaining part (good part). Show that, if the average error probability satisfies $\sum_{i=1}^{M} P(i)e_i \le \epsilon$, then $m \le \frac{\epsilon}{P(B)}$ holds for the maximum error probability. Especially the probability $P(i)$ is uniform for $i = 1, 2, \ldots, M$, we have $m \lesssim \frac{\epsilon}{t}$.

Exercise 8.5 Show the following properties for the Holevo mutual information.

(1) $I(P; W)$ has **concavity** with respect to P for any fixed W.
(2) $I(P; W)$ has **convexity** with respect to W for any fixed P.

Exercise 8.6 Show the following properties for the Holevo mutual information.

(1) For any density operator τ, we have $I(P; W) \le \sum_x P(x)D(W_x||\tau)$.
(2) $I(P; W) = \min_{\tau \in \mathcal{S}(\mathcal{H})} \sum_x P(x)D(W_x||\tau)$.

Exercise 8.7 If the function of two variables $f(x, y)$ has **concavity** with respect to x for any fixed y and has **convexity** with respect to y for any fixed x, then $\max_x \min_y f(x, y) = \min_y \max_x f(x, y)$ holds [23]. Applying this fact to $f(P, \tau) = \sum_x P(x)D(W_x||\tau)$, show the min-max representation of the classical-quantum channel capacity.

$$\max_{P \in \mathcal{P}(\mathcal{X})} I(P; W) = \min_{\tau \in \mathcal{S}(\mathcal{H})} \max_{x \in \mathcal{X}} D(W_x||\tau). \tag{8.95}$$

References

1. A.S. Holevo, Probl. Inform. Transm. **9**, 177–183 (1973)
2. A.S. Holevo, Probl. Inform. Transm. **15**, 247–253 (1979)
3. A.S. Holevo, IEEE Trans. Inform. Theory, **44**, 269–273 (1998), quant-ph/9611023 (1996)
4. B. Schumacher, M.D. Westmoreland, Phys. Rev. A **56**, 131–138 (1997)
5. P.W. Shor, Phys. Rev. A **52**, R2493–R2496 (1995)
6. A.M. Steane, Phys. Rev. Lett. **77**, 793–797 (1996)
7. F. Hiai, D. Petz, Commun. Math. Phys. **143**, 99–114 (1991)
8. T. Ogawa, H. Nagaoka, IEEE Trans. Inform. Theory **46**, 2428–2433 (2000)
9. K.M.R. Audenaert, J. Calsamiglia, Ll. Masanes, R. Munoz-Tapia, A. Acin, E. Bagan, F. Verstraete, Phys. Rev. Lett. **98**, 160501 (2007)
10. Y. Ogata, Lett. Math. Phys. **97**, 339–346 (2011)
11. V. Jaksic, Y. Ogata, C.-A. Pillet, R. Seiringer, Rev. Math. Phys. **24**, 130002 (2012)
12. D. Petz, *Quantum Information Theory and Quantum Statistics* (Springer, Berlin, 2008)
13. H. Nagaoka, M. Hayashi, IEEE Trans. Inform. Theory **53**, 534–549 (2007)
14. T.S. Han, *Information-Spectrum Methods in Information Theory* (Springer, Berlin, 2002) (Originally published in Japanese in 1998)
15. D. Petz, Rep. Math. Phys. **23**, 57–65 (1986)
16. A. Fujiwara, H. Nagaoka, IEEE Trans. Inform. Theory **44**, 1071–1086 (1998)
17. A. Winter, IEEE Trans. Inform. Theory **45**, 2481–2485 (1999)
18. T. Ogawa, H. Nagaoka, IEEE Trans. Inform. Theory **53**, 2261–2266 (2007)

19. M. Hayashi, H. Nagaoka, IEEE Trans. Inform. Theory **49**, 1753–1768 (2003)
20. M. Hayashi, *Quantum Information: An Introduction* (Springer, New York, 2006) (Originally published in Japanese in 2004)
21. C.E. Shannon, Bell Syst. Tech. J. **27**(379–423), 623–656 (1948)
22. T. Cover, J. Thomas, *Elem. Inf. Theory* (Wiley, New York, 1991)
23. R.T. Rockafellar, *Convex Analysis* (Princeton University Press, Princeton, 1970)

Chapter 9
Quantum Error Correction and Quantum Cryptography

9.1 Introduction

When we send a quantum state via a quantum channel, it is usual that the state is demolished due to the noise. Quantum error correction is a method to keep the quantum state from the effect by the noise. In quantum error correction, we transform the n-qubit quantum system to another quantum system with a larger dimension, which has a redundancy. Utilizing the redundancy, quantum error correction enables us to transmit the quantum state precisely by decreasing the effect by the noise. As the most typical method, we consider the method that uses the three-qubit system for transmitting the one-qubit system [1], in which, we transform a one-qubit state $a|0\rangle + b|1\rangle$ to a three-qubit state $a|000\rangle + b|111\rangle$, which is transmitted via the given quantum channel.

In this case, when the error occurs in only one qubit system, the error can be corrected as follows. First, we define the projection P_0 to the subspace spanned by $|000\rangle, |111\rangle$ corresponding to the no-error event, the projection P_1 to the subspace spanned by $|100\rangle, |011\rangle$ corresponding to the event of the error occurring in the first qubit, the projection P_2 to the subspace spanned by $|010\rangle, |101\rangle$ corresponding to the event of the error occurring in the second qubit, and the projection P_3 to the subspace spanned by $|001\rangle, |001\rangle$ corresponding to the event of the error occurring in the third qubit, Then, we apply the measurement corresponding to the instrument $\{P_i\}_{i=0}^3$. When the outcome i is not 0, the error can be corrected by flipping the ith basis $|0\rangle$ and $|1\rangle$ if the number of errors is less than one. However, the error might occur in more than two qubits. The above method does not necessarily work well against a general noise, which is written by a general TP-CP map.

In the following, we treat quantum error correction for the case when the state reduction by the noise in the quantum communication is given as a quantum channel, which is mathematically written by a TP-CP map. The sender transforms a quantum state in the original quantum system to be sent (the message system), to a quantum state in the input system of the given quantum channel. This process is called the encoding, and the device to encode or the map is called the encoder. On the other

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1_9,

hand, the receiver transforms the received quantum state in the output system of the given quantum channel, to a state in the message system. This process is called the decoding, and the device to decode or the map is called the decoder. In quantum error correction, the pair of the encoder and the decoder is called a code. We often restrict our encoder to the isometry into a larger system, in which, the message system can be identified with the subspace of the input system of the quantum channel. In the remaining part of this chapter, we summarize the fundamental knowledge of error correction of the classical system. Then, we discuss quantum error correction. Finally, we treat quantum cryptography as an application of quantum error correction.

9.2 Algebraic Error Correction in the Classical System

9.2.1 Formulation

We first treat the problem to transmit a bit sequence $X^n = (X_1, \ldots, X_n)$ taking values in $\{0, 1\}$ via a classical communication channel. In the following, for an algebraic treatment, we treat a bit consisting of $\{0, 1\}$ as the finite field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, in which, the addition is defined by Fig. 3.1 and the multiplication is defined by Table 3.1. Then, an n-bit sequence can be treated as an element of the vector space $\mathbb{F}_2^n$ over the finite field $\mathbb{F}_2$, whose detail is explained in Appendix A.7. Hence, we can define the sum $X^n + Y^n := (X_1 \oplus Y_1, \ldots, X_n \oplus Y_n)$ for arbitrary two elements $X^n, Y^n \in \mathbb{F}_2^n$.[1]

In the following, we treat the case when the noise is symmetric. That is, the noise $Y^n = (Y_1, \ldots, Y_n)$ in the channel occurs with the probability $P^{(n)}(Y^n)$, and the signal $X'^n := X^n + Y^n$ is received at the output system.[2] In order to recover the original message in the presence of the noise, we apply error correction, which is given as a combination of the encoder and the decoder. The sender transforms the original message to the input bit sequence, and the device or the process is called the **encoder**. The encoder is constructed as a one-to-one map so that there is no duplication among original messages corresponding to the input bit sequence. The receiver transforms the received bit sequence to the original message, and the device or the process is called the **decoder**. The pair of the encoder and the decoder is called the **code**.

When the set of messages to be sent is $\{1, \ldots, M\}$, generally, the encoder is described as a map ϕ from $\{1, \ldots, M\}$ to $\mathbb{F}_2^n$, and the decoder is described as a map ψ from $\mathbb{F}_2^n$ to $\{1, \ldots, M\}$. However, when we construct a code by the algebraic method, we can identify the encoder with the range of the encoder ϕ, which is a subset

[1] The sum in the vector space is written as $+$, and the sum in the finite field $\mathbb{F}_2$ is written as $\oplus$. Since the sum $+$ has the same meaning as the difference $-$ in a vector space over the finite field $\mathbb{F}_2$, we unify them to $+$.

[2] In the general noise, the probability flipping 0 to 1 dose not coincide with that the probability flipping 1 to 0. In the following, we assume that these two kinds of flipping probabilities are the same. Then, the above type description is possible.

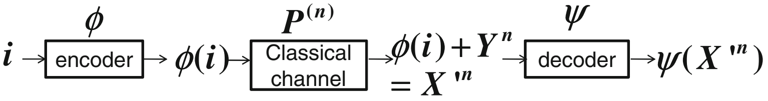


Fig. 9.1 Error correction in the classical channel

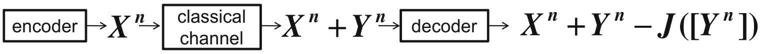


Fig. 9.2 Error correction with the algebraic structure in the classical channel

of $\mathbb{F}_2^n$, and we often define the encoder as a subset of $\mathbb{F}_2^n$. In our case, as is shown in Fig. 9.1, the message i is transformed to $\phi(i)$ and is changed to $X'^n = \phi(i) + Y^n$ by the addition with the noise Y^n. When the recovered message $\psi(X'^n)$ is different from i, the error correction is not successful. That is, the error correction is not successful if and only if $Y^n = X'^n + \phi(i)$ with $\psi(X'^n) \neq i$.

Since the noise Y^n obeys the distribution $P^{(n)}$, the (decoding) error probability is given as $\sum_{X'^n \in \mathbb{F}_2^n : \psi(X'^n) \neq i} P^{(n)}(X'^n + \phi(i))$ when the original messgae is i. Hence, the **average error probability** is given as

$$P_e(\phi, \psi) := \sum_{i=1}^{M} \frac{1}{M} \sum_{X'^n \in \mathbb{F}_2^n : \psi(X'^n) \neq i} P^{(n)}(X'^n + \phi(i))$$
$$= 1 - \sum_{i=1}^{M} \frac{1}{M} \sum_{X'^n \in \mathbb{F}_2^n : \psi(X'^n) = i} P^{(n)}(X'^n + \phi(i)).$$

The performance of the code is characterized with the pair of the size M of the message and the average error probability $P_e(\phi, \psi)$. The larger size M guarantees that we can send more information, and the smaller average error probability $P_e(\phi, \psi)$ does that we can send information more precisely. As the most popular decoder, we introduce the **maximum likelihood decoder** ψ_{ML}, which is given by $\psi_{\mathrm{ML}}(X'^n) := \operatorname{argmax}_i P^{(n)}(X'^n + \phi(i))$. The maximum likelihood decoder minimizes the above average error probability $P_e(\phi, \psi)$ with a given ϕ. Hence, we can evaluate the optimal performance of the encoder ϕ by the average error probability with the maximum likelihood decoder. When the number n of transmitted bits is larger, a larger size M of message can be transmitted. In this case, we focus on the **transmission rate** $\log M/n$.

Generally, a larger number n is required for a code whose transmission rate is large and whose average error probability is small. However, the calculation amounts of the encoder and the decoder are larger if a larger number n of transmitted bits is larger. It is hard to realize the above pair of the encoder and the decoder.

In order to reduce the complexity , we choose the image of ϕ (the codebook) as a vector subspace C of $\mathbb{F}_2^n$ according to Fig. 9.2. In this case, we call C the **code**

space. Then, the message set is given as a vector space $\mathbb{F}_2^k$ with the size 2^k. When the code space C is a k-dimensional vector space over the finite field $\mathbb{F}_2$, for reducing the complexity, the encoder ϕ is restricted to a one-to-one linear map over the finite field $\mathbb{F}_2$ from $\mathbb{F}_2^k$ to C, which is represented by an n-row k-column matrix called the **generating matrix** of the code space C. The linear map can be determined by k basis vectors of C. Hence, the generation matrix can be given by arranging k basis vectors of C. However, since the choice of k basis vectors is not unique for C, the generating matrix is not unique for the code space C.

In this construction, the error probability with the maximum likelihood decoder does not depend on the message. It is also independent of the choice of the map ϕ and depends only on the vector subspace C as long as the map ϕ is a one-to-one map. In the following, we assume that the encoder is linear map and is give by the generating matrix G. To see the structure of a decoder, we focus on an $n-k$-row n-column matrix H satisfying $HG = 0$, which is called a **parity check matrix** of the code C. A parity check matrix is not also unique for the code space C. When the received bit sequence $X'^n \in \mathbb{F}_2^n$ does not belong to C, we guess that the bit sequence is changed due to the noise Y^n. If we correctly identify the noise Y^n, we can recover the original message correctly. Since the original input bit sequence belongs to the kernel $\operatorname{Ker} H = H^{-1}(0) = C$, the occurring noise Y^n belongs to $H^{-1}(HX'^n) = H^{-1}(HY^n)$.

Hence, given the image of the parity check matrix HX'^n, we can decide the decoder ψ by choosing the bit sequence $J(HX'^n) \in H^{-1}(HX'^n) \subset \mathbb{F}_2^n$ that has the largest occurring probability. That is, the received bit sequence X'^n is decoded to $X'^n + J(HX'^n) \in C$. If and only if the decoded message coincides with the original message, the occurring noise Y^n belongs to the subset $\{J(Z)\}_{Z\in\mathbb{F}_2^{n-k}}$. Thus, the correctly decoding probability is given as $\sum_{Z\in\mathbb{F}_2^{n-k}} P^{(n)}(J(Z))$, and does not depend on the original message. That is, the error probability is given as $1 - \sum_{Z\in\mathbb{F}_2^{n-k}} P^{(n)}(J(Z))$. In particular, when $J(Z)$ is given as $\operatorname{argmax}_{X^n\in H^{-1}(Z)} P^{(n)}(X^n)$, it is written by $J_{\mathrm{ML}}(Z)$ because it gives the maximum likelihood decoder. In the following, we use the subspace C of $\mathbb{F}_2^n$ as the encoder, and denote the error probability with the maximum likelihood decoder by $\delta_{P^{(n)}}[C]$. When there is no possibility for confusion, we abbreviate the probability distribution $P^{(n)}$ for the noise. Since the error probability does not depend on the element $X^n \in C$, $\delta[C]$ coincides with the average error probability with the maximum likelihood decoder.

One may consider that the construction of the decoder depends on the choice of the parity check matrix H. Mathematically, the above discussion can be made without use of the parity check matrix H as follows. For this purpose, we employ the **quotient space** $\mathbb{F}_2^n/C$, which is given as the quotient of $\mathbb{F}_2^n$ by C. (For the detail, see Appendix A.7.) We denote the element of the quotient space $\mathbb{F}_2^n/C$ whose representative element is $X^n \in \mathbb{F}_2^n$ by $[X^n]$. Since the input bit sequence belongs to the subspace C of $\mathbb{F}_2^n$, the occurring noise Y^n belongs to $[X'^n]$ (See Exercise A.29.).

Hence, given an element of the quotient space $[X'^n] \in \mathbb{F}_2^n/C$, we can decide the decoder ψ by choosing the bit sequence $J([X'^n]) \in [X'^n] \subset \mathbb{F}_2^n$ that have the largest occurring probability. In this discussion, when $[X'^n]$ is regarded as an element of the quotient space $\mathbb{F}_2^n/C$, it corresponds to HX'^n. When $[X'^n]$ is regarded as a subset of $\mathbb{F}_2^n$, it corresponds to $H^{-1}(HX'^n)$. In particular, [0] does to the kernel Ker $H = H^{-1}(0)$. Using this correspondence, the above discussion can be reconstructed by use of the terminology of the quotient space instead of a parity check matrix. In the following, we discuss the decoder by using the quotient space.

Example 9.1 (**three-bit code**) In the case of $n = 3$, we can consider a typical code $C_{(3)} = \{(0,0,0)^T, (1,1,1)^T\}$, which is given by the generation matrix $(1,1,1)^T$. The vector space $\mathbb{F}_2^3$ can be divided to the union of elements of quotient space as $\{(0,0,0)^T, (1,1,1)^T\} \cup \{(1,0,0)^T, (0,1,1)^T\} \cup \{(0,1,0)^T, (1,0,1)^T\} \cup \{(0,0,1)^T, (1,1,0)^T\}$. The representative elements of the respective subsets can be given as $(0,0,0)^T$, $(1,0,0)^T$, $(0,1,0)^T$, $(0,0,1)^T$. Hence, $\mathbb{F}_2^3/C_{(3)}$ can be characterized as $\{[(0,0,0)^T], [(1,0,0)^T], [(0,1,0)^T], [(0,0,1)^T]\}$.

In the code, the original message is encoded to $(0,0,0)^T$ or $(1,1,1)^T$. Then, when the receiver receives $(0,0,0)^T$, $(1,0,0)^T$, $(0,1,0)^T$, or $(0,0,1)^T$, the receiver decides that only the error occurs only in one bit, and decodes it to $(0,0,0)^T$. Similarly, when the receiver receives $(1,1,1)^T$, $(1,1,0)^T$, $(0,1,1)^T$, or $(1,0,1)^T$, it is natural to decode it to $(1,1,1)^T$. The decoder is described by the map J defined in the following way:

$$J(\{(0,0,0)^T, (1,1,1)^T\}) = (0,0,0)^T,\ J(\{(1,0,0)^T, (0,1,1)^T\}) = (1,0,0)^T,$$
$$J(\{(0,1,0)^T, (1,0,1)^T\}) = (0,1,0)^T,\ J(\{(0,0,1)^T, (1,1,0)^T\}) = (0,0,1)^T. \tag{9.1}$$

Exercise 9.1 In the three-bit code, we assume that the noise $Y^3 \in \mathbb{F}_2^3$ obeys the 3-trial independent and identical distribution of the probability distribution $P = (1-p, p)$ over $\mathbb{F}_2$. Give the map $J_{\rm ML}$ corresponding to the maximum likelihood decoder.

When the noise $Y^n \in \mathbb{F}_2^n$ obeys the n-trial independent and identical distribution P^n of the probability distribution $P = (1-p, p)$ over $\mathbb{F}_2$ for $p \in (0, 1/2)$, the map $J_{\rm ML}$ corresponding to the maximum likelihood decoder can be defined as the choice of the bit sequence with the minimum number of 1 among the equivalent class $[X^n]$. Such a decoder is called the **minimum distance decoder**.

Exercise 9.2 Under the three-bit code, we assume that the noise $Y^3 \in \mathbb{F}_2^3$ obeys the 3-trial independent and identical distribution of the probability distribution $P = (1-p, p)$ over $\mathbb{F}_2$. Calculate the correctly decoding probability with the maximum likelihood decoder when $0 < p < 1/2$.

Example 9.2 (**Hamming code**) We consider the code space $C_{G,1} \subset \mathbb{F}_2^7$ defined by the following generating matrix:

$$G_1 := \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \\ 0\,1\,1\,1 \end{pmatrix}. \tag{9.2}$$

Then, the element of $C_{G,1}$ whose first, second, third, and fourth entries are zero is limited to $(0, 0, 0, 0, 0, 0, 0)^T$. Hence, in order to give representative elements of the three-dimensional space $\mathbb{F}_2^7/C_{G,1}$, we can choose them among bit sequences whose first, second, third, and fourth entries are zero. That is, all of elements of $\mathbb{F}_2^7/C_{G,1}$ are given as $[(0, 0, 0, 0, 0, 0, 0)^T]$, $[(0, 0, 0, 0, 1, 0, 0)^T]$, $[(0, 0, 0, 0, 0, 1, 0)^T]$, $[(0, 0, 0, 0, 1, 1, 0)^T]$, $[(0, 0, 0, 0, 0, 0, 1)^T]$, $[(0, 0, 0, 0, 1, 0, 1)^T]$, $[(0, 0, 0, 0, 0, 1, 1)^T]$, $[(0, 0, 0, 0, 1, 1, 1)^T]$.

Exercise 9.3 Give the minimum distance decoder for the above Hamming code $C_{G,1}$ with 7 bits. Further, show that the original message can be recovered whatever error occurs among one-bit errors if the minimum distance decoder is applied.

Exercise 9.4 Under the above Hamming code $C_{G,1}$ with 7 bits, we assume that the noise $Y^7 \in \mathbb{F}_2^7$ obeys the 7-trial independent and identical distribution of the probability distribution $P = (1 - p, p)$ over $\mathbb{F}_2$. Calculate the correctly decoding probability with the maximum likelihood decoder when $0 < p < 1/2$.

9.2.2 Evaluation of Error Probability Under Code Ensemble

As is mentioned in the above section, since the maximum likelihood decoder can realize the minimum error, the optimal performance of the code space C can be characterized by the minimum average error probability $\delta[C]$ with the maximum likelihood decoder. However, it is not so easy to evaluate the average error probability $\delta[C]$. In particular, when n is larger, the evaluation is more difficult. In order to resolve the problem, Shannon [2, 3] introduced the idea of **random coding**. In this method, we give up to evaluate the respective average error probability $\delta[C]$ for a given code C, and focus on the ensemble of codes and the expectation value of the average error probability $\delta[C]$ with respect to the ensemble of codes. One might consider that the evaluation of the expectation of $\delta[C]$ is more difficult than that of $\delta[C]$ for a specific code C. However, a probabilistic method enables us to evaluate the expectation. Since the original ensemble by Shannon is not an ensemble of code spaces, we treat an ensemble different from his original ensemble. In particular, we treat not a specific code ensemble but a code ensemble satisfying a certain condition. The code ensemble satisfying the condition is closely related to privacy amplification in the quantum cryptography, and plays an important role in the applied viewpoint.

In order to give the condition for the code ensemble, we choose the code space $C \subset \mathbb{F}_2^n$ according to a random variable Z. That is, we denote the code space C_Z determined by the random variable Z. When the code ensemble $\{C_Z\}_Z$ satisfies the following condition, we call it ϵ-**universal2** [4–6].

$$\Pr\{X^n \in C_Z\} \le \epsilon, \quad \forall X^n \neq 0 \in \mathbb{F}_2^n. \tag{9.3}$$

The condition for the code ensemble means that the code space C_Z is distributed almost uniformly in a sense, i.e., there is less bias for the choice of elements of C_Z except for the origin 0. In particular, a 2^{k-n}-universal2 code ensemble plays an important role among k-dimensional code spaces, and the example will be concretely given in Sect. 9.2.3. Then, we obtain the following theorem [6, 7].

Theorem 9.1 *An ϵ-universal2 code ensemble C_Z satisfies the inequality*

$$\mathrm{E}_Z \delta[C_Z] \le \min_{0 \le s \le 1} \epsilon^s 2^{\phi(s:P^{(n)})}, \tag{9.4}$$

where E_Z is the expectation with respect to the random variable Z and $\phi(s : P^{(n)}) := \log(\sum_{X^n \in \mathbb{F}_2^n} (P^{(n)}(X^n))^{\frac{1}{1+s}})^{1+s}$.

For the proof, we prepare the following lemma.

Lemma 9.1 (Gallager [7]) *Given a code space C, the error probability $\delta[C]$ with the maximum likelihood decoder can be evaluated as follows with arbitrary real numbers $s, t > 0$:*

$$\delta[C] \le \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{1-st} \left(\sum_{X'^n \in C \setminus \{0\}} P^{(n)}(X^n + X'^n)^t \right)^s. \tag{9.5}$$

Proof of Lemma 9.1 When the code space C and the maximum likelihood decoder are used, the error probability is given as $\delta[C] = \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n) \Delta_{\mathrm{ML}}(X^n)$, where the indicator function $\Delta_{\mathrm{ML}}(X^n)$ is given as

$$\Delta_{\mathrm{ML}}(X^n) := \begin{cases} 0 \text{ if } P^{(n)}(X^n) > P^{(n)}(X^n + X'^n), \quad \forall X'^n \in C \setminus \{0\} \\ 1 \text{ otherwise.} \end{cases}$$

Using

$$\Delta_{X'^n}(X^n) := \begin{cases} 0 \text{ if } P^{(n)}(X^n) > P^{(n)}(X^n + X'^n), \\ 1 \text{ otherwise,} \end{cases}$$

we can evaluate the indicator function $\Delta_{\mathrm{ML}}(X^n)$ as follows.

$$\Delta_{\mathrm{ML}}(X^n) \le \sum_{X'^n \in C\setminus\{0\}} \Delta_{X'^n}(X^n). \tag{9.6}$$

Then, taking the sth power in the both sides of (9.6) for $s > 0$, we obtain $\Delta_{\mathrm{ML}}(X^n) \le \left(\sum_{X'^n \in C\setminus\{0\}} \Delta_{X'^n}(X^n)\right)^s$, which implies that

$$\Delta_{X'^n}(X^n) \le \frac{P^{(n)}(X^n + X'^n)}{P^{(n)}(X^n)}. \tag{9.7}$$

Similarly, taking tth power in the both sides of (9.7) for $t > 0$, we obtain $\Delta_{X'^n}(X^n) = \Delta_{X'^n}(X^n)^t \le \frac{P^{(n)}(X^n+X'^n)^t}{P^{(n)}(X^n)^t}$. Summarizing the above inequalities, we have

$$\Delta_{\mathrm{ML}}(X^n) \le \left(\sum_{X'^n \in C\setminus\{0\}} \frac{P^{(n)}(X^n + X'^n)^t}{P^{(n)}(X^n)^t}\right)^s. \tag{9.8}$$

Hence, the error probability can be evaluated as

$$\begin{aligned}
\delta[C] &\le \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n) \left(\sum_{X'^n \in C\setminus\{0\}} \frac{P^{(n)}(X^n + X'^n)^t}{P^{(n)}(X^n)^t}\right)^s \\
&= \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{1-st} \left(\sum_{X'^n \in C\setminus\{0\}} P^{(n)}(X^n + X'^n)^t\right)^s.
\end{aligned} \tag{9.9}$$

□

Proof of Theorem 9.1 Substituting $t = \frac{1}{1+s}$ into (9.5) for $0 \le s \le 1$, we have

$$\delta[C_Z] \le \sum_{X^n \in \mathbb{F}_2^n} (P^{(n)}(X^n))^{\frac{1}{1+s}} \left(\sum_{X'^n \in C_Z\setminus\{0\}} (P^{(n)}(X^n + X'^n))^{\frac{1}{1+s}}\right)^s.$$

Then, taking the expectation with respect to the random variable Z and applying Jensen inequality (A.13) to the concave function $x \mapsto x^s$ and the random variable $\left(\sum_{X'^n \in C_Z\setminus\{0\}} P^{(n)}(X^n + X'^n)^{\frac{1}{1+s}}\right)$, we obtain

$$\begin{aligned}
\mathrm{E}_Z \delta[C_Z] \le& \mathrm{E}_Z \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{\frac{1}{1+s}} \left(\sum_{X'^n \in C_Z\setminus\{0\}} P^{(n)}(X^n + X'^n)^{\frac{1}{1+s}}\right)^s \\
\le& \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{\frac{1}{1+s}} \left(\mathrm{E}_Z \sum_{X'^n \in C_Z\setminus\{0\}} P^{(n)}(X^n + X'^n)^{\frac{1}{1+s}}\right)^s
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{\frac{1}{1+s}} \left(\sum_{X'^n \mathbb{F}_2^n \setminus \{0\}} \Pr\{X'^n \in C_Z\} P^{(n)}(X^n + X'^n)^{\frac{1}{1+s}} \right)^s \\
&\le \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{\frac{1}{1+s}} \left(\epsilon \sum_{X'^n \in \mathbb{F}_2^n} P^{(n)}(X^n + X'^n)^{\frac{1}{1+s}} \right)^s , \qquad (9.10)
\end{aligned}
$$

where the final inequality follows from the condition of ϵ-universal2 (9.3). Since $\left(\epsilon \sum_{X'^n \in \mathbb{F}_2^n} P^{(n)}(X^n + X'^n)^{\frac{1}{1+s}}\right)^s$ does not depend on X^n, the above value coincides with $\left(\epsilon \sum_{X'^n \in \mathbb{F}_2^n} P^{(n)}(X'^n)^{\frac{1}{1+s}}\right)^s = \epsilon^s \left(\sum_{X'^n \in \mathbb{F}_2^n} P^{(n)}(X'^n)^{\frac{1}{1+s}}\right)^s$. Hence, the right hand side of (9.10) equals the following value.

$$
\begin{aligned}
\sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{\frac{1}{1+s}} \epsilon^s \left(\sum_{X'^n \in \mathbb{F}_2^n} P^{(n)}(X'^n)^{\frac{1}{1+s}} \right)^s &= \epsilon^s \left(\sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{\frac{1}{1+s}} \right)^{1+s} \\
&= \epsilon^s 2^{\phi(s:P^{(n)})}. \qquad (9.11)
\end{aligned}
$$

□

9.2.3 Examples of Code Ensemble

In the following, we give concrete examples for an ϵ-universal2 code ensemble of k-dimensional subspaces of $\mathbb{F}_2^n$ when $\epsilon = 2^{k-n}$. Since a code space is determined by a generating matrix, we construct a code ensemble by constructing an ensemble of generating matrices.

Lemma 9.2 *Let B_Z be the $(n-k) \times k$ matrix whose $(n-k)k$ entries are independent uniform random variables taking values in $\mathbb{F}_2$. We choose the code space C_Z generated by the generating matrix $\begin{pmatrix} I \\ B_Z \end{pmatrix}$. Then, the code ensemble C_Z is 2^{k-n}-universal2.*

Proof of Lemma 9.2 In the following, we give a proof for a fixed $X^n := (X_1, \ldots, X_n) \neq 0 \in \mathbb{F}_2^n$. the probability that X^n belongs to the code space C_Z is 0. We also assume that (l, j)th entry of the matrix B_Z is given as $Z_{l,j}$. Hence, the bit sequence X^n belongs to the code space C_Z if and only if there exists a bit sequence $(Y_1, \ldots, Y_k)$ such that [3]

$$
X_t = Y_t, \quad X_{k+l} = \bigoplus_{j=1}^{k} Z_{l,j} \wedge Y_j, \quad l = 1, \ldots, n-k, \quad t = 1, \ldots, k,
$$

[3] $\wedge$ is the multiplication over the finite field $\mathbb{F}_2$, and is given in Table 3.1.

which is equivalent with

$$X_{k+l} = \bigoplus_{j=1}^{k} Z_{l,j} \wedge X_j, \quad l = 1, \ldots, n-k. \tag{9.12}$$

When the initial k entries of X^n are zero, the random variable X_{k+l} is independent of the random variable $X_{k+l'}$ with $l \neq l'$, and takes 0 and 1 with the probability $1/2$. Therefore, all of the above conditions for l hold with the probability $1/2^{n-k}$. □

The above construction requires $(n-k)k$ independent uniform random variables. However, the number can be reduced at least up to $n-1$ [8].

Lemma 9.3 *Let $Z = (Z_1, \ldots, Z_{n-1})$ be $n-1$ independent uniform random variables over $\mathbb{F}_2$. We define the $(n-k) \times k$ Toeplitz matrix A_Z by $(A_Z)_{l,j} := Z_{n-k-l+j}$, and the code space C_Z as the code generated by the generating matrix $\begin{pmatrix} I \\ A_Z \end{pmatrix}$. Then, the code ensemble C_Z is 2^{k-n}-universal2.*

Proof of Lemma 9.3 When the initial k entries of $X^n := (X_1, \ldots, X_n) \neq 0 \in \mathbb{F}_2^n$ are zero, the probability that X^n belongs to the code space C_Z is 0.

Hence, in the following, we consider the case when the initial k entries of X^n contain 1. Similar to Lemma 9.2, we treat Condition (9.12), but we need a modified treatment. For this purpose, we pick up bits whose value is 1 from k bits $X_1, \ldots, X_k$, and denote the bit with the largest index by X_t. Since $X_t = 1$, X^n belongs to the code space C_Z if and only if

$$\begin{aligned} X_{k+l} &= (\bigoplus_{j=1}^{k} (Z_{n-k-l+j} \wedge X_j)) \\ &= (\bigoplus_{j=1}^{t-1} (Z_{n-k-l+j} \wedge X_j)) \oplus Z_{n-k-l+t}, \quad l = 1, \ldots, n-k \end{aligned} \tag{9.13}$$

because $X_t = 0$ and $X_j = 0$ for $j > t$.

Now, we focus on Condition (9.13) with $l = n-k$. Since Z_t is independent of $Z_{t-1}, \ldots, Z_1$ and Z_t takes the value 0 and 1 with the equal probability, the condition holds with probability $1/2$. Next, we focus on Condition (9.13) with $l = u$ when Condition (9.13) holds with $l = u+1, \ldots, n-k$. Since $Z_{n-k-u+t}$ is independent of $Z_{n-k-u+t-1}, \ldots, Z_1$ and $Z_{n-k-u+t}$ takes the value 0 and 1 with the equal probability, the condition holds with probability $1/2$. Hence, Condition (9.13) holds with probability $1/2^{n-k}$. □

9.2.4 Asymptotic Theory

Up to now, we have treated the classical communication channel over the vector space $\mathbb{F}_2^n$ when the noise obeys a general probability distribution on $P^{(n)}$ over the vector space $\mathbb{F}_2^n$. In the following, we will treat the case when the probability distribution $P^{(n)}$ is the independent and identical distribution of the probability distribution $P = (1-p, p)$ on the finite field $\mathbb{F}_2$. Then, we have

$$\phi(s : P^n) = n\phi(s : P) = n(1+s)\log((1-p)^{\frac{1}{1+s}} + p^{\frac{1}{1+s}}). \tag{9.14}$$

In particular, the analysis of the above case with infinitely large n is called the asymptotic theory. For the analysis, we treat a code space C_n as a subspace of $\mathbb{F}_2^n$ for respective n, and focus on the sequence $\{C_n\}$. Then, we discuss the limit $\lim_{n\to\infty} \delta[C_n]$ of the error probability with the maximum likelihood decoder and the transmission rate $\lim_{n\to\infty} \frac{1}{n} \log |C_n|$. The entropy (Shannon entropy) plays an important role in the asymptotic theory, and is characterized as

$$H(P) = \lim_{s\to 0} \frac{\phi(s : P)}{s}. \tag{9.15}$$

Although we choose the codebook as a subspace of $\mathbb{F}_2^n$, when we choose the codebook as a subset of $\mathbb{F}_2^n$, the following theorem is known as Shannon's channel coding theorem.

Theorem 9.2 ([2, 3]) *For a sequence of codes whose nth codebook is chosen as a subset of $\mathbb{F}_2^n$, we impose the condition that the error probability of the code goes to zero. The maximum transmission rate under the condition is $1 - H(P)$.*

Next, we choose R satisfying

$$R > H(P), \tag{9.16}$$

and choose an integer k for n satisfying $k = \lfloor (1-R)n \rfloor$. Then, we apply Theorem 9.1 to the 2^{k-n}-universal2 code ensemble given in Lemma 9.3. Since the left hand side of (9.4) is the expectation of error probability with respect to the code ensemble, there exists a code space whose error probability with the maximum likelihood decoder is less than the right hand side of (9.4).

In the following, we treat a sequence of code spaces given in the above. The transmission rate of the above sequence of codes is $1 - R$, Relation (9.14) implies that the right hand side of (9.4) is $2^{-n \max_{0\le s\le 1}(sR-\phi(s:P))}$. Since Relation (9.15) holds, due to Condition (9.16), the relation $R > \frac{\phi(s:P)}{s}$ holds with a sufficiently small $s > 0$. Hence, we have $\max_{0\le s\le 1} sR - \phi(s : P) > 0$, which implies that the right hand side of (9.4) goes to zero exponentially for n. Thus, there exists a sequence of codes such that the error probability goes to zero and the transmission rate is close to $1 - H(P)$. Due to Theorem 9.2, the sequence of codes given here attains the asymptotically optimal transmission rate.

9.2.5 Error Correction with Confidentiality

If the transmitted information is partially leaked to the the eavesdropper, we need an additional art to disable the eavesdropper to obtain any meaningful information from the leaked information. For this purpose, we choose a space C in $\mathbb{F}_2^n$ and a subspace N of C, and consider the following coding method; the message to be sent is represented to not an element of C, but the element of the quotient space C/N [9].

The method to encode the message to the quotient space C/N is called **privacy amplification**. In the following, we denote the equivalent classes for the division by the subspaces N and C by $[X^n]_N$ and $[X^n]_C$, respectively. In this case, even when the received bit sequence is decoded to another element of the same equivalent class with respect to N as the original message, the decode is regarded as successful. Hence, when the noise Y^n obeys the distribution $P^{(n)}$, the correctly decoding probability with the decoder $\mathcal{J} := \{J([X^n]_C)\}_{[X^n]_C \in \mathbb{F}_2^n/C}$ is given as $P^{(n)}(\mathcal{J} + N) := \sum_{[X^n]_C \in \mathbb{F}_2^n/C, X''^n \in N} P^{(n)}(J([X^n]_C) + X''^n)$.

In particular, the probability that the message $[X^n]_N \in C/N$ is erroneously decoded to $[X^n]_N + [X'^n]_N \in C/N$ is given as $P^{(n)}\{\mathcal{J}, N\}([X'^n]_N) := P^{(n)}(\mathcal{J} + X'^n + N)$. In this case, if we replace $J([X^n]_C)$ by $J([X^n]_C) + X''^n$ with $X''^n \in N$, the finally decoded information is not changed, and then the error probability is not changed. The pair of subspaces $N \subset C$ given here is called a **code pair**. In particular, when the representative $J(x)$ of $x \in \mathbb{F}_2^n/C$ is given by $\operatorname{argmax}_{X^n \in x} \sum_{X''^n \in N} P^{(n)}(X^n + X''^n)$, it is called the **maximum likelihood decoder** for the code pair $N \subset C$ under the distribution $P^{(n)}$. The choice of the representatives yields the maximum correctly decoding probability, and we denote the error probability with the choice by $\delta_{P^{(n)}}$[C/N]. If there is no possibility for confusion, we abbreviate the probability distribution $P^{(n)}$.

Example 9.3 Consider the case with $C = \mathbb{F}_2^3$ and $N = C_{(3)}$. Even if the eavesdropper obtains any one-bit information from three-bit sequence $X \in \mathbb{F}_2^3$, the eavesdropper cannot obtain any information for $[X]_N \in \mathbb{F}_2^3/C_{(3)}$.

For example, assume that the eavesdropper knows only the first bit. If the first bit is 0, since the eavesdropper does not know the remaining two bits, the number of possible cases is 4. Then, in the respective one case, $[X]_N$ coincides with the respective element of $\mathbb{F}_2^3/C_{(3)} = \{[(0, 0, 0)^T], [(1, 0, 0)^T], [(0, 1, 0)^T], [(0, 0, 1)^T]\}$. Similarly, if the first bit is 1, in the respective one case, $[X]_N$ coincides with the respective element of $\mathbb{F}_2^3/C_{(3)} = \{[(0, 0, 0)^T], [(1, 0, 0)^T], [(0, 1, 0)^T], [(0, 0, 1)^T]\}$. Hence, even if the eavesdropper knows the first bit, the eavesdropper does not know what element of $\mathbb{F}_2^3/C_{(3)}$ equals $[X]_N$. The same fact can be shown for the case when the eavesdropper knows only the second bit or the third bit.

We consider the above kind of security in the general setting. For this purpose, we assume that X is the uniform random number on C and the eavesdropper knows only the i_1th bit, the i_2th bit, ..., the i_mth bit. Then, we denote the map from an n-bit sequence to an m-bit sequence of the i_1th bit, the i_2th bit, ..., and the i_mth bit, by $P^{i_1,i_2,\ldots,i_m}$. In this case, we can consider that the information $[X]_N$ is secure for the above eavesdropper when the random variable $P^{i_1,i_2,\ldots,i_m}(X)$ is independent of the random variable $[X]_N$. To discuss this issue, we define the matrix G'_N consists of the i_1th column, the i_2th column, ..., and the i_mth column of the generating matrix of the subspace N. Similarly, we define the matrix G'_C for the subspace C. Then, the security of the information $[X]_N$ is characterized as follows.

Lemma 9.4 *Under the above assumption, the random variable $P^{i_1,i_2,\ldots,i_m}(X)$ is independent of the random variable $[X]_N$ if and only if the image of G'_N is the same as the image of G'_C.*

Proof Firstly, we notice that the random variable $P^{i_1,i_2,\ldots,i_m}(X)$ is independent of the random variable $[X]_N$ if and only if the conditional probability distribution $P_{P^{i_1,i_2,\ldots,i_m}(X)|[X]_N=a}$ equals the probability distribution $P_{P^{i_1,i_2,\ldots,i_m}(X)}$ for any $a \in C/N$.

Assume that the image of G'_N is the same as the image of G'_C, and choose an element $b \in \operatorname{Ran} G'_C = \operatorname{Ran} G'_N$. Under the condition $[X']_N = [0]_N$, the number of cases of $P^{i_1,i_2,\ldots,i_m}(X') = b$ equals the cardinality of Ker $P^{i_1,i_2,\ldots,i_m}$, which does not depend on b. Then, under the condition $[X]_N = [x]_N$, X can be written as $X = X' + x$ with $X' \in N = [0]_N$. Since $P^{i_1,i_2,\ldots,i_m}(X) = P^{i_1,i_2,\ldots,i_m}(X') + P^{i_1,i_2,\ldots,i_m}(x)$, the number of cases of $P^{i_1,i_2,\ldots,i_m}(X) = b + P^{i_1,i_2,\ldots,i_m}(x)$ also does not depend on b under the condition $[X]_N = [x]_N$. Hence, the conditional probability distribution $P_{P^{i_1,i_2,\ldots,i_m}(X)|[X]_N}$ equals the probability distribution $P_{P^{i_1,i_2,\ldots,i_m}(X)}$.

Next, we assume that the conditional probability distribution $P_{P^{i_1,i_2,\ldots,i_m}(X)|[X]_N=a}$ equals the probability distribution $P_{P^{i_1,i_2,\ldots,i_m}(X)}$ for any $a \in C/N$. Since X is the uniform random number on C, $P_{P^{i_1,i_2,\ldots,i_m}(X)}(b) = \frac{1}{|\operatorname{Ran} G'_C|}$ for any $b \in \operatorname{Ran} G'_C$. Hence, $P_{P^{i_1,i_2,\ldots,i_m}(X)|[X]_N=[0]_N}(b) = \frac{1}{|\operatorname{Ran} G'_C|}$ for any $b \in \operatorname{Ran} G'_C$, which implies that $\operatorname{Ran} G'_C = \operatorname{Ran} G'_N$. □

Therefore, we can conclude that even when the eavesdropper obtains the i_1th bit, the i_2th bit, ..., and the i_mth bit, the eavesdropper cannot obtain any information for C/N as long as the image of the matrix G'_N is that of the matrix G'_C.

Example 9.4 Define the code space $C_{G,3}$ by the following generating matrix.

$$G_3 := \begin{pmatrix} 1\ 1\ 1 \\ 1\ 0\ 1 \\ 1\ 0\ 0 \\ 0\ 1\ 0 \\ 0\ 0\ 1 \end{pmatrix}. \tag{9.17}$$

We choose the code pair $N \subset C$ in $\mathbb{F}_2^5$ such that $N = C_{G,3}$ and $C_{G,3} \subset C$. (For example, $C = \mathbb{F}_2^5$.) A 2×3 matrix consisting of arbitrary two row vectors of G_3 has the image $\mathbb{F}_2^2$. Hence, under the condition that two bits of $X \in C$ are fixed, the probability that $[X]_N$ coincides with an element $[X']_N$ of C/N does not depend on the choice of $[X']_N$. That is, we cannot obtain any information for $[X]_N$ when we obtain only arbitrary two bits of X.

Exercise 9.5 Define the code $C_{G,2}$ by the following generating matrix.

$$G_2 := \begin{pmatrix} 1\ 1\ 0 \\ 0\ 1\ 1 \\ 1\ 0\ 1 \\ 1\ 1\ 1 \\ 1\ 0\ 0 \\ 0\ 1\ 0 \\ 0\ 0\ 1 \end{pmatrix}. \tag{9.18}$$

Then, show that the code space $C_{G,1}$ contains the code space $C_{G,2}$.

Example 9.5 As is discussed in Exercise 9.3, any one bit error can be corrected under the code $C_{G,1}$. Hence, when we employ the code $C_{G,1}/C_{G,2}$, we can correct any one bit error. $C_{G,1}/C_{G,2}$ has the following two elements.

$$\begin{aligned} &[(0,0,0,0,0,0,0)^T] \\ =&\{(0,0,0,0,0,0,0),(1,0,1,1,1,0,0),(1,1,0,1,0,1,0),(0,1,1,1,0,0,1), \\ &(0,1,1,0,1,1,0),(1,0,1,0,0,1,1),(1,1,0,0,1,0,1),(0,0,0,1,1,1,1)\} \\ &[(1,1,1,1,1,1,1)^T] \\ =&\{(1,1,1,1,1,1,1),(0,1,0,0,0,1,1),(0,0,1,0,1,0,1),(1,0,0,0,1,1,0), \\ &(1,0,0,1,0,0,1),(0,1,0,1,1,0,0),(0,0,1,1,0,1,0),(1,1,1,0,0,0,0)\}. \end{aligned}$$

Exercise 9.6 Let N be the code $C_{G,2}$. Given two cosets $[x]_N, [x']_N \in \mathbb{F}_2^7/N$, we assume that X and X' are subject to the uniform distribution over the cosets $[x]_N$ and $[x']_N$, respectively. We choose two bits among seven bits. Show that the two bits of X coincide with those of X' with probability $1/4$.

Exercise 9.7 Let N be the code $C_{G,2}$. List up all combinations of three bits that give a part of information for $[X]_N$.

Exercise 9.8 Let N be the code $C_{G,1}$. Given two cosets $[X]_N, [X']_N \in \mathbb{F}_2^7/N$, we assume that X and X' are subject to the uniform distribution over the cosets $[X]_N$ and $[X']_N$, respectively. We choose three bits among seven bits. Show that the three bits of X coincide with those of X' with probability $1/8$.

Exercise 9.9 Define the code $C_{G,4}$ in $\mathbb{F}_2^8$ by the following generating matrix.

$$G_4 := \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \\ 1\,1\,1\,0 \end{pmatrix} \tag{9.19}$$

Let N be the code $C_{G,4}$. Given two cosets $[X]_N, [X']_N \in \mathbb{F}_2^8/N$, we assume that X and X' are subject to the uniform distribution over the cosets $[X]_N$ and $[X']_N$, respectively. We choose three bits among eight bits. Show that the three bits of X coincide with those of X' with probability $1/8$.

Next, we consider the following setting, which might be strange, but is related to quantum cryptography. The subspace N is fixed priorly, and we can randomly choose the code space C containing N according to a random variable Z. In the following, we call a code ensemble C_Z in $\mathbb{F}_2^n$ satisfying $N \subset C_Z$ and the following condition ϵ-**universal2 extended code ensemble** of N [6].

$$\mathrm{P}_Z\{X^n \in C_Z\} \le \epsilon, \quad \forall X^n \in \mathbb{F}_2^n \setminus N. \tag{9.20}$$

Lemma 9.5 *For given a subspace N of $\mathbb{F}_2^n$, we denote the homomorphism from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n/N$ by π_N. When a code ensemble C_Z of $\mathbb{F}_2^n/N$ is ϵ-universal2, $\pi_N^{-1}(C_Z)$ is an ϵ-universal2 extended code ensemble of N.*

Due to this lemma, we can construct a code ensemble required in this subsection, based on a code ensemble given in Sect. 9.2.3. First, we obtain the following lemma as a generalization of Lemma 9.1. Its proof is available by replacing $\mathbb{F}_2^n\setminus\{0\}$ by $\mathbb{F}_2^n\setminus N$ in the proof of Lemma 9.1.

Lemma 9.6 *Given a code space C containing N, the error probability $\delta[C/N]$ of the code pair with the maximum likelihood decoder is evaluated by*

$$\delta[C/N] \le \sum_{X^n \in \mathbb{F}_2^n} P^{(n)}(X^n)^{1-st} \left(\sum_{X'^n \in C\setminus N} P^{(n)}(X^n + X'^n)^t \right)^s$$

with arbitrary real numbers $s, t > 0$.

Then, we obtain the following lemma as a generalization of Theorem 9.1. Its proof is available by replacing $\mathbb{F}_2^n\setminus\{0\}$ and ϵ-universal2 code ensemble by $\mathbb{F}_2^n\setminus N$ ϵ-universal2 extended code ensemble in the proof of Theorem 9.1, respectively.

Theorem 9.3 *When a code ensemble C_Z is an ϵ-universal2 extended code ensemble of N, the inequality $\mathrm{E}_Z \delta[C_Z/N] \le \min_{0\le s\le 1} \epsilon^s 2^{\phi(s:P^{(n)})}$ holds.*

9.3 Quantum Error Correcting Code

9.3.1 Pauli Channel

When we transmit a quantum state via a quantum channel (TPCP map) Λ, we discuss how to protect the quantum state from the noise of the quantum channel Λ. We introduce the Pauli channel as a typical noisy quantum channel. Since the Pauli matrix σ_x given in (2.22) satisfies $\sigma_x|0\rangle = |1\rangle$, $\sigma_x|1\rangle = |0\rangle$, we can consider that it represents **bit flip**.

On the other hand, the Pauli channel σ_z gives the flip with respect to the **phase basis** $|\hat{e}_j\rangle := \frac{1}{\sqrt{2}}(|0\rangle + (-1)^j|1\rangle)$, i.e., the **phase flip** $\sigma_z|\hat{e}_0\rangle = |\hat{e}_1\rangle$, $\sigma_z|\hat{e}_1\rangle = |\hat{e}_0\rangle$. These two matrices satisfy the following commutation relation.

$$\sigma_x\sigma_z = -\sigma_z\sigma_x.$$

Hence, letting $\mathsf{W}(s,t) := \sigma_x^s\sigma_z^t$ for $(s,t) \in \mathbb{F}_2^2$, we obtain

$$\mathsf{W}(s,t)\mathsf{W}(s',t') = (-1)^{s't\oplus t's}\mathsf{W}(s',t')\mathsf{W}(s,t).$$

Next, we focus on the n-qubit system $(\mathbb{C}^2)^{\otimes n}$. Denoting the action of $\mathsf{W}(s,t)$ to the ith qubit system by $\mathsf{W}_i(s,t)$, we define the unitary $\mathsf{W}^n(\vec{s})$ on the quantum system $(\mathbb{C}^2)^{\otimes n}$ with $\vec{s} := (\boldsymbol{s},\boldsymbol{t}) \in \mathbb{F}_2^{2n}$ and $\boldsymbol{s} := (s_1,\dots s_n)$, $\boldsymbol{t} := (t_1,\dots t_n) \in \mathbb{F}_2^n$ as follows.

$$\mathsf{W}^n(\vec{s}) := \mathsf{W}_1(s_1,t_1)\otimes\cdots\otimes\mathsf{W}_n(s_n,t_n).$$

Hence, defining the **symplectic inner product** $\langle\vec{s}_a,\vec{s}_b\rangle := \oplus_{i=1}^n((s_{b,i}\wedge t_{a,i}) \oplus (t_{b,i}\wedge s_{a,i}))$ for $\vec{s}_a,\vec{s}_b \in \mathbb{F}_2^{2n}$, we obtain the commutation relation [10]:

$$\mathsf{W}^n(\vec{s}_a)\mathsf{W}^n(\vec{s}_b) = (-1)^{\langle\vec{s}_a,\vec{s}_b\rangle}\mathsf{W}^n(\vec{s}_b)\mathsf{W}^n(\vec{s}_a). \tag{9.21}$$

Thus, when two vectors $\vec{s}_a,\vec{s}_b \in \mathbb{F}_2^{2n}$ are orthogonal in the sense of the above inner product, the two matrices $\mathsf{W}^n(\vec{s}_a)$ and $\mathsf{W}^n(\vec{s}_b)$ are commutative with each other.

Now, we consider the case when the unitary $\mathsf{W}^n(\vec{s})$ operates on the quantum system $(\mathbb{C}^2)^{\otimes n}$ as the noise with the probability $P^{(n)}(\vec{s})$. The state reduction can be described by a **Pauli channel** $\Lambda[P^{(n)}]$, which is defined by

$$\Lambda[P^{(n)}](\rho) := \sum_{\vec{s}\in\mathbb{F}_2^{2n}} P^{(n)}(\vec{s})\mathsf{W}^n(\vec{s})\rho\mathsf{W}^n(\vec{s})^\dagger. \tag{9.22}$$

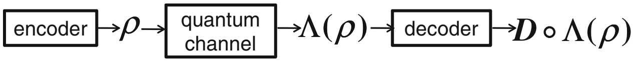


Fig. 9.3 Error correction with quantum channel

In particular, when the distribution $P^{(n)}$ is given as the n-trial independent and identical distribution P^n of the distribution P on $\mathbb{F}_2^2$, we obtain $\Lambda[P^n] = \Lambda[P]^{\otimes n}$.

Further, the entanglement fidelity given in Sect. 6.3.8 of the Pauli channel can be calculated by use of the formula (6.118) as follows

$$F_e^2(\rho_{\text{mix}}, \Lambda[P^{(n)}]) = P^{(n)}(0) \tag{9.23}$$

because $\operatorname{Tr} \rho_{\text{mix}} \mathsf{W}^n(0) = 1$ and $\operatorname{Tr} \rho_{\text{mix}} \mathsf{W}^n(\vec{s}) = 0$ for $\vec{s} \neq 0$. Finally, we introduce a notation for a Pauli channel. When a Pauli channel Λ is written as the form (9.22), we denote the probability distribution $P^{(n)}$ deciding the channel by $P[\Lambda]$.

9.3.2 Stabilizer Code

Now, we treat quantum error correction, which protects the quantum state when it is transmitted via a quantum channel (TPCP map) Λ. In the following discussion, both of the input and output systems of the quantum channel Λ are assumed to be written as the same Hilbert space $\mathcal{H}$. First, we fix the quantum system to be transmitted, which is called a **message system**. Then, we call the device or the process transforming the message system to the input system of the quantum channel the **encoder**, and call the device or the process transforming the output system of the quantum channel to the message system the **decoder** [11].

Generally, since the encoder and the decoder change the state, they are given as TPCP map. When we construct a quantum error correction code by an algebraic method, it is very often to restrict the encoder to the isometry embedding from the message system to the input system.[4] In this case, the encoder can be characterized by restricting the input system of the given quantum channel.

Hence, when we restrict the input system of the given quantum channel to the sub-Hilbert space $\mathcal{H}_0$ of $\mathcal{H}$, we call the sub-Hilbert space $\mathcal{H}_0$ a **code space**. In this case, the decoder is given as a TPCP map D from the output system of the channel to the sub-Hilbert space $\mathcal{H}_0$, as explained in Fig. 9.3.

In the following, we concretely give stabilizer codes, which are the most important class of quantum error correcting codes [13–16]. In the case of classical error correcting codes, we give a code by using the subspace of $\mathbb{F}_2^n$, and call it a classical code space for distinguishing it from a quantum code space.

Since we need to treat the bit and phase flips in the quantum system, when we treat the n qubit systems, we treat a subspace N of $\mathbb{F}_2^{2n}$. The subspace N is called

[4] It is known that this assumption does not change the asymptotically optimal transmission rate [12].

self-orthogonal if $\langle \vec{s}_a, \vec{s}_b \rangle = 0$ holds for arbitrary $\vec{s}_a, \vec{s}_b \in N$. The **orthogonal complementary space** $N^{\vDash}$ of N is defined as $N^{\vDash} := \{\vec{s}_a \in \mathbb{F}_2^{2n} | \langle \vec{s}_a, \vec{s}_b \rangle = 0, \quad \forall \vec{s}_b \in N\}$. Then, N is self-orthogonal if and only if $N \subset N^{\vDash}$.

In the following, we construct a quantum error correcting code based on a self-orthogonal space $N \subset \mathbb{F}_2^{2n}$. Due to the property (9.21), all of elements of $\{\mathsf{W}^n(\vec{s})\}_{\vec{s} \in N}$ can be diagonalized simultaneously with the form $\mathsf{W}^n(\vec{s}) = \sum_i f_i(\vec{s}) P_i$, where P_i is the projection to the simultaneous eigenspace and f_i is the map giving the eigenvalue. Now, we denote the set of the liner map from N to $\mathbb{F}_2$ over the finite field $\mathbb{F}_2$ by N^*. Then, the map f_i satisfies $f_i(\vec{s}_a) f_i(\vec{s}_b) = f_i(\vec{s}_a + \vec{s}_b)$ because $\mathsf{W}^n(\vec{s}_a)\mathsf{W}^n(\vec{s}_b) = \mathsf{W}^n(\vec{s}_a + \vec{s}_b)$ holds for $\vec{s}_a, \vec{s}_b \in N$. Hence, the map f_i is given as $f_i(\vec{s}) = (-1)^{x_i(\vec{s})}$ with $x_i \in N^*$. That is, since the eigenvalues of $\mathsf{W}^n(\vec{s})$ are ± 1, we can assign the simultaneous eigenspace $\mathcal{H}_x \subset (\mathbb{C}^2)^{\otimes n}$ corresponding to $x \in N^*$. Denoting the projection to $\mathcal{H}_x$ by P_x, we obtain the following simultaneous diagonalization:

$$\mathsf{W}^n(\vec{s}) = \sum_{x \in N^*} (-1)^{x(\vec{s})} P_x, \quad \forall \vec{s} \in N. \tag{9.24}$$

Since the scalar $[\vec{s}_b](\vec{s}_a) := \langle \vec{s}_b, \vec{s}_a \rangle$ does not depend on the choice of $\vec{s}_b$ of the equivalent class $[\vec{s}_b] \in \mathbb{F}_2^{2n}/N^{\vDash}$, we can regard $[\vec{s}_b]$ as an element of N^* via the relation $[\vec{s}_b](\vec{s}_a) = \langle \vec{s}_b, \vec{s}_a \rangle$. Conversely, since an arbitrary element of N^* can be represented by use of an element of $\mathbb{F}_2^{2n}/N^{\vDash}$, we can identify $\mathbb{F}_2^{2n}/N^{\vDash}$ and N^*. In particular, given $\vec{s}_a \in N$ and $\vec{s}_b \in \mathbb{F}_2^{2n}$, we obtain

$$\begin{aligned}\sum_{x \in N^*} (-1)^{x(\vec{s}_a)} \mathsf{W}^n(\vec{s}_b) P_x \mathsf{W}^n(\vec{s}_b)^\dagger &= \mathsf{W}^n(\vec{s}_b)\mathsf{W}^n(\vec{s}_a)\mathsf{W}^n(\vec{s}_b)^\dagger \\ &= (-1)^{[\vec{s}_b](\vec{s}_a)} \mathsf{W}^n(\vec{s}_a) = \sum_{x \in N^*} (-1)^{[\vec{s}_b](\vec{s}_a) + x(\vec{s}_a)} P_x \\ &= \sum_{x \in N^*} (-1)^{([\vec{s}_b]+x)(\vec{s}_a)} P_x = \sum_{x \in N^*} (-1)^{x(\vec{s}_a)} P_{x+[\vec{s}_b]}.\end{aligned} \tag{9.25}$$

Thus, the unitary $\mathsf{W}^n(\vec{s}_b)$ maps the sub-Hilbert space $\mathcal{H}_x$ to the sub-Hilbert space $\mathcal{H}_{x+[\vec{s}_b]}$.

Using the structure, we construct a quantum error correcting code. First, we choose a sub-Hilbert space $\mathcal{H}_0$ corresponding to $0 \in N^*$ as our code space . Then, we choose the representative $\vec{s}_x$ for a given $x \in N^* = \mathbb{F}_2^{2n}/N^{\vDash}$, and define the decoder $D(\rho) := \sum_{x \in N^*} \mathsf{W}^n(\vec{s}_x)^\dagger P_x \rho P_x \mathsf{W}^n(\vec{s}_x)$. Here, we do not have to choose the representative $\vec{s}_x$ satisfying $\vec{s}_x + \vec{s}_{x'} = \vec{s}_{x+x'}$. In order that our quantum error correcting code works against the noise effectively, it is better to choose the representative $\vec{s}_x$ such that the relation $\vec{s}_x + \vec{s}_{x'} = \vec{s}_{x+x'}$ does not necessarily hold. The above constructed quantum error correcting code from a self-orthogonal space N is called the **stabilizer code** whose **stabilizer** is the self-orthogonal space N. In particular, since we can identify the encoder $\mathcal{H}_0$ with the self-orthogonal space

N in the stabilizer code, we often call N the encoder. In the case of Pauli channel $\Lambda[P^{(n)}](\rho) = \sum_{\vec{s}\in\mathbb{F}_2^{2n}} P^{(n)}(\vec{s})\mathsf{W}^n(\vec{s})\rho\mathsf{W}^n(\vec{s})^\dagger$, we can think that the error $\mathsf{W}^n(\vec{s})$ occurs with probability $P^{(n)}(\vec{s})$.

When N is a k-dimensional subspace of $\mathbb{F}_2$, we have $|N^*| = 2^k$, and every simultaneous eigenspace $\mathcal{H}_x$ has dimension 2^{n-k}. That is, the code space $\mathcal{H}_0$ has dimension 2^{n-k}. Since $|N^{\vDash}| = 2^{2n-k}$, we obtain the following formula

$$\operatorname{Tr}\mathcal{H}_0 = 2^{n-k} = \frac{|\mathbb{F}_2^n|}{|N|} = \sqrt{\frac{|N^{\vDash}|}{|N|}}. \tag{9.26}$$

Further, we obtain $\operatorname{Tr}\mathsf{W}^n(\vec{s})|_{\mathcal{H}_0} = 0$ for $\vec{s} \in \mathbb{F}_2^{2n}\setminus N^{\vDash}$ because the unitary $\mathsf{W}^n(\vec{s})$ maps an element of the code space $\mathcal{H}_0$ to an element of $\mathcal{H}_{[\vec{s}]}$. On the other hand, $\mathsf{W}^n(\vec{s})|_{\mathcal{H}_0}$ is not a constant scalar for $\vec{s} \in N^{\vDash}\setminus N$ although the unitary $\mathsf{W}^n(\vec{s})$ maps an element of the code space $\mathcal{H}_0$ to an element of $\mathcal{H}_0$.

As a summary, we obtain

$$\operatorname{Tr}\mathsf{W}^n(\vec{s}-\vec{s}_x)|_{\mathcal{H}_0} = \begin{cases} 0 & \text{if } \vec{s}-\vec{s}_x \notin N \\ \operatorname{Tr} P_0 & \text{if } \vec{s}-\vec{s}_x \in N. \end{cases} \tag{9.27}$$

Denoting the quantum channel Λ with restricting the input system to $\mathcal{H}_0$ by $\Lambda_{\mathcal{H}_0}$ and letting $\mathcal{J} := \{\vec{s}_x\}_{x\in N^*}$, due to (6.118), we can characterize the entanglement fidelity of the quantum channel $D \circ \Lambda_{\mathcal{H}_0}$ as follows.

$$F_e^2(\rho_{\mathrm{mix}}, D\circ\Lambda_{\mathcal{H}_0}) = \sum_{x\in N^*,\vec{s}\in N} P^{(n)}(\vec{s}_x+\vec{s}) = P^{(n)}(\mathcal{J}+N). \tag{9.28}$$

Under a given code space $\mathcal{H}_0$ and the Pauli channel $\Lambda[P^{(n)}]$, the decoder realizing the maximum entanglement fidelity is given by choosing the representative to be $\operatorname{argmax}_{\vec{s}_x\in x}\sum_{\vec{s}\in N} P^{(n)}(\vec{s}_x+\vec{s})$ for $x \in N^* = \mathbb{F}_2^{2n}/N^{\vDash}$. The decoder is called the **maximum likelihood decoder** for the code space N under the probability distribution $P^{(n)}$. As the above mentioned way, the construction of the decoder of a stabilizer code and the evaluation of entanglement fidelity can be obtained by the classical discussion for the distribution $P^{(n)}$.

We employ the sub-Hilbert space $\mathcal{H}_{x'}$ as a code space instead of $\mathcal{H}_0$ and define the decoder by

$$D_{x'}(\rho) := \sum_{x\in N^*} \mathsf{W}^n(\vec{s}_{x-x'})^\dagger P_x\rho P_x \mathsf{W}^n(\vec{s}_{x-x'}). \tag{9.29}$$

Then, the quantum error correcting code has the same performance as that defined with the code space $\mathcal{H}_0$. For any element $[\vec{s}] \in N^{\vDash}/N$, the unitary $\mathsf{W}^n(\vec{s})$ preserves the sub-Hilbert spaces $\mathcal{H}_0$ and $\mathcal{H}_x$. The operations for these sub-Hilbert spaces do not depend on the choice of the representative except for the scalar times. Then, we denote the action to the sub-Hilbert space $\mathcal{H}_x$ by $\mathsf{W}^n|_{\mathcal{H}_x}([\vec{s}])$.

Defining the distribution $P^{(n)}\{\mathcal{J}+N\}([\vec{s}]) := P^{(n)}(\mathcal{J}+\vec{s}+N)$ for $[\vec{s}] \in N^{\vDash}/N$, we have

$$\begin{aligned} & P[D_x \circ \Lambda_{\mathcal{H}_x}]([\vec{s}]) \\ & \quad = \frac{1}{\dim \mathcal{H}_x^2} \langle\langle \mathsf{W}^n|_{\mathcal{H}_x}([\vec{s}])|((D_x \circ \Lambda_{\mathcal{H}_x}) \otimes \mathcal{I}_{\mathrm{R}})(|\, I_{\mathcal{H}_x}\rangle\rangle\langle\langle I_{\mathcal{H}_x}\, |)|\mathsf{W}^n|_{\mathcal{H}_x}([\vec{s}])\rangle\rangle \\ & \quad = P^{(n)}(\mathcal{J}+\vec{s}+N) = P^{(n)}\{\mathcal{J}+N\}([\vec{s}]), \end{aligned} \tag{9.30}$$

where the vector $|X\rangle\rangle \in \mathcal{H} \otimes \mathcal{H}_R$ is defined as $|X\rangle\rangle := \sum_{i,j} X_{i,j}|i,j\rangle$ for a given matrix X. That is, the application of the above quantum error correction to the Pauli channel $\Lambda[P^{(n)}]$ yields the Pauli channel with the distribution $P^{(n)}\{\mathcal{J}+N\}$.

9.3.3 CSS Code

In this subsection, we concretely give a stabilizer code by use of the structure $\mathbb{F}_2^{2n} = \mathbb{F}_2^n \times \mathbb{F}_2^n$ [17–19]. In the following discussion, when we need to distinguish the first part and the second part in $\mathbb{F}_2^{2n} = \mathbb{F}_2^n \times \mathbb{F}_2^n$, we denote them by $\mathbb{F}_{2,1}^n$ and $\mathbb{F}_{2,2}^n$, respectively. Based on the inner product $(\boldsymbol{s}|\boldsymbol{t}) := s_1t_1 + \cdots + s_nt_n$ in $\mathbb{F}_2^n$, we define the **orthogonal complementary space** $C^{\vdash} := \{\boldsymbol{s} \in \mathbb{F}_2^n|(\boldsymbol{s}|\boldsymbol{t}) = 0,\ \forall \boldsymbol{t} \in C\}$ of a subspace $C \subset \mathbb{F}_2^n$, which is a classical code space . Then, the dimension of $C^{\vdash}$ is n minus the dimension of C, and we obtain the following lemma.

Lemma 9.7 *The relation $C_2^{\vdash} \times C_1^{\vdash} = (C_1 \times C_2)^{\vDash}$ holds.*

Proof of Lemma 9.7 We can check that $C_2^{\vdash} \times C_1^{\vdash} \subset (C_1 \times C_2)^{\vDash}$ by showing that any element of $C_2^{\vdash} \times C_1^{\vdash}$ is orthogonal to any element of $C_1 \times C_2$.

Conversely, any element $(\boldsymbol{s}, \boldsymbol{t}) \in (C_1 \times C_2)^{\vDash}$ satisfies $(\boldsymbol{s}'|\boldsymbol{t}) = (\boldsymbol{s}|\boldsymbol{t}')$ for any elements $\boldsymbol{s}' \in C_1$ and $\boldsymbol{t}' \in C_2$. When $\boldsymbol{s}' = 0$, we have $\boldsymbol{s} \in C_2^{\vdash}$. When $\boldsymbol{t}' = 0$, we obtain $\boldsymbol{t} \in C_1^{\vdash}$, which implies the desired argument. □

Exercise 9.10 Show that $C_{G,1} = C_{G,2}^{\vdash}$.

When two subspaces $C_1, C_2 \subset \mathbb{F}_2^n$ satisfy the **torsion condition** $C_1 \subset C_2^{\vdash}$, the relation $C_2 \subset C_1^{\vdash}$ holds and $C_1 \times C_2 \subset \mathbb{F}_2^{2n}$ is a self-orthogonal subspace. We call the stabilizer code based on a self-orthogonal subspace **Calderbank-Shor-Steane (CSS) code**. Lemma 9.7 guarantees that $(C_1 \times C_2)^*$ is isomorphic to $\mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash}$. Due to the fact and (9.26), the dimension of the code space $\mathcal{H}_0$ of the CSS code can be given as

$$\frac{|\mathbb{F}_2|^n}{|C_1 \times C_2|} = \frac{|\mathbb{F}_2|^n}{|\mathbb{F}_2^n/C_2^{\vdash}| \cdot |\mathbb{F}_2^n/C_1^{\vdash}|} = \frac{|C_2^{\vdash}| \cdot |C_1^{\vdash}|}{|\mathbb{F}_2|^n}. \tag{9.31}$$

In particular, when the dimensions of $C_1^{\vdash}$ and $C_2^{\vdash}$ over the finite field $\mathbb{F}_2$ are k_1 and k_2, respectively, the dimension of $\mathcal{H}_0$ is $2^{k_1+k_2-n}$.

Then, given $[\boldsymbol{s}] \in C_2^{\vdash}/C_1$, we define the vector

$$|[\boldsymbol{s}]\rangle := \sum_{\boldsymbol{s}'\in[\boldsymbol{s}]} \frac{1}{\sqrt{|C_1|}} |\boldsymbol{s}'\rangle. \tag{9.32}$$

The orthonormal basis of $\mathcal{H}_0$ is given by $\{|[\boldsymbol{s}]\rangle\}_{[\boldsymbol{s}]\in C_2^{\vdash}/C_1}$. As a generalization of the vector $|[\boldsymbol{s}]\rangle$, we define the vector based on $([\boldsymbol{x}], [\boldsymbol{y}]) \in \mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash} = (C_1 \times C_2)^*$ and $[\boldsymbol{s}] \in C_2^{\vdash}/C_1$ as follows.

$$|[\boldsymbol{s}], [\boldsymbol{x}], [\boldsymbol{y}]\rangle := \sum_{\boldsymbol{s}'\in[\boldsymbol{s}]} \frac{1}{\sqrt{|C_1|}} (-1)^{\boldsymbol{s}'\cdot\boldsymbol{y}} |\boldsymbol{s}' + \boldsymbol{x}\rangle. \tag{9.33}$$

Then, the orthonormal basis of $\mathcal{H}_{([\boldsymbol{x}],[\boldsymbol{y}])}$ is given by $\{|[\boldsymbol{s}], [\boldsymbol{x}], [\boldsymbol{y}]\rangle\}_{[\boldsymbol{s}]\in C_2^{\vdash}/C_1}$.

Example 9.6 When $C_1 = C_2 = C_{G,2}$, the above exercise guarantees the torsion condition $C_{G,2} = C_1 \subset C_2^{\vdash} = C_{G,2}^{\vdash} = C_{G,1}$. Hence, we can define the CSS code with the stabilizer $C_{G,2} \times C_{G,2}$, and obtain

$$\begin{aligned}
&|[(0, 0, 0, 0, 0, 0, 0)^T], 0, 0\rangle \\
&\quad = \frac{1}{\sqrt{8}}(|0, 0, 0, 0, 0, 0, 0\rangle + |1, 0, 1, 1, 1, 0, 1\rangle + |1, 1, 0, 1, 0, 1, 0\rangle \\
&\qquad + |0, 1, 1, 0, 1, 1, 1\rangle + |0, 1, 1, 1, 0, 0, 1\rangle + |1, 1, 0, 0, 0, 0, 0\rangle \\
&\qquad + |1, 0, 1, 0, 0, 1, 1\rangle + |0, 0, 0, 1, 1, 1, 0\rangle) \\
&|[(1, 1, 1, 1, 1, 1, 1)^T], 0, 0\rangle \\
&\quad = \frac{1}{\sqrt{8}}(|1, 1, 1, 1, 1, 1, 1\rangle + |0, 1, 0, 0, 0, 1, 0\rangle + |0, 0, 1, 0, 1, 0, 1\rangle \\
&\qquad + |1, 0, 0, 1, 0, 0, 0\rangle + |1, 0, 0, 0, 1, 1, 0\rangle + |0, 0, 1, 1, 1, 1, 1\rangle \\
&\qquad + |0, 1, 0, 1, 1, 0, 0\rangle + |1, 1, 1, 0, 0, 0, 1\rangle).
\end{aligned}$$

In particular, the encoder from $\mathbb{C}^2$ to $\mathcal{H}_0$ is given by

$$|0\rangle \to |[(0, 0, 0, 0, 0, 0, 0)^T], 0, 0\rangle, \quad |1\rangle \to |[(1, 1, 1, 1, 1, 1, 1)^T], 0, 0\rangle.$$

Given $x \in \mathbb{F}_2^n/C_2^{\vdash}$ and $y \in \mathbb{F}_2^n/C_1^{\vdash}$, we choose representatives $\boldsymbol{s} \in x \subset \mathbb{F}_2^n$ and $\boldsymbol{t} \in y \subset \mathbb{F}_2^n$. Due to Lemma 9.7, a representative of $(x, y) \in (C_1 \times C_2)^*$ is given by $(\boldsymbol{s}, \boldsymbol{t}) \in (x, y) \subset \mathbb{F}_2^{2n}$. In this case, we can choose the representative $\boldsymbol{s}$ of x depending on y. This choice can be applied to the case of representative $\boldsymbol{t}$ of y.

When the noisy channel is given by a Pauli channel, we can consider that the error $\vec{s} = (\boldsymbol{s}, \boldsymbol{t})$ occurs with probability $P^{(n)}(\vec{s}) = P^{(n)}(\boldsymbol{s}, \boldsymbol{t})$. In this case, the error $\boldsymbol{s}$ for the first part concerns about the bit basis and is called the **bit error**, and the error

$\boldsymbol{t}$ for the second part concerns about the phase basis and is called the **phase error**. Hence, in the case of CSS codes, we can apply error correction to the bit error and the phase error, separately. When two errors $\boldsymbol{s}$ and $\boldsymbol{t}$ are independent of each other, i.e., the distribution $P^{(n)}(\vec{s})$ is given as the product distribution of two distributions $P_1^{(n)}$ and $P_2^{(n)}$ on $\mathbb{F}_2^n$, we can independently choose representatives $\boldsymbol{s}_x$ and $\boldsymbol{t}_y$ of $x \in C_1^*$ and $y \in C_2^*$, and can calculate the entanglement fidelity of the quantum channel $D \circ \Lambda_{\mathcal{H}_0}$ as

$$
\begin{aligned}
F_e^2(\rho_{\mathrm{mix}}, D \circ \Lambda_{\mathcal{H}_0}) &= \sum_{x \in \mathbb{F}_2^n / C_2^{\vdash}} \sum_{y \in \mathbb{F}_2^n / C_1^{\vdash}} \sum_{\boldsymbol{s}' \in C_1} \sum_{\boldsymbol{t}' \in C_2} P^{(n)}((\boldsymbol{s}_x, \boldsymbol{t}_y) + (\boldsymbol{s}', \boldsymbol{t}')) \\
&= \left(\sum_{x \in \mathbb{F}_2^n / C_2^{\vdash}, \boldsymbol{s}' \in C_1} P_1^{(n)}(\boldsymbol{s}_x + \boldsymbol{s}') \right) \\
&\quad \left(\sum_{y \in \mathbb{F}_2^n / C_1^{\vdash}, \boldsymbol{t}' \in C_2} P_2^{(n)}(\boldsymbol{t}_y + \boldsymbol{t}') \right). \qquad (9.34)
\end{aligned}
$$

The probability $\sum_{x \in \mathbb{F}_2^n / C_2^{\vdash}, \boldsymbol{s}' \in C_1} P_1^{(n)}(\boldsymbol{s}_x + \boldsymbol{s}')$ realizes the maximum value when the maximum likelihood decoder of the classical code pair $C_1 \subset C_2^{\vdash}$ is applied. The probability $\sum_{y \in \mathbb{F}_2^n / C_1^{\vdash}, \boldsymbol{t}' \in C_2} P_2^{(n)}(\boldsymbol{t}_y + \boldsymbol{t}')$ realizes the maximum value in the similar case. Hence, the maximum likelihood decoder of the CCS code can be realized by the simple combination of the both maximum likelihood decoders of the both classical code pairs $C_1 \subset C_2^{\vdash}$ and $C_2 \subset C_1^{\vdash}$.

Of course, even though the two errors $\boldsymbol{s}$ and $\boldsymbol{t}$ are not independent of each other, the relation (9.34) holds as a relation for the respective marginal distributions for $\boldsymbol{s}$ and $\boldsymbol{t}$. In this case, when we choose the representatives by use of the correlation between $\boldsymbol{s}$ and $\boldsymbol{t}$, we obtain a better decoder than the decoder with independent decoding.

When $P_1^{(n)}(\boldsymbol{s})$ is the marginal distribution for the first part $\mathbb{F}_{2,1}^n$ and $P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})$ is the conditional probability distribution for the second part $\mathbb{F}_{2,2}^n$ under the condition for the first part $\mathbb{F}_{2,1}^n$, using $P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})$, we can realize a larger (better) entanglement fidelity than (9.34).

In this construction, we choose our decoder $\boldsymbol{s}_x \in x$ and $\boldsymbol{t}_{x,y} \in y$ as follows. We, first, decide the representative $\boldsymbol{s}_x \in x$ for $x \in \mathbb{F}_2^n / C_2^{\vdash}$ based on $P_1^{(n)}(\boldsymbol{s})$. Next, we decide the representative $\boldsymbol{t}_{x,y} \in y$ of $y \in \mathbb{F}_2^n / C_1^{\vdash}$ depending on x based on $P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})$. Then, the entanglement fidelity of the quantum channel $D \circ \Lambda_{\mathcal{H}_0}$ can be characterized as

$$
F_e^2(\rho_{\mathrm{mix}}, D \circ \Lambda_{\mathcal{H}_0}) = \sum_{x \in \mathbb{F}_2^n / C_2^{\vdash}} \sum_{y \in \mathbb{F}_2^n / C_1^{\vdash}} \sum_{\boldsymbol{s}' \in C_1} \sum_{\boldsymbol{t}' \in C_2} P^{(n)}((\boldsymbol{s}_x, \boldsymbol{t}_{x,y}) + (\boldsymbol{s}', \boldsymbol{t}'))
$$

$$
\begin{aligned}
&= \sum_{x\in\mathbb{F}_2^n/C_2^\perp, \boldsymbol{s}'\in C_1} P_1^{(n)}(\boldsymbol{s}_x+\boldsymbol{s}') \\
&\quad \left(\sum_{y\in\mathbb{F}_2^n/C_1^\perp, \boldsymbol{t}'\in C_2} P_{2|1}^{(n)}(\boldsymbol{t}_{x,y}+\boldsymbol{t}'|\boldsymbol{s}_x+\boldsymbol{s}') \right).
\end{aligned}
$$

Indeed, it is easier to treat 1 minus the entanglement fidelity than the entanglement fidelity itself because the former value corresponds to the error probability.

In the following, we consider the case when $\boldsymbol{t}$ obeys the distribution $P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s}_x)$ and $\boldsymbol{t}_{x,y} \in y$ is decided to be $\boldsymbol{t}_{y:\boldsymbol{s}_x}$, which depends on x. That is, we define $\boldsymbol{t}_{y:\boldsymbol{s}} := \operatorname{argmax}_{\boldsymbol{t}\in y} \sum_{\boldsymbol{t}'\in C_2} P_{2|1}^{(n)}(\boldsymbol{t}+\boldsymbol{t}'|\boldsymbol{s})$. Restricting the range of the summand for $\boldsymbol{s}'$ to $\{0\}$, we obtain

$$
\begin{aligned}
&1 - F_e^2(\rho_{\mathrm{mix}}, D\circ\Lambda_{\mathcal{H}_0}) \\
&\le 1 - \sum_{x\in\mathbb{F}_2^n/C_2^\perp} P_1^{(n)}(\boldsymbol{s}_x) \left(\sum_{y\in\mathbb{F}_2^n/C_1^\perp, \boldsymbol{t}'\in C_2} P_{2|1}^{(n)}(\boldsymbol{t}_{x,y}+\boldsymbol{t}'|\boldsymbol{s}_x) \right) \\
&= \left(1 - \sum_{x\in\mathbb{F}_2^n/C_2^\perp} P_1^{(n)}(\boldsymbol{s}_x) \right) \\
&\quad + \sum_{x\in\mathbb{F}_2^n/C_2^\perp} P_1^{(n)}(\boldsymbol{s}_x) \left(1 - \sum_{y\in\mathbb{F}_2^n/C_1^\perp, \boldsymbol{t}'\in C_2} P_{2|1}^{(n)}(\boldsymbol{t}_{y:\boldsymbol{s}_x}+\boldsymbol{t}'|\boldsymbol{s}_x) \right) \\
&\le \left(1 - \sum_{x\in\mathbb{F}_2^n/C_2^\perp} P_1^{(n)}(\boldsymbol{s}_x) \right) \\
&\quad + \sum_{\boldsymbol{s}\in\mathbb{F}_2^n} P_1^{(n)}(\boldsymbol{s}) \left(1 - \sum_{y\in\mathbb{F}_2^n/C_1^\perp, \boldsymbol{t}'\in C_2} P_{2|1}^{(n)}(\boldsymbol{t}_{y:\boldsymbol{s}}+\boldsymbol{t}'|\boldsymbol{s}) \right).
\end{aligned} \tag{9.35}
$$

The evaluation of the entanglement fidelity can be reduced to the evaluation of the error probability of the classical code determined by the subspace $C_2^\perp$ and the quotient space $C_1^\perp/C_2$ in this way.

9.3.4 Asymptotic Theory

In the following, we treat the Pauli channel given by the n-trial independent and identical distribution P^n of the distribution P on $\mathbb{F}_2^2$. Similar to the classical case, the theory for the above channel with infinitely large n is called the asymptotic theory, in which, we treat a sequence of codes. We treat only CSS codes, i.e., treat a sequence $\{(C_{1,n}, C_{2,n})\}$ of code pairs satisfying the torsion condition. The most important quantities in the asymptotic theory are the limit of the entanglement fidelity and the transmission rate, which describes the asymptotic behavior of the dimension of the quantum system to be transmitted. Since it follows from (9.31) that the dimension of the quantum system to be transmitted is $\frac{|C_{1,n}^{\vdash}|\cdot|C_{2,n}^{\vdash}|}{|\mathbb{F}_2|^n}$, the latter is given as

$$\lim_{n\to\infty} \frac{1}{n} \log \frac{|C_{1,n}^{\vdash}| \cdot |C_{2,n}^{\vdash}|}{|\mathbb{F}_2|^n} = \lim_{n\to\infty} \frac{\log |C_{1,n}^{\vdash}||C_{2,n}^{\vdash}|}{n} - 1. \tag{9.36}$$

We also require that the former converges 1.

We suppose that the first part and the second part are independent of each other in the distribution P on $\mathbb{F}_2^2$, and denote their marginal distributions by P_1 and P_2. We choose R_1 and R_2 satisfying

$$R_1 > H(P_1), \quad R_2 > H(P_2), \tag{9.37}$$

and choose $k_1 := \lfloor (1 - R_1)n \rfloor$ and $k_2 := \lfloor (1 - R_2)n \rfloor$ for given n. Then, we choose a $2^{k_1 - n}$-universal2 code ensemble $C_{1,Z,n}^{\vdash}$ given in Lemma 9.3, which decides the code ensemble $C_{1,Z,n}$. Next, combining Lemmas 9.3 and 9.5, we give a $2^{k_2 - n}$-universal2 extended code ensemble $C_{2,Z',n}^{\vdash}$ of $C_{1,Z,n}$ [20, 21], where the random variable Z' is independent of the random variable Z. The dimension of $C_{1,Z,n}^{\vdash}$ is k_1, and that of $C_{2,Z',n}^{\vdash}$ is k_2. Hence, the dimension of the quantum system to be transmitted is $2^{k_1 + k_2 - n}$, which implies that the transmission rate is $1 - R_1 - R_2$.

Using discussions similar to proofs of Theorems 9.1 and 9.3, we can evaluate the expectation of right hand side of (9.35) with respect to the code ensemble as

$$\begin{aligned} &\mathrm{E}_{Z,Z'} \left(1 - \sum_{x \in \mathbb{F}_2^n / C_{2,Z',n}^{\vdash}} P_1^{(n)}(\boldsymbol{s}_x) \right) + \left(1 - \sum_{\substack{y \in \mathbb{F}_2^n / C_{1,Z,n}^{\vdash}, \\ \boldsymbol{t}' \in C_{2,Z',n}}} P_2^{(n)}(\boldsymbol{t} + \boldsymbol{t}') \right) \\ \leq &\min_{0 \leq s \leq 1} 2^{s(k_1 - n)} 2^{\phi(s : P_1^{(n)})} + \min_{0 \leq s \leq 1} 2^{s(k_2 - n)} 2^{\phi(s : P_2^{(n)})}. \end{aligned}$$

Hence, due to Condition (9.37), the above value converges zero exponentially with respect to n. Thus, the following rate can be attained [19]:

$$1 - H(P_1) - H(P_2) = 1 - H(P),$$

which coincides with coherent information $I_c(\rho_{\mathrm{mix}}; \Lambda[P])$ given in (6.67).

On the other hand, when the first part and the second part are not independent of each other in the distribution P on $\mathbb{F}_2^2$, we can apply the same discussion to the right hand side of (9.35). A similar discussion yields that the rate $1 - H(P)$ [19] can be attained [22].

9.4 Application to Quantum Secret Communication

9.4.1 Channel to the Environment System

If we succeed in transmitting a quantum state with keeping the coherency and without any error in the quantum channel, the information transmission has the perfect secrecy [23]. However, the real quantum communication does not necessarily keep the coherency. In order to treat the secrecy for such a case, we need to clarify how the information is leaked to the environment system. In this subsection, when a quantum channel Λ is given, we treat the quantum channel whose output is the quantum state leaked to the environment system of the given quantum channel Λ. For this purpose, we consider the Stinespring representation (5.71) of the quantum channel Λ, in which, $\mathcal{H}_{\mathrm{E}}$ is the environment system, ρ_{E} is the initial pure state in the environment system, and U is the unitary evolution of the composite system $\mathcal{H} \otimes \mathcal{H}_{\mathrm{E}}$. Then, the information leaked to the environment system can be given by the quantum channel to the environment system $\Lambda_{\mathrm{E}}(\rho) := \mathrm{Tr}_{\mathcal{H}}\, U\rho \otimes \rho_{\mathrm{E}} U^{\dagger}$. Note that the quantum channel Λ_{E} does not depend on the choice of Stinespring representation. That is, the quantum channel to the environment system based on a different Stinespring representation is given by addition of isometry to the quantum channel to the original environment system.

Then, applying the Kraus representation $\{F_m\}$, we can characterize Λ_{E} as follows because $U = \sum_m F_m |m\rangle$.

$$\Lambda_{\mathrm{E}}(\rho) = \sum_{m,m'} (\mathrm{Tr}\, F_m \rho F_{m'}^{\dagger}) |m\rangle\langle m'|. \tag{9.38}$$

Then, due to (9.38), the quantum channel $\Lambda[P^{(n)}]_{\mathrm{E}}$ to environment system of the given Pauli channel $\Lambda[P^{(n)}]$ is given by use of the basis $|\vec{s}_a\rangle$ of environment system as follows

$$\Lambda[P^{(n)}]_{\mathrm{E}}(\rho) = \sum_{\vec{s}_a, \vec{s}_b} \sqrt{P^{(n)}(\vec{s}_a)}\sqrt{P^{(n)}(\vec{s}_b)} [\mathrm{Tr}\, \mathsf{W}^n(\vec{s}_a)\rho \mathsf{W}^n(-\vec{s}_b)] |\vec{s}_a\rangle\langle \vec{s}_b|.$$

When the input state is given by a bit base $|s\rangle$, we obtain $\mathsf{W}^n(\vec{s}_a)|\boldsymbol{x}\rangle = (-1)^{\boldsymbol{t}\cdot\boldsymbol{x}} |\boldsymbol{x}+\boldsymbol{s}\rangle$, where $\vec{s}_a = (\boldsymbol{s},\boldsymbol{t})$. Hence, we can characterize the output state of the quantum channel $\Lambda[P^{(n)}]_{\mathrm{E}}$ to the environment system as

$$\begin{aligned}
\Lambda[P^{(n)}]_{\mathrm{E}}(|\boldsymbol{x}\rangle\langle\boldsymbol{x}|) &= \sum_{\vec{s}_a,\vec{s}_b} \sqrt{P^{(n)}(\vec{s}_a)}\sqrt{P^{(n)}(\vec{s}_b)}\langle\boldsymbol{x}|\mathsf{W}^n(-\vec{s}_b)\mathsf{W}^n(\vec{s}_a)|\boldsymbol{x}\rangle|\vec{s}_a\rangle\langle\vec{s}_b| \\
&= \sum_{\boldsymbol{s},\boldsymbol{t},\boldsymbol{s}',\boldsymbol{t}'} \sqrt{P^{(n)}(\boldsymbol{s},\boldsymbol{t})}\sqrt{P^{(n)}(\boldsymbol{s}',\boldsymbol{t}')}(-1)^{(\boldsymbol{t}-\boldsymbol{t}')\cdot\boldsymbol{x}}\langle\boldsymbol{x}+\boldsymbol{s}'|\boldsymbol{x}+\boldsymbol{s}\rangle|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s}',\boldsymbol{t}')| \\
&= \sum_{\boldsymbol{s},\boldsymbol{t},\boldsymbol{t}'} \sqrt{P^{(n)}(\boldsymbol{s},\boldsymbol{t})}\sqrt{P^{(n)}(\boldsymbol{s},\boldsymbol{t}')}(-1)^{(\boldsymbol{t}-\boldsymbol{t}')\cdot\boldsymbol{x}}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t}')| \\
&= \sum_{\boldsymbol{s}} P_1^{(n)}(\boldsymbol{s}) \sum_{\boldsymbol{t},\boldsymbol{t}'} \sqrt{P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})}\sqrt{P_{2|1}^{(n)}(\boldsymbol{t}'|\boldsymbol{s})}(-1)^{(\boldsymbol{t}-\boldsymbol{t}')\cdot\boldsymbol{x}}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t}')| \\
&= \sum_{\boldsymbol{s}} P_1^{(n)}(\boldsymbol{s})\rho_{\mathrm{E},\boldsymbol{s}}(\boldsymbol{x}),
\end{aligned}$$

where $\rho_{\mathrm{E},\boldsymbol{s}}(\boldsymbol{x}) := \sum_{\boldsymbol{t},\boldsymbol{t}'} \sqrt{P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})}\sqrt{P_{2|1}^{(n)}(\boldsymbol{t}'|\boldsymbol{s})}(-1)^{(\boldsymbol{t}-\boldsymbol{t}')\cdot\boldsymbol{x}}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t}')|$.

Finally, we introduce the **coherent information** $I_c(\rho;\Lambda)$ as the quantity describing the amount of the coherency kept by the quantum channel. We treat the coherency of the channel Λ, here because the channel Λ_{E} to the environment system is closely related to it. Let the input system of Λ be $\mathcal{H}_{\mathrm{A}}$, the output system be $\mathcal{H}_{\mathrm{B}}$, the state on the input system $\mathcal{H}_{\mathrm{A}}$ be ρ, and the purification of ρ by extending the input system from $\mathcal{H}_{\mathrm{A}}$ to $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{R}}$ be $|\Phi\rangle$. That is, $|\Phi\rangle$ is the pure state on $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{R}}$ satisfying $\mathrm{Tr}_{\mathrm{R}}\, |\Phi\rangle\langle\Phi| = \rho$. Then, the coherent information is given by $I_c(\rho;\Lambda) := H(\Lambda(\rho)) - H(\Lambda \otimes \mathcal{I}_{\mathrm{R}}(|\Phi\rangle\langle\Phi|))$ [24].

Using the Stinespring representation U, ρ_{E} of the channel Λ (ρ_{E} is a pure state), we obtain $H(\mathrm{Tr}_{\mathrm{BR}}\, U \otimes I(|\Phi\rangle\langle\Phi| \otimes \rho_E)U^\dagger \otimes I) = H(\Lambda \otimes \mathcal{I}_{\mathrm{R}}(|\Phi\rangle\langle\Phi|))$ because $U \otimes I(|\Phi\rangle\langle\Phi| \otimes \rho_E)U^\dagger \otimes I$ is the purification of the state $\Lambda \otimes \mathcal{I}_{\mathrm{R}}(|\Phi\rangle\langle\Phi|)$ on the system $\mathcal{H}_B \otimes \mathcal{H}_E$. Since $\mathrm{Tr}_{\mathrm{BR}}\, U \otimes I(|\Phi\rangle\langle\Phi|)U^\dagger \otimes I = \mathrm{Tr}_{\mathrm{B}}\, U\rho U^\dagger = \Lambda_{\mathrm{E}}(\rho)$, we have $I_c(\rho;\Lambda) = H(\Lambda(\rho)) - H(\Lambda_{\mathrm{E}}(\rho))$. In particular, when ρ is the completely mixed state ρ_{mix} and Λ is a Pauli channel $\Lambda[P^{(n)}]$, we obtain $I_c(\rho_{\mathrm{mix}};\Lambda[P^{(n)}]) = n - H(P^{(n)})$ because of

$$H(\Lambda_{\mathrm{E}}(\rho_{\mathrm{mix}})) = H(P^{(n)}). \tag{9.39}$$

Exercise 9.11 Show (9.39).

9.4.2 Leaked Information Without Privacy Amplification

In general, it is not easy to know what amount information the eavesdropper obtains from the information leaked to the environment system. Hence, we need to discuss the secrecy by assuming that the eavesdropper obtains all of the information leaked to the environment system of the channel Λ. In the following, we evaluate the leaked information. For this purpose, we give a framework for discussing the secrecy of the respective channel, quantitatively.

The information leaked to the eavesdropper can be evaluated by the correlation between the input and output systems of the channel Λ_{E} to the environment system. The first criterion is the Holevo mutual information given in (6.60). When the state $|x\rangle$ is generated in the input system with probability $Q^{(n)}(x)$, the quantum state of the diagonal elements of the eavesdropper's average state $\sum_x Q^{(n)}(x)\rho_{\mathrm{E},\boldsymbol{s}}(x)$ is $\sum_{\boldsymbol{t}} P^{(n)}_{2|1}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|$. Hence, due to (2) of Exercise 5.12, we have

$$H(\sum_x Q^{(n)}(x)\rho_{\mathrm{E},\boldsymbol{s}}(x))) \le H(\sum_{\boldsymbol{t}} P^{(n)}_{2|1}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|), \tag{9.40}$$

where the equality holds when $Q^{(n)}$ is the uniform distribution.

Since $\rho_{\mathrm{E},\boldsymbol{s}}(x)$ is a pure state, the Holevo mutual information is calculated as

$$\begin{aligned}
I(Q^{(n)};\Lambda_{\mathrm{E}}) :=& H(\Lambda_{\mathrm{E}}(\sum_x Q^{(n)}(x)|x\rangle\langle x|)) - \sum_x Q^{(n)}(x) H(\Lambda_{\mathrm{E}}(|x\rangle\langle x|)) \\
=& H(\sum_x Q^{(n)}(x)\sum_{\boldsymbol{s}} P^{(n)}_1(\boldsymbol{s})\rho_{\mathrm{E},\boldsymbol{s}}(x)) - \sum_x Q^{(n)}(x) H(\sum_{\boldsymbol{s}} P^{(n)}_1(\boldsymbol{s})\rho_{\mathrm{E},\boldsymbol{s}}(x)) \\
=& \sum_{\boldsymbol{s}} P^{(n)}_1(\boldsymbol{s})(-\log P^{(n)}_1(\boldsymbol{s}) + H(\sum_x Q^{(n)}(x)\rho_{\mathrm{E},\boldsymbol{s}}(x))) \\
&- \sum_x Q^{(n)}(x)\sum_{\boldsymbol{s}} P^{(n)}_1(\boldsymbol{s})(-\log P^{(n)}_1(\boldsymbol{s}) + H(\rho_{\mathrm{E},\boldsymbol{s}}(x))) \\
\le& \sum_{\boldsymbol{s}} P^{(n)}_1(\boldsymbol{s})(-\log P^{(n)}_1(\boldsymbol{s}) + H(\sum_{\boldsymbol{t}} P^{(n)}_{2|1}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|\sum_x Q^{(n)}(x)\rho_{\mathrm{E},\boldsymbol{s}}(x))) \\
&- \sum_x Q^{(n)}(x)\sum_{\boldsymbol{s}} P^{(n)}_1(\boldsymbol{s})(-\log P^{(n)}_1(\boldsymbol{s}) + H(\rho_{\mathrm{E},\boldsymbol{s}}(x))) \\
=& \sum_{\boldsymbol{s}} P^{(n)}_1(\boldsymbol{s}) H(\sum_{\boldsymbol{t}} P^{(n)}_{2|1}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|).
\end{aligned} \tag{9.41}$$

Theorem 9.4 [21, 25] *Let X_1^n and X_2^n be the random variables of the first and second parts of $\mathbb{F}_2^{2n}$, and $H_{P^{(n)}}(X_2^n|X_1^n)$ be the conditional entropy under the probability distribution $P^{(n)}$. Then, the distribution $Q^{(n)}$ for the input satisfies*

$$I(Q^{(n)};\Lambda[P^{(n)}]_{\mathrm{E}}) \le H_{P^{(n)}}(X_2^n|X_1^n) \le H_{P^{(n)}}(X) = H(P^{(n)}_2). \tag{9.42}$$

The equality in the first inequality holds when $Q^{(n)}$ is the uniform distribution P_{mix}.

Applying Inequality (6.45) to the random variable X_2^n, we obtain

$$H(P^{(n)}_2) \le (1 - P^{(n)}_2(0))n + h(1 - P^{(n)}_2(0)). \tag{9.43}$$

Theorem 9.4 implies

$$I(Q^{(n)}; \Lambda[P^{(n)}]_{\mathrm{E}}) \leq (1 - P_2^{(n)}(0))n + h(1 - P_2^{(n)}(0)). \tag{9.44}$$

Due to this inequality, we can evaluate the information leaked to the eavesdropper by the error probability $1 - P_2^{(n)}(0)$ with respect to the phase basis.

Proof of Theorem 9.4 Using (9.41), we have

$$\begin{aligned} I(Q^{(n)}; \Lambda_{\mathrm{E}}) \leq & \sum_{\boldsymbol{s}} P_1^{(n)}(\boldsymbol{s}) H(\sum_{\boldsymbol{t}} P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|) \\ & = H_{P^{(n)}}(X_2^n|X_1^n) \leq H_{P^{(n)}}(X_2^n) = H(P_2^{(n)}), \end{aligned}$$

where the final inequality follows from (6.39). The equality condition can be obtained from the equality condition of (9.40). □

Now, we define states ρ_{AE}, ρ_{A}, and ρ_{E} as

$$\rho_{\mathrm{AE}} := \sum_x Q^{(n)}(x)|x\rangle\langle x| \otimes \Lambda_{\mathrm{E}}(|x\rangle\langle x|), \quad \rho_{\mathrm{A}} := \mathrm{Tr}_{\mathrm{E}}\, \rho_{\mathrm{AE}}, \quad \rho_{\mathrm{E}} := \mathrm{Tr}_{\mathrm{A}}\, \rho_{\mathrm{AE}}.$$

Then, the Holevo mutual information $I(Q^{(n)}; \Lambda_{\mathrm{E}})$ is given as the quantum relative entropy $D(\rho_{\mathrm{AE}} \| \rho_{\mathrm{A}} \otimes \rho_{\mathrm{E}})$ between the real composite state ρ_{AE} and the product state $\rho_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$ of reduced densities.

Based on the fact, as another criterion, we consider the trace norm of the difference between ρ_{AE} and $\rho_{\mathrm{A}} \otimes \rho_{\mathrm{E}}$ as follows.[5]

$$\begin{aligned} d_1(Q^{(n)} : \Lambda_{\mathrm{E}}) := & \|\rho_{\mathrm{AE}} - \rho_{\mathrm{A}} \otimes \rho_{\mathrm{E}}\|_1 \\ & = \sum_x Q^{(n)}(x) \|\Lambda_{\mathrm{E}}(|x\rangle\langle x|) - \Lambda_{\mathrm{E}}(\sum_x Q^{(n)}(x)|x\rangle\langle x|)\|_1. \end{aligned} \tag{9.45}$$

Taking the maximum for the trace norm, we obtain the following criteiron.

$$d_{1,\max}(Q^{(n)} : \Lambda_{\mathrm{E}}) := \max_{x,x' : Q^{(n)}(x)>0} \|\Lambda_{\mathrm{E}}(|x\rangle\langle x|) - \Lambda_{\mathrm{E}}(|x'\rangle\langle x'|)\|_1.$$

This quantity represents the best situation for the eavesdropper. Then, the following theorem holds.[6]

[5] Renner [26] proposed the criterion $\|\rho_{\mathrm{AE}} - \rho_{\mathrm{mix}} \otimes \rho_{\mathrm{E}}\|_1$ so called universal composability, in which, the reduced density ρ_{A} is replaced by the completely mixed state ρ_{mix}. In our case, since ρ_{A} is the completely mixed state, both criteria coincide with each other.

[6] An evaluation formula slightly different from Theorem 9.5 is known [27].

Theorem 9.5

$$d_1(P_{\mathrm{mix}} : \Lambda[P^{(n)}]_{\mathrm{E}}) \le 3\sqrt{1 - P_2^{(n)}(0)} \tag{9.46}$$

$$d_{1,\max}(Q^{(n)} : \Lambda[P^{(n)}]_{\mathrm{E}}) \le 4\sqrt{1 - P_2^{(n)}(0)}. \tag{9.47}$$

Proof of Theorem 9.5 Since the matrix of the diagonal elements of $\rho_{\mathrm{E},\boldsymbol{s}}(x)$ is $\sum_{\boldsymbol{t}} P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|$, applying (A. 59) to the case of $E_i = |(\boldsymbol{s},0)\rangle\langle(\boldsymbol{s},0)|$, we obtain

$$\|\rho_{\mathrm{E},\boldsymbol{s}}(x) - \sum_{\boldsymbol{t}} P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|\|_1 \le 3\sqrt{1 - P_{2|1}^{(n)}(0|\boldsymbol{s})}. \tag{9.48}$$

Applying Jensen inequality (A.31) to the concave function $x \mapsto \sqrt{x}$, and taking the expectation with respect to $\boldsymbol{s}$, we obtain (9.46) when $Q^{(n)} = P_{\mathrm{mix}}$.

Since trace distance $d(A, B) := \frac{1}{2}\|A - B\|_1$ satisfies the axiom of the distance, applying (A.48) to the same case as the above, we obtain

$$\begin{aligned}
&\|\rho_{\mathrm{E},\boldsymbol{s}}(x) - \rho_{\mathrm{E},\boldsymbol{s}}(x')\|_1 \\
\le &\|\rho_{\mathrm{E},\boldsymbol{s}}(x) - P_{2|1}^{(n)}(0|\boldsymbol{s})|(\boldsymbol{s},0)\rangle\langle(\boldsymbol{s},0)|\|_1 \\
&+ \|P_{2|1}^{(n)}(0|\boldsymbol{s})|(\boldsymbol{s},0)\rangle\langle(\boldsymbol{s},0)| - \rho_{\mathrm{E},\boldsymbol{s}}(x')\|_1 \\
\le &4\sqrt{1 - P_{2|1}^{(n)}(0|\boldsymbol{s})}.
\end{aligned}$$

Applying Jensen inequality (A.31) to the concave function $x \mapsto \sqrt{x}$, and taking the expectation with respect to $\boldsymbol{s}$, we obtain (9.47). □

In the case of Pauli channels, the information leaked to the environment system can be evaluated by error probability $1 - P_2^{(n)}(0)$ concerning the phase basis.

This type evaluation can be extended to the case of a general quantum channel Λ as follows. We define the twirled channel $\overline{\Lambda}$ of the quantum channel Λ as

$$\overline{\Lambda}(\rho) := \sum_{\vec{s} \in \mathbb{F}_2^{2n}} \frac{1}{|\mathbb{F}_2^{2n}|} \mathsf{W}^n(-\vec{s})\Lambda(\mathsf{W}^n(\vec{s})\rho\mathsf{W}^n(\vec{s})^\dagger)\mathsf{W}^n(-\vec{s})^\dagger. \tag{9.49}$$

Then, the quantum channel $\overline{\Lambda}$ is a Pauli channel. Hence, we can choose a probability distribution $P^{(n)}$ such that $\overline{\Lambda} = \Lambda[P^{(n)}]$. The following theorem holds for the probability distribution $P^{(n)}$ [22, 28, 29].

Theorem 9.6 *The twirled channel* $\Lambda[P^{(n)}]$ *for any general quantum channel* Λ *satisfies*

$$I(P_{\mathrm{mix}}; \Lambda_{\mathrm{E}}) \le H(P_2^{(n)}) \le (1 - P_2^{(n)}(0)) \log |\mathbb{F}_2^n| + h(P_2^{(n)}(0)) \tag{9.50}$$

$$d_1(P_{\mathrm{mix}} : \Lambda_{\mathrm{E}}) \le 3\sqrt{1 - P_2^{(n)}(0)}. \tag{9.51}$$

In the above case, when the message to be transmitted obeys the uniform distribution, we obtain an evaluation similar to the case of Pauli channels under the criteria $I(P_{\mathrm{mix}}; \Lambda_{\mathrm{E}})$ and $d_1(P_{\mathrm{mix}} : \Lambda_{\mathrm{E}})$. However, when we adopt the criterion $d_{1,\max}(P_{\mathrm{mix}} : \Lambda_{\mathrm{E}})$, which focuses on the best situation for the eavesdropper, we cannot obtain a similar evaluation.

9.4.3 Leaked Information With Privacy Amplification

When the error probabilities with respect to the bit and phase bases are sufficiently small for a given quantum channel Λ, a reliable and confidential communication with small error and small leaked information is available. However, when these error probabilities are large in a given quantum channel Λ, and we use the channel Λ directly, our communication is not reliable or confidential, i.e., it might have a large error probability and be leaked to the third party. However, if we correct the errors in the bit and phase bases by applying quantum error correction explained in Sect. 9.3.2, we obtain a reliable and confidential communication with small error and small leaked information. In this scenario, the leaked information can be evaluated by the error probability in the phase basis of the quantum channel obtained by application of quantum error correction to the original quantum channel.

When a quantum channel is given as a Pauli channel $\Lambda[P^{(n)}]$, we apply the quantum error correction by the CSS code based on the classical code pair C_2 and C_1 satisfying the torsion condition. Then, we consider the decoder D based on the representative $(s_{[x]}, t_{[x],[y]})$ of $([x], [y]) \in \mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash} = (C_1 \times C_2)^*$. In this case, we can define the code space $\mathcal{H}_{([x],[y])}$ depending on the element $([x], [y]) \in \mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash} = (C_1 \times C_2)^*$. The bit basis of the code space $\mathcal{H}_{([x],[y])}$ is generated by the vectors $|[s], [x], [y]\rangle$, which depends on $[s] \in C_2^{\vdash}/C_1$. When the input state is a bit base of the code space $\mathcal{H}_{([x],[y])}$, we define two output states as follows.

$$\begin{aligned}
W_{[x],[y]}([s]) :=& \Lambda[P^{(n)}]_{\mathrm{E}}(|[s], [x], [y]\rangle\langle [s], [x], [y]|) \\
\hat{W}_{[x],[y]}([s]) :=& (D \circ \Lambda[P^{(n)}])_{\mathrm{E}}(|[s], [x], [y]\rangle\langle [s], [x], [y]|).
\end{aligned}$$

The former represents the eavesdropper's state when the eavesdropper can access only the environment system of the channel $\Lambda[P^{(n)}]$. The latter represents the eavesdropper's state when the eavesdropper can access the environment system of the decoder D as well as the environment system of $\Lambda[P^{(n)}]$. The latter is not realistic, but can be easily treated by the discussion in Sect. 9.4.2 because the channel $D \circ \Lambda[P^{(n)}]$ is the Pauli channel defined by the probability distribution $P^{(n)}\{\mathcal{J} + N\}$, as is mentioned in Sect. 9.3.2. Further, since the latter has wider accessibility than the former, the amount of information leaked to the latter is larger than that to the former. That is, the environment system of the channel $D \circ \Lambda[P^{(n)}]$ is written as $\mathcal{H}_{\mathrm{E}} \otimes \mathcal{H}_D$

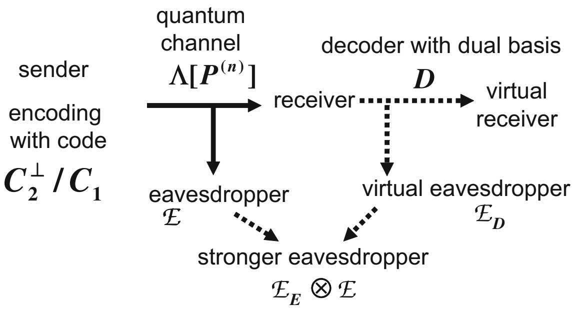


Fig. 9.4 Virtual receiver and virtual eavesdropper

when the environment system of the decoder D is $\mathcal{H}_D$ and the environment system of the channel $\Lambda[P^{(n)}]$ is $\mathcal{H}_{\mathrm{E}}$, which can be operated by the eavesdropper. Thus, the above argument is a conclusion obtained mathematically from the information processing inequality with respect to the partial trace for $\mathcal{H}_D$. The situation can be easily understood by considering the virtual receiver, the virtual eavesdropper, and the stronger eavesdropper, as is explained in Fig. 9.4. That is, the above argument can be summarized as the Holevo mutual information $I(Q; W_{[\boldsymbol{x}],[\boldsymbol{y}]})$ between the eavesdropper and the transmitted message in bit basis subject to the distribution Q on $C_2^{\perp}/C_1$ in the following inequality (9.52).

$$I(Q; W_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le I(Q; \hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \tag{9.52}$$

$$\le H(P^{(n)}\{\mathcal{J}+N\}_2) \tag{9.53}$$

$$\le (1 - P^{(n)}\{\mathcal{J}+N\}_2(0)) \log \dim \mathcal{H}_{[\boldsymbol{x}],[\boldsymbol{y}]} + h(P^{(n)}\{\mathcal{J}+N\}_2(0)), \tag{9.54}$$

where (9.53) follows from the application of Theorem 9.4 to the case of $N = C_1 \times C_2$ and $\mathcal{J} = \{(\boldsymbol{s}_{[\boldsymbol{x}]}, \boldsymbol{t}_{[\boldsymbol{x}],[\boldsymbol{y}]})\}_{([\boldsymbol{x}],[\boldsymbol{y}]) \in N^*}$. Inequality (9.54) follows from Inequality (9.43) for the binary entropy $h(p)$.

When we define $\mathcal{J}_{2,[\boldsymbol{x}]} := \{\boldsymbol{t}_{[\boldsymbol{x}],[\boldsymbol{y}]}\}_{[\boldsymbol{y}]}$, the probability $P^{(n)}\{\mathcal{J}+N\}_2(0)$ is the probability that no error occurs in the phase basis with the quantum error correction, and is calculated as

$$P^{(n)}\{\mathcal{J}+N\}_2(0) = \sum_{[\boldsymbol{x}] \in \mathbb{F}_2^n / C_2^{\perp}} P_1^{(n)}([\boldsymbol{x}]) P_{2|1}^{(n)}(\mathcal{J}_{2,[\boldsymbol{x}]} + C_2 | [\boldsymbol{x}]). \tag{9.55}$$

Then, Theorem 9.5 and the information processing inequality yield that

$$d_1(P_{\mathrm{mix}} : W_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le d_1(P_{\mathrm{mix}} : \hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le 3\sqrt{1 - P^{(n)}\{\mathcal{J}+N\}_2(0)} \tag{9.56}$$

$$d_{1,\max}(Q : W_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le d_{1,\max}(Q : \hat{W}_{[\boldsymbol{x}],[\boldsymbol{y}]}) \le 4\sqrt{1 - P^{(n)}\{\mathcal{J}+N\}_2(0)}. \tag{9.57}$$

Hence, when we choose our quantum error correcting code so that the probability $1-P^{(n)}\{\mathcal{J}+N\}_2(0)$ is sufficiently small, we obtain a reliable communication whose secrecy is guaranteed.

However, in order to perform quantum error correction, we need a quantum operation, which requires a large amount of cost. When the quantum channel is given as a Pauli channel $\Lambda[P^{(n)}]$, applying the classical error correction with the privacy amplification based on the code pair $C_1 \subset C_2^{\perp}$ in $\mathbb{F}_2^n$ explained in Sect. 9.2.5, we can guarantee the security that is equivalent with the security based on the above quantum error correcting code by the CSS code [30]. For a given $[\boldsymbol{x}] \in \mathbb{F}_2^n/C_2^{\perp}$ and $[\boldsymbol{s}] \in C_2^{\perp}/C_1$, we consider the case when Alice generates an element $\boldsymbol{s}' \in [\boldsymbol{x} + bx]$ with equal probability. In this case, Eve receives the averaged state

$$W_{\mathrm{mix},[\boldsymbol{x}]}(\boldsymbol{s}) := \sum_{\boldsymbol{s}' \in [\boldsymbol{s}]} \frac{1}{|C_1|} \Lambda[P^{(n)}]_{\mathrm{E}}(|\boldsymbol{s}' + \boldsymbol{x}\rangle\langle \boldsymbol{s}' + \boldsymbol{x}|).$$

When $[\boldsymbol{x}] = [0]$, the averaged state $W_{\mathrm{mix},[0]}(\boldsymbol{s})$ has another mixture form as follows

$$W_{\mathrm{mix},[0]}(\boldsymbol{s}) = \sum_{[\boldsymbol{y}] \in \mathbb{F}_2^n/C_1^{\perp}} \frac{1}{|C_2|} W_{[0],[\boldsymbol{y}]}([\boldsymbol{s}]).$$

Then, using the joint convexity of quantum relative entropy and the trace distance ((iv) of Lemma 5.5 and (ii) of Lemma 5.9), we can evaluate the information of the classical-quantum channel $W_{\mathrm{mix},[0]}$ from Alice to Eve, which can be regarded as the leaked information to Eve [21, 27].

$$\begin{aligned} I(Q; W_{\mathrm{mix},[0]}) &\le \sum_{[\boldsymbol{y}] \in \mathbb{F}_2^n/C_1^{\perp}} \frac{1}{|C_2|} I(Q : W_{[0],[\boldsymbol{y}]}) \\ d_1(Q : W_{\mathrm{mix},[0]}) &\le \sum_{[\boldsymbol{y}] \in \mathbb{F}_2^n/C_1^{\perp}} \frac{1}{|C_2|} d_1(Q : W_{[0],[\boldsymbol{y}]}) \\ d_{1,\max}(Q : W_{\mathrm{mix},[0]}) &\le \sum_{[\boldsymbol{y}] \in \mathbb{F}_2^n/C_1^{\perp}} \frac{1}{|C_2|} d_{1,\max}(Q : W_{[0],[\boldsymbol{y}]}). \end{aligned}$$

Thus, due to (9.52), (9.54), (9.56), and (9.57), the respective right hand sides can be upperly bounded by the right hand sides of (9.54), (9.56), and (9.57).

Now, we define

$$\delta_{P^{(n)}}[[C_1 \times C_2]] := 1 - \max_{\mathcal{J}=\{\vec{s}_x\}_{x \in (C_1 \times C_2)^*}} P^{(n)}\{\mathcal{J} + C_1 \times C_2\}_2(0) \tag{9.58}$$

for a given code pair $C_1 \subset C_2^{\perp}$ in $\mathbb{F}_2^n$. Then, the following theorem holds.

Theorem 9.7 *When we apply the classical error correction with the privacy amplification based on the code pair $C_1 \subset C_2^{\vdash}$ in $\mathbb{F}_2^n$ to the Pauli channel $\Lambda[P^{(n)}]$, the following relation holds for an arbitrary probability distribution Q on the input system $C_2^{\vdash}/C_1$.*

$$\begin{aligned} I(Q; W_{\mathrm{mix},[0]}) \le & \delta_{P^{(n)}}[[C_1 \times C_2]] \log \dim \mathcal{H}_0 + h(\delta_{P^{(n)}}[[C_1 \times C_2]]) \\ d_1(Q : W_{\mathrm{mix},[0]}) \le & 3\sqrt{\delta_{P^{(n)}}[[C_1 \times C_2]]} \\ d_{1,\max}(Q : W_{\mathrm{mix},[0]}) \le & 4\sqrt{\delta_{P^{(n)}}[[C_1 \times C_2]]}. \end{aligned}$$

On the other hand, similar to the case of a Pauli channel, we define the output states $W_{[\boldsymbol{x}],[\boldsymbol{y}]}([\boldsymbol{s}])$ and $W_{\mathrm{mix},[\boldsymbol{x}]}(\boldsymbol{s})$ for the environment system of the general quantum channel Λ. Then, we can show the following theorem by using Theorem 9.6 [22].

Theorem 9.8 *When we denote the twirled channel of a general quantum channel Λ by $\Lambda[P^{(n)}]$, we obtain*

$$\begin{aligned} \sum_{[\boldsymbol{x}] \in \mathbb{F}_2^n / C_2^{\vdash}} \frac{1}{|C_2|} I(Q; W_{\mathrm{mix},[\boldsymbol{x}]}) \le & \delta_{P^{(n)}}[[C_1 \times C_2]] \log \dim \mathcal{H}_0 \\ & + h(\delta_{P^{(n)}}[[C_1 \times C_2]]) \qquad (9.59) \\ \sum_{[\boldsymbol{x}] \in \mathbb{F}_2^n / C_2^{\vdash}} \frac{1}{|C_2|} d_1(P_{\mathrm{mix}} : W_{\mathrm{mix},[\boldsymbol{x}]}) \le & 3\sqrt{\delta_{P^{(n)}}[[C_1 \times C_2]]}. \qquad (9.60) \end{aligned}$$

Since $(C_1 \times C_2)^*$ is isomorphic to $\mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash}$, assuming that $\vec{s}_{x,y}$ has the form $(\boldsymbol{s}_x, \boldsymbol{t}_y)$ for $(x, y) \in \mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash}$, we have the following from (9.55).

$$\begin{aligned} & P^{(n)}\{\{(\boldsymbol{s}_x, \boldsymbol{t}_y)\}_{(x,y)\in \mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash}} + C_1 \times C_2\}_2(0) \\ & \qquad = P_2^{(n)}(\{\boldsymbol{t}_y\}_{y \in \mathbb{F}_2^n/C_1^{\vdash}} + C_2). \qquad (9.61) \end{aligned}$$

because the probability distribution of the second input of $P^{(n)}\{\{(\boldsymbol{s}_x, \boldsymbol{t}_y)\}_{(x,y)\in \mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash}} + C_1 \times C_2\}$ can be characterized by the distribution $P_2^{(n)}$ of the second input.

Hence, comparing the range of the maximization with respect to $\mathcal{J} = \{\vec{s}_x\}_{x \in (C_1 \times C_2)^*}$, we obtain the inequality

$$\delta_{P^{(n)}}[[C_1 \times C_2]] \le 1 - \max_{\mathcal{J}_2 = \{\boldsymbol{t}_y\}_{y \in \mathbb{F}_2^n/C_1^{\vdash}}} P_2^{(n)}(\mathcal{J}_2 + C_2) = \delta_{P_2^{(n)}}[C_1^{\vdash}/C_2]. \qquad (9.62)$$

When the errors in the bit and phase bases are independent in the probability distribution $P^{(n)}$, even when the representative $\vec{s}_{(x,y)}$ has the general form $(\boldsymbol{s}_{x,y}, \boldsymbol{t}_{x,y})$, Relation (9.55) yields

$$P^{(n)}\{\{(\boldsymbol{s}_{x,y}, \boldsymbol{t}_{x,y})\}_{(x,y)\in \mathbb{F}_2^n/C_2^{\vdash} \times \mathbb{F}_2^n/C_1^{\vdash}} + C_1 \times C_2\}_2(0)$$

$$= \sum_{x \in \mathbb{F}_2^n / C_2^{\vdash}} P_1^{(n)}(x) P_2^{(n)}(\{\boldsymbol{t}_{x,y}\}_{y \in \mathbb{F}_2^n / C_1^{\vdash}} + C_2), \tag{9.63}$$

which implies the equality in (9.62).

On the other hand, when we know only the marginal distribution $P_2^{(n)}$ and do not know the correlation between the bit and phase bases while there exists a stochastic correlation between both bases, we can evaluate only $\delta_{P^{(n)}}[[C_1 \times C_2]]$. However, since Relation (9.62) holds, we can use the formulas (9.59) and (9.60) with substituting $\delta_{P_2^{(n)}}[C_1^{\vdash}/C_2]$ into $\delta_{P^{(n)}}[[C_1 \times C_2]]$.

In the following, we consider a more practical setting, in which, we can perform only operations for the bit basis. The code $C_2^{\vdash}$ is used for the error correction in the bit basis and the subcode C_1 is used for the privacy amplification in the bit basis.

For the error correction, we need to use a code whose encoding and decoding algorithms have been established because the code for the error correction has the problem of the decoding complexity. However, we do not have to consider the decoding time for the code C_1 for the privacy amplification. Hence, we choose an m-dimensional code ensemble for C_1 such that the dual code $C_1^{\vdash}$ is a 2^{-m}-universal2 extended code ensemble of C_2. The above code ensemble of C_1 is denoted by $C_{1,Z}$. Then, Theorem 9.3 yields

$$\mathrm{E}_Z \delta_{P_2^{(n)}}[C_{1,Z}^{\vdash}/C_2] \le \min_{0 \le s \le 1} 2^{\phi(s:P_2^{(n)})-m},$$

which enables us to evaluate the average performance.[7]

9.5 Application to Quantum Cryptography (Quantum Key Distribution)

Thanks to the previous discussion, when the bit and phase error rates are known, we can realize secure and reliable communication by applying the classical error correction and the privacy amplification. However, it is difficult to guarantee that the phase error rate is less than a certain level. Quantum key distribution (QKD) is a protocol enabling us to check that the phase error rate of the communication channel is less then a given threshold. Hence, the protocol enables two distinct parties to securely share secret random number. The most fundamental QKD protocol is the attachment of the classical error correction and the privacy amplification to **BB84 protocol** proposed by Bennett and Brassard in 1984 [31]. In this book, we identify quantum cryptography with quantum key distribution because we do not treat any quantum cryptographic except for quantum key distribution while quantum cryptography means all of cryptographic protocols based quantum system, in general.

[7] As another method for the security analysis, the method based on the universal2 property of the Hash function is knwon [26].

First, we describe a QKD protocol given as an attachment of the classical error correction and the privacy amplification to the original BB84 protocol, which is called modified BB84 protocol [30, 32, 33].

(1) Transmission: Alice (sender) randomly selects the bit or phase basis with probability $\frac{1}{2}$, randomly chooses a bit 0 or 1, and decides the state with the the selected basis. Then, she sends the state via the quantum channel. She repeats the process many times.

(2) Reception: Bob (receiver) randomly selects the bit or phase basis with probability $\frac{1}{2}$, and performs the measurement corresponding to the selected basis. Then, he obtains a random bit 0 or 1. He also repeats the process many times.

(3) Basis matching: Alice and Bob exchange their basis via the public channel. They keep the bits corresponding to the matched bases,[8] and discard the remaining bits.

(4) Error estimation: Alice randomly chooses check bits with the ratio α among the matched bases with respect to the both bases. She sends Bob what bits correspond to the check bits via the public channel. Alice and Bob exchange the check bits via the public channel. They estimate the bit error rate p_{bit} and the phase error rate p_{phase}.

(*) In the following, we describe the protocols for error correction and privacy amplification. While steps **(5)** and **(6)** deal with the bit basis, we apply the same process to the phase basis after steps **(5)** and **(6)**. We call the obtained bits in the bit basis the raw keys and denote their length by n. We denote Alice's and Bob's raw keys by $\boldsymbol{s}$ and $\boldsymbol{s}'$.

(5) Error correction: Alice and Bob choose a classical code $C_2^{\vdash}$ in $\mathbb{F}_2^n$ that corrects the error between $\boldsymbol{s}$ and $\boldsymbol{s}'$ dependently of the estimated bit error rate p_{bit}. They prepare a set of representatives $\{\boldsymbol{s}^2_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{F}_2^n/C_2^{\vdash}}$, which will be used for the decoding of the code space $C_2^{\vdash}$. They also prepare another set of representatives $\{\boldsymbol{s}^1_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{F}_2^n/C_2^{\vdash}}$. They exchange the informations $[\boldsymbol{s}]$, $[\boldsymbol{s}']$ in the quotient space $\mathbb{F}_2^n/C_2^{\vdash}$ via the public channel. Alice obtains the element $\boldsymbol{x} := \boldsymbol{s} - \boldsymbol{s}^1_{[\boldsymbol{s}]}$ in $C_2^{\vdash}$, and Bib obtains the element $\boldsymbol{x}' := \boldsymbol{s}' - \boldsymbol{s}^1_{[\boldsymbol{s}]} - \boldsymbol{s}^2_{[\boldsymbol{s}'-\boldsymbol{s}]}$ in $C_2^{\vdash}$.

(6) Privacy amplification Alice and Bob choose a subspace C_1 of $C_2^{\vdash}$ such that the code pair $C_1^{\vdash}/C_2$ can correct the error subject to the probability distribution $P_2^{(n)}$. Alice and Bob keep

[8] In this book, when Alice's basis is the same as Bob's basis, the basis is called matched.

the elements $[\boldsymbol{x}]$, $[\boldsymbol{x}']$ in the quotient space $C_2^{\perp}/C_1$ as the final keys, respectively.

Here, since the representatives $\{\boldsymbol{s}^2_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{F}_2^n/C_2^{\perp}}$ are used for error correction, they choose them by taking into account the complexity so that the error probability is sufficiently small. On the other hand, since the other representatives $\{\boldsymbol{s}^1_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{F}_2^n/C_2^{\perp}}$ are used for transforming $\boldsymbol{s}$ to the element $\boldsymbol{s}-\boldsymbol{s}^1_{[\boldsymbol{s}]}$ of $C_2^{\perp}$, the error probability does not depend on their choice. Hence, they can choose them with small complexity. Due to the above discussion, they need to choose the code C_2 with representatives $\{\boldsymbol{s}^2_{[\boldsymbol{s}]}\}_{[\boldsymbol{s}]\in\mathbb{F}_2^n/C_2^{\perp}}$ whose complexity is sufficiently small. Since the code space C_1 does not require the decoding, they can randomly choose C_1 under the condition that $C_2 \subset C_1^{\perp}$. More concretely, they choose $C_1^{\perp}$ as an ϵ-universal2 extended code ensemble of C_2 [6, 27].

When Λ is the quantum channel transmitting the n raw keys, the security of the obtained final keys is equivalent with the security of the message transmitted via the quantum channel Λ, which is evaluated by Theorem 9.8 [30]. Hence, when $\Lambda[P^{(n)}]$ is the twirled channel of Λ, the security can be guaranteed by use of (9.59) and (9.60) based on the probability distribution $P^{(n)}$. The process for estimating $P^{(n)}$ is Step **(4) Error estimation**. In the method, it is impossible to estimate the correlation between the phase error and the bit error even though there exists a stochastic correlation between both errors. However, due to (9.62), the security can be evaluated by (9.59) and (9.60) with replacing $\delta_{P^{(n)}}[[C_1 \times C_2]]$ by $\delta_{P_2^{(n)}}[C_1^{\perp}/C_2]$.

When C_1 is chosen from the above ensemble, the average performance can be evaluated as follows. The right hand sides of (9.59) and (9.60) are convex functions for $\delta_{P_2^{(n)}}[C_1^{\perp}/C_2]$. Letting $W^{\mathrm{E}}(\boldsymbol{x})$ be the eavesdropper's state corresponding to Alice's final key $\boldsymbol{x}$ and Q be the probability distribution of Alice's final key $\boldsymbol{x}$, we obtain the following inequality from (9.59)

$$\mathrm{E}_{C_1} I(Q, W^{\mathrm{E}}) \le (\mathrm{E}_{C_1}\delta_{P_2^{(n)}}[C_1^{\perp}/C_2]) \log d + h(\mathrm{E}_{C_1}\delta_{P_2^{(n)}}[C_1^{\perp}/C_2]), \tag{9.64}$$

where d is the size of the final keys. When Alice chooses the bits subject to the uniform distribution in Step **(1) Transmission**, Alice's final key $\boldsymbol{x}$ obeys the uniform distribution P_{mix}. Then, due to (9.60), we obtain

$$\mathrm{E}_{C_1} d_1(P_{\mathrm{mix}}, W^{\mathrm{E}}) \le 3\sqrt{\mathrm{E}_{C_1}\delta_{P_2^{(n)}}[C_1^{\perp}/C_2]}. \tag{9.65}$$

On the other hand, the above evaluation cannot be applied to the criterion $\mathrm{E}_{C_1} d_{1,\max}(P_{\mathrm{mix}}, W^{\mathrm{E}})$, which describes the best case for the eavesdropper. Hence, we need a little modification. That is, Alice generates the bit subject to the uniform distribution in Step **(1): Transmission**, and modifies Step **(5) Error correction** as follows. We call the protocol obtained from the modification **BB84 protocol with twirling modification** [21, 27].

(5)′ Error correction Alice and Bob generate random numbers from $\boldsymbol{s}$ and $\boldsymbol{s}'$ in the following way, respectively. Alice generates other random numbers $\boldsymbol{x} \in C_2^{\perp}$, and sends $\boldsymbol{y} := \boldsymbol{x} - \boldsymbol{s}$ via public channel to Bob. Bob performs the error correction to $\boldsymbol{y} + \boldsymbol{s}' = \boldsymbol{x} - \boldsymbol{s} + \boldsymbol{s}'$, and obtains the random numbers $\boldsymbol{x}' \in C_2^{\perp}$.

We denote the quantum channel transmitting the n bits raw keys by Λ. The eavesdropper's information for $\boldsymbol{x} \in \mathbb{F}_2^n$ in the above modified protocol coincides with that of the following protocol. This fact can be shown because the state in the bit basis is invariant with respect to the action of the unitary $\mathsf{W}^n(\boldsymbol{s}, 0)$.

Protocol A Alice generates the random number $\boldsymbol{x}$ subject to the uniform distribution on $C_2^{\perp}$, and the random numbers $\boldsymbol{y}$ and $\mathbf{z}$ subject to the uniform distribution on $\mathbb{F}_2^n$. She sends Bob $\boldsymbol{y}$ and $\mathbf{z}$ via the public channel. She sets the initial state to be $|\boldsymbol{x}\rangle$, and operates the unitary $\mathsf{W}^n(-\boldsymbol{y}, -\mathbf{z})$ to the initial state. Then, she sends Bob the quantum state via the quantum channel Λ. Bob receives the output state of the quantum channel Λ, operates the unitary $\mathsf{W}^n(\boldsymbol{y}, \mathbf{z})$ to the output state, measure it with the bit basis, and obtains the bit sequence $\boldsymbol{x}''$. Finally, Bob applies error correction to the bit sequence $\boldsymbol{x}''$, and obtains the bit sequence $\boldsymbol{x}' \in C_2^{\perp}$.

In the above **Protocol A**, Alice's operation is equivalent with the operation sending the bit sequence $\boldsymbol{x} \in C_2^{\perp}$ via the twirled channel $\Lambda[P^{(n)}]$ of the quantum channel Λ [19, 27].

If the eavesdropper can control the environment systems of the quantum channel Λ and knows the choice of $(\boldsymbol{y}, \mathbf{z})$, the eavesdropper's information coincides with the information in the environment system of the Pauli quantum channel $\Lambda[P^{(n)}]$. Hence, since the security analysis of BB84 protocol with twirling modification can be reduced to that of **Protocol A**, it can be reduced to the security analysis of Pauli channel $\Lambda[P^{(n)}]$, and can be analyzed by the formula (9.47). Hence, letting Q be the probability distribution of Alice's final keys $\boldsymbol{x}$, we obtain the following relation from the concavity of the right hand side of (9.47) [27].

$$\mathrm{E}_{C_1} d_{1,\max}(Q : W^{\mathrm{E}}) \leq 4\sqrt{\mathrm{E}_{C_1} \delta_{P_2^{(n)}}[C_1^{\perp}/C_2]}.$$

The true distributions $P_1^{(n)}$ and $P_2^{(n)}$ are sufficiently close to the n-trial independent and identical distributions of $(1 - p_{\mathrm{bit}}, p_{\mathrm{bit}})$ and $(1 - p_{\mathrm{phase}}, p_{\mathrm{phase}})$, which are estimated by Step **(4) Error estimation**. Thus, in order that $\mathrm{E}_{C_1} \delta_{P_2^{(n)}}[C_1^{\perp}/C_2]$ converges to 0, due to discussions in Sect. 9.3.4, it is asymptotically enough to choose the size of C_1 to be $2^{nh(p_{\mathrm{phase}})}$. If they could choose an ideal code for the code $C_2^{\perp}$ for error correction, it is enough for correcting errors to choose the size of $C_2^{\perp}$ to be $2^{nh(p_{\mathrm{bit}})}$. Hence, it is possible to attain the asymptotic secure key generation rate $1 - h(p_{\mathrm{bit}}) - h(p_{\mathrm{phase}})$.

However, in the real setting, it is impossible to make a code with infinitely many n. Hence, we need to evaluate the right hand side of (9.64) and (9.65) with a finite

n. Such an analysis is called finite size security and have been studied recently. For this analysis, we need to evaluate the relation between the true distributions $P_1^{(n)}$ and $P_2^{(n)}$ and the distribution obtained by Step **(4) Error estimation**. This evaluation requires very complicated discussion based on hypergeometric distribution [21, 34].

References

1. M.A. Nielsen, I.L. Chuang, in *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)
2. C.E. Shannon, Bell Syst. Tech. J. **27**(379–423), 623–656 (1948)
3. C.E. Shannon, W. Weaver, in *The Mathematical Theory of Communication* (University of Illinois Press, Urbana, 1949)
4. J.L. Carter, M.N. Wegman, J. Comput. System Sci. **18**, 143–154 (1979)
5. D.R. Stinson, J. Combin. Math. Combin. Comput. **42**, 3–31 (2002)
6. T. Tsurumaru, M. Hayashi, IEEE Trans. Inform. Theory **59**, 4700–4717 (2013)
7. R.G. Gallager, in *Information Theory and Reliable Communication* (Wiley, New York, 1968)
8. M. Hayashi, IEEE Trans. Inform. Theory **57**, 3989–4001 (2011)
9. A.D. Wyner, Bell Syst. Tech. J. **54**, 1355–1387 (1975)
10. H. Weyl, in *Gruppentheorie und Quantenmechanik* (Verlag von S. Hirzel, Leipzig 1928) (English translation by H. P. Robertson, The Theory of Groups and Quantum Mechanics (1931), reprinted by Dover (1950))
11. P.W. Shor, Phys. Rev. A **52**, R2493–R2496 (1995)
12. H. Barnum, H. Knill, M.A. Nielsen, IEEE. Trans. Inform. Theory **46**, 1317–1329 (2000)
13. A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, Phys. Rev. Lett. **78**, 405–408 (1997)
14. A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, IEEE Trans. Inform. Theory **44**, 1369–1387 (1998)
15. D. Gottesman, Phys. Rev. A **54**, 1862–1868 (1996)
16. M. Hamada, Int. J. Quantum Inf. **1**, 443–463 (2003)
17. A.R. Calderbank, P.W. Shor, Phys. Rev. A **54**, 1098–1105 (1996)
18. A.M. Steane, Proc. Roy. Soc. Lond. A **452**, 2551–2577 (1996)
19. M. Hamada, J. Phys. A: Math. Gen. **37**, 8303–8328 (2004)
20. S. Watanabe, T. Matsumoto, T. Uyematsu, Int. J. Quantum Inf. **4**, 935–946 (2006)
21. M. Hayashi, Phys. Rev. A **74**, 022307 (2006)
22. M. Hayashi, *A Group Theoretic Approach to Quantum Information* (Kyoritsu-shuppan, Tokyo, 2014)
23. B.W. Schumacher, Phys. Rev. A. **54**, 2614–2628 (1996)
24. B. Schumacher, M.D. Westmoreland, Phys. Rev. A **56**, 131–138 (1997)
25. T. Miyadera, Phys. Rev. A **73**, 042317 (2006)
26. R. Renner, *Security of Quantum Key Distribution* PhD thesis, ETH Zurich (2005), arXiv:quant-ph/0512258.
27. M. Hayashi, Phys. Rev. A **76**, 012329 (2007)
28. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Phys. Rev. A **54**, 3824–3851 (1996)
29. M. Hamada, Phys. Rev. A **68**, 012301 (2003)
30. P.W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441–444 (2000)
31. C.H. Bennett, G. Brassard, in *Proceeding of IEEE International Conference on Computers, Systems and Signal Processing*, (1984) pp. 175–179
32. D. Mayers, in *Advances in Cryptography: Proceedings of Crypto'96*. Lecture Notes in Computer Science, vol. 1109 (Springer, New York, 1996), pp. 343–357
33. D. Mayers, J. Assoc. Comp. Mach. **48**, 351–406 (2001)
34. M. Hayashi, T. Tsurumaru, New J. Phys. **14**, 093014 (2012)

Appendix A
Foundations of Linear Algebra and Basic Mathematics

A.1 Symbols

- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{N}$ are the sets of complex, real, integer, and natural numbers, respectively.
- The absolute value, complex conjugate, real part, and imaginary part of a complex number c are denoted by $|c|$, $\overline{c}$, $\mathrm{Re}\, c$, $\mathrm{Im}\, c$, respectively.
- We use $\forall$, $\exists$, and $\exists 1$ to mean "for all", "there exists", and "there uniquely exists", respectively. We sometimes omit the symbol $\forall$ when it is clear from the context. For statements A and B, $A \Rightarrow B$ (or $B \Leftarrow A$) means that the statement A implies statement B; $A \Leftrightarrow B$ means that A and B are equivalent; A s.t. B means A satisfying B where $s.t.$ is the abbreviation of "such that".
- $A := B$, $B =: A$, and $A \overset{def}{\Leftrightarrow} B$ mean that A is defined by B.
- For sets X, Y, the direct product is $X \times Y := \{(x, y) \mid x \in X, y \in Y\}$.

A.2 Hilbert Space and Linear Operators

In this appendix, we review a vector space, especially Hilbert space, and linear operators on it, which are necessary for the study of quantum information science in a logically closed manner as much as possible.

A.2.1 Vector Space

Let $\mathbb{K}$ be $\mathbb{R}$ (the set of real numbers) or $\mathbb{C}$ (the set of complex number).[1] We call V a **vector space** (or a **linear space**) if V entails two operations, the addition $|\psi\rangle, |\phi\rangle \in$

[1] Though $\mathbb{K}$ can be any field, but for the moment, it is enough to restrict it to $\mathbb{R}$ or $\mathbb{C}$. See Sect. A.7 for a vector space on a finite field.

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1,

$V \to |\psi\rangle + |\phi\rangle \in V$ and the scalar multiplication $|\psi\rangle \in V, a \in \mathbb{K} \to a \cdot |\psi\rangle \in V$ that satisfy the following properties (v1)–(v8)[2]:

(v1) $|\psi\rangle + |\phi\rangle = |\phi\rangle + |\psi\rangle$ (commutative law),
(v2) $|\psi\rangle + (|\phi\rangle + |\xi\rangle) = (|\psi\rangle + |\phi\rangle) + |\xi\rangle$ (associative law),
(v3) $\exists 1\ |\theta\rangle \in V$ s.t. $\forall |\psi\rangle \in V,\ |\psi\rangle + |\theta\rangle = |\psi\rangle$ (existence of the zero element),[3]
(v4) $\forall |\psi\rangle \in V, \exists 1\ |\xi\rangle \in V$ s.t. $|\psi\rangle + |\xi\rangle = |\theta\rangle$ (existence of the inverse element)[4]
(v5) $a \cdot (b \cdot |\psi\rangle) = (ab) \cdot |\psi\rangle$ (associative law),
(v6) $1 \cdot |\psi\rangle = |\psi\rangle$,
(v7) $a \cdot (|\psi\rangle + |\phi\rangle) = a \cdot |\psi\rangle + b \cdot |\phi\rangle$ (distributive law 1),
(v8) $(a + b) \cdot |\psi\rangle = a \cdot |\psi\rangle + b \cdot |\psi\rangle$ (distributive law 2),

where $a, b \in \mathbb{K}$. V is called a real (or complex) vector space if $\mathbb{K} = \mathbb{R}$ (or $\mathbb{K} = \mathbb{C}$). Elements of V and $\mathbb{K}$ are called a vector and a scalar, respectively. $|\theta\rangle$ in (v3) is called the **zero vector** and is simply denoted by $|\theta\rangle = 0$. $|\xi\rangle$ in (v4) is called the **inverse vector** of $|\psi\rangle$, and is denoted by $-|\psi\rangle$. We omit the symbol "$\cdot$" for the scalar multiplication.

Exercise A.1 Show that for all elements $|\psi\rangle$ of a vector space V, $0 \cdot |\psi\rangle = 0$ and $-1 \cdot |\psi\rangle = -|\psi\rangle$.

In the following, $|\psi\rangle, |\phi\rangle, |\xi\rangle, \ldots$ always represent vectors while a, b, c, x, y, z represent scalars, and d, k, l, m, n represent natural numbers.

Example A.1 Let $\mathbb{K}^d$ be the set of all the column vectors $|\psi\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} = (x_1, \ldots, x_d)^T$ with $x_i \in \mathbb{K}$. We can introduce an addition and a scalar multiplication on $\mathbb{K}^d$ by

$$\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_d + y_d \end{pmatrix}, \quad a \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} = \begin{pmatrix} ax_1 \\ \vdots \\ ax_d \end{pmatrix}. \tag{A.1}$$

It is easy to show that $\mathbb{K}^d$ is a vector space where the zero vector $0 = (0, \ldots, 0)^T$ and the inverse vector of $|\psi\rangle = (x_1, \ldots, x_d)^T$ is $-|\psi\rangle = (-x_1, \ldots, -x_d)^T$. (The reader should check all the properties (v1) $-$ (v8).)

By applying the associative law of the addition (v2) repeatedly, the addition of more than two vectors is defined irrespective of the order of the addition. For subsets

[2] See Sect. 2.2.2 for the notation of vector.

[3] $\exists 1$ means that there uniquely exists. You can remove the uniqueness here as it automatically follows.

[4] The uniqueness of the inverse element also automatically follows.

$\{|\psi_i\rangle\}_{i=1}^n \subset V$ and $\{a_i\}_{i=1}^n \subset \mathbb{K}$, the element $\sum_{i=1}^n a_i|\psi_i\rangle := a_1|\psi_1\rangle + \cdots a_n|\psi_n\rangle \in V$ is called **linear combination** of $\{|\psi_i\rangle\}_{i=1}^n$. If a nonempty subset W of V is closed under the addition and the scalar multiplication, i.e., $\forall|\psi\rangle, |\phi\rangle \in W, a \in \mathbb{K},\ |\psi\rangle + |\phi\rangle \in W, a|\psi\rangle \in W$, W is called a **subspace** of V. A subspace W is a vector space with the addition and the scalar multiplication of V. The **linear span** of a subset $X \subset V$ is the set of all the linear combinations of the elements of X, and is denoted by $\mathrm{span}X := \{\sum_i a_i|\psi_i\rangle \mid a_i \in \mathbb{K}, |\psi_i\rangle \in X\}$.

A set of vectors $\{|\psi_i\rangle\}_{i=1}^n$ is called **linearly independent** if $\sum_{i=1}^n a_i|\psi_i\rangle = 0 \Rightarrow \forall i, a_i = 0$; Otherwise, it is called **linearly dependent**. A vector space V is called **finite-dimensional** if there is an upper bound of the number of linearly independent vectors, and the maximum number is called the **dimension** and is denoted by $\dim V$. In the following, we assume that V is a finite-dimensional vector space, i.e., $d := \dim V < \infty$. A set of vectors $\{|\psi_i\rangle\}_{i=1}^n$ is called **complete** (or the generating system of V) if any vector $|\phi\rangle \in V$ is written by a linear combination of $\{|\psi_i\rangle\}_{i=1}^n$; $\exists a_i \in \mathbb{K}$, s.t. $|\phi\rangle = \sum_{i=1}^n a_i|\psi_i\rangle$. This is equivalent to $\mathrm{span}\,\{|\psi_i\rangle\}_{i=1}^n = V$. Moreover, $\{|\psi_i\rangle\}_{i=1}^n$ is called a **basis** of V if it is linearly independent and complete. One can show that a set of d linearly independent vectors is a basis.[5] This also implies the existence of a basis for d-dimensional vector space. Conversely, if $\{|\psi_i\rangle\}_{i=1}^n$ is a basis of d-dimensional vector space V, then $d = n$.[6]

Exercise A.2 Let $\{|\psi_i\rangle\}_{i=1}^d$ be a basis of a vector space V. For any $|\psi\rangle \in V$, show that coefficients a_i of the expansion $|\psi\rangle = \sum_i a_i|\psi_i\rangle$ are uniquely determined.

Exercise A.3 Given a linearly independent set $\{|\psi_j\rangle\}_{j=1}^n$ in a d-dimensional vector space V $(n < d)$. Show that there exists $n - d$ vectors $|\psi_{n+1}\rangle, \ldots, |\psi_d\rangle$ in V such that the set $\{|\psi_j\rangle\}_{j=1}^d$ forms a basis of V.

Exercise A.4 Let $|e_1\rangle := (1, 0, \ldots, 0)^T, |e_2\rangle := (0, 1, 0, \ldots, 0)^T, \ldots, |e_d\rangle = (0, \ldots, 0, 1)^T$. Show that $\{|e_i\rangle\}_{i=1}^d$ is a basis of $\mathbb{K}^d$. This is called the **standard basis** or **computational basis**. From this, the dimension of $\mathbb{K}^d$ is d.

[5] To show this, it is enough to see the completeness of $\{|\psi_i\rangle\}_{i=1}^d$. With an arbitrary vector $|\phi\rangle =: |\psi_0\rangle$, the set $\{|\psi_i\rangle\}_{i=0}^d$ is linearly dependent by the definition of the dimension. Thus, $\sum_{i=0}^d a_i|\psi_i\rangle = 0$ implies that at least one of $\{a_i\}$ is non-zero. Moreover, the linear independence of $\{|\psi_i\rangle\}_{i=1}^d$ implies that $a_0 \neq 0$. Therefore, we get $|\phi\rangle = |\psi_0\rangle = \sum_{i=1}^d \frac{-a_i}{a_0}|\psi_i\rangle$, which implies that $\{|\psi_i\rangle\}_{i=1}^d$ is complete.

[6] By the definition of dimension, we have $n \leq d$. Let us assume $n < d$. Let $\{|\psi'_j\rangle\}_{j=1}^d$ be a basis of V. (See footnote 5). The completeness of $\{|\psi_i\rangle\}_{i=1}^n$ implies that $|\psi'_j\rangle = \sum_{i=1}^n a_{ij}|\psi_i\rangle$ $(j = 1, \ldots, d)$ with $a_{ij} \in \mathbb{C}$. Now consider the equation $\sum_{j=1}^d x_j|\psi'_j\rangle = 0$, which implies that $0 = \sum_j x_j(\sum_i a_{ij}|\psi_i\rangle) = \sum_i(\sum_j a_{ij}x_j)|\psi_i\rangle$. So, the linear independence of $\{|\psi_i\rangle\}_{i=1}^n$ yields that $\sum_j a_{ij}x_j = 0$ $(\forall i)$. It is well-known that simultaneous linear equations of x_j have $d - r$ nontrivial solutions where r is the rank of the matrix $[a_{ji}]$. By $r \leq n < d$, $d - r > d - n > 0$. Thus, there is at least one nontrivial solution. On the other hand, the equation $\sum_{i=1}^d x_i|\psi'_i\rangle = 0$ can have only trivial solution $x_j = 0$ by the linear independence of $\{|\psi_j\rangle\}_{j=1}^d$, which leads to contradiction. Thus, we get $n = d$.

Vector spaces V_1 and V_2 on $\mathbb{K}$ are called isomorphic if there exists a bijection[7] $f\colon V_1 \to V_2$ such that f preserves the linear structure: $f(|\psi\rangle + |\phi\rangle) = f(|\psi\rangle) + f(|\phi\rangle)$, $f(a|\psi\rangle) = af(|\psi\rangle)$ for all $|\psi\rangle, |\phi\rangle \in V_1, a \in \mathbb{K}$.

Proposition A.1 *d-dimensional vector spaces on $\mathbb{K}$ are all isomorphic.*

Proof Let V_1, V_2 be d dimensional vector spaces on $\mathbb{K}$ and let $\{|\psi_i\rangle\}_{i=1}^d, \{|\phi_i\rangle\}_{i=1}^d$ be bases of V_1, V_2, respectively. Define a map $f\colon V_1 \to V_2$ by $f|\psi\rangle = f(\sum_i a_i|\psi_i\rangle) := \sum_i a_i|\phi_i\rangle$ (See Exercise A.2). Then, the bijectivity of f is trivially satisfied. The preservation of linear structure are left for readers' exercise. □

This implies that any d-dimensional vector space V on $\mathbb{K}$ is isomorphic to $\mathbb{K}^d$. In particular, using the standard basis $\{|e_i\rangle\}_{i=1}^d$ of $\mathbb{K}^d$, a bijection map $f\colon V \to \mathbb{K}^d$ is naturally defined by $f(\sum_i a_i|\psi_i\rangle) := (a_1, \ldots, a_d)^T$, which is called a **representation** of a vector by a column vector of $\mathbb{K}^d$.

A.2.2 Hilbert Space

A vector space V is called an **inner product space** if V has an operation $|\psi\rangle, |\phi\rangle \in V \to \langle\psi|\phi\rangle \in \mathbb{K}$ with the following properties (p1)-(p3):
(p1) $\langle\psi|\psi\rangle \geq 0$ (positivity); the equality holds iff $|\psi\rangle = 0$ (non-degeneracy)
(p2) $\overline{\langle\psi|\phi\rangle} = \langle\phi|\psi\rangle$ (symmetry),
(p3) $\langle\psi|a\phi + b\xi\rangle = a\langle\psi|\phi\rangle + b\langle\psi|\xi\rangle$ (linearity).[8]

In particular, when $\mathbb{K} = \mathbb{R}$ ($\mathbb{K} = \mathbb{C}$), V is called a real (complex) inner product space. When $\mathbb{K} = \mathbb{C}$, the inner products satisfying the above properties are sometimes called **(Hermitian) inner products**. From (p3), an inner product between zero vector and an arbitrary vector is zero. Applying (p3) repeatedly, we have $\langle\psi|\sum_i a_i\psi_i\rangle = \sum_i a_i\langle\psi|\psi_i\rangle$.

If $\mathbb{K} = \mathbb{C}$, from (p2) and (p3) the inner product is anti-linear for the left vector: $\langle a\phi + b\xi|\psi\rangle = \overline{a}\langle\phi|\psi\rangle + \overline{b}\langle\xi|\psi\rangle$.

An inner product space has a **norm** (a magnitude of a vector) defined by $||\psi|| := \sqrt{\langle\psi|\psi\rangle}$. A vector with a unit norm is called a **unit vector**. We say a sequence of vectors $(|\psi_n\rangle)_{n\in\mathbb{N}}$ converges to a vector $|\psi\rangle$ if $||\psi - \psi_n|| \to 0$ as $n \to \infty$.[9] A sequence of vectors $(|\psi_n\rangle)_{n\in\mathbb{N}}$ is called a **Cauchy sequence** if $||\psi_n - \psi_m|| \to 0$ as $n, m \to \infty$[10] and is called a **convergent sequence** if there

[7] A map $f\colon V_1 \to V_2$ is called **surjective**, or onto, if for all $|\psi\rangle \in V_2$ there exists $|\phi\rangle \in V_1$ such that $|\psi\rangle = f(|\phi\rangle)$. f is called **injective**, or one-to-one, if $f(|\psi\rangle) = f(|\phi\rangle)$ implies $|\psi\rangle = |\phi\rangle$. f is called **bijective** if f is surjective and injective. Note that the inverse map $f^{-1}\colon V_2 \to V_1$ is well-defined for a bijective map f.

[8] We follow the physicist convention where the linearity holds in the right element in an inner product.

[9] Namely, $\forall\epsilon > 0, \exists n_0 \in \mathbb{N}$, s.t. $\forall n \geq n_0, ||\psi - \psi_n|| < \epsilon$.

[10] Namely, $\forall\epsilon > 0, \exists n_0 \in \mathbb{N}$, s.t. $\forall n, m \geq n_0, ||\psi_n - \psi_m|| < \epsilon$.

exists a vector $|\psi\rangle \in V$ such that $||\psi - \psi_n|| \to 0$ as $n \to \infty$. An inner product space is called **complete** if any Cauchy sequence is a convergent sequence. A complete inner product space is called a **Hilbert space**. A finite-dimensional inner product space on $\mathbb{K}$ is automatically complete from the completeness of real (or complex) number [1]. Therefore, it is not necessary to distinguish an inner product space and a Hilbert space for finite-dimensional cases. In what follows, $\mathcal{H}$ denotes a d-dimensional Hilbert space.

Vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ are called **orthogonal** if $\langle\psi|\phi\rangle = 0$. A set of unit vectors $\{|\psi_i\rangle\}_{i=1}^n$ orthogonal to each other is called an **orthonormal system**. The orthonormal condition can be written as $\langle\psi_i|\psi_j\rangle = \delta_{ij}$.

We can show that an orthonormal system is linearly independent.[11] Thus, when an orthonormal system consists of d vectors, it forms a basis of a d-dimensional vector space and is called an **orthonormal basis** (or **complete orthonormal system**) and is abbreviated by **ONB** (or **CONS**).

Exercise A.5 Show that the coefficients of the expansion of $|\psi\rangle$ with respect to ONB $\{|\psi_i\rangle\}_{i=1}^d$ are $\langle\psi_i|\phi\rangle$. Namely, we have $|\psi\rangle = \sum_{i=1}^d \langle\psi_i|\phi\rangle|\psi_i\rangle$.

The **Gram-Schmidt orthogonalization** is a method to make an orthonormal system from a linearly independent set $\{|\psi_i\rangle\}_{i=1}^n$ of vectors as follows. Let $|\psi'_1\rangle := |\psi_1\rangle/||\psi_1||$ and let $|\psi'_i\rangle$ $(i = 2, \ldots, n)$ be a normalization of $|\psi_i\rangle - \sum_{j=1}^{i-1}\langle\psi'_j|\psi_i\rangle|\psi'_j\rangle$. Then, the set $\{|\psi'_i\rangle\}_{i=1}^n$ satisfies the orthonormal condition.[12] The reader should also consider the geometric meaning of the Gram-Schmidt orthogonalization.

Exercise A.6 Given an orthonormal system $\{|\psi_j\rangle\}_{j=1}^n$ of a d-dimensional vector space V, show that there exist $d-n$ vectors $|\psi_{n+1}\rangle, \ldots, |\psi_d\rangle$ in V such that $\{|\psi_j\rangle\}_{j=1}^d$ is an orthonormal basis of V.

Exercise A.7 Show $\langle\psi|\xi\rangle = \langle\psi|\chi\rangle$ $(\forall|\psi\rangle \in \mathcal{H}) \Leftrightarrow |\xi\rangle = |\chi\rangle$.

Example A.2 The set $\mathbb{K}^d$ (See Example A.1) has a natural inner product defined by

$$\langle\psi|\phi\rangle := \sum_{i=1}^{d} \overline{x_i} y_i \quad (|\psi\rangle = (x_1, \ldots, x_d)^T, |\phi\rangle = (y_1, \ldots, y_d)^T \in \mathbb{K}^d). \tag{A.2}$$

This is called the **Euclidean inner product** and $\mathbb{K}^d$ is called (real or complex) **Euclidean space**. The readers should check the properties (p1)-(p3) and also that the standard basis of $\mathbb{K}^d$ is an orthonormal basis.

[11] Taking the inner product between $|\psi_j\rangle$ $(j = 1, \ldots, d)$ and $0 = \sum_{i=1}^n a_i|\psi_i\rangle$, we get $0 = \sum_{i=1}^n a_i\langle\psi_j|\psi_i\rangle = a_j$.

[12] It follows from the linearly independence of $\{|\psi_i\rangle\}_{i=1}^n$ that the vector $|\psi_i\rangle - \sum_{j=1}^{i-1}\langle\psi'_j|\psi_i\rangle|\psi'_j\rangle$ is not the zero vector. So, we denote its normalization by $|\psi'_i\rangle$. In the following, we show the orthogonality condition of $\{|\psi'_i\rangle\}_{i=1}^n$ by induction. First, $\langle\psi'_1|\psi'_2\rangle \propto \langle\psi'_1|\psi_2 - \langle\psi'_1|\psi_2\rangle\psi'_1\rangle = \langle\psi'_1|\psi_2\rangle - \langle\psi'_1|\psi_2\rangle\langle\psi'_1|\psi'_1\rangle = 0$. Next, assume $\langle\psi'_i|\psi'_k\rangle = 0$ $(\forall i = 1, \ldots, k-1)$ for $k \geq 2$. Then, for all $i = 1, \ldots, k$, we have $\langle\psi'_i|\psi'_{k+1}\rangle \propto \langle\psi'_i|\psi_{k+1} - \sum_{j=1}^k\langle\psi'_j|\psi_{k+1}\rangle|\psi'_j\rangle\rangle = \langle\psi'_i|\psi_{k+1}\rangle - \langle\psi'_i|\psi_{k+1}\rangle\langle\psi'_i|\psi'_i\rangle = 0$. This completes the proof.

Theorem A.1 (Pythagorean Theorem) *Orthogonal vectors* $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ *satisfy*

$$||\psi + \phi||^2 = ||\psi||^2 + ||\phi||^2.$$

Proof From $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle = 0$ and the definition of norm, we have $||\psi + \phi||^2 = \langle\psi + \phi|\psi + \phi\rangle = \langle\psi|\psi\rangle + \langle\psi|\phi\rangle + \langle\phi|\psi\rangle + \langle\phi|\phi\rangle = ||\psi||^2 + ||\phi||^2$. □

Theorem A.2 (Schwarz inequality) *For any vectors* $|\psi\rangle, |\phi\rangle$,

$$|\langle\psi|\phi\rangle| \leq ||\psi||||\phi||. \tag{A.3}$$

The equality holds iff $\{|\psi\rangle, |\phi\rangle\}$ *are linearly dependent.*[13]

Proof The inequality (A.3) follows from the positivity of norm of a vector $|\xi\rangle := ||\psi||^2|\phi\rangle - \langle\psi|\phi\rangle|\psi\rangle$. The equality condition also follows from the non-degeneracy of it[14] □

We say that subspaces W_1 and W_2 of $\mathcal{H}$ are orthogonal, which is denoted by $W_1 \perp W_2$ if all vectors from W_1 and W_2 are orthogonal. Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, the set $\mathcal{H}_1 \oplus \mathcal{H}_2 := \{|\xi, \eta\rangle \mid |\xi\rangle \in \mathcal{H}_1, |\eta\rangle \in \mathcal{H}_2\}$ is a Hilbert space when the addition, scalar multiplication, and inner product are defined as

$$\begin{aligned} a|\xi, \eta\rangle &= |a\xi, a\eta\rangle \\ |\xi, \eta\rangle + |\xi', \eta'\rangle &= |\xi + \xi', \eta + \eta'\rangle \\ \langle\xi, \eta|\xi', \eta'\rangle &= \langle\xi|\xi'\rangle + \langle\eta|\eta'\rangle. \end{aligned}$$

Then, we say that the Hilbert space $\mathcal{H}_1 \oplus \mathcal{H}_2$ is the **direct sum** of two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$,

We say Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$ are **isomorphic** if there exists a bijection $f : \mathcal{H}_1 \to \mathcal{H}_2$ such that the linear structure and the inner product are preserved; $f(|\psi\rangle + |\phi\rangle) = f(|\psi\rangle) + f(|\phi\rangle)$, $f(a|\psi\rangle) = af(|\psi\rangle)$, and $\langle\psi|\phi\rangle = \langle f(|\psi\rangle)|f(|\phi\rangle)\rangle$.

Proposition A.2 *All* Hilbert *spaces with the same dimension are isomorphic.*

Proof Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be d-dimensional Hilbert space and let $\{|\psi_i\rangle\}_{i=1}^d, \{|\phi_i\rangle\}_{i=1}^d$ be ONBs of $\mathcal{H}_1$,$\mathcal{H}_2$, respectively. One can use the same map f in Proposition A.1, which satisfies the bijectivity and preservation of the linear structure. Moreover, for $|\psi\rangle = \sum_i a_i|\psi_i\rangle, |\phi\rangle = \sum_j b_j|\psi_j\rangle$, we have $\langle\psi|\phi\rangle = \sum_{i,j} \overline{a_i}b_j\langle\psi_i|\psi_j\rangle = \sum_i \overline{a_i}b_i = \sum_{i,j} \overline{a_i}b_j\langle\phi_i|\phi_j\rangle = \langle f(|\psi\rangle)|f(|\phi\rangle)\rangle$ where we have used the orthonormal condition $\langle\psi_i|\psi_j\rangle = \langle\phi_i|\phi_j\rangle = \delta_{ij}$. □

Therefore, any d-dimensional Hilbert space $\mathcal{H}$ is isomorphic to Euclidean space $\mathbb{K}^d$. In particular, by using the standard basis of $\mathcal{H}$, the map f: $\mathcal{H} \to \mathbb{K}^d$ in the above proof is written as

[13] This is equivalent to the condition that $|\psi\rangle = 0$ or there exists $a \in \mathbb{K}$ such that $|\phi\rangle = a|\psi\rangle$. Therefore, roughly speaking, this is the case where $|\psi\rangle$ and $|\phi\rangle$ have the same direction.

[14] The reader should think of the geometrical meaning of the Schwarz inequality.

$$f(|\psi\rangle) = (\langle\psi_1|\psi\rangle, \ldots, \langle\psi_d|\psi\rangle)^T \in \mathbb{K}^d. \tag{A.4}$$

Therefore, by fixing a basis, one can identify a vector of $\mathcal{H}$ to a column vector of $\mathbb{K}^d$.

A.3 Linear Operators

In this section, let V_1, V_2 be d_1, d_2-dimensional vector spaces and $\mathcal{H}, \mathcal{K}$ be d_1, d_2-dimensional Hilbert spaces, respectively.

A.3.1 Linear Operators

A map $A : V_1 \to V_2$ is called a **linear operator** if it satisfies the **linearity** condition:

$$A(a|\psi\rangle + b|\phi\rangle) = aA|\psi\rangle + bA|\phi\rangle \quad (\forall|\psi\rangle, |\phi\rangle \in \mathcal{H}, a, b \in \mathbb{K}). \tag{A.5}$$

The zero map 0: $V_1 \to V_2$ which maps arbitrary vectors of V_1 to the zero vector of V_2 and the identity map I: $V_1 \to V_1$ which maps a vector to itself are examples of linear operators. In the following, $A, B, C \cdots$ are used to denote linear operators. The set of all linear operators from V_1 to V_2 are denoted by $\mathcal{L}(V_1, V_2)$. If $V_1 = V_2$, we simply denote it by $\mathcal{L}(V_1) := \mathcal{L}(V_1, V_2)$. The **range** of A is defined as Ran $A := \{A|\psi\rangle \in V_2 \mid |\psi\rangle \in V_1\}$. The **kernel** of A is defined as Ker $A := \{|\psi\rangle \in V_1 \mid A|\psi\rangle = 0\}$. It is easy to show that a necessary and sufficient condition for A to be injective is that Ker $A = \{0\}$. Ran A, ker A are subspaces of V_2,V_1, respectively. The **rank** for A is the dimension of Ran A and is denoted by rank A.

Example A.3 A $d_2 \times d_1$ complex matrix $A = [a_{ij}]$ gives an example of a linear operator from $\mathcal{H} = \mathbb{C}^{d_1}$ to $\mathcal{K} = \mathbb{C}^{d_2}$ where the map is defined by

$$y_i = \sum_{j=1}^{d_1} a_{ij}x_j \quad (\forall i = 1, \ldots, d_2). \tag{A.6}$$

Conversely, if one uses the vector representation of (A.4) for both $\mathcal{H}$ and $\mathcal{K}$, then any linear operator from $\mathcal{H}$ to $\mathcal{K}$ is represented by a $d_2 \times d_1$ complex matrix where the map is given by (A.6). Let $\{|\psi_i\rangle\}_{i=1}^{d_1}, \{|\phi_j\rangle\}_{j=1}^{d_2}$ be ONBs of $\mathcal{H}, \mathcal{K}$ and define a matrix by $a_{ij} := \langle\phi_i|A\psi_j\rangle$. Then, we have

$$y_i := \langle\phi_i|A\psi\rangle = \langle\phi_i|A(\sum_j x_j|\psi_j\rangle)\rangle = \sum_j a_{ij}x_j \ (x_j := \langle\psi_j|\psi\rangle).$$

The matrix $[a_{ij} := \langle\phi_i|A\psi_j\rangle]$ is called the **representation matrix** of A. Therefore, by fixing bases, one can identify linear operators with matrices.[15]

There are several methods to identify a linear operator: Most directly, one can identify a linear operator A by specifying the output $A|\psi\rangle$ for an arbitrary vector $|\psi\rangle$. To do so, it is enough to specify outputs of a basis.[16]

The following properties are quite useful in comparing linear operators on Hilbert spaces:

Proposition A.3 *(i) For any $A, B \in \mathcal{L}(\mathcal{H}, \mathcal{K})$,*

$$A = B \Leftrightarrow \langle\phi|A\psi\rangle = \langle\phi|B\psi\rangle \ (\forall|\psi\rangle \in \mathcal{H}, |\phi\rangle \in \mathcal{K}).$$

(ii) For any $A, B \in \mathcal{L}(\mathcal{H})$,

$$A = B \Leftrightarrow \langle\psi|A\psi\rangle = \langle\psi|B\psi\rangle \ (\forall|\psi\rangle \in \mathcal{H}).$$

Proof (i) From Exercise A.7, we have $\langle\phi|A\psi\rangle = \langle\phi|B\psi\rangle \ (\forall\psi \in \mathcal{H}, \phi \in \mathcal{K}) \Leftrightarrow A|\psi\rangle = B|\psi\rangle \ (\forall\psi \in \mathcal{H}) \Leftrightarrow A = B$.

(ii) [$\Leftarrow$]: Note the following identity:

$$\begin{aligned}\langle\phi|A\psi\rangle = \frac{1}{4}\Big(&\langle\psi+\phi|A(\psi+\phi)\rangle - \langle\psi-\phi|A(\psi-\phi)\rangle \\ &+ i\langle\psi+i\phi|A(\psi+i\phi)\rangle - i\langle\psi-i\phi|A(\psi-i\phi)\rangle\Big).\end{aligned} \tag{A.7}$$

Using this, if $\langle\xi|A\xi\rangle = \langle\xi|B\xi\rangle$ for all $|\xi\rangle \in \mathcal{H}$, then $\langle\phi|A\psi\rangle = \langle\phi|B\psi\rangle \ (\forall|\psi\rangle \in \mathcal{H}, |\phi\rangle \in \mathcal{K})$ for all $|\psi\rangle \in \mathcal{H}, |\phi\rangle \in \mathcal{K}$; from (i), we have $A = B$.

The opposite implication [$\Rightarrow$] trivially holds. □

For finite-dimensional vector spaces V_1, V_2, if their dimensions are the same, then the surjectivity and bijectivity are equivalent.[17] Therefore, we have

$$AB = I_{V_2} \Leftrightarrow BA = I_{V_1} \tag{A.8}$$

for $A \in \mathcal{L}(V_1, V_2)$, $B \in \mathcal{L}(V_2, V_1)$. The operator B in (A.8) is called the **inverse operator** of A and is denoted by A^{-1}.

[15] One can show that a linear operator on a linear vector space can be always represented by a matrix as well. (Show this.)

[16] Letting $\{|\psi_i\rangle\}_{i=1}^d$ be a basis of V_1 and $|\psi_i\rangle \mapsto |\psi_i'\rangle := A|\psi_i\rangle$, the linearity of A automatically determines the output of A for an arbitrary $|\psi\rangle$ by $A|\psi\rangle = A(\sum_i a_i|\psi_i\rangle) = \sum_i a_i|\psi_i'\rangle$.

[17] (i) Assume that A is injective. Then, by the injectivity of A, it is easy to see that $\{A|\phi_i\rangle\}_i^d$ forms a basis of V_2 with any basis $\{|\phi_i\rangle\}_i^d$ of V_1. Thus, an arbitrary $|\psi\rangle \in V_2$ can be written as $|\psi\rangle = \sum_i y_i A|\phi_i\rangle = A(\sum_i y_i|\phi_i\rangle)$, which implies that A is surjective. (ii) Assume that A is surjective. Then, a basis of V_2 has a form $\{A|\phi_i\rangle\}_{i=1}^d$, and it is easy to see that $\{|\phi_i\rangle\}_{i=1}^d$ is also a basis of V_1. From Exercise A.2, one can show that A is injective because $\mathrm{Ker}\, A = \{0\}$ is equivalent to the injectivity of A.

A.3.2 Algebra of Linear Operators

One can naturally define an addition and a scalar multiplication of linear operators by

$$A + B \in \mathcal{L}(V_1, V_2) \overset{def}{\Leftrightarrow} (A + B)|\psi\rangle := A|\psi\rangle + B|\psi\rangle \ (\forall|\psi\rangle \in V_1) \qquad \text{(A.9)}$$

$$aA \in \mathcal{L}(V_1, V_2) \overset{def}{\Leftrightarrow} (aA)|\psi\rangle := a(A|\psi\rangle) \ (\forall|\psi\rangle \in V_1,\ a \in \mathbb{K}). \quad \text{(A.10)}$$

In the case $V_1 = V_2 := V$, a product of operators is also defined by

$$AB \in \mathcal{L}(V) \overset{def}{\Leftrightarrow} (AB)|\psi\rangle := A(B|\psi\rangle) \ (\forall|\psi\rangle \in V). \qquad \text{(A.11)}$$

The readers should check that these are indeed linear operators.

Exercise A.8 Let V_1, V_2 be d_1, d_2-dimensional vector spaces, respectively. Show that $\mathcal{L}(V_1, V_2)$ is a $d_1 d_2$-dimensional vector space with the addition (A.9) and the scalar multiplication (A.10).

A.3.3 Adjoint Operator

Proposition A.4 *For any $A \in \mathcal{L}(\mathcal{H}, \mathcal{K})$, there uniquely exists a linear operator $B \in \mathcal{L}(\mathcal{K}, \mathcal{H})$ which satisfies*

$$\langle\phi|A\psi\rangle = \langle B\phi|\psi\rangle \quad (\forall\psi \in \mathcal{H}, \phi \in \mathcal{K}). \qquad \text{(A.12)}$$

Proof Let $\{|\psi_i\rangle\}_{i=1}^{d_1}$ be an ONB of $\mathcal{H}$. Given $A \in \mathcal{L}(\mathcal{H}, \mathcal{K})$, it is easy to see that a map $B : |\phi\rangle \in \mathcal{K} \mapsto \sum_{j=1}^{d_1} \langle A\psi_j|\phi\rangle|\psi_j\rangle \in \mathcal{H}$ is a linear operator and satisfies (A.12). The uniqueness follows from Proposition A.3. □

The operator $B \in \mathcal{L}(\mathcal{K}, \mathcal{H})$ in (A.12), which is uniquely specified by $A \in \mathcal{L}(\mathcal{H}, \mathcal{K})$, is called the **adjoint operator** of A and is denoted by $B = A^\dagger$[18]:

$$\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle \quad (\forall\psi \in \mathcal{H}, \phi \in \mathcal{K}). \qquad \text{(A.13)}$$

Notice that the matrix representation of $A^\dagger$ is a conjugate transpose of the matrix representation of A.[19] Note that a set of linear operators $\mathcal{L}(\mathcal{K}, \mathcal{H})$ forms a vector

[18] It is a physics convention to use the dagger symbol † to denote an adjoint operator, while the asterisk symbol $*$ is often used in mathematics.

[19] Let $[a_{ij}] := \langle\psi_i|A\phi_j\rangle$ be a matrix representation of A. With the same bases, the matrix representation of $A^\dagger$ is $\langle\psi_i|A^\dagger\phi_j\rangle$. By using (A.13), one has $\langle\psi_i|A^\dagger\phi_j\rangle = \overline{\langle A^\dagger\phi_j|\psi_i\rangle} = \overline{\langle\phi_j|A\psi_i\rangle} = \overline{a_{ji}}$, which is the conjugate transpose of the matrix $[a_{ij}]$.

space. If vector spaces $\mathcal{H}'$, $\mathcal{K}'$ are given as sets of linear operators, e.g., $\mathcal{L}(\mathcal{K}_1, \mathcal{H}_1)$ and $\mathcal{L}(\mathcal{K}_2, \mathcal{H}_2)$, we sometimes call $A \in \mathcal{L}(\mathcal{H}', \mathcal{K}')$ a map (or a super operator) from $\mathcal{H}'$ to $\mathcal{K}'$, and $A^\dagger$ an **adjoint map** of A.

Exercise A.9 Show the following four properties for any operators $A, B \in \mathcal{L}(\mathcal{H}, \mathcal{K})$ and any complex numbers $a, b \in \mathbb{C}$: (i) $(A^\dagger)^\dagger = A$, (ii) $(A + B)^\dagger = A^\dagger + B^\dagger$, (iii) $(aA)^\dagger = \overline{a} A^\dagger$, and (iv) $(AB)^\dagger = B^\dagger A^\dagger$.

Exercise A.10 Show that $|\phi\rangle\langle\psi|^\dagger = |\psi\rangle\langle\phi|$ (See (5.5)).

A.3.4 Eigenvalues and Eigenvectors

Let $\mathcal{H}$ be the d-dimensional Hilbert space. If a linear operator A on $\mathcal{H}$ (i.e., a linear operator A from $\mathcal{H}$ to $\mathcal{H}$) and a complex number $a \in \mathbb{C}$ satisfy

$$A|\psi\rangle = a|\psi\rangle$$

with a non-zero vector $|\psi\rangle \neq 0$, the complex number a is called an **eigenvalue** of the operator A and the vector $|\psi\rangle$ is called an **eigenvector** of A belonging to the eigenvalue a. The subspace $\mathcal{E}_a := \{|\psi\rangle \in \mathcal{H} \mid A|\psi\rangle = a|\psi\rangle\}$ is called the **eigenspace** of A belonging to the eigenvalue a. There exists at least one eigenvalue for any linear operator, and at most d distinct eigenvalues.[20] We denote by $\sigma(A)$ the set of all eigenvalues of A.

A.3.5 Important Class of Linear Operators

[Normal Operators]. We say that operators $A, B \in \mathcal{L}(\mathcal{H})$ are **commutative** if $AB = BA$. An operator A is called **normal** if A and $A^\dagger$ are commutative.

Exercise A.11 Show the following properties for a normal operator $A \in \mathcal{L}(\mathcal{H})$.
(i) Let a be an eigenvalue of A with an eigenvector $|\psi\rangle$: $A|\psi\rangle = a|\psi\rangle$. Then, $\overline{a}$ is an eigenvalue of $A^\dagger$ with an eigenvector $|\psi\rangle$: $A^\dagger|\psi\rangle = \overline{a}|\psi\rangle$.
(ii) Eigenvectors of A belonging to distinct eigenvalues are orthogonal.

[Unitary Operators]. An operator $U \in \mathcal{L}(\mathcal{H}, \mathcal{K})$ is called **unitary** if it satisfies $UU^\dagger = I_\mathcal{K}$ and $U^\dagger U = I_\mathcal{H}$. When $\dim \mathcal{H} = \dim \mathcal{K}$, it is enough by (A.8) to check either $UU^\dagger = I_\mathcal{K}$ or $U^\dagger U = I_\mathcal{H}$ to show that U is unitary. A useful necessary and sufficient condition for a linear operator U to be unitary is that $\{U|\phi_i\rangle\}_{i=1}^d$ is an ONB

[20] In linear algebra, it can be shown that eigenvalues are solutions of the eigenvalue equation ($\det(x\,I - A) = 0$) with degree d for a matrix representation of A.

for any ONB $\{|\phi_i\rangle\}_{i=1}^d$ of $\mathcal{H}$.[21] Note that a unitary operator $U \in \mathcal{L}(\mathcal{H})$ is normal since $UU^\dagger = I = UU^\dagger$.

Exercise A.12 Show that for any ONB $\{|\phi_i\rangle\}_{i=1}^d$ and $\{|\psi_i\rangle\}_{i=1}^d$, there exists a unitary operator U satisfying $|\phi_i\rangle = U|\psi_i\rangle$ $(i = 1, \ldots, d)$.

[Hermitian Operators] An operator $A \in \mathcal{L}(\mathcal{H})$ is called **Hermitian** (or **self-adjoint**) if $A = A^\dagger$. A Hermitian operator is also normal since $AA^\dagger = A^2 = A^\dagger A$. The following proposition is quite useful sufficient and necessary condition for an operator to be Hermitian.

Proposition A.5 $A = A^\dagger \Leftrightarrow \langle\psi|A\psi\rangle \in \mathbb{R}$ $(\forall|\psi\rangle \in \mathcal{H})$.

Proof Assume that $A = A^\dagger$. By (A.13), the relation $\overline{\langle\psi|A\psi\rangle} = \langle A\psi|\psi\rangle = \langle\psi|A^\dagger\psi\rangle = \langle\psi|A\psi\rangle$ holds for any $|\psi\rangle$. Next, let $\langle\psi|A\psi\rangle \in \mathbb{R}$ $(\forall|\psi\rangle \in \mathcal{H})$. Then, it follows that $\langle\psi|A^\dagger\psi\rangle = \langle A\psi|\psi\rangle = \overline{\langle\psi|A\psi\rangle} = \langle\psi|A\psi\rangle$. By Proposition A.3 (ii), we have $A = A^\dagger$. □

[Positive Operators] An operator $A \in \mathcal{L}(\mathcal{H})$ is called **positive** (or **non-negative**) if it satisfies $\langle\psi|A\psi\rangle \geq 0$ for any $|\psi\rangle \in \mathcal{H}$. By $A \geq 0$ we mean that A is positive. By Proposition A.5, a positive operator is Hermitian.

Exercise A.13 Show that $B^\dagger B \geq 0$ for any $B \in \mathcal{L}(\mathcal{H})$.

[Projection Operators] An operator $P \in \mathcal{L}(\mathcal{H})$ is called a **projection operator** if it satisfies $P^2 = P = P^\dagger$. One can show that a projection operator is positive. Indeed, for any $|\psi\rangle \in \mathcal{H}$, it follows that $\langle\psi|P\psi\rangle = \langle\psi|P^2\psi\rangle = \langle P^\dagger\psi|P\psi\rangle = \langle P\psi|P\psi\rangle = ||P\psi||^2 \geq 0$.

For each subspace $W \subset \mathcal{H}$, one can construct the projection operator as follows: Let $\{|\psi_i\rangle\}_{i=1}^n$ be an ONB of W and let $P := \sum_{i=1}^n |\psi_i\rangle\langle\psi_i|$. By Exercises A.9-(ii) and A.10, one has $P = P^\dagger$, and by Exercise 5.1, and the orthonormal condition, one has $P = P^2$. We call P the projection operator onto W.[22] Note that Ran $P = W$. Conversely, for any subspace W, there uniquely exists a projection operator P such that Ran $P = W$.

The projection operator onto an eigenspace $\mathcal{E}_a$ belonging to an eigenvalue a is called the **spectral projection**.

Exercise A.14 Show that an orthonormal system $\{|\psi_i\rangle\}_{i=1}^n$ in $\mathcal{H}$ is complete if and only if $\sum_{i=1}^n |\psi_i\rangle\langle\psi_i| = I$.

Exercise A.15 Let P_1, P_2 be projection operators onto subspaces W_1, W_2 which are orthogonal to each other. Show that the projection operator onto $W_1 \oplus W_2$ is $P_1 + P_2$.

Exercise A.16 Show that the eigenvalues of a Hermitian operator, a unitary operator, a positive operator, a projection operator are real numbers, complex numbers with the absolute value 1, non-negative real numbers, and 0 or 1, respectively.

[21] Show this. [Hint: For a unitary operator U, note the relation $\langle U\phi_i|U\phi_j\rangle = \langle\phi_i|U^\dagger U\phi_j\rangle = \langle\phi_i|\phi_j\rangle$.

[22] One can also define P by the operator to map any vector to the nearest vector on W.

A.3.6 Spectral Decomposition

In this section, let $\mathcal{H}$ be a d-dimensional Hilbert space and $A, B \in \mathcal{L}(\mathcal{H})$ be normal operators on $\mathcal{H}$. A subspace $W \subset \mathcal{H}$ is called an **invariant subspace** of the operator A if W is closed under the operation of A, namely, for any $|\psi\rangle \in W$, we have $A|\psi\rangle \in W$.

Lemma A.1 *An eigenspace $\mathcal{E}_a$ of a normal operator A is an invariant subspace of both A and $A^\dagger$.*

Proof Suppose $|\psi\rangle \in \mathcal{E}_a$, i.e., $A|\psi\rangle = a|\psi\rangle$. Since $\mathcal{E}_a$ is a subspace, and is closed under the operation of a scalar multiplication, $A|\psi\rangle \in \mathcal{E}_a$. Thus, $\mathcal{E}_a$ is an invariant subspace of A. Next, by Exercise A.11-(i), we have $A^\dagger|\psi\rangle = \overline{a}|\psi\rangle \in \mathcal{E}_a$ with the same reasoning above. Thus, $\mathcal{E}_a$ is also an invariant subspace of $A^\dagger$. □

The **orthogonal complementary space** of a subspace W is the set of all vectors orthogonal to any vectors from W and is denoted by $W^\perp$.

$$W^\perp := \{|\psi\rangle \in \mathcal{H} \mid \langle\psi|\phi\rangle = 0 \ \forall|\phi\rangle \in W\}.$$

Let A be a normal operator and define $\mathcal{E} := \oplus_{a\in\sigma(A)}\mathcal{E}_a$, which is the orthogonal sums of all eigenspaces $\mathcal{E}_a$ belonging to eigenvalues $a \in \sigma(A)$. Remind that $\mathcal{E}_a \perp \mathcal{E}_{a'}$ $(a \neq a')$ by Exercise A.11-(ii). Then, we have the following lemma:

Lemma A.2 *The orthogonal complementary space $\mathcal{E}^\perp$ of $\mathcal{E}$ is an invariant subspace of A.*

Proof Fix an arbitrary element $|\psi\rangle \in \mathcal{E}^\perp$. For any vector $|\phi\rangle \in \mathcal{E}$, we have $A^\dagger|\phi\rangle \in \mathcal{E}$ by Lemma A.1, and thus $\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle = 0$. This shows that $A|\psi\rangle \in \mathcal{E}^\perp$. □

Proposition A.6 *Suppose A is a normal operator and let P_a $(a \in \sigma(A))$ be the spectral projections. Then we have*

$$\sum_{a\in\sigma(A)} P_a = I \text{ (completeness)}, \tag{A.14}$$

$$P_a P_b = \delta_{ab} P_a \ (a, b \in \sigma(A)) \text{ (orthonormality)}. \tag{A.15}$$

Proof Notice that $\sum_{a\in\sigma(A)} P_a$ is the projection operator onto the subspace $\mathcal{E} = \oplus_{a\in\sigma(A)}\mathcal{E}_a$ by Exercise A.15. From this fact, the condition (A.14) is equivalent to $\mathcal{E} = \mathcal{H}$. Suppose, on the contrary, $\mathcal{E} \neq \mathcal{H}$, then the dimension of $\mathcal{E}^\perp$ is greater or equal to 1. By Lemma A.2, $\mathcal{E}^\perp$ is an invariant subspace of A, one can define the linear operator $\tilde{A}$ on $\mathcal{E}^\perp$ by restricting the operation of A to $\mathcal{E}^\perp$. Note that any linear operator has at least one eigenvalue and its eigenvector: Let $\tilde{A}|\phi\rangle = a|\phi\rangle, \ 0 \neq |\phi\rangle \in \mathcal{E}^\perp$. However, as $\tilde{A}$ is the restriction of A to $\mathcal{E}^\perp$, we have also $A|\phi\rangle = a|\phi\rangle$. The space $\mathcal{E}$ is already constructed by summing all the eigenspaces, which yields contradiction. Thus we have $\mathcal{E} = \mathcal{H}$ and the condition (A.14) has been shown.

Condition (A.15) immediately follows from the property of projection operator and Exercise A.11-(ii). □

Theorem A.3 (Spectral decomposition theorem) *Any normal operator A can be written in the form*

$$A = \sum_{a\in\sigma(A)} aP_a, \tag{A.16}$$

where P_a is a projection satisfying $P_aP_b = \delta_{ab}P_a$. This is called the ***spectral decomposition*** *of A.*[23]

Proof We show that, for any $|\psi\rangle \in \mathcal{H}$, $A|\psi\rangle = (\sum_{a\in\sigma(A)} aP_a)|\psi\rangle$ in order to prove (A.16). By (A.14), we have $A|\psi\rangle = A(\sum_a P_a)|\psi\rangle = \sum_a A(P_a|\psi\rangle)$. Since $P_a|\psi\rangle \in \mathcal{E}_a$, we have $A(P_a|\psi\rangle) = aP_a|\psi\rangle$. Therefore, $A|\psi\rangle = \sum_a a(P_a|\psi\rangle) = (\sum_a aP_a)|\psi\rangle$. Orthonormality of $\{P_a\}$ is already proved in Proposition A.6. □

Corollary A.1 (Eigenvalue decomposition) *Any normal operator A has an ONB $\{|\psi_i\rangle\}_{i=1}^d$ composed of eigenvectors. In particular, letting a_i be an eigenvalue corresponding to the eigenvector $|\psi_i\rangle$, the operator A can be written in the form*

$$A = \sum_{i=1}^d a_i|\psi_i\rangle\langle\psi|. \tag{A.17}$$

This is called an ***eigenvalue decomposition****.*[24]

Proof Note that the spectral projection P_a can be written as $P_a = \sum_i |\psi_i\rangle\langle\psi_i|$ with an ONB $\{|\psi_i\rangle\}$ of $\mathcal{E}_a$. Therefore, one gets (A.17) from (A.16). □

Proposition A.7 *A necessary and sufficient condition for an operator A to be positive is that the operator A is Hermitian and all eigenvalues are non negative.*

Proof We have already seen the necessity in Exercise A.16. Suppose that the operator A is Hermitian (and thus normal) and all eigenvalues are non negative. Let $A = \sum_a aP_a$ be the spectral decomposition of A. Then, noting $P_a \geq 0, a \geq 0$, we have $\langle\psi|A\psi\rangle = \sum_a a\langle\psi|P_a\psi\rangle \geq 0$ for any $|\psi\rangle \in \mathcal{H}$. This shows that A is positive. □

A vector $|\psi\rangle$ is called a **simultaneous eigenvector** of A and B if $|\psi\rangle$ is eigenvector of both A and B.

[23] The PVM $\{P_a\}$ of A derived from this theorem uniquely gives a PVM measurement of a normal operator A. In infinite-dimensional case, one can consider subnormal operator, which gives a wider class of normal operators. It can be also shown that there uniquely exists a POVM measurement of any subnormal operator [2].

[24] In fact, it can be shown that this statement is equivalent to the elementary but important result of diagonalization theorem of a normal matrix: any normal matrix A is diagonalizable with unitary matrix U by $UAU^\dagger$ (See also (A.21)).

Proposition A.8 (Simultaneous diagonalization) *If A and B are commutative normal operators, there exists an ONB $\{|\psi_i\rangle\}_{i=1}^{d}$ composed of simultaneous eigenvectors of A and B. In particular, letting a_i, b_i be eigenvalues corresponding to the eigenvector $|\psi_i\rangle$ for A and B, respectively, A and B can be written in the forms*

$$A = \sum_{i=1}^{d} a_i |\psi_i\rangle\langle\psi_i|, \quad B = \sum_{i=1}^{d} b_i |\psi_i\rangle\langle\psi_i|. \tag{A.18}$$

*This is called a **simultaneous diagonalization** of A and B.*

Proof Let $\mathcal{E}_a$ be an eigenspace of A belonging to an eigenvalue a. For any $|\psi\rangle \in \mathcal{E}_a$, $AB|\psi\rangle = BA|\psi\rangle = aB|\psi\rangle$ as A and B are commutative. This shows that $\mathcal{E}_a$ is an invariant subspace of B. From this fact, one can consider the restriction $\tilde{B}_a$ of B on $\mathcal{E}_a$, which is again normal on $\mathcal{E}_a$. By Corollary A.1, there exists ONB $\{|\psi_{a,b}\rangle\}_b$ of $\mathcal{E}_a$ composed of eigenvectors of $\tilde{B}_a$. From the completeness (A.14) of A, $\{|\psi_{a,b}\rangle\}_{a,b}$ is an ONB of $\mathcal{H}$. Using this, one easily gets (A.18). □

A.3.7 Function of Operator

In this section, for an arbitrary function $f(x)$, we define a function $f(A)$ of an operator A. While information quantities in quantum system play an important role in this book, these definitions require the concept of "a function of an operator" (See Sect. 6.3).

For any operator $A \in \mathcal{L}(\mathcal{H})$, a polynomial function of A is naturally defined as follows: Let $f(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ be a polynomial function, then $f(A) \in \mathcal{L}(\mathcal{H})$ is defined by

$$f(A) := a_n A^n + a_{n-1}A^{n-1} + \cdots a_1 A + a_0 I \tag{A.19}$$

by using (A.9)–(A.11).

When f is not necessarily a polynomial function, we recall the **spectral decomposition** $A = \sum_i a_i E_i$ of a Hermitian operator A, where $\{a_i\}$ is the set of disjoint eigenvalues and E_i is the projection corresponding to the eigenvalue a_i. Then, the Hermitian operator $f(A)$ is defined as

$$f(A) := \sum_i f(a_i) E_i, \tag{A.20}$$

where we assume that all of eigenvalues $\{a_i\}$ are contained in the domain of the function $f(x)$.

When the function f is a power x^n ($n = 0, 1, 2, \ldots$), A^n is given as the n-fold multiplication of A in (A.19). We examine whether the operator A^n defined in (A.20) coincides with the operator A^n defined in (A.19). For example, when $f(x) = x^2$, the relation $E_i E_j = \delta_{i,j} E_i$ implies that

$$A^2 = \Bigl(\sum_i a_i E_i\Bigr)\Bigl(\sum_j a_j E_j\Bigr) = \sum_{i,j} a_i a_j E_i E_j = \sum_i a_i^2 E_i = f(A).$$

Hence, the both definitions coincide with each other. Similarly, we can check that the operator A^n defined in (A.20) coincides with the operator A^n defined in (A.19) for all natural numbers n. Hence, we can check the same fact when f is a polynomial $\sum_{n=0}^N a_n x^n$. Moreover, when $f(x)$ is given as the Taylor expansion $f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!}(x-x_0)^n$, we can show that $f(A) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!}(A-x_0\, I)^n$ based on a suitable treatment for the convergence in the infinite summation. That is, we can find that $f(A)$ can be given as the Taylor expansion with replacement of x by A. Further, when $f(x) = x^{-1}$, the operator $f(A)$ coincides with the inverse operator A^{-1} of A.

Here, we see the relation of a function of an operator with its diagonalization in the d-dimensional case. We denote the eigenvalues of a given Hermitian operator A by a_k ($k = 1, 2, \ldots, d$), where we list eigenvalues with the duplicative way when there exist duplicate eigenvalues. Then, we can choose orthogonal eigenvectors $|\phi_k\rangle$ ($k = 1, 2, \ldots, d$) such that $A = \sum_{k=1}^d a_k |\phi_k\rangle\langle\phi_k|$ (eigenvalue decomposition (Corollary A.1)). When there is no duplicate eigenvalue, the eigenvalue decomposition is unique and coincides with the spectral decomposition. When we regard $|\phi_k\rangle$ as a column vector, $V = (|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_d\rangle)$ is a d-dimensional unitary operator. When we denote the diagonal matrix with diagonal elements $a_1, a_2, \ldots, a_d$ by $\mathrm{diag}(a_1, a_2, \ldots, a_d)$, the Hermitian operator A can be diagonalized as

$$A = \sum_{k=1}^d a_k |\phi_k\rangle\langle\phi_k| = V \mathrm{diag}(a_1, a_2, \ldots, a_d) V^{\dagger}. \tag{A.21}$$

Then, the Hermitian operator $f(A)$ can be diagonalized by using the same unitary operator V as follows.

$$f(A) = \sum_{k=1}^d f(a_k)|\phi_k\rangle\langle\phi_k| = V \mathrm{diag}(f(a_1), f(a_2), \ldots, f(a_d)) V^{\dagger}. \tag{A.22}$$

Therefore, we find that the Hermitian operator $f(A)$ can be obtained by the application of the function f to the eigenvalues of A after the diagonalization of A.

Now, we check whether the relation

$$f(UAU^{\dagger}) = Uf(A)U^{\dagger} \tag{A.23}$$

holds for an arbitrary unitary U. In fact, when the spectral decomposition of the Hermitian operator A is $A = \sum_i a_i E_i$, the eigenvalue decomposition of $UAU^{\dagger}$ (Corollary A.1) is given as $UAU^{\dagger} = \sum_i a_i U E_i U^{\dagger}$. Since

$$f(UAU^\dagger) = \sum_i f(a_i) U E_i U^\dagger = U \left(\sum_i f(a_i) E_i \right) U^\dagger = U f(A) U^\dagger,$$

we obtain (A.23). The relation (A.23) can be used for showing the unitary invariance of various information quantities in the quantum system. A typical function, we often use the square root $\sqrt{A} := \sum_a \sqrt{a} P_a$ for a non-negative operator A. We can easily check that $\sqrt{A}$ is a non-negative operator and satisfies $\sqrt{A}^2 = A$. Finally, we notice that for a Hermitian operator A, $\exp(iA) = \sum_a \exp(ia) P_a$ is a unitary operator.

Exercise A.17 Suppose A is a Hermitian operator and let P_a be a spectral projection belonging to an eigenvalue a. Show that P_a can be written as a polynomial function of A.

A.3.8 Trace of Operator

We can define the **trace** of an operator $A \in \mathcal{L}(\mathcal{H})$ by

$$\operatorname{Tr} A := \sum_{i=1}^{d} \langle \phi_i | A \phi_i \rangle, \tag{A.24}$$

where $\{|\phi_i\rangle\}_{i=1}^d$ is an arbitrary ONB of $\mathcal{H}$. It should be noticed that this quantity does not depend on the choice of ONBs.[25] Note also that the trace is a sum of all diagonal elements of the matrix representation $[a_{ij} = \langle \phi_i | A \phi_j \rangle]$ of A.

Exercise A.18 Suppose A is a normal operator. Using the eigenvalue decomposition of A, show that $\operatorname{Tr} A$ is the sum of eigenvalues.[26]

Proposition A.9 (Properties of Trace) *For $A, B \in \mathcal{L}(\mathcal{H})$, $a, b \in \mathbb{C}$, we have*

$$\operatorname{Tr}(aA + bB) = a \operatorname{Tr}(A) + b \operatorname{Tr}(B) \text{ (Linearity)}, \tag{A.25}$$

$$\operatorname{Tr}(AB) = \operatorname{Tr}(BA) \text{ (Cyclic Property)}, \tag{A.26}$$

$$\overline{\operatorname{Tr} A} = \operatorname{Tr} A^\dagger. \tag{A.27}$$

Proof Linearity immediately follows from the definition of the trace. To see the cyclic property, let $\{|\phi_i\rangle\}_{i=1}^d$ be an ONB. Then by using Exercise A.14, we have

[25] When we choose another ONB $\{|\psi_i\rangle\}_{i=1}^d$, Exercise A.14 guarantees that $\sum_{i=1}^d \langle \psi_i | A \psi_i \rangle = \sum_{i=1}^d \langle \psi_i | A (\sum_{j=1}^d |\phi_j\rangle\langle\phi_j|) \psi_i \rangle = \sum_{i=1}^d \sum_{j=1}^d \langle \psi_i | A \phi_j \rangle \langle \phi_j | \psi_i \rangle = \sum_{j=1}^d \langle \phi_j | (\sum_{i=1}^d |\psi_i\rangle\langle\psi_i|) A \phi_j \rangle = \sum_{j=1}^d \langle \phi_j | A \phi_j \rangle$.

[26] This is true for any linear operator. One can show this e.g. by using Jordan decomposition.

$\mathrm{Tr}(AB)$
$= \sum_i \langle \phi_i | AB\phi_i \rangle = \sum_i \langle \phi_i | A(\sum_j |\phi_j\rangle\langle\phi_j|)B\phi_i \rangle = \sum_j \langle \phi_j | B(\sum_i |\phi_i\rangle\langle\phi_i|)A\phi_j \rangle$
$= \sum_j \langle \phi_j | BA\phi_j \rangle = \mathrm{Tr}(BA)$. Finally, (A.27) follows as $\overline{\mathrm{Tr}\, A} = \sum_{i=1}^d \overline{\langle \phi_i | A\phi_i \rangle}$
$= \sum_{i=1}^d \langle \phi_i | A^\dagger \phi_i \rangle = \mathrm{Tr}\, A^\dagger$. □

Proposition A.10 *Suppose* $A, B \in \mathcal{L}(\mathcal{H})$ *be positive. Then,* $\mathrm{Tr}\, AB \geq 0$ *where the equality holds if and only if* $AB = 0$. *In particular, by putting* $B = I$, *we have* $\mathrm{Tr}\, A \geq 0$ *and also* $\mathrm{Tr}\, A = 0 \Leftrightarrow A = 0$.

Proof Let $B = \sum_{i=1}^d b_i |\phi_i\rangle\langle\phi_i|$ be an eigenvalue decomposition of B. Note that $\{|\phi_i\rangle\}_{i=1}^d$ is an ONB and $b_i \geq 0$ as $B \geq 0$. Since $A \geq 0$, we have $\mathrm{Tr}(AB) = \sum_i \langle \phi_i | AB\phi_i \rangle = \sum_i b_i \langle \phi_i | A\phi_i \rangle \geq 0$. To see the equality condition, suppose $\mathrm{Tr}(AB) = 0$. Then, it follows that $b_i > 0 \Rightarrow ||\sqrt{A}\phi_i||^2 = \langle \phi_i | A\phi_i \rangle = 0 \Rightarrow A|\phi_i\rangle = 0$. From this fact, for any $|\psi\rangle$, we have $AB|\psi\rangle = \sum_i b_i \langle \phi_i|\psi\rangle A|\phi_i\rangle$. Therefore $AB = 0$. The converse is trivial. □

We can define an inner product between operators by

$$\langle A|B\rangle_{HS} := \mathrm{Tr}(A^\dagger B). \tag{A.28}$$

This is called the **Hilbert-Schmidt inner product**.

Proposition A.11 *(i)* (A.28) *satisfies the axioms of the inner product. In particular,* $\mathcal{L}(\mathcal{H})$ *forms a* d^2*-dimensional Hilbert space with respect to the Hilbert-Schmidt inner product. (ii) For any ONB* $\{|\phi_i\rangle\}_{i=1}^d$ *of* $\mathcal{H}$, *the set of operators* $\{|\phi_i\rangle\langle\phi_j|\}_{i,j=1}^d$ *is an ONB of* $\mathcal{L}(\mathcal{H})$.

Proof (i) We show that (A.28) satisfies the axioms of inner product (p1), (p2), and (p3): (p1) From Exercise A.13 and Proposition A.10, we have $\langle A|A\rangle_{HS} = \mathrm{Tr}\, A^\dagger A \geq 0$, and $\mathrm{Tr}\, A^\dagger A \Leftrightarrow A^\dagger A = 0 \Leftrightarrow A = 0$. (p2) follows from (A.27) and $(A^\dagger B)^\dagger = B^\dagger A$. (p3) follows from the linearity of the trace (A.25). In Exercise A.8, we have seen that $\mathcal{L}(\mathcal{H})$ is a d^2-dimensional vector space. This shows that $\mathcal{L}(\mathcal{H})$ is a d^2-dimensional Hilbert space with respect to the Hilbert-Schmidt inner product.

(ii) Since the dimension of $\mathcal{L}(\mathcal{H})$ is d^2, it is enough to show that $\{|\phi_i\rangle\langle\phi_j|\}_{i,j=1}^d$ is an orthonormal system of $\mathcal{L}(\mathcal{H})$. However, by using Exercise A.19, we have $\mathrm{Tr}((|\phi_i\rangle\langle\phi_j|)^\dagger |\phi_k\rangle\langle\phi_l|) = \mathrm{Tr}(|\phi_j\rangle\langle\phi_i||\phi_k\rangle\langle\phi_l|) = \langle\phi_i|\phi_k\rangle\, \mathrm{Tr}\, |\phi_j\rangle\langle\phi_l| = \langle\phi_i|\phi_k\rangle \langle\phi_l|\phi_j\rangle = \delta_{ik}\delta_{kl}$. □

A.4 Convex Functions and Operator Convex Functions

For given two elements $v_1, v_2 \in V$ and $p \in [0, 1]$, the element $pv_1 + (1 - p)v_2$ of the vector space V is called a **convex combination** of v_1 and v_2 with respect to p. In particular, a subset W of V is called a **convex (sub)set** when the convex combination of arbitrary two elements $w_1, w_2 \in W$ with respect to an arbitrary $p \in [0, 1]$ belongs to W. Geometrically, a convex set is a subset with no "dent". For example, the set of probability distributions with d events $\{(p_i)_{i=1}^d | \sum_{i=1}^d p_i = 1, p_i \geq 0\}$ is a convex set. As is mentioned in Proposition 5.5, the set of density operators is a convex set. For a convex set W and a probability distribution $(p_i)_{i=}^d$ on d events, we can define the convex combination $\sum_{i=1}^d p_i w_i \in W$.

In particular, an element w of a convex set W is called an **extreme point** when the element w is not written as any non-trivial convex combination, that is, two elements $w_1, w_2 \in W$ and $p \in (0, 1)$ satisfy $w = pw_1 + (1 - p)w_2$ if and only if $w = w_1 = w_2$ (trivial case). Geometrically, an extreme point is a "corner" in a convex set. Here the corner is not necessarily spinous. In the set of probability distributions on d events, an extreme point is a distribution, in which, only one event occurs with probability 1. As is mentioned in Proposition 5.6, any pure state is an extreme point in the set of density operators.

A map f from a convex set W to another convex set V is called **affine** when the map f preserves the convex combination, i.e., the relation

$$f(pw_1 + (1 - p)w_2) = pf(w_1) + (1 - p)f(w_2) \tag{A.29}$$

holds for any $p \in [0, 1]$ and any elements w_1, w_2 of W.

Next, a real-valued map f on a convex set W is called a **convex function** when arbitrary two elements $w_1, w_2 \in W$ and an arbitrary $p \in (0, 1)$ satisfy

$$f(pw_1 + (1 - p)w_2) \leq pf(w_1) + (1 - p)f(w_2). \tag{A.30}$$

In particular, it is called a **strictly convex function** when the equality in (A.30) holds only when $w_1 = w_2$. The condition (A.30) is equivalent to the following condition for a probability distribution $(p_i)_{i=1}^d$ on d events and d points $w_1, \ldots, w_d \in W$:

$$f(\sum_{i=1}^d p_i w_i) \leq \sum_{i=1}^d p_i f(w_i), \tag{A.31}$$

which is called **Jensen inequality** and plays an important role for treating information quantities.

Conversely, f is called a **concave function** when $-f$ is a convex function. Similarly, f is called a strictly concave function when $-f$ is a strictly convex function. The following proposition holds for convex functions. (Its proof is omitted.)

Proposition A.12 *A twice differentiable function $f : \mathbb{R} \to \mathbb{R}$ is convex if and only if the second derivative $\frac{d^2 f}{dx^2}(x)$ satisfies $\frac{d^2 f}{dx^2}(x) \geq 0$. In particular, f is strictly convex if and only if $\frac{d^2 f}{dx^2}(x) > 0$.*

Example A.4 The function $x \mapsto x^2 \in \mathbb{R}$ is a strictly convex function. More generally, the function $x \mapsto x^{1+s} \in \mathbb{R}$ is a strictly convex function for $s \in (0, \infty)$. The function $x \mapsto x^{-s} \in \mathbb{R}$ is also a strictly convex function for $s \in (0, \infty)$. Further, the exponential function $x \mapsto e^x \in \mathbb{R}$ is also a strictly convex function. For $s \in (0, 1)$, the function $x \mapsto x^s \in \mathbb{R}$ is a strictly concave function. Also the functions $x \mapsto \log x \in \mathbb{R}$ and $x \mapsto -x \log x \in \mathbb{R}$ are strictly concave functions.

A.5 Tensor Product Hilbert Space

In this section, we explain tensor product Hilbert spaces, which is one of most important mathematical structures to study quantum information theory. This is because a composite state, including an entangled state, is described by a vector (or an operator) of the tensor product Hilbert spaces. While there are several ways to introduce the tensor product structure, we think that the following way would be most appropriate for the study of quantum information theory.

A.5.1 Tensor Product Between Vectors

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be d_1 and d_2-dimensional Hilbert spaces, respectively. The **tensor product Hilbert space** $\mathcal{H}_{12}$ of $\mathcal{H}_1$ and $\mathcal{H}_2$ is a $d_1 d_2$-dimensional Hilbert space with the **tensor product operation** $\otimes$, which is a map from $\mathcal{H}_1 \times \mathcal{H}_2$ to $\mathcal{H}_{12}$, denoted as $(|\psi\rangle, |\phi\rangle) \in \mathcal{H}_1 \times \mathcal{H}_2 \mapsto |\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_{12}$, satisfying the following properties:
(i) [Bilinearity[27]]

$$\begin{aligned}(a|\psi_1\rangle + b|\psi_2\rangle) \otimes |\phi\rangle &= a(|\psi_1\rangle \otimes |\phi\rangle) + b(|\psi_2\rangle \otimes |\phi\rangle),\\ |\psi\rangle \otimes (a|\phi_1\rangle + b|\phi_2\rangle) &= a(|\psi\rangle \otimes |\phi_1\rangle) + b(|\psi\rangle \otimes |\phi_2\rangle).\end{aligned} \tag{A.32}$$

(ii) [Inner product]

$$\langle \psi_1 \otimes \phi_1 | \psi_2 \otimes \phi_2 \rangle = \langle \psi_1 | \psi_2 \rangle \langle \phi_1 | \phi_2 \rangle. \tag{A.33}$$

The tensor product Hilbert space $\mathcal{H}_{12}$ is denoted by $\mathcal{H}_{12} := \mathcal{H}_1 \otimes \mathcal{H}_2$ using the same symbol $\otimes$ above. The reader might anticipate whether there indeed exist such Hilbert spaces or not. Later, in this section, we show that there uniquely exists a tensor product Hilbert space for arbitrary Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ up to isomorphism.

Notice that, the vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is not only a product of the form $|\psi\rangle \otimes |\phi\rangle$, but in general a linear combination of them, e.g., $|\psi\rangle \otimes |\phi\rangle + |\psi'\rangle \otimes |\phi'\rangle$. From the next

[27] The condition of bilinearity is equivalent to the conditions (a) $(|\psi_1\rangle + |\psi_2\rangle) \otimes |\phi\rangle = |\psi_1\rangle \otimes |\phi\rangle + |\psi_2\rangle \otimes |\phi\rangle$, (b) $|\psi\rangle \otimes (|\phi_1\rangle + |\phi_2\rangle) = |\psi\rangle \otimes |\phi_1\rangle + |\psi\rangle \otimes |\phi_2\rangle$, and (c) $a(|\psi\rangle \otimes |\phi\rangle) = (a|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (a|\phi\rangle)$.

proposition, one can choose an ONB of $\mathcal{H}_1 \otimes \mathcal{H}_2$ which is composed of the product forms. Therefore, the tensor product Hilbert space is linearly spanned by the product forms.

Proposition A.13 *Let $\{|\psi_i\rangle\}_{i=1}^{d_1}$ and $\{|\phi_j\rangle\}_{j=1}^{d_2}$ be ONBs of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i=1}^{d_1}{}_{j=1}^{d_2}$ is an ONB of $\mathcal{H}_1 \otimes \mathcal{H}_2$. In particular, $\mathcal{H}_1 \otimes \mathcal{H}_2 = span\{|\psi\rangle \otimes |\phi\rangle \mid |\psi\rangle \in \mathcal{H}_1, |\phi\rangle \in \mathcal{H}_2\}$.*

Proof Since the dimension of $\mathcal{H}_1 \otimes \mathcal{H}_2$ is $d_1 d_2$ from the definition of the tensor product Hilbert space, it is enough to show that $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i,j}$ is an orthonormal system. This immediately follows from (A.33). Since we have orthonormal basis of the product form, it is trivial that the vectors of the product forms span the tensor product space. □

In the following, by using the above proposition, we show the existence and also the uniqueness of the tensor product Hilbert space. Here, the uniqueness is mathematically formulated as follows: let $\otimes$ and $\otimes'$ be tensor product operations satisfying (A.32) and (A.33), and let $\mathcal{H}_{12}$ and $\mathcal{H}'_{12}$ be $d_1 d_2$-dimensional Hilbert spaces generated by the tensor product operations $\otimes$ and $\otimes'$, respectively. Then, there uniquely exists a unitary operator $U : \mathcal{H}_{12} \to \mathcal{H}'_{12}$ such that $|\psi\rangle \otimes' |\phi\rangle = U|\psi\rangle \otimes |\phi\rangle$ for $|\psi\rangle \in \mathcal{H}_1, |\phi\rangle \in \mathcal{H}_2$.

Proposition A.14 *For any Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$, there uniquely exists a tensor product Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ up to unitary equivalence.*

Proof To show the existence, let $\mathcal{H}_{12}$ be an arbitrary $d_1 d_2$-dimensional Hilbert space. By reordering indexes, one has an ONB of $\mathcal{H}_{12}$ of the form $\{|\xi_{ij}\rangle\}_{i=1}^{d_1}{}_{j=1}^{d_2}$. Let $\{|\psi_i\rangle\}_{i=1}^{d_1}$ and $\{|\phi_j\rangle\}_{j=1}^{d_2}$ be arbitrary ONBs of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, we can define the tensor product operation $\otimes$ by $|\psi\rangle = \sum_i x_i |\psi_i\rangle \in \mathcal{H}_1, |\phi\rangle = \sum_j y_j |\phi_j\rangle \in \mathcal{H}_2 \mapsto |\psi\rangle \otimes |\phi\rangle := \sum_{ij} x_i y_j |\xi_{ij}\rangle$. From the definition, (i) bilinearity and (ii) inner product property immediately follows. Therefore, $\mathcal{H}_{12}$ with $\otimes$ is indeed a tensor product Hilbert space of $\mathcal{H}_1$ and $\mathcal{H}_2$.

Next, to show the uniqueness, let $\mathcal{H}_{12}$ and $\mathcal{H}'_{12}$ be $d_1 d_2$ Hilbert spaces with tensor product operations $\otimes$ and $\otimes'$, respectively. By Proposition A.13, $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i=1}^{d_1}{}_{j=1}^{d_2}$ and $\{|\psi_i\rangle \otimes' |\phi_j\rangle\}_{i=1}^{d_1}{}_{j=1}^{d_2}$ are ONBs of $\mathcal{H}_{12}$ and $\mathcal{H}'_{12}$, respectively. Now define a unitary operator $U : \mathcal{H}_{12} \to \mathcal{H}'_{12}$ by $|\psi_i\rangle \otimes' |\phi_j\rangle = U|\psi_i\rangle \otimes |\phi_j\rangle$. Then, for any $|\psi\rangle = \sum_i x_i |\psi_i\rangle \in \mathcal{H}_1$ and $|\phi\rangle = \sum_j y_j |\phi_j\rangle \in \mathcal{H}_2$, it follows from bilinearity that $|\psi\rangle \otimes' |\phi\rangle = U|\psi\rangle \otimes |\phi\rangle$. This shows that $U' = U\otimes$. □

Let us consider a vector representation with respect to an ONB of the product forms $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i,j}$. To do this, first reorder the indexes of the ONB as $\{|\psi_1\rangle \otimes |\phi_1\rangle \ldots, |\psi_1\rangle \otimes |\phi_{d_2}\rangle, |\psi_2\rangle \otimes |\phi_1\rangle \ldots, |\psi_2\rangle \otimes |\phi_{d_2}\rangle, \ldots, |\psi_{d_1}\rangle \otimes |\phi_2\rangle \ldots, |\psi_{d_1}\rangle \otimes |\phi_{d_2}\rangle\}$, and use the representation (A.4). Then, any vector of $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be represented as a column vector of $\mathbb{C}^{d_1 d_2}$. In particular, letting $(x_1, \ldots, x_{d_1})^T := (\langle\psi_1|\psi\rangle, \ldots, \langle\psi_{d_1}|\psi\rangle)^T$ and $(y_1, \ldots, y_{d_2})^T := (\langle\phi_1|\phi\rangle, \ldots, \langle\phi_{d_2}|\phi\rangle)^T$ be vector representations of $|\psi\rangle \in \mathcal{H}_1$ and $|\phi\rangle \in \mathcal{H}_2$, we have the vector representation of $|\psi\rangle \otimes |\phi\rangle$ as

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} x_1 \begin{pmatrix} y_1 \\ \vdots \\ y_{d_2} \end{pmatrix} \\ x_2 \begin{pmatrix} y_1 \\ \vdots \\ y_{d_2} \end{pmatrix} \\ \vdots \\ x_{d_1} \begin{pmatrix} y_1 \\ \vdots \\ y_{d_2} \end{pmatrix} \end{pmatrix} \in \mathbb{C}^{d_1 d_2} . \tag{A.34}$$

See (2.31) for the example of $d_1 = d_2 = 2$.

One can introduce the tensor product Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ for more than 2 Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2, \ldots \mathcal{H}_n$ in a similar manner. We denote the tensor product Hilbert spaces for n identical Hilbert spaces $\mathcal{H}$ by $\mathcal{H}^{\otimes n}$.

Note that by Proposition A.13 any vector of $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be written in the form $|\psi\rangle = \sum_{i,j} \alpha_{ij} |\phi_i\rangle \otimes |\xi_j\rangle$ with arbitrary ONBs $\{|\phi_i\rangle\}_{i=1}^{d_1}$ and $\{|\xi_j\rangle\}_{j=1}^{d_2}$ of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Due to the following theorem, we can choose suitable ONBs of $\mathcal{H}_1$ and $\mathcal{H}_2$ so that any vector $|\psi\rangle$ of $\mathcal{H}_1 \otimes \mathcal{H}_2$ has a diagonal form $|\psi\rangle = \sum_i \alpha_{ii} |\phi_i\rangle \otimes |\xi_i\rangle$.

Theorem A.4 (Schmidt Decomposition) *For any unit vector $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, there exist $p_i > 0$ $(i = 1, \ldots, l \leq \min[d_1, d_2])$ and orthonormal systems $\{|\zeta_i\rangle\}_{i=1}^{l}$ of $\mathcal{H}_1$ and $\{|\eta_j\rangle\}_{j=1}^{l}$ of $\mathcal{H}_2$ such that*

$$|\psi\rangle = \sum_{i=1}^{l} \sqrt{p_i} |\zeta_i\rangle \otimes |\eta_i\rangle. \tag{A.35}$$

This is called the ***schmidt decomposition****. l is called the* ***schmidt rank*** *and p_is are called the* ***Schmidt coefficient****, which satisfy $\sum_{i=1}^{l} p_i = 1$.*

Proof Without loss of generality, let $d := d_1 \leq d_2$. Letting $\{|\phi_i\rangle\}_{i=1}^{d}$ and $\{|\xi_j\rangle\}_{j=1}^{d_2}$ be ONBs of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, an arbitrary state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written as $|\psi\rangle = \sum_{i,j} \alpha_{ij} |\phi_i\rangle \otimes |\xi_j\rangle = \sum_{i=1}^{d} |\phi_i\rangle \otimes |\chi_i\rangle$, where $|\chi_i\rangle := \sum_{j=1}^{d_2} \alpha_{ij} |\xi_j\rangle$. Note that, since the $d \times d$ complex matrix $X := (\langle \chi_i | \chi_j \rangle)_{ij}$ is a positive matrix,[28] all the eigenvalues of X are non-negative. Let $\sqrt{p_1} \leq \sqrt{p_2} \cdots \leq \sqrt{p_d}$ be the eigenvalues of X, and let $l (\leq d)$ be the number of non-zero eigenvalues.

Let $|\eta'_j\rangle := \sum_{j=1}^{d} U_{ji} |\chi_i\rangle, |\zeta_k\rangle := \sum_{i=1}^{d} \overline{U_{ik}} |\phi_i\rangle$ $(j, k = 1, \ldots, d)$ where $U = (U_{ij})_{ij}$ is the $d \times d$ unitary matrix which diagonalizes X. The choice of

[28] Note that for any $y = (y_1, \ldots, y_d)^T \in \mathbb{C}^d$, $\langle y | X y \rangle = \sum_{i,j} \overline{y}_j \langle \chi_i | \chi_j \rangle y_j = \langle \sum_i y_i \chi_i \sum_j y_j \chi_j \rangle \geq 0$.

the unitary matrix U guarantees that $\sum_{k,l} \overline{U_{ki}} X_{kl} U_{lj} = \sqrt{p_i}\delta_{ij}$, which implies $\langle \eta'_i | \eta'_j \rangle = \sqrt{p_i}\delta_{ij}$. Hence, $\{|\eta_j\rangle := \frac{1}{\sqrt{p_i}} |\eta'_i\rangle\}_{i=1,\dots,l}$ forms an orthonormal system of $\mathcal{H}_2$.

Since U is a unitary matrix, the equation

$$|\chi_i\rangle = \sum_k \overline{U}_{ik} |\eta'_k\rangle \tag{A.36}$$

holds, and the set $\{|\zeta_k\rangle\}_{k=1}^d$ forms ONB of $\mathcal{H}_1$. Therefore, the (A.36) and the definitions of $|\zeta_k\rangle$ and $|\eta_j\rangle$ yield

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^d |\phi_i\rangle \otimes |\chi_i\rangle = \sum_{k=1}^l \overline{U}_{ik} \sum_{i=1}^d |\phi_i\rangle \otimes |\eta'_k\rangle \\ &= \sum_{k=1}^l |\zeta_k\rangle \otimes |\eta'_k\rangle = \sum_{i=1}^l \sqrt{p_i} |\zeta_i\rangle \otimes |\eta_i\rangle, \end{aligned}$$

which is the desired argument. It is easy to check $1 = \langle \psi | \psi \rangle = \sum_i p_i$ by using orthonormality of $|\zeta_i\rangle$ and $|\eta_i\rangle$. □

A.5.2 Tensor Product of Linear Operators

For linear operators $A \in \mathcal{L}(\mathcal{H}_1)$, $B \in \mathcal{L}(\mathcal{H}_2)$, we define a linear operator $A \otimes B$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ by

$$(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) := (A|\psi\rangle) \otimes (B|\phi\rangle) \; (\forall |\psi\rangle \in \mathcal{H}_1, |\phi\rangle \in \mathcal{H}_2). \tag{A.37}$$

Notice that the operation $\otimes$ in (A.37) is indeed the tensor product operation from the Hilbert spaces $\mathcal{L}(\mathcal{H}_1)$, $\mathcal{L}(\mathcal{H}_2)$ to the Hilbert space $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ with the Hilbert-Schmidt inner product (A.28). Therefore, we have $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2) = \mathcal{L}(\mathcal{H}_1) \otimes \mathcal{L}(\mathcal{H}_2)$. In particular, all the linear operators on $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be written by the sum of linear operators of the form $A \otimes B$ ($A \in \mathcal{L}(\mathcal{H}_1)$, $B \in \mathcal{L}(\mathcal{H}_2)$).

Exercise A.19 Show that (i)$(A \otimes B)(C \otimes D) = AC \otimes BD$, (ii) $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

Exercise A.20 Show that a matrix representation of $A \otimes B$ is given by the **Kronecker product**:

$$\begin{pmatrix} a_{11} \begin{pmatrix} b_{11} & \cdots & b_{1d_2} \\ \vdots & \dots & \vdots \\ b_{d_2 1} & \cdots & b_{d_2 d_2} \end{pmatrix} & \cdots & a_{1d_1} \begin{pmatrix} b_{11} & \cdots & b_{1d_2} \\ \vdots & \dots & \vdots \\ b_{d_2 1} & \cdots & b_{d_2 d_2} \end{pmatrix} \\ \vdots & \dots & \vdots \\ a_{d_1 1} \begin{pmatrix} b_{11} & \cdots & b_{1d_2} \\ \vdots & \dots & \vdots \\ b_{d_2 1} & \cdots & b_{d_2 d_2} \end{pmatrix} & \cdots & a_{d_1 d_1} \begin{pmatrix} b_{11} & \cdots & b_{1d_2} \\ \vdots & \dots & \vdots \\ b_{d_2 1} & \cdots & b_{d_2 d_2} \end{pmatrix} \end{pmatrix},$$

where $[a_{ij}]$, $[b_{kl}]$ are matrix representations of A, B, respectively.

A.6 Advanced Topics for Operators

A.6.1 Polar Decomposition for Operators

In this section, we explain the polar decomposition for operators, the operator norm, and the trace norm. For the detail of this section, see [1, 3, 4], which is a textbook treating the details of these topics for infinite-dimensional operators as well as finite-dimensional operators. A linear operator $W : \mathcal{H} \to \mathcal{K}$ is called an **isometry** when the relation $\|Wx\| = \|x\|$ holds for any $x \in \mathcal{H}$ where the norm $\|x\|$ is defined by $\|x\| = \langle x, x\rangle^{1/2}$. Since $A = B$ is equivalent with the relation $\langle x, Ax\rangle = \langle x, Bx\rangle$ for $\forall x \in \mathcal{H}$, we can show that

$$\begin{aligned} W \text{ is an isometry} &\Leftrightarrow \forall x \in \mathcal{H},\ \langle Wx, Wx\rangle = \langle x, x\rangle \Leftrightarrow W^\dagger W = I_{\mathcal{H}} \\ &\Leftrightarrow \forall x, \forall y \in \mathcal{H},\ \langle Wx, Wy\rangle = \langle x, y\rangle. \end{aligned} \tag{A.38}$$

Hence, an isometry can be regarded as a linear operator preserving the inner product. Remember that W is a unitary if and only if the relations $W^\dagger W = I_{\mathcal{H}}$ and $WW^\dagger = I_{\mathcal{K}}$ hold. A linear operator W is called a **partial isometry** when the linear operator W restricted in $(\ker W)^\perp$ is an isometry. We also define the **absolute value** $|A|$ of an operator A as the linear operator $\sqrt{A^\dagger A}$. When we choose a linear operator $B = |A|$, we have the relations $B^\dagger B = B^2 = A^\dagger A$. Using these concepts, we give the polar decomposition theorem as follows.

Theorem A.5 (Polar decomposition theorem) For a given linear operator $A : \mathcal{H} \to \mathcal{K}$, there exists a partial isometry $W : \mathcal{H} \to \mathcal{K}$ such that $A = W|A|$. In particular, when $\dim \mathcal{H} = \dim \mathcal{K} < \infty$, W can be taken as a unitary matrix.

In order to show the above theorem, we prove the following lemma with a more general framework.

Lemma A.3 Assume that the relation $B^\dagger B = A^\dagger A$ holds for two linear operators $A : \mathcal{H} \to \mathcal{K}_1$ and $B : \mathcal{H} \to \mathcal{K}_2$. Then, there exists an isometry $W : \operatorname{Ran} B \to \operatorname{Ran} A$ such that $A = WB$.

Proof Due to the assumption, the relation

$$\begin{aligned} \|Bx\|^2 &= \langle Bx, Bx\rangle = \langle x, B^\dagger Bx\rangle \\ &= \langle x, A^\dagger Ax\rangle = \langle Ax, Ax\rangle = \|Ax\|^2 \end{aligned} \tag{A.39}$$

holds for an arbitrary vector $x \in \mathcal{H}$. Hence, we can define the linear operator $W : y = Bx \in \operatorname{Ran} B \mapsto z = Ax \in \operatorname{Ran} A$. In fact, when the vector $y \in \operatorname{Ran} B$ can be written in two different ways as $y = Bx_1 = Bx_2$, since $\|Ax_1 - Ax_2\| = \|A(x_1 - x_2)\| = \|B(x_1 - x_2)\| = 0$, we have $Wy = Ax_1 = Ax_2$, and hence, the image of y is uniquely determined. That is, W gives a map. The linearity of W is trivial from the definition. Relation (A.39) yields the relation $\ker A = \ker B$. This relation and the definition of W imply that $A = WB$. Further, Relation (A.39) guarantees that W is an isometry form $\operatorname{Ran} B$ to $\operatorname{Ran} A$. □

Next, we show Polar decomposition theorem. Apply the above lemma to the case of $B = |A|$. There exists a partial isometry $W : \operatorname{Ran} |A| \to \operatorname{Ran} A$ such that $A = W|A|$. We extend the domain of W such that $Wy = 0$ for any $y \in (\operatorname{Ran} |A|)^\perp$. Then, W is a partial isometry from $\mathcal{H}$ to $\mathcal{K}$. That is, in order to extend the domain of W to $\mathcal{H} = \operatorname{Ran} |A| \oplus (\operatorname{Ran} |A|)^\perp$, it is sufficient to define the image of W for the elements of $(\operatorname{Ran} |A|)^\perp$. In particular, there uniquely exists an extension of W such that $\ker W = (\operatorname{Ran} |A|)^\perp$.

Next, we show that we can choose the above partial isometry W as a unitary when $\dim \mathcal{H} = \dim \mathcal{K} < \infty$. Since $W : \operatorname{Ran} |A| \to \operatorname{Ran} A$ is a partial isometry, we have $\dim(\operatorname{Ran} |A|) = \dim(\operatorname{Ran} A) < \infty$. Due to the relation $\dim \mathcal{H} = \dim \mathcal{K}$, we can show that $\dim(\operatorname{Ran} |A|)^\perp = \dim(\operatorname{Ran} A)^\perp$. Now, we choose the map W such that the orthogonal basis of $(\operatorname{Ran} |A|)^\perp$ is mapped to that of $(\operatorname{Ran} A)^\perp$. Then, W is a unitary from $\mathcal{H}$ to $\mathcal{K}$. Then, we obtain Theorem A.5.

A.6.2 Operator Norm

In this section, we treat the operator norm $\|A\|$ of an operator A. We have defined the norm $\|x\| := \sqrt{\langle x, x\rangle}$ for any element $x \in \mathcal{H}$ of a Hilbert space $\mathcal{H}$ as the length of the vector x. The norm can be characterized as a function of a vector satisfying the following conditions.

Definition A.1 A function $x \in V \mapsto \|x\|$ of a vector space V over the field $\mathbb{K}$ ($= \mathbb{R}$ or $\mathbb{C}$) is called a **norm** when the relations

(i) $\|x\| \ge 0$ ($\|x\| = 0 \Leftrightarrow x = 0$)
(ii) $\|x + y\| \le \|x\| + \|y\|$

(iii) $\|\alpha x\| = |\alpha|\|x\|$

hold for any $x, y \in V$, $\alpha \in \mathbb{K}$.

Here, we should remark that there exist infinitely many norms for a given vector space V as follows. For example, the vector space $\mathbb{C}^n$ has the following norms

$$\|x\|_1 = \sum_{k=1}^{n} |x_k|, \quad \|x\|_2 = \left(\sum_{k=1}^{n} |x_k|^2\right)^{\frac{1}{2}}, \quad \|x\|_\infty = \max_{k=1,\ldots,n} |x_k|$$

for any vector $x = (x_1, \ldots, x_n)^T \in \mathbb{C}^n$. It is easily checked that the above functions satisfy the conditions for the norm. When a norm $\|\cdot\|$ is given on a vector space V, the function $d(x, y) := \|x - y\|$ satisfies the following conditions for a distance over the vector space V.

Definition A.2 A two-variable function $(x, y) \mapsto d(x, y)$ is called a **distance** when the relations

(i) (Non-negativity) $d(x, y) \geq 0$, $d(x, y) = 0 \Leftrightarrow x = y$
(ii) (Symmetry) $d(x, y) = d(y, x)$
(iii) (Triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$

hold. These relations are often called the axiom of distance.

Exercise A.21 Show that the two-variable function $d(x, y) := \|x - y\|$ satisfies the conditions for a distance when $\|x - y\|$ is a norm.

Now, we define the operator norm $\|A\|$ for an operator $A \in \mathcal{L}(\mathcal{H})$ over the Hilbert space $\mathcal{H}$ by the following.

$$\|A\| = \max_{x \in \mathcal{H}:\, x \neq 0} \frac{\|Ax\|}{\|x\|} = \max_{x \in \mathcal{H}:\, \|x\|=1} \|Ax\|. \tag{A.40}$$

Since $\|A\|$ satisfies the conditions (i)∼(iii) for a norm over the vector space $\mathcal{L}(\mathcal{H})$, it is called the **operator norm**. Since the operator norm $\|A\|$ corresponds to the norm $\|x\|_\infty$ on $\mathbb{C}^n$, it is often described by $\|A\|_\infty$. The operator norm $\|A\|$ can be regarded as the maximum expansion rate of the operator A with respect to the length $\|x\|$ of the vector x. The definition of the operator norm implies the following relation.

$$\forall x \in \mathcal{H}, \quad \|Ax\| \leq \|A\|\|x\|. \tag{A.41}$$

Exercise A.22 Show that the operator norm $\|A\|$ satisfies the conditions (i)∼(iii) for a norm.

Next, we show that the norm $\|A\|$ coincides with the maximum singular value of the operator A, i.e., the maximum eigenvalue of $|A| = \sqrt{A^\dagger A}$. Since $|A|$ is a positive operator, we choose the eigenvalues $a_1 \geq a_2 \geq \cdots \geq a_d \geq 0$ and the corresponding eigenvectors $|e_1\rangle, |e_2\rangle, \ldots, |e_d\rangle$, where $d = \dim \mathcal{H}$. Due to the eigenvalue decomposition (Corollary A.1), the relation $|A| = \sum_{k=1}^d a_k |e_k\rangle\langle e_k|$ holds. Since any normalized vector $|x\rangle$ ($\|x\| = 1$) is written as $|x\rangle = \sum_{k=1}^d x_k |e_k\rangle$ by using the coefficients $\sum_{k=1}^d |x_k|^2 = 1$, we have $|A||x\rangle = \sum_{k=1}^d a_k x_k |e_k\rangle$. Hence, the relation (A.39) with the case $B = |A|$ yields the following equation.

$$\|Ax\|^2 = \||A|x\|^2 = \sum_k a_k^2 |x_k|^2 \quad \Big(\sum_k |x_k|^2 = 1\Big). \tag{A.42}$$

The maximum value of the above is $\|A\|^2 = a_1^2$, which can be attained when $|x\rangle = |e_1\rangle$. Hence, $\|A\| = a_1$, which implies that $\|A\|$ is the maximum singular value. In particular, when A is Hermitian, $\|A\|$ is the maximum eigenvalue of A. A Hermitian operator A also satisfies

$$\|A\| = \max_{x \in \mathcal{H}:\, x \neq 0} \frac{|\langle x, Ax\rangle|}{\|x\|^2} = \max_{x \in \mathcal{H}:\, \|x\|=1} |\langle x, Ax\rangle|. \tag{A.43}$$

In fact, Schwartz inequality implies that

$$\max_{x \in \mathcal{H}:\, \|x\|=1} |\langle x, Ax\rangle| \le \max_{x \in \mathcal{H}:\, \|x\|=1} \|Ax\| = \|A\|. \tag{A.44}$$

The equality holds when x is the eigenvector corresponding to the eigenvalue of A whose absolute value is the maximum.

Lemma A.4 *The operator norm* $\|\cdot\|$ *satisfies*

(i) $\|AB\| \le \|A\|\|B\|$
(ii) $\|A^\dagger\| = \|A\|$, $\|A^\dagger A\| = \|A\|^2$
(iii) $A \ge B \ge 0 \Rightarrow \|A\| \ge \|B\|$.

Proof Since the relation (A.41) yields that $\|ABx\| \le \|A\|\|Bx\| \le \|A\|\|B\|\|x\|$, we can show (i) as follows.

$$\|AB\| = \max_{x \in \mathcal{H}:\, \|x\|=1} \frac{\|ABx\|}{\|x\|} \le \|A\|\|B\|. \tag{A.45}$$

Next, we show (ii). Since (ii) is trivial in the case of $A = 0$, we assume that $A \neq 0$. Relation (A.40) and Schwartz inequality imply that

$$\begin{aligned}\|A\|^2 &= \max_{\|x\|=1} \langle Ax, Ax\rangle = \max_{\|x\|=1} \langle x, A^\dagger Ax\rangle \\ &\le \max_{\|x\|=1} \|A^\dagger Ax\| = \|A^\dagger A\| \le \|A^\dagger\|\|A\|,\end{aligned} \tag{A.46}$$

where the final inequality follows from (i). Hence, $\|A^\dagger\| \le \|A\|$. Exchanging the roles of A and$A^\dagger$, we can show that $\|A\| \le \|A^\dagger\|$, which implies $\|A^\dagger\| = \|A\|$. Applying $\|A^\dagger\| = \|A\|$ in (A.46), we can show that $\|A^\dagger A\| = \|A\|^2$.

When $A \geq B \geq 0$ holds, A and B are Hermitian and $\langle x, Ax\rangle \geq \langle x, Bx\rangle \geq 0$. Taking the maximum with respect to $x \in \mathcal{H}$ with the condition $\|x\| = 1$, we can show (iii) by using the relation (A.43). □

A.6.3 Trace Norm

For a given operator $A \in \mathcal{L}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$, we define $\|A\|_1 := \operatorname{Tr}|A| = \operatorname{Tr}\sqrt{A^\dagger A}$. Since as is shown later, the function $\|\cdot\|_1$ is also a norm on the vector space $\mathcal{L}(\mathcal{H})$, it is called the **trace norm**.

Lemma A.5 *The trace norm $\|A\|_1$ and the operator norm $\|A\|$ satisfy*

(i) $\operatorname{Tr}|A| = \max_{X\in\mathcal{L}(\mathcal{H}):\,\|X\|=1} |\operatorname{Tr} XA| = \max_{X\in\mathcal{L}(\mathcal{H}):\,\|X\|\leq 1} |\operatorname{Tr} XA|$
(The maximum can be attained when X is a partial isometry.)
(ii) $|\operatorname{Tr} XA| \leq \operatorname{Tr}|XA| \leq \|X\|\operatorname{Tr}|A|$
(iii) $\|\cdot\|_1$ *is a norm.*
(iv) $\|A\|_1 = \operatorname{Tr}|A| = \operatorname{Tr}|A^\dagger|$
(v) $\|X\| = \max_{A\in\mathcal{L}(\mathcal{H}):\,\|A\|_1\leq 1} |\operatorname{Tr} XA|$.

Proof First, we show the following relation

$$|\operatorname{Tr} XA| \leq \|X\|\operatorname{Tr}|A|. \tag{A.47}$$

Let the eigenvalues of $|A| = \sqrt{A^\dagger A}$ be $\{a_k\}$, and the corresponding eigenvectors be $\{|e_k\rangle\}$. Since the eigenvalue decomposition (Corollary A.1) implies $|A| = \sum_k a_k|e_k\rangle\langle e_k|$, the relation (A.39) with $B = |A|$ yields that

$$\operatorname{Tr}|A| = \sum_k a_k = \sum_k \||A|e_k\| = \sum_k \|Ae_k\|. \tag{A.48}$$

Hence, the triangle inequality and Schwartz inequality imply

$$\begin{aligned}|\operatorname{Tr} XA| &= \left|\sum_k \langle e_k, XAe_k\rangle\right| \leq \sum_k |\langle X^\dagger e_k, Ae_k\rangle| \\ &\leq \sum_k \|X^\dagger e_k\|\|Ae_k\| \leq \|X^\dagger\|\sum_k \|Ae_k\| = \|X\|\operatorname{Tr}|A|. \end{aligned}\tag{A.49}$$

Here, the final inequality follows from the inequality $\|X^\dagger e_k\| \leq \|X^\dagger\|\|e_k\| = \|X^\dagger\|$, which can be derived from (A.41). The final equality follows from $\|X\| = \|X^\dagger\|$ (Lemma A.4).

Now, we show (i). We make use of the polar decomposition $A = W|A|$ (Theorem A.5), which implies that $|A| = W^\dagger A$. Since W is partial isometry and $\|W\| = \|W^\dagger\| = 1$, the relations

$$\mathrm{Tr}\,|A| = |\,\mathrm{Tr}\,W^\dagger A| \le \max_{X:\,\|X\|=1} |\,\mathrm{Tr}\,XA| \le \max_{X:\,\|X\|\le 1} |\,\mathrm{Tr}\,XA| \le \mathrm{Tr}\,|A| \tag{A.50}$$

hold, where the final inequality follows from (A.47). The maximum can be attained when X is a partial isometry $W^\dagger$.

Next, we show (ii). The first inequality can be shown as

$$|\,\mathrm{Tr}\,I\,XA| \le \max_{Y:\,\|Y\|=1} |\,\mathrm{Tr}\,YXA| = \mathrm{Tr}\,|XA|. \tag{A.51}$$

Using the polar decomposition $XA = W|XA|$ and the relation $\|W^\dagger\| = 1$, we can show

$$\mathrm{Tr}\,|XA| = |\,\mathrm{Tr}\,W^\dagger XA| \le \|W^\dagger\|\|X\|\,\mathrm{Tr}\,|A| = \|X\|\,\mathrm{Tr}\,|A|, \tag{A.52}$$

which implies the second inequality.

Next, we show that $\|\cdot\|_1$ satisfies the norm condition (Definition A.1) (i)∼(iii). The norm condition (i) "$\|A\|_1 \ge 0$" can be checked by (A.48). Here, the equality $\|A\|_1 = 0$ holds only when $\|Ae_k\| = 0$ for $\forall k$. Since $\{|e_k\rangle\}$ is an orthonormal basis, the equality $\|A\|_1 = 0$ holds only in the case $A = 0$. The norm condition (ii) "triangle inequality" can be checked as follows.

$$\begin{aligned}\|A+B\|_1 &= \max_{X:\,\|X\|=1} |\,\mathrm{Tr}\,X(A+B)| \\ &\le \max_{X:\,\|X\|=1} |\,\mathrm{Tr}\,XA| + \max_{X:\,\|X\|=1} |\,\mathrm{Tr}\,XB| = \|A\|_1 + \|B\|_1.\end{aligned} \tag{A.53}$$

The norm condition (iii) can be checked by the relations $\|\alpha A\|_1 = \mathrm{Tr}\,\sqrt{(\alpha A)^\dagger(\alpha A)} = |\alpha|\|A\|_1$. That is, we showed (iii) of Lemma A.5.

Next, we show (iv), i.e., $\mathrm{Tr}\,|A| = \mathrm{Tr}\,|A^\dagger|$. Using the polar decomposition $A = W|A|$, we have $|A^\dagger|^2 = AA^\dagger = W|A|^2W^\dagger$. On the other hand, since

$$(W|A|W^\dagger)^2 = W|A|W^\dagger W|A|W^\dagger = W|A|^2W^\dagger, \tag{A.54}$$

we have $|A^\dagger| = (W|A|^2W^\dagger)^{1/2} = W|A|W^\dagger$. Hence,

$$\mathrm{Tr}\,|A^\dagger| = \mathrm{Tr}\,W|A|W^\dagger = \mathrm{Tr}\,W^\dagger W|A| = \mathrm{Tr}\,|A|. \tag{A.55}$$

Finally, we show (v). The relation (A.47) yields the following inequality:

$$\max_{A\in\mathcal{L}(\mathcal{H}):\,\|A\|_1=1} |\,\mathrm{Tr}\,XA| \le \max_{A\in\mathcal{L}(\mathcal{H}):\,\|A\|_1\le 1} |\,\mathrm{Tr}\,XA| \le \|X\|. \tag{A.56}$$

We will give an operator A satisfying the equality in the above. Using the polar decomposition $X = W|X|$ of X, we choose the eigenvalues of $|X|$ as $x_1 \ge x_2 \ge \cdots \ge x_d \ge 0$, $(d = \dim\mathcal{H})$. Then, we have the eigenvalue decomposition (Corollary A.1) $|X| = \sum_{k=1}^d x_k|f_k\rangle\langle f_k|$. Since $\|X\|$ is the maximum eigenvalue of $|X|$, we have $\|X\| = x_1$. Here, when $A = |f_1\rangle\langle f_1|W^\dagger$, the relation $\|A\|_1 = 1$ holds. Hence, the equality in (A.56) can be shown as follows.

$$\begin{aligned}\operatorname{Tr} XA &= \operatorname{Tr} W\left(\sum_{k=1}^{d} x_k |f_k\rangle\langle f_k|\right)\Big(|f_1\rangle\langle f_1|\Big)W^\dagger = x_1 \operatorname{Tr} W^\dagger W |f_1\rangle\langle f_1| \\ &= x_1 \operatorname{Tr} |f_1\rangle\langle f_1| = \|X\|. \end{aligned} \tag{A.57}$$

□

In the following, we assume that A is a positive Hermitian operator satisfying $\operatorname{Tr} A = 1$. For any projection E_i, there exist unitaries U and U' such that $\|(I-E_i)A\|_1 = \operatorname{Tr}(I-E_i)AU$ and $\|E_iA(I-E_i)\|_1 = \operatorname{Tr} E_iA(I-E_i)U'$. Hence, applying Schwarz inequality (Theorem A.2) to the inner product $\operatorname{Tr} X^\dagger AY =: \langle X, Y\rangle$ on $\mathcal{L}(\mathcal{H})$, we have

$$\begin{aligned} &\|A - E_iAE_i\|_1 = \|(I-E_i)A + E_iA(I-E_i)\|_1 \\ &= \|(I-E_i)A\|_1 + \|E_iA(I-E_i)\|_1 = \operatorname{Tr}(I-E_i)AU + \operatorname{Tr} E_iA(I-E_i)U' \\ &\le \sqrt{\operatorname{Tr}(I-E_i)A(I-E_i)\operatorname{Tr} U^\dagger AU} \\ &\quad + \sqrt{\operatorname{Tr} E_iAE_i \operatorname{Tr} U'^\dagger (I-E_i)A(I-E_i)U'} \\ &= \sqrt{\operatorname{Tr}(I-E_i)A} + \sqrt{\operatorname{Tr} E_iA \operatorname{Tr}(I-E_i)A} \le 2\sqrt{\operatorname{Tr}(I-E_i)A}. \end{aligned} \tag{A.58}$$

Further, when $\sum_i E_i = I$, we obtain

$$\begin{aligned} \|A - \sum_i E_iAE_i\|_1 &= \|(A - E_iAE_i) + \sum_{j\neq i} E_jAE_j\|_1 \\ \le & \|A - E_iAE_i\| + \operatorname{Tr}\sum_{j\neq i} E_jAE_j \\ \le & 2\sqrt{\operatorname{Tr}(I-E_i)A} + \operatorname{Tr}(I-E_i)A \le 3\sqrt{\operatorname{Tr}(I-E_i)A}. \end{aligned} \tag{A.59}$$

In the following, we assume that A is a Hermitian operator, which is not necessarily positive. When E_i is the projection corresponding to the eigenvalue a_i of A, the spectral decomposition is given as $A = \sum_i a_iE_i$. Then, we define "the projector to the positive part of A" by[29]

$$\{A > 0\} := \sum_{i:a_i>0} E_i. \tag{A.60}$$

The projection is commutative with A and satisfies $0 \le \{A > 0\} \le I$. The projection $\{A \le 0\}$ is defined similarly, and satisfies $\{A > 0\} + \{A \le 0\} = I$. The **positive**

[29] The notation is taken from [5].

part A_+ and the **negative part** A_- of the Hermitian operator A are given as

$$A_+ := A\{A > 0\} = \sum_{i: a_i > 0} a_i E_i \tag{A.61}$$

$$A_- := -A\{A \le 0\} = \sum_{i: a_i \le 0} |a_i| E_i. \tag{A.62}$$

The above definition guarantees that A_+ and A_- are positive operators. Then, we obtain the Jordan decomposition $A = A_+ - A_-$. Since $A^\dagger A = A^2 = \sum_i a_i^2 E_i$, the **absolute value** $|A| := \sqrt{A^\dagger A}$ satisfies

$$|A| = \sum_i |a_i| E_i = A_+ + A_- = A\{A > 0\} - A\{A \le 0\}. \tag{A.63}$$

Hence, the trace norm of the Hermitian operator A is given as

$$\|A\|_1 = \operatorname{Tr} A_+ + \operatorname{Tr} A_- = \operatorname{Tr} A\big(\{A > 0\} - \{A \le 0\}\big). \tag{A.64}$$

Here, when we define $X := \{A > 0\} - \{A \le 0\}$, we have $-I \le X \le I$, $\|X\| = 1$. Thus, the operator X attains the equality in Lemma A.5, which implies the relation

$$\|A\|_1 = \max_{X: -I \le X \le I} |\operatorname{Tr} XA| \quad (A \in \mathcal{L}_h(\mathcal{H})). \tag{A.65}$$

The following lemma plays an important role for the trace norm distance (Sect. 6.3.5) and the property of quantum Neyman-Pearson test (Sect. 8.2.3).

Lemma A.6 *For any Hermitian operator A and any operator T satisfying $0 \le T \le I$, we have*

$$\operatorname{Tr} A\{A > 0\} \ge \operatorname{Tr} AT. \tag{A.66}$$

The equality holds when $T = \{A > 0\}$, and

$$\operatorname{Tr} A_+ = \operatorname{Tr} A\{A > 0\} = \max_{T: 0 \le T \le I} \operatorname{Tr} AT. \tag{A.67}$$

Proof We make use of the Jordan decomposition $A = A_+ - A_-$. Since $\operatorname{Tr} A_- T \ge 0$, we have

$$\operatorname{Tr} AT = \operatorname{Tr} A_+ T - \operatorname{Tr} A_- T \le \operatorname{Tr} A_+ T \le \operatorname{Tr} A_+ = \operatorname{Tr} A\{A > 0\}.$$

Here the final inequality follows from $\operatorname{Tr} A_+(I - T) \ge 0$, which can be shown by $I - T \ge 0$. Since the equality holds when $T = \{A > 0\}$, we obtain (A.67). □

A.6.4 Operator Monotone Function

In this section, we treat operator monotone functions and operator convex functions, which are operator versions of convex functions given in Sect. A.4; for details, see [6]. In this section, these concepts are treated as those defined for operators on a finite-dimensional Hilbert space.

Remember a real-valued function is called a monotone function when the function preserves the order of real numbers. A function is called an **operator monotone function** when it preserves the order of operators $A \le B \Leftrightarrow B - A \ge 0$.

Definition A.3 (*Operator monotone function*) A real-valued function f is called an operator monotone function if the following condition holds. When any two operators A and B, whose eigenvalues belong to the domain of f, satisfy $A \le B$, the relation $f(A) \le f(B)$ holds.

Now, we only give examples for operator monotone functions without proof; for the proof, see [6]. Any operator monotone function is clearly a monotone function, however, the converse does not hold in general.

Example A.5 (Examples of operator monotone function)

(i) $f(x) = \log x$ is an operator monotone function.
(ii) $f(x) = x^s$ $(0 \le s \le 1)$ is an operator monotone function.
(iii) $f(x) = x^s$ $(s \ge 2)$ is a monotone function, but is not an operator monotone function.

As a generalization of a convex function, we can define an **operator convex function** as follows.

Definition A.4 (*Operator convex function*) A real-valued function f is called an operator convex function, when any two operators A and B, whose eigenvalues belong to the domain of f, satisfy the relation $f(tA+(1-t)B) \le tf(A)+(1-t)f(B)$ for $0 \le \forall t \le 1$.

The following are examples for operator convex functions. Any operator convex function is clearly a convex function, however, the converse does not hold in general.

Example A.6 (Examples of operator convex function)

(i) $f(x) = -\log x$ is an operator convex function.
(ii) $f(x) = -x^s$ $(0 \le s \le 1)$ is an operator convex function.
(iii) $f(x) = x^s$ $(1 \le s \le 2, -1 \le s \le 0)$ is an operator convex function.
(iv) $f(x) = x^s$ $(s \ge 2, s \le -1)$ is a convex function, but is not an operator convex function.

A.7 Vector Space Over Finite Field

Up to now, we have treated vector spaces over the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. When a set has addition and invertible multiplication like $\mathbb{R}$ and $\mathbb{C}$, it is called a **field**. In fact, a vector space can be defined over a general field instead of $\mathbb{R}$ or $\mathbb{C}$. In the following, we give a precise definition of a field. That is, a set $\mathbb{K}$ satisfying the following conditions is called a field.

(1) A commutative operation "addition" is defined, and relations $a + b = b + a$ and $(a + b) + c = a + (b + c)$ hold for arbitrary elements $a, b, c \in \mathbb{K}$.
(2) There exists the unit element $0 \in \mathbb{K}$ with respect to the addition satisfying that $a + 0 = 0 + a = a$. The unit element is called zero.
(3) For an arbitrary element $a \in \mathbb{K}$, there exists the minus element $-a \in \mathbb{K}$ satisfying that $a + (-a) = (-a) + a = 0$.
(4) A commutative operation "multiplication" is defined, and relations $ab = ba$ and $(ab)c = a(bc)$ hold for $a, b, c \in \mathbb{K}$.
(5) There exists a unit element $1 \in \mathbb{K}$ with respect to the multiplication satisfying that $a1 = 1a = a$.
(6) For an arbitrary non-zero element $a \in \mathbb{K}$, there exists the invertible element $a^{-1} \in \mathbb{K}$ satisfying that $a(a^{-1}) = (a^{-1})a = 1$.
(7) The distributive law holds, i.e., the relations $a(b+c) = ab+ac$ and $(a+b)c = ac + bc$ hold for arbitrary elements $a, b, c \in \mathbb{K}$.

For example, the set $\mathbb{F}_2 := \{0, 1\}$ is a filed when the addition and the multiplication are defined in the following way.
Addition The addition is defined as exclusive OR $\oplus$. (See Fig. 3.1 in Sect. 3.3.)
Multiplication The multiplication is defined as $\wedge$. (See Table 3.1 in Sect. 3.3.)

Exercise A.23 Check that the set $\mathbb{F}_2$ is a filed under the above defined addition and multiplication.

Hence, we have an example of a field $\mathbb{F}_2$ in addition to $\mathbb{R}$ or $\mathbb{C}$. A field with finite elements is called a finite field. The set V is called a **vector space** V over the finite filed $\mathbb{F}_2$, when for arbitrary elements $\psi, \phi \in V$ and $a \in \mathbb{F}_2$, we have the sum $\psi + \phi \in V$ and the scalar[30] multiplication $a \cdot \psi \in V$ satisfying the following conditions: For arbitrary elements $\psi, \phi, \xi \in V$ and $a, b \in \mathbb{F}_2$,

(v1) $\psi + \phi = \phi + \psi$ (commutative law),
(v2) $\psi + (\phi + \xi) = (\psi + \phi) + \xi$ (associative law),
(v3) $\exists 1\theta \in V$ s.t. $\forall\psi \in V,\ \psi + \theta = \psi$ (existence of zero element),
(v4) $\forall\psi \in V, \exists 1\xi \in V$ s.t. $\psi + \xi = \theta$ (existence of inverse element),
(v5) $a \cdot (b \cdot \psi) = (ab) \cdot \psi$ (associative law),
(v6) $1 \cdot \psi = \psi$,
(v7) $a \cdot (\psi + \phi) = a \cdot \psi + b \cdot \phi$ (distributive law 1),
(v8) $(a + b) \cdot \psi = a \cdot \psi + b \cdot \psi$ (distributive law 2).

[30] An element of the finite field $\mathbb{F}_2$ is called scalar

θ in (v3) is called the **zero vector** and is simply denoted by $\theta = 0$. ξ in (v4) is called the **inverse vector** of ψ and is denoted by $-\psi$. In the following, we omit the notation "$\cdot$" for the scalar multiplication. The Greek letters $\psi, \phi, \xi, \cdots$ express vectors, the letters a, b, c, x, y, z express the scalar, and the letters $d, n, m, k \cdots$ express natural numbers.

Example A.7 Let $\mathbb{F}_2^d$ be the set of column vectors

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} = (x_1, \ldots, x_d)^T,$$

where $x_i \in \mathbb{F}_2$. When the addition and the scalar multiplication are defined by

$$\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} = \begin{pmatrix} x_1 \oplus y_1 \\ \vdots \\ x_d \oplus y_d \end{pmatrix}, a \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} = \begin{pmatrix} a \wedge x_1 \\ \vdots \\ a \wedge x_d \end{pmatrix},$$

the set $\mathbb{F}_2^d$ is a vector space over $\mathbb{F}_2$.

Exercise A.24 Find the zero vector in the vector space $\mathbb{F}_2^d$. Also, find the inverse vector for an arbitrary element $\psi = (x_1, \ldots, x_d) \in \mathbb{F}_2^d$.

Then, similar to Sect. A.2, we can define the linear independence and the linear dependence for plural elements of the vector space V. Similarly, the dimension of the vector space is defined as the maximum number of linearly independent vectors, and the basis is defined in the same way as in the case of vector space over $\mathbb{R}$ or $\mathbb{C}$.

Exercise A.25 Show that the set $\mathbb{F}_2$ is a vector space over the finite field $\mathbb{F}_2$. Find the dimension.

Exercise A.26 Let V be a vector space over the finite field $\mathbb{F}_2$ with dimension d. Find the number of elements of V.

Example A.8 A subset C of $\mathbb{F}_2^d$ is called a subspace of $\mathbb{F}_2^d$ if C is a vector space over $\mathbb{F}_2$.

Example A.9 We define the quotient space $\mathbb{F}_2^d/C$ for a subspace C of $\mathbb{F}_2^d$ by the following way. First, two elements x and $y \in \mathbb{F}_2^d$ are called equivalent to each other when $x - y \in C$. Then the subset of $\mathbb{F}_2^d$ composed of elements equivalent to x is called the equivalence class of x and is denoted by $[x]$. and call the subset the equivalence class. We denote the set of equivalence class by $\mathbb{F}_2^d/C$.

The scalar multiplication and the addition for the equivalence class are defined by
Scalar multiplication $a[x] := [ax]$ $(a \in \mathbb{F}_2)$
Addition $[x] + [y] := [x + y]$.

Then, the set $\mathbb{F}_2^d/C$ becomes a vector space with the above operations and is called the **quotient space**.

Exercise A.27 Assume that C be a subspace of the vector space $\mathbb{F}_2^d$ over $\mathbb{F}_2$ with dimension k. Find the dimension of $\mathbb{F}_2^d/C$.

Exercise A.28 Under the assumption as the above exercise, show that $y \in \mathbb{F}_2^d$ belongs to $[x+y]$ for any $x \in C$.

Similar to Sect. A.3, for given two vector spaces V and W over $\mathbb{F}_2$, a map $A : V \to W$ is called a **linear operator** from V to W when the map A satisfies the following conditions (**linearity**):

$$A(a\psi + b\phi) = aA\psi + bA\phi \quad (\forall \psi, \phi \in V, a, b \in \mathbb{F}_2). \tag{A.68}$$

In particular, a linear operator from $\mathbb{F}_2^{d_1}$ to $\mathbb{F}_2^{d_2}$ is given as (A.6) by using a $d_2 \times d_1$ matrix with entries in $\mathbb{F}_2$.

Especially, the set V^* of linear operators from the vector space V to $\mathbb{F}_2$ is a vector space over $\mathbb{F}_2$. The vector space V^* is called the **dual space** of V.

Exercise A.29 Let V be a vector space over the finite filed $\mathbb{F}_2$ with dimension d. Find the dimension of the dual space V^*.

For a given vector space V over the finite filed $\mathbb{F}_2$, a map $Q : V \times V \to \mathbb{F}_2$ is called a bilinear form when it satisfies the following condition.
Bilinearity The maps $Q(\cdot, y) : x \mapsto Q(x, y)$ and $Q(y, \cdot) : x \mapsto Q(y, x)$ are linear for arbitrary $y \in V$.

Hence, the maps $Q(\cdot, y)$ and $Q(y, \cdot)$ can be regarded as elements of the dual space V^* for $y \in V$. When the sets $\{Q(\cdot, y)\}_{y \in V}$ and $\{Q(y, \cdot)\}_{y \in V}$ coincide with the set V^*, the bilinear symmetric form Q is called non-degenerate. Otherwise, it is called degenerate.

When the bilinear form Q satisfies the symmetry condition (the skew-symmetry condition), it is called a bilinear symmetric form (a bilinear skew-symmetric form), respectively.

Symmetry The relation $Q(x, y) = Q(y, x)$ holds for arbitrary $x, y \in V$.
Skew-symmetry The relation $Q(x, y) = -Q(y, x)$ holds for arbitrary $x, y \in V$.

When the bilinear form Q is a bilinear symmetric form or a bilinear skew-symmetric form, Q is degenerate if and only if there exists a non-zero element $y \in V$ such that

$$Q(x, y) = 0, \quad \forall x \in V. \tag{A.69}$$

Exercise A.30 Define the inner product $(\boldsymbol{s}|\boldsymbol{t}) := (s_1 \wedge t_1) \oplus \cdots \oplus (s_n \wedge t_n)$ for elements $\boldsymbol{s} = (s_1, \ldots s_n), \boldsymbol{t} = (t_1, \ldots t_n) \in \mathbb{F}_2^n$. Show that the inner product is a non-degenerate bilinear symmetric form.

Exercise A.31 Define the **symplectic inner product** $\langle \boldsymbol{s}, \boldsymbol{s}' \rangle := \oplus_{i=1}^n ((s_i' \wedge t_i) \oplus (t_i' \wedge s_i))$ for elements $\boldsymbol{s} = (\boldsymbol{s}, \boldsymbol{t}), \boldsymbol{s}' = (\boldsymbol{s}', \boldsymbol{t}') \in \mathbb{F}_2^{2n}$. Show that the inner product is a non-degenerate bilinear skew-symmetric form.

A.8 Convergence

As is explained in Chap. 6, many information quantities satisfy the addivitity. However, some of them does not satisfy it. In such a case, the following lemma plays an important role.

Lemma A.7 *If a sequence of real numbers* $\{a_n\}_{n=1}^{\infty}$ *satisfies* $a_{m+n} \geq a_m + a_n$ *and* $\sup_{n\geq 1} \frac{a_n}{n} < \infty$*, then there exists* $\lim_{n\to\infty} \frac{a_n}{n}$*, and we have*

$$\lim_{n\to\infty} \frac{a_n}{n} = \sup_{n\geq 1} \frac{a_n}{n}. \tag{A.70}$$

Proof First we fix an integer m arbitrarily, and represent n by $n = lm + r$ $(0 \leq r < m)$. Then we have

$$\frac{a_n}{n} = \frac{a_{lm+r}}{lm+r} \geq \frac{la_m}{lm+r} + \frac{a_r}{lm+r} \xrightarrow{(n\to\infty)} \frac{a_m}{m}, \tag{A.71}$$

and hence $\liminf_{n\to\infty} \frac{a_n}{n} \geq \frac{a_m}{m}$ holds. Since m is arbitrary, we have

$$\liminf_{n\to\infty} \frac{a_n}{n} \geq \sup_{m\geq 1} \frac{a_m}{m} \geq \limsup_{m\to\infty} \frac{a_m}{m}, \tag{A.72}$$

which proves the lemma. □

Appendix B
Solution for Exercises

Exercise 2.1
$\langle\psi|\phi\rangle = \overline{(1+2i)} \times (-5-3i) + \overline{(2-i)} \times 4 + \overline{3} \times (2+i) = 3+14i.$

Exercise 2.2
(i) We have $A = |\phi\rangle\langle\psi| = \begin{pmatrix} 2i \\ 3 \end{pmatrix} (1, -i) = \begin{pmatrix} 2i & 2 \\ 3 & -3i \end{pmatrix}$, $|\chi'\rangle = \begin{pmatrix} 2i & 2 \\ 3 & -3i \end{pmatrix} \begin{pmatrix} 3 \\ -i \end{pmatrix}$ $= \begin{pmatrix} 4i \\ 6 \end{pmatrix}$, and $\langle\xi|\chi'\rangle = A|\chi\rangle = \overline{(1+i)} \times 4i + \overline{2} \times 6 = 16+4i$. Alternatively, (ii) we have $\langle\xi|\phi\rangle = \overline{(1+i)} \times 2i + \overline{2} \times 3 = 8+2i$, $\langle\psi|\chi\rangle = \overline{1} \times 3 + \overline{i} \times -i = 2$, and $\langle\xi|\phi\rangle\langle\psi|\chi\rangle = 16+4i$.

Exercise 2.3
Under a measurement of the basis (2.16), the probability to get 0 is $|\langle\xi_0|\psi\rangle|^2 = |\frac{1}{\sqrt{2}}(1, 1).(\frac{i}{\sqrt{3}}, \sqrt{\frac{2}{3}})^T|^2 = |\frac{i+\sqrt{2}}{\sqrt{6}}|^2 = \frac{1}{2}$. Thus, the probability to get 1 is $1 - \frac{1}{2} = \frac{1}{2}$. (The reader should also show the direct calculation $|\langle\xi_1|\psi\rangle|^2$ to get the same result.) Under a measurement of the basis (2.17), the probability to get 0 is $|\langle\eta_0|\psi\rangle|^2 = \frac{3+2\sqrt{2}}{6}(\simeq 0.97)$, thus the probability to get 1 is $1 - \frac{3+2\sqrt{2}}{6} = \frac{3-2\sqrt{2}}{6}(\simeq 0.03)$.

Exercise 2.4
Omit.

Exercise 2.5
By the direct computation, show the condition $AA^\dagger(= A^\dagger A) = I$ for each matrix.

Exercise 2.6
The final state is $|\psi'\rangle = \sigma_x|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{i}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \end{pmatrix} = \begin{pmatrix} \frac{2}{\sqrt{5}} \\ \frac{i}{\sqrt{5}} \end{pmatrix}$. Therefore, the probabilities to obtain 0 and 1 of the measurement of the computational basis under the final state are $|\langle 0|\psi'\rangle|^2 = \frac{4}{5}$ and $|\langle 1|\psi'\rangle|^2 = \frac{1}{5}$, respectively.

Exercise 2.7
Directly show (2.27) and (2.28) by using (2.22).

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1,

Exercise 2.8
Omit.

Exercise 2.9
Note that "inner products" between $|\xi_i\rangle$ $(i = 0, 1)$ on the right qubit and the state $|\psi\rangle$ are given by $\langle\xi_0|\psi\rangle = \frac{1}{\sqrt{15}}(|0\rangle\langle\xi_0|0\rangle + 3|0\rangle\langle\xi_0|1\rangle - |1\rangle\langle\xi_0|0\rangle + 2|1\rangle\langle\xi_0|1\rangle) = \frac{1}{\sqrt{30}}(4|0\rangle + |1\rangle)$ and $\langle\xi_1|\psi\rangle = -\frac{1}{\sqrt{30}}(2|0\rangle + 3|1\rangle)$, respectively. Therefore, from (2.36), the probabilities to get outcomes $i = 0, 1$ are $||\langle\xi_0|\psi\rangle||^2 = \frac{17}{30}$ and $||\langle\xi_1|\psi\rangle||^2 = \frac{13}{30}$. From (2.37), the post-measurement states for the outcome $i = 0, 1$ are $\langle\xi_0|\psi\rangle/||\langle\xi_0|\psi\rangle|| \otimes |\xi_0\rangle = \frac{1}{\sqrt{17}}(4|0\rangle + |1\rangle) \otimes |\xi_0\rangle$ and $\langle\xi_1|\psi\rangle/||\langle\xi_1|\psi\rangle|| \otimes |\xi_1\rangle = \frac{1}{\sqrt{13}}(2|0\rangle + 3|1\rangle) \otimes |\xi_1\rangle$, respectively.

Exercise 3.1
$f(n) = O(\log^{\log n} n)$ since $\log^{\log n} n/n^2 \to \infty$ as $n \to \infty$.

Exercise 3.2
(Sketch) Let K be the total number of circuits that consist of at most $2^n/2n$ gates. Then, $\Pr_f\{\mathcal{C}(f) < 2^n/2n\} = K/2^{2^n}$.

Exercise 3.3
See Sect. 2.3.3.

Exercise 3.4
(Sketch) Similarly to the Z-Y decomposition.

Exercise 4.1
(Sketch) The 1-bit case is done as in the hint. For general n-bit case, apply induction on n.

Exercise 4.2
Note that the (i, j)th component of D_N can be represented by $\langle i|D_N|j\rangle$. ($|i\rangle$ is identical to a column vector that has 1 in the ith coordinate and 0 in the others.) Since $|\phi_0\rangle = \sum_x |x\rangle/\sqrt{2^n}$, $\langle i|(-I + 2|\phi_0\rangle\langle\phi_0|)|i\rangle = -1 + 2|\langle i||\phi_0\rangle|^2 = -1 + 2/2^n$. For $j \neq i$, we have $\langle i|(-I + 2|\phi_0\rangle\langle\phi_0|)|j\rangle = 2(\langle i||\phi_0\rangle)(\langle\phi_0||j\rangle) = 2/2^n$.

Exercise 4.3
(Sketch) The analysis is quite similar to the case of a single solution.

Exercise 4.4
(Sketch) If a solution x_0 is obtained by making $O(\sqrt{N})$ queries, the given f has a solution, and otherwise, we regard that f has no solution. When x_0 is obtained, the answer is correct with probability 1. If a non-solution x is obtained, f has no solution with high probability.

Exercise 4.5
(Sketch) Verify $FF^\dagger = I$.

Exercise 4.6
If k is a multiple of N, we can write $k = cN$ for some integer c. Then, we have $S_N(cN) = \sum_{\ell=0}^{N-1} \omega_N^{\ell cN} = \sum_{\ell=0}^{N-1} 1^{\ell c} = N$. If k is not a multiple of N, since it holds

that $(\omega_N^k - 1)S_N(k) = (\omega_N^k - 1)(\omega_N^{k(N-1)} + \omega_N^{k(N-2)} + \cdots + \omega_N^k + \omega_N^0) = \omega_N^{kN} - 1 = 0$, and $\omega_N^k - 1 \neq 0$, we have $S_N(k) = 0$.

Exercise 5.1
By using (5.5) and the linearity of the inner product, we have $\langle\phi'|(|\phi\rangle\langle\psi|)\psi'\rangle = \langle\phi'|\langle\psi|\psi'\rangle\phi\rangle = \langle\psi|\psi'\rangle\langle\phi'|\phi\rangle$.

Let $|\xi\rangle$ be an arbitrary vector. We have $(|\psi\rangle\langle\phi||\psi'\rangle\langle\phi'|)|\xi\rangle = |\psi\rangle\langle\phi|(|\psi'\rangle\langle\phi'||\xi\rangle)$ $= |\psi\rangle\langle\phi|(\langle\phi'|\xi\rangle|\psi'\rangle) = \langle\phi'|\xi\rangle(|\psi\rangle\langle\phi||\psi'\rangle) = \langle\phi'|\xi\rangle\langle\phi|\psi'\rangle|\psi\rangle = \langle\phi|\psi'\rangle\langle\phi'|\xi\rangle|\psi\rangle$ $= (\langle\phi|\psi'\rangle|\psi\rangle\langle\phi'|)|\xi\rangle$, which shows (5.7). (Alternatively, by using the notion of the bra and combining $\langle\phi|$ and $|\psi\rangle$ first, (5.7) immediately follows.)

Exercise 5.2
We have to show both the positivity $\langle\psi|P_a\psi\rangle \geq 0$ and the normalization condition $\sum_{a\in\sigma(A)}\langle\psi|P_a\psi\rangle = 1$. By using the conditions of the projection operator, i.e., $P_a = P_a^\dagger = P_a^2$, the positivity follows as $\langle\psi|P_a\psi\rangle = \langle\psi|P_a^2\psi\rangle$ $= \langle P_a^\dagger\psi|P_a\psi\rangle = ||P_a\psi||^2 \geq 0$. The normalization condition follows as $\sum_a\langle\psi|P_a\psi\rangle$ $= \langle\psi|(\sum_a P_a)\psi\rangle = \langle\psi|\, I\, \psi\rangle = ||\psi||^2 = 1$ by the completeness condition $\sum P_a = I$.

Exercise 5.3
Solve the eigenvalue equations: $\det(\lambda\, I - A) = 0$ for $A = \sigma_x, \sigma_y, \sigma_z$.

Exercise 5.4
By the definition (A.24) of the trace, we have $\mathrm{Tr}(A|\psi\rangle\langle\phi|) = \sum_i\langle\phi_i|(A|\psi\rangle\langle\phi|)\phi_i\rangle = \sum_i\langle\phi_i|A\psi\rangle\langle\phi|\phi_i\rangle = \sum_i\langle\phi|\phi_i\rangle\langle\phi_i|A\psi\rangle = \langle\phi|(\sum_i|\phi_i\rangle\langle\phi_i|)A\psi\rangle = \langle\phi|\, I\, A\psi\rangle = \langle\phi|A\psi\rangle$ where $\{|\phi_i\rangle\}$ is an ONB of $\mathcal{H}$.

Exercise 5.5
The density operator corresponding to s_1 is $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\, I$ where we have used the completeness condition $|0\rangle\langle 0| + |1\rangle\langle 1| = I$. In the same way, the density operator of s_2 is $\rho_2 = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{1}{2}\, I$.

Exercise 5.6
By the eigenvalue decomposition $\sigma_x = |+\rangle\langle +| - |-\rangle\langle -|$ and the Born rule (5.35), the probability to get 1 is $\mathrm{Tr}\,\rho|+\rangle\langle +| = \langle +|\rho|+\rangle = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})\begin{pmatrix}\frac{1}{2} & -\frac{1}{6}\\ -\frac{1}{6} & \frac{1}{2}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} =$ $1/3$. Therefore, the probability to get -1 is $1 - 1/3 = 2/3$. (Of course, one can compute $\mathrm{Tr}\,\rho|-\rangle\langle -|$ to get the same answer.)

Exercise 5.7
Let $\rho = \sum_{i=1}^d p_i|\phi_i\rangle\langle\phi_i|$ be an eigenvalue decomposition of ρ. Using the Schwarz inequality $|\langle\psi|\phi_i\rangle| \leq ||\psi||||\phi_i|| = 1$, we have $\langle\psi|\rho\psi\rangle = \sum_i p_i|\langle\psi|\phi_i\rangle|^2 \leq \sum_i p_i = 1$.

Exercise 5.8
Let $\rho = \sum_{i=1}^d p_i|\phi_i\rangle\langle\phi_i|$ be an eigenvalue decomposition of ρ. We have $\mathrm{Tr}(\rho^2) = \sum_k\langle\phi_k|(\sum_{i=1}^d p_i|\phi_i\rangle\langle\phi_i|)^2|\phi_k\rangle = \sum_i p_i^2$ by using $\langle\phi_i|\phi_j\rangle = \delta_{ij}$. Since $p_i \leq 1$, we

obtain $\mathrm{Tr}(\rho^2) = \sum_i p_i^2 \leq \sum_i p_i = 1$. The upper bound is achieved if and only if ρ is pure as is already shown in Proposition 4.6-(c).

The Schwarz inequality between d dimensional vectors $\boldsymbol{a} := (1/d, \ldots, 1/d)^T$ and $\boldsymbol{p} := (p_1, \ldots, p_d)^T$ reads $|\sum_i \frac{1}{d} p_i|^2 \leq (\sum_i \frac{1}{d}^2)(\sum_i p_i^2)$. Since $\sum_i p_i = 1$, we obtain $\frac{1}{d} \leq \sum_i p_i^2 = \mathrm{Tr}(\rho^2)$. To see the equality condition of the lower bound of (5.43), one can use the equality condition of Schwarz inequality implying that $\boldsymbol{a}$ and $\boldsymbol{p}$ are linearly dependent. However, by $\sum_i p_i = 1$, we have $\boldsymbol{p} = \boldsymbol{a}$. Therefore, we have shown that the lower bound is achieved if and only if the state is the completely mixed state $\rho = \sum_{i=1}^d \frac{1}{d} |\phi_i\rangle\langle\phi_i| = \frac{1}{d} I$.

Exercise 5.9

Let the characteristic equation of 2×2 matrix A be $\det(\lambda I - A) = \lambda^2 - c_1\lambda + c_0 = (\lambda - \lambda_1)(\lambda - \lambda_2)$ where λ_1 and λ_2 are eigenvalues of A. Using $\lambda_1 + \lambda_2 = c_1$, $\lambda_1\lambda_2 = c_2$, it is easy to see that $\lambda_1 \geq 0$, $\lambda_2 \geq 0$ if and only if $c_1 \geq 0$, $c_2 \geq 0$. By direct computations of $\det(\lambda I - A)$, we have $c_1 = a_{11} + a_{22} = \mathrm{Tr}\, A$ and $c_0 = a_{11}a_{22} - a_{12}a_{21} = (\mathrm{Tr}\, A)^2 - \mathrm{Tr}(A^2)$. This completes the proof.

Exercise 5.10

(1) Let $C = \sum_j A_j \otimes B_j$ and fix arbitrary $|\psi\rangle, |\phi\rangle \in \mathcal{H}_\mathrm{S}$. By (5.49), we have $\langle\psi| \mathrm{Tr}_\mathrm{E}\, C\phi\rangle = \langle\psi|(\sum_j \mathrm{Tr}\, B_j) A_j \phi\rangle = \sum_j (\sum_k \langle e_k|B_j e_k\rangle)\langle\psi|A_j\phi\rangle = \sum_k \langle\psi \otimes e_k|(\sum_j A_j \otimes B_j)\phi \otimes e_k\rangle = \sum_k \langle\psi \otimes e_k|C|\phi \otimes e_k\rangle$. On the other hand, if we define the partial trace by (5.50), we have $\langle\psi|(\mathrm{Tr}_\mathrm{E}\, C)\phi\rangle := \sum_k \langle\psi \otimes e_k|(\sum_j A_j \otimes B_j)|\phi \otimes e_k\rangle = \langle\psi|(\sum_j (\mathrm{Tr}\, B_j) A)\phi\rangle$, and thus obtain (5.49). Notice that we also observed here that the definition (5.49) is independent of the decompositions of $C = \sum_j A_j \otimes B_j$.

(2) Let $C = \sum_j A_j \otimes B_j$. We have $\mathrm{Tr}(A(\mathrm{Tr}_\mathrm{E}\, C)) = \mathrm{Tr}(A((\sum_j \mathrm{Tr}\, B_j)A_j)) = \mathrm{Tr}(A \otimes I_\mathrm{E}(\sum_j A_j \otimes B_j)) = \mathrm{Tr}(A \otimes I_\mathrm{E}\, C)$.

(3) By using (5.50) and the positivity condition for C, $\langle\psi| \mathrm{Tr}_\mathrm{E}\, C\psi\rangle = \sum_k \langle\psi \otimes e_k|C|\psi \otimes e_k\rangle \geq 0$ for any $|\psi\rangle \in \mathcal{H}_\mathrm{S}$.

(4) By using (5.50), we have $\langle\psi|(\mathrm{Tr}_\mathrm{E}(\alpha C_1 + \beta C_2))\phi\rangle = \sum_k \langle\psi \otimes e_k|(\alpha C_1 + \beta C_2)\phi \otimes e_k\rangle = \alpha \sum_k \langle\psi \otimes e_k|C_1\phi \otimes e_k\rangle + \beta \sum_k \langle\psi \otimes e_k|C_2\phi \otimes e_k\rangle = \alpha\langle\psi| \mathrm{Tr}_\mathrm{E}\, C_1\phi\rangle + \beta\langle\psi| \mathrm{Tr}_\mathrm{E}\, C_2\phi\rangle = \langle\psi|(\alpha\, \mathrm{Tr}_\mathrm{E}\, C_1 + \beta\, \mathrm{Tr}_\mathrm{E}\, C_2)\phi\rangle$ for any $|\psi\rangle$ and $|\phi\rangle$.

Exercise 5.11

The density operator of the total system is $\rho = |\psi\rangle\langle\psi| = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) = \frac{1}{2}|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{2}|0\rangle\langle 1| \otimes |0\rangle\langle 1| + \frac{1}{2}|1\rangle\langle 0| \otimes |1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \otimes |1\rangle\langle 1|$. By (5.49), one has $\rho_\mathrm{S} = \mathrm{Tr}_\mathrm{E}\, \rho = \frac{1}{2}(\mathrm{Tr}_\mathrm{E}\, |0\rangle\langle 0|)|0\rangle\langle 0| + \frac{1}{2}(\mathrm{Tr}_\mathrm{E}\, |0\rangle\langle 1|)|0\rangle\langle 1| + \frac{1}{2}(\mathrm{Tr}_\mathrm{E}\, |1\rangle\langle 0|)|1\rangle\langle 0| + \frac{1}{2}(\mathrm{Tr}_\mathrm{E}\, |1\rangle\langle 1|)|1\rangle\langle 1| = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2} I_\mathrm{S}$.

Exercise 5.12

Let $P = |+\rangle\langle +|$ and $Q = |0\rangle\langle 0|$. Under a state ρ, the probability to get an outcome 1 of the measurement M is given by

$$\Pr(M = 1|\rho) = \frac{1}{2}\Pr(\sigma_x = 1|\rho) + \frac{1}{2}\Pr(\sigma_z = 1|\rho) = \frac{1}{2}\,\mathrm{Tr}\, P\rho + \frac{1}{2}\,\mathrm{Tr}\, Q\rho = \mathrm{Tr}\, E\rho,$$

where $E = \frac{1}{2}(P + Q)$. It is easily shown that E is not a projection operator. (Notice, however, that $0 \le E \le I$.) Thus, the measurement M cannot be described by any single Hermitian operator.

Exercise 5.13

By definitions of E_1, E_2 and E_3, we have $E_1 \ge 0$, $E_2 \ge 0$ and $\sum_i E_i = I$. To show the positivity of E_3, it is enough to check that eigenvalues of E_3 are all non-negative since E_3 is Hermitian. Noting that $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, the matrix representation of E_3 with respect to the basis $\{|0\rangle, |1\rangle\}$ reads $\begin{pmatrix} 0.4 & -0.2 \\ -0.2 & 0.8 \end{pmatrix}$, which has the eigenvalues $0.6 \pm 0.2\sqrt{2} \ge 0$. (Alternatively, one can just check the coefficients of the characteristic equation of E_3 to be non-negative. (See Exercise 5.9).

Exercise 5.14

Let $\mathcal{L}(\mathcal{H})_+$ and $\mathcal{L}(\mathcal{H})_h$ be the set of all positive and Hermitian operators on $\mathcal{H}$, respectively. We construct the linear extension of f by first extending it to $\mathcal{L}(\mathcal{H})_+$, and next to $\mathcal{L}(\mathcal{H})_h$, and finally to $\mathcal{L}(\mathcal{H})$.

Notice that any positive operator $A \in \mathcal{L}(\mathcal{H})_+$ can be uniquely expressed as $A = a\rho$ with non-negative $a := \operatorname{Tr} A \ge 0$ and the density operator $\rho := A/a$ (except for the case $A = 0$ where one does not have to define ρ). Using this, we have the unique extension f' to $\mathcal{L}(\mathcal{H})_+$ by $f'(A) := af(\rho)$ $(\forall A = a\rho \in \mathcal{L}(\mathcal{H})_+)$. From the affine property of f, it is easy to see (p1) $f'(A + B) = f'(A) + f'(B)$ and (p2) $f'(aA) = af'(A)$ $(\forall A, B \in \mathcal{L}(\mathcal{H})_+, a \ge 0)$.

Next, notice that any Hermitian operator $A \in \mathcal{L}(\mathcal{H})_h$ can be expressed as $A = B - C$ with two positive operators $B, C \in \mathcal{L}(\mathcal{H})_+$. (For instance, with the spectral decomposition $A = \sum_a aP_a$, let $B := \sum_{a;a\ge 0} aP_a$ and $C := -\sum_{a;a<0} aP_a$.) Thus, we have an extension f'' to $\mathcal{L}(\mathcal{H})_h$ by $f''(A) := f'(B) - f'(C)$ $(\forall A = B - C \in \mathcal{L}(\mathcal{H})_h)$. For the well-definedness, it is necessary to show that the definition of f'' is independent of the ways of the decomposition $A = B - C$. However, this can be directly shown by using (p1). Moreover, we have the conditions: (l1) $f''(A + B) = f''(A) + f''(B)$ from (p1) and (l2) $f''(aA) = af''(A)$ $(\forall A, B \in Y, a \in \mathbb{R})$ from (p2). Finally, observe that any linear operator $A \in \mathcal{L}(\mathcal{H})$ has the unique decomposition $A = A_R + iA_I$ with Hermitian operators $A_R := (A + A^\dagger)/2$ and $A_I := (A - A^\dagger)/(2i)$. Therefore, we have the unique extension $\tilde{f}$ to $\mathcal{L}(\mathcal{H})$ by $\tilde{f}(A) := f''(A_R) + if''(A_I)$. From (l1) and (l2), it is easy to see that $\tilde{f}$ satisfies the linearity condition.

From the above proof, we have also observed that any operator $A \in \mathcal{L}(\mathcal{H})$ can be expressed as $A = A_R + iA_I = (A_+ - A_-) + i(B_+ - B_-) = p_0\rho_0 - p_2\rho_2 + ip_1\rho_1 - ip_3\rho_3 = \sum_{k=0}^{3} i^k p_k\rho_k$ with non-negative numbers p_0, p_1, p_2, p_3 and density operators $\rho_0, \rho_1, \rho_2, \rho_3$. Hence, with this expression $A = \sum_{k=0}^{3} i^k p_k\rho_k$, the linear extension of f to $\mathcal{L}(\mathcal{H})$ is given by $\tilde{f}(A) = \sum_{k=0}^{3} i^k p_k f(\rho_k)$.

Exercise 5.15

Let $W_\perp$ be the orthogonal complement of W. Let $\{|\phi_i\rangle\}_{i=1}^{m}$ and $\{|\phi_i\rangle\}_{i=m+1}^{d}$ be ONBs of W and $W_\perp$, respectively, and let $|\phi'_i\rangle := U|\phi_i\rangle$ $(i = 1, \ldots, m)$. Since the inner product is preserved on W, $\{|\phi'_i\rangle\}_{i=1}^{m}$ forms an orthonormal system of $\mathcal{H}$. Therefore, one can complement an orthonormal system so that $\{|\phi'_i\rangle\}_{i=1}^d$ is an ONB of $\mathcal{H}$. If we define a linear operator U' on $\mathcal{H}$ by $U'|\phi_i\rangle = |\phi'_i\rangle$ $(i = 1, \ldots, d)$, U' is obviously a linear extension of U which is unitary.

Exercise 5.16

Notice that $P^\perp := I - P$ is a projection operator which satisfies $PP^\perp = 0$. For any $|\psi\rangle \in \mathcal{H}$, we have $||F^{1/2}P^\perp|\psi\rangle||^2 = \langle P^\perp\psi|FP^\perp\psi\rangle \leq \langle P^\perp\psi|PP^\perp\psi\rangle = 0$, where in the second inequality we have used $F \leq P$. Thus, we have $F^{1/2}P^\perp = 0$, from which we obtain $F(I - P) = 0$. Therefore, we have $FP = F = F^\dagger = (FP)^\dagger = PF$.

Exercise 5.17

(i) The linearity of Λ easily follows. Observe that $\mathrm{Tr}_{\mathrm{AB}}\,\Lambda(A) = \mathrm{Tr}_{\mathrm{AB}}\,A \otimes \sigma = \mathrm{Tr}_{\mathrm{A}}\,A\,\mathrm{Tr}_{\mathrm{B}}\,\sigma = \mathrm{Tr}_{\mathrm{A}}\,A$. Therefore, Λ is a trace preserving map. By noting that the tensor product of positive operators is positive, it is easy to show that Λ is a completely positive map.

(ii) The linearity and the trace preserving property follows immediately. With an ONB $\{|e_k\rangle\}_k$ of $\mathcal{H}_{\mathrm{A}}$, define linear operators $V_k : \mathcal{H}_{\mathrm{AB}} \to \mathcal{H}_{\mathrm{B}}$ by $V_k|\psi\rangle = |\phi_k\rangle$ $(\forall|\psi\rangle = \sum_k |e_k \otimes \phi_k\rangle)$. As is easily seen, we have $V_k^\dagger|\phi\rangle = |e_k \otimes \phi\rangle$ $(|\phi\rangle \in \mathcal{H}_{\mathrm{B}})$. In the following, we show that

$$\mathrm{Tr}_{\mathrm{A}}\,C = \sum_k V_k C V_k^\dagger, \tag{B.1}$$

which implies that Λ is a completely positive map by Theorem 5.4-(iv). To show (B.1), it is enough to consider C of the form $C = |\xi\rangle\langle\chi|$ with arbitrary $|\xi\rangle = \sum_k |e_k \otimes \xi_k\rangle$, $|\chi\rangle = \sum_k |e_k \otimes \chi_k\rangle \in \mathcal{H}_{\mathrm{AB}}$. By the definition of V_k, we have $\sum_k V_k|\xi\rangle\langle\chi|V_k^\dagger = \sum_k |V_k\xi\rangle\langle V_k\chi| = \sum_k |\xi_k\rangle\langle\chi_k|$. Thus, for any $|\psi\rangle, |\phi\rangle \in \mathcal{H}_{\mathrm{B}}$, we have $\langle\psi|(\sum_k V_k C V_k^\dagger)\phi\rangle = \sum_k\langle\psi|\xi_k\rangle\langle\chi_k|\phi\rangle$. On the other hand, by (5.50), we have $\langle\psi|(\mathrm{Tr}_{\mathrm{A}}\,C)\phi\rangle = \sum_k\langle e_k \otimes \psi|Ce_k \otimes \phi\rangle = \sum_k\langle e_k \otimes \psi|\xi\rangle\langle\chi|e_k \otimes \phi\rangle = \sum_k\langle\psi|\xi_k\rangle\langle\chi_k|\phi\rangle$. Therefore, we have shown that (B.1) holds for any $C = |\xi\rangle\langle\chi|$.

Exercise 6.1

A direct calculation yields

$$\begin{aligned} h'(p) &= -\frac{1}{\log_e 2}\left\{\log_e p + 1 - \log_e(1-p) - 1\right\} \\ &= -\frac{1}{\log_e 2}\left\{\log_e p - \log_e(1-p)\right\}, \\ h''(p) &= -\frac{1}{\log_e 2}\left(\frac{1}{p} + \frac{1}{1-p}\right) = -\frac{1}{\log_e 2}\cdot\frac{1}{p(1-p)}. \end{aligned}$$

Thus we have $h''(p) < 0$ $(0 < p < 1)$, and the concavity of $h(p)$ follows from Proposition A.12. Noting that $h'(\frac{1}{2}) = 0$, $h(\frac{1}{2}) = 1$, $\lim_{p\searrow 0} h'(p) = \infty$, $\lim_{p\nearrow 1} h'(p) = -\infty$, and $h(0) = h(1) = 0$, we can verify the shape of Fig. 6.1.

Exercise 6.2
Using $-\log\frac{1}{2^1}=1$, $-\log\frac{1}{2^2}=2$, and $-\log\frac{1}{2^3}=3$, we have $\frac{1}{2}+\frac{2}{4}+\frac{3}{8}+\frac{3}{8}=\frac{7}{4}$.

Exercise 6.3
$\lceil\log_2 M\rceil$ bits are required, where $\lceil x\rceil$ is the ceiling function defined in Sect. 3.2.

Exercise 6.4
(1) Since Z is a non-negative random variable, we have

$$\begin{aligned}E[Z]=&\sum_{z\geq 0} zP_Z(z)=\sum_{z:\,z>a} zP_Z(z)+\sum_{z:\,0\leq z\leq a} zP_Z(z)\geq\sum_{z:\,z>a} zP_Z(z)\\ =&\,a\Pr\{Z>a\}.\end{aligned}$$

Dividing both sides by $a>0$ gives Markov's inequality.
(2) Since $\epsilon>0$, we have $|X-\mu|>\epsilon\Leftrightarrow(X-\mu)^2>\epsilon^2$. Thus using Markov's inequality, we obtain Chebyshev's inequality:

$$\Pr\{|X-\mu|>\epsilon\}=\Pr\{(X-\mu)^2>\epsilon^2\}\leq\frac{E[(X-\mu)^2]}{\epsilon^2}=\frac{V[X]}{\epsilon^2}.$$

(3) The expectation of S_n is given by $E[S_n]=\frac{1}{n}\sum_{i=1}^{n}E[X_i]=\mu$. The variance is calculated as

$$\begin{aligned}V[S_n]=&E\left[(S_n-\mu)^2\right]=E\left[\left\{\frac{1}{n}\sum_{i=1}^{n}(X_i-\mu)\right\}^2\right]\\ =&\frac{1}{n^2}\sum_{i,j}E\left[(X_i-\mu)(X_j-\mu)\right].\end{aligned}$$

Using $E\left[(X_i-\mu)(X_j-\mu)\right]=0\ (i\neq j)$, we have $V[S_n]=\frac{1}{n^2}\sum_i E\left[(X_i-\mu)^2\right]$ $=\frac{1}{n}E\left[(X_1-\mu)^2\right]=\frac{V[X_1]}{n}$. Hence Chebyshev's inequality leads to

$$\Pr\left\{\left|\frac{1}{n}\sum_{i=1}^{n}X_i-E[X_1]\right|>\epsilon\right\}\leq\frac{V[S_n]}{\epsilon^2}=\frac{V[X_1]}{n\epsilon^2}\to 0\quad(n\to\infty).$$

Exercise 6.5
(1) Let $N(a|x^n)$ be the number of occurrences of the symbol a in $x^n=(x_1,x_2,\ldots,x_n)$. Then the type (empirical distribution) is given by $P_{x^n}(a)=\frac{N(a|x^n)}{n}$. Note that the arithemtic mean of a function $f(x)$ is written as $\frac{1}{n}\sum_{i=1}^{n}f(x_i)=\frac{1}{n}\sum_{a\in\mathcal{X}}N(a|x^n)$ $f(a)=\sum_{a\in\mathcal{X}}P_{x^n}(a)f(a)$, which equals the expectation by the type. Taking $f(x)=-\log P(x)$ yields the assertion.
(2) For any $x^n\in B_{n,\epsilon}$ we have $P_{X^n}(x^n)\neq 0$, and the triangle inequality yield

$$\left|-\frac{1}{n}\log P_{X^n}(x^n)-H(P)\right|=\left|\sum_{a\in\mathcal{X}:\,P(a)\neq 0}(P_{x^n}(a)-P(a))(-\log P(a))\right|$$
$$\le\sum_{a\in\mathcal{X}:\,P(a)\neq 0}|P_{x^n}(a)-P(a)|\cdot M\le\sum_{a\in\mathcal{X}:\,P(a)\neq 0}P(a)\epsilon\cdot M\le M\epsilon.$$

Exercise 6.6

(1) The assertion follows from $P_{XY}(x,y)=P_X(x)P_{Y|X}(y|x)$.
(2) It follows from $\sum_y P_{XY}(x,y)=P_X(x)$ that

$$-\sum_x\sum_y P_{XY}(x,y)\log P_X(x)=-\sum_x \log P_X(x)P_X(x).$$

Combining this equality and (1), we can show the chain rule.

Exercise 6.7

Taking the expectation of $\log\frac{P_{X_1Y_1}(x,y)}{P_{X_2Y_2}(x,y)}=\log\frac{P_{X_1}(x)}{P_{X_2}(x)}+\log\frac{P_{Y_1}(y)}{P_{Y_2}(y)}$ by the probability distribution $P_{X_1Y_1}(x,y)$ yields the additivity.

Exercise 6.8

Taking the expectation by $P_{XY}(x,y)$ on the both sides of

$$\log\frac{P_{XY}(x,y)}{P_X(x)P_Y(y)}=\{-\log P_X(x)\}+\{-\log P_Y(y)\}-\{-\log P_{XY}(x,y)\}$$

gives (6.26). In the same way, taking the expectation of $\log\frac{P_{XY}(x,y)}{P_X(x)P_Y(y)}=\{-\log P_X(x)\}-\{-\log P_{X|Y}(x|y)\}$ leads to (6.27). It is also possible to show (6.27) by using (6.26) and the chain rule (6.7).

Exercise 6.9

From (6.26), we have $I(X;Y)=H(X)+H(Y)-H(X,Y)$. In the same way, $I(X;Z|Y)=H(X|Y)+H(Z|Y)-H(X,Z|Y)$ follows. Thus we have

$$\begin{aligned}&I(X;Y)+I(X;Z|Y)\\&=H(X)+H(Y)-H(X,Y)+H(X|Y)+H(Z|Y)-H(X,Z|Y)\\&=H(X)+H(Y)-H(X,Y)+\{H(X,Y)-H(Y)\}\\&\quad+\{H(Y,Z)-H(Y)\}-\{H(X,Y,Z)-H(Y)\}\\&=H(X)+H(Y,Z)-H(X,Y,Z)=I(X;YZ).\end{aligned}$$

Exercise 6.10

We choose the random variable $\hat{X}$ as the constant x, i.e., $\hat{X}=x$ holds with probability 1. Using Fano inequality (6.42), we obtain (6.45) because $P_e=1-P(X=x)$ and $H(X|\hat{X})=H(X)$.

Exercise 6.11
Using (6.46), we can show the unitary invariance:

$$
\begin{aligned}
&D(U\rho U^\dagger \| U\sigma U^\dagger) = \operatorname{Tr}\left[U\rho U^\dagger \left\{\log(U\rho U^\dagger) - \log(U\sigma U^\dagger)\right\}\right] \\
&= \operatorname{Tr}\left[U\rho U^\dagger \left\{U(\log\rho)U^\dagger - U(\log\sigma)U^\dagger\right\}\right] \\
&= \operatorname{Tr}\left[\rho U^\dagger \left\{U(\log\rho)U^\dagger - U(\log\sigma)U^\dagger\right\} U\right] = D(\rho\|\sigma).
\end{aligned}
$$

The additivity is shown as follows:

$$
\begin{aligned}
&D(\rho_A \otimes \rho_B \| \sigma_A \otimes \sigma_B) = \operatorname{Tr}(\rho_A \otimes \rho_B)\{\log(\rho_A \otimes \rho_B) - \log(\sigma_A \otimes \sigma_B)\} \\
&= \operatorname{Tr}(\rho_A \otimes \rho_B)\{\log\rho_A \otimes I_B + I_A \otimes \log\rho_B - \log\sigma_A \otimes I_B - I_A \otimes \log\sigma_B\} \\
&= \operatorname{Tr}(\rho_A \otimes \rho_B)\{(\log\rho_A - \log\sigma_A) \otimes I_B\} \\
&\quad + \operatorname{Tr}(\rho_A \otimes \rho_B)\{I_A \otimes (\log\rho_B - \log\sigma_B)\} \\
&= D(\rho_A\|\sigma_A) + D(\rho_B\|\sigma_B).
\end{aligned}
$$

Exercise 6.12
(1) Let $U = -P + (I - P)$. Then U is a unitary transformation and $\frac{1}{2}(\rho + U\rho U) = P\rho P + (I - P)\rho(I - P)$ holds. Thus the concavity of the von Neumann entropy yields the assertion.
(2) Applying (1) inductively gives to the assertion.

Exercise 6.13
(1) Let W be a partial isometry. From Appendix (A.38), $W^\dagger W$ acts as the identity on $(\operatorname{Ker} W)^\perp$. Thus $W^\dagger W$ is the projection onto the subspace $(\operatorname{Ker} W)^\perp$, from which $WW^\dagger W = W$ follows. Conversely, suppose that $WW^\dagger W = W$ holds. Multiplying the both sides by $W^\dagger$ from the left, we have $(W^\dagger W)^2 = W^\dagger W$. Thus $W^\dagger W$ is the projection onto the subspace $(\operatorname{Ker} W)^\perp$, and hence, W is a partial isometry.
(2) Taking the Hermitian conjugate of the both sides, we have $WW^\dagger W = W \Leftrightarrow W^\dagger W W^\dagger = W^\dagger$. Hence the assertion follows from (1).
(3) The assertion follows from $WW^\dagger W = W \Leftrightarrow W^T W^{T\dagger} W^T = W^T$.

Exercise 6.14
By (6.103) we have $\|\sqrt{\rho}V - \sqrt{\sigma}W\|_2 = \|\sqrt{\rho} - \sqrt{\sigma}WV^\dagger\|_2$. If V and W vary within the set of unitary operators, $U = WV^\dagger$ also varies in the whole set of unitary operators. Hence we have $B(\rho,\sigma) = \min_U \|\sqrt{\rho} - \sqrt{\sigma}U\|_2$. We show that $B(\rho,\sigma)$ satisfies the axiom of the distance. The positivity $B(\rho,\sigma) \geq 0$ obviously holds. If $B(\rho,\sigma) = 0$, then there exist unitary operators V and W such that $\sqrt{\rho}V = \sqrt{\sigma}W$, from which $\rho = (\sqrt{\rho}V)(\sqrt{\rho}V)^\dagger = (\sqrt{\sigma}W)(\sqrt{\sigma}W)^\dagger = \sigma$ holds. The symmetry property is obvious by definition. We show the triangle inequality. From the triangle inequality of 2-norms, we have $\|\sqrt{\rho}V - \sqrt{\sigma}W\|_2 = \|\sqrt{\rho}V - \tau + \tau - \sqrt{\sigma}W\|_2 \leq \|\sqrt{\rho}V - \tau\| + \|\tau - \sqrt{\sigma}W\|_2$. Minimizing the both sides with respect to V and W leads to the assersion.

Exercise 6.15

The assertion obviously follows from Lemma 6.10 and Lemma 6.11.

Exercise 6.16

(1) $1 - F(\rho,\sigma)^2 = (1 + F(\rho,\sigma))(1 - F(\rho,\sigma)) \le 2(1 - F(\rho,\sigma))$.
(2) The assertion follows from (1), Lemma 6.13, and (6.102).

Exercise 7.1

Let $|\Psi\rangle \equiv |\phi^+\rangle$. The four Bell bases are written as $|\Psi_i\rangle = (U_i \otimes I)|\Psi\rangle$ using unitary operators U_i's. Let σ be a mixed state on X, and $|\Psi_{i\mathrm{XA}}\rangle$ be a post measurement state after the Bell state measurement on A and X (for the outcome i). The state of B then becomes

$$\begin{aligned}
\sigma'_{\mathrm{B}} &= \langle \varPsi_{i\mathrm{XA}}|(U_i^{\dagger} \otimes I_{\mathrm{A}} \otimes I_{\mathrm{B}})\,(\sigma_{\mathrm{X}} \otimes |\varPsi_{\mathrm{AB}}\rangle\langle\varPsi_{\mathrm{AB}}|)\,(U_i \otimes I_{\mathrm{A}} \otimes I_{\mathrm{B}})|\varPsi_{i\mathrm{XA}}\rangle \\
&= \langle \varPsi_{\mathrm{XA}}|(U_i^{\dagger}\sigma_{\mathrm{X}} \otimes I_{\mathrm{A}} \otimes I_{\mathrm{B}})|\varPsi_{\mathrm{AB}}\rangle\langle\varPsi_{\mathrm{AB}}|(U_i \otimes I_{\mathrm{A}} \otimes I_{\mathrm{B}})|\varPsi_{\mathrm{XA}}\rangle \\
&= \langle \varPsi_{\mathrm{XA}}|(I_{\mathrm{X}} \otimes \sigma_{\mathrm{A}}^{T}\bar{U}_i \otimes I_{\mathrm{B}})|\varPsi_{\mathrm{AB}}\rangle\langle\varPsi_{\mathrm{AB}}|(I_{\mathrm{X}} \otimes U_i^{T} \otimes I_{\mathrm{B}})|\varPsi_{\mathrm{XA}}\rangle \\
&= \langle \varPsi_{\mathrm{XA}}|(I_{\mathrm{X}} \otimes I_{\mathrm{A}} \otimes U_i^{\dagger}\sigma_{\mathrm{B}})|\varPsi_{\mathrm{AB}}\rangle\langle\varPsi_{\mathrm{AB}}|(I_{\mathrm{X}} \otimes I_{\mathrm{A}} \otimes U_i)|\varPsi_{\mathrm{XA}}\rangle \\
&= \mathrm{tr}_{\mathrm{XA}}(I_{\mathrm{X}} \otimes I_{\mathrm{A}} \otimes U_i^{\dagger}\sigma_{\mathrm{B}})|\varPsi_{\mathrm{AB}}\rangle\langle\varPsi_{\mathrm{AB}}|(I_{\mathrm{X}} \otimes I_{\mathrm{A}} \otimes U_i)|\varPsi_{\mathrm{XA}}\rangle\langle\varPsi_{\mathrm{XA}}| \\
&= \frac{1}{2}\mathrm{tr}_{\mathrm{A}}(I_{\mathrm{A}} \otimes U_i^{\dagger}\sigma_{\mathrm{B}})|\varPsi_{\mathrm{AB}}\rangle\langle\varPsi_{\mathrm{AB}}|(I_{\mathrm{A}} \otimes U_i) = \frac{1}{4}U_i^{\dagger}\sigma_{\mathrm{B}}U_i,
\end{aligned}$$

where (7.4) was used in the third and fourth equality. As a result, $U_i\sigma'_{\mathrm{B}}U_i^{\dagger} \propto \sigma_{\mathrm{B}}$ and hence a mixed state on the qubit X is teleported to the qubit B. For a state σ_{YX} that is entangled with Y, in the same way as above, we have $\sigma'_{\mathrm{YB}} = \frac{1}{4}(I_{\mathrm{Y}} \otimes U_i^{\dagger})\sigma_{\mathrm{YB}}(I_{\mathrm{Y}} \otimes U_i)$.

Exercise 7.2

Letting $\epsilon_i \equiv \sum_{k=0}^{i-1} 2^{J_k}$ and $\delta_i \equiv \log_2(d^l - \epsilon_i) - \lfloor \log_2(d^l - \epsilon_i) \rfloor$, we have $0 < \epsilon_i < d^l$, $0 \le \delta_i < 1$, and

$$\begin{aligned}
\frac{1}{l}\sum_{i=0}^{e}\frac{2^{J_i}}{d^l}J_i &= \sum_{i=0}^{e}\frac{2^{J_i}}{d^l}\frac{1}{l}[\log_2(d^l - \epsilon_i) - \delta_i] \to \sum_{i=0}^{e}\frac{2^{J_i}}{d^l}\frac{1}{l}\log_2(d^l - \epsilon_i) \\
&= \sum_{i=0}^{e}\frac{2^{J_i}}{d^l}[\log_2 d + \frac{1}{l}\log_2(1 - \frac{\epsilon_i}{d^l})] \\
&= \sum_{i=0}^{e}[\frac{2^{J_i}}{d^l}\log_2 d + \frac{1}{l}2^{-\delta_i}(1 - \frac{\epsilon_i}{d^l})\log_2(1 - \frac{\epsilon_i}{d^l})] \\
&\to \sum_{i=0}^{e}\frac{2^{J_i}}{d^l}\log_2 d = \log_2 d.
\end{aligned}$$

Exercise 7.3

The stochastic conversion of $|\psi\rangle \to |\phi\rangle$ by A's local filtering is possible if and only if there exists an operator A such that

$$(A \otimes I)|\psi\rangle\langle\psi|(A^\dagger \otimes I) = p|\phi\rangle\langle\phi|, \tag{B.2}$$

where $p > 0$ is the normalization. The probability of success is then equal to p, because $\mathrm{tr}(A \otimes I)|\psi\rangle\langle\psi|(A^\dagger \otimes I) = p$. Moreover, since $\{A^\dagger A, I - A^\dagger A\}$ must construct a POVM, $I - A^\dagger A \geq 0$ must hold (the POVM element of $I - A^\dagger A$ corresponds to the event that a qubit does not pass through a filter). Let us denote the matrix elements of A by A_{ij}. Taking the expected value on the both sides of (B.2) with respect to $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, we have $A_{01} = A_{10} = 0$. Moreover, taking the expected value with respect to $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, we have $\sqrt{1/6}A_{00} = \sqrt{1/3}A_{11}$. From this and $I - A^\dagger A \geq 0$, we have $|A_{00}|^2 \leq 1$ and $|A_{11}|^2 \leq 1/2$. Finally, taking the expected value on the both sides of (B.2) with respect to $|\phi\rangle$, we have $p = |\sqrt{1/6}A_{00} + \sqrt{1/3}A_{11}|^2 = (4/3)|A_{11}|^2 \leq 2/3$.

Exercise 7.4

Let $|\psi\rangle$ be a pure state on three qubits A, B, and C. When $\mathrm{rank}(\sigma_\mathrm{A}) = 1$, it is found by considering the Schmidt decomposition for the grouping of A:BC that $|\psi\rangle$ must have the form of $|\psi\rangle = |f\rangle_\mathrm{A} \otimes |\phi\rangle_{BC}$. Moreover, considering the Schmidt decomposition of $|\phi\rangle_{BC}$, $\mathrm{rank}(\sigma_\mathrm{B}) = \mathrm{rank}(\sigma_\mathrm{C})$ must hold, and hence $\mathrm{rank}(\sigma_\mathrm{B}) = 1$ and $\mathrm{rank}(\sigma_\mathrm{C}) = 2$ do not hold simultaneously.

Exercise 7.5

$$\begin{aligned}
\mathrm{Tr}\, X^{T_\mathrm{A}} &= \sum_{ij} \langle ij|X^{T_\mathrm{A}}|ij\rangle = \sum_{ij} \langle ij|X|ij\rangle = \mathrm{Tr}\, X, \\
\mathrm{Tr}\, X^{T_\mathrm{A}} Y^{T_\mathrm{A}} &= \sum_{ijkl} \langle ij|X^{T_\mathrm{A}}|kl\rangle\langle kl|Y^{T_\mathrm{A}}|ij\rangle = \sum_{ijkl} \langle kj|X|il\rangle\langle il|Y|kj\rangle = \mathrm{Tr}\, XY.
\end{aligned}$$

Exercise 7.6

Let $\langle i|Y_1|j\rangle = Y_{1;ij}$, $\langle mn|X|op\rangle = X_{mnop}$, and so on. We then have

$$\begin{aligned}
&\langle ij|\{(Y_1 \otimes Y_2)X(Y_3 \otimes Y_4)\}^{T_\mathrm{A}}|kl\rangle = \langle kj|(Y_1 \otimes Y_2)X(Y_3 \otimes Y_4)|il\rangle \\
&= \sum_{mnop} Y_{1;km} Y_{2;jn} X_{mnop} Y_{3;oi} Y_{4;pl} = \sum_{mnop} Y_{1;km} Y_{2;jn} X^{T_\mathrm{A}}_{onmp} Y_{3;oi} Y_{4;pl} \\
&= \sum_{mnop} Y^T_{3;io} Y_{2;jn} X^{T_\mathrm{A}}_{onmp} Y^T_{1;mk} Y_{4;pl} = \langle ij|(Y_3^T \otimes Y_2)X^{T_\mathrm{A}}(Y_1^T \otimes Y_4)|kl\rangle.
\end{aligned}$$

Moreover, to change the basis to which a partial transposition is applied, let us apply the local unitary transformation of $(U \otimes V)$ to σ and then apply the partial transposition to it. Since $\{(U \otimes V)\sigma(U^\dagger \otimes V^\dagger)\}^{T_{\mathrm{A}}} = (\bar{U} \otimes V)\sigma^{T_{\mathrm{A}}}(U^T \otimes V)$, it is found that the eigenvalues of $\{(U \otimes V)\sigma(U^\dagger \otimes V\dagger)\}^{T_{\mathrm{A}}}$ are equal to the eigenvalues of $\sigma^{T_{\mathrm{A}}}$, regardless of $(U \otimes V)$.

Exercise 7.7
Denoting the Schmidt decomposition of a bipartite pure state by $|\psi\rangle = \sum_i \sqrt{q_i}|ii\rangle$, we have

$$\begin{aligned}(|\psi\rangle\langle\psi|)^{T_{\mathrm{A}}} &= \sum_{ij} \sqrt{q_i q_j}(|ii\rangle\langle jj|)^{T_{\mathrm{A}}} = \sum_{ij} \sqrt{q_i q_j}|ji\rangle\langle ij| \\ &= \sum_i q_i|ii\rangle\langle ii| + \sum_{i\neq j} \sqrt{q_i q_j}|ji\rangle\langle ij| \\ &= \sum_i q_i|ii\rangle\langle ii| + \sum_{i<j} \sqrt{q_i q_j}(|\psi_{ij}^+\rangle\langle\psi_{ij}^+| - |\psi_{ij}^-\rangle\langle\psi_{ij}^-|),\end{aligned}$$

where $|\psi_{ij}^\pm\rangle \equiv (|ij\rangle \pm |ji\rangle)/\sqrt{2}$. Since $\{|ii\rangle, |\psi_{ij}^+\rangle, |\psi_{ij}^-\rangle\}$ are mutually orthogonal with each other, they are the eigenstates of $(|\psi\rangle\langle\psi|)^{T_{\mathrm{A}}}$. The corresponding eigenvalues are $\{q_i, \sqrt{q_i q_j}, -\sqrt{q_i q_j}\}$. When $|\psi\rangle$ is entangled, at least two of q_i are not zero. Denoting those by q_0 and q_1, we have $-\sqrt{q_0 q_1} < 0$ and hence $(|\psi\rangle\langle\psi|)^{T_{\mathrm{A}}}$ has at least one negative eigenvalue.

Exercise 7.8
Since an unentangled state σ satisfies $\sigma^{T_{\mathrm{A}}} \geq 0$ and $\mathrm{Tr}\,\sigma^{T_{\mathrm{A}}} = 1$ due to the Peres criterion, $\sigma^{T_{\mathrm{A}}}$ is considered to be a density operator of a certain state. Moreover, putting $q_i = 1/d$ in the result of Exercise 7.7, it is found that the maximal7 eigenvalue of $(|\Psi\rangle\langle\Psi|)^{T_{\mathrm{A}}}$ is $1/d$. Since the averaged value of $(|\Psi\rangle\langle\Psi|)^{T_{\mathrm{A}}}$ with respect to a state is always less than or equal to the maximal eigenvalue,

$$\langle\Psi|\sigma|\Psi\rangle = \mathrm{Tr}\,\sigma|\Psi\rangle\langle\Psi| = \mathrm{Tr}\,\sigma^{T_{\mathrm{A}}}(|\Psi\rangle\langle\Psi|)^{T_{\mathrm{A}}} \leq \frac{1}{d}.$$

Exercise 7.9
Since $\rho^{T_{\mathrm{A}}} \geq 0$ for any unentangled state ρ, we have

$$\mathrm{Tr}\,\rho W = \mathrm{Tr}\,\rho(|\mu\rangle\langle\mu|)^{T_{\mathrm{A}}} = \mathrm{Tr}\,\rho^{T_{\mathrm{A}}}|\mu\rangle\langle\mu| = \langle\mu|\rho^{T_{\mathrm{A}}}|\mu\rangle \geq 0,$$

and hence the expected value of W with respect to any unentangled state is non-negative. On the other hand, since

$$\mathrm{Tr}\,\sigma W = \mathrm{Tr}\,\sigma(|\mu\rangle\langle\mu|)^{T_{\mathrm{A}}} = \mathrm{Tr}\,\sigma^{T_{\mathrm{A}}}|\mu\rangle\langle\mu| = \langle\mu|\sigma^{T_{\mathrm{A}}}|\mu\rangle = \mu < 0,$$

W is an entanglement witness. Moreover, if $|\mu\rangle$ is assumed to be unentangled, we have $(|\mu\rangle\langle\mu|)^{T_{\mathrm{A}}} \geq 0$ (see Exercise 7.7), which contradicts to $\mathrm{Tr}\,\sigma(|\mu\rangle\langle\mu|)^{T_{\mathrm{A}}} < 0$.

Exercise 7.10
Considering U such that $U|m_0\rangle = -|m_0\rangle$, the matrix elements of A other than $|mn\rangle\langle mn|$, $|mn\rangle\langle nm|$, and $|mm\rangle\langle nn|$ are equal to zero. Moreover, considering U such that $U|m_0\rangle = i|m_0\rangle$, the matrix elements of $|mn\rangle\langle nm|$ $(m \neq n)$ are equal to zero. Moreover, considering U such that it exchanges $|m_0\rangle$ and $|m_1\rangle$, it is found, for example, that the coefficients of $|mn\rangle\langle mn|$ $(m \neq n)$ are all equal to each other, and so on, and A must have the form of

$$A = x \sum_{m \neq n} |mn\rangle\langle mn| + y \sum_{m \neq n} |mm\rangle\langle nn| + z \sum_{m} |mm\rangle\langle mm|,$$

with x, y, and z being real parameters. Now, considering U such that $U|m\rangle = (|m\rangle + |n\rangle)/\sqrt{2}$ and $U|n\rangle = (|m\rangle - |n\rangle)/\sqrt{2}$ in the two-dimensional subspace spanned by $|m\rangle$ and $|n\rangle$, $(U \otimes \bar{U})$ transforms as

$$\begin{aligned}
&x|mn\rangle\langle mn| + y|mm\rangle\langle nn| + z|mm\rangle\langle mm| + (m \leftrightarrow n) \\
\to\ &\frac{1}{2}(x + y + z)|mm\rangle\langle mm| + \frac{1}{2}(-x + y + z)|mm\rangle\langle nn| \\
&+\frac{1}{2}(x - y + z)|mn\rangle\langle mn| + \frac{1}{2}(-x - y + z)|mn\rangle\langle nm| + (m \leftrightarrow n),
\end{aligned}$$

and hence $z = x + y$ must hold. Namely,

$$\begin{aligned}
A &= x \sum_{m \neq n} |mn\rangle\langle mn| + y \sum_{m \neq n} |mm\rangle\langle nn| + (x + y) \sum_{m} |mm\rangle\langle mm| \\
&= x \sum_{mn} |mn\rangle\langle mn| + y \sum_{mn} |mm\rangle\langle nn| = x(I \otimes I) + yd|\Psi\rangle\langle\Psi|,
\end{aligned}$$

and hence A must be written in the form of a sum of a unit operator $(I \otimes I)$ and a maximally entangled state $|\Psi\rangle = (1/\sqrt{d}) \sum_m |mm\rangle$. It is obvious from (7.4) that A in this form is invariant under the unitary transformation of $(U \otimes \bar{U})$ for any U.

Exercise 7.11
It is confirmed by calculating each element that $A^T \sigma_y A = (\det A)\sigma_y$ for any operator A on $\mathbb{C}^2$. From (7.4), when $|\psi\rangle$ is a maximally entangled state on $\mathbb{C}^2 \otimes \mathbb{C}^2$, it is written as $|\psi\rangle = (U \otimes I)|\phi^+\rangle$, where U is a unitary operator and $|\phi^+\rangle \equiv (|00\rangle + |11\rangle)/\sqrt{2}$. Since

$$\begin{aligned}
|\tilde{\psi}\rangle &= (\sigma_y \otimes \sigma_y)\overline{(U \otimes I)|\phi^+\rangle} = (\sigma_y \bar{U} \otimes \sigma_y)|\phi^+\rangle = -(\sigma_y \bar{U} \sigma_y \otimes I)|\phi^+\rangle \\
&= -(\sigma_y \bar{U} \sigma_y U^\dagger \otimes I)|\psi\rangle = -(\det U^\dagger)|\psi\rangle,
\end{aligned}$$

we have $|\langle\psi|\tilde{\psi}\rangle| = 1$. When $|\psi\rangle$ is unentangled, it is written as $|\psi\rangle = (U \otimes V)|00\rangle$ and hence

$$\begin{aligned}|\tilde{\psi}\rangle &= (\sigma_y \bar{U} \otimes \sigma_y \bar{V})|00\rangle = (UU^\dagger \sigma_y \bar{U} \otimes VV^\dagger \sigma_y \bar{V})|00\rangle \\ &= (\det \bar{U} \det \bar{V})(U\sigma_y \otimes V\sigma_y)|00\rangle = -(\det \bar{U} \det \bar{V})(U \otimes V)|11\rangle.\end{aligned}$$

Since $(U \otimes V)|00\rangle$ and $(U \otimes V)|11\rangle$ are orthogonal, we have $|\langle\psi|\tilde{\psi}\rangle| = 0$.

Exercise 7.12
According to Exercise 7.11, we have $|\tilde{\psi}\rangle = -\sqrt{p}|11\rangle - \sqrt{1-p}|00\rangle$ and $\langle\psi|\tilde{\psi}\rangle = -2\sqrt{p(1-p)}$. Since $\sqrt{|\psi\rangle\langle\psi|\tilde{\psi}\rangle\langle\tilde{\psi}|\psi\rangle\langle\psi|} = 2\sqrt{p(1-p)}|\psi\rangle\langle\psi|$ and $l_0 - l_1 - l_2 - l_3 = 2\sqrt{p(1-p)} \geq 0$, we have $C = 2\sqrt{p(1-p)}$. Moreover, since $\tilde{\sigma} = F|\mathrm{EPR}\rangle\langle\mathrm{EPR}| + (1-F)(I \otimes I - |\mathrm{EPR}\rangle\langle\mathrm{EPR}|)/3 = \sigma$, we have $\sqrt{\sqrt{\sigma}\tilde{\sigma}\sqrt{\sigma}} = \sigma$. Then, $l_0 - l_1 - l_2 - l_3 = (1-F)/3 - 2(1-F)/3 - F = -(1+2F)/3$ for $F < 1/4$, and $l_0 - l_1 - l_2 - l_3 = F - 3(1-F)/3 = 2F - 1$ for $1/4 \leq F$. Therefore, $C = 0$ for $0 \leq F \leq 1/2$, and $C = 2F - 1$ for $F > 1/2$.

Exercise 7.13
According to Exercise 7.7, since the eigenvalues of $(|\psi\rangle\langle\psi|)^{T_{\mathrm{A}}}$ are $\{q_i, \sqrt{q_i q_j}, -\sqrt{q_i q_j}\}$, the eigenvalues of $|(|\psi\rangle\langle\psi|)^{T_{\mathrm{A}}}|$ are $\{q_i, \sqrt{q_i q_j}, \sqrt{q_i q_j}\}$. Therefore,

$$\operatorname{Tr}|(|\psi\rangle\langle\psi|)^{T_{\mathrm{A}}}| = \sum_i q_i + 2\sum_{i<j}\sqrt{q_i q_j} = \sum_{ij}\sqrt{q_i q_j} = \left(\sum_i \sqrt{q_i}\right)^2,$$

and hence $\log_2 \operatorname{Tr}|(|\psi\rangle\langle\psi|)^{T_{\mathrm{A}}}| = 2\log_2(\sum_i \sqrt{q_i})$. Since $q_i = 1/d$ for a maximally entangled state $|\Psi\rangle$ on two d-dimensional systems, $\log_2 \operatorname{Tr}|(|\Psi\rangle\langle\Psi|)^{T_{\mathrm{A}}}| = 2\log_2(d/\sqrt{d}) = \log_2 d$.

Exercise 8.1
The eigenvalues and the eigenvectors of $A - B = \frac{1}{2}\begin{pmatrix} b^2 & -ab \\ -ab & -b^2 \end{pmatrix}$ are, respectively, $\lambda_1 = \frac{b}{2}$, $(a, b-1)^T$ and $\lambda_2 = -\frac{b}{2}$, $(a, b+1)^T$. Hence the projection to the positive part is given by $S = \frac{1}{a^2+(b-1)^2}\begin{pmatrix} a & b-1 \end{pmatrix}\begin{pmatrix} a \\ b-1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+b & -a \\ -a & 1-b \end{pmatrix}$.

Exercise 8.2
$Y = \frac{1}{4}\begin{pmatrix} 2 - b(b+1) & ab \\ ab & b(b-1) \end{pmatrix}$. Since $(0,1)Y(0,1)^T = \frac{1}{4}b(b-1) < 0$ $(0 < b < 1)$, Y is not non-negative. The Beysian error is given by $\operatorname{Tr} Y = \frac{1-b}{2}$. Note that it is better than the test that chose either of the hypotheses with probability $\frac{1}{2}$ without any measurement.

Exercise 8.3
Since $\|\sqrt{A} - \sqrt{B}\|_2^2 = \operatorname{Tr} A + \operatorname{Tr} B - 2\operatorname{Tr}\sqrt{A}\sqrt{B}$, we have

$$\begin{aligned}(6.109) &\Leftrightarrow \|\sqrt{A} - \sqrt{B}\|_2^2 \leq \|A - B\|_1 \\ &\Leftrightarrow \operatorname{Tr}(A+B) - \operatorname{Tr}|A - B| \leq 2\operatorname{Tr}\sqrt{A}\sqrt{B}\end{aligned}$$

The last inequality is a special case of (8.17) ($s = 1/2$) [7, 8].

Exercise 8.4
By the way to construct G and B, we have $e_i \geq m$ for any $i \in B$, and hence, $\sum_i P(i)e_i = \sum_{i \in G} P(i)e_i + \sum_{i \in B} P(i)e_i \geq P(B)m$. Thus we have $m \leq \frac{\sum_i P(i)e_i}{P(B)} \leq \frac{\epsilon}{P(B)}$.

Exercise 8.5
Fix a classical-quantum channel W and consider the formula $I(P; W) = H(W_P) - \sum_x P(x)H(W_x)$. Since the correspondence $P \mapsto W_P = \sum_x P(x)W_x$ is linear with respect to P and the von Neumann entropy is concave, the first term is a concave functional of P. It is obvious that the second term is linear with respect to P. Thus $I(P; W)$ is concave with respect to P. Fix a probability P and consider the formula $I(P; W) = \sum_x P(x)D(W_x||W_P)$. Given two classical-quantum channels $W_1 : x \mapsto W_{1,x}$ and $W_2 : x \mapsto W_{2,x}$, let $W_{t,x} = tW_{1,x} + (1-t)W_{2,x}$ with a real number $0 \leq t \leq 1$. Since $W_{t,P} = tW_{1,P} + (1-t)W_{2,P}$, the joint convexity of the quantum relative entropy yields

$$\begin{aligned} I(P; W_t) &= \sum_x P(x)D(W_{t,x}||W_{t,P}) \\ &\leq \sum_x P(x)\left\{tD(W_{1,x}||W_{1,P}) + (1-t)D(W_{2,x}||W_{2,P})\right\} \\ &= (1-t)I(P; W_1) + (1-t)I(P; W_2). \end{aligned}$$

Thus $I(P; W_P)$ is convex with respect to W.

Exercise 8.6
Since we have

$$\begin{aligned} &\sum_x P(x)D(W_x||\tau) - \sum_x P(x)D(W_x||W_P) \\ =&\sum_x P(x) \operatorname{Tr} W_x(\log W_P - \log\tau) \\ =&\operatorname{Tr} W_P(\log W_P - \log\tau) = D(W_P||\tau) \geq 0, \end{aligned}$$

the inequality $I(P; W) \leq \sum_x P(x)D(W_x||\tau)$ holds with the equality if and only if $\tau = W_P$. Hence we have $I(P; W) = \min_{\tau \in \mathcal{S}(\mathcal{H})} \sum_x P(x)D(W_x||\tau)$.

Exercise 8.7
For a fixed τ, $f(P, \tau) = \sum_x P(x)D(W_x||\tau)$ is linear and especially concave with respect to P. For a fixed P, $f(P, \tau)$ is convex with respect to τ due to the joint convexity of the quantum relative entropy. Hence we have

$$\begin{aligned}\max_{P\in\mathcal{P}(\mathcal{X})} I(P;W) &= \max_{P\in\mathcal{P}(\mathcal{X})}\min_{\tau\in\mathcal{S}(\mathcal{H})}\sum_x P(x)D(W_x\|\tau)\\ &= \min_{\tau\in\mathcal{S}(\mathcal{H})}\max_{P\in\mathcal{P}(\mathcal{X})}\sum_x P(x)D(W_x\|\tau)\\ &= \min_{\tau\in\mathcal{S}(\mathcal{H})}\max_{x\in\mathcal{X}} D(W_x\|\tau).\end{aligned}$$

In the last equality, we used the fact that the maximization with respect to the probability P is attained by the delta measure concentrated on the point x where the maximum of $D(W_x\|\tau)$ occurs.

Exercise 9.1
When $1/2 > p \ge 0$, the map J_{ML} is given by (9.1). When $1 \ge p > 1/2$, it is given by

$$\begin{aligned}&J_{\mathrm{ML}}(\{(0,0,0),(1,1,1)\}) = (1,1,1),\ J_{\mathrm{ML}}(\{(1,0,0),(0,1,1)\}) = (0,1,1),\\ &J_{\mathrm{ML}}(\{(0,1,0),(1,0,1)\}) = (1,0,1),\ J_{\mathrm{ML}}(\{(0,0,1),(1,1,0)\}) = (1,1,0).\end{aligned}$$

When $p = 1/2$, the map J_{ML} is maximum likelihood decoder, whatever J_{ML} is.

Exercise 9.2
$(1-p)^3 + 3p(1-p)^2$.

Exercise 9.3
The image of the minimum distance decoder is given as an element having minimum number of 1 among the equivalent class. The image of the minimum distance decoders for the equivalent classes, $[(0,0,0,0,0,0,0)^T]$, $[(0,0,0,0,1,0,0)^T]$, $[(0,0,0,0,0,1,0)^T]$, and $[(0,0,0,0,0,0,1)^T]$ are given by $(0,0,0,0,0,0,0)^T$, $(0,0,0,0,1,0,0)^T$, $(0,0,0,0,0,1,0)^T$, and $(0,0,0,0,0,0,1)^T$, respectively. On the other hand, the equivalent classes $[(0,0,0,0,1,1,0)^T]$, $[(0,0,0,0,1,0,1)^T]$, $[(0,0,0,0,1,0,1)^T]$, $[(0,0,0,0,0,1,1)^T]$, and $[(0,0,0,0,1,1,1)^T]$ uniquely contain bit sequences $(1,0,0,0,0,0,0)^T$, $(0,0,1,0,0,0,0)^T$, $(0,1,0,0,0,0,0)^T$, and $(0,0,0,1,0,0,0)^T$ including 1 at once, respectively. Hence, the bit sequences is the image of the minimum distance decoders, respectively. Therefore, since the set $\{J([X^n])\}_{[X^n]\in\mathbb{F}_2^7/C_{H,1}}$ contains all of bit sequences including 1 at most once, any one bit error can be corrected.

Exercise 9.4
$(1-p)^7 + 7p(1-p)^6$.

Exercise 9.5
Since all of column vectors of H_2 are given as linear combinations of column vectors of H_1, the code space $C_{H,1}$ contains the code space $C_{H,2}$.

Exercise 9.6
Due to the preceding discussions, it is sufficient to show that arbitrary two row vectors of the generating matrix H_2 of $C_{H,2}$ are linearly independent. This fact can be easily shown from the definition of H_2.

Exercise 9.7

When the 3×3 matrix given from the three row vectors is not surjective, the three bits have information concerning $[X]_N$. That is, it is sufficient to choose three linearly dependent row vectors. All of such three row vectors are the following 7 cases. (1,2,3), (1,5,6), (2,6,7), (3,5,7), (1,4,7), (2,4,5), (3,4,6).

Exercise 9.8

Due to the preceding discussion, it is sufficient to show that any three row vectors of the generating matrix H_1 of $C_{H,1}$ are linearly independent. This fact can be checked by the definition of H_1.

Exercise 9.9

Due to the preceding discussion, it is sufficient to show that any three row vectors of the generating matrix H_4 of $C_{H,4}$ are linearly independent. This fact can be checked by the definition of H_4.

Exercise 9.10

Since all of column vectors of the matrix H_1 are orthogonal to all of column vectors of the matrix H_2, we obtain $C_{H,1} \subset C_{H,2}^{\vdash}$. Because both dimensions of $C_{H,1}$ and $C_{H,2}^{\vdash}$ are 4, $C_{H,1} = C_{H,2}^{\vdash}$.

Exercise 9.11

First, we see that $\sum_{\boldsymbol{x}} 2^{-n}(-1)^{(\boldsymbol{t}-\boldsymbol{t}')\cdot\boldsymbol{x}} = 0$ for $\boldsymbol{t} \neq \boldsymbol{t}'$ and $\sum_{\boldsymbol{x}} 2^{-n}(-1)^{(\boldsymbol{t}-\boldsymbol{t})\cdot\boldsymbol{x}} = 1$. Hence,

$$
\begin{aligned}
&(\Lambda_{\mathrm{E}}(\rho_{\mathrm{mix}})) \\
=&\sum_{\boldsymbol{x}} 2^{-n} \sum_{\boldsymbol{s}} P_1^{(n)}(\boldsymbol{s}) \sum_{\boldsymbol{t},\boldsymbol{t}'} \sqrt{P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})}\sqrt{P_{2|1}^{(n)}(\boldsymbol{t}'|\boldsymbol{s})}(-1)^{(\boldsymbol{t}-\boldsymbol{t}')\cdot\boldsymbol{x}}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t}')| \\
=&\sum_{\boldsymbol{s}} P_1^{(n)}(\boldsymbol{s}) \sum_{\boldsymbol{t}} \sqrt{P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})}\sqrt{P_{2|1}^{(n)}(\boldsymbol{t}|\boldsymbol{s})}|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})| \\
=&\sum_{\boldsymbol{s},\boldsymbol{t}} P_1^{(n)}(\boldsymbol{s},\boldsymbol{t})|(\boldsymbol{s},\boldsymbol{t})\rangle\langle(\boldsymbol{s},\boldsymbol{t})|.
\end{aligned}
$$

Thus, we obtain (9.39).

Exercise A.1

Properties (v6) and (v8) imply that $|\psi\rangle = (1+0)\cdot|\psi\rangle = |\psi\rangle + 0\cdot|\psi\rangle$. Adding $-|\psi\rangle$ in the both side, we obtain $0 = 0 + 0\cdot|\psi\rangle = 0\cdot|\psi\rangle$. Property (v8) yields that $|\psi\rangle + -1\cdot|\psi\rangle = (1-1)\cdot|\psi\rangle = 0$. Due to Property (v4) (Uniqueness of the inverse element), we obtain $-1\cdot|\psi\rangle = -|\psi\rangle$.

Exercise A.2

Let $\{|\psi_i\rangle\}_{i=1}^d$ be a basis of the vector space V. When the relation $\sum_{i=1}^d a_i|\psi_i\rangle = \sum_{i=1}^d a_i'|\psi_i\rangle$ holds, we have $\sum_{i=1}^d (a_i - a_i')|\psi_i\rangle = 0$. Since all of basis are linearly independent of each other, the relation $a_i - a_i' = 0$ holds for all i.

Exercise A.3

Assume that there does not exists a vector linearly independent of $\{|\psi_i\rangle\}_{i=1}^n$. Then, we see that the set $\{|\psi_i\rangle\}_{i=1}^n$ is complete in V. This contradicts the footnote 6 of Appendix A. Repeating the same discussion, we can choose $d-n$ vectors linearly independent of other $d-n-1$ vectors and $\{|\psi_i\rangle\}_{i=1}^n$.

Exercise A.4

The relation (A.1) guarantees that the linear independence and the completeness of the set $\{|e_i\rangle\}_{i=1}^d$.

Exercise A.5

Taking the inner product between $|\psi_j\rangle$ and the both sides of $|\psi\rangle = \sum_i a_i|\psi_i\rangle$, we obtain $a_j = \langle\psi_j|\psi\rangle$.

Exercise A.6

Using the discussion in Exercise A.3, we make a basis of V. Then, applying Gram-Schmidt orthogonalization, we obtain an ONB of V.

Exercise A.7

[⇒]: When $|\psi_i\rangle$ is an ONB of $\mathcal{H}$, we have $\langle\psi_i|\xi-\chi\rangle = 0\ \forall i$. Due to Exercise A.5, we have $|\xi\rangle - |\chi\rangle = \sum_i 0|\psi_i\rangle = 0$.

[⇐]: Trivial.

Exercise A.8

It is immediate that (A.9) and (A.10) satisfy (v1)-(v8). (In particular, zero vector and the inverse vector of A are given by the zero operator and $-1\cdot A$.) Let $\{|\psi_i\rangle\}_{i=1}^{d_1}$ and $\{|\phi_i\rangle\}_{i=1}^{d_2}$ be bases of V_1 and V_2. Define d_1d_2 linear operators $A_{ij}\in\mathcal{L}(V_1,V_2)$ $(i=1,\dots,d_1,\ j=1,\dots,d_2)$ by $A_{ij}|\psi_k\rangle = \delta_{jk}|\phi_i\rangle$ $(k=1,\dots,d_1)$. Then, we can show that $\{A_{ij}\}_{i,j}$ forms a basis of the vector space $\mathcal{L}(V_1.V_2)$. (Show this fact.) Hence, $\mathcal{L}(V_1.V_2)$ is a d_1d_2-dimensional vector space.

Exercise A.9

Properties (i), (ii) and (iii) can be checked by straightforward calculations.

Property (iv) can be shown as follows. Since $\langle\phi|AB\psi\rangle = \langle A^\dagger\phi|B\psi\rangle = \langle B^\dagger A^\dagger\phi|\psi\rangle$, (A.13) implies that $(AB)^\dagger = B^\dagger A^\dagger$.

Exercise A.10

Since the relation $\langle(|\psi\rangle\langle\phi|)\xi|\eta\rangle = \langle\langle\phi|\xi\rangle\psi|\eta\rangle = \overline{\langle\phi|\xi\rangle}\langle\psi|\eta\rangle = \langle\xi|\langle\psi|\eta\rangle\phi\rangle = \langle\xi|(|\phi\rangle\langle\psi|)\eta\rangle$ holds for an arbitrary element $|\xi\rangle, |\eta\rangle\in\mathcal{H}$, (A.13) guarantees that $|\psi\rangle\langle\phi| = |\phi\rangle\langle\psi|^\dagger$.

Exercise A.11

(i) Since $A|\psi\rangle = a|\psi\rangle$, we have $0 = ||(A-a\,I)\psi||^2 = \langle(A-a\,I)\psi|(A-a\,I)\psi\rangle = \langle\psi|(A-a\,I)^\dagger(A-a\,I)\psi\rangle = \langle\psi|(A^\dagger-\overline{a}\,I)(A-a\,I)\psi\rangle = \langle\psi|(A-a\,I)(A^\dagger-\overline{a}\,I)\psi\rangle = \langle(A^\dagger-\overline{a}\,I)\psi|(A^\dagger-\overline{a}\,I)\psi\rangle = ||(A^\dagger-\overline{a}\,I)\psi||^2$, where the fifth equation follows from the relation $AA^\dagger = A^\dagger A$. Hence, we obtain $A^\dagger|\psi\rangle = \overline{a}|\psi\rangle$.

(ii) We choose two eigenvectors $|\psi_a\rangle$ and $|\psi_b\rangle$ satisfying that $A|\psi_a\rangle = a|\psi_a\rangle$, $A|\psi_b\rangle = b|\psi_b\rangle$ ($a \neq b, |\psi_a\rangle, |\psi_b\rangle \neq 0$). Property (i) implies that $a\langle\psi_b|\psi_a\rangle = \langle\psi_b|a\psi_a\rangle = \langle\psi_b|A\psi_a\rangle = \langle A^\dagger\psi_b|\psi_a\rangle = \langle\overline{b}\psi_b|a\psi_a\rangle = b\langle\psi_b|\psi_a\rangle$. Since $(a - b)\langle\psi_a|\psi_b\rangle = 0$ ($a \neq b$), we obtain $\langle\psi_a|\psi_b\rangle = 0$.

Exercise A.12
Define a linear operator U by the relation $|\psi_i\rangle = U|\phi_i\rangle$ (See footnote 16 in Appendix A.3.1). By observing that $\langle\phi_i|\mathrm{i}\phi_j\rangle = \delta_{ij} = \langle\psi_i|\psi_j\rangle = \langle U\phi_i|U\phi_j\rangle = \langle\phi_i|U^\dagger U\phi_j\rangle$, one has the unitarity condition $UU^\dagger = I$.

Exercise A.13
For any $|\psi\rangle \in \mathcal{H}$, we have $\langle\psi|B^\dagger B\psi\rangle = \langle B\psi|B\psi\rangle \geq 0$.

Exercise A.14
The desired argument can be shown from Exercise A.5.

Exercise A.15
Assume that the dimensions of W_1 and W_2 are n and l. We choose their ONBs $\{|\phi_i\rangle\}_{i=1}^{n}$ and $\{|\phi_i\rangle_{i=n+1}^{n+l}\}$. Then, we have $P_1 = \sum_{i=1}^{n}|\phi_i\rangle\langle\phi_i|$, $P_2 = \sum_{i=n+1}^{n+l}|\phi_i\rangle\langle\phi_i|$. Since $\{|\phi_i\rangle\}_{i=1}^{n+l}$ is a normalized orthogonal system, we obtain $W_1 \oplus W_2 =$ span $\{|\phi_i\rangle\}_{i=1}^{n+l}$. Hence, the projection operator onto $W_1 \oplus W_2$ is $\sum_{i=1}^{n+l}|\phi_i\rangle\langle\phi_i| = P_1 + P_2$.

Exercise A.16
For a Hermitian operator A, we choose an eigenvalue a and the corresponding eigenvector $|\psi\rangle$. Hence, $A|\psi\rangle = a|\psi\rangle$ ($|\psi\rangle \neq 0$), which implies $a\langle\psi|\psi\rangle = \langle\psi|A\psi\rangle = \langle A^\dagger\psi|\psi\rangle = \langle A\psi|\psi\rangle = \langle a\psi|\psi\rangle = \overline{a}\langle\psi|\psi\rangle$. Thus, $a = \overline{a}$.

For a unitary operator U, we choose an eigenvalue u and the corresponding eigenvector $|\psi\rangle$. Hence, $U|\psi\rangle = u|\psi\rangle$ ($|\psi\rangle \neq 0$), which implies $|u|^2\langle\psi|\psi\rangle = \langle u\psi|u\psi\rangle = \langle U\psi|U\psi\rangle = \langle\psi|U^\dagger U\psi\rangle = \langle\psi|\psi\rangle$. Thus, we obtain $|u| = 1$.

For a positive operator B, we choose an eigenvalue b and the corresponding eigenvector $|\psi\rangle$. We have $B|\psi\rangle = b|\psi\rangle$ ($|\psi\rangle \neq 0$). Hence, $b\langle\psi|\psi\rangle = \langle\psi|B\psi\rangle \geq 0$. Thus, $b \geq 0$.

For a projection operator P, we choose an eigenvalue p and the corresponding eigenvector $|\psi\rangle$. We have $P|\psi\rangle = p|\psi\rangle$ ($|\psi\rangle \neq 0$). Hence, $p\langle\psi|\psi\rangle = \langle\psi|P\psi\rangle = \langle\psi|P^2\psi\rangle = p^2\langle\psi|\psi\rangle$. Thus $p^2 = p \Leftrightarrow p = 0, 1$.

Exercise A.17
Assume that A is a Hermitian operator on a d-dimensional vector space. Since a Hermitian operator A has at most d eigenvalues, the function $f_a(x) := \Pi_{b\in\sigma(A)}(x - b)/\Pi_{a\neq b\in\sigma(A)}(a - b)$ is a polynomial. Since the relation $f_a(b) = \delta_{ab}$ ($b \in \sigma(A)$) holds, we obtain $f_a(A) = \sum_{b\in\sigma(A)} f_a(b)P_b = P_a$.

Exercise A.18

Taking a trace over $A = \sum_i a_i |\phi_i\rangle\langle\phi_i|$, which is an eigenvalue-decomposition of A, we have $\mathrm{Tr} A = \sum_i a_i \mathrm{Tr}(|\phi_i\rangle\langle\phi_i|) = \sum_i a_i$.

Exercise A.19

$\mathrm{Tr}(A|\psi\rangle\langle\phi|) = \sum_i \langle\phi_i|(A|\psi\rangle\langle\phi|)\phi_i\rangle = \sum_i \langle\phi|\phi_i\rangle\langle\phi_i|A\psi\rangle = \langle\phi|(\sum_i |\phi_i\rangle\langle\phi_i|) A\psi\rangle = \langle\phi|A\psi\rangle$.

Exercise A.20

The matrix representation given in this exercise can be obtained by considering the matrix representation based on the basis used in the vector representation (A.34).

Exercise A.21

The condition (i) of a norm implies the condition (i) of a distance. The condition (ii) of a norm implies the condition (ii) of a distance. The condition (iii) of a norm implies the condition (iii) of a distance.

Exercise A.22

(i) $\|A\| \geq 0$ is trivial. When $\|A\| = 0$, (A.41) guarantees the relations $\|Ax\| \leq \|A\|\|x\| = 0$ for any $x \neq 0$. Since $Ax = 0$ holds for $\forall x \in \mathcal{H}$, we have $A = 0$.
(ii) $\|A + B\| = \max_{x\neq 0} \frac{\|(A+B)x\|}{\|x\|} \leq \max_{x\neq 0} \frac{\|Ax\|}{\|x\|} + \max_{x\neq 0} \frac{\|Bx\|}{\|x\|} = \|A\| + \|B\|$.
(iii) The relation $\|\alpha A\| = |\alpha|\|A\|$ is trivial.

Exercise A.23

The unit element with respect to addition in $\mathbb{F}_2$ is 0. The unit element with respect to multiplication in $\mathbb{F}_2$ is 1. Hence, we can find that $\mathbb{F}_2$ satisfies the conditions of a field.

Exercise A.24

The zero vector of $\mathbb{F}_2^d$ is $(0, \ldots, 0)^T$. Since $\psi + \psi = (x_1 \oplus x_1, \ldots, x_d \oplus x_d)^T = (0, \ldots, 0)^T$, the inverse vector of ψ is ψ.

Exercise A.25

The set $\mathbb{F}_2$ is a one-dimensional vector space over the finite field $\mathbb{F}_2$.

Exercise A.26

2^d

Exercise A.27

$d - k$

Exercise A.28

Since $(x + y) - y = x \in C$, y belongs to $[x + y]$.

Exercise A.29

d

Exercise A.30

It is sufficient to show that for any non-zero vector $\boldsymbol{s} \in \mathbb{F}_2^n$, there exists a vector $\boldsymbol{t} \in \mathbb{F}_2^n$ such that $(\boldsymbol{s}|\boldsymbol{t})$ is not 0. The vector $\boldsymbol{s}$ has one non-zero component at least. Assume that the jth component of $\boldsymbol{s}$ is not zero. We choose the vector $\boldsymbol{t}$ such that the jth component of $\boldsymbol{t}$ is 1 and the other component of $\boldsymbol{t}$ is 0. Hence, the vector $\boldsymbol{t}$ satisfies the above requirement.

Exercise A.31

It is sufficient to show that for any non-zero vector $\vec{s} \in \mathbb{F}_2^{2n}$, there exists a vector $\vec{s}' \in \mathbb{F}_2^{2n}$ such that $\langle \vec{s}, \vec{s}' \rangle$ is not 0. The vector $\vec{s}$ has one non-zero component at least. Assume that the jth component of $\vec{s}$ is not zero. When $j > n$, we choose the vector $\vec{s}'$ such that the $j - n$th component of $\vec{s}'$ is 1 and the other component of $\vec{s}'$ is 0. Hence, the vector $\vec{s}'$ satisfies the above requirement. When $j \leq n$, we choose the vector $\vec{s}'$ such that the $j + n$th component of $\vec{s}'$ is 1 and the other component of $\vec{s}'$ is 0. Hence, the vector $\vec{s}'$ satisfies the above requirement.

References

1. M. Reed, B. Simon, *Methods of Modern Mathematical Physics I: Functional Analysis* (Academic Press, San Diego, 1980)
2. M. Hayashi, F. Sakaguchi, J. Phys. A Math. Gen. **33**, 7793–7820 (2000)
3. J.B. Conway, *A Course in Functional Analysis*, 2nd edn. (Springer, Heidelberg, 1990)
4. A.S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982)
5. H. Nagaoka, M. Hayashi, IEEE Trans. Inform. Theory **53**, 534–549 (2007)
6. R. Bhatia, *Matrix Analysis* (Springer, Heidelberg, 1997)
7. Y. Ogata, Lett. Math. Phys. **97**, 339–346 (2011)
8. M. Hayashi, *Quantum Information: An Introduction* (Springer, Berlin, 2006). Originally published in Japanese in 2004

Index

M. Hayashi et al., *Introduction to Quantum Information Science*,
Graduate Texts in Physics, DOI: 10.1007/978-3-662-43502-1,