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,

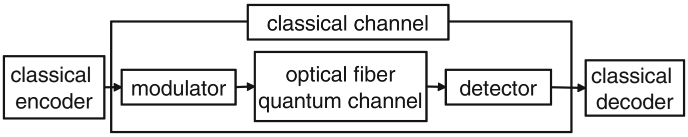

Fig. 1.1 Classical treatment of the optical communication

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.

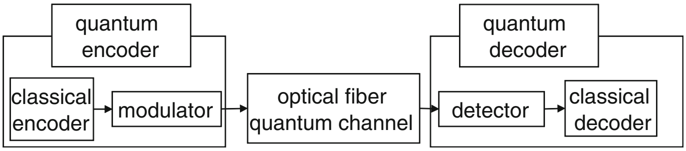

Fig. 1.2 Optical communication as quantum channel

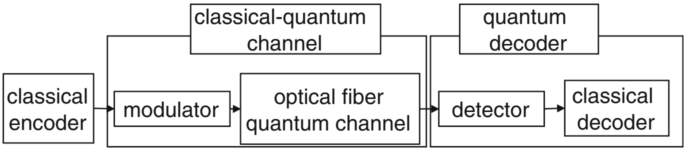

Fig. 1.3 Optical communication as classical-quantum channel

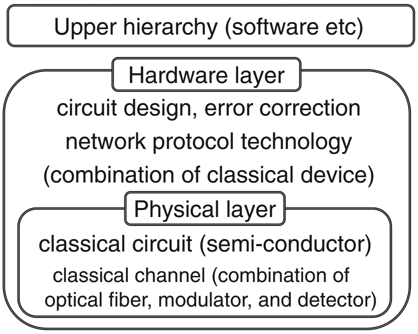

Fig. 1.4 Current hierarchical structure of information processing (Computer and communication)

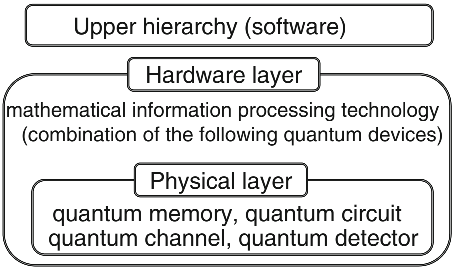

Fig. 1.5 Future hierarchical structure of information processing (Computer and communication)

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)

http://www.springer.com/978-3-662-43501-4

Introduction to Quantum Information Science
Hayashi, M.; Ishizaka, S.; Kawachi, A.; Kimura, G.;
Ogawa, T.
2015, XIV, 332 p. 31 illus., 1 illus. in color., Hardcover
ISBN: 978-3-662-43501-4