Long-distance quantum communication with remote nondestructive parity measurement

Koji Azuma

Osaka University
Graduate School of Engineering Science

March 2010

Long-distance quantum communication with remote nondestructive parity measurement

A dissertation submitted to

THE GRADUATE SCHOOL OF ENGINEERING SCIENCE
OSAKA UNIVERSITY

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN SCIENCE

presented by

Koji Azuma

born May 12, 1982, in Japan

supervised by

Prof. Dr. Nobuyuki Imoto.

March 2010

Acknowledgements

I would like to thank Prof. Dr. Nobuyuki Imoto. His trust and support have given me the power to continue my researches with a robust will and to boost my abilities, and his clever ideas appearing in discussions have guided me to the right direction of my studies. In addition, I can never forget his encouragement that has been given when I was disappointed. I am also genuinely grateful to Prof. Dr. Masato Koashi. Without his insightful and ingenious advices not only on my studies and but also on the crossroads in my life, my researches and my life would be widely different from the present ones. It is not exaggerate to say that my efforts on the studies have devoted to get his positive acceptations. I was looking forward to discussing with him. I also appreciate all my collaborators, Prof. Dr. Kazuto Ohshima, Dr. Junichi Shimamura, Dr. Hosho Katsura, Naoya Sota, Dr. Ryo Namiki, Dr. Şahin Kaya Özdemir, Dr. Takashi Yamamoto, and Hitoshi Takeda. They have taught many things needed to develop the studies to me. Moreover, my time passing with them was fruitful and significant, which has provided me driving forces. My special thanks go to Prof. Dr. Naoto Nagaosa, Prof. Dr. Hideaki Ujino, Prof. Dr. Shuich Murakami, Dr. Kei Sawada, Dr. Naoyuki Sugimoto, Takashi Ohnishi, and Shun-ichi Kuga. They have triggered my decision to go this doctoral course, and have taught me many things to live as a researcher. A lot of people have helped my studies, both directly and indirectly. A part of the people is composed of Yoritoshi Adachi, Sachiko Arimoto, Aya Bouno, Dr. Yuki Fuseya, Yuya Kobayashi, Shugo Mikami, Dr. Toshiyuki Tashima, Dr. Yuuki Tokunaga, Toshiyuki Yamagata, and Kazuhiro Yokota. I owe many thanks to Prof. Dr. Masahiro Kitagawa and Prof. Dr. Hiroshi Yoshida for examining this thesis. Finally, I would like to thank my family for their continuous support and encouragement of my study. This work was supported by JSPS Research Fellowships for Young Scientists 19·1377.

Koji Azuma
Osaka University

Preface

About 80 years have passed since quantum mechanics was completed. For those days, quantum mechanics not only has presented clear understanding of physical phenomena ranging from particle physics to cosmology, but also has contributed to engineering through the design of materials. However, these successes seem to be merely indirect evidence to ensure the validity of quantum mechanics itself, because several principles of quantum mechanics – e.g., the back action inevitably caused by the measurement – are not needed for the successes and are not sufficiently tested. In other words, for giving the direct proof of the validity of quantum mechanics, we have to list various phenomena that can be predictable solely by the combinations of the all the principles of quantum mechanics, and we must test them. This kind of concepts has already been taken by quantum information theory.

Quantum information theory is an area where, by constructively utilizing all the principles of quantum mechanics and by borrowing the concept of information theory, it is tried to seek striking quantum phenomena, the possibility of novel applications for information processing, and the fundamental limits lying in the quantum world. This new approach has already revealed many novel aspects of quantum mechanics ranging from the fundamentals to the novel applications. In fact, the non-locality [1, 2, 3] of distant quantum systems – which is called quantum entanglement – is featured as a fundamental property of the quantum world, and the quantification and the operational characterizations have been successfully accomplished [4]. Moreover, quantum computation and communication – which are recognized as significant goals of the development of quantum technologies – are shown to be applications that are considered intractable on conventional computers and communication. In fact, quantum computation has the potential to efficiently solve several problems that seem to be beyond the active field of classical computers, e.g., finding the prime factors of large integers [5], simulating the dynamics of quantum systems [6, 7], and searching marked data in a lot of data [8]. Quantum communication promises to enable novel applications such as absolutely secure communication [9, 10, 11, 12, 13, 14, 15, 16, 17, 18] and distributed quantum computation [19]. However, at present, merely primitive operations of quantum computation are realized [20, 21, 22, 23, 24, 25], and quantum communication more than 300 km has not yet been reported [26, 27]. Hence, it has become really important to seek feasible architectures for long-distance ($\sim$ 1000 km) quantum communication and quantum computation.

As the first step toward this goal, in this thesis, we quest a promising architecture to make quantum communication possible over long distances. Quantum communication usually utilizes optical pulses as the carrier of quantum information. However, the real transmission channel for optical pulses suffers from the loss that increases exponentially with the channel length, which

makes it practically impossible to extend the distance of quantum communication based on the direct distribution of optical pulses. Instead, for long-distance quantum communication, it is known to be better to invoke quantum repeater protocols [28, 29], which need repeaters with quantum memories between the two-end parties as the infrastructure. The protocols aim to generate quantum entanglement between the two-end parties, relying on the quantum teleportation protocol [30] that enables quantum communication by consuming quantum entanglement. Actually, there are several repeater protocols depending on the types of quantum memories [31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43].

One promising candidate of quantum repeaters is based on atomic-ensemble quantum memories [31, 32, 33, 34, 35, 36]. These protocols are composed of two primitive operations, 'entanglement generation between repeaters' and 'entanglement connection.' Under the situation where only photon losses are considered as error, the protocols enable the communication time to scale sub-exponentially with the communication length. However, since the protocols have difficulties to implement a scheme to recover quantum entanglement – entanglement distillation, these protocols do not have countermeasures against the other types of noises.

Another candidate called 'hybrid quantum repeater protocols' [40, 41, 42, 43] is based on an off-resonance coupling between an optical pulse and a qubit, which allows us to use various qubit systems as the quantum memories. For example, individual Λ-type atoms, single electrons trapped in quantum dots, and nitrogen-vacancy (NV) centers in a diamond with a nuclear spin degree of freedom can be used as quantum memories. However, for achieving a sufficient coupling between an optical pulse and a qubit, it may be needed to confine the qubit in a cavity. Differently from the repeater protocols based on atomic-ensemble quantum memories, the hybrid quantum repeater protocols are composed of all the primitive operations that are considered to be needed for general settings, i.e., entanglement generation between repeaters, entanglement connection, and entanglement distillation. Although it has been reported [40, 43] that the protocol shows efficient communication times, the entanglement connection and the entanglement distillation rely on hypothetically efficient local gates on two qubits (CZ gate) [44, 45]. In fact, the local gates are too complicated to be accomplished with such high efficiencies [46].

In this thesis, we present a single module on two qubits – remote nondestructive parity measurement (RNPM) – that promises to accomplish efficient long-distance quantum communication under arbitrary types of noises. The RNPM is based on the same quantum memories and off-resonance coupling that are used in the hybrid quantum repeater protocols, which implies the applicability of the RNPM to various qubit systems. In particular, the RNPM is achieved by application of off-resonance laser pulses to be reflected dependently on the state of qubits and by manipulation on the pulses based on a simple combination of beam splitters and photon detectors. Despite this simplicity, the RNPM allows us to implement all the operations needed for long-distance quantum communication, namely, entanglement generation, entanglement connection, and entanglement distillation. In addition, we prove that the entanglement generation based on the RNPM achieves the theoretical limit of performance among arbitrary protocols to generate entanglement with one type of error. Moreover, we show that the progressive improvement of RNPM opens up the possibility of measurement-based quantum computation [47, 48, 49].

This thesis is organized as follows. Chapter 1 and Chapter 2 are brief reviews on quantum mechanics and quantum communication. In Chapter 3, we provide an entanglement generation protocol between distant qubits, and we show that it has higher efficiencies than known protocols [31, 37, 38, 40, 41, 42, 43] found in the development of quantum repeaters. In Chapter 4, deriving the theoretical limit of performance of protocols to generate entanglement with only one type

of error, we prove that the proposed protocol achieves the upper limit. In Chapter 5, we show that the proposed protocol actually plays the role of the RNPM, and we further clarify the possibility of striking applications of the RNPM. In Chapter 6, we estimate the performance of long-distance quantum communication based on the RNPM, and show that the communication time scales sub-exponentially with the channel length. There, we further show that the nested-purification repeater protocol [28, 29] is also achievable by the RNPM. Chapter 7 concludes this thesis.

This thesis is based on three papers as follows:

Chapter 3: Koji Azuma, Naoya Sota, Ryo Namiki, Şahin Kaya Özdemir, Takashi Yamamoto, Masato Koashi, and Nobuyuki Imoto, Optimal entanglement generation for efficient hybrid quantum repeaters. Phys. Rev. A **80**, 060303 (R) (2009).

Chapter 4: Koji Azuma, Naoya Sota, Masato Koashi, and Nobuyuki Imoto, Tight bound on coherent-state-based entanglement generation over lossy channels. arXiv:0908.2735 [Phys. Rev. A (to be published)].

Chapters 5 and 6: Koji Azuma, Hitoshi Takeda, Masato Koashi, and Nobuyuki Imoto, Quantum repeaters built on a single module: Remote nondestructive parity measurement. In preparation.

Contents

1

Quantum mechanics

One of most successful theories in physics is the so-called *quantum mechanics*. This theory features considering the back action of the measurement process as a law of nature. In this chapter, we briefly review the principle of quantum mechanics†. In the last of this chapter, we provide the no-cloning theorem clarifying a striking difference between our ordinary worldview and the quantum world. This chapter contains the basic knowledge to understand the subsequent chapters.

1.1 Properties for linear operators.

Quantum mechanics is based on the *linear algebra*. Without proofs‡, here we mention on several properties of representative linear operators:

Normal operators: A linear operator $\hat{A}$ satisfying $\hat{A}^\dagger\hat{A} = \hat{A}\hat{A}^\dagger$ is called *normal operator*. For a normal operator $\hat{A}$, we can always find an orthonormal basis $\{|i\rangle\}$ such that $\hat{A} = \sum_i a_i|i\rangle\langle i|$. The form of $\hat{A} = \sum_i a_i|i\rangle\langle i|$ is specifically called the *spectral decomposition* of $\hat{A}$.

Hermitian operators: A linear operator $\hat{A}$ satisfying $\hat{A}^\dagger = \hat{A}$ is called *Hermitian operator*. Since any Hermitian operator $\hat{A}$ is normal, $\hat{A}$ can be always represented by $\hat{A} = \sum_i a_i|i\rangle\langle i|$ with an orthonormal basis $\{|i\rangle\}$. Note that $\hat{A}^\dagger = \hat{A}$ means $a_i^* = a_i$. Thus, any Hermitian operator $\hat{A}$ can be always represented by $\hat{A} = \sum_i a_i|i\rangle\langle i|$ with an orthonormal basis $\{|i\rangle\}$ and real numbers $\{a_i\}$.

Positive operators: A linear operator $\hat{A}$ is called *positive operator* if and only if $\langle\phi|\hat{A}|\phi\rangle \geq 0$ holds for any vector $|\phi\rangle$. Since any positive operator $\hat{A}$ is Hermitian§, the operator $\hat{A}$ can be always represented by $\hat{A} = \sum_i a_i|i\rangle\langle i|$ with an orthonormal basis $\{|i\rangle\}$ and nonnegative numbers $\{a_i\}$.

Unitary operators: A linear operator $\hat{A}$ satisfying $\hat{A}^\dagger\hat{A} = \hat{A}\hat{A}^\dagger = \hat{I}$ is called *unitary operator*. Any unitary operator $\hat{A}$ can be represented by $\hat{A} = \sum_i |w_i\rangle\langle v_i|$ with complete orthonormal bases $\{|v_i\rangle\}$ and $\{|w_i\rangle\}$.

We may use *operator functions* defined by the following: If we have a function f mapping complex numbers to complex numbers, we can define the operator function on normal operators

† This chapter is based on the lectures of Koashi, on the text book of Nielsen and Chuang [50], and on the lecture note of Preskill [51].

‡ For example, the proofs can be found in Ref. [52]

§ This fact is proved as follows. Note $\hat{A} = \hat{B} + i\hat{C}$ with $\hat{B} := (\hat{A} + \hat{A}^\dagger)/2$ and $\hat{C} := (\hat{A} - \hat{A}^\dagger)/(2i)$. Then, $\langle\phi|\hat{C}|\phi\rangle = \mathrm{Im}[\langle\phi|\hat{A}|\phi\rangle]$ holds but $\hat{C}$ is an Hermitian operator. This means $\langle\phi|\hat{C}|\phi\rangle = 0$, which concludes $\hat{A} = \hat{A}^\dagger$.

as $f(\hat{A}) := \sum_i f(a_i)|a_i\rangle\langle a_i|$, where $\hat{A}$ is a normal operator with spectral decomposition $\hat{A} = \sum_i a_i|a_i\rangle\langle a_i|$.

We may also use the following theorem†:

Theorem 1.1 (Simultaneous spectral decomposition for Hermitian operators) *Suppose that two Hermitian operators $\hat{A}$ and $\hat{B}$ commute, i.e., $[\hat{A}, \hat{B}] := \hat{A}\hat{B} - \hat{B}\hat{A} = 0$. Then, there exists an orthonormal basis $\{|a, b, k\rangle\}_{a,b,k}$ such that $\hat{A} = \sum_{a,b,k} a|a, b, k\rangle\langle a, b, k|$ and $\hat{B} = \sum_{a,b,k} b|a, b, k\rangle\langle a, b, k|$.*

1.2 The postulates of quantum mechanics

In the classical world, the measurement is merely a process of giving us an outcome to learn the state of a physical system, and it is considered to be, in principle, performed without disturbing the state of the system. That is, in the classical mechanics, the state of a system is, in principle, determined by sequential measurements of various physical quantities on the system. But, in the quantum world, the measurement is not such a simple process. In fact, there is a measurement that not only returns such an outcome but also inevitably causes a back action on the system. In order to describe phenomena including this complicated measurement process, quantum mechanics divides the description of the state from that of the measurement process.

The quantum mechanics is formed by the following four postulates:

Postulate 1: A physical system corresponds to a *Hilbert space* $\mathcal{H}$ – a vector space with an inner product $(|v\rangle, |w\rangle) =: \langle v|w\rangle$ that is also a complete metric space with respect to the distance function induced by norm $|||v\rangle|| := \sqrt{\langle v|v\rangle}$. The state of the system is described by a *ray* $|\psi\rangle$, which is $|\psi\rangle \in \{\alpha|\psi\rangle \mid \alpha \in \boldsymbol{C}, |\alpha| = 1, |\psi\rangle \in \mathcal{H}\}$.

Postulate 2: The time evolution of a closed system is represented by a unitary operator. Let $|\psi(t)\rangle$ be a state of the system at time t. The time evolution from time t_i to time t_f satisfies

$$|\psi(t_f)\rangle = \hat{U}|\psi(t_i)\rangle, \tag{1.1}$$

where $\hat{U}$ is a unitary operator. Note that, by regarding $\hat{U} = \exp[-i\hat{H}(t_f - t_i)/\hbar]$, Eq. (1.1) corresponds to the solution of the well-known *Schrödinger equation*:

$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle, \tag{1.2}$$

where $\hat{H}$ is an Hermitian operator called *Hamiltonian*, and $\hbar$ is defined as $\hbar := h/(2\pi)$ with the *Plank constant* h.

Postulate 3: A physical quantity A corresponds to an Hermitian operator $\hat{A}$.‡ Since $\hat{A}$ is an Hermitian operator, $\hat{A}$ is diagonalizable as follows:

$$\hat{A} = \sum_i a_i|a_i\rangle\langle a_i|, \tag{1.3}$$

where a_i is an eigenvalue of $\hat{A}$ and $|a_i\rangle$ is an eigenvector corresponding to the eigenvalue a_i. Then, we regard a_i as a possible outcome given by the measurement of $\hat{A}$, and $|a_i\rangle$ as a state always giving the measurement outcome a_i. Such an operator $\hat{A}$ is particularly

† For example, the proofs can be found in Ref. [50].

‡ More precisely, the operator $\hat{A}$ is the so-called *self-adjoint operator*.

called an *observable*. In addition, by making measurement of $\hat{A}$ on an initial state $|\psi\rangle$, the state $|\psi\rangle$ is found in state $|a_i\rangle$ with probability

$$p(a_i) = |\langle a_i|\psi\rangle|^2. \tag{1.4}$$

This measurement is called *projective measurement*. From Eq. (1.4), the expectation value $\langle\hat{A}\rangle$ of $\hat{A}$ is given by

$$\langle\hat{A}\rangle = \sum_i a_i p(a_i) = \sum_i a_i \langle\psi|a_i\rangle\langle a_i|\psi\rangle = \langle\psi|\hat{A}|\psi\rangle. \tag{1.5}$$

Postulate 4: Suppose that $\mathcal{H}_A$ and $\mathcal{H}_B$ correspond to physical systems A and B, respectively. Then, the composite system AB corresponds to $\mathcal{H}_A \otimes \mathcal{H}_B$. Moreover, if the systems A and B are prepared in state $|\psi\rangle_A$ and $|\phi\rangle_B$ respectively, the state of $\mathcal{H}_A \otimes \mathcal{H}_B$ corresponds to $|\psi\rangle_A \otimes |\phi\rangle_B (=: |\psi\rangle_A|\phi\rangle_B)$.

Postulate 1 gives the description of a physical system and the state. Postulate 2 determines the dynamics of the physical system. Postulate 3 defines the relation between the physical state and the outcome obtained by the measurement. Postulate 4 specifies the stage to describe a composite system.

As an example, we consider the so-called *qubit* system. This system corresponds to a two-dimensional Hilbert space $\mathcal{H}_A$. Thus, the state of the system can be described by

$$|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A, \tag{1.6}$$

where $|0\rangle$ and $|1\rangle$ are a complete orthonormal basis, $\alpha, \beta \in \boldsymbol{C}$, and $|\alpha|^2 + |\beta|^2 = 1$. The basis $\{|0\rangle, |1\rangle\}$ is specifically called *computational basis* in the context of quantum information processing. The unitary operator of the system is generally represented by

$$\hat{U}^A_{\boldsymbol{n},\varphi} = e^{-i\varphi \boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}^A/2} = \cos\left(\frac{\varphi}{2}\right)\hat{I}^A - i\sin\left(\frac{\varphi}{2}\right)(n_x\hat{X}^A + n_y\hat{Y}^A + n_z\hat{Z}^A), \tag{1.7}$$

where $\varphi \in \boldsymbol{R}$, $\boldsymbol{n} = (n_x, n_y, n_z) \in \boldsymbol{R}^3$ such that $|\boldsymbol{n}| = 1$, $\hat{I}^A = |0\rangle\langle 0|_A + |1\rangle\langle 1|_A$, and $\hat{\boldsymbol{\sigma}}^A = (\hat{X}^A, \hat{Y}^A, \hat{Z}^A)$ with

$$\hat{Z}^A := \hat{\sigma}_z^A := |0\rangle\langle 0|_A - |1\rangle\langle 1|_A, \tag{1.8}$$

$$\hat{X}^A := \hat{\sigma}_x^A := |0\rangle\langle 1|_A + |1\rangle\langle 0|_A, \tag{1.9}$$

$$\hat{Y}^A := \hat{\sigma}_y^A := -i(|0\rangle\langle 1|_A - |1\rangle\langle 0|_A). \tag{1.10}$$

A well used and important unitary operator is the *Hadamard gate* defined by

$$\hat{H}^A := |0_x\rangle\langle 0|_A + |1_x\rangle\langle 1|_A, \tag{1.11}$$

where $|0_x\rangle_A := |+\rangle_A := (|0\rangle_A + |1\rangle_A)/\sqrt{2}$ and $|1_x\rangle_A := |-\rangle_A := (|0\rangle_A - |1\rangle_A)/\sqrt{2}$. The operator $\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}^A$ is an Hermitian operator, and hence this is an observable of the qubit system. By defining $(n_x, n_y, n_z) =: (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, the observable $\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}^A$ can be written as

$$\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}^A = n_x\hat{X}^A + n_y\hat{Y}^A + n_z\hat{Z}^A = |0_{\boldsymbol{n}}\rangle\langle 0_{\boldsymbol{n}}|_A - |1_{\boldsymbol{n}}\rangle\langle 1_{\boldsymbol{n}}|_A \tag{1.12}$$

with

$$\begin{aligned} |0_{\boldsymbol{n}}\rangle_A &= \cos\left(\frac{\theta}{2}\right)|0\rangle_A + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle_A, \\ |1_{\boldsymbol{n}}\rangle_A &= \sin\left(\frac{\theta}{2}\right)|0\rangle_A - e^{i\phi}\cos\left(\frac{\theta}{2}\right)|1\rangle_A. \end{aligned} \tag{1.13}$$

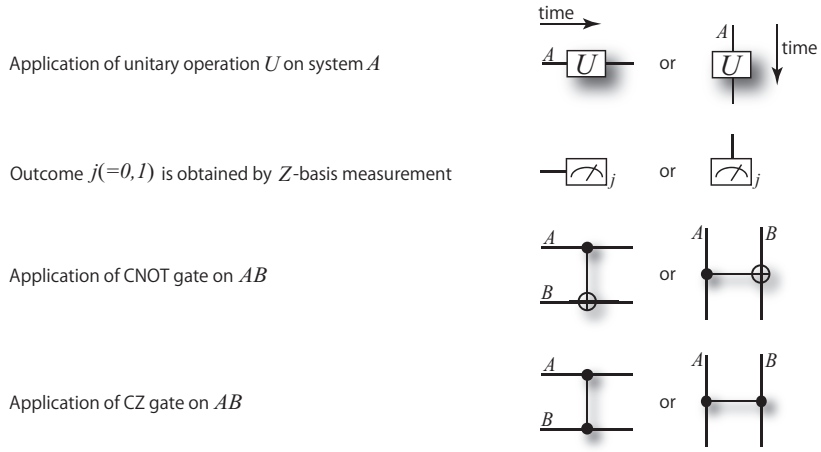

Fig. 1.1. The definition of the schematic descriptions of operations.

The projective measurement of the basis $\{|0_{\boldsymbol{n}}\rangle_A, |1_{\boldsymbol{n}}\rangle_A\}$ is called $\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}^A$-basis measurement. Eq. (1.12) reduces $\hat{U}^A_{\boldsymbol{n},\varphi}$ to a simple form

$$\hat{U}^A_{\boldsymbol{n},\varphi} = e^{-i\varphi/2}|0_{\boldsymbol{n}}\rangle\langle 0_{\boldsymbol{n}}|_A + e^{i\varphi/2}|1_{\boldsymbol{n}}\rangle\langle 1_{\boldsymbol{n}}|_A. \tag{1.14}$$

The combined system of qubit A and qubit B corresponds to the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and hence the state of the system is described by

$$|\psi\rangle_{AB} = \alpha|00\rangle_{AB} + \beta|01\rangle_{AB} + \delta|10\rangle_{AB} + \gamma|11\rangle_{AB} \tag{1.15}$$

with $\alpha, \beta, \delta, \gamma \in \boldsymbol{C}$ and $|\alpha|^2 + |\beta|^2 + |\delta|^2 + |\gamma|^2 = 1$. An important unitary operation of the two qubits is the so-called *CNOT gate* defined by

$$\hat{C}^{AB}_X := |0\rangle\langle 0|_A \otimes \hat{I}_B + |1\rangle\langle 1|_A \otimes \hat{X}^B. \tag{1.16}$$

Since CNOT gate is asymmetric under the change $A \leftrightarrow B$, for clarity, A and B are called *control qubit* and *target qubit*, respectively. A similar unitary operation on two qubits

$$\hat{C}^{AB}_Z := |0\rangle\langle 0|_A \otimes \hat{I}_B + |1\rangle\langle 1|_A \otimes \hat{Z}^B \tag{1.17}$$

is called *CZ gate*. In contrast to CNOT gate, CZ gate is symmetric under the change $A \leftrightarrow B$. In this thesis, these operations are described as in Fig. 1.1.

1.3 The description of the measurement on a subsystem

Here we consider the description of the measurement process on a subsystem and of the state of the subsystem. Let $|\Psi\rangle_{AB}$ be a state of physical systems shared by Alice and Bob. Let us consider a process where Alice and Bob make projective measurements represented by complete orthonormal bases $\{|a_i\rangle_A\}$ and $\{|b_j\rangle_B\}$ on their systems. Then, the probability $p(a_i, b_j)$ with which Alice and Bob find their systems in state $|a_i\rangle_A|b_j\rangle_B$ is given by

$$p(a_i, b_j) = |{}_A\langle a_i|{}_B\langle b_j||\Psi\rangle_{AB}|^2, \tag{1.18}$$

from Postulate 3.

Suppose that the measurement process is actually done through the following two steps: (i)

Alice first makes measurement $\{|a_i\rangle_A\}$ on her system, and finds the system A in state $|a_i\rangle_A$; (ii) Bob then makes measurement $\{|b_j\rangle_B\}$ on his system, and finds the system B in state $|b_j\rangle_B$. Let us assume that Bob's system is described by a state $|\psi_i\rangle_B$ after Alice's measurement. Since Bob makes the measurement on his system in state $|\psi_i\rangle_B$, the probability $p(b_j|a_i)$ with which Bob finds his system in state $|b_j\rangle_B$ is

$$p(b_j|a_i) = |{}_B\langle b_j|\psi_i\rangle_B|^2. \tag{1.19}$$

Substituting Eqs. (1.18) and (1.19) for a relation of probability theory, $p(b_j|a_i)p(a_i) = p(a_i, b_j)$, we have

$$|{}_A\langle a_i|{}_B\langle b_j||\Psi\rangle_{AB}| = |\sqrt{p(a_i)}{}_B\langle b_j|\psi_i\rangle_B|. \tag{1.20}$$

Since this relation should hold for any projective measurement $\{|b_j\rangle_B\}$, we conclude

$$|\psi_i\rangle_B = \frac{{}_A\langle a_i||\Psi\rangle_{AB}}{\sqrt{p(a_i)}}, \tag{1.21}$$

where we used the fact that $|\langle x|y\rangle| = |\langle x|z\rangle|$ for any ray $|x\rangle$ means $|y\rangle = |z\rangle$.

Now, what if Bob does not know what Alice does. More precisely, Bob knows the state $|\Psi\rangle_{AB}$ of a composite system AB, but he never communicate with Alice. Then, how should we describe the state of Bob's system? Probability $p(b_j)$ with which Bob gets result $|b_j\rangle$ from his measurement is

$$\begin{aligned} p(b_j) =& \sum_i p(a_i, b_j) = \sum_i p(b_j|a_i)p(a_i) = \sum_i p(a_i)|{}_B\langle b_j|\psi_i\rangle_B|^2 \\ =& {}_B\langle b_j| \left(\sum_i p(a_i)|\psi_i\rangle_{BB}\langle\psi_i| \right) |b_j\rangle_B \\ =:& {}_B\langle b_j|\hat{\rho}^B|b_j\rangle_B, \end{aligned} \tag{1.22}$$

where we introduced *density operator* $\hat{\rho}^B$ defined by

$$\hat{\rho}^B = \sum_i p(a_i)|\psi_i\rangle_{BB}\langle\psi_i|. \tag{1.23}$$

Since density operator $\hat{\rho}^B$ gives the correct probability distribution $\{p(b_j)\}$ of Bob's measurement, it is a good candidate for the description of the state of Bob's system. From Eq. (1.21), the density operator $\hat{\rho}^B$ can be rewritten as

$$\hat{\rho}^B = \sum_i {}_A\langle a_i||\Psi\rangle_{ABAB}\langle\Psi||a_i\rangle_A \tag{1.24}$$

$$:= \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|], \tag{1.25}$$

where $\mathrm{Tr}_A[\cdot]$ is known as the *partial trace* over system A. Since the partial trace has a property

$$\mathrm{Tr}_A[\hat{C}^A|\Psi\rangle_{ABAB}\langle\Psi|] = \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|\hat{C}^A] \tag{1.26}$$

for any operator $\hat{C}^A$, we have

$$\mathrm{Tr}_A[\hat{U}^A|\Psi\rangle_{ABAB}\langle\Psi|(\hat{U}^A)^\dagger] = \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|] \tag{1.27}$$

for any unitary operator $\hat{U}^A$, which implies that $\hat{\rho}^B$ is invariant for Alice's local unitary operation $\hat{U}^A$. Thus, the density operator $\hat{\rho}^B$ is determined independently of Alice's measurement $\{|a_i\rangle_A\}$, which is compatible with the assumption that Bob does not know what kind of measurement

Alice makes on her system. Hence, it seems to be good to describe the state of system B by the density operator $\hat{\rho}^B$. In the subsequent sections, one can also see why the density operator is a good description of a subsystem.

In this section, we have seen how to describe the measurement process on a subsystem and the state of a subsystem. These can be summarized as follows:

Theorem 1.2 (Projective measurement on a subsystem) *Suppose that a party has system AB in state $|\Psi\rangle_{AB}$, and makes projective measurement represented by a complete orthonormal basis $\{|a_i\rangle_A\}$. If the measurement indicates that the state $|\Psi\rangle_{AB}$ is in state $|a_i\rangle_A$, the state of subsystem B is described by*

$$|\psi_i\rangle_B = \frac{{}_A\langle a_i||\Psi\rangle_{AB}}{\sqrt{p(a_i)}}, \tag{1.28}$$

where $p(a_i)$ is probability with which the party finds the system A in state $|a_i\rangle_A$, and is given by

$$p(a_i) = ||{}_A\langle a_i||\Psi\rangle_{AB}||^2 = \mathrm{Tr}[{}_A\langle a_i||\Psi\rangle_{AB AB}\langle\Psi||a_i\rangle_A]. \tag{1.29}$$

Theorem 1.3 (The description of a subsystem) *Suppose that a composite system AB is in state $|\Psi\rangle_{AB}$. If a party holding subsystem B does not know how system A is manipulated, the state of subsystem B can be described by*

$$\hat{\rho}^B = \mathrm{Tr}_A[|\Psi\rangle_{AB AB}\langle\Psi|]. \tag{1.30}$$

Probability $p(b_i)$ with which state $\hat{\rho}^B$ is found in a state $|b_i\rangle_B$ by projective measurement represented by a complete orthonormal basis $\{|b_i\rangle_B\}$ is

$$p(b_i) = {}_B\langle b_i|\hat{\rho}^B|b_i\rangle_B. \tag{1.31}$$

1.4 The density operator

Here we introduce several properties of the density operator. We start with giving the formal definition of the density operator.

Definition 1.1 *For an ensemble $\{p_i, |\psi_i\rangle\}$, density operator $\hat{\rho}$ is defined by*

$$\hat{\rho} := \sum_i p_i|\psi_i\rangle\langle\psi_i|. \tag{1.32}$$

This indicates that the operator $\hat{\rho}^B$ of Eq. (1.23) is an example of the density operators. We have an equivalent expression of the density operator:

Theorem 1.4 (Density operators) *An operator $\hat{\rho}$ is the density operator if and only if (i) $\mathrm{Tr}[\hat{\rho}] = 1$, and (ii) $\hat{\rho}$ is positive.*

Proof. Suppose that $\hat{\rho}$ satisfies conditions (i) and (ii). Since $\hat{\rho}$ is positive, we can write $\hat{\rho} = \sum_i p_i|i\rangle\langle i|$ with an orthonormal basis $\{|i\rangle\}$ and $p_i \geq 0$. From condition (i), we have $\sum_i p_i = 1$, which concludes that $\hat{\rho}$ has the form of the density operator defined by Eq. (1.32).

Conversely, suppose that $\hat{\rho}$ is a density operator defined by Eq. (1.32). Then, for any vector $|x\rangle$, we have

$$\langle x|\hat{\rho}|x\rangle = \sum_i p_i|\langle x|\psi_i\rangle|^2 \geq 0, \tag{1.33}$$

which means that $\hat{\rho}$ is positive. We can also check $\mathrm{Tr}[\hat{\rho}] = 1$. □

From Theorem 1.4, it is shown that any density operator $\hat{\rho}^A$ of the qubit system A can be described by

$$\hat{\rho}^A = \frac{\hat{I}^A + \boldsymbol{v} \cdot \hat{\boldsymbol{\sigma}}^A}{2}, \tag{1.34}$$

where $\boldsymbol{v} \in \boldsymbol{R}^3$ and $|\boldsymbol{v}| \leq 1$. $\boldsymbol{v}$ is called *Bloch vector*, and it uniquely corresponds to the density operator $\hat{\rho}^A$.

We mention on several terms. Let $\hat{\rho}^{AB}$ be a density operator for a composite system AB. Then, an operator defined by $\hat{\rho}^B := \mathrm{Tr}_A[\hat{\rho}^{AB}]$ is also a density operator on system B. The density operator $\hat{\rho}^B$ is particularly called a *reduced density operator* on system B. If a density operator $\hat{\rho}$ can be written as $\hat{\rho} = |\psi\rangle\langle\psi|$ with a normalized vector $|\psi\rangle$, the density operator $\hat{\rho}$ is called a *pure state*; otherwise the density operator is called a *mixed state*, or a *mixture* of pure states. Here we give a useful fact to judge whether a density operator $\hat{\rho}$ is pure or mixed.

Theorem 1.5 (Pure or mixed?) $\mathrm{Tr}[\hat{\rho}^2] \leq 1$. *The equality holds if and only if $\hat{\rho}$ is a pure state.*

Proof. We represent $\hat{\rho}$ as $\hat{\rho} = \sum_i p_i |i\rangle\langle i|$ with an orthonormal basis $\{|i\rangle\}$. Then, we have

$$\mathrm{Tr}[\hat{\rho}^2] = \sum_i p_i^2 \leq 1. \tag{1.35}$$

Note that $\mathrm{Tr}[\hat{\rho}^2] = 1$ means the existence of i satisfying $p_i = 1$. Conversely, if $\hat{\rho} = |\psi\rangle\langle\psi|$ with a state $|\psi\rangle$, then $\mathrm{Tr}[\hat{\rho}^2] = 1$. Thus, this theorem is proved. □

The ensemble of density operators $\{p_i, \hat{\rho}_i\}$ is also a density operator:

Theorem 1.6 (The mixture of density operators) *Suppose that $\{\hat{\rho}_i\}$ is a set of density operators, and $\{p_i\}$ is a probability distribution. Then, $\hat{\rho} := \sum_i p_i \hat{\rho}_i$ is also a density operator.*

Proof. $\hat{\rho}_i$ can be written as $\hat{\rho}_i = \sum_j q_{j|i} |\psi_{j,i}\rangle\langle\psi_{j,i}|$ with probability distribution $\{q_{j|i}\}_j$ and pure states $\{|\psi_{j,i}\rangle\}_j$. Thus, $\hat{\rho}$ can be represented by

$$\hat{\rho} = \sum_i p_i \hat{\rho}_i = \sum_i \sum_j p_i q_{j|i} |\psi_{j,i}\rangle\langle\psi_{j,i}|, \tag{1.36}$$

which is a density operator. □

Suppose that we are given a system in a state $\hat{\rho}_i$ with probability p_i. If we are interested in the probability distribution to be obtained by a measurement on a system in an ensemble $\{p_i, \hat{\rho}_i\}$, this theorem implies that the probability distribution is equivalent to one to be given by the measurement on a system in state $\hat{\rho} = \sum_i p_i \hat{\rho}_i$.

1.5 Schmidt decomposition and purification

In this section, we introduce two powerful tools called *Schmidt decomposition* and *purification*.

Theorem 1.7 (Schmidt decomposition) *Let $|\Psi\rangle_{AB}$ be a pure state of a composite system AB, and define $\hat{\rho}^B := \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|]$. Then, using an eigenbasis $\{|b_i\rangle_B\}$ and the eigenvalues $\{p_i\}$ of $\hat{\rho}^B$, we can write the state $|\Psi\rangle_{AB}$ as*

$$|\Psi\rangle_{AB} = \sum_i \sqrt{p_i}|a_i\rangle_A|b_i\rangle_B, \tag{1.37}$$

where $\{|a_i\rangle_A\}$ is an eigenbasis of $\hat{\rho}^A := \mathrm{Tr}_B[|\Psi\rangle_{ABAB}\langle\Psi|]$. $\{p_i\}$ is called Schmidt co-efficients, and the number of non-zero $\{p_i\}$ is called the Schmidt number.

Proof. From the assumption, the reduced density operator $\hat{\rho}^B$ can be diagonalized as $\hat{\rho}^B = \sum_i p_i|b_i\rangle_{BB}\langle b_i|$ with an orthonormal basis $\{|b_i\rangle_B\}$. Then, we have

$$\begin{aligned}
{}_{AB}\langle\Psi||b_j\rangle_{BB}\langle b_i||\Psi\rangle_{AB} =& \sum_k {}_{AB}\langle\Psi||a_k\rangle_A|b_j\rangle_{BA}\langle a_k|_B\langle b_i||\Psi\rangle_{AB} \\
=& \sum_k \langle a_k|_B\langle b_i||\Psi\rangle_{ABAB}\langle\Psi||a_k\rangle_A|b_j\rangle_B \\
=& {}_B\langle b_i|\hat{\rho}^B|b_j\rangle_B \\
=& p_i\delta_{ij},
\end{aligned}$$

which indicates that $|a_i\rangle_A := {}_B\langle b_i||\Psi\rangle_{AB}/\sqrt{p_i}$ composes an orthonormal basis $\{|a_i\rangle_A\}$. For the bases $\{|a_i\rangle_A\}$ and $\{|b_i\rangle_B\}$, $|\Psi\rangle_{AB}$ is expressed in the form of Eq. (1.37). □

This theorem enables us to reduce a general description of a bipartite state,

$$|\Psi\rangle_{AB} = \sum_{i,j} c_{ij}|a_i\rangle_A|b_j\rangle_B \tag{1.38}$$

with co-efficients $\{c_{ij}\}$ of the complex numbers, into a simple form of Eq. (1.37). The simple form for any bipartite state $|\Psi\rangle_{AB}$ is useful for proving many results.

We proceed to the relation between bipartite pure states $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ with the same Schmidt co-efficients.

Theorem 1.8 *$|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ have the identical Schmidt co-efficients if and only if there are unitary operators $\hat{U}^A$ and $\hat{V}^B$ such that*

$$|\Phi\rangle_{AB} = (\hat{U}^A \otimes \hat{V}^B)|\Psi\rangle_{AB}. \tag{1.39}$$

Proof. Suppose that the dimension of system A is d_A, and that of system B is d_B. From the assumption, $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ are written as

$$|\Psi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{p_i}|a_i\rangle_A|b_i\rangle_B, \tag{1.40}$$

$$|\Phi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{p_i}|a'_i\rangle_A|b'_i\rangle_B, \tag{1.41}$$

where $\{p_i\}_{i=1,\ldots,d}$ are Schmidt co-efficients with $p_i \neq 0$, and $\{|a_i\rangle_A\}$, $\{|a'_i\rangle_A\}$, $\{|b_i\rangle_B\}$, and $\{|b'_i\rangle_B\}$ are orthogonal states. Let us define $\hat{U}^A$ and $\hat{V}^B$ as

$$\hat{U}^A = \sum_{i=1}^{d_A} |a'_i\rangle_{AA}\langle a_i|, \tag{1.42}$$

$$\hat{V}^B = \sum_{i=1}^{d_B} |b'_i\rangle_{BB}\langle b_i|, \tag{1.43}$$

by adding extra bases $\{|a_i\rangle_A\}_{d+1,\ldots,d_A}$, $\{|a'_i\rangle_A\}_{d+1,\ldots,d_A}$, $\{|b_i\rangle_B\}_{d+1,\ldots,d_B}$, and $\{|b'_i\rangle_B\}_{d+1,\ldots,d_B}$ if they are necessary. These $\hat{U}^A$ and $\hat{V}^B$ are unitary operations satisfying Eq. (1.39), and hence the direct part is proved.

The converse part is trivial, because local unitary operations preserve the eigenvalues of $\hat{\rho}^A = \mathrm{Tr}_B[|\Psi\rangle_{ABAB}\langle\Psi|]$ (and $\hat{\rho}^B = \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|]$). □

This theorem suggests a nontrivial fact as follows. Let a composite system AB be in state $|\Psi\rangle_{AB}$. Suppose that Alice and Bob, who are separated parties, hold system A and system B, respectively. According to the theorem, by their local unitary operation $\hat{U}^A \otimes \hat{V}^B$, Alice and Bob can freely transform the state $|\Psi\rangle_{AB}$ into a state $|\Phi\rangle_{AB}$ with the same Schmidt coefficients as those of $|\Psi\rangle_{AB}$. Thus, $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ should be regarded as equivalent states under situations where Alice and Bob can freely use local unitary operations.

Let us proceed to another useful technique called purification, which relates a density operator $\hat{\rho}^B$ of a system B with a pure state $|\Psi\rangle_{AB}$ of a composite system AB by introducing a fictitious system A. The fictitious system A is called a *reference system*.

Theorem 1.9 (Purification) *Let $\hat{\rho}^B$ be a density operator of a system B. Then, there exists a pure state $|\Psi\rangle_{AB}$ of a composite system AB with a reference system A such that $\hat{\rho}^B = \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|]$. The pure state $|\Psi\rangle_{AB}$ is called a purification of $\hat{\rho}^B$.*

Proof. We write $\hat{\rho}^B$ as $\hat{\rho}^B := \sum_i p_i |b_i\rangle_{BB}\langle b_i|$ with an orthonormal basis $\{|b_i\rangle_B\}$. Suppose that $\{|a_i\rangle_A\}$ is an orthonormal basis of system A. Then, we define $|\Psi\rangle_{AB}$ as

$$|\Psi\rangle_{AB} := \sum_i \sqrt{p_i}|a_i\rangle_A|b_i\rangle_B, \tag{1.44}$$

which satisfies $\hat{\rho}^B = \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|]$. Thus, the theorem is proved. □

Note that the purification of a density operator is not unique as follows.

Theorem 1.10 (Freedom in purifications) *Let $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ be arbitrary purifications of a density operator $\hat{\rho}^B$. Then, there is a unitary operation $\hat{U}^A$ such that*

$$|\Phi\rangle_{AB} = (\hat{U}^A \otimes \hat{I}^B)|\Psi\rangle_{AB}. \tag{1.45}$$

Proof. From the assumption, we have

$$\hat{\rho}^B = \mathrm{Tr}_A[|\Psi\rangle_{ABAB}\langle\Psi|] = \mathrm{Tr}_A[|\Phi\rangle_{ABAB}\langle\Phi|]. \tag{1.46}$$

Then, from Theorem 1.7, by using an eigenbasis $\{|b_i\rangle_B\}_{i=1,\dots,d}$ and the eigenvalues $\{p_i\}_{i=1,\dots,d}$ of the reduced density operator $\hat{\rho}^B$, we can represent the states $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ as

$$|\Psi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{p_i}|a_i\rangle_A|b_i\rangle_B, \tag{1.47}$$

$$|\Phi\rangle_{AB} = \sum_{i=1}^{d} \sqrt{p_i}|a'_i\rangle_A|b_i\rangle_B \tag{1.48}$$

with orthonormal bases $\{|a_i\rangle_A\}_{i=1,\dots,d}$ and $\{|a'_i\rangle_A\}_{i=1,\dots,d}$. Therefore, by defining

$$\hat{U}^A := \sum_{i=1}^{\dim\mathcal{H}_A} |a'_i\rangle\langle a_i|_A \tag{1.49}$$

through adding extra bases $\{|a_i\rangle_A\}_{i=d+1,\dots,\dim\mathcal{H}_A}$ and $\{|a'_i\rangle_A\}_{i=d+1,\dots,\dim\mathcal{H}_A}$ if they are necessary, we have Eq. (1.45). □

This theorem indicates the following important fact. Suppose that a composite system AB is in a purification $|\Psi\rangle_{AB}$ of a density operator $\hat{\rho}^B$, and the systems A and B are held by Alice and Bob, respectively. The theorem indicates that Alice can freely convert the state $|\Psi\rangle_{AB}$ into another purification $|\Phi\rangle_{AB}$ of the density operator $\hat{\rho}^B$ by her local unitary operation $\hat{U}^A$. This conversion is achievable by Alice alone, independently of the distance between Alice and Bob. Here Bob must not have the ability to discriminate whether the conversion is executed by Alice, without communicating with her, because, if it were possible, she could send him a signal faster than light. Actually, signaling faster than light is prohibited even in quantum mechanics, as represented by the fact that both of the reduced density operators of $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ on system B are the same. Thus, the theorem suggests not only that quantum mechanics satisfies *no-signaling* , but also that we should describe the subsystem of quantum systems as a density operator.

Let us imagine that two ensembles give the same density operator. Then, can we discriminate the ensembles? The answer is given in the proof of the following theorem.

Theorem 1.11 (Freedom in ensembles for a density operator) *Both* $\{p_i, |\psi_i\rangle\}$ *and* $\{q_i, |\phi_i\rangle\}$ *give an identical density operator* $\hat{\rho}$*, namely* $\{p_i, |\psi_i\rangle\}$ *and* $\{q_i, |\phi_i\rangle\}$ *satisfy*

$$\hat{\rho} = \sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_i q_i|\phi_i\rangle\langle\phi_i|, \tag{1.50}$$

if and only if

$$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\phi_j\rangle \tag{1.51}$$

holds for a unitary matrix u_{ij}*.*

Proof. Suppose that $\{p_i, |\psi_i\rangle\}$ and $\{q_i, |\phi_i\rangle\}$ satisfy Eq. (1.50). Let us define pure states $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ as follows:

$$|\Psi\rangle_{AB} := \sum_i \sqrt{p_i}|a_i\rangle_A|\psi_i\rangle_B, \tag{1.52}$$

$$|\Phi\rangle_{AB} := \sum_i \sqrt{q_i}|a_i\rangle_A|\phi_i\rangle_B, \tag{1.53}$$

where $\{|a_i\rangle_A\}$ is an orthonormal basis of a reference system A. Note that the states $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ are purifications of the density operators $\hat{\rho}^B$ of Eq. (1.50). Then, from Theorem 1.10, there is a unitary operation $\hat{U}^A$ such that

$$\sum_i \sqrt{p_i}|a_i\rangle_A|\psi_i\rangle_B = \sum_i \sqrt{q_i}(\hat{U}^A|a_i\rangle_A)|\phi_i\rangle_B. \tag{1.54}$$

Applying ${}_A\langle a_i|$ to this equation, we have

$$\sqrt{p_i}|\psi_i\rangle_B = \sum_j u_{ij}\sqrt{q_j}|\phi_j\rangle_B, \tag{1.55}$$

where $u_{ij} := {}_A\langle a_i|\hat{U}^A|a_j\rangle_A$ is a unitary matrix. This equation is equivalent to Eq. (1.51).

Conversely, suppose that Eq. (1.51) holds. Then, we have

$$\begin{aligned}\sum_i p_i|\psi_i\rangle\langle\psi_i| &= \sum_i \sum_{j,j'} u_{ij}u^*_{ij'}\sqrt{q_j q_{j'}}|\phi_j\rangle\langle\phi_{j'}| \\ &= \sum_{j,j'}\left(\sum_i (u^\dagger)_{j'i}u_{ij}\right)\sqrt{q_j q_{j'}}|\phi_j\rangle\langle\phi_{j'}| \\ &= \sum_i q_i|\phi_i\rangle\langle\phi_i|,\end{aligned} \tag{1.56}$$

which means that both $\{p_i, |\psi_i\rangle\}$ and $\{q_i, |\phi_i\rangle\}$ give an identical density operator. Thus, the theorem is proved. □

This proof implies that we cannot discriminate between two ensembles $\{p_i, |\psi_i\rangle_B\}$ and $\{q_i, |\phi_i\rangle_B\}$ giving the same density operator. Suppose that systems A and B in state $|\Psi\rangle_{AB}$ of Eq. (1.52) are held by Alice and Bob, respectively. Then, Eq. (1.54) implies that Alice can give Bob not only ensemble $\{p_i, |\psi_i\rangle_B\}$ by making measurement $\{|a_i\rangle_A\}$, but also ensemble $\{q_i, |\phi_i\rangle_B\}$ by making measurement $\{\hat{U}^\dagger_A|a_i\rangle_A\}$. Here, if Bob could discriminate between the two ensembles, he could learn Alice's choice between the two measurement procedures, which contradicts the no-signaling. Thus, discrimination between the two ensembles should be impossible, and actually, the impossibility is ensured by the fact that ensembles $\{p_i, |\psi_i\rangle_B\}$ and $\{q_i, |\phi_i\rangle_B\}$ give the same density operator.

1.6 The postulates of quantum mechanics for density operators

As seen above, the density operator is a good description of the state of a physical system. Hence, it is better to rewrite the postulates of quantum mechanics for the density operator. In terms of the density operators, the postulates of the quantum mechanics are rephrased as follows:

Postulate 1: A physical system corresponds to a Hilbert space $\mathcal{H}$. The state is described by a density operator $\hat{\rho}$ on the Hilbert space $\mathcal{H}$.

Postulate 2: The time evolution of a closed system is represented by a unitary operator $\hat{U}$. Let $\hat{\rho}$ and $\hat{\rho}'$ be an initial state and the final state of the system, respectively. Then, the relation between the states is described by

$$\hat{\rho}' = \hat{U}\hat{\rho}\hat{U}^{\dagger}. \tag{1.57}$$

Postulate 3: Suppose that $\hat{A}$ is an observable described by $\hat{A} = \sum_i a_i |a_i\rangle\langle a_i|$. By the measurement of $\hat{A}$ on an initial state $\hat{\rho}$, the state $\hat{\rho}$ is found in state $|a_i\rangle$ with probability

$$p(a_i) = \langle a_i|\hat{\rho}|a_i\rangle. \tag{1.58}$$

From Eq. (1.58), the expectation value $\langle\hat{A}\rangle$ of $\hat{A}$ is given by

$$\langle\hat{A}\rangle = \sum_i a_i p(a_i) = \sum_i a_i \langle a_i|\hat{\rho}|a_i\rangle = \mathrm{Tr}[\hat{A}\hat{\rho}]. \tag{1.59}$$

Postulate 4: Suppose that $\mathcal{H}_A$ and $\mathcal{H}_B$ correspond to physical systems A and B, respectively. Then, the composite system AB corresponds to $\mathcal{H}_A \otimes \mathcal{H}_B$. Moreover, if the systems A and B are prepared in state $\hat{\rho}^A$ and $\hat{\sigma}^B$ respectively, the state of $\mathcal{H}_A \otimes \mathcal{H}_B$ corresponds to $\hat{\rho}^A \otimes \hat{\sigma}^B$.

Similarly, Theorem 1.2 and Theorem 1.3 can be rewritten as follows.

Theorem 1.12 (Projective measurement on a subsystem) *Suppose that a party has system AB in state $\hat{\rho}^{AB}$, and makes measurement represented by a complete orthonormal basis $\{|a_i\rangle_A\}$. If the measurement indicates that the subsystem A is in state $|a_i\rangle_A$, the state of subsystem B is described by*

$$\hat{\rho}_i^B = \frac{{}_A\langle a_i|\hat{\rho}^{AB}|a_i\rangle_A}{p(a_i)}, \tag{1.60}$$

where $p(a_i)$ is the probability with which such an event occurs and it is given by

$$p(a_i) = \mathrm{Tr}[{}_A\langle a_i|\hat{\rho}^{AB}|a_i\rangle_A]. \tag{1.61}$$

Theorem 1.13 (The description of a subsystem) *Suppose that a composite system AB is in state $\hat{\rho}^{AB}$. If a party holding subsystem B does not know how system A is manipulated, the state of subsystem B is described by*

$$\hat{\rho}^B = \mathrm{Tr}_A[\hat{\rho}^{AB}]. \tag{1.62}$$

1.7 Generalized measurement

The most important process in physics is the measurement. In this section, we consider the description of generalized measurement in quantum mechanics.

Without loss of generality, measurement on a physical system A can be regarded as the following process (Fig. 1.2):

(i) We first prepare physical system E in a standard state $|\Sigma\rangle_E$, which is called an *ancilla* or an *auxiliary system*;

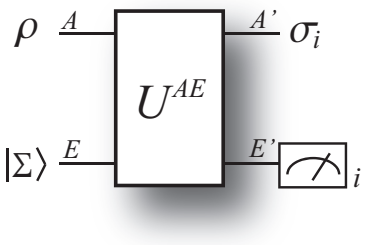

Fig. 1.2. A schematic picture of generalized measurement.

(ii) In order to extract information of system A, we make the physical system A interact with ancilla E according to a unitary operation $\hat{U}^{AE}$ on systems AE;

(iii) We make projective measurement represented by a complete orthonormal basis $\{|i\rangle_{E'}\}$ on ancilla E' such that $\mathcal{H}_A \otimes \mathcal{H}_E = \mathcal{H}_{A'} \otimes \mathcal{H}_{E'}$, and we find that ancilla E' is in state $|i\rangle_{E'}$.

Suppose that system A is initially in a state $\hat{\rho}^A$. Then, the state $\hat{\sigma}^{A'E'}$ after the interaction $\hat{U}^{AE}$ is described by

$$\hat{\sigma}^{A'E'} = \hat{U}^{AE}(\hat{\rho}^A \otimes |\Sigma\rangle_{EE}\langle\Sigma|)\hat{U}^{AE\dagger}. \tag{1.63}$$

Making measurement $\{|i\rangle_{E'}\}$ on system E', we find system E' in state $|i\rangle_{E'}$ with probability

$$p_i = \mathrm{Tr}[{}_{E'}\langle i|\hat{\sigma}^{A'E'}|i\rangle_{E'}], \tag{1.64}$$

where we have used Theorem 1.12. From Theorem 1.12, we also conclude that the state of system A is in state

$$\hat{\sigma}_i^{A'} = \frac{{}_{E'}\langle i|\hat{\sigma}^{A'E'}|i\rangle_{E'}}{p_i}. \tag{1.65}$$

By introducing a set of operators

$$\hat{M}_i := {}_{E'}\langle i|\hat{U}^{AE}|\Sigma\rangle_E, \tag{1.66}$$

p_i and $\hat{\sigma}_i^{A'}$ are simply rewritten as follows:

$$p_i = \mathrm{Tr}[\hat{M}_i^\dagger \hat{M}_i \hat{\rho}^A], \tag{1.67}$$

$$\hat{\sigma}_i^{A'} = \frac{\hat{M}_i \hat{\rho}^A \hat{M}_i^\dagger}{p_i}. \tag{1.68}$$

Note that

$$\sum_i \hat{M}_i^\dagger \hat{M}_i = \hat{I}^A. \tag{1.69}$$

The operators $\{\hat{M}_i\}$ satisfying Eq. (1.69) are called *Kraus operators*. Therefore, any measurement process can be represented by Kraus operators $\{\hat{M}_i\}$.

Conversely, the measurement corresponding to Kraus operators $\{\hat{M}_i\}$ always exists. From

Eq. (1.69), we have

$$\left(\sum_i \hat{M}_i|\phi\rangle_A|i\rangle_{E'}\right)^\dagger \left(\sum_i \hat{M}_i|\psi\rangle_A|i\rangle_{E'}\right) = (|\phi\rangle_A|\Sigma\rangle_E)^\dagger(|\psi\rangle_A|\Sigma\rangle_E) \tag{1.70}$$

for arbitrary states $|\psi\rangle_A$ and $|\phi\rangle$, a standard state $|\Sigma\rangle_E$, and an orthonormal basis $\{|i\rangle_{E'}\}$ of a system E'. This fact suggests that $\{\sum_i \hat{M}_i|k\rangle_A|i\rangle_{E'}\}_{k=1,\ldots,\dim\mathcal{H}_A}$ with a complete orthonormal basis $\{|k\rangle_A\}_{k=1,\ldots,\dim\mathcal{H}_A}$ is an orthogonal basis of system $\mathcal{H}_{A'} \otimes \mathcal{H}_{E'}$. Thus,

$$\hat{U} := \sum_{k=1}^{\dim\mathcal{H}_A} \left(\sum_i \hat{M}_i|k\rangle_A|i\rangle_{E'}\right) {}_A\langle k|_E\langle\Sigma| \tag{1.71}$$

is shown to be an *isometry*† from $\mathcal{H}_A \otimes |\Sigma\rangle_E$ to $\mathcal{H}_{A'} \otimes \mathcal{H}_{E'}$, and it satisfies

$$\hat{U}|\psi\rangle_A|\Sigma\rangle_E = \sum_i \hat{M}_i|\psi\rangle_A|i\rangle_{E'}. \tag{1.72}$$

Since we can make a unitary operator $\hat{U}^{AE}$ as an extension of the isometry $\hat{U}$, we can achieve the measurement corresponding to given Kraus operators $\{\hat{M}_i\}$ by applying the unitary operation $\hat{U}^{AE}$ on system A and system E in a standard state $|\Sigma\rangle_E$ and by projective measurement $\{|i\rangle_{E'}\}$ on system E'.

The description of the generalized measurement is summarized as follows.

Theorem 1.14 (Generalized measurement) *Any measurement on system A is described by a set $\{\hat{M}_i\}$ of operators, where $\hat{M}_i$ is an operator mapping system A into system A' and satisfying $\sum_i \hat{M}_i^\dagger \hat{M}_i = \hat{I}^A$. If we make the measurement on system A in state $\hat{\rho}^A$, we receive an outcome indicating that the left quantum system A' is in state*

$$\hat{\sigma}_i^{A'} = \frac{\hat{M}_i \hat{\rho}^A \hat{M}_i^\dagger}{p_i}, \tag{1.73}$$

with probability

$$p_i = \mathrm{Tr}[\hat{M}_i^\dagger \hat{M}_i \hat{\rho}^A]. \tag{1.74}$$

1.7.1 POVM measurement

In practice, there are cases where we are interested in only the probability distribution $\{p_i\}$ obtained by a measurement $\{\hat{M}_i\}$. In such cases, it is better to use a set of operators $\{\hat{E}_i\}$ with $\hat{E}_i := \hat{M}_i^\dagger \hat{M}_i$, because p_i is determined only by operator $\hat{E}_i$ as Eq. (1.74) indicates. The set $\{\hat{E}_i\}$ is called a *POVM* (Positive Operator-Valued Measure). More formally, the POVM elements are defined to be operators satisfying the following two properties: (i) $\hat{E}_i$ is positive; (ii) $\sum_i \hat{E}_i = \hat{I}$. In fact, the operators $\{\hat{E}_i\}$ with these properties are related with Kraus operators as follows. From property (i), we can ensure the existence of operator $\sqrt{\hat{E}_i}$. Combined this with property (ii), $M_i := \sqrt{\hat{E}_i}$ can be regarded as Kraus operators, which ensures the achievability of POVM measurements.

† A linear operator $\hat{A}$ from $\boldsymbol{C}^m$ to $\boldsymbol{C}^n$ is called an isometry if $\langle x|\hat{A}^\dagger\hat{A}|y\rangle = \langle x|y\rangle$ for any $|x\rangle, |y\rangle \in \boldsymbol{C}^m$.

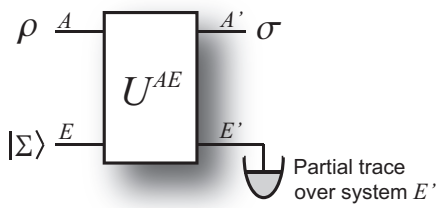

Fig. 1.3. Completely-positive trace-preserving (CPTP) map.

1.7.2 CPTP map and CP map

As represented by Theorem 1.14, generalized measurement returns an outcome i and a quantum system in the corresponding state $\hat{\sigma}_i^{A'}$, with probability p_i. Here, if we cannot get the measurement outcome i or we forget the outcome i, we should consider that the measurement returns only an ensemble $\{p_i, \hat{\sigma}_i^{A'}\}$. In this case, we should consider the left quantum system to be in state

$$\hat{\sigma}^{A'} = \sum_i p_i \hat{\sigma}_i^{A'} = \sum_i \hat{M}_i \hat{\rho}^A \hat{M}_i^\dagger, \tag{1.75}$$

where we used Eq. (1.73). The right-hand side of this equation can be considered to be a quantum operation mapping system A to system A'. This operation is called a *deterministic operation* or a *completely-positive trace-preserving (CPTP) map*. Using the fact that $\{\hat{M}_i\}$ is executed through a unitary operator $\hat{U}^{AE}$ satisfying Eq. (1.72) [or Eq.(1.66)], we obtain

$$\hat{\sigma}^{A'} = \sum_i {}_{E'}\langle i|\hat{U}^{AE}(\hat{\rho}^A \otimes |\Sigma\rangle_{EE}\langle\Sigma|)\hat{U}^{AE\dagger}|i\rangle_{E'} = \mathrm{Tr}_{E'}[\hat{U}^{AE}(\hat{\rho}^A \otimes |\Sigma\rangle_{EE}\langle\Sigma|)\hat{U}^{AE\dagger}]. \tag{1.76}$$

This equation implies that the CPTP map is implementable by unitary operation $\hat{U}^{AE}$ on system A and ancilla E followed by the partial trace over system E' (see Fig.1.3).

More generally, by the generalized measurement $\{M_i\}_{i\in\mathcal{S}}$, we may receive an outcome μ only ensuring that the outcome is included in a subset $\mathcal{S}' \subset \mathcal{S}$. In this case, we should consider that the measurement returns ensemble $\{p_i/(\sum_{j\in\mathcal{S}'} p_j), \hat{\sigma}_i^{A'}\}_{i\in\mathcal{S}'}$. Thus, the left state can be described by

$$\hat{\sigma}_\mu^{A'} = \frac{1}{\sum_{j\in\mathcal{S}'} p_j} \sum_{j\in\mathcal{S}'} p_i \hat{\sigma}_i^{A'} = \frac{1}{\sum_{j\in\mathcal{S}'} p_j} \sum_{j\in\mathcal{S}'} \hat{M}_i \hat{\rho}^A \hat{M}_i^\dagger. \tag{1.77}$$

This process is also considered to be a quantum operation mapping system A to system A'. Unless $\sum_{j\in\mathcal{S}'} p_j = 1$, the operation is called a *probabilistic operation* or a *completely-positive (CP) map*.

Here we provide several examples of CPTP maps. An important CPTP map on qubit A is the so-called *bit-flip channel* described by

$$\mathcal{E}_r^A(\hat{\rho}) = \frac{1+r}{2}\hat{\rho} + \frac{1-r}{2}\hat{X}^A\hat{\rho}\hat{X}^A \tag{1.78}$$

with $-1 \le r \le 1$, where the factor $(1-r)/2$ is called *bit error rate*. A similar CPTP map

$$\Lambda_r^A(\hat{\rho}) = \frac{1+r}{2}\hat{\rho} + \frac{1-r}{2}\hat{Z}^A\hat{\rho}\hat{Z}^A \tag{1.79}$$

is called *phase-flip channel*, and the factor $(1-r)/2$ is called *phase error rate*. These CPTP maps are known as the simplest models of noisy channels.

1.8 The description of general processes

Here we consider to describe an arbitrary process $\mathcal{E}$. Suppose that $\mathcal{E}$ is a map transforming density operator $\hat{\rho}$ of system $\mathcal{H}_A$ into density operator $\hat{\rho}'$ of an output system $\mathcal{H}_{A'}$. For the map, we require the following three axioms:

Axiom 1: $0 \leq \mathrm{Tr}[\mathcal{E}(\hat{\rho})] \leq 1$ holds for any input $\hat{\rho}$.
Axiom 2: $\mathcal{E}$ is a linear map for any input.
Axiom 3: $\mathcal{E}$ is a *completely positive map*.

Axiom 1 is required so that $\mathcal{E}(\hat{\rho})$ corresponds to an (unnormalized) density operator. Axiom 2 is a sufficient condition for reconciling with any ensemble interpretation. In fact, Axiom 2 gives

$$\mathcal{E}(p\hat{\rho}_1 + (1-p)\hat{\rho}_2) = p\mathcal{E}(\hat{\rho}_1) + (1-p)\mathcal{E}(\hat{\rho}_2) \tag{1.80}$$

for any $0 \leq p \leq 1$. The completely positive map in Axiom 3 is defined as follows: $\mathcal{E}$ is called a completely positive map, if $(\mathcal{E}\otimes I^E)(\hat{\sigma}^{AE})$ is positive for any positive operator $\hat{\sigma}^{AE}$ of a composite system $\mathcal{H}_A \otimes \mathcal{H}_E$, where I^E is the identity map on system $\mathcal{H}_E$. Axiom 3 should hold, because, even if a system AE in a state $\hat{\sigma}^{AE}$ passes through a physical process $\mathcal{E}$ for system A, the output $(\mathcal{E} \otimes I^E)(\hat{\sigma}^{AE})$ must be in a physically plausible state.

Here we derive the representation of the general process $\mathcal{E}$:

Theorem 1.15 (The description of a general process) *A map $\mathcal{E}$ satisfies the above three axioms if and only if*

$$\mathcal{E}(\hat{\rho}) = \sum_i \hat{M}_i \hat{\rho} \hat{M}_i^\dagger, \tag{1.81}$$

where $\{M_i\}$ is a set of linear operators transforming a state of input system $\mathcal{H}_A$ into a state of output system $\mathcal{H}_{A'}$ and satisfies $\sum_i \hat{M}_i^\dagger \hat{M}_i \leq \hat{I}^A$.

Proof. Suppose that $\mathcal{E}$ satisfies the above three axioms. Let $|\psi\rangle = \sum_\mu c_\mu |\mu\rangle_A$ be a state of $\mathcal{H}_A$, where $\{|\mu\rangle_A\}$ is an orthonormal basis of $\mathcal{H}_A$. Let us introduce a vector $|\Phi\rangle_{AE}$ of a composite system $\mathcal{H}_A \otimes \mathcal{H}_E$ as follows:

$$|\Phi\rangle_{AE} = \sum_\mu |\mu\rangle_A |\mu\rangle_E, \tag{1.82}$$

where $\{|\mu\rangle_E\}$ is an orthonormal basis of $\mathcal{H}_E$. Let $|\psi^*\rangle_E := \sum_\mu c_\mu^* |\mu\rangle_E$. Then, from Axiom 2, we obtain

$${}_E\langle\psi^*| \left(\mathcal{E} \otimes I^E\right) (|\Phi\rangle_{AEAE}\langle\Phi|) |\psi^*\rangle_E = \mathcal{E}(|\psi\rangle_{AA}\langle\psi|). \tag{1.83}$$

On the other hand, since $\left(\mathcal{E} \otimes I^E\right) (|\Phi\rangle_{AEAE}\langle\Phi|)$ is positive from Axiom 3, it can be diagonalized as follows:

$$(\mathcal{E} \otimes I^E)(|\Phi\rangle_{AEAE}\langle\Phi|) = \sum_i |v_i\rangle_{A'EA'E}\langle v_i|. \tag{1.84}$$

Let us define a map $\hat{M}_i(|\psi\rangle_A)$ as $\hat{M}_i(|\psi\rangle_A) := {}_E\langle\psi^*||v_i\rangle_{A'E}$, which is a linear map. Combined with Eqs. (1.84) and (1.83), this shows

$$\sum_i \hat{M}_i|\psi\rangle_{AA}\langle\psi|\hat{M}_i^\dagger = \sum_i {}_E\langle\psi^*||v_i\rangle_{A'EA'E}\langle v_i||\psi^*\rangle_E \tag{1.85}$$

$$= {}_E\langle\psi^*|\left(\mathcal{E}\otimes I^E\right)(|\Phi\rangle_{AEAE}\langle\Phi|)|\psi^*\rangle_E \tag{1.86}$$

$$= \mathcal{E}(|\psi\rangle_{AA}\langle\psi|). \tag{1.87}$$

In addition, from Axiom 2 and the linearity of $\hat{M}_i$, we can show

$$\sum_i \hat{M}_i\hat{\rho}\hat{M}_i^\dagger = \mathcal{E}(\hat{\rho}), \tag{1.88}$$

for any state $\hat{\rho}$ of $\mathcal{H}_A$. We can also show $\sum_i \hat{M}_i^\dagger\hat{M}_i \leq \hat{I}^A$ from Axiom 1. Thus, ~~the~~ the direct part of the theorem is proved.

On the other hand, the converse part is trivial, and hence the theorem is proved. □

This theorem indicates that the general operation $\mathcal{E}$ is equivalent to a CP map or a CPTP map. Therefore, general operations can be always represented by a CP map or a CPTP map. In what follows, we give several basic theorems as examples of the application of this result.

1.8.1 The no-cloning theorem

The description of general processes enables us to clarify many features of the quantum world. One of the most important features is the *no-cloning theorem* [53, 54, 55]. Before getting down to the no-cloning theorem, we give a useful lemma:

Lemma 1.1 (The existence of a unitary operator) *Let $\{|\Phi_i\rangle\}_{i=1,\ldots,n}$ and $\{|\Psi_i\rangle\}_{i=1,\ldots,n}$ be sets of pure states. Then, there is a unitary operator $\hat{U}$ such that $|\Psi_i\rangle = \hat{U}|\Phi_i\rangle$ if and only if $\langle\Phi_i|\Phi_j\rangle = \langle\Psi_i|\Psi_j\rangle$ holds for any i and j.*

Proof. Suppose that $\langle\Phi_i|\Phi_j\rangle = \langle\Psi_i|\Psi_j\rangle$ holds for any i and j. We introduce states

$$|\alpha\rangle_{AB} := \frac{1}{\sqrt{n}}\sum_{i=1}^n |\Phi_i\rangle_A|i\rangle_B,$$

$$|\beta\rangle_{AB} := \frac{1}{\sqrt{n}}\sum_{i=1}^n |\Psi_i\rangle_A|i\rangle_B,$$

where $\{|i\rangle_B\}$ is an orthonormal basis of system B. Then, from the assumption, we have

$$\mathrm{Tr}_A[|\alpha\rangle\langle\alpha|_{AB}] = \mathrm{Tr}_A[|\beta\rangle\langle\beta|_{AB}].$$

Since this equation means that the reduced density operator of $|\alpha\rangle_{AB}$ on system B is the same as that of $|\beta\rangle_{AB}$, from Theorem 1.10, there is a unitary operator $\hat{U}^A$ on $\mathcal{H}_A$ such that

$$|\alpha\rangle_{AB} = (\hat{U}^A\otimes\hat{1}^B)|\beta\rangle_{AB}. \tag{1.89}$$

This indicates the existence of $\hat{U}^A$ such that $|\Psi_i\rangle = \hat{U}^A|\Phi_i\rangle$.

Converse part of the proof is trivial, and the lemma is thus proved. □

This lemma gives the no-cloning theorem:

Theorem 1.16 (No-cloning theorem for a set of quantum states) *Suppose that we are given a state $|\psi_i\rangle$ secretly chosen from a set $\{|\psi_i\rangle\}_{i=1,\ldots,n}$ of states. Then, it is impossible to deterministically make the copies $|\psi_i\rangle|\psi_i\rangle$ from one copy $|\psi_i\rangle$ if and only if the set $\{|\psi_i\rangle\}_{i=1,\ldots,n}$ includes a nonorthogonal (and nonidentical) pair.*

Proof. Recall that any deterministic map (CPTP map) can be expressed by unitary operation $\hat{U}^{AE}$ acting on the combined space $\mathcal{H}_A \otimes \mathcal{H}_E$, where $\mathcal{H}_E$ represents an auxiliary system initially prepared in a standard state $|\Sigma\rangle_E$. Hence, any cloning process is described by

$$\hat{U}^{AE}(|\psi_i\rangle_A|\Sigma\rangle_E) = |\psi_i\rangle_A|\psi_i\rangle_B|\Sigma_i\rangle_{E'} \tag{1.90}$$

for all i, where $\mathcal{H}_A \otimes \mathcal{H}_E = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{E'}$. Thus, we can make the copies $|\psi_i\rangle|\psi_i\rangle$ if and only if there exist a unitary operator $\hat{U}^{AE}$ and states $\{|\Sigma_i\rangle_{E'}\}$ satisfying Eq. (1.90). From Lemma 1.1, such a unitary operation $\hat{U}^{AE}$ exists if and only if

$$\langle\psi_i|\psi_j\rangle = \langle\psi_i|\psi_j\rangle^2\langle\Sigma_i|\Sigma_j\rangle \tag{1.91}$$

holds for any i and j. Eq. (1.91) holds for any i and j if and only if $|\psi_i\rangle$ is orthogonal to $|\psi_j\rangle$ or the same as $|\psi_j\rangle$. Hence, we cannot make the copies $|\psi_i\rangle|\psi_i\rangle$ if and only if the set $\{|\psi_i\rangle\}_{i=1,\ldots,n}$ includes a nonorthogonal (and nonidentical) pair. □

The no-cloning theorem can be considered to be the basis to determine whether a physical state $|\psi_i\rangle$ has classical or quantum information. For clarifying this statement, let us consider a game. Suppose that Alice wants to send a message $i \in \{1, \ldots, n\}$ to Bob. The communication is easily achievable by sending a memorandum in which the message i is written. Moreover, even if Alice encodes the message i into a quantum system in state $|i\rangle$ of orthogonal states $\{|i\rangle\}_{i=1,\ldots,n}$ and sends it to Bob, they can achieve the communication. In fact, Bob can discriminate $|i\rangle$ from the other candidates by making projective measurement $\{|i\rangle\}_{i=1,\ldots,n}$ on the received quantum system. Thus, the state $|i\rangle$ essentially plays the same role as the message i, and hence we should consider that the state $|i\rangle$ includes only *classical information*. In this sense, we call the states *classical states*.

Now, what if Alice encodes the message i into state $|\psi_i\rangle$ of nonorthogonal states $\{|\psi_i\rangle\}_{i=1,\ldots,n}$? In this case, the no-cloning theorem prohibits Bob from cloning the state $|\psi_i\rangle$. The impossibility of the cloning implies that Bob cannot discriminate $|\psi_i\rangle$ from the other states. Hence, Bob cannot receive complete message i from Alice. Therefore, we should consider that the state $|\psi_i\rangle$ includes non-classical information, i.e., *quantum information*. In what follows, a state that cannot be cloned is called *quantum state*.

As is represented by this consideration, the no-cloning theorem shows an essential difference between classical information and quantum information. By giving a well-known form of the no-cloning theorem as a corollary of Theorem 1.16, we close this section:

Corollary 1.1 (No-cloning theorem for a completely unknown quantum state) *Suppose that we receive a quantum state $|\psi\rangle = \sum_i c_i|i\rangle$ with unknown parameters, $c_i \in \mathcal{C}$. We cannot clone the state deterministically.*

1.8.2 Probabilistic cloning and unambiguous state discrimination

The no-cloning theorem states that we cannot generate the copies $|\psi_i\rangle|\psi_i\rangle$ from an unknown quantum state $|\psi_i\rangle$ via *deterministic* ways. Then, one might naturally ask: Can we make

the copies $|\psi_i\rangle^{\otimes k}$ from one copy $|\psi_i\rangle$ even if we permit *probabilistic* failure. Here we consider *probabilistic cloning* [56], which is a probabilistic process to make the copies of an unknown input state. We also consider a process that probabilistically discriminates a given quantum state $|\psi_i\rangle$ from the other candidates, which is called *unambiguous state discrimination* [57, 58, 59, 60].

1.8.2.1 Probabilistic cloning

Here we consider whether we can generate the copies from an unknown quantum state by a probabilistic way. We begin with noting an important fact about positive matrices.

Lemma 1.2 (Positive matrices) *For an $n \times n$ matrix A, there exists a set of unnormalized states $\{|\chi_i\rangle\}_{i=1,\ldots,n}$ satisfying $A = [\langle\chi_i|\chi_j\rangle]$ if and only if A is positive.*

Proof. Suppose that A is positive. Then, since A can be diagonalized, A can be written as

$$\begin{aligned} A_{ij} =& [UDU^\dagger]_{ij} = \sum_\mu U_{i\mu} d_\mu U^*_{j\mu} \\ =& \left(\sum_\mu \sqrt{d_\mu} U_{i\mu} \langle\mu| \right) \left(\sum_\nu \sqrt{d_\nu} U^*_{j\nu} |\nu\rangle \right), \end{aligned}$$

where U is a unitary matrix, D is a diagonal matrix, and $\{|\mu\rangle\}_{\mu=1,\ldots,n}$ is a complete orthonormal basis. Thus, defining $|\chi_i\rangle$ as

$$|\chi_i\rangle := \sum_\nu \sqrt{d_\nu} U^*_{i\nu} |\nu\rangle,$$

we have $A = [\langle\chi_i|\chi_j\rangle]$, which concludes the direct part of the proof.

Conversely, suppose that A can be written as $A = [\langle\chi_i|\chi_j\rangle]$. Then, for any vector $\boldsymbol{x} = (x_1, \ldots, x_n)^T$, we have

$$\boldsymbol{x}^\dagger A \boldsymbol{x} = \sum_{i,j} x_i^* \langle\chi_i|\chi_j\rangle x_j = \left|\left| \sum_i x_i |\chi_i\rangle \right|\right|^2 \geq 0,$$

which concludes that A is positive. Therefore, the lemma is proved. □

Using this lemma, we can easily derive the necessary and sufficient condition for the existence of probabilistic cloning processes [56] as follows.

Theorem 1.17 (Probabilistic cloning) *Suppose that $|\psi_i\rangle$ is a state secretly chosen from a set $\{|\psi_i\rangle\}_{i=1,\ldots,n}$ of quantum states. There exists a process that succeeds in generating $|\psi_i\rangle^{\otimes k}$ from state $|\psi_i\rangle$ with probability γ_i, if and only if there are normalized states $\{|P_i\rangle_{E'}\}_{i=1,\ldots,n}$ such that the matrix $X - \sqrt{\Gamma} Y \sqrt{\Gamma}$ is positive, where*

$$\begin{aligned} X &:= [\langle\psi_i|\psi_j\rangle], \\ Y &:= [\langle\psi_i|\psi_j\rangle^k \langle P_i|P_j\rangle], \\ \Gamma &:= \mathrm{diag}(\gamma_1, \gamma_2, \ldots, \gamma_n) \end{aligned} \tag{1.92}$$

are $n \times n$ matrices.

Proof. Without loss of generality, probabilistic cloning can be regarded as a unitary operation $\hat{U}^{AE}$ on a given system A in state $|\psi_i\rangle_A$ and on an ancilla E in a standard state $|\Sigma\rangle_E$ followed by a projective measurement on system E' to learn an outcome, 'success' or 'failure.' Thus, there

exists a process that succeeds in generating $|\psi_i\rangle^{\otimes k}$ from state $|\psi_i\rangle$ with probability γ_i, if and only if there are a unitary operation $\hat{U}^{AE}$, normalized states $\{|P_i\rangle_{E'}\}_{i=1,\ldots,n}$, and unnormalized states $\{|\Omega_i\rangle_{AE}\}_{i=1,\ldots,n}$ such that

$$\hat{U}^{AE}(|\psi_i\rangle_A|\Sigma\rangle_E) = \sqrt{\gamma_i}|\psi_i\rangle^{\otimes k}|P_i\rangle_{E'} + |\Omega_i\rangle_{A'E'}, \tag{1.93}$$

and

$${}_{E'}\langle P_i||\Omega_j\rangle_{A'E'} = 0 \tag{1.94}$$

for any i and j. From Lemma 1.1 and Eqs. (1.93) and (1.94), there exists the unitary operation $\hat{U}^{AE}$ if and only if

$$X - \sqrt{\Gamma}Y\sqrt{\Gamma} = \Omega \tag{1.95}$$

holds, where $\Omega := [\langle\Omega_i|\Omega_j\rangle]$.

From Lemma 1.2, the right-hand side of Eq. (1.95) is positive, and hence $X - \sqrt{\Gamma}Y\sqrt{\Gamma}$ should be positive. Conversely, if $X - \sqrt{\Gamma}Y\sqrt{\Gamma}$ is positive, from Lemma 1.2, there exist (possibly unnormalized) states $\{|\Omega_i\rangle\}_{i=1,\ldots,n}$ satisfying Eq. (1.95). This ensures the existence of the wished probabilistic cloning. Thus, this theorem is proved. □

It is instructive to derive the optimal success probability for the cloning by using this theorem. Suppose that we want to clone a state $|\psi_i\rangle$ chosen randomly from a set $\{|\psi_i\rangle\}_{i=1,2}$. Then, the matrix $X - \sqrt{\Gamma}Y\sqrt{\Gamma}$ is

$$X - \sqrt{\Gamma}Y\sqrt{\Gamma} = \begin{pmatrix} 1-\gamma_1 & \langle\psi_1|\psi_2\rangle - \sqrt{\gamma_1\gamma_2}\langle\psi_1|\psi_2\rangle^k\langle P_1|P_2\rangle \\ \langle\psi_2|\psi_1\rangle - \sqrt{\gamma_1\gamma_2}\langle\psi_2|\psi_1\rangle^k\langle P_2|P_1\rangle & 1-\gamma_2 \end{pmatrix}. \tag{1.96}$$

For a probabilistic cloning process to exist, $X - \sqrt{\Gamma}Y\sqrt{\Gamma}$ should be positive, which is equivalent to $\gamma_i \leq 1$ and $\det(X - \sqrt{\Gamma}Y\sqrt{\Gamma}) \geq 0$. From $\gamma_i \leq 1$, $\det(X - \sqrt{\Gamma}Y\sqrt{\Gamma}) \geq 0$ is equivalent to

$$0 \leq \sqrt{(1-\gamma_1)(1-\gamma_2)} - |\langle\psi_1|\psi_2\rangle - \sqrt{\gamma_1\gamma_2}\langle\psi_1|\psi_2\rangle^k\langle P_1|P_2\rangle|. \tag{1.97}$$

By noting that

$$|\langle\psi_1|\psi_2\rangle - \sqrt{\gamma_1\gamma_2}\langle\psi_1|\psi_2\rangle^k\langle P_1|P_2\rangle| \geq |\langle\psi_1|\psi_2\rangle| - \frac{\gamma_1+\gamma_2}{2}|\langle\psi_1|\psi_2\rangle|^k \tag{1.98}$$

$$\sqrt{(1-\gamma_1)(1-\gamma_2)} \leq 1 - \frac{\gamma_1+\gamma_2}{2}, \tag{1.99}$$

Eq. (1.97) is reduced to

$$\frac{\gamma_1+\gamma_2}{2} \leq \frac{1-|\langle\psi_1|\psi_2\rangle|}{1-|\langle\psi_1|\psi_2\rangle|^k}, \tag{1.100}$$

where the equality holds when $\langle P_1|P_2\rangle\langle\psi_1|\psi_2\rangle = |\langle\psi_1|\psi_2\rangle|$ and $\gamma_1 = \gamma_2$. Since the left-hand side of this equation indicates the success probability of the probabilistic cloning, the right-hand side of this equation gives an upper bound on the success probability. Noting that we can set parameters $\{|P_i\rangle\}_{i=1,2}$ and $\{\gamma_i\}_{i=1,2}$ so that $\langle P_1|P_2\rangle\langle\psi_1|\psi_2\rangle = |\langle\psi_1|\psi_2\rangle|$ and $\gamma_1 = \gamma_2$, we conclude that the optimal success probability $p^{\rm opt}$ is

$$p^{\rm opt} = \frac{1-|\langle\psi_1|\psi_2\rangle|}{1-|\langle\psi_1|\psi_2\rangle|^k}. \tag{1.101}$$

The optimal success probability $p^{\rm opt}$ monotonically decreases with $|\langle\psi_1|\psi_2\rangle|$ and k. This implies reasonable conclusions: (i) $|\langle\psi_1|\psi_2\rangle|$ represents the difficulty of cloning; (ii) the increase of the number k of copies incurs the decrease of the efficiency of the cloning.

As can be seen here, the evaluation of success probabilities of quantum cloning can be expected to lead to quantitative understanding of quantum information the state has. However, actually, such an evaluation seems to be difficult if the number of possible states $\{|\psi_i\rangle\}$ is three or more.

1.8.2.2 Unambiguous state discrimination

There is a fundamental process that has been considered [57, 58, 59, 60] before the probabilistic cloning. The process is called unambiguous state discrimination, where one tries to probabilistically identify a state $|\psi_i\rangle$ secretly chosen from states $\{|\psi_i\rangle\}$. Actually, this process can be regarded as a kind of probabilistic cloning from the following intuition: if we had infinite copies of a quantum state $|\psi_i\rangle$ secretly chosen from the set $\{|\psi_i\rangle\}$, we could discriminate the state $|\psi_i\rangle$ from the other candidates. In fact, similarly for probabilistic cloning, we can obtain a formula to derive the efficiency of unambiguous state discrimination:

Theorem 1.18 (Unambiguous discrimination) *Suppose that $|\psi_i\rangle$ is secretly chosen from a set $\{|\psi_i\rangle\}_{i=1,\ldots,n}$ of quantum states. There exists a process that succeeds in unambiguously discriminating state $|\psi_i\rangle$ with probability γ_i, if and only if the matrix $X-\Gamma$ is positive, where $X := [\langle\psi_i|\psi_j\rangle]$ and $\Gamma := \mathrm{diag}(\gamma_1, \gamma_2, \ldots, \gamma_n)$ are $n \times n$ matrices.*

Proof. We can unambiguously discriminate $|\psi_i\rangle$ from the other candidates with probability γ_i if and only if there exist a unitary operation $\hat{U}^{AE}$ and unnormalized states $\{|\Omega_i\rangle_{AE}\}$ such that

$$\hat{U}^{AE}(|\psi_i\rangle_A|\Sigma\rangle_E) = \sqrt{\gamma_i}|i\rangle_{AE} + |\Omega_i\rangle_{AE}, \tag{1.102}$$

where $\{|i\rangle_{AE}\}$ is an orthonormal basis. By this fact, the theorem can be proved by a similar manner to the proof of Theorem 1.17. □

This theorem suggests the validity of the above intuition. In fact, if we take the limit of $k \to \infty$ in Theorem 1.17 under the condition $|\langle\psi_i|\psi_j\rangle| < 1$ for any $i \neq j$, the theorem is reduced into Theorem 1.18. Thus, we conclude that, if a set $\{|\psi_i\rangle\}$ is composed of different quantum states, making infinite copies of an input $|\psi_i\rangle$ probabilistically is equivalent to unambiguous state discrimination of the quantum states $\{|\psi_i\rangle\}$.

By using this fact, we can easily derive the optimal success probability of unambiguous discrimination of quantum states $\{|\psi_i\rangle\}_{i=1,2}$. Suppose that $|\psi_i\rangle$ is randomly chosen from states $\{|\psi_i\rangle\}_{i=1,2}$. Then, since the optimal success probability $p^{\rm opt}$ of the unambiguous discrimination is equivalent to the limit $k \to \infty$ of Eq. (1.101), it is concluded to be

$$p^{\rm opt} = 1 - |\langle\psi_1|\psi_2\rangle|. \tag{1.103}$$

1.9 Fidelity

As seen in Sections 1.8.2.1 and 1.8.2.2, the magnitude of the inner product between states is a measure representing the difficulty of distinguishing the states, namely a closeness of the states. As such a measure indicating a 'distance' between the states $\hat{\rho}$ and $\hat{\sigma}$, we use *fidelity* [61]

$$F(\hat{\rho}, \hat{\sigma}) := ||\sqrt{\hat{\rho}}\sqrt{\hat{\sigma}}||^2 \tag{1.104}$$

with $||\hat{X}|| := \mathrm{Tr}\sqrt{\hat{X}^\dagger \hat{X}}$. Note that the fidelity satisfies

$$0 \leq F(\hat{\rho}, \hat{\sigma}) \leq 1, \tag{1.105}$$

and $F(\hat{\rho}, \hat{\sigma}) = 1$ implies $\hat{\rho} = \hat{\sigma}$.

In the case of $\hat{\sigma} = |\psi\rangle\langle\psi|$, the fidelity is reduced to

$$F(\hat{\rho}, |\psi\rangle) = \langle\psi|\hat{\rho}|\psi\rangle, \tag{1.106}$$

which implies $F(|\phi\rangle, |\psi\rangle) = |\langle\phi|\psi\rangle|^2$. Therefore, the fidelity may be regarded as a natural generalization of the magnitude of the inner product between states.

2

Quantum communication

Quantum communication is the basic technique to enable faithful transmission of unknown quantum states, which is shown to enable important applications such as the distribution of unconditionally secure key and the distributed quantum computation. The *ideal quantum channel* is described by a single Kraus operator

$$\hat{1}^{A\to B} = |0\rangle_{BA}\langle 0| + |1\rangle_{BA}\langle 1|. \tag{2.1}$$

In fact, it enables us to transmit an unknown quantum state $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$ of system A to system B according to

$$\hat{1}^{A\to B}|\psi\rangle_A = \alpha|0\rangle_B + \beta|1\rangle_B = |\psi\rangle_B. \tag{2.2}$$

One way to achieve the quantum communication is the direct transmission of quantum systems through a channel. However, this way is not necessarily the best solution, because the practical channel inevitably causes errors on the transmitted state. Instead, here we introduce a scenario to accomplish quantum communication in an indirect manner based on the so-called *quantum teleportation* protocol [30]. The goal of this manner is to share *Bell states* between the sender and the receiver through a practical channel. The Bell states are defined by

$$\begin{aligned}
|\Phi^+\rangle_{AB} &:= |B_{00}\rangle_{AB} := \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}),\\
|\Psi^+\rangle_{AB} &:= |B_{01}\rangle_{AB} := \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}) = \hat{X}^A|\Phi^+\rangle = \hat{X}^B|\Phi^+\rangle,\\
|\Phi^-\rangle_{AB} &:= |B_{10}\rangle_{AB} := \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB}) = \hat{Z}^A|\Phi^+\rangle = \hat{Z}^B|\Phi^+\rangle,\\
|\Psi^-\rangle_{AB} &:= |B_{11}\rangle_{AB} := \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}) = \hat{Z}^A\hat{X}^A|\Phi^+\rangle = \hat{X}^B\hat{Z}^B|\Phi^+\rangle.
\end{aligned} \tag{2.3}$$

In order to see why sharing Bell states is sufficient for achieving quantum communication, we begin with clarifying the role of the quantum teleportation protocol.

2.1 Quantum teleportation and entanglement swapping

Suppose that Alice wants to transmit a quantum state $|\psi\rangle_{A_1} = \alpha|0\rangle_{A_1} + \beta|1\rangle_{A_1}$ with unknown parameters $\alpha, \beta \in \mathcal{C}$. Then, from the no-cloning theorem (Corollary 1.1), Alice cannot clone the state $|\psi\rangle_{A_1}$, let alone knowing parameters α and β. This implies that Alice cannot send Bob the state $|\psi\rangle_{A_1}$ only by classical communication channels between them.

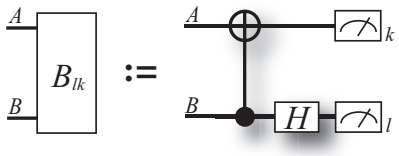

Fig. 2.1. Bell measurement.

Fig. 2.2. Quantum teleportation (QT) protocol. CC (QC) indicates classical channel (quantum channel).

However, the transmission of the quantum state $|\psi\rangle_{A_1}$ is achievable if Alice and Bob share system A_2B in Bell state $|\Phi^+\rangle_{A_2B}$ in advance and they can use classical communication. In fact, Alice and Bob can accomplish the transmission through the following protocol:

(i) Alice first makes the so-called *Bell measurement* $\{\hat{B}_{jk}^{A_1A_2}\}_{j,k=0,1}$ on system A_1A_2;
(ii) Alice sends the outcome jk to Bob by using classical communication;
(iii) On receiving the outcome jk, Bob applies unitary operation $(\hat{Z}^B)^j(\hat{X}^B)^k$.

Here Bell measurement is defined by Kraus operators

$$\begin{aligned}\hat{B}_{00}^{A_1A_2} &:= {}_{A_1A_2}\langle\Phi^+|,\\ \hat{B}_{01}^{A_1A_2} &:= {}_{A_1A_2}\langle\Psi^+|,\\ \hat{B}_{10}^{A_1A_2} &:= {}_{A_1A_2}\langle\Phi^-|,\\ \hat{B}_{11}^{A_1A_2} &:= -{}_{A_1A_2}\langle\Psi^-|,\end{aligned} \tag{2.4}$$

and it is achievable in a manner in Fig. 2.1. This protocol is called quantum teleportation [30]. The protocol indicates that the consumption of a Bell state and two-bit classical communication has the same power as the ideal quantum channel (see Fig. 2.2).

Let us proceed to showing why the quantum teleportation succeeds in the transmission of the unknown quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. By the Bell measurement at step (i), Alice receives outcome jk with probability

$$p_{jk} := {}_{A_1}\langle\psi|_{A_2B}\langle\Phi^+|((\hat{B}_{jk}^{A_1A_2})^\dagger\hat{B}_{jk}^{A_1A_2}\otimes\hat{1}^B)|\psi\rangle_{A_1}|\Phi^+\rangle_{A_2B}, \tag{2.5}$$

and the left state is described by $|\phi_{jk}\rangle_B := (\hat{B}_{jk}^{A_1A_2}|\psi\rangle_{A_1}|\Phi^+\rangle_{A_2B})/\sqrt{p_{jk}}$. Through the communication at step (ii), Bob also knows the outcome jk. Since Bob applies unitary operation $(\hat{Z}^B)^j(\hat{X}^B)^k$ on system B in state $|\phi_{jk}\rangle_B$ as step (iii), the final state $|\phi'_{jk}\rangle_B$ is described by

$$|\phi'_{jk}\rangle_B := \frac{1}{\sqrt{p_{jk}}}(\hat{Z}^B)^j(\hat{X}^B)^k\hat{B}_{jk}^{A_1A_2}|\psi\rangle_{A_1}|\Phi^+\rangle_{A_2B}. \tag{2.6}$$

Thus, for proving $|\phi'_{jk}\rangle_B = |\psi\rangle_B$, it is sufficient to show

$$\frac{1}{\sqrt{p_{jk}}}(\hat{Z}^B)^j(\hat{X}^B)^k\hat{B}_{jk}^{A_1A_2}|\Phi^+\rangle_{A_2B} = |0\rangle_{BA_1}\langle 0| + |1\rangle_{BA_1}\langle 1|. \tag{2.7}$$

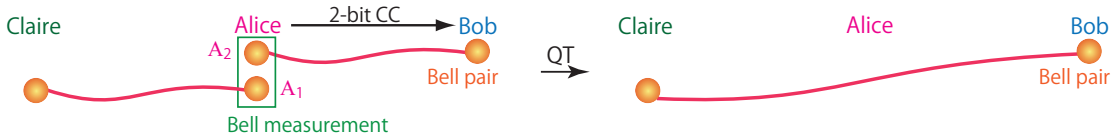

Fig. 2.3. Entanglement swapping.

Note that the right-hand side of this equation is equivalent to the description of the ideal quantum channel $A_1 \to B$.

To show Eq. (2.7), we start with noting

$$\begin{aligned}
|0\rangle_{A_1}|\Phi^+\rangle_{A_2B} =& \frac{1}{\sqrt{2}}(|00\rangle_{A_1A_2}|0\rangle_B + |01\rangle_{A_1A_2}|1\rangle_B) \\
=& \frac{1}{2}[(|\Phi^+\rangle_{A_1A_2} + |\Phi^-\rangle_{A_1A_2})|0\rangle_B + (|\Psi^+\rangle_{A_1A_2} + |\Psi^-\rangle_{A_1A_2})|1\rangle_B], \\
|1\rangle_{A_1}|\Phi^+\rangle_{A_2B} =& \frac{1}{\sqrt{2}}(|10\rangle_{A_1A_2}|0\rangle_B + |11\rangle_{A_1A_2}|1\rangle_B) \\
=& \frac{1}{2}[(|\Psi^+\rangle_{A_1A_2} - |\Psi^-\rangle_{A_1A_2})|0\rangle_B + (|\Phi^+\rangle_{A_1A_2} - |\Phi^-\rangle_{A_1A_2})|1\rangle_B].
\end{aligned}$$

This indicates

$$\begin{aligned}
\hat{B}_{jk}^{A_1A_2}|0\rangle_{A_1}|\Phi^+\rangle_{A_2B} =& \frac{1}{2}(\hat{Z}^B)^j(\hat{X}^B)^k|0\rangle_B, \\
\hat{B}_{jk}^{A_1A_2}|1\rangle_{A_1}|\Phi^+\rangle_{A_2B} =& \frac{1}{2}(\hat{Z}^B)^j(\hat{X}^B)^k|1\rangle_B,
\end{aligned}$$

and thus we have $p_{jk} = 1/4$ and

$$\hat{B}_{jk}^{A_1A_2}|\Phi^+\rangle_{A_2B} = \frac{1}{2}(\hat{Z}^B)^j(\hat{X}^B)^k(|0\rangle_{BA_1}\langle 0| + |1\rangle_{BA_1}\langle 1|).$$

These relations conclude Eq. (2.7).

As an application of the quantum teleportation, we introduce a way to connect two entangled pairs. Suppose that, in addition to the Bell pair $|\Phi^+\rangle_{A_2B}$, Alice shares a Bell pair $|\Phi^+\rangle_{CA_1}$ with another party, Claire (see Fig. 2.3). Here we consider that Alice transmits the state of system A_1 to Bob by using the teleportation. As can be convinced by Eq. (2.7), the teleportation acts as the ideal channel $A_1 \to B$ at the expense of system A_1A_2. Hence, it transforms two Bell pairs $|\Phi^+\rangle_{CA_1}|\Phi^+\rangle_{A_2B}$ to a Bell pair $|\Phi^+\rangle_{BC}$. This teleportation process is particularly called *entanglement swapping* [62]. The entanglement swapping suggests that the Bell pairs connecting Bob with Claire through the intermediary of Alice are sufficient for presenting a Bell pair between Bob and Claire. Thus, the entanglement swapping is regarded as the connection of Bell pairs.

Note that quantum teleportation and entanglement swapping work independently of positions of the users, as long as they share Bell pairs in advance and can use classical communication. Therefore, the working principle of these protocols is independent of the physical distances between the users.

2.2 Entanglement-based quantum key distribution protocol

As seen in the previous section, if Alice and Bob share a Bell pair, they can simulate the ideal quantum channel. Here we show that the Bell pair also provides them an unconditionally secure

bit [10, 11]. The secret bit is in the form of

$$\hat{\rho}_{\rm key}^{ABE} = \frac{1}{2}\sum_{i=0,1} |ii\rangle\langle ii|_{AB} \otimes \hat{\sigma}^E, \tag{2.8}$$

where E is assumed to be held by an eavesdropper, Eve. In fact, from the state $\hat{\rho}_{\rm key}^{ABE}$, Alice and Bob can obtain a complete correlated bit by their local projective measurement $\{|ij\rangle_{AB}\}_{ij}$, whereas the state $\hat{\sigma}^E$ of Eve's system cannot have any correlation with their bit. Thus, state $\hat{\rho}_{\rm key}^{ABE}$ corresponds to a situation where Alice and Bob can share an unconditionally secure bit.

Suppose that Alice and Bob share qubits AB in a Bell pair $|\Phi^+\rangle_{AB}$. Then, from Theorem 1.9 and 1.10, the arbitrary purification of state $|\Phi^+\rangle_{AB}$ is expressed as $|\Phi^+\rangle_{AB}\otimes|\chi\rangle_{E'}$ with a reference E'. Since a part or the entire of reference system E' corresponds to the system E, without loss of generality, the state of Alice, Bob, and Eve is described by $\hat{\rho}_{\rm mes}^{ABE} := |\Phi^+\rangle\langle\Phi^+|_{AB} \otimes \hat{\sigma}^E$ with state $\hat{\sigma}^E := {\rm Tr}_{\bar{E}}[|\chi\rangle\langle\chi|_{E'}]$, where $\mathcal{H}_{E'} = \mathcal{H}_E \otimes \mathcal{H}_{\bar{E}}$. Thus, by applying CPTP map $\mathcal{P}^A(\hat{\rho}) = |0\rangle_{AA}\langle 0|({}_A\langle 0|\hat{\rho}|0\rangle_A) + |1\rangle_{AA}\langle 1|({}_A\langle 1|\hat{\rho}|1\rangle_A)$ on Alice's system, Alice and Bob obtain state

$$\mathcal{P}^A(\hat{\rho}_{\rm mes}^{ABE}) = \hat{\rho}_{\rm key}^{ABE}, \tag{2.9}$$

which is the secret bit. Hence, Alice and Bob can generate an unconditionally secure bit from a Bell pair.

In practice, Alice and Bob should check whether the state $\hat{\rho}^{AB}$ of their shared qubits is the Bell state $|\Phi^+\rangle_{AB}$ or not. This is achievable if they share additional check qubits that can be considered to be in the same state $\hat{\rho}^{AB}$. Suppose that Alice and Bob make local measurements $\{|ij\rangle_{AB}\}_{i,j=0,1}$ and $\{|k_x l_x\rangle_{AB}\}_{k,l=0,1}$ on the check qubits†. Noting

$$\begin{aligned} |00\rangle_{AB} =& \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{AB} + |\Phi^-\rangle_{AB}), \quad |01\rangle_{AB} = \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{AB} + |\Psi^-\rangle_{AB}), \\ |10\rangle_{AB} =& \frac{1}{\sqrt{2}}(|\Psi^+\rangle_{AB} - |\Psi^-\rangle_{AB}), \quad |11\rangle_{AB} = \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{AB} - |\Phi^-\rangle_{AB}), \end{aligned} \tag{2.10}$$

and Eq. (A2.1)‡, if the measurements $\{|ij\rangle_{AB}\}_{i,j=0,1}$ and $\{|k_x l_x\rangle_{AB}\}_{k,l=0,1}$ always return outcomes (i,j,k,l) satisfying $i\oplus j = 0$ and $k\oplus l = 0$, then the state $\hat{\rho}^{AB}$ must be $|\Phi^+\rangle_{AB}$. Therefore, Alice and Bob can check whether their shared pair is in the Bell state or not.

2.3 Quantum entanglement

As represented by the quantum teleportation protocol, Bell states are the resource of quantum communication. Then, naturally arising question is what kind of the property of the Bell state enables quantum communication? The property is considered to be *quantum entanglement*, which is a correlation that is essentially different from classical one.

For grasping the nature of quantum entanglement, it is better to consider what we can do under the situations where we can freely use classical correlation. Such a situation can be obtained in a paradigm called *local operations and classical communication (LOCC)*. Suppose that separated parties, Alice and Bob, share a state $\hat{\rho}_{AB}$. In the class of LOCC, Alice and Bob are allowed to use local operations (LO) and classical communication (CC) between them. In particular, under LOCC, Alice and Bob can take the following tactics: (i) Alice makes generalized measurement

† Note that the check qubits are used only for the identification of the state $\hat{\rho}^{AB}$, and it will be discarded after the measurement.

‡ Eq. (A$*$) means equation ($*$) in Appendix.

on her system, and sends the output i_1 to Bob by CC; (ii) Depending on the data i_1, Bob selects quantum operations to be applied to his system, executes them, and sends the output j_1 to Alice; (iii) Depending on the previous data (i_1, j_1), Alice selects $\cdots$, and vice versa. Thus, the net LOCC is the map from a density operator $\hat{\rho}_{AB}$ into an unnormalized state

$$(\mathcal{A}_{i_{n+1}}^{(i_1,j_1,\ldots,i_n,j_n)} \otimes \mathcal{B}_{j_{n+1}}^{(i_1,j_1,\ldots,i_n,j_n,i_{n+1})}) \cdots (\mathcal{A}_{i_2}^{(i_1,j_1)} \otimes \mathcal{B}_{j_2}^{(i_1,j_1,i_2)})(\mathcal{A}_{i_1} \otimes \mathcal{B}_{j_1}^{(i_1)})(\hat{\rho}_{AB}), \tag{2.11}$$

where $\{\mathcal{A}_y^{(x)}\}_y$ ($\{\mathcal{B}_y^{(x)}\}_y$) is the set of quantum operations that might depends on the previous outcomes x, and $\mathcal{A}_y^{(x)}$ ($\mathcal{B}_y^{(x)}$) is the operation corresponding to outcome y. Thus, LOCC can be described by a stochastic map composed of separable operators.

Similarly, we can define LOCC between multi-party. However, for simplicity, here we focus on LOCC between two parties, Alice and Bob.

Through LOCC, we define entanglement as follows:

Definition 2.1 (Entanglement) *Quantum entanglement or entanglement is a class of correlations that cannot be freely strengthened by LOCC.*

From this definition, states in the form of

$$\hat{\rho}_{\text{sep}}^{AB} = \sum_i p_i \hat{\rho}_i^A \otimes \hat{\sigma}_i^B \tag{2.12}$$

are not entangled states, because this state can be always generated by LOCC. These states are particularly called *separable states*. In contrast, it seems that Bell states cannot be freely generated by LOCC. Is it true? To answer this question, we proceed to finding monotonicity of LOCC.

2.3.1 Entanglement monotones

Here we clarify monotonicity of LOCC. More precisely, we show the existence of quantities that do not increase on average under LOCC. Such quantities are called *entanglement monotones*. The formal definition of the entanglement monotones is the following [63]:

Definition 2.2 (Entanglement monotones) *Suppose that $\mu(\hat{\rho}^{AB})$ is a function on bipartite density operators $\hat{\rho}^{AB}$. If magnitude $\mu(\hat{\rho}^{AB})$ does not, on average, increase under LOCC between Alice and Bob, we call it entanglement monotone.*

In other words, entanglement monotones $\mu(\hat{\rho}^{AB})$ are quantities satisfying the following two conditions:

Condition 1: For any local quantum operation $\mathcal{E}_k^X$ on a subsystem $X = A, B$ in a state $\hat{\rho}^{AB}$, $\mu(\hat{\rho}^{AB})$ satisfies

$$\mu(\hat{\rho}^{AB}) \geq \sum_k p_k \mu(\hat{\rho}_k^{AB}), \tag{2.13}$$

where $p_k := \text{Tr}[\mathcal{E}_k^X(\hat{\rho}^{AB})]$ and $\hat{\rho}_k^{AB} := \mathcal{E}_k^X(\hat{\rho}^{AB})/p_k$.

Condition 2: For any ensemble $\{p_k, \hat{\rho}_k^{AB}\}$, $\mu(\hat{\rho}^{AB})$ satisfies

$$\sum_k p_k \mu(\hat{\rho}_k^{AB}) \geq \mu(\hat{\rho}^{AB}), \tag{2.14}$$

where $\hat{\rho}^{AB} := \sum_k p_k \hat{\rho}_k^{AB}$.

Under LOCC, Alice and Bob are allowed to implement generalized measurements locally. Condition 1 indicates that μ does not increase on average under such local operations. In addition, under LOCC, there are cases where Alice and Bob forget outcomes k of the previous measurements and describe their state as $\hat{\rho}^{AB} := \sum_k p_k \hat{\rho}_k^{AB}$. Condition 2 implies that μ does not increase under such discard of the outcomes.

Let us proceed to showing that entanglement monotones exist. Before giving such monotones, we introduce a manner to compose an entanglement monotone.

Theorem 2.1 (Composition of an entanglement monotone) *Let f be an operator function mapping an operator of a Hilbert space $\mathcal{H}$ to a real number. The function is assumed to satisfy the following two properties: (i) function f is invariant under unitary operations, namely satisfies*

$$f(\hat{U}\hat{\rho}\hat{U}^\dagger) = f(\hat{\rho}) \tag{2.15}$$

for any density operator $\hat{\rho}$ of system $\mathcal{H}$ and any unitary operation $\hat{U}$; (ii) function f is concave for any density operator, namely it satisfies

$$f(p\hat{\rho}_1 + (1-p)\hat{\rho}_2) \geq pf(\hat{\rho}_1) + (1-p)f(\hat{\rho}_2) \tag{2.16}$$

for any density operators $\hat{\rho}_1$, $\hat{\rho}_2$ of system $\mathcal{H}$ and any p such that $0 \leq p \leq 1$.

By using function f, we define magnitude $\mu(\rho)$ as the following: for pure states of a system AB, μ is defined by

$$\mu(|\psi\rangle_{AB}) := f(\mathrm{Tr}_B[|\psi\rangle\langle\psi|_{AB}]) \,(= f\left(\mathrm{Tr}_A[|\psi\rangle\langle\psi|_{AB}]\right)); \tag{2.17}$$

for mixed states of the system AB, μ is defined by

$$\mu(\hat{\rho}^{AB}) := \min_{\{p_i,\, |\psi_i\rangle_{AB}\}} \sum_j p_j \mu(|\psi_j\rangle_{AB}), \tag{2.18}$$

where the minimum is taken over all ensembles $\{p_i, |\psi_i\rangle_{AB}\}$ satisfying $\hat{\rho}^{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|_{AB}$. Then, the function μ is an entanglement monotone for the system AB, namely it satisfies Condition 1 and Condition 2.

Proof. First we show the convexity of the function μ, which is equivalent to Condition 2. Let us consider any ensemble $\{p_k, \hat{\rho}_k^{AB}\}$ such that $\sum_k p_k \hat{\rho}_k^{AB} = \hat{\rho}^{AB}$. For each state $\hat{\rho}_k^{AB}$, let us introduce an ensemble $\{q_{l|k}, |\psi_{kl}\rangle_{AB}\}$ satisfying

$$\mu(\hat{\rho}_k^{AB}) = \sum_l q_{l|k} \mu(|\psi_{kl}\rangle_{AB}), \tag{2.19}$$

$$\hat{\rho}_k^{AB} = \sum_l q_{l|k} |\psi_{kl}\rangle\langle\psi_{kl}|_{AB}. \tag{2.20}$$

Combined with Eq. (2.18) and $\hat{\rho}^{AB} = \sum_k p_k \hat{\rho}_k^{AB} = \sum_{k,l} p_k q_{l|k} |\psi_{kl}\rangle\langle\psi_{kl}|_{AB}$, these imply

$$\mu(\hat{\rho}^{AB}) \leq \sum_k p_k \sum_l q_{kl} \mu(|\psi_{kl}\rangle_{AB}) = \sum_k p_k \mu(\hat{\rho}_k^{AB}). \tag{2.21}$$

Hence, the function μ is convex.

Let us show that the function μ satisfies Condition 1. Assume that system A and system B in a state $\hat{\rho}^{AB}$ are held by Alice and Bob, respectively. For density operator $\hat{\rho}^{AB}$, we introduce

an ensemble $\{q_i, |\phi_i\rangle_{AB}\}$ such that

$$\mu(\hat{\rho}^{AB}) = \sum_i q_i \mu(|\phi_i\rangle_{AB}), \tag{2.22}$$

$$\hat{\rho}^{AB} = \sum_i q_i |\phi_i\rangle\langle\phi_i|_{AB}. \tag{2.23}$$

By quantum operation $\mathcal{E}_k^X(\cdot)$ $(X = A, B)$, $\hat{\rho}^{AB}$ and $|\phi_i\rangle_{AB}$ are converted to normalized states

$$\hat{\rho}_k^{AB} := \frac{\mathcal{E}_k^X(\hat{\rho}^{AB})}{p_k}, \tag{2.24}$$

$$\hat{\rho}_{ik}^{AB} := \frac{\mathcal{E}_k^X(|\phi_i\rangle\langle\phi_i|_{AB})}{p_{k|i}}. \tag{2.25}$$

From the latter equation and the fact that $\sum_k \mathcal{E}_k^X(\cdot)$ is a CPTP map on system X, we have

$$\sum_k p_{k|i} \mathrm{Tr}_X[\hat{\rho}_{ik}^{AB}] = \mathrm{Tr}_X\left[\sum_k \mathcal{E}_k^X(|\phi_i\rangle\langle\phi_i|_{AB})\right] = \mathrm{Tr}_X(|\phi_i\rangle\langle\phi_i|_{AB}). \tag{2.26}$$

In addition, from the linearity of $\mathcal{E}_k^X$, $\hat{\rho}_{ki}^{AB}$ and $\hat{\rho}_k^{AB}$ have a relation

$$p_k \hat{\rho}_k^{AB} = \sum_i q_i p_{k|i} \hat{\rho}_{ik}^{AB}. \tag{2.27}$$

We further note that, for any density operator $\hat{\sigma}^{AB} = \sum_i r_i |\eta_i\rangle\langle\eta_i|_{AB}$, we have

$$\mu(\hat{\sigma}) \leq \sum_i r_i \mu(|\eta_i\rangle_{AB}) = \sum_i r_i f(\mathrm{Tr}_X[|\eta_i\rangle\langle\eta_i|_{AB}]) \leq f\left(\sum_i r_i \mathrm{Tr}_X[|\eta_i\rangle\langle\eta_i|_{AB}]\right) = f(\mathrm{Tr}_X[\sigma^{AB}]) \tag{2.28}$$

from the concavity of f. Eq. (2.22), Eqs. (2.26)-(2.28), the concavity of f, and the convexity of μ indicate

$$\begin{aligned}
\mu(\hat{\rho}) &= \sum_i q_i \mu(|\phi_i\rangle_{AB}) = \sum_i q_i f(\mathrm{Tr}_X[|\phi_i\rangle\langle\phi_i|_{AB}]) = \sum_i q_i f\left(\sum_k p_{k|i} \mathrm{Tr}_X[\hat{\rho}_{ik}^{AB}]\right) \\
&\geq \sum_{i,k} q_i p_{k|i} f(\mathrm{Tr}_X[\hat{\rho}_{ik}^{AB}]) \geq \sum_{i,k} q_i p_{k|i} \mu(\hat{\rho}_{ik}^{AB}) = \sum_{i,k} p_k \frac{q_i p_{k|i}}{p_k} \mu(\hat{\rho}_{ik}^{AB}) \\
&\geq \sum_k p_k \mu\left(\sum_i \frac{q_i p_{k|i}}{p_k} \hat{\rho}_{ik}^{AB}\right) = \sum_k p_k \mu(\hat{\rho}_k^{AB}),
\end{aligned} \tag{2.29}$$

which means that function μ satisfies Condition 2. Therefore, the theorem is proved. □

This theorem implies that all the functions μ based on the operator functions f are entanglement monotones. Thus, it is expected that many entanglement monotones exist. In the next section, we give an explicit example among such entanglement monotones. The example clarifies that LOCC has a fundamental limit of its performance.

2.3.2 Entanglement formation

Here we present an example of entanglement monotones by using Theorem 2.1. We first give a lemma.

Lemma 2.1 *Let $f(x)$ be a concave function from real numbers to real numbers, and let $\hat{A}$, $\hat{B}$ be Hermitian operators. Then, for any $0 \leq p \leq 1$,*

$$\mathrm{Tr}[f(p\hat{A} + (1-p)\hat{B})] \geq p\mathrm{Tr}[f(\hat{A})] + (1-p)\mathrm{Tr}[f(\hat{B})], \tag{2.30}$$

where $f(\hat{A})$ is the operator function based on $f(x)$. This inequality indicates the concavity of function $\mathrm{Tr}[f(\hat{A})]$.

Proof. For any Hermitian operator $\hat{A}$ to be diagonalized as $\hat{A} = \sum_i a_i |a_i\rangle\langle a_i|$ and any state $|\phi\rangle$, we have

$$f(\langle\phi|\hat{A}|\phi\rangle) = f\left(\sum_i |\langle\phi|a_i\rangle|^2 a_i\right) \geq \sum_i |\langle\phi|a_i\rangle|^2 f(a_i) = \langle\phi|\left(\sum_i f(a_i)|a_i\rangle\langle a_i|\right)|\phi\rangle = \langle\phi|f(\hat{A})|\phi\rangle. \tag{2.31}$$

Let us define Hermitian operator $\hat{C} := p\hat{A} + (1-p)\hat{B}$. We can write the operator $\hat{C}$ as $\hat{C} = \sum_i c_i |i\rangle\langle i|$ with an orthonormal basis $\{|i\rangle\}$. Then, from Eq. (2.31) and the concavity of f, we have

$$\begin{aligned}
\mathrm{Tr}[f(\hat{C})] =& \mathrm{Tr}\left[\sum_i f(c_i)|i\rangle\langle i|\right] = \sum_i f(c_i) = \sum_i f(\langle i|\hat{C}|i\rangle) = \sum_i f(p\langle i|\hat{A}|i\rangle + (1-p)\langle i|\hat{B}|i\rangle) \\
\geq& p\sum_i f(\langle i|\hat{A}|i\rangle) + (1-p)\sum_i f(\langle i|\hat{B}|i\rangle) \geq p\sum_i \langle i|f(\hat{A})|i\rangle + (1-p)\sum_i \langle i|f(\hat{B})|i\rangle \\
=& p\mathrm{Tr}[f(\hat{A})] + (1-p)\mathrm{Tr}[f(\hat{B})],
\end{aligned} \tag{2.32}$$

which is equivalent to Eq. (2.30). □

Let us introduce a concave function $f(x) := -x\log_2 x$ for $x \geq 0$. Then, we define an operator function $S(\hat{\rho})$ with a density operator $\hat{\rho}$ as

$$S(\hat{\rho}) := \mathrm{Tr}[f(\hat{\rho})] = -\mathrm{Tr}[\hat{\rho}\log_2\hat{\rho}], \tag{2.33}$$

where $f(\hat{\rho})$ is the operator function defined by f. This function S is called *von Neumann entropy*. For the spectral decomposition $\hat{\rho} = \sum_i p_i |i\rangle\langle i|$, von Neumann entropy S is reduce to

$$S(\hat{\rho}) = -\sum_i p_i \log_2 p_i =: H(\{p_i\}), \tag{2.34}$$

where the function $H(\{p_i\})$ is called *Shannon entropy*. Since this equation indicates that $S(\hat{\rho})$ is determined only by the eigenvalues of $\hat{\rho}$,

$$S(\hat{\rho}) = S(\hat{U}\hat{\rho}\hat{U}^\dagger) \tag{2.35}$$

holds for any unitary operator $\hat{U}$. In addition, Lemma 2.1 ensures that S is concave. Hence, from Theorem 2.1, von Neumann entropy S generates an entanglement monotone E_f for bipartite states by definitions:

$$E(|\psi\rangle) := S(\mathrm{Tr}_B[|\psi\rangle\langle\psi|]); \tag{2.36}$$

$$E_f(\hat{\rho}) := \min_{\{p_i, |\psi_i\rangle\}} \sum_j p_j E(|\psi_j\rangle). \tag{2.37}$$

E is called *entropy of entanglement*, and E_f is called *entanglement formation* [64]. Note that $E_f(|\psi\rangle) = E(|\psi\rangle)$.

We mention on several simple properties of the entanglement formation.

Corollary 2.1

$$E_f(\hat{\rho}^{AB}_{\rm sep}) = 0, \tag{2.38}$$
$$E_f(\hat{\rho}^{AB}) \leq \min\{S(\hat{\rho}^A), S(\hat{\rho}^B)\}, \tag{2.39}$$

where $\hat{\rho}^{AB}_{\rm sep}$ is a separable state in the form of Eq. (2.12).

Proof. Since $\hat{\rho}^{AB}_{\rm sep} = \sum_i p_i q_{j|i} r_{k|i} |\psi_{ij}\rangle\langle\psi_{ij}|_A \otimes |\phi_{ik}\rangle\langle\phi_{ik}|_B$, we have

$$E_f(\hat{\rho}^{AB}_{\rm sep}) \leq \sum_i p_i q_{j|i} r_{k|i} E(|\psi_{ij}\rangle_A |\phi_{ik}\rangle_B) = 0.$$

Combining this with $E_f \geq 0$, we obtain Eq. (2.38).

For $X = A, B$ and $\hat{\rho}^{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|_{AB}$, we can show

$$E_f(\hat{\rho}^{AB}) \leq \sum_i p_i E(|\psi_i\rangle_{AB}) = \sum_i p_i S({\rm Tr}_X[|\psi_i\rangle\langle\psi_i|_{AB}]) \leq S\left(\sum_i p_i {\rm Tr}_X[|\psi_i\rangle\langle\psi_i|_{AB}]\right) = S(\hat{\rho}^{\bar{X}}), \tag{2.40}$$

where $\bar{A} = B$ and $\bar{B} = A$. This is equivalent to Eq. (2.39). □

For example, let us evaluate the entanglement of state

$$|\Psi^d_{\rm mes}\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle_{AB} \tag{2.41}$$

defined by an orthonormal basis $\{|i\rangle_A |j\rangle_B\}$ on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$. The state with $d = 2$ is equivalent to Bell state $|\Phi^+\rangle_{AB}$. From

$${\rm Tr}_B[|\Psi^d_{\rm mes}\rangle\langle\Psi^d_{\rm mes}|_{AB}] = \hat{I}^A/d, \tag{2.42}$$

we have

$$E_f(|\Psi^d_{\rm mes}\rangle_{AB}) = E(|\Psi^d_{\rm mes}\rangle_{AB}) = S(\hat{I}^A/d) = \log_2 d. \tag{2.43}$$

Combined this with Eq. (2.39), for any density operator $\hat{\rho}^{AB}$, we have

$$E_f(\hat{\rho}^{AB}) \leq S(\hat{\rho}^A) \leq \log_2 d = E_f(|\Psi^d_{\rm mes}\rangle_{AB}). \tag{2.44}$$

Therefore, $|\Psi^d_{\rm mes}\rangle_{AB}$ is called a *maximally entangled state*. In addition, the monotonicity of the entanglement formation provides an operational meaning of the maximally entangled state: Alice and Bob cannot transform state $\hat{\rho}^{AB}$ with $E_f(\hat{\rho}^{AB}) < E_f(|\Psi^d_{\rm mes}\rangle_{AB})$ to the maximally entangled state by LOCC. Thus, the state $|\Psi^d_{\rm mes}\rangle_{AB}$ should be considered to be a state with maximal entanglement.

2.4 Entanglement distillation: recurrence method

Thanks to quantum teleportation protocol introduced in Sec. 2.1, for achieving quantum communication, it is sufficient to share Bell pairs. However, in Sec. 2.3, we see that separated parties, Alice and Bob, cannot increase entanglement by LOCC, let alone generating Bell pairs from scratch. Thus, in order to share a Bell pair, Alice and Bob have no choice but to use a

practical channel that can convey quantum systems. Such a channel inevitably causes noise on the quantum systems, and hence it will return mixed state $\hat{\rho}^{AB}$. Therefore, we need a way to regain entanglement from the mixed state by LOCC. Such a way is called *entanglement distillation*. Although there are several methods to achieve entanglement distillation actually, in this section, we focus on the most realistic distillation called *recurrence method* [64, 65, 66].

In what follows, we consider a system composed of qubits. We begin with introducing a measurement called *parity check measurement*, which is known to be a key operation not only for the recurrence method but also for the other quantum operations such as a fusion gate of cluster states. The measurement is CNOT gate followed by $\hat{Z}$-basis measurement $\{|k\rangle\}_{k=0,1}$ on the target qubit (see Fig. 2.4). In particular, the measurement is described by Kraus operators

$$\begin{aligned}\hat{R}_0^{AB\to B} :=& {}_A\langle 0|\hat{C}_X^{BA} = |0\rangle_{BAB}\langle 00| + |1\rangle_{BAB}\langle 11| = |+\rangle_{BAB}\langle\Phi^+| + |-\rangle_{BAB}\langle\Phi^-|,\\ \hat{R}_1^{AB\to B} :=& {}_A\langle 1|\hat{C}_X^{BA} = |0\rangle_{BAB}\langle 10| + |1\rangle_{BAB}\langle 01| = |+\rangle_{BAB}\langle\Psi^+| - |-\rangle_{BAB}\langle\Psi^-|,\end{aligned} \tag{2.45}$$

where $\hat{C}_X^{CT}$ represents CNOT gate.

The goal of the recurrence method is to transform two entangled pairs into a more entangle pair. Suppose that the two pairs of qubits are shared by Alice and Bob, and called A_1B_1 and A_2B_2, respectively. In the recurrence method, Alice (Bob) executes parity check measurement $\{\hat{R}_k^{A_1A_2\to A_2}\}_{k=0,1}$ ($\{\hat{R}_k^{B_1B_2\to B_2}\}_{k=0,1}$). Then, they exchange the outcomes of the measurement by classical communication, and they declare the success of the recurrence method if their outcomes are the same. From Eqs. (2.45), (A2.1), and (A2.2), the successful measurement of Alice and Bob can be described by Kraus operators

$$\begin{aligned}\hat{R}_0^{A_1A_2\to A_2}\otimes\hat{R}_0^{B_1B_2\to B_2} =& \frac{1}{\sqrt{2}}|\Phi^+\rangle_{A_2B_2}({}_{A_1B_1}\langle\Phi^+|_{A_2B_2}\langle\Phi^+| + {}_{A_1B_1}\langle\Phi^-|_{A_2B_2}\langle\Phi^-|)\\ &+ \frac{1}{\sqrt{2}}|\Psi^+\rangle_{A_2B_2}({}_{A_1B_1}\langle\Psi^+|_{A_2B_2}\langle\Psi^+| + {}_{A_1B_1}\langle\Psi^-|_{A_2B_2}\langle\Psi^-|)\\ &+ \frac{1}{\sqrt{2}}|\Phi^-\rangle_{A_2B_2}({}_{A_1B_1}\langle\Phi^+|_{A_2B_2}\langle\Phi^-| + {}_{A_1B_1}\langle\Phi^-|_{A_2B_2}\langle\Phi^+|)\\ &+ \frac{1}{\sqrt{2}}|\Psi^-\rangle_{A_2B_2}({}_{A_1B_1}\langle\Psi^+|_{A_2B_2}\langle\Psi^-| + {}_{A_1B_1}\langle\Psi^-|_{A_2B_2}\langle\Psi^+|),\\ \hat{R}_1^{A_1A_2\to A_2}\otimes\hat{R}_1^{B_1B_2\to B_2} =& \frac{1}{\sqrt{2}}|\Phi^+\rangle_{A_2B_2}({}_{A_1B_1}\langle\Phi^+|_{A_2B_2}\langle\Phi^+| - {}_{A_1B_1}\langle\Phi^-|_{A_2B_2}\langle\Phi^-|)\\ &+ \frac{1}{\sqrt{2}}|\Psi^+\rangle_{A_2B_2}({}_{A_1B_1}\langle\Psi^+|_{A_2B_2}\langle\Psi^+| - {}_{A_1B_1}\langle\Psi^-|_{A_2B_2}\langle\Psi^-|)\\ &+ \frac{1}{\sqrt{2}}|\Phi^-\rangle_{A_2B_2}({}_{A_1B_1}\langle\Phi^+|_{A_2B_2}\langle\Phi^-| - {}_{A_1B_1}\langle\Phi^-|_{A_2B_2}\langle\Phi^+|)\\ &+ \frac{1}{\sqrt{2}}|\Psi^-\rangle_{A_2B_2}({}_{A_1B_1}\langle\Psi^+|_{A_2B_2}\langle\Psi^-| - {}_{A_1B_1}\langle\Psi^-|_{A_2B_2}\langle\Psi^+|).\end{aligned} \tag{2.46}$$

Leaving the pair A_2B_2, these Kraus operators announce that the pairs A_1B_1 and A_2B_2 have been in a state living in the Hilbert subspace spanned by $|\Phi^\pm\rangle_{A_1B_1}|\Phi^\pm\rangle_{A_2B_2}$, $|\Phi^\pm\rangle_{A_1B_1}|\Phi^\mp\rangle_{A_2B_2}$, $|\Psi^\pm\rangle_{A_1B_1}|\Psi^\pm\rangle_{A_2B_2}$, and $|\Psi^\pm\rangle_{A_1B_1}|\Psi^\mp\rangle_{A_2B_2}$. In what follows, we demonstrate how the recurrence method works.

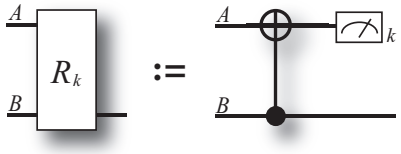

Fig. 2.4. The parity check measurement $\{\hat{R}_k^{AB\to B}\}_{k=0,1}$, which is CNOT gate followed by $\hat{Z}$-basis measurement on the target qubit.

2.4.1 On Bell-diagonal states

Suppose that Alice and Bob apply a unitary operation randomly chosen from $\{\hat{1}^A \otimes \hat{1}^B, \hat{Z}^A \otimes \hat{Z}^B, \hat{X}^A \otimes \hat{X}^B, \hat{Y}^A \otimes \hat{Y}^B\}$ on the pairs A_1B_1 and A_2B_2. Then, their system $A_1B_1A_2B_2$ becomes in a *Bell-diagonal state* ${\hat{\rho}_1}^{A_1B_1} \otimes {\hat{\rho}_2}^{A_2B_2}$ satisfying

$$\hat{\rho}_k^{A_kB_k} = \sum_{i,j=0,1} \langle B_{ij}|\hat{\rho}_k^{A_1B_1}|B_{ij}\rangle |B_{ij}\rangle\langle B_{ij}|_{A_kB_k} \tag{2.47}$$

for $k = 1, 2$ [64, 65, 66]. If Alice and Bob succeed in performing the recurrence method on the system, from Eq. (2.46), the state $\hat{\sigma}^{A_2B_2}$ of the left system A_2B_2 is

$$\begin{aligned}
\langle\Phi^+|\hat{\sigma}^{A_2B_2}|\Phi^+\rangle =& \frac{\langle\Phi^+|\hat{\rho}_1^{A_1B_1}|\Phi^+\rangle\langle\Phi^+|\hat{\rho}_2^{A_2B_2}|\Phi^+\rangle + \langle\Phi^-|\hat{\rho}_1^{A_1B_1}|\Phi^-\rangle\langle\Phi^-|\hat{\rho}_2^{A_2B_2}|\Phi^-\rangle}{P_s^d},\\
\langle\Psi^+|\hat{\sigma}^{A_2B_2}|\Psi^+\rangle =& \frac{\langle\Psi^+|\hat{\rho}_1^{A_1B_1}|\Psi^+\rangle\langle\Psi^+|\hat{\rho}_2^{A_2B_2}|\Psi^+\rangle + \langle\Psi^-|\hat{\rho}_1^{A_1B_1}|\Psi^-\rangle\langle\Psi^-|\hat{\rho}_2^{A_2B_2}|\Psi^-\rangle}{P_s^d},\\
\langle\Phi^-|\hat{\sigma}^{A_2B_2}|\Phi^-\rangle =& \frac{\langle\Phi^+|\hat{\rho}_1^{A_1B_1}|\Phi^+\rangle\langle\Phi^-|\hat{\rho}_2^{A_2B_2}|\Phi^-\rangle + \langle\Phi^-|\hat{\rho}_1^{A_1B_1}|\Phi^-\rangle\langle\Phi^+|\hat{\rho}_2^{A_2B_2}|\Phi^+\rangle}{P_s^d},\\
\langle\Psi^-|\hat{\sigma}^{A_2B_2}|\Psi^-\rangle =& \frac{\langle\Psi^+|\hat{\rho}_1^{A_1B_1}|\Psi^+\rangle\langle\Psi^-|\hat{\rho}_2^{A_2B_2}|\Psi^-\rangle + \langle\Psi^-|\hat{\rho}_1^{A_1B_1}|\Psi^-\rangle\langle\Psi^+|\hat{\rho}_2^{A_2B_2}|\Psi^+\rangle}{P_s^d},
\end{aligned} \tag{2.48}$$

where P_s^d is the success probability described by

$$\begin{aligned}
P_s^d =& (\langle\Phi^+|\hat{\rho}_1^{A_1B_1}|\Phi^+\rangle + \langle\Phi^-|\hat{\rho}_1^{A_1B_1}|\Phi^-\rangle)(\langle\Phi^+|\hat{\rho}_2^{A_2B_2}|\Phi^+\rangle + \langle\Phi^-|\hat{\rho}_2^{A_2B_2}|\Phi^-\rangle)\\
&+ (\langle\Psi^+|\hat{\rho}_1^{A_1B_1}|\Psi^+\rangle + \langle\Psi^-|\hat{\rho}_1^{A_1B_1}|\Psi^-\rangle)(\langle\Psi^+|\hat{\rho}_2^{A_2B_2}|\Psi^+\rangle + \langle\Psi^-|\hat{\rho}_2^{A_2B_2}|\Psi^-\rangle).
\end{aligned} \tag{2.49}$$

Note that state $\hat{\sigma}^{A_2B_2}$ is still Bell-diagonal, and it is thus uniquely determined by Eq. (2.48). In Ref. [67], Macchiavello has considered the performance of this recurrence method in the case of $\hat{\rho}_1 = \hat{\rho}_2$, and has shown that the iteration of this method will asymptotically produce a Bell pair if one of four components $\{\langle B_{ij}|\hat{\rho}_1^{A_1B_1}|B_{ij}\rangle\}_{i,j=0,1}$ is greater than 1/2.

As an example of Bell-diagonal states, here we consider a case where the states $\hat{\rho}_1^{A_1B_1}$ and $\hat{\rho}_2^{A_2B_2}$ are the copies of a state described by

$$\hat{\rho}_O = F|\Phi^+\rangle\langle\Phi^+| + (1-F)|\Psi^+\rangle\langle\Psi^+|. \tag{2.50}$$

This state includes only one type of error, i.e., bit-error. In fact, this state can be expressed as

$$\hat{\rho}_O = \mathcal{E}_{2F-1}^A(|\Phi^+\rangle_{AB}\langle\Phi^+|_{AB}) \tag{2.51}$$

with bit-flip channel $\mathcal{E}^A_{2F-1}$ of Eq. (1.78). Then, Eqs. (2.48) and (2.49) are reduced to

$$\begin{aligned}
&\langle\Phi^+|\hat{\sigma}_O^{A_2B_2}|\Phi^+\rangle = \frac{F^2}{P^d_{s,O}},\\
&\langle\Psi^+|\hat{\sigma}_O^{A_2B_2}|\Psi^+\rangle = \frac{(1-F)^2}{P^d_{s,O}},\\
&\langle\Phi^-|\hat{\sigma}_O^{A_2B_2}|\Phi^-\rangle = 0,\\
&\langle\Psi^-|\hat{\sigma}_O^{A_2B_2}|\Psi^-\rangle = 0,\\
&P^d_{s,O} = F^2 + (1-F)^2.
\end{aligned} \tag{2.52}$$

Clearly, $\langle\Phi^+|\hat{\sigma}_O^{A_2B_2}|\Phi^+\rangle$ is larger than $\langle\Phi^+|\hat{\rho}_O^{A_2B_2}|\Phi^+\rangle$ for any $1/2 < F < 1$. In addition, the output state $\hat{\sigma}_O^{A_2B_2}$ also includes only one-type of error, suggesting that the subsequent distillation from the states $\hat{\sigma}_O^{A_2B_2}$ works similarly. Hence, the iteration of this recurrence method on entangled states $\hat{\rho}_O$ will asymptotically give a Bell pair. Curve (i) in Fig. 2.5 indicates $\langle\Phi^+|\hat{\sigma}_O^{A_2B_2}|\Phi^+\rangle$ as a function of $\langle\Phi^+|\hat{\rho}_O^{A_2B_2}|\Phi^+\rangle$.

2.4.2 On Werner states

As another important examples of Bell-diagonal states, we consider the cases where the two pairs A_1B_1 and A_2B_2 are the copies of a so-called *Werner state*

$$\hat{\rho}_W := F|\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3}(|\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^-\rangle\langle\Psi^-|). \tag{2.53}$$

This state is always obtained by applying a unitary operation randomly chosen from $\{\hat{Z}^A_{\pi/2} \otimes \hat{Z}^B_{\pi/2}, \hat{X}^A_{\pi/2} \otimes \hat{X}^B_{\pi/2}, \hat{Y}^A_{\pi/2} \otimes \hat{Y}^B_{\pi/2}\}$ and a unitary operation $\hat{Z}^B\hat{X}^B$ on a Bell-diagonal state [64, 65]. Then, from Eqs. (2.48) and (2.49), the recurrence method returns a state $\hat{\sigma}_W^{A_2B_2}$ parametrized as

$$\begin{aligned}
\langle\Phi^+|\hat{\sigma}_W^{A_2B_2}|\Phi^+\rangle =& \frac{10F^2 - 2F + 1}{9P^d_{s,W}},\\
\langle\Psi^+|\hat{\sigma}_W^{A_2B_2}|\Psi^+\rangle =& \frac{2(1-F)^2}{9P^d_{s,W}},\\
\langle\Phi^-|\hat{\sigma}_W^{A_2B_2}|\Phi^-\rangle =& \frac{2F(1-F)}{3P^d_{s,W}},\\
\langle\Psi^-|\hat{\sigma}_W^{A_2B_2}|\Psi^-\rangle =& \frac{2(1-F)^2}{9P^d_{s,W}},
\end{aligned} \tag{2.54}$$

with success probability

$$P^d_{s,W} = \frac{1}{9}(8F^2 - 4F + 5). \tag{2.55}$$

Thus, $\langle\Phi^+|\hat{\sigma}_W^{A_2B_2}|\Phi^+\rangle$ is larger than $\langle\Phi^+|\hat{\rho}_W^{A_2B_2}|\Phi^+\rangle$ for any $1/2 < F < 1$. Therefore, combining the fact that any pair with a fidelity F to a Bell state can be transformed to a Werner state with the same F by LOCC, we can always generate an almost perfect Bell pair from many entangled pairs with $F > 1/2$ by recursively using this recurrence method. Curve (ii) in Fig. 2.5 indicates $\langle\Phi^+|\hat{\sigma}_W^{A_2B_2}|\Phi^+\rangle$ as a function of $\langle\Phi^+|\hat{\rho}_W^{A_2B_2}|\Phi^+\rangle$.

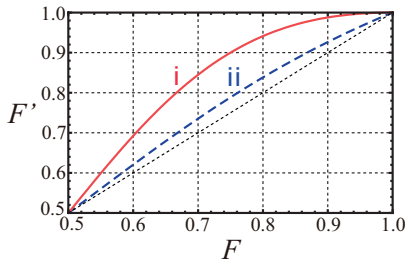

Fig. 2.5. The efficiencies of the recurrence method. F is the fidelity of initial entangled pairs to a Bell state, and F' is the fidelity of a returned pair to a Bell state. The curve (i) is the case where the initial entangled pairs are the copies of $\hat{\rho}_O$. The curve (ii) is the case where the initial entangled pairs are the copies of $\hat{\rho}_W$.

2.5 Apparatuses for quantum communication

As seen in the previous section, entanglement distillation enables us to obtain an almost perfect Bell pair from (possibly many) noisy entangled pairs. To share noisy entangled pairs, we have no choice but to transmit quantum systems through a practical channel. A promising candidate of the transmittable quantum systems is the *photons*. In this section, we briefly review available operations on the photons† and properties of the photons as the carrier of quantum information.

On the other hand, it is known that the interaction among photons are too weak to perform global operations, e.g., CNOT gate. In addition, it is difficult to stop the motion of the photons, which implies that the photons are not appropriate to be used as a kind of memories. Hence, quantum information held by the photons must be transferred to another quantum systems that allow us to use global operations and that can store up the quantum information. Such quantum systems should be called a *quantum memory*. In this section, we also give an example of the quantum memories that can interact with photons.

2.5.1 Photons and those manipulation

In this section, we briefly review the description of the photons and those manipulations. In the last of this section, we show a protocol to realize quantum communication based only on photons.

2.5.1.1 The state of photons

Here we provide a method to describe the state of photons. In quantum mechanics, the free electromagnetic field $\{\hat{\boldsymbol{E}}(\boldsymbol{r}), \hat{\boldsymbol{H}}(\boldsymbol{r})\}$ in a cubic cavity with volume L^3 can be described by

$$\hat{\boldsymbol{E}}(\boldsymbol{r}) = \sum_{\boldsymbol{k}s} \boldsymbol{\epsilon}_{\boldsymbol{k}s} \mathcal{E}_{\boldsymbol{k}} (\hat{a}_{\boldsymbol{k}s} e^{i\boldsymbol{k}\cdot\boldsymbol{r}} + \hat{a}^\dagger_{\boldsymbol{k}s} e^{-i\boldsymbol{k}\cdot\boldsymbol{r}}), \tag{2.56}$$

$$\hat{\boldsymbol{H}}(\boldsymbol{r}) = \frac{1}{\mu_0} \sum_{\boldsymbol{k}s} \frac{\boldsymbol{k} \times \boldsymbol{\epsilon}_{\boldsymbol{k}s}}{\nu_k} \mathcal{E}_{\boldsymbol{k}} (\hat{a}_{\boldsymbol{k}s} e^{i\boldsymbol{k}\cdot\boldsymbol{r}} + \hat{a}^\dagger_{\boldsymbol{k}s} e^{-i\boldsymbol{k}\cdot\boldsymbol{r}}), \tag{2.57}$$

where $\hat{\boldsymbol{E}}(\boldsymbol{r})$ is the electric field, $\hat{\boldsymbol{H}}(\boldsymbol{r})$ is the magnetic field, s is the freedom of the polarization, $\boldsymbol{k}$ is defined by $(k_x, k_y, k_z) = (2\pi n_x/L, 2\pi n_y/L, 2\pi n_z/L)$ with integers $n_x, n_y, n_z = 0, \pm 1, \pm 2, \ldots$, $\nu_k := c|\boldsymbol{k}|$ is the frequency of a plane wave, $\mathcal{E}_{\boldsymbol{k}} := [(\hbar\nu_k)/(2\epsilon_0 L^3)]^{1/2}$, ϵ_0 is the free space

† This review is based on a text book of Mandel and Wolf [68].

permittivity, μ_0 is the free space permeability, $\boldsymbol{\epsilon}_{\boldsymbol{k}s}$ is the unit vector satisfying $\boldsymbol{k}\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s}=0$ and $\boldsymbol{\epsilon}^*_{\boldsymbol{k}s}\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s'}=\delta_{ss'}$, and $\hat{a}_{\boldsymbol{k}s}$ is the *bosonic operator* defined by

$$\begin{aligned}[\hat{a}_{\boldsymbol{k}s},\hat{a}_{\boldsymbol{k}'s'}]&=0,\\ [\hat{a}^\dagger_{\boldsymbol{k}s},\hat{a}^\dagger_{\boldsymbol{k}'s'}]&=0,\\ [\hat{a}_{\boldsymbol{k}s},\hat{a}^\dagger_{\boldsymbol{k}'s'}]&=\delta_{\boldsymbol{k}\boldsymbol{k}'}\delta_{ss'}.\end{aligned}\tag{2.58}$$

The Hamiltonian of the free electromagnetic field is described by

$$\hat{H}=\sum_{\boldsymbol{k}s}\hbar\nu_k\left(\hat{a}^\dagger_{\boldsymbol{k}s}\hat{a}_{\boldsymbol{k}s}+\frac{1}{2}\right).\tag{2.59}$$

Hence, in the Heisenberg picture, the electromagnetic field $\{\hat{\boldsymbol{E}}(\boldsymbol{r},t),\hat{\boldsymbol{H}}(\boldsymbol{r},t)\}$ is

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t)=e^{i\hat{H}t/\hbar}\hat{\boldsymbol{E}}(\boldsymbol{r})e^{-i\hat{H}t/\hbar}=\sum_{\boldsymbol{k}s}\boldsymbol{\epsilon}_{\boldsymbol{k}s}\mathcal{E}_{\boldsymbol{k}}(\hat{a}_{\boldsymbol{k}s}e^{i\boldsymbol{k}\cdot\boldsymbol{r}-i\nu_k t}+\hat{a}^\dagger_{\boldsymbol{k}s}e^{-i\boldsymbol{k}\cdot\boldsymbol{r}+i\nu_k t}),\tag{2.60}$$

$$\hat{\boldsymbol{H}}(\boldsymbol{r},t)=e^{i\hat{H}t/\hbar}\hat{\boldsymbol{H}}(\boldsymbol{r})e^{-i\hat{H}t/\hbar}=\frac{1}{\mu_0}\sum_{\boldsymbol{k}s}\frac{\boldsymbol{k}\times\boldsymbol{\epsilon}_{\boldsymbol{k}s}}{\nu_k}\mathcal{E}_{\boldsymbol{k}}(\hat{a}_{\boldsymbol{k}s}e^{i\boldsymbol{k}\cdot\boldsymbol{r}-i\nu_k t}+\hat{a}^\dagger_{\boldsymbol{k}s}e^{-i\boldsymbol{k}\cdot\boldsymbol{r}+i\nu_k t}),\tag{2.61}$$

where we used relation

$$e^{i\hat{a}^\dagger_{\boldsymbol{k}s}\hat{a}_{\boldsymbol{k}s}\nu_k t}\hat{a}_{\boldsymbol{k}s}(\boldsymbol{r})e^{-i\hat{a}^\dagger_{\boldsymbol{k}s}\hat{a}_{\boldsymbol{k}s}\nu_k t}=\hat{a}_{\boldsymbol{k}s}e^{-i\nu_k t}\tag{2.62}$$

derived from formula

$$e^{\hat{A}}\hat{B}e^{-\hat{A}}=\hat{B}+[\hat{A},\hat{B}]+\frac{1}{2!}[\hat{A},[\hat{A},\hat{B}]]+\ldots.\tag{2.63}$$

Therefore, the state of the electromagnetic field lives in the Hilbert space the bosonic operators $\{\hat{a}_{\boldsymbol{k}s}\}_{\boldsymbol{k}s}$ act on.

In what follows, for the simplicity, we omit $\boldsymbol{k}s$ of operator $\hat{a}_{\boldsymbol{k}s}$, and denote it as $\hat{a}$. Let us consider how to describe the state of the Hilbert space $\hat{a}$ acts on. Since $\hat{n}:=\hat{a}^\dagger\hat{a}$ is a positive operator, we can diagonalize it as follows

$$\hat{n}=\sum_n n|n\rangle\langle n|\tag{2.64}$$

with

$$n\geq 0.\tag{2.65}$$

The operator $\hat{n}$ is called the number operator. Noting $[\hat{n},\hat{a}]=-\hat{a}$, i.e., $\hat{n}\hat{a}=\hat{a}\hat{n}-\hat{a}$, we have

$$\hat{n}(\hat{a}|n\rangle)=(n-1)\hat{a}|n\rangle,\tag{2.66}$$

which implies that $\hat{a}|n\rangle$ is the eigenstate of $\hat{n}$ with eigenvalue $n-1$. This indicates that $\hat{a}^k|n\rangle$ is the eigenstate of $\hat{n}$ with eigenvalue $n-k$ for any k, but this fact must be compatible with Eq. (2.65). Hence, n should be a non-negative integer and $\hat{a}|0\rangle=0$. The state $|n\rangle$ with $n=0,1,\ldots$ is called a *number state*, and $|0\rangle$ is specifically called the *vacuum state*. The normalization of state $\hat{a}|n\rangle$ implies

$$\hat{a}|n\rangle=\sqrt{n}|n-1\rangle\tag{2.67}$$

for any n. By applying $\hat{a}^\dagger$ to this equation, we have

$$\hat{a}^\dagger|n\rangle=\sqrt{n+1}|n+1\rangle,\tag{2.68}$$

which implies

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle. \tag{2.69}$$

Since this indicates that $|n\rangle$ is generated by applying $\hat{a}^\dagger$ to the vacuum state $|0\rangle$, $\hat{a}^\dagger$ is called *creation operator*. Conversely, $\hat{a}$ is called *annihilation operator*.

Since $\{|n\rangle\}_{n=0,1,\ldots}$ is an complete orthonormal basis, we have $\sum_{n=0}^{\infty}|n\rangle\langle n| = \hat{I}$. This implies that any state $|\psi\rangle$ of a single-mode electromagnetic field can be described by

$$|\psi\rangle = \hat{I}|\psi\rangle = \sum_{n=0}^{\infty}\langle n|\psi\rangle|n\rangle. \tag{2.70}$$

Similarly, the state of general electromagnetic fields is described by

$$|\psi\rangle = \bigotimes_{\boldsymbol{k}s}\left(\sum_{n_{\boldsymbol{k}s}=0}^{\infty}|n_{\boldsymbol{k}s}\rangle\langle n_{\boldsymbol{k}s}|\right)|\psi\rangle. \tag{2.71}$$

Let us introduce the so-called *coherent state*. This state is the description of an output pulse of the laser. A coherent state $|\alpha\rangle$ is defined as

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle = e^{-|\alpha|^2/2}e^{\alpha\hat{a}^\dagger}|0\rangle \tag{2.72}$$

with a complex number α. From Eq. (2.67), we can show

$$\hat{a}|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=1}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\sqrt{n}|n-1\rangle = \alpha|\alpha\rangle, \tag{2.73}$$

which means that this state is an eigenstate of annihilation operator $\hat{a}$. The coherent state can be also considered as a displaced vacuum state. In particular, the state $|\alpha\rangle$ can be described by

$$|\alpha\rangle = \hat{D}_\alpha|0\rangle \tag{2.74}$$

with the *displacement operator*

$$\hat{D}_\alpha := e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}. \tag{2.75}$$

Eq. (2.74) can be ensured from

$$\hat{D}_\alpha = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = e^{-|\alpha|^2/2}e^{\alpha\hat{a}^\dagger}e^{-\alpha^*\hat{a}}, \tag{2.76}$$

where we used the *Campbell-Baker-Hausdorff relation* for two operators $\hat{A}$, $\hat{B}$, i.e.,

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}}e^{\hat{B}}e^{-[\hat{A},\hat{B}]/2}, \tag{2.77}$$

provided that

$$[\hat{A},[\hat{A},\hat{B}]] = [\hat{B},[\hat{A},\hat{B}]] = 0. \tag{2.78}$$

The displacement operators have properties

$$\hat{D}_\alpha^\dagger\hat{D}_\alpha = \hat{D}_\alpha\hat{D}_\alpha^\dagger = \hat{I}, \tag{2.79}$$

$$\hat{D}_\alpha^\dagger = \hat{D}_{-\alpha}, \tag{2.80}$$

$$\hat{D}_\alpha\hat{D}_\beta = e^{i\mathrm{Im}[\alpha\beta^*]}\hat{D}_{\alpha+\beta}. \tag{2.81}$$

Eqs. (2.79) and (2.80) are confirmed from Eq. (2.76), and Eq. (2.81) is shown from the Campbell-Baker-Hausdorff relation.

2.5.1.2 Linear optical elements

Let us introduce unitary operations obtained by basic linear optical elements, *phase shifters* and *beam splitters*. The phase shifter can be considered to be a gate on a single-mode optical field as in Fig. 2.6 (a). The time evolution given by the phase shifter corresponds to a unitary operator $\hat{P}_\theta$ relating an input bosonic operator $\hat{a}_1$ with an output operator $\hat{a}_2$ as

$$\hat{a}_2 = e^{i\theta}\hat{P}_\theta \hat{a}_1 \hat{P}_\theta^\dagger, \tag{2.82}$$

where θ is a real number. Noting

$$[\hat{U}\hat{A}\hat{U}^\dagger, \hat{U}\hat{B}\hat{U}^\dagger] = \hat{U}[\hat{A}, \hat{B}]\hat{U}^\dagger \tag{2.83}$$

for any unitary operator $\hat{U}$ and arbitrary operators $\hat{A}$ and $\hat{B}$, we have

$$[\hat{a}_2, \hat{a}_2^\dagger] = \hat{P}_\theta[\hat{a}_1, \hat{a}_1^\dagger]\hat{P}_\theta^\dagger = 1 \tag{2.84}$$

which implies that $\hat{a}_2$ is also a bosonic operator. The number operator $\hat{a}_1^\dagger\hat{a}_1$ satisfies

$$\hat{P}_\theta \hat{a}_1^\dagger \hat{a}_1 \hat{P}_\theta^\dagger = \hat{a}_2^\dagger \hat{a}_2. \tag{2.85}$$

Combined with the fact that a state $|\psi\rangle$ evolves into $\hat{P}_\theta|\psi\rangle$, this indicates

$$\langle\phi|\hat{P}_\theta^\dagger \hat{a}_2^\dagger \hat{a}_2 \hat{P}_\theta|\psi\rangle = \langle\phi|\hat{a}_1^\dagger\hat{a}_1|\psi\rangle \tag{2.86}$$

for arbitrary states $|\psi\rangle$ and $|\phi\rangle$. Thus, the role of number operator $\hat{a}_1^\dagger\hat{a}_1$ on a system is replaced with that of number operator $\hat{a}_2^\dagger\hat{a}_2$ on the system outputted by the phase shifter $\hat{P}_\theta$. This implies

$$\hat{P}_\theta|0\rangle = |0\rangle. \tag{2.87}$$

Actually, this equation and Eq. (2.82) are sufficient for determining the effect of the unitary operator $\hat{P}_\theta$.

The beam splitter can be considered to be a gate on two single-mode optical fields as in Fig. 2.6 (b). The time evolution given by the beam splitter corresponds to a unitary operator $\hat{B}_{t,r,t',r'}$ relating input bosonic operators $\{\hat{a}_1, \hat{a}_2\}$ with output operators $\{\hat{a}_3, \hat{a}_4\}$ as

$$\begin{aligned} \hat{a}_3 =& \hat{B}_{t,r,t',r'}(t'\hat{a}_1 + r\hat{a}_2)\hat{B}_{t,r,t',r'}^\dagger, \\ \hat{a}_4 =& \hat{B}_{t,r,t',r'}(r'\hat{a}_1 + t\hat{a}_2)\hat{B}_{t,r,t',r'}^\dagger, \end{aligned} \tag{2.88}$$

where t, r, t', r' are parameters satisfying

$$|r'| = |r|, \tag{2.89}$$
$$|t'| = |t|, \tag{2.90}$$
$$|r|^2 + |t|^2 = 1, \tag{2.91}$$
$$r^*t' + r't^* = 0, \tag{2.92}$$
$$r^*t + r't'^* = 0. \tag{2.93}$$

Note that Eq. (2.88) can be also described by

$$\begin{pmatrix} \hat{a}_3 \\ \hat{a}_4 \end{pmatrix} = B \begin{pmatrix} \hat{B}_{t,r,t',r'}\hat{a}_1\hat{B}_{t,r,t',r'}^\dagger \\ \hat{B}_{t,r,t',r'}\hat{a}_2\hat{B}_{t,r,t',r'}^\dagger \end{pmatrix} \tag{2.94}$$

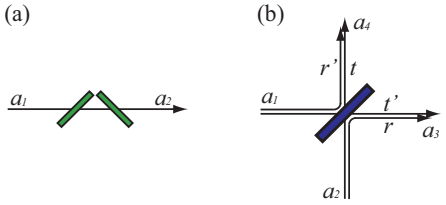

Fig. 2.6. Linear optical elements. (a) Phase shifter. (b) Beam splitter.

with a matrix

$$B := \begin{pmatrix} t' & r \\ r' & t \end{pmatrix}. \tag{2.95}$$

Then, Eqs. (2.89)-(2.93) are equivalent to the unitarity of matrix B, i.e., $B^\dagger B = BB^\dagger = I$. From Eqs. (2.89)-(2.91) and (2.83), we have

$$[\hat{a}_3, \hat{a}_3^\dagger] = \hat{B}_{t,r,t',r'}[t'\hat{a}_1 + r\hat{a}_2, t'^*\hat{a}_1^\dagger + r^*\hat{a}_2^\dagger]\hat{B}_{t,r,t',r'}^\dagger = 1, \tag{2.96}$$

$$[\hat{a}_4, \hat{a}_4^\dagger] = \hat{B}_{t,r,t',r'}[r'\hat{a}_1 + t\hat{a}_2, r'^*\hat{a}_1^\dagger + t^*\hat{a}_2^\dagger]\hat{B}_{t,r,t',r'}^\dagger = 1, \tag{2.97}$$

which indicates that operators $\{\hat{a}_3, \hat{a}_4\}$ are also bosonic operators. From Eq. (2.93) and (2.83), we obtain

$$[\hat{a}_3, \hat{a}_4^\dagger] = \hat{B}_{t,r,t',r'}[t'\hat{a}_1 + r\hat{a}_2, r'^*\hat{a}_1^\dagger + t^*\hat{a}_2^\dagger]\hat{B}_{t,r,t',r'}^\dagger = 0, \tag{2.98}$$

which concludes that the mode of $\hat{a}_3$ is different from that of $\hat{a}_4$. From Eq. (2.92), the total number operator of $\hat{a}_1^\dagger\hat{a}_1 + \hat{a}_2^\dagger\hat{a}_2$ satisfies

$$\hat{B}_{t,r,t',r'}(\hat{a}_1^\dagger\hat{a}_1 + \hat{a}_2^\dagger\hat{a}_2)\hat{B}_{t,r,t',r'}^\dagger = \hat{a}_3^\dagger\hat{a}_3 + \hat{a}_4^\dagger\hat{a}_4. \tag{2.99}$$

This implies that the role of number operator $\hat{a}_1^\dagger\hat{a}_1 + \hat{a}_2^\dagger\hat{a}_2$ on a system is replaced with that of number operator $\hat{a}_3^\dagger\hat{a}_3 + \hat{a}_4^\dagger\hat{a}_4$ on the system outputted by the beam splitter $\hat{B}_{t,r,t',r'}$. This indicates

$$\hat{B}_{t,r,t',r'}|0\rangle = |0\rangle. \tag{2.100}$$

Similarly to the phase shifter, this equation and Eq. (2.88) are sufficient for determining the action of the unitary operator $\hat{B}_{t,r,t',r'}$.

As an example, let us apply the phase shifter and the beam splitter to a system in a coherent state. If we perform phase shifter $\hat{P}_\theta$ on a system in coherent state $|\alpha\rangle_1$, we will obtain state

$$\hat{P}_\theta|\alpha\rangle_1 = e^{-|\alpha|^2/2}\hat{P}_\theta e^{\alpha\hat{a}_1^\dagger}\hat{P}_\theta^\dagger\hat{P}_\theta|0\rangle = e^{-|\alpha|^2/2}e^{\alpha\hat{P}_\theta\hat{a}_1^\dagger\hat{P}_\theta^\dagger}|0\rangle = e^{-|\alpha|^2/2}e^{\alpha e^{i\theta}\hat{a}_2^\dagger}|0\rangle = |\alpha e^{i\theta}\rangle_2, \tag{2.101}$$

where we used Eqs. (2.82) and (2.87). On the other hand, if we apply beam splitter $\hat{B}_{t,r,t',r'}$ to a system in a coherent state $|\alpha\rangle_1|\beta\rangle_2$, we will obtain state

$$\begin{aligned}
\hat{B}_{t,r,t',r'}|\alpha\rangle_1|\beta\rangle_2 =& e^{-(|\alpha|^2+|\beta|^2)/2}\hat{B}_{t,r,t',r'}e^{\alpha\hat{a}_1^\dagger+\beta\hat{a}_2^\dagger}\hat{B}_{t,r,t',r'}^\dagger\hat{B}_{t,r,t',r'}|0\rangle \\
=& e^{-(|\alpha|^2+|\beta|^2)/2}e^{\hat{B}_{t,r,t',r'}(\alpha\hat{a}_1^\dagger+\beta\hat{a}_2^\dagger)\hat{B}_{t,r,t',r'}^\dagger}|0\rangle \\
=& e^{-(|\alpha|^2+|\beta|^2)/2}e^{\alpha(t'^*\hat{a}_3^\dagger+r'^*\hat{a}_4^\dagger)+\beta(r^*\hat{a}_3^\dagger+t^*\hat{a}_4^\dagger)}|0\rangle \\
=& |t'^*\alpha + r^*\beta\rangle_3|r'^*\alpha + t^*\beta\rangle_4,
\end{aligned} \tag{2.102}$$

where we used Eqs. (2.88) and (2.100).

For simplicity, we may define a beam splitter as

$$\hat{B}_T := \hat{B}_{\sqrt{T},\sqrt{1-T},\sqrt{T},-\sqrt{1-T}} \tag{2.103}$$

with real parameter $0 \leq T \leq 1$, because the combination of this beam splitter and proper phase shifters can simulate arbitrary beam splitters represented by Eq. (2.88). T is called the *transmittance*. In this case, Eq. (2.102) is reduced to

$$\hat{B}_T|\alpha\rangle_1|\beta\rangle_2 = |\sqrt{T}\alpha + \sqrt{1-T}\beta\rangle_3|-\sqrt{1-T}\alpha + \sqrt{T}\beta\rangle_4. \tag{2.104}$$

The beam splitter plays important roles in manipulation of photons. As an example of applications of the beam splitter, we show that the displacement operator $\hat{D}_\gamma$ is implementable by the combination of a beam splitter and an additional pulse in a coherent state. Let us assume $\beta = (\sqrt{T}/\sqrt{1-T})\gamma$ in Eq. (2.104). Then, the equation is altered to

$$\hat{B}_T|\alpha\rangle_1|(\sqrt{T}/\sqrt{1-T})\gamma\rangle_2 = |\sqrt{T}(\alpha+\gamma)\rangle_3|-\sqrt{1-T}\alpha + (T/\sqrt{1-T})\gamma\rangle_4. \tag{2.105}$$

From $\langle\alpha|\beta\rangle = e^{-(|\alpha|^2+|\beta|^2)/2}e^{\alpha^*\beta}$ for coherent states $|\alpha\rangle$ and $|\beta\rangle$, we have

$$\begin{aligned}
&{}_4\langle(T/\sqrt{1-T})\gamma| - \sqrt{1-T}\alpha + (T/\sqrt{1-T})\gamma\rangle_4 \\
&\quad = e^{-[T^2/(1-T)|\gamma|^2+(1-T)|\alpha|^2+(T^2/1-T)|\gamma|^2-T(\alpha^*\gamma+\alpha\gamma^*)]/2}e^{-T\alpha\gamma^*+(T^2/1-T)|\gamma|^2} \\
&\quad = e^{(1-T)|\alpha|^2/2}e^{T(\alpha^*\gamma-\alpha\gamma^*)/2} = e^{(1-T)|\alpha|^2/2}e^{iT\mathrm{Im}[\gamma\alpha^*]},
\end{aligned} \tag{2.106}$$

which means

$$|-\sqrt{1-T}\alpha + (T/\sqrt{1-T})\gamma\rangle_4 \overset{T\to1}{\longrightarrow} e^{i\mathrm{Im}[\gamma\alpha^*]}|\phi(\gamma)\rangle_4 \tag{2.107}$$

for a state $|\phi(\gamma)\rangle_4 := \lim_{T\to1}|(T/\sqrt{1-T})\gamma\rangle_4$ depending only on γ. Hence, in the limit of $T \to 1$, Eq. (2.105) is reduced to

$$\lim_{T\to1}\hat{B}_T|\alpha\rangle_1|(\sqrt{T}/\sqrt{1-T})\gamma\rangle_2 = e^{i\mathrm{Im}[\gamma\alpha^*]}|\alpha+\gamma\rangle_3|\phi(\gamma)\rangle_4 = (\hat{D}_\gamma|\alpha\rangle_3)\otimes|\phi(\gamma)\rangle_4. \tag{2.108}$$

Therefore, the displacement operation is implementable by a beam splitter and an optical pulse in a coherent state.

2.5.1.3 Transmission channel

Transmission channels of the photons such as optical fibers are useful for quantum communication. An ideal transmission channel will enable us to faithfully send an unknown state $|\psi\rangle$ of the input bosonic mode to the output bosonic mode. However, practical channels are not such an ideal one. In particular, the practical channels inevitably leak a fraction of the transmitted photons into the environment e. This noise is specifically called *photon loss*. To describe the practical channels with such an imperfection, we conventionally use the beam splitter $\hat{B}_{t,r,t',r'}$. As noted in the previous section, the beam splitter $\hat{B}_{t,r,t',r'}$ relates the two bosonic operators $\{\hat{a}_1, \hat{a}_2\}$ to the two output operators $\{\hat{a}_3, \hat{a}_4\}$ according to Eq. (2.88). Here, for the description of the practical channel, we regard the bosonic mode $\hat{a}_1$ as the input mode $\hat{a}_{\mathrm{in}}$ of the channel, the bosonic mode $\hat{a}_2$ as the input mode $\hat{a}_e$ of the environment, the bosonic mode $\hat{a}_3$ as the output mode $\hat{a}_{\mathrm{out}}$ of the channel, and the bosonic mode $\hat{a}_4$ as the output mode $\hat{a}_e$ of the environment. We further assume that the initial state of the environment e is the vacuum state $|0\rangle_e$. These assumptions define an isometry $\hat{N}_{t,r,t',r'}$ as a theoretical model of the practical channel.

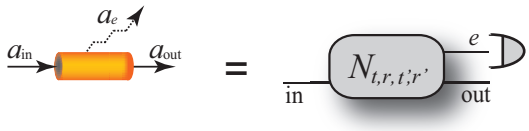

Fig. 2.7. Transmission channel.

Let us consider that a boson in state $|n\rangle_{\text{in}}$ is inputted into such a practical channel. Then, the channel returns state

$$\begin{aligned}\hat{N}_{t,r,t',r'}|n\rangle_{\text{in}} :=& \hat{B}_{t,r,t',r'}|n\rangle_{\text{in}}|0\rangle_e = \hat{B}_{t,r,t',r'}\frac{(\hat{a}^\dagger_{\text{in}})^n}{\sqrt{n!}}|0\rangle = \frac{1}{\sqrt{n!}}\hat{B}_{t,r,t',r'}(\hat{a}^\dagger_{\text{in}})^n\hat{B}^\dagger_{t,r,t',r'}\hat{B}_{t,r,t',r'}|0\rangle \\ =& \frac{1}{\sqrt{n!}}(\hat{B}_{t,r,t',r'}\hat{a}^\dagger_{\text{in}}\hat{B}^\dagger_{t,r,t',r'})^n|0\rangle = \frac{1}{\sqrt{n!}}(t'^*\hat{a}^\dagger_{\text{out}} + r'^*\hat{a}^\dagger_e)^n|0\rangle \\ =& \frac{1}{\sqrt{n!}}\sum_{k=0}^{n}\left(\begin{array}{c} n \\ k \end{array}\right)(t'^*\hat{a}^\dagger_{\text{out}})^k(r'^*\hat{a}^\dagger_e)^{n-k}|0\rangle \\ =& \sum_{k=0}^{n}\sqrt{\left(\begin{array}{c} n \\ k \end{array}\right)}(t'^*)^k(r'^*)^{n-k}|k\rangle_{\text{out}}|n-k\rangle_e\end{aligned} \tag{2.109}$$

as the output, where we define

$$\hat{N}_{t,r,t',r'} := \hat{B}_{t,r,t',r'}|0\rangle_e. \tag{2.110}$$

Since we cannot access the state of the environment e, the partial trace over system e is applied after the isometry $\hat{N}_{t,r,t',r'}$, implying that the practical channel corresponds to a channel depicted in Fig. 2.7. Combining these with the fact that any state $|\psi\rangle_{\text{in}}$ can be described by the superposition of the state $|n\rangle_{\text{in}}$, we can uniquely determine the output state of the practical channel for any input state.

For example, if we input a pulse in coherent state $|\alpha\rangle$ to the practical channel, we receive

$$\hat{N}_{t,r,t',r'}|\alpha\rangle_{\text{in}} = \hat{B}_{t,r,t',r'}|\alpha\rangle_{\text{in}}|0\rangle_e = |t'^*\alpha\rangle_{\text{out}}|r'^*\alpha\rangle_e, \tag{2.111}$$

as the output state. Here we used Eq. (2.102).

In practice, we use a transmission channel whose parameters t, r, t', r' are estimated in advance. In such a case, up to the freedom of phase shifters on the input/output modes, the channel can be characterized only by the transmittance T such that

$$\hat{N}_T := \hat{B}_{\sqrt{T},-\sqrt{1-T},\sqrt{T},\sqrt{1-T}}|0\rangle_e. \tag{2.112}$$

In practical setups, the parameters of the channel may fluctuate because of noises such as thermal noises, but even in this situation, there are cases where the model of Eq. (2.112) becomes valid by utilizing an additional optical pulse as the reference of the fluctuations.

Actually, the transmittance T of the channel $\hat{N}_T$ is related with the channel distance L. The relation is described by

$$T = e^{-L/L_{\text{att}}} \tag{2.113}$$

with an *attenuation length* $L_{\rm att}$†. That is, the transmittance of the channel decreases exponentially with the channel length, which makes long-distance quantum communication difficult to be achieved as shown later.

2.5.1.4 Photon detectors

A *photon detector* is a device to count photons. The most ideal photon detector is called the *ideal photon-number-resolving detector*, whose POVM elements $\{\hat{E}_m^{(\infty)}\}_{m=0,1,\ldots}$ are described by $\hat{E}_m^{(\infty)} = |m\rangle\langle m|$ with the number state $|m\rangle$. In general, the photon detectors cannot necessarily count photons up to infinite numbers, namely, there are possibilities such that they can count photons up to $N(\geq 0)$. More precisely, the photon detector returns outcome m if it catches $m(\leq N)$ photons, but it gives outcome $N+1$ if it receives photons more than N. The $(N+2)$ POVM elements of the detector are described by

$$\hat{E}_m^{(N)} = \begin{cases} |m\rangle\langle m|, & (0 \leq m \leq N), \\ \sum_{n=N+1}^{\infty} |n\rangle\langle n|, & (m = N+1). \end{cases} \tag{2.114}$$

This POVM is described as in Fig. 2.8 (a). The detector with $N = 1$ is called *single photon detector*, and the detector with $N = 0$ is called *threshold detector*.

In practice, there are various imperfections of the detectors. For example, not all the incident photons are caught by the detector. This imperfection can be modeled as a transmission channel $\hat{N}_\eta$ in front of the detector (see Fig. 2.8 (b)). The transmittance η is specifically called the *quantum efficiency*. The POVM elements of the detector with quantum efficiency η are described by $\{E_m^{(N,\eta)}\}_{m=0,\ldots,N+1}$ in Fig. 2.8 (b).

Another type of the imperfections is the so-called *dark counts*. The dark counts are caused by an event where the photons from the environment are mixed with the signal mode. The redundant photons are effectively described by

$$\hat{\rho}_\nu := \sum_{m=0}^{\infty} \frac{e^{-\nu}\nu^m}{m!} |m\rangle\langle m|, \tag{2.115}$$

where $\nu \geq 0$ indicates *mean dark count*. This implies that m additional photons are appended to the signal mode with probability $(e^{-\nu}\nu^m)/(m!)$. Thus, the probability with which the number of the signal photons is k but the photon detector announces the arrival of $m(\geq k)$ photons is $(e^{-\nu}\nu^{m-k})/[(m-k)!]$. This indicates that the POVM elements $\hat{E}_m^{(N,1,\nu)}$ of the photon detector with threshold N and mean dark count ν are described by

$$\hat{E}_m^{(N,1,\nu)} = \begin{cases} \sum_{k=0}^{m} \frac{e^{-\nu}\nu^{m-k}}{(m-k)!} |k\rangle\langle k|, & (0 \leq m \leq N), \\ \sum_{n=N+1}^{\infty} \sum_{k=0}^{n} \frac{e^{-\nu}\nu^{n-k}}{(n-k)!} |k\rangle\langle k|, & (m = N+1). \end{cases} \tag{2.116}$$

This POVM is described as in Fig. 2.8 (c).

More generally, there are detectors with threshold N, quantum efficiency η, and mean dark count ν. The POVM are described by $\{E_m^{(N,\eta,\nu)}\}_{m=0,\ldots,N+1}$ in Fig. 2.8 (d).

2.5.1.5 Quantum communication based on the direct transmission of photons

As an example, we introduce a way to share entanglement between separated parties, Alice and Bob. Suppose that they are distance $2L$ apart, and Claire is located in the middle point between

† The attenuation length is determined by the physical properties of the channel.

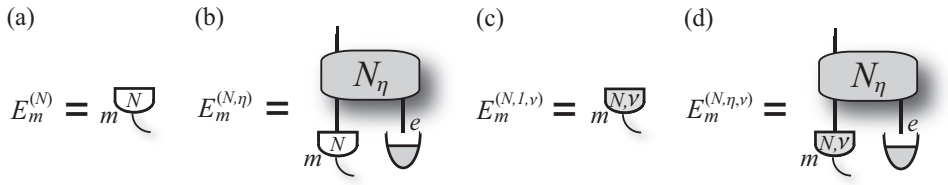

Fig. 2.8. Photon detectors. (a) Ideal photon detector with threshold N. (b) Photon detector with threshold N and quantum efficiency η. (c) Photon detector with threshold N and mean dark count ν. (d) Photon detector with threshold N, quantum efficiency η, and mean dark count ν.

Alice and Bob. Alice prepares a bosonic Bell state described by

$$|\Psi^+_{\rm boson}\rangle_{aa_c} := \frac{1}{\sqrt{2}}(\hat{a}^\dagger_{a_c} + \hat{a}^\dagger_a)|0\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{aa_c} + |10\rangle_{aa_c}), \tag{2.117}$$

and she sends the photon in mode a_c to Claire through transmission channel $\hat{N}_T^{a_c\to c_a}$. Bob also prepares the same state $|\Psi^+_{\rm boson}\rangle_{bb_c}$, and sends the photon in mode b_c to Claire through transmission channel $\hat{N}_T^{b_c\to c_b}$. At this point, from Eq. (2.109), the total state $|\psi\rangle_{\rm in}$ is described by

$$\begin{aligned}
|\psi_{\rm in}\rangle =& \hat{N}_T^{a_c\to c_a}\hat{N}_T^{b_c\to c_b}\frac{1}{2}(\hat{a}^\dagger_{a_c} + \hat{a}^\dagger_a)(\hat{a}^\dagger_{b_c} + \hat{a}^\dagger_b)|0\rangle \\
=& \frac{1}{2}(\sqrt{T}\hat{a}^\dagger_{c_a} + \sqrt{1-T}\hat{a}^\dagger_{e_a} + \hat{a}^\dagger_a)(\sqrt{T}\hat{a}^\dagger_{c_b} + \sqrt{1-T}\hat{a}^\dagger_{e_b} + \hat{a}^\dagger_b)|0\rangle \\
=& \frac{1}{2}[T\hat{a}^\dagger_{c_a}\hat{a}^\dagger_{c_b} + (1-T)\hat{a}^\dagger_{e_a}\hat{a}^\dagger_{e_b} + \hat{a}^\dagger_a\hat{a}^\dagger_b + \sqrt{T(1-T)}(\hat{a}^\dagger_{c_a}\hat{a}^\dagger_{e_b} + \hat{a}^\dagger_{c_b}\hat{a}^\dagger_{e_a}) \\
&+ \sqrt{T}(\hat{a}^\dagger_{c_a}\hat{a}^\dagger_b + \hat{a}^\dagger_{c_b}\hat{a}^\dagger_a) + \sqrt{1-T}(\hat{a}^\dagger_{e_a}\hat{a}^\dagger_b + \hat{a}^\dagger_{e_b}\hat{a}^\dagger_a)]|0\rangle \\
=& \frac{1}{2}[T|00\rangle_{ab}|11\rangle_{c_ac_b}|00\rangle_{e_ae_b} + (1-T)|00\rangle_{ab}|00\rangle_{c_ac_b}|11\rangle_{e_ae_b} + |11\rangle_{ab}|00\rangle_{c_ac_b}|00\rangle_{e_ae_b} \\
&+ \sqrt{T(1-T)}(|00\rangle_{ab}|10\rangle_{c_ac_b}|01\rangle_{e_ae_b} + |00\rangle_{ab}|01\rangle_{c_ac_b}|10\rangle_{e_ae_b}) \\
&+ \sqrt{T}(|01\rangle_{ab}|10\rangle_{c_ac_b}|00\rangle_{e_ae_b} + |10\rangle_{ab}|01\rangle_{c_ac_b}|00\rangle_{e_ae_b}) \\
&+ \sqrt{1-T}(|01\rangle_{ab}|00\rangle_{c_ac_b}|10\rangle_{e_ae_b} + |10\rangle_{ab}|00\rangle_{c_ac_b}|01\rangle_{e_ae_b})]
\end{aligned} \tag{2.118}$$

where e_a and e_b are modes in the environment.

On receiving the bosons, Claire applies a beam splitter $\hat{B}_T^{c_ac_b\to d_ad_b}$ with $T = 1/2$, and she counts photons of the output modes d_ad_b. If she detects a single photon at either mode d_a or d_b, she declares the success. The Kraus operators in the success cases are described by

$${}_{d_ad_b}\langle 10|(\hat{B}_{1/2}^{c_ac_b\to d_ad_b})^\dagger = \frac{1}{\sqrt{2}}({}_{c_ac_b}\langle 10| + {}_{c_ac_b}\langle 01|), \tag{2.119}$$

$${}_{d_ad_b}\langle 01|(\hat{B}_{1/2}^{c_ac_b\to d_ad_b})^\dagger = \frac{1}{\sqrt{2}}({}_{c_ac_b}\langle 10| - {}_{c_ac_b}\langle 01|). \tag{2.120}$$

Hence, we have

$${}_{d_ad_b}\langle 10|(\hat{B}_{1/2}^{c_ac_b\to d_ad_b})^\dagger|\psi_{\rm in}\rangle = \frac{\sqrt{T}}{2}(|\Psi^+\rangle_{ab}|00\rangle_{e_ae_b} + \sqrt{1-T}|00\rangle_{ab}|\Psi^+\rangle_{e_ae_b}), \tag{2.121}$$

$${}_{d_ad_b}\langle 01|(\hat{B}_{1/2}^{c_ac_b\to d_ad_b})^\dagger|\psi_{\rm in}\rangle = \frac{\sqrt{T}}{2}(|\Psi^-\rangle_{ab}|00\rangle_{e_ae_b} + \sqrt{1-T}|00\rangle_{ab}|\Psi^-\rangle_{e_ae_b}), \tag{2.122}$$

where $|\Psi^-\rangle := (|01\rangle - |10\rangle)/\sqrt{2}$. Assuming that Alice applies phase shifter $\hat{P}_\pi^a$ if detector d_b announces the arrival of a single photon, Alice and Bob will share state

$$\hat{\rho}^{ab} = \frac{1}{2-T}|\Psi^+\rangle\langle\Psi^+|_{ab} + \frac{1-T}{2-T}|00\rangle\langle 00|_{ab} \tag{2.123}$$

with probability $P_s := T(2-T)/2$. Since T decreases exponentially with distance L of the channel, from Eq. (2.113), for large L, the success probability P_s becomes

$$P_s \sim T = e^{-L/L_{\rm att}}. \tag{2.124}$$

Therefore, quantum communication is achievable by the direct transmission of photons, but the efficiency decreases exponentially with the channel length.

2.5.2 Λ-type system and the interaction with photons

As shown in Sec. 2.5.1.5, we can achieve entanglement distribution by the direct transmission of photons through a transmission channel such as an optical fiber. But, because of the exponential increase of the photon loss, the efficiency decreases exponentially with the channel length, which will strongly restrict the achievable distances of quantum communication. To avoid the exponential increase of the photon loss, we have no choice but to give up the direct transmission of photons over long distances. Instead, actually, we have two protocols to achieve long-distance quantum communication against the photon loss: one way is the so-called *quantum repeater protocol*; the other way is the so-called *satellite-based quantum communication*. Either way needs quantum memories that can interact with photons, and is based on entanglement generation between moderately distant quantum memories by utilizing photons. In this section, we introduce a quantum memory that can be realizable by various two-level quantum systems, and we show how the quantum memory interacts with photons. We further show that the interaction is achievable even by Λ-type systems. An entanglement generation protocol and several methods to achieve long-distance quantum communication based on this quantum memory will be shown in the subsequent chapters.

2.5.2.1 The interaction of a single two-level system with a single-mode optical field

Let us consider the interaction between a single two-level system and a single-mode optical field with frequency ν_k. Suppose that the two-level system has the parity symmetry. In the dipole approximation ($\boldsymbol{k}\cdot\boldsymbol{r} \ll 1$), the Hamiltonian of the combined system is [69, 70] described by

$$\hat{H} = \hat{H}_{\rm field} + \hat{H}_{\rm two-level} + \hat{H}_{\rm int}, \tag{2.125}$$

$$\hat{H}_{\rm field} = \hbar\nu_k \left(\hat{a}_{\boldsymbol{k}s}^\dagger \hat{a}_{\boldsymbol{k}s} + \frac{1}{2}\right), \tag{2.126}$$

$$\hat{H}_{\rm two-level} = E_e|e\rangle\langle e| + E_g|g\rangle\langle g|, \tag{2.127}$$

$$\hat{H}_{\rm int} = -q\hat{\boldsymbol{r}}\cdot\hat{\boldsymbol{E}}_{\boldsymbol{k}s}(\boldsymbol{0}), \tag{2.128}$$

where $\hat{\boldsymbol{E}}_{\boldsymbol{k}s}(\boldsymbol{0})$ is the electric field at the origin, $q\hat{\boldsymbol{r}}$ is the dipole moment, E_e and $E_g(< E_e)$ are the eigenvalues of $\hat{H}_{\rm two-level}$, and $|e\rangle$ and $|g\rangle$ are the eigenstates of $\hat{H}_{\rm two-level}$. From Eq. (2.56), $\hat{H}_{\rm int}$ can be rewritten as

$$\begin{aligned}\hat{H}_{\rm int} =& (|e\rangle\langle e| + |g\rangle\langle g|)(-q\hat{\boldsymbol{r}}\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s}\mathcal{E}_{\boldsymbol{k}})(|e\rangle\langle e| + |g\rangle\langle g|)(\hat{a}_{\boldsymbol{k}s} + \hat{a}_{\boldsymbol{k}s}^\dagger)\\ =& [(-q\mathcal{E}_{\boldsymbol{k}}\langle e|\hat{\boldsymbol{r}}|g\rangle\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s})\hat{\sigma}_+ + (-q\mathcal{E}_{\boldsymbol{k}}\langle g|\hat{\boldsymbol{r}}|e\rangle\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s})\hat{\sigma}_-](\hat{a}_{\boldsymbol{k}s} + \hat{a}_{\boldsymbol{k}s}^\dagger)\end{aligned} \tag{2.129}$$

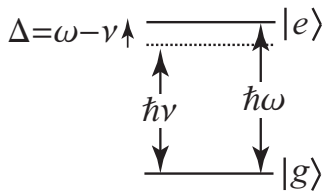

Fig. 2.9. A single two-level system. ν is the frequency of a single-mode optical field and $\hbar\omega$ is the difference between energies of $|e\rangle$ and $|g\rangle$.

where we define $\hat{\sigma}_+ := |e\rangle\langle g|$ and $\hat{\sigma}_- := |g\rangle\langle e|$, and we used $\langle g|\hat{\boldsymbol{r}}|g\rangle = \langle e|\hat{\boldsymbol{r}}|e\rangle = 0$ from the parity symmetry of the eigenstates $\{|e\rangle, |g\rangle\}$. Since the terms $\hat{\sigma}_+\hat{a}^\dagger_{\boldsymbol{k}s}$ and $\hat{\sigma}_-\hat{a}_{\boldsymbol{k}s}$ represent processes that do not conserve energy, they are eliminated in the rotating wave approximation. Thus, the interaction Hamiltonian $\hat{H}_{\rm int}$ can be approximately reduced to

$$\begin{aligned}\hat{H}_{\rm int} \simeq& [(-q\mathcal{E}_{\boldsymbol{k}}\langle e|\hat{\boldsymbol{r}}|g\rangle\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s})\hat{a}_{\boldsymbol{k}s}\hat{\sigma}_+ + (-q\mathcal{E}_{\boldsymbol{k}}\langle g|\hat{\boldsymbol{r}}|e\rangle\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s})\hat{a}^\dagger_{\boldsymbol{k}s}\hat{\sigma}_-] \\ =& \frac{\hbar\Omega}{2}(\hat{a}_{\boldsymbol{k}s}e^{i\phi}\hat{\sigma}_+ + \hat{a}^\dagger_{\boldsymbol{k}s}e^{-i\phi}\hat{\sigma}_-),\end{aligned} \tag{2.130}$$

where $\hbar\Omega/2 := |-q\mathcal{E}_{\boldsymbol{k}}\langle e|\hat{\boldsymbol{r}}|g\rangle\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s}|$ and $\phi := \arg[-q\mathcal{E}_{\boldsymbol{k}}\langle e|\hat{\boldsymbol{r}}|g\rangle\cdot\boldsymbol{\epsilon}_{\boldsymbol{k}s}]$. The frequency Ω is called *Rabi frequency*. By defining $\hat{a} =: \hat{a}_{\boldsymbol{k}s}e^{i\phi}$, $\nu := \nu_k$, and $\hbar\omega := E_e - E_g$ for the simplicity, the total Hamiltonian $\hat{H}$ is reduced into *Jaynes-Cummings Hamiltonian* $\hat{H}_{\rm JC}$ such that

$$\hat{H} - \frac{E_e+E_g}{2} - \frac{\hbar\nu}{2} \simeq \hat{H}_{\rm JC} := \hbar\nu\hat{a}^\dagger\hat{a} + \frac{\hbar\omega}{2}\hat{\sigma}_z + \frac{\hbar\Omega}{2}(\hat{a}\hat{\sigma}_+ + \hat{a}^\dagger\hat{\sigma}_-) =: \hat{H}_0 + \hat{H}_1, \tag{2.131}$$

$$\hat{H}_0 = \frac{\hbar\nu}{2}\hat{\sigma}_z + \hbar\nu\hat{a}^\dagger\hat{a}, \tag{2.132}$$

$$\hat{H}_1 = \frac{\hbar\Delta}{2}\hat{\sigma}_z + \frac{\hbar\Omega}{2}(\hat{a}\hat{\sigma}_+ + \hat{a}^\dagger\hat{\sigma}_-), \tag{2.133}$$

where $\hat{\sigma}_z := |e\rangle\langle e| - |g\rangle\langle g|$ and $\Delta := \omega - \nu$.

Let us consider the spectral decomposition of the Jaynes-Cummings Hamiltonian $\hat{H}_{\rm JC}$. Let $\{|e\rangle|m\rangle, |g\rangle|n\rangle\}_{m,n=0,1,\ldots}$ be the eigenbasis of $\hat{H}_0$. Since

$$\hat{H}_0|e\rangle|m\rangle = \hbar\nu\left(\frac{1}{2}+m\right)|e\rangle|m\rangle, \tag{2.134}$$

$$\hat{H}_0|g\rangle|n\rangle = \hbar\nu\left(-\frac{1}{2}+n\right)|g\rangle|n\rangle, \tag{2.135}$$

states $|e\rangle|m\rangle$ and $|g\rangle|m+1\rangle$ with $m \geq 0$ have the same eigenvalue of Hamiltonian $\hat{H}_0$. On the other hand, noting $[\hat{\sigma}_z, \hat{\sigma}_\pm] = \pm 2\hat{\sigma}_\pm$, $[\hat{a}^\dagger\hat{a}, \hat{a}^\dagger] = \hat{a}^\dagger$ and $[\hat{a}^\dagger\hat{a}, \hat{a}] = -\hat{a}$, we have $[\hat{H}_0, \hat{H}_1] = 0$. This implies that, from Theorem 1.1, $\hat{H}_0$ and $\hat{H}_1$ are simultaneously diagonalizable. Hence, defining a projector $\hat{P}_m := |e\rangle\langle e| \otimes |m\rangle\langle m| + |g\rangle\langle g| \otimes |m+1\rangle\langle m+1|$ $(m \geq 0)$ – the projector on the eigenspace of eigenvalue $\hbar\nu(1/2+m)$ of $\hat{H}_0$, we can decompose $\hat{H}_0$ and $\hat{H}_1$ as

$$\hat{H}_0 = \sum_{m=0}^{\infty}\hbar\nu\left(\frac{1}{2}+m\right)\hat{P}_m - \frac{\hbar\nu}{2}|g\rangle\langle g| \otimes |0\rangle\langle 0|, \tag{2.136}$$

$$\hat{H}_1 = \sum_{m=0}^{\infty}\hat{P}_m\hat{H}_1\hat{P}_m + (|g\rangle\langle g| \otimes |0\rangle\langle 0|)\hat{H}_1(|g\rangle\langle g| \otimes |0\rangle\langle 0|). \tag{2.137}$$

Note $\langle g|\langle 0|\hat{H}_1|g\rangle|0\rangle = -\hbar\Delta/2$. Let us further diagonalize $\hat{P}_m\hat{H}_1\hat{P}_m$. From

$$\hat{H}_1|e\rangle|m\rangle = \frac{\hbar\Delta}{2}|e\rangle|m\rangle + \frac{\hbar\Omega\sqrt{m+1}}{2}|g\rangle|m+1\rangle, \tag{2.138}$$

$$\hat{H}_1|g\rangle|m+1\rangle = -\frac{\hbar\Delta}{2}|g\rangle|m+1\rangle + \frac{\hbar\Omega\sqrt{m+1}}{2}|e\rangle|m\rangle, \tag{2.139}$$

$\hat{P}_m\hat{H}_1\hat{P}_m$ can be viewed as a matrix described by

$$\begin{pmatrix} \langle e|\langle m|\hat{H}_1|e\rangle|m\rangle & \langle e|\langle m|\hat{H}_1|g\rangle|m+1\rangle \\ \langle g|\langle m+1|\hat{H}_1|e\rangle|m\rangle & \langle g|\langle m+1|\hat{H}_1|g\rangle|m+1\rangle \end{pmatrix}$$
$$= \lambda_m \left[\cos\theta_m \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \sin\theta_m \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right], \tag{2.140}$$

where

$$\begin{aligned} \lambda_m &:= \sqrt{\left(\frac{\hbar\Delta}{2}\right)^2 + \left(\frac{\hbar\Omega\sqrt{m+1}}{2}\right)^2}, \\ \cos\theta_m &:= \frac{\hbar\Delta}{2\lambda_m}, \\ \sin\theta_m &:= \frac{\hbar\Omega\sqrt{m+1}}{2\lambda_m}. \end{aligned} \tag{2.141}$$

Hence, the eigenvalues of $\hat{P}_m\hat{H}_1\hat{P}_m$ are $\pm\lambda_m (=: \lambda_{m,\pm})$, and the corresponding eigenvectors are

$$|\lambda_{m,+}\rangle := \cos\left(\frac{\theta_m}{2}\right)|e\rangle|m\rangle + \sin\left(\frac{\theta_m}{2}\right)|g\rangle|m+1\rangle, \tag{2.142}$$

$$|\lambda_{m,-}\rangle := \sin\left(\frac{\theta_m}{2}\right)|e\rangle|m\rangle - \cos\left(\frac{\theta_m}{2}\right)|g\rangle|m+1\rangle, \tag{2.143}$$

which implies

$$\hat{P}_m\hat{H}_1\hat{P}_m = \lambda_m(|\lambda_{m,+}\rangle\langle\lambda_{m,+}| - |\lambda_{m,-}\rangle\langle\lambda_{m,-}|). \tag{2.144}$$

Therefore, the spectral decomposition of the total Hamiltonian $\hat{H}$ is

$$\begin{aligned} \hat{H}_{\rm JC} &= \hat{H}_0 + \hat{H}_1, \\ \hat{H}_0 &= \sum_{m=0}^{\infty} \hbar\nu\left(\frac{1}{2}+m\right)(|\lambda_{m,+}\rangle\langle\lambda_{m,+}| + |\lambda_{m,-}\rangle\langle\lambda_{m,-}|) - \frac{\hbar\nu}{2}|g\rangle\langle g|\otimes|0\rangle\langle 0|, \\ \hat{H}_1 &= \sum_{m=0}^{\infty} \lambda_m(|\lambda_{m,+}\rangle\langle\lambda_{m,+}| - |\lambda_{m,-}\rangle\langle\lambda_{m,-}|) - \frac{\hbar\Delta}{2}|g\rangle\langle g|\otimes|0\rangle\langle 0|. \end{aligned} \tag{2.145}$$

Time evolution of the system with the Hamiltonian $\hat{H}$ is determined by

$$|\psi(t)\rangle = e^{-i\hat{H}_{\rm JC}t/\hbar}|\psi(0)\rangle, \tag{2.146}$$

where $|\psi(0)\rangle$ is the initial state of the system, and $|\psi(t)\rangle$ is the final state of the system. From

the decomposition in Eq. (2.145), the final state $|\psi(t)\rangle$ is described by

$$\begin{aligned}|\psi(t)\rangle =& e^{-i\hat{H}_{\rm JC}t/\hbar}|\psi(0)\rangle \\ =& \sum_{m=0}^{\infty} e^{-i(\hbar\nu/2+m\hbar\nu+\lambda_m)t/\hbar}\langle\lambda_{m,+}|\psi(0)\rangle|\lambda_{m,+}\rangle + \sum_{m=0}^{\infty} e^{-i(\hbar\nu/2+m\hbar\nu-\lambda_m)t/\hbar}\langle\lambda_{m,-}|\psi(0)\rangle|\lambda_{m,-}\rangle \\ & + e^{-i\omega t/2}\langle g|\langle 0||\psi(0)\rangle|g\rangle|0\rangle.\end{aligned} \tag{2.147}$$

This is the solution of the Schrödinger equation.

Let us consider the solution of the off-resonant case, i.e., $|\Delta| \gg \Omega$. In this case, since

$$\begin{aligned}\lambda_m &\simeq \frac{\hbar|\Delta|}{2} + \frac{\hbar\Omega^2(m+1)}{4|\Delta|}, \\ |\lambda_{m,+}\rangle &\simeq \begin{cases} |e\rangle|m\rangle, & (\Delta \geq 0), \\ |g\rangle|m+1\rangle, & (\Delta < 0), \end{cases} \\ |\lambda_{m,-}\rangle &\simeq \begin{cases} |g\rangle|m+1\rangle, & (\Delta \geq 0), \\ |e\rangle|m\rangle, & (\Delta < 0), \end{cases}\end{aligned} \tag{2.148}$$

hold, we have

$$\begin{aligned}\hat{H}_1 \simeq& \sum_{m=0}^{\infty}\left(\frac{\hbar\Delta}{2} + \frac{\hbar\Omega^2(m+1)}{4\Delta}\right)(|e\rangle\langle e|\otimes|m\rangle\langle m| - |g\rangle\langle g|\otimes|m+1\rangle\langle m+1|) - \frac{\hbar\Delta}{2}|g\rangle\langle g|\otimes|0\rangle\langle 0| \\ =& \frac{\hbar\Omega^2}{8\Delta} + \left(\frac{\hbar\Delta}{2} + \frac{\hbar\Omega^2}{8\Delta}\right)\hat{\sigma}_z + \frac{\hbar\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}\hat{\sigma}_z.\end{aligned} \tag{2.149}$$

This indicates

$$\hat{H}_{\rm JC} \simeq \frac{\hbar\Omega^2}{8\Delta} + \hbar\nu\hat{a}^\dagger\hat{a} + \left(\frac{\hbar\omega}{2} + \frac{\hbar\Omega^2}{8\Delta}\right)\hat{\sigma}_z + \frac{\hbar\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}\hat{\sigma}_z. \tag{2.150}$$

Therefore, the solution of the Schrödinger equation is

$$|\psi(t)\rangle = e^{-i\nu\hat{a}^\dagger\hat{a}t}e^{-i(\frac{\omega}{2}+\frac{\Omega^2}{8\Delta})\hat{\sigma}_z t}e^{-i\frac{\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}\hat{\sigma}_z t}|\psi(0)\rangle. \tag{2.151}$$

In the following chapters, one can see that this interaction plays a central role of long-distance quantum communication.

In contrast to the on-resonant interaction ($\Delta = 0$), the off-resonant interaction ($|\Delta| \gg \Omega$) does not restrict the frequency ν of the single-mode electromagnetic field. This implies that the off-resonant interaction can be observed in various two-level quantum systems [40, 41, 42, 44, 45]. Hence, the off-resonant interaction of Eq. (2.151) can be considered to be a universal interaction between a two-level system and a single-mode optical field.

2.5.2.2 The interaction between Λ-type system and a single-mode optical field

As seen in the previous section, we see the interaction between a single two-level system composed of states $\{|e\rangle, |g\rangle\}$ and a single-mode optical field. Actually, it is not good to use the two-level system as a quantum memory, because the system suffers from the spontaneous emission turning state $|e\rangle$ into state $|g\rangle$. Instead of the two-level system, it is known to be better to use a three-level system called Λ-*type system* as a quantum memory.

The Λ-type system is composed of three states $\{|0\rangle, |1\rangle, |e\rangle\}$ as in Fig. 2.10. This system is

supposed to have a selection rule that prohibits the dipole transition $|0\rangle \leftrightarrow |1\rangle$. But the system allows us to induce dipole transitions $|0\rangle \leftrightarrow |e\rangle$ and $|1\rangle \leftrightarrow |e\rangle$ by proper electromagnetic fields. The selection rule releases the states $|0\rangle$ and $|1\rangle$ from the noise caused by the spontaneous emission, which implies that the states $|0\rangle$ and $|1\rangle$ are stable enough to be used as the computational basis of a quantum memory. In addition, we can apply unitary operations on the qubit by *Raman processes* [69, 70, 71]. The Raman processes are induced by two electromagnetic fields whose frequency difference $\nu_0 - v_1$ matches the separation of the two ground states, $(E_1 - E_0)/\hbar$ (see Fig. 2.10), and whose frequencies ν_0 and ν_1 are sufficiently detuned from the resonances of the transitions $|0\rangle \leftrightarrow |e\rangle$ and $|1\rangle \leftrightarrow |e\rangle$, respectively. Therefore, the Λ-type systems are good candidates for quantum memories.

Moreover, such a quantum memory based on the Λ-type system can couple with a single-mode optical field [40, 41, 42, 44]. For coupling a single-mode optical field with the quantum memory, it is sufficient to apply a single-mode optical field with an off-resonance frequency ν_0. In this case, since the field can activate only the transition $|0\rangle \leftrightarrow |e\rangle$, this process is essentially considered to be the off-resonant interaction between two levels of $|0\rangle$ and $|e\rangle$ and the field. Thus, from the consideration in the previous section (e.g., from Eq. (2.150)), the total Hamiltonian of the system is approximately described by

$$\hat{H} - \frac{\hbar\nu}{2} \simeq \hat{H}_0 + \hat{H}_{\rm JC}, \tag{2.152}$$

$$\hat{H}_0 = E_1|1\rangle\langle 1| + \frac{E_e + E_0}{2}(|e\rangle\langle e| + |0\rangle\langle 0|), \tag{2.153}$$

$$\hat{H}_{\rm JC} \simeq \frac{\hbar\Omega^2}{8\Delta}(|e\rangle\langle e| + |0\rangle\langle 0|) + \hbar\nu\hat{a}^\dagger\hat{a} + \left(\frac{\hbar\omega}{2} + \frac{\hbar\Omega^2}{8\Delta}\right)\hat{\sigma}_z + \frac{\hbar\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}\hat{\sigma}_z, \tag{2.154}$$

where

$$\omega := (E_e - E_0)/\hbar, \tag{2.155}$$

$$\Delta := \omega - \nu_0, \tag{2.156}$$

$$\hat{\sigma}_z := |e\rangle\langle e| - |0\rangle\langle 0|. \tag{2.157}$$

Note that $\hat{H}_0$ and $\hat{H}_{\rm JC}$ are commute. We further note

$$\begin{aligned}
\hat{H}_0\hat{P}_{\rm qubit} =& E_1|1\rangle\langle 1| + \frac{E_e + E_0}{2}|0\rangle\langle 0|, \\
\hat{H}_{\rm JC}\hat{P}_{\rm qubit} \simeq& \frac{\hbar\Omega^2}{8\Delta}|0\rangle\langle 0| + \hbar\nu_0\hat{a}^\dagger\hat{a} - \left(\frac{\hbar\omega}{2} + \frac{\hbar\Omega^2}{8\Delta}\right)|0\rangle\langle 0| - \frac{\hbar\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}|0\rangle\langle 0| \\
=& \hbar\nu_0\hat{a}^\dagger\hat{a} - \frac{\hbar\omega}{2}|0\rangle\langle 0| - \frac{\hbar\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}|0\rangle\langle 0|
\end{aligned}$$

for projector $\hat{P}_{\rm qubit} := |0\rangle\langle 0| + |1\rangle\langle 1|$. Thus, the unitary operator $\hat{U}(t)$ at time t on the qubit represented by $\{|0\rangle, |1\rangle\}$ and on the single-mode optical field is given by

$$\hat{U}(t) := \hat{P}_{\rm qubit}e^{-i(\hat{H}_0 + \hat{H}_{\rm JC})t/\hbar}\hat{P}_{\rm qubit} = e^{-i\nu_0\hat{a}^\dagger\hat{a}t}e^{-i(E_0|0\rangle\langle 0| + E_1|1\rangle\langle 1|)t/\hbar}e^{i\frac{\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}|0\rangle\langle 0|t}. \tag{2.158}$$

The operators $e^{-i\nu_0\hat{a}^\dagger\hat{a}t}$ and $e^{-i(E_0|0\rangle\langle 0| + E_1|1\rangle\langle 1|)t/\hbar}$ can be offset by proper local unitary operations on the qubit and on the single-mode optical fields, which means that they cannot make coherent coupling between the systems. In contrast, $e^{i\frac{\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}|0\rangle\langle 0|t}$ is an essential unitary operation to

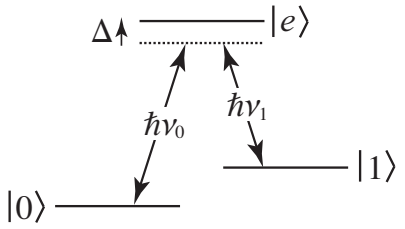

Fig. 2.10. Λ-type system. ν_0 and ν_1 are the frequencies of single-mode optical fields.

couple the systems. In fact, the unitary operation works as

$$\begin{aligned} e^{i\theta\hat{a}^\dagger\hat{a}|0\rangle\langle 0|}|0\rangle|\alpha\rangle &= |0\rangle|\alpha e^{i\theta}\rangle, \\ e^{i\theta\hat{a}^\dagger\hat{a}|0\rangle\langle 0|}|1\rangle|\alpha\rangle &= |1\rangle|\alpha\rangle, \end{aligned} \tag{2.159}$$

where $|\alpha\rangle$ is a coherent state of the optical field and $\theta := (\Omega^2 t)/(4\Delta)$, and hence, we can easily generate an entangled state in the form of

$$e^{i\theta\hat{a}^\dagger\hat{a}|0\rangle\langle 0|}(\sqrt{q_0}|0\rangle + \sqrt{q_1}|1\rangle)|\alpha\rangle = \sqrt{q_0}|0\rangle|\alpha e^{i\theta}\rangle + \sqrt{q_1}|1\rangle|\alpha\rangle \tag{2.160}$$

with $q_0 + q_1 = 1$ and $0 < q_0 < 1$. Hence, we can expect the unitary operator $e^{i\frac{\Omega^2}{4\Delta}\hat{a}^\dagger\hat{a}|0\rangle\langle 0|t}$ to play an important role in the coherent manipulation of the qubit. The importance of this unitary operation will be ensured in the subsequent chapters.

3

Entanglement generation based on a two-probe protocol

As seen in Sec. 2.5.1.5, the communication efficiency of quantum communication based on the direct transmission of photons decreases exponentially with the channel length. The goal in what follows is to avoid the exponential decrease of the communication efficiency, and to compose alternative architectures to achieve long-distance quantum communication efficiently. Although there are candidates of such architectures, e.g., quantum-repeater-based or satellite-based quantum communication, either ways are based on entanglement generation between distant quantum memories, and further execute entanglement distillation and entanglement swapping if necessary.

In this chapter, we provide an entanglement generation protocol between quantum memories by utilizing the off-resonant interaction in the form of†

$$\begin{aligned}\hat{U}_\theta(|0\rangle_M|\alpha\rangle_c) =& |0\rangle_M|\alpha e^{i\theta/2}\rangle_c,\\ \hat{U}_\theta(|1\rangle_M|\alpha\rangle_c) =& |1\rangle_M|\alpha e^{-i\theta/2}\rangle_c,\end{aligned} \tag{3.1}$$

where $\hat{U}_\theta$ is the unitary operator, $\{|j\rangle_M\}_{j=0,1}$ is the computational basis of the quantum memory M, $|\alpha\rangle_c$ is a coherent state, and the parameter θ depends on the strength of the interaction‡. The entanglement generation protocol is composed of a simple combination of linear optical elements and photon detectors, and it can generate entanglement with only one type of error, which is a favorable property that makes subsequent entanglement distillation efficient (see Fig. 2.5). In the case where ideal photon-number-resolving detectors are used, the performance of the protocol in terms of fidelity and efficiency exceeds all known protocols [37, 38, 40, 41, 42, 43] including a protocol generating entanglement with two types of errors [40, 41]. In fact, it is shown that the protocol achieves the theoretical limit of performance among the protocols with the single-error-type property. In addition, even if realistic photon detectors are used, the protocol shows higher performance than known realistic protocols. Thus, the protocol introduced here is a promising protocol for efficient production of entanglement.

3.1 Two-probe protocol

Let us consider the entanglement generation protocol illustrated in Fig. 3.1. In what follows, we call the sender and the receiver as Alice and Bob, respectively, who are connected via an optical fiber with transmittance $T = e^{-l/l_0}$, where l is the distance between the nodes. Alice first prepares a probe pulse in a coherent state $|\alpha\rangle_a$ with $\alpha \geq 0$ and a quantum memory A in

† Note that this unitary $\hat{U}_\theta$ is equivalent to the unitary operation of Eq. (2.159) up to a phase shifter on the optical field.
‡ According to Ref. [40], $\theta \sim 0.01$ is achievable.

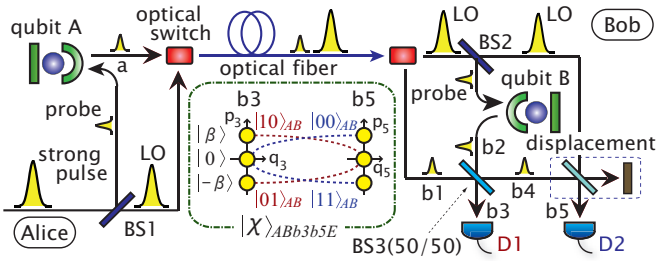

Fig. 3.1. Schematic diagram of the two-probe protocol.

state $(e^{-i(\xi+\zeta)}|0\rangle_A + e^{i(\xi+\zeta)}|1\rangle_A)/\sqrt{2}$ with

$$\begin{aligned}\zeta :=& (1/2)T\alpha^2 \sin\theta, \\ \xi :=& (1/2)(1-T)\alpha^2 \sin\theta,\end{aligned} \tag{3.2}$$

where phase factors ξ and ζ are chosen to offset irrelevant phases appearing later. Alice then makes the probe pulse interact with her memory by $\hat{U}_\theta$, and sends the output probe pulse to Bob through the fiber together with the local oscillator (LO). Optical loss in the fiber is effectively described by

$$\hat{N}|\alpha\rangle_a = |\sqrt{T}\alpha\rangle_{b_1}|\sqrt{1-T}\alpha\rangle_E, \tag{3.3}$$

where $\hat{N}$ is an isometry from input mode a into output mode b_1 and the environment E. Then, the state of Alice's memory A, the received probe pulse in mode b_1, and the environment E is described by

$$|\psi\rangle_{Ab_1E} = \frac{1}{\sqrt{2}}(|0\rangle_A|u_0\rangle_{b_1}|v_0\rangle_E + |1\rangle_A|u_1\rangle_{b_1}|v_1\rangle_E) \tag{3.4}$$

with

$$\begin{aligned}|u_j\rangle_{b_1} &:= e^{-i(-1)^j\zeta}|\sqrt{T}\alpha e^{i(-1)^j\theta/2}\rangle_{b_1} \\ |v_j\rangle_E &:= e^{-i(-1)^j\xi}|\sqrt{1-T}\alpha e^{i(-1)^j\theta/2}\rangle_E.\end{aligned} \tag{3.5}$$

The above recipe for Alice is also shared by the protocols in Refs. [40, 41, 42], while that for Bob is not. In these protocols, Bob first interacts the received probe pulse with his memory, and then he either performs homodyne measurement on the probe pulse (protocol I) [40, 41] or displaces the probe pulse and conducts photon counting (protocol II) [42]. As seen below, the protocol introduced here differs from these in the sense that it uses two probe pulses, which inherits the approach adopted by Duan *et al.* [31, 32, 33, 34, 37, 38]. Hence, in what follows, we call it *two-probe protocol*.

In the two-probe protocol, upon receiving the probe pulse and the LO pulse, Bob first generates a second probe pulse in state $|\sqrt{T}\alpha\rangle_{b_2}$ from the LO with a beam splitter (BS2), and then makes it interact with his memory initialized in state $(e^{-i\zeta}|0\rangle_B + e^{i\zeta}|1\rangle_B)/\sqrt{2}$. Then, his memory and the second probe pulse are in state $|\phi\rangle_{Bb_2} = (|0\rangle_B|u_0\rangle_{b_2} + |1\rangle_B|u_1\rangle_{b_2})/\sqrt{2}$. Bob further applies a 50/50 BS (BS3) described by $|\alpha_1\rangle_{b_1}|\alpha_2\rangle_{b_2} \to |(\alpha_2-\alpha_1)/\sqrt{2}\rangle_{b_3}|(\alpha_2+\alpha_1)/\sqrt{2}\rangle_{b_4}$ to the pulses in modes b_1 and b_2, which is followed by a phase-space displacement $\hat{D}_{-\sqrt{2T}\alpha\cos(\theta/2)}$ to the pulse in mode b_4. Note that the displacement operation is achieved by the combination of LO and a

beam splitter, as shown in Sec. 2.5.1.2. These operations correspond to the following isometry:

$$\begin{aligned}
|u_0\rangle_{b_1}|u_0\rangle_{b_2} &\to |0\rangle_{b_3}|\beta\rangle_{b_5}, \\
|u_0\rangle_{b_1}|u_1\rangle_{b_2} &\to |-\beta\rangle_{b_3}|0\rangle_{b_5}, \\
|u_1\rangle_{b_1}|u_0\rangle_{b_2} &\to |\beta\rangle_{b_3}|0\rangle_{b_5}, \\
|u_1\rangle_{b_1}|u_1\rangle_{b_2} &\to |0\rangle_{b_3}|-\beta\rangle_{b_5},
\end{aligned} \tag{3.6}$$

where $\beta := i\sqrt{2T}\alpha \sin(\theta/2)$. Then, the state of the total system is described by

$$\begin{aligned}
|\chi\rangle_{ABb_3b_5E} =& |0\rangle_{b_3}(|00\rangle_{AB}|\beta\rangle_{b_5}|v_0\rangle_E + |11\rangle_{AB}|-\beta\rangle_{b_5}|v_1\rangle_E)/2 \\
&+ |0\rangle_{b_5}(|01\rangle_{AB}|-\beta\rangle_{b_3}|v_0\rangle_E + |10\rangle_{AB}|\beta\rangle_{b_3}|v_1\rangle_E)/2.
\end{aligned} \tag{3.7}$$

The pulses in b_3 and b_5 go to photon detectors D1 and D2, respectively, and Bob announces the success of the protocol when either photon detector D1 or D2, but not both, reports the arrival of nonzero photons.

Let us consider the case where D1 and D2 are ideal photon number-resolving detectors. Since the detectors have no dark counts, the output state $|\chi\rangle_{ABb_3b_5E}$ never provokes an event where both detectors receive photons. Hence the two-probe protocol fails only when the pulses in modes b_3 and b_5 are in the vacuum state $|0\rangle_{b_3}|0\rangle_{b_5}$, which leads to the success probability of

$$P_s(\alpha) = 1 - ||_{b_3}\langle 0|_{b_5}\langle 0||\chi\rangle_{ABb_3b_5E}||^2 = 1 - e^{-2T\alpha^2 \sin^2(\theta/2)}. \tag{3.8}$$

The type of the generated entanglement in qubits AB depends on which detector informs how many photons have arrived. If detector D1 announces that the number of arriving photons is odd (even but nonzero), the generated entangled state has fidelity

$$F(\alpha) = (1 + e^{-2(1-T)\alpha^2 \sin^2(\theta/2)})/2 \tag{3.9}$$

to the nearest Bell state $|\Psi^-\rangle_{AB} := (|01\rangle_{AB} - |10\rangle_{AB})/\sqrt{2}$ ($|\Psi^+\rangle_{AB} := (|01\rangle_{AB} + |10\rangle_{AB})/\sqrt{2}$), and it is diagonalized by Bell states $\{|\Psi^\pm\rangle_{AB}\}$. Similarly, detector D2 informs whether the nearest Bell state to the obtained entanglement is $|\Phi^-\rangle_{AB} := (|00\rangle_{AB} - |11\rangle_{AB})/\sqrt{2}$ or $|\Phi^+\rangle_{AB} := (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$. These facts can be confirmed by simple calculations, e.g., ${}_{b_3}\langle n||\chi\rangle_{ABb_3b_5E} = |0\rangle_{b_5}(\langle n| - \beta\rangle|01\rangle_{AB}|v_0\rangle_E + \langle n|\beta\rangle|10\rangle_{AB}|v_1\rangle_E)/2$ for the number state $|n\rangle_{b_3}$ ($n > 0$), $\langle n|\beta\rangle = (-1)^n\langle n| - \beta\rangle$, and $\langle v_1|v_0\rangle = e^{-2(1-T)\alpha^2 \sin^2(\theta/2)}$. Then, using a local unitary operation depending on the outcome of the detectors, Alice and Bob can transform the generated entangled state into the standard state,

$$F(\alpha)|\Phi^+\rangle\langle\Phi^+|_{AB} + (1 - F(\alpha))|\Phi^-\rangle\langle\Phi^-|_{AB}. \tag{3.10}$$

Since this standard state includes only one type of error, from these states, we can efficiently distill a Bell pair according to Fig. 2.5. This property is also shared by protocol II [42] and by another protocol [43].

In order to evaluate the potential of the two-probe protocol, we compare its performance with protocols I and II in Fig. 3.2, assuming ideal photon number-resolving detectors and ideal homodyne detectors. The figure suggests that the two-probe protocol has the best performance among the protocols. In addition, the figure shows that, in the vicinity of zero success probability, protocol II and the two-probe protocol achieve a fidelity close to unity, while protocol I does not unless $T = 1$ ($l = 0$). This difference comes from the choice of different types of detectors, and it is further amplified with the increase of distance l: In fact, for $l \geq 40$ km, protocol I can generate almost separable states at best [42], but the two-probe protocol and protocol II can

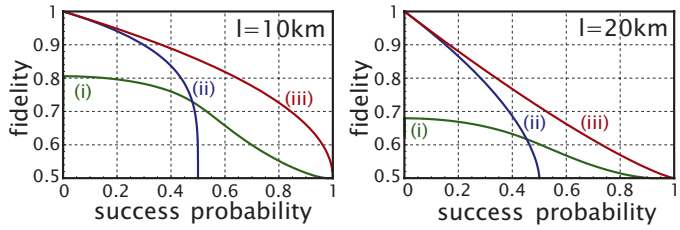

Fig. 3.2. The performance of protocols with ideal detectors: fidelity of the obtained entanglement to a Bell state as a function of the success probability when $l_0 = 25$ km (corresponding to ~ 0.17 dB/km attenuation) and $\theta = 0.01$, for (i) protocol I [40, 41], (ii) protocol II [42], and (iii) the two-probe protocol.

generate acceptable entanglement. The better performance of the two-probe protocol was also supported by numerical simulations for various values of T.

3.2 Optimality of the two-probe protocol

Actually, the high potential of the two-probe protocol is not accidental, because it can be shown to have the maximal performance among a wide range of protocols, which generate entangled states with only one type of error. The complete proof of this fact is somewhat complicated, and hence it is given in Chap. 4. Instead, in this section, we provide a preliminary result of it, namely we derive the upper bound of entanglement generation in qubits AB among all the protocols that satisfy the following two conditions:

(i) Alice prepares qubit A and pulse a in a state $(\sum_{j=0,1} e^{i\varphi_j}|j\rangle_A|\alpha_j\rangle_a)/\sqrt{2}$ with $\{|\alpha_j\rangle_a\}_{j=0,1}$ being arbitrary coherent states, and sends the pulse a to Bob;

(ii) Upon receiving the pulse (in mode b_1), Bob may perform arbitrary operations and measurements on b_1, the LO, and his memory qubit B, but whenever he declares success, Alice and Bob must be able to apply a local unitary operation $\hat{U}_A \otimes \hat{U}_B$ such that the final state of AB is represented only by $\{|\Phi^{\pm}\rangle\}$ (contained in the subspace spanned by $\{|\Phi^{\pm}\rangle\}$).

Condition (i) is satisfied by protocol I-III, and the others [37, 38, 40, 41, 42, 43]. In the proof to be given in Chap. 4, this condition will be omitted as an unnecessary assumption. Condition (ii) suggests that considered protocols generate entanglement with only one type of error, and it is met by protocols II and III.

Let us proceed to the proof. From condition (i), we see that the state of the system Ab_1E when the pulse arrives at Bob is written by

$$|\psi\rangle_{Ab_1E} = \sum_{j=0,1} |j\rangle_A|u_j\rangle_{b_1}|v_j\rangle_E/\sqrt{2} \tag{3.11}$$

with

$$(1-T)\ln|\langle u_1|u_0\rangle| = T\ln|\langle v_1|v_0\rangle|, \tag{3.12}$$

where T is the transmittance of the fiber. Since the cases with $|\langle v_1|v_0\rangle| = 1$ are trivial, we assume $|\langle v_1|v_0\rangle| < 1$ in what follows, and we use condition (ii) and Eq. (3.11) to derive bounds on the success probability P_s and the fidelity F in terms of $|\langle u_1|u_0\rangle|$ and $|\langle v_1|v_0\rangle|$. Then we use Eq. (3.12) to determine the achievable region of (P_s, F) for given T.

Let us define a phase flip channel Λ_A on qubit A by

$$\Lambda_A(\hat{\rho}) := q\hat{\rho} + (1-q)\hat{\sigma}_z^A \hat{\rho} \hat{\sigma}_z^A \tag{3.13}$$

with $\hat{\sigma}_z^A := |0\rangle\langle 0|_A - |1\rangle\langle 1|_A$ and

$$q := \frac{1 + |\langle v_1|v_0\rangle|}{2}. \tag{3.14}$$

From Eq. (3.11), we have

$$\mathrm{Tr}_E[|\psi\rangle\langle\psi|_{Ab_1E}] = \Lambda_A(|\psi'\rangle\langle\psi'|_{Ab_1}),$$

where $|\psi'\rangle_{Ab_1} := \sum_{j=0,1} e^{i(-1)^j\varphi}|j\rangle_A|u_j\rangle_{b_1}/\sqrt{2}$ with $2\varphi := \arg[\langle v_1|v_0\rangle]$. The effect of the lossy channel is thus equivalently described as preparation of $|\psi'\rangle_{Ab_1}$ followed by Λ_A. Since any operation of Bob commutes with Λ_A, the protocol is equivalent to the following sequence: (a) System Ab_1 is prepared in $|\psi'\rangle_{Ab_1}$; (b) Bob does his operations and measurements, and leaves system AB in a state $\hat{\rho}_{AB}$; (c) Λ_A is applied on qubit A.

Now condition (ii) requires that, whenever Bob declares success, there exists a unitary $\hat{U}_A \otimes \hat{U}_B$ such that $\langle\Psi'^{\pm}|\Lambda_A(\hat{\rho}_{AB})|\Psi'^{\pm}\rangle = 0$ with $|\Psi'^{\pm}\rangle_{AB} := \hat{U}_A^\dagger \otimes \hat{U}_B^\dagger|\Psi^{\pm}\rangle_{AB}$. Since $\hat{\rho}_{AB}$ is positive and $0 < q < 1$, we have

$$\begin{aligned} \sqrt{\hat{\rho}_{AB}}|\Psi'^{\pm}\rangle &= 0, \\ \sqrt{\hat{\rho}_{AB}}\hat{\sigma}_z^A|\Psi'^{\pm}\rangle &= 0 \end{aligned} \tag{3.15}$$

for both $\pm$. Adding and subtracting these equations, we obtain

$$\sqrt{\hat{\rho}_{AB}}|x_j\rangle_A|y_{j\oplus 1}\rangle_B = \sqrt{\hat{\rho}_{AB}}\hat{\sigma}_z^A|x_j\rangle_A|y_{j\oplus 1}\rangle_B = 0 \tag{3.16}$$

for $j = 0, 1$, where

$$\begin{aligned} |x_j\rangle_A &:= \hat{U}_A^\dagger|j\rangle_A \\ |y_j\rangle_B &:= \hat{U}_B^\dagger|j\rangle_B. \end{aligned} \tag{3.17}$$

Since $\hat{\rho}_{AB} \neq 0$, the set $\{|x_j\rangle_A|y_{j\oplus 1}\rangle_B, \hat{\sigma}_z^A|x_j\rangle_A|y_{j\oplus 1}\rangle_B\}_{j=0,1}$ must be linearly dependent, which only happens when $\{|x_j\rangle_A\}_{j=0,1}$ is an eigenbasis of $\hat{\sigma}_z^A$.

Without loss of generality, the fidelity F of the final state is given by

$$F = \langle\Phi'^{+}|\Lambda_A(\hat{\rho}_{AB})|\Phi'^{+}\rangle, \tag{3.18}$$

where $|\Phi'^{\pm}\rangle_{AB} := \hat{U}_A^\dagger \otimes \hat{U}_B^\dagger|\Phi^{\pm}\rangle_{AB} = (|x_0\rangle_A|y_0\rangle_B \pm |x_1\rangle_A|y_1\rangle_B)/\sqrt{2}$. Since $\{|x_j\rangle_A\}_{j=0,1}$ is an eigenbasis of $\hat{\sigma}_z^A$, we have $\hat{\sigma}_z^A|\Phi'^{+}\rangle = \pm|\Phi'^{-}\rangle$. Hence $F = q\langle\Phi'^{+}|\hat{\rho}_{AB}|\Phi'^{+}\rangle + (1-q)\langle\Phi'^{-}|\hat{\rho}_{AB}|\Phi'^{-}\rangle$, leading to

$$F \leq (1 + |\langle v_1|v_0\rangle|)/2 \tag{3.19}$$

from Eq. (3.14).

In order to find a bound on P_s, imagine a situation where, after the steps (a)–(c) above, Alice and Bob proceeds as follows: (d) Bob measures qubit B on basis $\{|y_k\rangle_B\}_{k=0,1}$; (e) Alice measures qubit A on basis $\{|j\rangle_A\}_{j=0,1}$. Whenever Bob has declared success, we see from Eq. (3.16) that the state of qubit A after step (d) should be $|x_k\rangle_A$, which is an eigenvector of $\hat{\sigma}_z^A$. Hence Bob can certainly predict Alice's outcome j in step (e). Now if we look at the whole sequence (a)–(e), we notice that Alice's measurement (e) can be equivalently done just after (a), and (c) becomes redundant. Then, when Alice finishes steps (a) and (e), Bob is provided with $\{|u_j\rangle_{b_1}\}_{j=0,1}$ with

equal *a priori* probabilities, from which he proceeds with steps (b) and (d). At this point, he can determine the value of j precisely whenever he declares success. Thus, the total success probability P_s is not larger than that of the unambiguous state discrimination (USD), which is $1-|\langle u_1|u_0\rangle|$ from Eq. (1.103). Hence we have

$$P_s \leq 1-|\langle u_1|u_0\rangle|. \tag{3.20}$$

Combining Eqs. (3.12), (3.19), and (3.20), we conclude that, for given $T<1$, the performance (P_s, F) of any protocol satisfying conditions (i) and (ii) must lie within the boundary $\{(1-t, (1+t^{(1-T)/T})/2) \mid 0 \leq t \leq 1\}$. Conversely, as Eqs. (3.8)-(3.9) suggest, this boundary is always achievable by the two-probe protocol with the choice of amplitude α satisfying $t = e^{-2T\alpha^2\sin^2(\theta/2)}$.

3.3 The performance of the two-probe protocol with realistic photon detectors

Here we show that the two-probe protocol shows high performance even if we replace the photon number-resolving detectors with threshold detectors (TDs) that just report the arrival of photons and do not tell how many of them have arrived. We represent quantum efficiency and mean dark count of the detector as η and ν, respectively. From Sec. 2.5.1.4, the function of a TD is represented by the following POVM elements:

$$\begin{aligned}\hat{E}_{\rm nc} =& \sum_{m=0}^{\infty} e^{-\nu}(1-\eta)^m |m\rangle\langle m|,\\ \hat{E}_{\rm c} =& \hat{I}-\hat{E}_{\rm nc},\end{aligned} \tag{3.21}$$

where $\hat{E}_{\rm c}$ ($\hat{E}_{\rm nc}$) corresponds to an event reporting the arrival (non-arrival) of photons. When the used TDs are ideal ($\eta=1$, $\nu=0$), the generated state has only one type of error and has fidelity $(1+e^{-2\alpha^2\sin^2(\theta/2)})/2$ to the nearest Bell state. The success probability is the same as that with ideal photon number-resolving detectors. For the realistic values of (η,ν), the success probability and the fidelity are described by

$$\begin{aligned}P_s(\eta,\nu,\alpha) =& e^{-\nu-2T\eta\alpha^2\sin^2(\theta/2)}[1-2e^{-\nu}+e^{2T\eta\alpha^2\sin^2(\theta/2)}],\\ F(\eta,\nu,\alpha) =& \frac{e^{-2\nu}e^{-2T\alpha^2\sin^2(\theta/2)}}{2P_s(\eta,\nu,\alpha)}[e^{2T(1-\eta)\alpha^2\sin^2(\theta/2)}(e^{\nu}e^{2T\eta\alpha^2\sin^2(\theta/2)}-1)\\ &- e^{-2(1-T)\alpha^2\sin^2(\theta/2)}e^{-2T(1-\eta)\alpha^2\sin^2(\theta/2)}(e^{\nu}e^{-2T\eta\alpha^2\sin^2(\theta/2)}-1)].\end{aligned} \tag{3.22}$$

We show numerically estimated performance $(P_s(\eta,\nu,\alpha), F(\eta,\nu,\alpha))$ of the two-probe protocol in Fig. 3.3. Note that the chosen values (η,ν) are typical for currently available detectors, e.g., TES (superconducting transition-edge sensors) [72] and APD (avalanche photodiode) [73]. The dark counts of such detectors increase the types of errors occurring in generated entanglement. However, such additional errors occur with a small probability $\sim \nu(P_s^{-1}-1)+\mathcal{O}(\nu^2)$, and hence can be neglected. To evaluate the performance of the two-probe protocol, we also plotted the performance of protocol I with an ideal homodyne detector, and that of protocol II with its photon number-resolving detector replaced by TD1 and TD2. The figure shows that the two-probe protocol has higher efficiency than protocol II. We see that there is a region where the performance of protocol I exceeds that of ours, but this region decreases with the increase of distance l. Hence, we can safely say that the two-probe protocol outperforms the other protocols in the cases where long-distance and/or high quality entanglement generation is required. It is

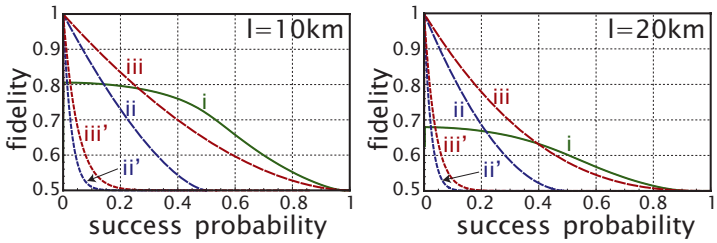

Fig. 3.3. The performance of protocols with realistic detectors: (i) protocol I with an ideal homodyne detector, (ii) protocol II with a TD1 ($\eta = 0.89,\ \nu = 1.4 \times 10^{-6}$), (ii') protocol II with a TD2 ($\eta = 0.12,\ \nu = 3.2 \times 10^{-7}$), (iii) the two-probe protocol with TD1s, (iii') the two-probe protocol with TD2s.

also worth to mention that entanglement generated by protocol I always includes two types of non-negligible errors, which will affect its performance in the entanglement distillation stage.

3.4 Summary

In conclusion, we have proposed a two-probe entanglement generation scheme, which outperforms the generation schemes proposed so far. More importantly, as shown in this chapter, the two-probe protocol can achieve the optimal performance among all the schemes satisfying a couple of plausible conditions [(i) and (ii) above]. Actually, the optimality can be ensured even if we omit physically meaningless condition (i) (see the next chapter). Therefore, the two-probe protocol is not only a feasible and efficient entanglement generation protocol but also a fundamental protocol enlightening us a quantum mechanical limit of single-error-type entanglement generation. The distinguished importance of the protocol will be also authenticated with its striking applications given in Chapters 5 and 6.

4

Tight bound on coherent-state-based entanglement generation over lossy channels

In Chapter 3, we have provided a protocol that can generate entanglement with only one type of error by using a unitary operator $\hat{V}$ in the form of

$$\begin{aligned} \hat{V}|0\rangle_A|\alpha\rangle_a &= |0\rangle_A|\alpha_0\rangle_a, \\ \hat{V}|1\rangle_A|\alpha\rangle_a &= |1\rangle_A|\alpha_1\rangle_a, \end{aligned} \tag{4.1}$$

where A is a qubit, a is a single-mode optical field, and $|\alpha\rangle_a$ and $\{|\alpha_j\rangle_a\}_{j=0,1}$ are coherent states. As in Fig. 2.5, we can efficiently distill an almost maximally entangled pair from the single-error-type entangled states. Thus, protocols producing entanglement with only one type of error are favorable for rendering the total performance of quantum communication efficient. In this chapter, considering a general paradigm of single-error-type entanglement generation in which, through a lossy channel, a sender sends the receiver an optical field entangled with sender's qubit by interaction $\hat{V}$, we derive the tight upper bound on the performances of these protocols stated in terms of the average singlet fraction of generated entanglement and the success probability. This derived bound is determined only by the channel loss, i.e., the length of the channel, which clarifies how the loss in the channel affects the entanglement generation in a quantitative way. In order to derive the bound, we require no additional assumption, differently from Sec. 3.2, where the quantum memory of the sender is additionally assumed to start from a symmetric state $(|0\rangle_A + |1\rangle_A)/\sqrt{2}$. Moreover, the general bound is shown to be achievable by utilizing the *symmetric protocol*† in Sec. 3.1 that is realizable by linear optical elements and photon-number-resolving detectors, and starts with the symmetric state $(|0\rangle_A + |1\rangle_A)/\sqrt{2}$.

This chapter is organized as follows. In Sec. 4.1, we define protocols to generate entanglement with only one type of error, and the measure of the performance. We derive an upper bound on those performances in Sec. 4.2, which is the main theorem in this chapter. In Sec. 4.3, we show that the upper bound is achievable by convex combination of the symmetric protocol and a trivial protocol. In Sec. 4.4, we derive an explicit expression of the tight upper bound as a function of the transmittance of the channel loss.

4.1 Single-error-type entanglement generation and the measure of its performance

Let us define the family of single-error-type entanglement generation protocols. We require Alice and Bob to make an entangled state with only one type of error. More precisely, Alice and Bob

† In fact, the symmetric protocol was dubbed the two-probe protocol in Chapter 3 in order to distinguish it from the other entanglement generation protocols based on a single probe. But, in this chapter, because we do not care about the number of the used probe pulses, we rename the protocol in order to clarify the initial state of the memory of the sender.

are required to make qubits AB in an entangled state that can be transformed into a state contained in the subspace spanned by Bell states $\{|\Phi^{\pm}\rangle_{AB}\}$ via local unitary operations, where $|\Phi^{\pm}\rangle_{AB} := (|00\rangle_{AB} \pm |11\rangle_{AB})/\sqrt{2}$.

To generate such an entangled state, Alice and Bob execute the following steps (Fig. 4.1): (i) Alice prepares qubit A in her desired state $|\phi\rangle_A = \sum_{j=0,1} e^{i\Theta_j}\sqrt{q_j}|j\rangle_A$ with real parameters Θ_j, $q_j \geq 0$, and $\sum_j q_j = 1$, and she makes it interact with a pulse in a coherent state $|\alpha\rangle_a = e^{-|\alpha|^2/2}e^{\alpha\hat{a}^\dagger}|0\rangle_a$ via a unitary operation $\hat{V}$ of Eq. (4.1). (ii) Alice sends the pulse a to Bob, through a lossy channel described by an isometry

$$\hat{N}|\alpha\rangle_a = |\sqrt{T}\alpha\rangle_b|\sqrt{1-T}\alpha\rangle_E, \tag{4.2}$$

where $0 < T < 1$ is the transmittance of the channel and system E is the environment. (iii) Upon receiving the pulse in mode b, Bob may perform arbitrary operations and measurements involving pulse b and his memory qubit B, and declare success outcome k occurring with a probability p_k or failure. (iv) If Step (iii) succeeds, depending on the outcome k, Alice and Bob apply a local unitary operation $\hat{U}_k^A \otimes \hat{U}_k^B$ to the obtained state, in order to satisfy that the final state $\hat{\tau}_k^{AB}$ is contained in the subspace spanned by $\{|\Phi^{\pm}\rangle_{AB}\}$, and also that the nearest Bell state to the state $\hat{\tau}_k^{AB}$ is $|\Phi^{+}\rangle_{AB}$.

We evaluate the performance of the protocols by the total success probability,

$$P_s = \sum_k p_k, \tag{4.3}$$

and the averaged fidelity of the obtained entangled states

$$F = \frac{1}{P_s}\sum_k p_k F_k, \tag{4.4}$$

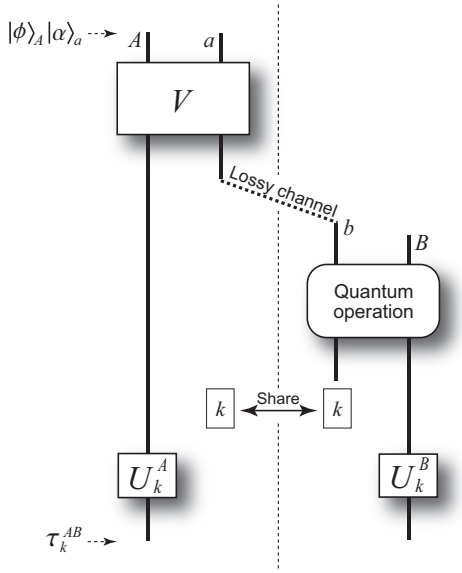

Fig. 4.1. The scenario of entanglement generation protocols. $|\phi\rangle_A := \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j}|j\rangle_A$. Bob's quantum operation returns qubit B in the state depending on outcome k, and he shares the outcome with Alice by using classical communication.

where F_k is

$$F_k := \langle \Phi^+ | \hat{\tau}_k^{AB} | \Phi^+ \rangle. \tag{4.5}$$

Thanks to the choice of the unitary operation in Step (iv), F_k is equivalent to so-called *singlet fraction* [64]. Since $\hat{\tau}_k^{AB}$ is contained in the subspace spanned by $\{|\Phi^{\pm}\rangle_{AB}\}$, $F_k \geq 1/2$ holds. This means

$$F \geq 1/2. \tag{4.6}$$

We also allow Alice and Bob to switch among two or more protocols probabilistically. The performance of such a mixed protocol is determined as follows. Suppose that Alice and Bob can execute a protocol with performance $(P_s^{(1)}, F^{(1)})$ and a protocol with performance $(P_s^{(2)}, F^{(2)})$. Then, by choosing these protocols with probabilities $\{r, 1-r\}$, Alice and Bob can achieve performance (P_s', F') determined by

$$\begin{pmatrix} P_s' \\ P_s' F' \end{pmatrix} = r \begin{pmatrix} P_s^{(1)} \\ P_s^{(1)} F^{(1)} \end{pmatrix} + (1-r) \begin{pmatrix} P_s^{(2)} \\ P_s^{(2)} F^{(2)} \end{pmatrix}. \tag{4.7}$$

It is thus convenient to describe the performance of a protocol by point $(P_s, P_s F)$. Then, the set of achievable points $(P_s, P_s F)$ forms a convex set.

4.2 An upper bound on the performance of a single-error-type entanglement generation protocol

We first introduce a protocol equivalent to the single-error-type entanglement generation protocol. Steps (i) and (ii) indicate that, when the pulse arrives at Bob, the state of the total system AbE is written in the form of

$$|\psi\rangle_{AbE} = \sum_{j=0,1} \sqrt{q_j} |j\rangle_A |u_j\rangle_b |v_j\rangle_E \tag{4.8}$$

with $0 \leq q_0 \leq 1$, $q_0 + q_1 = 1$, and

$$|\langle u_1 | u_0 \rangle|^{1-T} = |\langle v_1 | v_0 \rangle|^T > 0. \tag{4.9}$$

Let us define a phase flip channel Λ_A on qubit A by

$$\Lambda_A(\hat{\rho}) := f\hat{\rho} + (1-f)\hat{\sigma}_z^A \hat{\rho} \hat{\sigma}_z^A \tag{4.10}$$

with

$$f := \frac{1 + |\langle v_1 | v_0 \rangle|}{2} = \frac{1 + |\langle u_1 | u_0 \rangle|^{\frac{1-T}{T}}}{2} \tag{4.11}$$

and $\hat{\sigma}_z^A := |0\rangle\langle 0|_A - |1\rangle\langle 1|_A$. From Eqs. (4.8), (4.10), and (4.11), we have

$$\mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AbE}] = \Lambda_A(|\psi'\rangle\langle\psi'|_{Ab}), \tag{4.12}$$

where

$$|\psi'\rangle_{Ab} := \sum_{j=0,1} \sqrt{q_j} e^{i(-1)^j \varphi} |j\rangle_A |u_j\rangle_b \tag{4.13}$$

with $2\varphi := \arg[\langle v_1 | v_0 \rangle]$. The effect of the lossy channel is thus equivalently described as preparation of $|\psi'\rangle_{Ab}$ followed by Λ_A. Since any operation of Bob commutes with Λ_A, the protocol is

equivalent to the following sequence (Fig. 4.2): (1) System Ab is prepared in $|\psi'\rangle_{Ab}$; (2) Bob's successful measurement leaves system AB in a state $\hat{\rho}_k^{AB}$; (3) Λ_A is applied on qubit A.

In what follows, according to the equivalent protocol of Fig. 4.2, we show that, for fixed T and $|\langle u_1|u_0\rangle|$, the performance (P_s, P_sF) of an arbitrary protocol must be in the triangle with the apexes,

$$\begin{aligned} X_0 :=& (0,0), \\ X_1 :=& \left(1-|\langle u_1|u_0\rangle|, (1-|\langle u_1|u_0\rangle|)\frac{1+|\langle u_1|u_0\rangle|^{\frac{1-T}{T}}}{2}\right), \\ X_2 :=& (1, 1/2)\,. \end{aligned} \tag{4.14}$$

a) $|q_0 - q_1| = 1$ *or* $|\langle u_1|u_0\rangle| = 1$. In these cases, from Eq. (4.13), $|\psi'\rangle_{Ab}$ is a product state between system A and b. This implies that $\hat{\tau}_k^{AB}$ is a separable state, which means $F_k \leq 1/2$. From Eq. (4.6), $F = 1/2$. Thus, in this case, the performance (P_s, P_sF) of protocols must be on the segment X_0X_2.

b) $|q_0 - q_1| < 1$ *and* $|\langle u_1|u_0\rangle| < 1$. As stated in Step (iv), whenever Bob declares success outcome k, the state $\hat{\tau}_k^{AB}$ of their qubits satisfies

$$\langle\Psi^{\pm}|\hat{\tau}_k^{AB}|\Psi^{\pm}\rangle = \langle\Psi_k'^{\pm}|\Lambda_A(\hat{\rho}_k^{AB})|\Psi_k'^{\pm}\rangle = 0 \tag{4.15}$$

with $|\Psi_k'^{\pm}\rangle_{AB} := \hat{U}_k^{A\dagger} \otimes \hat{U}_k^{B\dagger}|\Psi^{\pm}\rangle_{AB} = (|x_k^0\rangle_A|y_k^1\rangle_B \pm |x_k^1\rangle_A|y_k^0\rangle_B)/\sqrt{2}$, $|\Psi^{\pm}\rangle_{AB} := (|01\rangle_{AB} \pm |10\rangle_{AB})/\sqrt{2}$, $|x_k^j\rangle_A := \hat{U}_k^{A\dagger}|j\rangle_A$, and $|y_k^j\rangle_B := \hat{U}_k^{B\dagger}|j\rangle_B$ $(j = 0, 1)$. Since $\hat{\rho}_k^{AB}$ is positive and

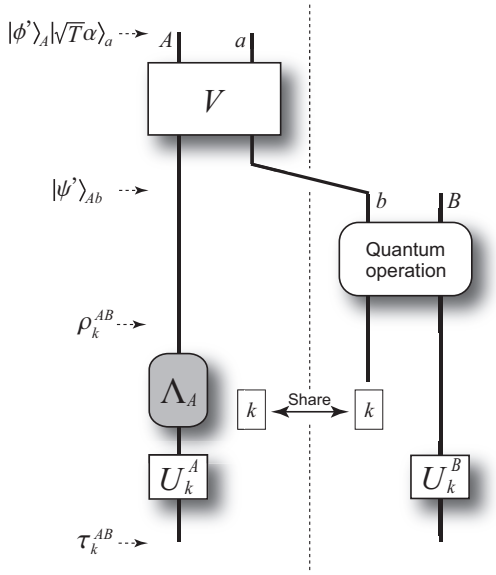

Fig. 4.2. An imaginary protocol equivalent to the real protocol in Fig. 1. $|\phi'\rangle_A := \sum_{j=0,1}\sqrt{q_j}e^{i\Theta_j+i(-1)^j\varphi}|j\rangle_A$. Channel $a \to b$ becomes ideal at the expense of the application of a phase-flip channel Λ_A.

$0 < f < 1$, Eq. (4.15) indicates

$$\sqrt{\hat{\rho}_k^{AB}}|\Psi_k'^{\pm}\rangle_{AB} = 0, \tag{4.16}$$

$$\sqrt{\hat{\rho}_k^{AB}}\hat{\sigma}_z^A|\Psi_k'^{\pm}\rangle_{AB} = 0, \tag{4.17}$$

for both $\pm$. Note that Eq. (4.16) implies

$$\hat{\rho}_k^{AB} = \frac{1+a_k}{2}|\Phi_k'^{+}\rangle\langle\Phi_k'^{+}|_{AB} + \frac{1-a_k}{2}|\Phi_k'^{-}\rangle\langle\Phi_k'^{-}|_{AB} + \frac{b_k}{2}|\Phi_k'^{+}\rangle\langle\Phi_k'^{-}|_{AB} + \frac{b_k^*}{2}|\Phi_k'^{-}\rangle\langle\Phi_k'^{+}|_{AB}, \tag{4.18}$$

where $|\Phi_k'^{\pm}\rangle_{AB} := \hat{U}_k^{A\dagger}\otimes\hat{U}_k^{B\dagger}|\Phi^{\pm}\rangle_{AB} = (|x_k^0\rangle_A|y_k^0\rangle_B \pm |x_k^1\rangle_A|y_k^1\rangle_B)/\sqrt{2}$, and the positivity of $\hat{\rho}_k^{AB}$ implies

$$a_k^2 + |b_k|^2 \leq 1. \tag{4.19}$$

Note that $0 \leq a_k \leq 1$ is satisfied by the choice of the unitary operation $\hat{U}_k^A \otimes \hat{U}_k^B$ in Step (iv). Adding and subtracting Eqs. (4.16) and (4.17), we obtain

$$\begin{aligned}\sqrt{\hat{\rho}_k^{AB}}|x_k^0\rangle_A|y_k^1\rangle_B &= \sqrt{\hat{\rho}_k^{AB}}\hat{\sigma}_z^A|x_k^0\rangle_A|y_k^1\rangle_B \\ &= \sqrt{\hat{\rho}_k^{AB}}|x_k^1\rangle_A|y_k^0\rangle_B = \sqrt{\hat{\rho}_k^{AB}}\hat{\sigma}_z^A|x_k^1\rangle_A|y_k^0\rangle_B = 0.\end{aligned} \tag{4.20}$$

Since $\hat{\rho}_k^{AB} \neq 0$, the four states, $|x_k^0\rangle_A|y_k^1\rangle_B$, $\hat{\sigma}_z^A|x_k^0\rangle_A|y_k^1\rangle_B$, $|x_k^1\rangle_A|y_k^0\rangle_B$, and $\hat{\sigma}_z^A|x_k^1\rangle_A|y_k^0\rangle_B$, must be linearly dependent, which only happens when $\{|x_k^j\rangle_A\}_{j=0,1}$ is a set of eigenvectors of $\hat{\sigma}_z^A$. Combining this fact with Eq. (4.18), we obtain

$$\hat{\rho}_k^A := \mathrm{Tr}_B[\hat{\rho}_k^{AB}] = \frac{\hat{1}^A + z_k\hat{\sigma}_z^A}{2}, \tag{4.21}$$

where $z_k := \pm\mathrm{Re}(b_k)$.

The fidelity F_k of the final state is given by $F_k = \langle\Phi^+|\hat{\tau}_k^{AB}|\Phi^+\rangle = \langle\Phi_k'^{+}|\Lambda_A(\hat{\rho}_k^{AB})|\Phi_k'^{+}\rangle$. Since $\{|x_k^j\rangle_A\}_{j=0,1}$ is an eigenbasis of $\hat{\sigma}_z^A$, we have $\hat{\sigma}_z^A|\Phi_k'^{+}\rangle = \pm|\Phi_k'^{-}\rangle$, which means $F_k = f\langle\Phi_k'^{+}|\hat{\rho}_k^{AB}|\Phi_k'^{+}\rangle + (1-f)\langle\Phi_k'^{-}|\hat{\rho}_k^{AB}|\Phi_k'^{-}\rangle$. From Eqs. (4.18) and (4.11), the fidelity F_k is rewritten as

$$F_k = \frac{1}{2}(1 + |\langle v_1|v_0\rangle|a_k). \tag{4.22}$$

Combining this equation, Eq. (4.19), and the definition of z_k, we have

$$\left(\frac{2F_k - 1}{|\langle v_1|v_0\rangle|}\right)^2 + z_k^2 \leq 1. \tag{4.23}$$

Let us consider the success probability of the protocol. Suppose that Bob's failure measurement returns a state $\hat{\rho}_f^{AB}$ with probability $1 - P_s$. Since Alice does nothing until the end of Bob's generalized measurement, Alice's averaged density operator is unchanged through the measurement, i.e.,

$$\hat{\psi}'^A = P_s\hat{\rho}_s^A + (1-P_s)\hat{\rho_f}^A, \tag{4.24}$$

where $\hat{\psi}'^A := \mathrm{Tr}_b[|\psi'\rangle\langle\psi'|_{Ab}]$, $\hat{\rho}_s^A := (\sum_k p_k\hat{\rho}_k^A)/P_s$ and $\hat{\rho_f}^A := \mathrm{Tr}_B[\hat{\rho_f}^{AB}]$. Eq. (4.13) indicates that $\hat{\psi}'^A$ is in the form of

$$\hat{\psi}'^A = \frac{\hat{1}^A + x_0\hat{\sigma}_x^A + y_0\hat{\sigma}_y^A + z_0\hat{\sigma}_z^A}{2}, \tag{4.25}$$

where $\hat{\sigma}_x^A := |0\rangle\langle 1|_A + |1\rangle\langle 0|_A$, $\hat{\sigma}_y^A := -i|0\rangle\langle 1|_A + i|1\rangle\langle 0|_A$, and x_0, y_0 and z_0 satisfy

$$\begin{aligned} z_0 &= q_0 - q_1, \\ x_0^2 + y_0^2 &= 4q_0q_1|\langle u_1|u_0\rangle|^2 = (1-z_0^2)|\langle u_1|u_0\rangle|^2. \end{aligned} \tag{4.26}$$

On the other hand, $\hat{\rho}_s^A$ is written as

$$\hat{\rho}_s^A = \frac{1}{P_s}\sum_k p_k\hat{\rho}_k^A = \frac{\hat{1} + z_s\hat{\sigma}_z^A}{2}, \tag{4.27}$$

where $z_s := (\sum_k p_k z_k)/P_s$, and it satisfies

$$\left(\frac{2F-1}{|\langle v_1|v_0\rangle|}\right)^2 + z_s^2 \leq 1 \tag{4.28}$$

from Eq. (4.23) and the convexity of function x^2. Note that this inequality implies

$$F \leq \frac{1+|\langle v_1|v_0\rangle|}{2} = \frac{1+|\langle u_1|u_0\rangle|^{\frac{1-T}{T}}}{2}, \tag{4.29}$$

where we used Eq. (4.9). We also decompose $\hat{\rho}_f^A$ as

$$\hat{\rho}_f^A = \frac{\hat{1}^A + x_f\hat{\sigma}_x^A + y_f\hat{\sigma}_y^A + z_f\hat{\sigma}_z^A}{2} \tag{4.30}$$

with real numbers x_f, y_f, z_f satisfying

$$x_f^2 + y_f^2 + z_f^2 \leq 1. \tag{4.31}$$

From Eq. (4.24), we have

$$\begin{aligned} x_0 &= (1-P_s)x_f, \\ y_0 &= (1-P_s)y_f, \\ z_0 &= P_s z_s + (1-P_s)z_f. \end{aligned} \tag{4.32}$$

From these equations, Eq. (4.26) and Eq. (4.31), we obtain

$$g(P_s) := P_s^2(1-z_s^2) - 2P_s(1-z_0z_s) + (1-|\langle u_1|u_0\rangle|^2)(1-z_0^2) \geq 0, \tag{4.33}$$

or equivalently, we have

$$\begin{aligned} &\left[(1-|\langle u_1|u_0\rangle|^2)z_0 - P_sz_s\right]^2 \\ &\leq \left[1-(1-z_s^2)|\langle u_1|u_0\rangle|^2\right]\left(P_s - \frac{1-|\langle u_1|u_0\rangle|^2}{1-|\langle u_1|u_0\rangle|\sqrt{1-z_s^2}}\right)\left(P_s - \frac{1-|\langle u_1|u_0\rangle|^2}{1+|\langle u_1|u_0\rangle|\sqrt{1-z_s^2}}\right). \end{aligned} \tag{4.34}$$

Since $z_0^2 < 1$ and $0 < |\langle u_1|u_0\rangle| < 1$, we have

$$g(1-|\langle u_1|u_0\rangle|^2) = -\left(1-|\langle u_1|u_0\rangle|^2\right)\left[\left(1-z_s^2\right)|\langle u_1|u_0\rangle|^2 + (z_0-z_s)^2\right] < 0, \tag{4.35}$$

and

$$g(1) = -\left(1-z_0^2\right)|\langle u_1|u_0\rangle|^2 - (z_0-z_s)^2 < 0, \tag{4.36}$$

which mean $g(P_s) < 0$ for $P_s \geq 1 - |\langle u_1|u_0\rangle|^2$ because $g(P_s)$ is linear or convex. Thus, Eq. (4.33) implies

$$P_s < 1 - |\langle u_1|u_0\rangle|^2. \tag{4.37}$$

To satisfy inequality (4.34), the right-hand side of the inequality should be nonnegative, which occurs only when

$$P_s \leq \frac{1 - |\langle u_1|u_0\rangle|^2}{1 + |\langle u_1|u_0\rangle|\sqrt{1 - z_s^2}} \tag{4.38}$$

under the condition of Eq. (4.37). Combining Eq. (4.28), we have

$$P_s \leq \frac{1 - |\langle u_1|u_0\rangle|^2}{1 + |\langle u_1|u_0\rangle| \left(\frac{2F-1}{|\langle v_1|v_0\rangle|}\right)}, \tag{4.39}$$

which can be rewritten as

$$\begin{aligned} P_sF \leq & \frac{1}{2}\left(1 - \frac{|\langle v_1|v_0\rangle|}{|\langle u_1|u_0\rangle|}\right) P_s + \frac{1}{2}(1 - |\langle u_1|u_0\rangle|^2)\frac{|\langle v_1|v_0\rangle|}{|\langle u_1|u_0\rangle|} & (4.40)\\ = & \frac{1}{2}\left(1 - |\langle u_1|u_0\rangle|^{\frac{1-2T}{T}}\right) P_s + \frac{1}{2}(1 - |\langle u_1|u_0\rangle|^2)|\langle u_1|u_0\rangle|^{\frac{1-2T}{T}}, & (4.41) \end{aligned}$$

where we used Eq. (4.9).

Since Eq. (4.6), Eq. (4.29), and Eq. (4.41) must be satisfied at the same time, the performance (P_s, P_sF) of an arbitrary protocol must be in the triangle with the apexes X_0, X_1, and

$$X_3 := \left(1 - |\langle u_1|u_0\rangle|^2, \frac{1}{2}(1 - |\langle u_1|u_0\rangle|^2)\right), \tag{4.42}$$

which is included in the triangle $X_0X_1X_2$. This completes the proof.

4.3 Simulatability of an arbitrary protocol via symmetric protocols

Here we show that the performance of an arbitrary protocol, which is in the triangle defined by Eq. (4.14) with fixed T and $|\langle u_1|u_0\rangle|$, is simulatable by utilizing the symmetric protocol in Sec. 3.1. In the protocol, Alice starts with preparing system A in a symmetric state $|\phi\rangle_A = (|0\rangle_A + |1\rangle_A)/\sqrt{2}$, and, upon receiving pulses from Alice, Bob carries out a measurement that is composed of a simple combination of linear optical elements and photon-number-resolving detectors. With a proper choice of the intensity of pulse a, the symmetric protocol can achieve (P_s, P_sF) with

$$\begin{aligned} P_s = & 1 - u, \\ F = & \frac{1 + u^{\frac{1-T}{T}}}{2}, \end{aligned} \tag{4.43}$$

for any u with $0 < u \leq 1$ (see Sec. 3.1). This indicates that the symmetric protocol can achieve performances $(P_s, P_sF) = X_0$ by choosing $u = 1$, and $(P_s, P_sF) = X_1$ by choosing $u = |\langle u_1|u_0\rangle|$. On the other hand, the performance $(P_s, P_sF) = X_2$ is also achievable by a trivial protocol in which Alice and Bob prepare their memories in state $|00\rangle_{AB}$ and declare success all the time. The achievability of points X_0, X_1, and X_2 indicates that all the points in the triangle $X_0X_1X_2$ are achievable by mixing. Since this fact holds for any $|\langle u_1|u_0\rangle|$, we conclude that, for given T,

the performance of an arbitrary protocol is simulatable by combining symmetric protocols and the trivial protocol.

4.4 Optimal performance of single-error-type entanglement generation

Here we calculate the optimal performance of the mixture of arbitrary single-error-type entanglement generation protocols for given T. As shown in the preceding section, for any T, the performance (P_s, P_sF) of an arbitrary protocol is achievable by mixing symmetric protocols and the trivial protocol. Since the performance achieved by a symmetric protocol or the trivial protocol can be described by a point $(P_s, P_sF) = (P_s, P_sF^{\rm sym}(P_s))$ with

$$F^{\rm sym}(P_s) := \frac{1+(1-P_s)^{\frac{1-T}{T}}}{2},\ (0 \le P_s \le 1), \tag{4.44}$$

the performance of the mixture of arbitrary protocols must be in the convex hull of the region $\mathcal{S} := \{(P_s, P_sF) \mid 0 \le P_s \le 1,\ 1/2 \le F \le F^{\rm sym}(P_s)\}$. In what follows, we show that the convex hull, $\mathrm{Conv}(\mathcal{S})$, is given by the region $\mathcal{C}_{\mathcal{S}} := \{(P_s, P_sF) \mid 0 \le P_s \le 1,\ 1/2 \le F \le F^{\rm opt}(P_s)\}$ with $F^{\rm opt}(P_s)$ defined by

$$F^{\rm opt}(P_s) := \begin{cases} \frac{1+(1-P_s)^{\frac{1-T}{T}}}{2}, & (P_s \le \frac{T}{1-T}), \\ \frac{1}{2} + \frac{1-P_s}{2P_s}\frac{T}{1-2T}\left(\frac{1-2T}{1-T}\right)^{\frac{1-T}{T}}, & (P_s > \frac{T}{1-T}). \end{cases} \tag{4.45}$$

Note that $P_s > T/(1-T)$ holds only when $T < 1/2$. The tight upper bound $F^{\rm opt}(P_s)$ is depicted in Fig. 4.3.

Let us proceed to the proof of $\mathcal{C}_{\mathcal{S}} = \mathrm{Conv}(\mathcal{S})$. From Eq. (4.44), we have

$$\frac{\mathrm{d}P_sF^{\rm sym}(P_s)}{\mathrm{d}P_s} = \frac{1}{2}\left[1 + \left(1-\frac{P_s}{T}\right)(1-P_s)^{\frac{1-2T}{T}}\right], \tag{4.46}$$

$$\frac{\mathrm{d}^2P_sF^{\rm sym}(P_s)}{\mathrm{d}{P_s}^2} = \frac{1}{2}\frac{1-T}{T}\left(\frac{P_s}{T}-2\right)(1-P_s)^{\frac{1-3T}{T}}. \tag{4.47}$$

The latter equation indicates

$$\begin{aligned} \frac{\mathrm{d}^2P_sF^{\rm sym}(P_s)}{\mathrm{d}{P_s}^2} &> 0,\ (P_s > 2T), \\ \frac{\mathrm{d}^2P_sF^{\rm sym}(P_s)}{\mathrm{d}{P_s}^2} &\le 0,\ (P_s \le 2T). \end{aligned} \tag{4.48}$$

a) $T \ge 1/2$. In this case, $F^{\rm opt}(P_s) = F^{\rm sym}(P_s)$, and hence $\mathcal{S} = \mathcal{C}_{\mathcal{S}}$. In addition, Eq. (4.48) indicates that $P_sF^{\rm sym}(P_s)$ is concave for $0 \le P_s \le 1$. These facts imply that $\mathrm{Conv}(\mathcal{S})$ is equivalent to $\mathcal{S}$, namely, to $\mathcal{C}_{\mathcal{S}}$.

b) $T < 1/2$. Let P_s^* be $P_s^* := T/(1-T)$. The proof begins with noting the following facts: (i) $F^{\rm opt}(P_s) = F^{\rm sym}(P_s)$ for $0 \le P_s < P_s^*$; (ii) $F^{\rm opt}(P_s^*) = F^{\rm sym}(P_s^*)$; (iii) $F^{\rm opt}(1) = F^{\rm sym}(1)$; (iv) $P_sF^{\rm opt}(P_s)$ and $(\mathrm{d}P_sF^{\rm opt}(P_s))/(\mathrm{d}P_s)$ are continuous at $P_s = P_s^*$; (v)

$$\frac{\mathrm{d}^2P_sF^{\rm opt}(P_s)}{\mathrm{d}{P_s}^2} \begin{cases} < 0, & (0 \le P_s < P_s^*), \\ = 0, & (P_s^* < P_s); \end{cases} \tag{4.49}$$

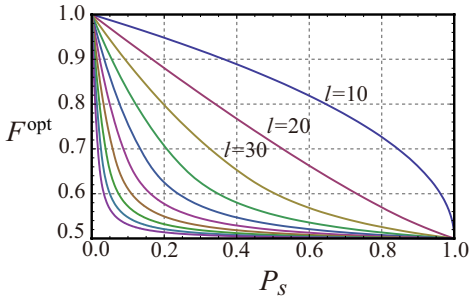

Fig. 4.3. The optimal performances of single-error-type entanglement generation for $10 \leq l \leq 100$ km at intervals of 10 km, where we assume $T = e^{-l/l_0}$ and $l_0 = 25$ km (corresponding to ~ 0.17 dB/km attenuation).

(vi) $F^{\rm opt}(P_s) > F^{\rm sym}(P_s)$ for $P_s^* < P_s < 1$. Facts (i)-(v) are easily confirmed from Eqs. (4.44)-(4.45). Fact (vi) is proven by facts (ii)-(iii),

$$\frac{{\rm d}P_s F^{\rm opt}(P_s^*)}{{\rm d}P_s} = \frac{{\rm d}P_s F^{\rm sym}(P_s^*)}{{\rm d}P_s}, \tag{4.50}$$

and by Eqs. (4.48)-(4.49). Facts (iv)-(v) show that $\mathcal{C}_{\mathcal{S}}$ is convex. Facts (i)-(iii) and (vi) imply $\mathcal{S} \subset \mathcal{C}_{\mathcal{S}}$. From facts (i)-(v), we have $\mathcal{C}_{\mathcal{S}} \subset {\rm Conv}(\mathcal{S})$. Therefore, we conclude ${\rm Conv}(\mathcal{S}) = \mathcal{C}_{\mathcal{S}}$.

4.5 Summary

In conclusion, we have provided the tight upper bound on the performances of protocols that generate entanglement with only one type of error by transmitting pulses in coherent states through a lossy channel. As represented by Eq. (4.45), the tight upper bound is stated in terms of the success probability P_s and the average singlet fraction F of generated entanglement, and is determined only by the transmittance T of the channel. In addition, we have shown that the upper bound is achievable without large-scale quantum operations, namely by utilizing the symmetric protocol composed of linear optical elements and photon-number-resolving detectors.

The arts enabling us to derive such a general bound can be summarized as follows. The proof begins with replacing the real protocol in Fig. 4.1 by an equivalent (virtual) protocol in Fig. 4.2. Thanks to the replacement, the effect of the optical loss in the practical channel is reduced to a *local* phase-flip channel acting on Alice's memory, and the quality of final entanglement is bounded by the form of the local density operator of the memory A fed to the phase-flip channel (see Eqs. (4.21) and (4.23)). Since the local density operator can only be altered by Bob remotely at the expense of a failure probability, we are led to Eq. (4.24) relating the change in Alice's local density operator and the success probability. This relation enables us to derive a trade-off relation Eq. (4.41) between the success probability P_s and the average singlet fraction F, which leads to the tight upper bound of arbitrary protocols.

Throughout this chapter, we have focused on the entanglement generation protocols with only one type of error, based on the fact that the known simple distillation protocols work more efficiently against such a restricted type of errors. This has allowed us to treat the entanglement generation protocols separately from distillation protocols. If we look into the properties of the distillation protocols in more detail, there is a possibility that accepting multiple types of errors for higher success probability in the generation protocol could lead to a better result if there

exists a distillation protocol with a less penalty on the multiple types of errors. Pursuing such a possibility is important for implementation of quantum repeaters, and is also interesting in connection to the fundamental question of what is the best way of distributing entanglement against an optical loss in the channel. We expect that the arts introduced here may be also useful in solving such general problems in the search of good entanglement generation protocols.

5

Remote nondestructive parity measurement

As shown in Chapters 3 and 4, the two-probe protocol (or the symmetric protocol) is an efficient, feasible, and fundamental tool to generate entanglement between distant quantum memories. In this chapter, we open up the possibility of more striking applications of the two-probe protocol. This chapter starts with showing that the two-probe protocol actually corresponds to the *nondestructive parity measurement* on qubits AB. The nondestructive measurement is defined by Kraus operators

$$\begin{aligned}\hat{P}_{\Phi}^{AB} :=& |\Phi^+\rangle\langle\Phi^+|_{AB} + |\Phi^-\rangle\langle\Phi^-|_{AB} = |00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}, \\ \hat{P}_{\Psi}^{AB} :=& |\Psi^+\rangle\langle\Psi^+|_{AB} + |\Psi^-\rangle\langle\Psi^-|_{AB} = |01\rangle\langle 01|_{AB} + |10\rangle\langle 10|_{AB}.\end{aligned} \tag{5.1}$$

Since the protocol allows us to implement the nondestructive parity measurement even if the qubits AB are distant, we call it *remote nondestructive parity measurement (RNPM)* protocol. We further show that the RNPM protocol can act as a single module for accomplishing quantum information processing.

5.1 Apparatuses for RNPM protocol

First of all, we summarize physical systems and operations required for the implementation of the RNPM protocol. We assign capital letters to quantum memories, and small letters to optical pulses. The number states of optical pulses are denoted by small letters, e.g., $|m\rangle_a$, whereas the coherent states are denoted by the Greek alphabets, e.g., $|\alpha\rangle_a$.

The quantum memory A used here is assumed to interact with an optical pulse a in coherent state $|\alpha\rangle_a$ with amplitude $\alpha \geq 0$ according to

$$\begin{aligned}\hat{U}_{\theta}^{Aa}|0\rangle_A|\alpha\rangle_a &= |0\rangle_A|\alpha e^{i\theta/2}\rangle_a, \\ \hat{U}_{\theta}^{Aa}|1\rangle_A|\alpha\rangle_a &= |1\rangle_A|\alpha e^{-i\theta/2}\rangle_a,\end{aligned} \tag{5.2}$$

where $\hat{U}_{\theta}^{Aa}$ is a unitary operator, the parameter θ is determined by the strength of the interaction (e.g. $\theta \sim 0.01$ [40]). Note that this unitary operation is achievable by applying a phase shifter after the unitary operation of Eq. (2.159). We assume that the quantum memory allows us to use the following unitary operations:

$$\begin{aligned}\hat{Z}^A &:= |0\rangle\langle 0|_A - |1\rangle\langle 1|_A, \\ \hat{H}^A &:= |+\rangle\langle 0|_A + |-\rangle\langle 1|_A, \\ \hat{Z}_{\xi}^A &:= e^{-i\xi\sigma_z^A/2} = e^{-i\xi/2}|0\rangle\langle 0|_A + e^{i\xi/2}|1\rangle\langle 1|_A,\end{aligned} \tag{5.3}$$

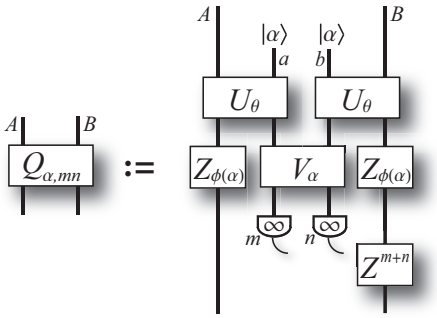

Fig. 5.1. RNPM protocol with complete photon-number-resolving detectors. The operation is represented by Kraus operators $\{\hat{Q}^{AB}_{\alpha,mn}\}_{m,n=0,1,\ldots}$. If photon-number-resolving detectors announce $m > 0$ ($n > 0$), this operation acts as the nondestructive parity measurement $\hat{P}^{AB}_{\Psi}$ ($\hat{P}^{AB}_{\Phi}$). If the detectors inform of $m = n = 0$, the gate does not work, but the system AB receives no disturbance, i.e., $\hat{Q}^{AB}_{\alpha,00} \propto \hat{1}^{AB}$.

where $|\pm\rangle_A := (|0\rangle_A \pm |1\rangle_A)/\sqrt{2}$. We also suppose that $\hat{Z}$-basis measurement on the quantum memory is also implementable.

Optical pulses can be transmitted from mode a to mode b through a lossy channel described by

$$\hat{N}^{a\to b}_T|\alpha\rangle_a = |\sqrt{T}\alpha\rangle_b|\sqrt{1-T}\alpha\rangle_e, \tag{5.4}$$

where $\hat{N}^{a\to b}_T$ is an isometry, $0 \le T \le 1$ represents the transmittance of the channel, and system e is the environment. We use beam splitter $\hat{B}^{ab\to a'b'}_T$ defined by

$$\hat{B}^{ab\to a'b'}_T|\alpha\rangle_a|\beta\rangle_b = |-\sqrt{T}\alpha + \sqrt{1-T}\beta\rangle_{a'}|\sqrt{T}\alpha + \sqrt{1-T}\beta\rangle_{b'} \tag{5.5}$$

for coherent states $|\alpha\rangle_a$ and $|\beta\rangle_b$. By utilizing a beam splitter and a pulse in a coherent state, we can achieve a displacement operation $\hat{D}^{a\to b'}_\alpha$ described by

$$\hat{D}^{a\to b'}_\alpha|\beta\rangle_a = e^{i\mathrm{Im}[\alpha\beta^*]}|\alpha+\beta\rangle_{b'} \tag{5.6}$$

as shown in Sec. 2.5.1.2. We also use a photon detector in Sec. 2.5.1.4 to make the projective measurement on the number states $\{|m\rangle_a\}_{m=0,1,\ldots}$.

5.2 RNPM protocol

In Section 5.2.1, we consider the RNPM protocol using ideal optical channels and photon detectors. In practice, the optical channel are lossy and photon detectors are imperfect, and thus, in Section 5.2.2, we also consider the effect of the imperfections on the RNPM.

5.2.1 RNPM protocol with ideal channels

Throughout Section 5.2.1, we assume that the used optical channels are ideal. Section 5.2.1.1 gives the working principle of the RNPM protocol with perfect detectors. In Sec. 5.2.1.2, we consider cases where photon detectors can count up to $N(\ge 0)$. In Appendix 1, we also consider cases where the detectors have dark counts.

5.2.1.1 RNPM protocol with complete photon-number-resolving detector

As the first step, we show that the nondestructive parity measurement $\{\hat{P}_\Phi, \hat{P}_\Psi\}$ is achievable by RNPM protocol (Fig. 5.1) using interaction $\hat{U}_\theta^{Aa}$, the ideal photon-number-resolving detectors, and beam splitters. The RNPM protocol starts with making measurement described by Kraus operators,

$$\hat{M}_{\alpha,mn}^{AB} := {}_a\langle m|_b\langle n|\hat{Z}_{\phi(\alpha)}^A \hat{Z}_{\phi(\alpha)}^B \hat{V}_\alpha^{ab} \hat{U}_\theta^{Aa} \hat{U}_\theta^{Bb} |\alpha\rangle_a |\alpha\rangle_b, \tag{5.7}$$

where $\alpha \geq 0$, and $\hat{V}_\alpha^{ab}$ and $\phi(\alpha)$ are defined as

$$\hat{V}_\alpha^{ab} := \hat{D}_{-\sqrt{2}\alpha\cos(\theta/2)}^{b\to b} \hat{B}_{1/2}^{ab\to ab}, \tag{5.8}$$

$$\phi(\alpha) := \arg\langle \alpha e^{-i\theta/2} | \alpha e^{i\theta/2}\rangle = \alpha^2 \sin\theta. \tag{5.9}$$

Kraus operator $\hat{M}_{\alpha,mn}^{AB}$ corresponds to an event where the ideal photon-number-resolving detector on mode a (on mode b) announces the arrival of m photons (n photons). By noting relations

$$\begin{aligned}
&\hat{V}_\alpha^{ab} |\alpha e^{i\theta/2}\rangle_a |\alpha e^{i\theta/2}\rangle_b = e^{i\phi(\alpha)} |0\rangle_a |\beta(\alpha)\rangle_b, \\
&\hat{V}_\alpha^{ab} |\alpha e^{i\theta/2}\rangle_a |\alpha e^{-i\theta/2}\rangle_b = |-\beta(\alpha)\rangle_a |0\rangle_b, \\
&\hat{V}_\alpha^{ab} |\alpha e^{-i\theta/2}\rangle_a |\alpha e^{i\theta/2}\rangle_b = |\beta(\alpha)\rangle_a |0\rangle_b, \\
&\hat{V}_\alpha^{ab} |\alpha e^{-i\theta/2}\rangle_a |\alpha e^{-i\theta/2}\rangle_b = e^{-i\phi(\alpha)} |0\rangle_a |-\beta(\alpha)\rangle_b,
\end{aligned} \tag{5.10}$$

with

$$\beta(\alpha) := i\sqrt{2}\alpha \sin(\theta/2), \tag{5.11}$$

we can show that measurement $\hat{M}_{\alpha,mn}^{AB}$ acts on qubits AB as

$$\begin{aligned}
&\hat{M}_{\alpha,mn}^{AB} |00\rangle_{AB} = \delta_{m0} \langle n|\beta(\alpha)\rangle |00\rangle_{AB}, \\
&\hat{M}_{\alpha,mn}^{AB} |01\rangle_{AB} = \delta_{n0} (-1)^m \langle m|\beta(\alpha)\rangle |01\rangle_{AB}, \\
&\hat{M}_{\alpha,mn}^{AB} |10\rangle_{AB} = \delta_{n0} \langle m|\beta(\alpha)\rangle |10\rangle_{AB}, \\
&\hat{M}_{\alpha,mn}^{AB} |11\rangle_{AB} = \delta_{m0} (-1)^n \langle n|\beta(\alpha)\rangle |11\rangle_{AB}.
\end{aligned} \tag{5.12}$$

This implies

$$\hat{M}_{\alpha,mn}^{AB} = \begin{cases}
\langle n|\beta(\alpha)\rangle [|00\rangle\langle 00|_{AB} + (-1)^n |11\rangle\langle 11|_{AB}], & (m=0, n>0), \\
\langle m|\beta(\alpha)\rangle [(-1)^m |01\rangle\langle 01|_{AB} + |10\rangle\langle 10|_{AB}], & (m>0, n=0), \\
\langle 0|\beta(\alpha)\rangle \hat{1}^{AB}, & (m=n=0), \\
0, & (m>0, n>0).
\end{cases} \tag{5.13}$$

By applying $(\hat{Z}^B)^{m+n}$ after the measurement $\hat{M}_{\alpha,mn}^{AB}$, the net Kraus operator $(\hat{Z}^B)^{m+n} \hat{M}_{\alpha,mn}^{AB}$ is shown to be

$$\hat{Q}_{\alpha,mn}^{AB} := (\hat{Z}^B)^{m+n} \hat{M}_{\alpha,mn}^{AB} = \begin{cases}
\langle n|\beta(\alpha)\rangle \hat{P}_\Phi^{AB}, & (m=0, n>0), \\
\langle m|\beta(\alpha)\rangle \hat{P}_\Psi^{AB}, & (m>0, n=0), \\
\langle 0|\beta(\alpha)\rangle \hat{1}^{AB}, & (m=n=0), \\
0, & (m>0, n>0).
\end{cases} \tag{5.14}$$

Therefore, the RNPM protocol in Fig. 5.1 implements the nondestructive parity measurement with success probability $1 - r(\alpha)$ with

$$r(\alpha) := |\langle \alpha e^{-i\theta/2} | \alpha e^{i\theta/2} \rangle| = |\langle 0 | \beta(\alpha) \rangle|^2 = e^{-2\alpha^2 \sin^2(\theta/2)} = e^{-\alpha^2(1-\cos\theta)}. \tag{5.15}$$

Note that, even if the measurement outcome is $m + n = 0$, the system AB receives no disturbance, implying that one can freely repeat this measurement until getting a success event (m, n) satisfying $m+n > 0$. We also note that, if we use coherent states with $\alpha \to \infty$, $\hat{Q}^{AB}_{\alpha,mn}$ is reduced to

$$\hat{Q}^{AB}_{\infty,mn} = \begin{cases} \hat{P}^{AB}_{\Phi}, & (m = 0, n > 0), \\ \hat{P}^{AB}_{\Psi}, & (m > 0, n = 0), \end{cases} \tag{5.16}$$

which implies that the nondestructive parity measurement $\{\hat{P}^{AB}_{\Phi}, \hat{P}^{AB}_{\Psi}\}$ is achievable without failure.

5.2.1.2 RNPM protocol with photon detector with a threshold

Let us consider how the RNPM protocol works in the case where the photon detectors can count up to $N(\geq 0)$ photons (see Fig. 5.2). More precisely, the detector gives outcome $m(\leq N)$ if the number of arrival photons is $m(\leq N)$, but it returns outcome $N + 1$ if the number of arrival photons exceeds N. Note that the detector with $N = 1$ is called the single-photon detector, and the detector with $N = 0$ is called the threshold detector.

Let us see the equivalence of Fig. 5.2, namely the fact that the measurement with outcome (m, n) in Fig. 5.2 is equivalent to the ideal nondestructive parity measurement followed by a phase-flip channel $\Lambda^{m+n}_{2t(N,\alpha)-1}$, where

$$t_e(N, \alpha) := \frac{\sum_{m \in \{2n | n \in \boldsymbol{Z}, 2n \geq N+1\}} |\langle m | \beta(\alpha) \rangle|^2}{\sum_{m=N+1}^{\infty} |\langle m | \beta(\alpha) \rangle|^2}, \tag{5.17}$$

$$t(N, \alpha) := \max\{t_e(N, \alpha),\ 1 - t_e(N, \alpha)\}, \tag{5.18}$$

$$\Lambda_r(\hat{\rho}) := \frac{1+r}{2}\hat{\rho} + \frac{1-r}{2}\hat{Z}\hat{\rho}\hat{Z}, \tag{5.19}$$

$$\Lambda^k_{2t(N,\alpha)-1} := \begin{cases} I, & (0 \leq k \leq N), \\ \Lambda_{2t(N,\alpha)-1}, & (k = N+1). \end{cases} \tag{5.20}$$

To show the equivalence, we first note

$$\begin{aligned}
&\frac{\sum_{k=1}^{N} (\hat{Z}^B)^k \hat{M}^{AB}_{\alpha,0k} \hat{\rho}^{AB} [(\hat{Z}^B)^k \hat{M}^{AB}_{\alpha,0k}]^\dagger}{\sum_{k=1}^{N} |\langle k | \beta(\alpha) \rangle|^2} = \hat{P}^{AB}_{\Phi} \hat{\rho}^{AB} \hat{P}^{AB}_{\Phi}, \\
&\frac{\hat{Z}^B_{N,\alpha,0(N+1)} \left(\sum_{k>N} \hat{M}^{AB}_{\alpha,0k} \hat{\rho}^{AB} (\hat{M}^{AB}_{\alpha,0k})^\dagger \right) \hat{Z}^B_{N,\alpha,0(N+1)}}{\sum_{k>N} |\langle k | \beta(\alpha) \rangle|^2} = \Lambda^B_{2t(N,\alpha)-1}(\hat{P}^{AB}_{\Phi} \hat{\rho}^{AB} \hat{P}^{AB}_{\Phi}), \\
&\frac{\sum_{k=1}^{N} (\hat{Z}^B)^k \hat{M}^{AB}_{\alpha,k0} \hat{\rho}^{AB} [(\hat{Z}^B)^k \hat{M}^{AB}_{\alpha,k0}]^\dagger}{\sum_{k=1}^{N} |\langle k | \beta(\alpha) \rangle|^2} = \hat{P}^{AB}_{\Psi} \hat{\rho}^{AB} \hat{P}^{AB}_{\Psi}, \\
&\frac{\hat{Z}^B_{N,\alpha,(N+1)0} \left(\sum_{k>N} \hat{M}^{AB}_{\alpha,k0} \hat{\rho}^{AB} (\hat{M}^{AB}_{\alpha,k0})^\dagger \right) \hat{Z}^B_{N,\alpha,(N+1)0}}{\sum_{k>N} |\langle k | \beta(\alpha) \rangle|^2} = \Lambda^B_{2t(N,\alpha)-1}(\hat{P}^{AB}_{\Psi} \hat{\rho}^{AB} \hat{P}^{AB}_{\Psi}),
\end{aligned} \tag{5.21}$$

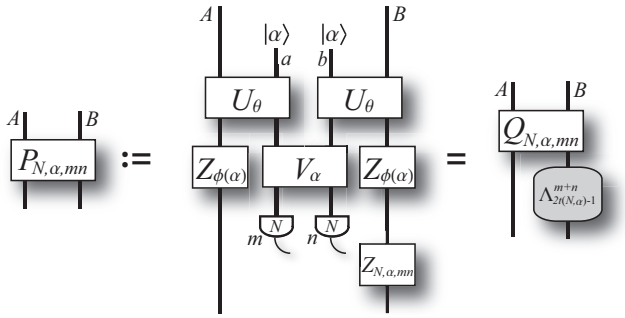

Fig. 5.2. RNPM protocol with photon detectors with threshold N. This operation is denoted as quantum operations $\{P^{AB}_{N,\alpha,mn}\}_{m,n=0,\ldots,N+1}$. $\{\hat{Q}^{AB}_{N,\alpha,mn}\}_{m,n=0,\ldots,N+1}$ works as the ideal nondestructive parity measurement for $m+n>0$ and as the identity channel for $m+n=0$.

where $\hat{Z}_{N,\alpha,mn}$ is defined as

$$\hat{Z}_{N,\alpha,mn} := \begin{cases} \hat{Z}^{m+n}, & (0 \le m+n \le N), \\ \hat{1}, & (m+n=N+1,\ t_e(N,\alpha) \ge 1/2), \\ \hat{Z}, & (m+n=N+1,\ t_e(N,\alpha) < 1/2). \end{cases} \tag{5.22}$$

Eq. (5.21) indicates that the measurement transforms an input state $\hat{\rho}^{AB}$ into unnormalized states according to

$$\hat{\rho}^{AB} \xrightarrow{P_{N,\alpha,mn}} \begin{cases} (\sum_{k=1}^{N} |\langle k|\beta(\alpha)\rangle|^2)\hat{P}^{AB}_{\Phi}\hat{\rho}^{AB}\hat{P}^{AB}_{\Phi}, & (m=0, 0<n\le N), \\ (\sum_{k=N+1}^{\infty} |\langle k|\beta(\alpha)\rangle|^2)\Lambda^{B}_{2t(N,\alpha)-1}(\hat{P}^{AB}_{\Phi}\hat{\rho}^{AB}\hat{P}^{AB}_{\Phi}), & (m=0, n=N+1), \\ (\sum_{k=1}^{N} |\langle k|\beta(\alpha)\rangle|^2)\hat{P}^{AB}_{\Psi}\hat{\rho}^{AB}\hat{P}^{AB}_{\Psi}, & (0<m\le N, n=0), \\ (\sum_{k=N+1}^{\infty} |\langle k|\beta(\alpha)\rangle|^2)\Lambda^{B}_{2t(N,\alpha)-1}(\hat{P}^{AB}_{\Psi}\hat{\rho}^{AB}\hat{P}^{AB}_{\Psi}), & (m=N+1, n=0), \\ |\langle 0|\beta(\alpha)\rangle|^2\hat{\rho}^{AB}, & (m=n=0), \\ 0, & (m>0, n>0). \end{cases} \tag{5.23}$$

With Kraus operators

$$\hat{Q}_{N,\alpha,mn} := \begin{cases} |\langle n|\beta(\alpha)\rangle|\hat{P}^{AB}_{\Phi}, & (m=0, 0<n\le N), \\ \sqrt{\sum_{k=N+1}^{\infty} |\langle k|\beta(\alpha)\rangle|^2}\hat{P}^{AB}_{\Phi}, & (m=0, n=N+1), \\ |\langle m|\beta(\alpha)\rangle|\hat{P}^{AB}_{\Psi}, & (0<m\le N, n=0), \\ \sqrt{\sum_{k=N+1}^{\infty} |\langle k|\beta(\alpha)\rangle|^2}\hat{P}^{AB}_{\Psi}, & (m=N+1, n=0), \\ |\langle 0|\beta(\alpha)\rangle|\hat{I}^{AB}, & (m=n=0), \\ 0, & (m>0, n>0), \end{cases} \tag{5.24}$$

we can summarize the working principle of the RNPM protocol as in Fig. 5.2. Therefore, the RNPM protocol based on photon detectors with threshold N works as the ideal channel for outcome $m+n=0$ occurring with probability $|\langle 0|\beta(\alpha)\rangle|^2 = r(\alpha)$, as the ideal nondestructive parity measurement for outcomes $0<m+n\le N$ occurring with probability $\sum_{k=1}^{N} |\langle k|\beta(\alpha)\rangle|^2$, and as the ideal nondestructive parity measurement with phase flip channel $\Lambda^{B}_{2t(N,\alpha)-1}$ for outcomes $m+n=N+1$ occurring with probability $\sum_{k>N} |\langle k|\beta(\alpha)\rangle|^2$. Hence, allowing the mixture of a

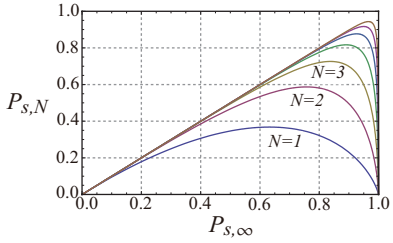

Fig. 5.3. $P_{s,N}(\alpha) := \sum_{k=1}^{N} |\langle k|\beta(\alpha)\rangle|^2$ with $N = 1, 2 \ldots, 7$ for $P_{s,\infty}(\alpha) = 1 - r(\alpha)$.

phase-flip channel, we can regard all the outcomes (m, n) with $m+n > 0$ as the success events of the RNPM protocol. Thus, the success probability of this protocol is $1 - |\langle 0|\beta(\alpha)\rangle|^2 = 1 - r(\alpha)$.

However, in the RNPM protocol with photon detectors with $N > 0$, one can regard events satisfying $m + n = N + 1$ as failure events, in order to prevent the mixture of phase flip channel $\Lambda^B_{2t(N,\alpha)-1}$. In this case, the success probability is $P_{s,N}(\alpha) := \sum_{k=1}^{N} |\langle k|\beta(\alpha)\rangle|^2$. We describe the relation between this success probability and the ideal one $P_{s,\infty}(\alpha)$ in Fig. 5.3. This figure suggests that $P_{s,N}(\alpha)$ with $N \gtrsim 5$ are comparable with $P_{s,\infty}(\alpha)$. Thus, the power of the RNPM protocol with detectors with moderate threshold $N \gtrsim 5$ is approximately equal to the ideal RNPM protocol. In addition, Fig. 5.3 suggests that the penalty of discarding events with $m + n = N + 1$, i.e., $P_{s,\infty}(\alpha) - P_{s,N}(\alpha)$, is very small for small α. From these facts, there will be cases where it is better to consider events satisfying $m + n = N + 1$ to be failure.

5.2.2 Realistic RNPM protocol

In the previous section, we have shown that the nondestructive parity measurement is implementable by ideal optical channels, beam splitters, and photon detectors. Actually, the loss of photons is inevitably caused by practical devices, e.g., optical channels, quantum memories, and photon detectors. Here we clarify the effect of such losses for the RNPM protocol, which is based on several equivalences on quantum operations. We begin with showing the equivalences.

5.2.2.1 A channel equivalent to the discard of a pulse entangled with qubit-state

We consider the effect of the discard of pulse a entangled with quantum memory A by interaction $\hat{U}^{Aa}_{\theta}$ (Fig. 5.4). More precisely, we seek an effect equivalent to $\hat{U}^{Aa}_{\theta}|\alpha\rangle_a$ followed by the partial trace over pulse a. We note

$$\begin{aligned} |j\rangle\langle k|_A \otimes |\alpha\rangle\langle\alpha|_a &\xrightarrow{\hat{U}^{Aa}_{\theta}} |j\rangle\langle k|_A \otimes |\alpha e^{i(-1)^j\theta/2}\rangle\langle\alpha e^{i(-1)^k\theta/2}|_a \\ &\xrightarrow{\mathrm{Tr}_a} \langle\alpha e^{i(-1)^k\theta/2}|\alpha e^{i(-1)^j\theta/2}\rangle|j\rangle\langle k|_A \\ &= |\langle\alpha e^{i(-1)^k\theta/2}|\alpha e^{i(-1)^j\theta/2}\rangle| e^{i\arg\langle\alpha e^{i(-1)^k\theta/2}|\alpha e^{i(-1)^j\theta/2}\rangle}|j\rangle\langle k|_A \\ &= \Lambda^A_{r(\alpha)}(\hat{Z}^A_{-\phi(\alpha)}|j\rangle\langle k|_A(\hat{Z}^A_{-\phi(\alpha)})^\dagger). \end{aligned} \tag{5.25}$$

Since the map consisting of $\hat{U}^{Aa}_{\theta}|\alpha\rangle_a$ and the partial trace over system a are linear, Eq. (5.25) indicates the equivalence in Fig. 5.4.

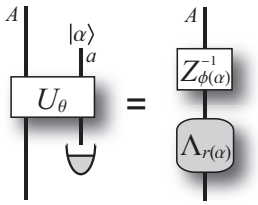

Fig. 5.4. Equivalence between the discard of a pulse entangled with qubit-state and the combination of rotation $\hat{Z}^A_{-\phi(\alpha)}$ and phase-flip channel $\Lambda^A_{r(\alpha)}$.

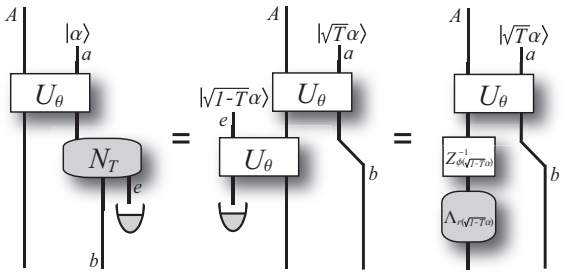

Fig. 5.5. Equivalence between the loss for a pulse entangled with qubit-state and the unitary operation $\hat{U}^{Aa}_\theta$ followed by rotation $\hat{Z}^A_{-\phi(\sqrt{1-T}\alpha)}$ and phase-flip channel $\Lambda^A_{r(\sqrt{1-T}\alpha)}$.

5.2.2.2 A channel equivalent to the loss for a pulse entangled with qubit-state

We consider the effect of the loss occurring on the morrow of the interaction $\hat{U}_\theta$ (Fig. 5.5). We begin with showing

$$
\begin{aligned}
&|j\rangle\langle k|_A \otimes |\alpha\rangle\langle\alpha|_a \xrightarrow{\hat{U}^{Aa}_\theta} |j\rangle\langle k|_A \otimes |\alpha e^{i(-1)^j\theta/2}\rangle\langle\alpha e^{i(-1)^k\theta/2}|_a \\
&\xrightarrow{\hat{N}^{a\to b}_T} |j\rangle\langle k|_A \otimes |\sqrt{T}\alpha e^{i(-1)^j\theta/2}\rangle\langle\sqrt{T}\alpha e^{i(-1)^k\theta/2}|_b \otimes |\sqrt{1-T}\alpha e^{i(-1)^j\theta/2}\rangle\langle\sqrt{1-T}\alpha e^{i(-1)^k\theta/2}|_e \\
&\quad = \hat{U}^{Ae}_\theta \hat{U}^{Ab}_\theta (|j\rangle\langle k|_A \otimes |\sqrt{T}\alpha\rangle\langle\sqrt{T}\alpha|_b \otimes |\sqrt{1-T}\alpha\rangle\langle\sqrt{1-T}\alpha|_e)(\hat{U}^{Ab}_\theta)^\dagger(\hat{U}^{Ae}_\theta)^\dagger, \qquad (5.26)
\end{aligned}
$$

where T represents the net transmittance of the optical channel. This shows the first equivalence in Fig. 5.5. The second equivalence in Fig. 5.5 is shown from the equivalence in Fig. 5.4.

5.2.2.3 A channel equivalent to the loss in photon detectors

Practical detectors do not necessarily announce the arrival of photons even if the detectors actually receive photons, namely their quantum efficiencies η can be non-unity. Such a practical detector can be regarded as an ideal detector following a lossy optical channel with transmittance η (see Fig. 2.8 (b)). Because the photon detectors are used after unitary operation $\hat{V}^{ab}_\gamma$ in the RNPM protocol, for clarifying the imperfection coming from the non-unity quantum efficiency, it is sufficient to consider the effect of the lossy channels after unitary operation $\hat{V}^{ab}_\gamma$ (Fig. 5.6). Here we show that the effect of the lossy channels can be regarded as lossy channels before unitary operation $\hat{V}^{ab}_{\sqrt{\eta}\gamma}$.

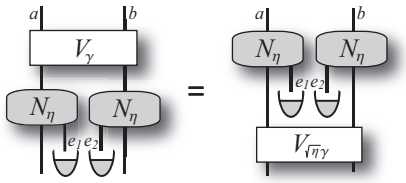

Fig. 5.6. Equivalence between unitary operator $\hat{V}_\gamma^{ab}$ followed by lossy channels $\hat{N}_\eta^{a\to a}\otimes\hat{N}_\eta^{b\to b}$ and lossy channels $\hat{N}_\eta^{a\to a}\otimes\hat{N}_\eta^{b\to b}$ followed by unitary operator $\hat{V}_{\sqrt{\eta}\gamma}^{ab}$.

By comparing process

$$|\alpha\rangle_a|\beta\rangle_b \xrightarrow{\hat{V}_\gamma^{ab}} e^{i\mathrm{Im}[-\gamma\cos(\theta/2)(\alpha^*+\beta^*)]}|(-\alpha+\beta)/\sqrt{2}\rangle_a|(\alpha+\beta)/\sqrt{2}-\sqrt{2}\gamma\cos(\theta/2)\rangle_b \tag{5.27}$$

$$\xrightarrow{\hat{N}_\eta^{a\to a}\otimes\hat{N}_\eta^{b\to b}} e^{i\mathrm{Im}[-\gamma\cos(\theta/2)(\alpha^*+\beta^*)]}|\sqrt{\eta}(-\alpha+\beta)/\sqrt{2}\rangle_a|\sqrt{\eta}(\alpha+\beta)/\sqrt{2}-\sqrt{2\eta}\gamma\cos(\theta/2)\rangle_b$$
$$\otimes|\sqrt{1-\eta}(-\alpha+\beta)/\sqrt{2}\rangle_{e_1}|\sqrt{1-\eta}(\alpha+\beta)/\sqrt{2}-\sqrt{2(1-\eta)}\gamma\cos(\theta/2)\rangle_{e_2} \tag{5.28}$$

and process

$$|\alpha\rangle_a|\beta\rangle_b \xrightarrow{\hat{N}_\eta^{a\to a}\otimes\hat{N}_\eta^{b\to b}} |\sqrt{\eta}\alpha\rangle_a|\sqrt{\eta}\beta\rangle_b|\sqrt{1-\eta}\alpha\rangle_{e_1}|\sqrt{1-\eta}\beta\rangle_{e_2} \tag{5.29}$$

$$\xrightarrow{\hat{V}_{\sqrt{\eta}\gamma}^{ab}} e^{i\mathrm{Im}[-\gamma\cos(\theta/2)\eta(\alpha^*+\beta^*)]}|\sqrt{\eta}(-\alpha+\beta)/\sqrt{2}\rangle_a|\sqrt{\eta}(\alpha+\beta)/\sqrt{2}-\sqrt{2\eta}\gamma\cos(\theta/2)\rangle_b$$
$$\otimes|\sqrt{1-\eta}\alpha\rangle_{e_1}|\sqrt{1-\eta}\beta\rangle_{e_2} \tag{5.30}$$

$$\xrightarrow{\hat{V}_{\sqrt{1-\eta}\gamma}^{e_1e_2}} e^{i\mathrm{Im}[-\gamma\cos(\theta/2)(\alpha^*+\beta^*)]}|\sqrt{\eta}(-\alpha+\beta)/\sqrt{2}\rangle_a|\sqrt{\eta}(\alpha+\beta)/\sqrt{2}-\sqrt{2\eta}\gamma\cos(\theta/2)\rangle_b$$
$$\otimes|\sqrt{1-\eta}(-\alpha+\beta)/\sqrt{2}\rangle_{e_1}|\sqrt{1-\eta}(\alpha+\beta)/\sqrt{2}-\sqrt{2(1-\eta)}\gamma\cos(\theta/2)\rangle_{e_2}, \tag{5.31}$$

we see that these processes are equivalent. Even if one adds the partial trace over system e_1e_2 to these processes, the total operations are equivalent. On the other hand, the partial trace over system e_1e_2 following the process of Eq. (5.31) is equivalent to one following the process of Eq. (5.30), because the partial trace over system e_1e_2 is invariant under unitary operator $\hat{V}_{\sqrt{1-\eta}\gamma}^{e_1e_2}$ on system e_1e_2. Therefore, the equivalence in Fig. 5.6 holds.

5.2.2.4 Realistic RNPM protocol

Considering the effect of photon losses, we reconstruct nondestructive parity measurement as in Fig. 5.7, which is denoted by the measurement $\{P_{T_A,T_B,\eta,N,\alpha,mn}^{AB}\}_{m,n=0,\ldots,N+1}$. In the figure, T_A (T_B) represents the net transmittance of the optical channel $a\to c_1$ ($b\to c_2$), and η is the quantum efficiency of the photon detector. The first equivalence in Fig. 5.7 is proved by equivalences of Fig. 5.5 and Fig. 5.6, by commutability of Λ_r and $\hat{Z}_\xi$ for any r,ξ, and by equation

$$\Lambda_r\Lambda_s=\Lambda_{rs} \tag{5.32}$$

for any r and s. The second and the third equivalences in Fig. 5.7 are shown from Fig. 5.2. Hence, the realistic nondestructive parity measurement $P_{T_A,T_B,\eta,N,\alpha,mn}^{AB}$ is effectively the same as the nondestructive parity measurement $P_{N,\alpha,mn}^{AB}$ followed by the phase flip channel $\Lambda^A_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)}\otimes\Lambda^B_{r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}$. This implies that a phase flip channel is added to the nondestructive parity

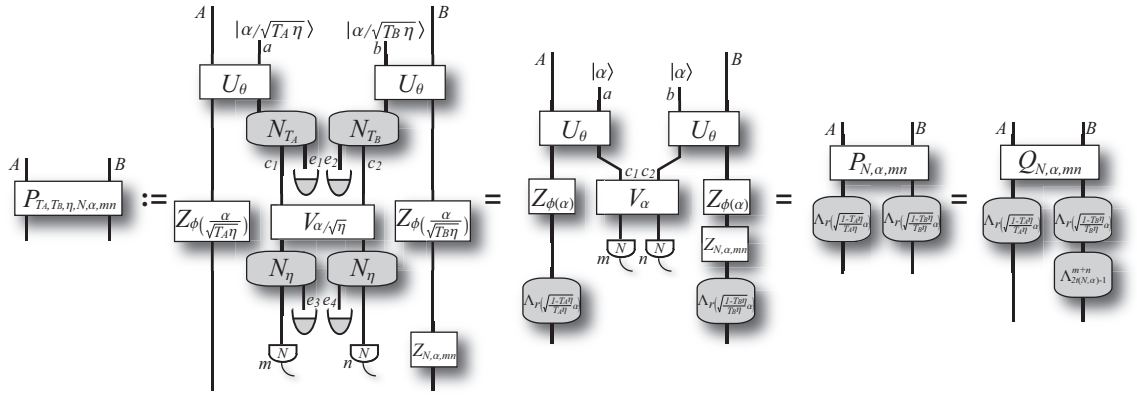

Fig. 5.7. Realistic RNPM protocol $\{P^{AB}_{T_A,T_B,\eta,N,\alpha,mn}\}_{m,n=0,\ldots,N+1}$. This operation is equivalent to nondestructive parity measurement $\{P^{AB}_{N,\alpha,mn}\}_{m,n=0,\ldots,N+1}$ followed by phase-flip channels $\Lambda^{A}_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)} \otimes \Lambda^{B}_{r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}$.

measurement $P^{AB}_{N,\alpha,mn}$ as the penalty of the photon losses. Moreover, the phase error rates show a trade-off relation to the success probability through amplitude α of the used pulses. In fact, the phase error rates $[1 - r(\sqrt{(1 - T_X\eta)/(T_X\eta)}\alpha)]/2$ $(X = A, B)$ and the success probability $1 - r(\alpha)$ monotonically increase with α. Therefore, the realistic RNPM protocol performs as RNPM with a trade-off between the success probability and the phase error rates.

5.2.2.5 Realistic RNPM protocol on distant quantum memories

Here we show that the realistic nondestructive parity measurement $\{P^{AB}_{T_A,T_B,\eta,N,\alpha,mn}\}_{m,n=0,\ldots,N+1}$ is applicable even if quantum memories AB are distant. Suppose that the memory A (B) is held by Alice (Bob), and they locate over distance L_0. Alice (Bob) is connected to a station C by an optical channel $a_1 \to c_1$ with length l_A ($b_1 \to c_2$ with length $L_0 - l_A$), where $0 \leq l_A \leq L_0$. In this case, we should assume

$$\begin{aligned} T_A =& \tau e^{-l_A/L_{\rm att}}, \\ T_B =& \tau e^{-(L_0-l_A)/L_{\rm att}}, \end{aligned} \tag{5.33}$$

where τ is the transmittance of the local optical channel, and $L_{\rm att}$ is the attenuation length of the used channels. For accomplishing the realistic nondestructive parity measurement, Alice (Bob) should send the local oscillators (LOs) to station C through the same channel $a_1 \to c_1$ ($b_1 \to c_2$) with the signal pulses so that the party in station C can offset unwished phase shifts occurring in the channel. By these modifications, distant parties, Alice and Bob, can achieve the realistic nondestructive parity measurement $\{P^{AB}_{T_A,T_B,\eta,N,\alpha,mn}\}_{m,n=0,\ldots,N+1}$ with Eq. (5.33).

5.3 Applications of RNPM protocol

In this section, we show several striking applications of the RNPM protocol. In particular, the RNPM protocol enables parity check measurement, Bell measurement, isometry $\hat{C}^{AB}_Z|+\rangle_A$, and CZ gate $\hat{C}^{AB}_Z$. These operations play the primary role for implementing long-distance quantum communication and quantum computation.

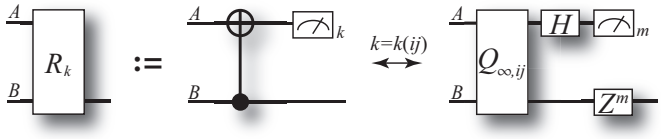

Fig. 5.8. Ideal parity check measurement $\{\hat{R}_k^{AB\to B}\}_{k=0,1}$, which is CNOT gate followed by $\hat{Z}$-basis measurement on the target qubit. The measurement can be also executed by using the ideal nondestructive parity measurement $\{\hat{Q}_{\infty,ij}^{AB}\}_{i,j=0,1,\ldots}$.

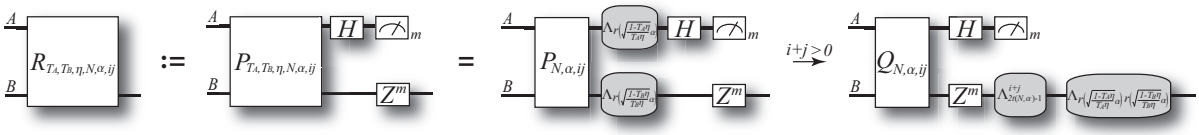

Fig. 5.9. Realistic parity check measurement $\{R_{T_A,T_B,\eta,N,\alpha,ij}^{AB\to B}\}_{i,j=0,\ldots,N+1}$.

5.3.1 Parity check measurement

The parity check measurement $\{\hat{R}_k\}_{k=0,1}$ was introduced in Sec. 2.4. The measurement is CNOT gate followed by $\hat{Z}$-basis measurement $\{|k\rangle\}_{k=0,1}$ on the target qubit (see Fig. 5.8), and the Kraus operators are

$$\begin{aligned}\hat{R}_0^{AB\to B} &:= {}_A\langle 0|\hat{C}_X^{BA} = |0\rangle_{BAB}\langle 00| + |1\rangle_{BAB}\langle 11| = |+\rangle_{BAB}\langle\Phi^+| + |-\rangle_{BAB}\langle\Phi^-|,\\ \hat{R}_1^{AB\to B} &:= {}_A\langle 1|\hat{C}_X^{BA} = |0\rangle_{BAB}\langle 10| + |1\rangle_{BAB}\langle 01| = |+\rangle_{BAB}\langle\Psi^+| - |-\rangle_{BAB}\langle\Psi^-|,\end{aligned} \tag{5.34}$$

where $\hat{C}_X^{CT}$ represents CNOT gate defined by

$$\hat{C}_X^{CT} := |0\rangle\langle 0|_C \otimes \hat{1}^T + |1\rangle\langle 1|_C \otimes \hat{X}^T. \tag{5.35}$$

As seen in Sec. 2.4, the measurement is essential for implementing the recurrence method. In addition, the measurement is also utilized as a fusion gate of cluster states [74, 75]. In this section, we show that the parity check measurement is implementable by the RNPM protocol.

5.3.1.1 Ideal parity check measurement

We begin with showing that the parity check measurement is achievable by utilizing the ideal nondestructive parity measurement $\{\hat{Q}_{\infty,ij}^{AB}\}_{i,j=0,1,\ldots}$. From Eq. (5.16) and

$$\begin{aligned}{}_A\langle m|\hat{H}^A|\Phi^\pm\rangle_{AB} &= \frac{1}{2}(|0\rangle_B \pm (-1)^m|1\rangle_B) \overset{(Z^B)^m}{\longrightarrow} \frac{1}{\sqrt{2}}|\pm\rangle_B,\\ {}_A\langle m|\hat{H}^A|\Psi^\pm\rangle_{AB} &= \frac{1}{2}(|1\rangle_B \pm (-1)^m|0\rangle_B) \overset{(Z^B)^m}{\longrightarrow} \pm\frac{(-1)^m}{\sqrt{2}}|\pm\rangle_B,\end{aligned} \tag{5.36}$$

we have

$$(\hat{Z}^B)^m {}_A\langle m|\hat{H}^A\hat{Q}_{\infty,0j}^{AB} = \frac{1}{\sqrt{2}}(|+\rangle_{BAB}\langle\Phi^+| + |-\rangle_{BAB}\langle\Phi^-|) = \frac{1}{\sqrt{2}}\hat{R}_0^{AB\to B}, \tag{5.37}$$

$$(\hat{Z}^B)^m {}_A\langle m|\hat{H}^A\hat{Q}_{\infty,i0}^{AB} = \frac{(-1)^m}{\sqrt{2}}(|+\rangle_{BAB}\langle\Psi^+| - |-\rangle_{BAB}\langle\Psi^-|) = \frac{(-1)^m}{\sqrt{2}}\hat{R}_1^{AB\to B}, \tag{5.38}$$

for $i, j > 0$. This fact implies the equivalence in Fig. 5.8, where

$$k(ij) := \begin{cases} 0, & (i = 0,\ j > 0), \\ 1, & (i > 0,\ j = 0). \end{cases} \tag{5.39}$$

Hence we conclude that the parity check measurement $\{\hat{R}_k\}_{k=0,1}$ is achievable by using the nondestructive parity measurement $\{\hat{Q}^{AB}_{\infty,ij}\}_{i,j=0,1,\ldots}$.

5.3.1.2 Realistic parity check measurement

Here we consider a parity check measurement based on the realistic RNPM protocol. The realistic parity measurement is defined as in Fig. 5.9, and it is denoted by $\{R^{AB}_{T_A,T_B,\eta,N,\alpha,ij}\}_{i,j=0,\ldots,N+1}$. In order to clarify the property of the realistic parity check measurement, we show several equivalences in Fig. 5.9. The first equivalence in the figure is shown from Fig. 5.7. The last arrow in the figure indicates the equivalence holding only when $i+j > 0$, which is shown from the equivalence in Fig. A2.1 (b). The last figure in Fig. 5.9 and Fig. 5.8 imply that, for $i + j > 0$, the realistic parity check measurement $R^{AB\to B}_{T_A,T_B,\eta,N,\alpha,ij}$ is the same as the ideal parity check $\hat{R}_{k(ij)}$ followed by phase-flip channel $\Lambda^B_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}\Lambda^{i+j,B}_{2t(N,\alpha)-1}$. Therefore, by the realistic RNPM protocol, we can perform the parity check measurement with a phase flip channel. The failure outcome ($i + j = 0$) of the parity check measurement $\{R^{AB}_{T_A,T_B,\eta,N,\alpha,ij}\}_{i,j=0,\ldots,N+1}$ occurs with probability $r(\alpha)$.

5.3.2 Bell measurement

As represented in Sec. 2.1, Bell measurement is defined by Kraus operators

$$\begin{aligned} \hat{B}^{AB}_{00} &:= {}_{AB}\langle\Phi^+|, \\ \hat{B}^{AB}_{01} &:= {}_{AB}\langle\Psi^+|, \\ \hat{B}^{AB}_{10} &:= {}_{AB}\langle\Phi^-|, \\ \hat{B}^{AB}_{11} &:= -{}_{AB}\langle\Psi^-|. \end{aligned} \tag{5.40}$$

The measurement is essential for executing the quantum teleportation protocol and the entanglement swapping. In this section, we show that the Bell measurement is implementable by the RNPM protocol.

5.3.2.1 Ideal Bell measurement

Here we start with noting that Bell measurement is achievable by the ideal parity check measurement $\{\hat{R}^{AB\to B}_k\}_{k=0,1}$ and $\hat{X}$-basis measurement on system B. This fact is easily confirmed by

$$\begin{aligned} {}_B\langle 0|\hat{H}^B\hat{R}^{AB\to B}_0 &= {}_{AB}\langle\Phi^+| = \hat{B}^{AB}_{00}, \\ {}_B\langle 0|\hat{H}^B\hat{R}^{AB\to B}_1 &= {}_{AB}\langle\Psi^+| = \hat{B}^{AB}_{01}, \\ {}_B\langle 1|\hat{H}^B\hat{R}^{AB\to B}_0 &= {}_{AB}\langle\Phi^-| = \hat{B}^{AB}_{10}, \\ {}_B\langle 1|\hat{H}^B\hat{R}^{AB\to B}_1 &= -{}_{AB}\langle\Psi^-| = \hat{B}^{AB}_{11}. \end{aligned} \tag{5.41}$$

Since the measurement $\{\hat{R}^{AB\to B}_k\}_{k=0,1}$ is achievable by ideal nondestructive parity measurement $\{\hat{Q}^{AB}_{\infty,ij}\}_{i,j=0,1,\ldots}$, the ideal Bell measurement $\{\hat{B}_{lk}\}_{k,l=0,1,\ldots}$ is also achievable by utilizing $\{\hat{Q}^{AB}_{\infty,ij}\}_{i,j=0,1,\ldots}$. This equivalence is described in Fig. 5.10.

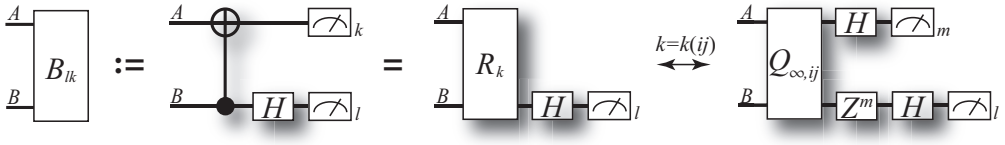

Fig. 5.10. Ideal Bell measurement $\{\hat{B}^{AB}_{lk}\}_{k,l=0,1}$. This measurement can be also executed by the ideal nondestructive parity measurement $\{\hat{Q}^{AB}_{\infty,ij}\}_{i,j=0,1,...}$.

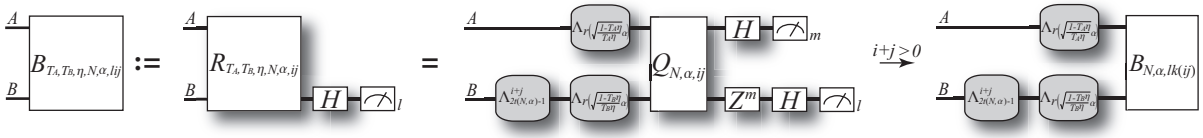

Fig. 5.11. Realistic Bell measurement $\{B^{AB}_{T_A,T_B,\eta,N,\alpha,lij}\}_{i,j=0,...,N+1;\, l=0,1}$.

5.3.2.2 Realistic Bell measurement

Here we introduce Bell measurement based on the realistic RNPM protocol. The realistic Bell measurement $\{B^{AB}_{T_A,T_B,\eta,N,\alpha,lij}\}_{i,j=0,...,N+1;\, l=0,1}$ is executed by the realistic parity check measurement $\{R^{AB\to B}_{T_A,T_B,\eta,N,\alpha,ij}\}_{i,j=0,...,N+1}$ and $\hat{X}$-basis measurement on system B, as in Fig. 5.11. The equivalence in Fig. 5.11 is derived from the equivalence in Fig. A2.1 (a). This equivalence and Fig. 5.10 imply that, when $i+j>0$, the realistic Bell measurement $B^{AB}_{T_A,T_B,\eta,N,\alpha,lij}$ is the same as the ideal Bell measurement $\hat{B}_{lk(ij)}$ following $\Lambda^A_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)}\otimes\Lambda^B_{r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}\Lambda^{i+j,B}_{2t(N,\alpha)-1}$. Hence, by the realistic RNPM protocol, we can accomplish the Bell measurement with a phase error. The failure outcome ($i+j=0$) of the Bell measurement $\{B^{AB}_{T_A,T_B,\eta,N,\alpha,lij}\}_{i,j=0,...,N+1;\, l=0,1}$ occurs with probability $r(\alpha)$. For simplicity, we describe this working principle by the last figure of 5.11, where $\hat{B}^{AB}_{N,\alpha,lk(mn)}$ are (partial) Kraus operators

$$\hat{B}^{AB}_{N,\alpha,lk(mn)} := \begin{cases} |\langle n|\beta(\alpha)\rangle|\hat{B}^{AB}_{l0}, & (m=0, 0<n\le N),\\ \sqrt{\sum_{k=N+1}^{\infty}|\langle k|\beta(\alpha)\rangle|^2}\hat{B}^{AB}_{l0}, & (m=0, n=N+1),\\ |\langle m|\beta(\alpha)\rangle|\hat{B}^{AB}_{l1}, & (0<m\le N, n=0),\\ \sqrt{\sum_{k=N+1}^{\infty}|\langle k|\beta(\alpha)\rangle|^2}\hat{B}^{AB}_{l1}, & (m=N+1, n=0),\\ 0, & (m>0, n>0). \end{cases} \tag{5.42}$$

5.3.3 Isometry $\hat{C}^{AB}_Z|+\rangle_A$

The CZ gate defined by

$$\hat{C}^{AB}_Z := |0\rangle\langle 0|_A\otimes\hat{1}^B + |1\rangle\langle 1|_A\otimes\hat{Z}^B \tag{5.43}$$

is essential for generating the so-called *graph state* [47, 48, 49]. The graph state is known [48, 49] as an entangled state enabling universal quantum computation through sequential one-qubit projective measurements. Actually, for connecting a qubit A in state $|+\rangle_A$ with a qubit B in a graph state through a single bond, isometry $\hat{C}^{AB}_Z|+\rangle_A$ is sufficient [49]. The isometry $\hat{C}^{AB}_Z|+\rangle_A$

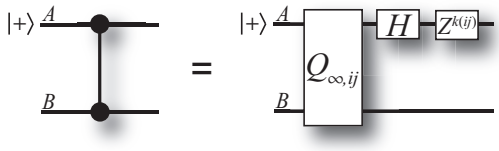

Fig. 5.12. The operation to add a qubit to a graph state. This operation is achievable by the ideal nondestructive parity measurement.

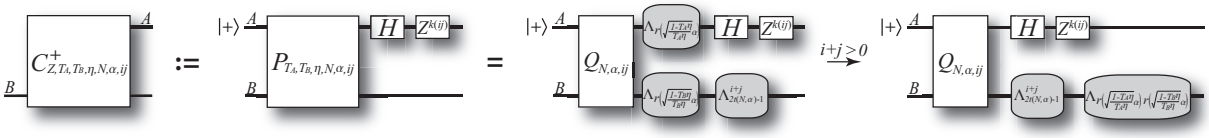

Fig. 5.13. The operation to add a qubit to a graph state based on the realistic nondestructive parity measurement.

is described by

$$\hat{C}_Z^{AB}|+\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes \hat{1}^B + |1\rangle_A \otimes \hat{Z}^B). \tag{5.44}$$

Here we show that this operation is achieved by the RNPM protocol.

5.3.3.1 Isometry $\hat{C}_Z^{AB}|+\rangle_A$ based on the ideal nondestructive parity measurement

Here we begin with showing that the isometry $\hat{C}_Z^{AB}|+\rangle_A$ is achieved by the ideal nondestructive parity measurement $\{\hat{Q}^{AB}_{\infty,ij}\}_{i,j=0,1,...}$. This fact is easily confirmed by noting

$$\begin{aligned}
\hat{H}^A\hat{Q}^{AB}_{\infty,0j}|+\rangle_A &= (|+0\rangle\langle 00|_{AB} + |-1\rangle\langle 11|_{AB})|+\rangle_A = \frac{1}{\sqrt{2}}\hat{C}_Z^{AB}|+\rangle_A, \\
\hat{Z}^A\hat{H}^A\hat{Q}^{AB}_{\infty,i0}|+\rangle_A &= (|-1\rangle\langle 01|_{AB} + |+0\rangle\langle 10|_{AB})|+\rangle_A = \frac{1}{\sqrt{2}}\hat{C}_Z^{AB}|+\rangle_A,
\end{aligned} \tag{5.45}$$

for $i, j > 0$. This equivalence is shown in Fig. 5.12.

5.3.3.2 Isometry $\hat{C}_Z^{AB}|+\rangle_A$ based on the realistic nondestructive parity measurement

Let us consider the operation $\{C^{+,B\to AB}_{Z,T_A,T_B,\eta,N,\alpha,ij}\}_{i,j=0,...,N+1}$ in Fig. 5.13. From the equivalences in Figs. 5.7 and A2.1 (b), one can confirm the equivalence in Fig. 5.13. The last figure in Fig. 5.13 and Fig, 5.12 indicate that, in the case of $i+j>0$, the net operation is equivalent to the isometry $\hat{C}_Z^{AB}|+\rangle_A$ followed by phase-flip channel $\Lambda^B_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}\Lambda^{i+j,B}_{2t(N,\alpha)-1}$. Thus, by the RNPM protocol, we can achieve the isometry $\hat{C}_Z^{AB}|+\rangle_A$ with a phase error. The failure outcome ($i+j=0$) of the operation $\{C^{+,B\to AB}_{Z,T_A,T_B,\eta,N,\alpha,ij}\}_{i,j=0,...,N+1}$ occurs with probability $r(\alpha)$.

5.3.4 CZ gate $\hat{C}_Z^{AB}$

CZ gate is essential for implementing quantum computing. In fact, universal quantum computation is achievable by the combination of CZ gates and one-qubit unitary operations [50]. In addition, even for generating closed loops in a graph state, CZ gate is required to connect qubits AB in a graph $\mathcal{C}$. In this section, we show that CZ gate is achievable by the RNPM protocol.

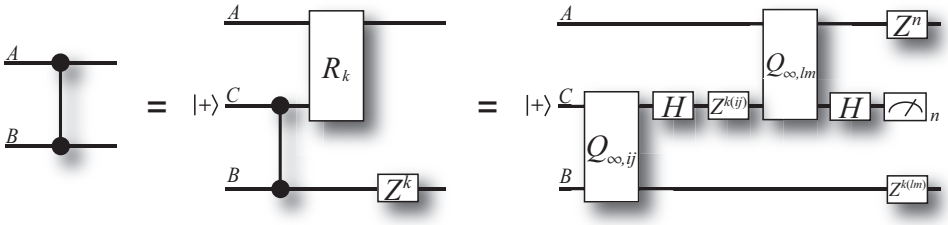

Fig. 5.14. CZ gate. The CZ gate is achievable by the nondestructive parity measurements.

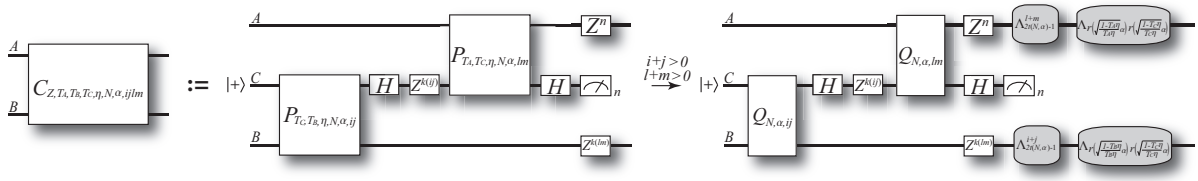

Fig. 5.15. CZ gate based on the realistic nondestructive parity measurements.

5.3.4.1 CZ gate by the ideal nondestructive parity measurement

Here we show that CZ gate is achievable by the ideal nondestructive parity measurement $\{\hat{Q}_{\infty,ij}\}_{i,j=0,1,\ldots}$. The relations

$$\hat{R}_0^{AC\to A}\hat{C}_Z^{BC}|+\rangle_C = (|0\rangle_{AAC}\langle 00| + |1\rangle_{AAC}\langle 11|)\frac{1}{\sqrt{2}}(\hat{1}^B\otimes|0\rangle_C + \hat{Z}^B\otimes|1\rangle_C) = \frac{1}{\sqrt{2}}\hat{C}_Z^{AB} \tag{5.46}$$

$$\hat{Z}^B\hat{R}_1^{AC\to A}\hat{C}_Z^{BC}|+\rangle_C = (|0\rangle_{AAC}\langle 01| + |1\rangle_{AAC}\langle 10|)\frac{1}{\sqrt{2}}(\hat{Z}^B\otimes|0\rangle_C + \hat{1}^B\otimes|1\rangle_C) = \frac{1}{\sqrt{2}}\hat{C}_Z^{AB}, \tag{5.47}$$

imply the first equivalence in Fig. 5.14. The second equivalence is shown from the equivalences in Figs. 5.8 and 5.12. The last figure indicates that CZ gate can be accomplished by the combination of the two ideal nondestructive parity measurements.

5.3.4.2 CZ gate by the realistic nondestructive parity measurement

Let us consider the operation $\{C^{AB}_{Z,T_A,T_B,T_C,\eta,N,\alpha,ijlm}\}_{i,j,l,m=0,\ldots,N+1}$ in Fig. 5.15. From Figs. 5.7 and A2.1 (b), one can show the validity of the arrow in Fig. 5.15. The last figure in Fig. 5.15 and Fig. 5.14 indicate that, for $i+j>0$ and $l+m>0$, the operation $C^{AB}_{Z,T_A,T_B,T_C,\eta,N,\alpha,ijlm}$ is equivalent to CZ gate followed by phase-flip channel $\Lambda^A_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)r(\sqrt{(1-T_C\eta)/(T_C\eta)}\alpha)}\Lambda^{l+m,A}_{2t(N,\alpha)-1}\otimes\Lambda^B_{r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)r(\sqrt{(1-T_C\eta)/(T_C\eta)}\alpha)}\Lambda^{i+j,B}_{2t(N,\alpha)-1}$. Hence, by the RNPM protocols, we can achieve the CZ gate with a phase error with probability $[1-r(\alpha)]^2$.

5.3.5 Summary

In this section, we have shown that several primitive quantum operations for implementing long-distance quantum communication and universal quantum computation are realizable by using

only the RNPM protocols and single-qubit operations. This implies that the RNPM protocols and single-qubit operations can be a universal set for arbitrary quantum operations. However, because the practical RNPM protocol has noises such as photon losses, the RNPM protocol inevitably has a trade-off between the success probability and the received phase error rate. Therefore, it should be clarified whether, against such a trade-off, the RNPM protocol really works as a useful gate. In the next chapter, as the first step of this trial, we show that the RNPM protocol properly works for accomplishing efficient long-distance quantum communication.

6

Quantum repeaters with remote nondestructive parity measurement

If two distant parties, Alice and Bob, hold quantum memories in a maximally entangled state (Bell state), they can accomplish quantum communication by quantum teleportation. In order to prepare their memories in a Bell state, optical pulses are used as the carrier of quantum information of the memories. However, the real transmission channel for optical pulses suffers from photon losses that increase exponentially with the length of the channel, and furthermore there are inevitable residual imperfections in physical systems. The way out of the photon losses will be the combination of entanglement generation between quantum memories of quantum repeaters and entanglement swapping at the repeaters [31]. The residual imperfections will be compensated by entanglement distillation [28, 29]. In this chapter, we show that a single protocol – RNPM protocol – is sufficient for efficient implementation of long-distance quantum communication through accomplishing entanglement generation, entanglement swapping, and entanglement distillation.

6.1 Basic operations for quantum repeater protocols

In this section, we show that the three basic operations needed for efficient long-distance quantum communication – entanglement generation, entanglement swapping, and entanglement distillation – are implementable by the realistic RNPM protocol.

6.1.1 Entanglement generation based on the realistic RNPM protocol

We show that the entanglement generation is achieved by the realistic RNPM protocol, using the fact that the RNPM protocol on qubits AB is implementable even if the qubits AB are distant (see Sec. 5.2.2.5). According to the conclusion in Sec. 5.2.2.5, Alice (Bob) is connected to a station C by an optical channel $a_1 \to c_1$ with length l_A ($b_1 \to c_2$ with length $L_0 - l_A$), and the net transmittances of the channels are described by

$$\begin{aligned} T_A =& \tau e^{-l_A/L_{\rm att}}, \\ T_B =& \tau e^{-(L_0-l_A)/L_{\rm att}}, \end{aligned} \tag{6.1}$$

where τ is the transmittance of the local optical channel, and $L_{\rm att}$ is the attenuation length of the used channels. Based on these facts, entanglement generation is accomplished by the RNPM $\{P^{AB}_{T_A,T_B,\eta,N,\alpha,mn}\}_{m,n=0,\ldots,N+1}$ on distant quantum memories AB in state $|++\rangle_{AB} = (|\Phi^+\rangle_{AB} + |\Psi^+\rangle_{AB})/\sqrt{2}$. In fact, from Fig. 5.7, the measurement $P^{AB}_{T_A,T_B,\eta,N,\alpha,mn}$ transforms

state $|++\rangle_{AB}$ into unnormalized states according to

$$
|++\rangle_{AB} \overset{P^{AB}_{T_A,T_B,\eta,N,\alpha,mn}}{\longrightarrow}
\begin{cases}
(1/2)(\sum_{n=1}^{N}|\langle n|\beta(\alpha)\rangle|^2)\Lambda^B_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}(|\Phi^+\rangle\langle\Phi^+|_{AB}), \\
\qquad\qquad (m=0, 0<n\leq N), \\
(1/2)(\sum_{n=N+1}^{\infty}|\langle n|\beta(\alpha)\rangle|^2)\Lambda^B_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)[2t(N,\alpha)-1]}(|\Phi^+\rangle\langle\Phi^+|_{AB}), \\
\qquad\qquad (m=0, n=N+1), \\
(1/2)(\sum_{m=1}^{N}|\langle m|\beta(\alpha)\rangle|^2)\Lambda^B_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}(|\Psi^+\rangle\langle\Psi^+|_{AB}), \\
\qquad\qquad (0<m\leq N, n=0), \\
(1/2)(\sum_{m=N+1}^{\infty}|\langle m|\beta(\alpha)\rangle|^2)\Lambda^B_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)[2t(N,\alpha)-1]}(|\Psi^+\rangle\langle\Psi^+|_{AB}), \\
\qquad\qquad (m=N+1, n=0), \\
|\langle 0|\beta(\alpha)\rangle|^2[\Lambda^A_{r(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha)}\otimes\Lambda^B_{r(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha)}(|++\rangle\langle++|_{AB})], \\
\qquad\qquad (m=n=0),
\end{cases}
\tag{6.2}
$$

where $\beta(\alpha)=i\sqrt{2}\alpha\sin(\theta/2)$. Therefore, the RNPM protocol fails in generating entanglement for outcome $m=n=0$ occurring with probability $|\langle 0|\beta(\alpha)\rangle|^2=r(\alpha)$, and succeeds in producing entanglement for the other outcomes occurring with probability $1-|\langle 0|\beta(\alpha)\rangle|^2=1-r(\alpha)$. Actually, the obtained entangled states are divided into two types, dependently on the received phase error rate: Compared with entanglement generated in the cases of $0<m+n\leq N$, entanglement obtained in the cases of $m+n=N+1$ receives an additional phase error with rate $1-t(N,\alpha)$ coming from finite threshold N of the photon detectors.

For a fixed L_0, the choice of $l_A=L_0/2$ gives the best performance of this entanglement generation protocol. On the other hand, the entanglement generation with $l_A=L_0$ is equivalent to the two-probe protocol in Fig. 3.1, and hence it has a technical merit in stabilizing the relative phase between pulses c_1 and c_2. Moreover, the optimality proof in Chapter 4 can be generalized to be applicable for any $0\leq l_A\leq L_0$, which will show that the entanglement generation introduced here achieves the theoretical limit of performance of single-error-type entanglement generation protocols.

6.1.2 Entanglement connection based on the realistic RNPM protocol

As represented by entanglement swapping, we can transform the state $|\Phi^+\rangle_{AC_1}|\Phi^+\rangle_{C_2B}$ into a Bell state $|\Phi^+\rangle_{AB}$ by making Bell measurement on system C_1C_2. However, in practice, there are cases where the initial state of the system AC_1C_2B is not the complete Bell state $|\Phi^+\rangle_{AC_1}|\Phi^+\rangle_{C_2B}$ but an entangled state described by $\hat{\rho}_1^{AC_1}\otimes\hat{\rho}_2^{C_2B}$. Here we consider the effect of Bell measurement on system in such a state $\hat{\rho}_1^{AC_1}\otimes\hat{\rho}_2^{C_2B}$. Let us call this operation *entanglement connection*.

6.1.2.1 Entanglement connection by the ideal Bell measurement

Let us consider to connect two Bell diagonal states $\hat{\rho}_1^{AC_1}\otimes\hat{\rho}_2^{C_2B}$ by the ideal Bell measurement $\{\hat{B}_{lk}^{C_1C_2}\}_{k,l=0,1}$. Then, from Eqs. (A2.3)-(A2.6), when the Bell measurement returns outcome

$lk = 00$, the state $\hat{\sigma}_{00}^{AB} := {}_{4C_1C_2}\langle\Phi^+|\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}|\Phi^+\rangle_{C_1C_2}$ is represented by

$$\begin{aligned}
\hat{\sigma}_{00}^{AB} = &|\Phi^+\rangle\langle\Phi^+|_{AB}(\langle\Phi^+|\hat{\rho}_1^{AC_1}|\Phi^+\rangle\langle\Phi^+|\hat{\rho}_2^{C_2B}|\Phi^+\rangle + \langle\Phi^-|\hat{\rho}_1^{AC_1}|\Phi^-\rangle\langle\Phi^-|\hat{\rho}_2^{C_2B}|\Phi^-\rangle \\
&+\langle\Psi^+|\hat{\rho}_1^{AC_1}|\Psi^+\rangle\langle\Psi^+|\hat{\rho}_2^{C_2B}|\Psi^+\rangle + \langle\Psi^-|\hat{\rho}_1^{AC_1}|\Psi^-\rangle\langle\Psi^-|\hat{\rho}_2^{C_2B}|\Psi^-\rangle) \\
&+|\Psi^+\rangle\langle\Psi^+|_{AB}(\langle\Phi^+|\hat{\rho}_1^{AC_1}|\Phi^+\rangle\langle\Psi^+|\hat{\rho}_2^{C_2B}|\Psi^+\rangle + \langle\Phi^-|\hat{\rho}_1^{AC_1}|\Phi^-\rangle\langle\Psi^-|\hat{\rho}_2^{C_2B}|\Psi^-\rangle \\
&+\langle\Psi^+|\hat{\rho}_1^{AC_1}|\Psi^+\rangle\langle\Phi^+|\hat{\rho}_2^{C_2B}|\Phi^+\rangle + \langle\Psi^-|\hat{\rho}_1^{AC_1}|\Psi^-\rangle\langle\Phi^-|\hat{\rho}_2^{C_2B}|\Phi^-\rangle) \\
&+|\Phi^-\rangle\langle\Phi^-|_{AB}(\langle\Phi^+|\hat{\rho}_1^{AC_1}|\Phi^+\rangle\langle\Phi^-|\hat{\rho}_2^{C_2B}|\Phi^-\rangle + \langle\Phi^-|\hat{\rho}_1^{AC_1}|\Phi^-\rangle\langle\Phi^+|\hat{\rho}_2^{C_2B}|\Phi^+\rangle \\
&+\langle\Psi^+|\hat{\rho}_1^{AC_1}|\Psi^+\rangle\langle\Psi^-|\hat{\rho}_2^{C_2B}|\Psi^-\rangle + \langle\Psi^-|\hat{\rho}_1^{AC_1}|\Psi^-\rangle\langle\Psi^+|\hat{\rho}_2^{C_2B}|\Psi^+\rangle) \\
&+|\Psi^-\rangle\langle\Psi^-|_{AB}(\langle\Phi^+|\hat{\rho}_1^{AC_1}|\Phi^+\rangle\langle\Psi^-|\hat{\rho}_2^{C_2B}|\Psi^-\rangle + \langle\Phi^-|\hat{\rho}_1^{AC_1}|\Phi^-\rangle\langle\Psi^+|\hat{\rho}_2^{C_2B}|\Psi^+\rangle \\
&+\langle\Psi^+|\hat{\rho}_1^{AC_1}|\Psi^+\rangle\langle\Phi^-|\hat{\rho}_2^{C_2B}|\Phi^-\rangle + \langle\Psi^-|\hat{\rho}_1^{AC_1}|\Psi^-\rangle\langle\Phi^+|\hat{\rho}_2^{C_2B}|\Phi^+\rangle).
\end{aligned} \tag{6.3}$$

Note that this state is also a Bell diagonal state. In the other cases, the left states are determined by

$$\begin{aligned}
\hat{\sigma}_{01}^{AB} &:= {}_{4C_1C_2}\langle\Psi^+|\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}|\Psi^+\rangle_{C_1C_2} = \hat{X}^B {}_{C_1C_2}\langle\Phi^+|\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}|\Phi^+\rangle_{C_1C_2}\hat{X}^B, \\
\hat{\sigma}_{10}^{AB} &:= {}_{4C_1C_2}\langle\Phi^-|\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}|\Phi^-\rangle_{C_1C_2} = \hat{Z}^B {}_{C_1C_2}\langle\Phi^+|\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}|\Phi^+\rangle_{C_1C_2}\hat{Z}^B, \\
\hat{\sigma}_{11}^{AB} &:= {}_{4C_1C_2}\langle\Psi^-|\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}|\Psi^-\rangle_{C_1C_2} = \hat{Z}^B\hat{X}^B {}_{C_1C_2}\langle\Phi^+|\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}|\Phi^+\rangle_{C_1C_2}\hat{X}^B\hat{Z}^B.
\end{aligned} \tag{6.4}$$

Therefore, the entanglement connection on Bell-diagonal states $\hat{\rho}_1 \otimes \hat{\rho}_2$ returns $\hat{\sigma}_{lk}^{AB}$ according to outcome lk.

6.1.2.2 Entanglement connection by Bell measurement based on the realistic RNPM protocol

Let us consider to connect two Bell diagonal states $\hat{\rho}_1^{AC_1} \otimes \hat{\rho}_2^{C_2B}$ by the realistic Bell measurement $\{B_{\tau,\tau,\eta,N,\alpha,lij}^{C_1C_2}\}_{i,j=0,\ldots,N+1;\, l=0,1}$. Here τ represents the net transmittance of the local optical channel. As can be seen from Figs. 5.10 and 5.11, when $i+j>0$, the realistic Bell measurement $B_{\tau,\tau,\eta,N,\alpha,lij}^{C_1C_2}$ is the same as the ideal Bell measurement $\hat{B}_{lk(ij)}^{C_1C_2}$ following $\Lambda^A_{r(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha)} \otimes \Lambda^B_{r(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha)}\Lambda^{i+j,B}_{2t(N,\alpha)-1}$. Hence, in the case of the success of the Bell measurement ($i+j>0$), from the equivalence in Fig. A2.2, the remaining state is $\Lambda^A_{r^2(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha)}\Lambda^{i+j,A}_{2t(N,\alpha)-1}(\hat{\sigma}^{AB}_{lk(ij)})$, where states $\{\hat{\sigma}_{lk}^{AB}\}_{k,l=0,1}$ are defined by Eqs. (6.3) and (6.4). Therefore, the successful operation works as the entanglement connection having a phase error. The phase error rate changes, dependently on whether outcome ij satisfies $i+j=N+1$, because $\Lambda^{i+j,A}_{2t(N,\alpha)-1} = I$ for $0 < i+j \le N$ and $\Lambda^{i+j,A}_{2t(N,\alpha)-1} = \Lambda^A_{2t(N,\alpha)-1}$ for $i+j=N+1$. Here, the failure outcome ($i+j=0$) of the Bell measurement $\{B_{\tau,\tau,\eta,N,\alpha,lij}^{C_1C_2}\}_{i,j=0,\ldots,N+1;\, l=0,1}$ occurs with probability $|\langle 0|\beta(\alpha)\rangle|^2 = r(\alpha) = e^{-2\alpha^2\sin^2(\theta/2)}$.

6.1.3 Entanglement distillation based on the realistic RNPM protocol

Suppose that, in the recurrence method for Bell-diagonal state $\hat{\rho}_1{}^{A_1B_1} \otimes \hat{\rho}_2{}^{A_2B_2}$, Alice (Bob) uses the realistic parity check measurement $\{\hat{R}^{A_1A_2\to A_2}_{\tau,\tau,\eta,N,\alpha,ij}\}_{i,j=0,\ldots,N+1}$ ($\{\hat{R}^{B_1B_2\to B_2}_{\tau,\tau,\eta,N,\alpha,lm}\}_{l,m=0,\ldots,N+1}$). Here τ represents the net transmittance of the local optical channel. Then, from Figs. 5.8 and 5.9, the recurrence method succeeds with probability

$$[1-r(\alpha)]^2 P_s^d, \tag{6.5}$$

and the remaining state is

$$\Lambda^{A_2}_{r^2(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha)}\Lambda^{i+j,A_2}_{2t(N,\alpha)-1}\otimes\Lambda^{B_2}_{r^2(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha)}\Lambda^{l+m,B_2}_{2t(N,\alpha)-1}(\hat{\sigma}^{A_2B_2}), \tag{6.6}$$

where $i+j>0$, $l+m>0$, P_s^d is defined by Eq. (2.49), and $\hat{\sigma}^{A_2B_2}$ is the Bell-diagonal state defined by Eq. (2.48). Therefore, the distillation from Bell-diagonal state $\hat{\rho}_1{}^{A_1B_1}\otimes\hat{\rho}_2{}^{A_2B_2}$ can be achievable even by the realistic Bell measurement $\{B^{C_1C_2}_{\tau,\tau,\eta,N,\alpha,lij}\}_{i,j=0,\ldots,N+1;\,l=0,1}$, if one allows the mixture of a phase error. The phase error rates depend on outcomes ij and lm, because $\Lambda^k_{2t(N,\alpha)-1}=I$ for $0\le k\le N$ and $\Lambda^k_{2t(N,\alpha)-1}=\Lambda_{2t(N,\alpha)-1}$ for $k=N+1$.

6.2 Quantum repeaters with entanglement generation and entanglement connection

We consider a quantum repeater protocol [31] composed of entanglement generation and entanglement connection. Suppose that Alice and Bob want to communicate over distance $L=2^nL_0$. In the protocol, 2^n-1 nodes with a repeater are set at intervals L_0 between Alice and Bob, and they begin with entanglement generation between quantum memories at neighboring nodes. Once the generation protocols make neighboring entangled pairs with length L_0, by implementing entanglement connection of the pairs, they try to generate an entangled pair with length $2L_0$. Similarly, the jth ($j=1,2,3,\ldots,n$) entanglement connection receives two neighboring entangled pairs with length $2^{j-1}L_0$, and returns an entangled pair with 2^jL_0. Hence, at the end of the nth entanglement connection, they will obtain an entangle pair between A and B.

Let us estimate the time needed to generate the entangled pair AB. Considering that the entanglement generation protocol succeeds with probability $P_s^{(0)}$, the average time needed to make the entanglement generation protocol succeed is proportional to $1/P_s^{(0)}$. Similarly, by assuming that the jth entanglement connection succeeds with probability $P_s^{(j)}$, the average time needed to make the jth entanglement connection succeed is proportional to $1/P_s^{(j)}$. Since the first entanglement connection (jth entanglement connection) can start after the success of neighboring entanglement generation protocols (after the success of $(j-1)$th entanglement connections), the total time needed to make entanglement between AB will scale as $1/(\prod_{j=0,\ldots,n}P_s^{(j)})$. In fact, the total time $T^{\rm tot}$ is approximately described [36] by

$$T^{\rm tot}\simeq\frac{L_0}{c}\left(\frac{3}{2}\right)^n\frac{1}{\prod_{j=0,\ldots,n}P_s^{(j)}}=:T, \tag{6.7}$$

where L_0/c is the communication time in the entanglement generation, and the operation time of local manipulations is ignored.

In what follows, we consider a protocol parametrized by Fig, 6.1. In this protocol, we use the RNPM protocols $\{P_{T_A,T_B,\eta,N,\alpha_g,ij}\}_{i,j=0,\ldots,N+1}$ for entanglement generation, and the realistic Bell measurements $\{B_{\tau,\tau,\eta,N,\alpha_s,lij}\}_{i,j=0,\ldots,N+1;\,l=0,1}$ for entanglement connection, where τ represents the transmittance of the local optical channel, and T_A and T_B are defined by Eq. (6.1). In what follows, we estimate the time T by allowing the use of photon detectors with $N=\infty$, $N=1$, and $N=0$. From Figs. 5.7, 5.11 and A2.1, this protocol is shown to be equivalent to the Fig. 6.2 in the case of $i_1+j_1,\ldots,i_{2^n}+j_{2^n},i'_1+j'_1,\ldots,i'_{2^n-1}+j'_{2^n-1}>0$.

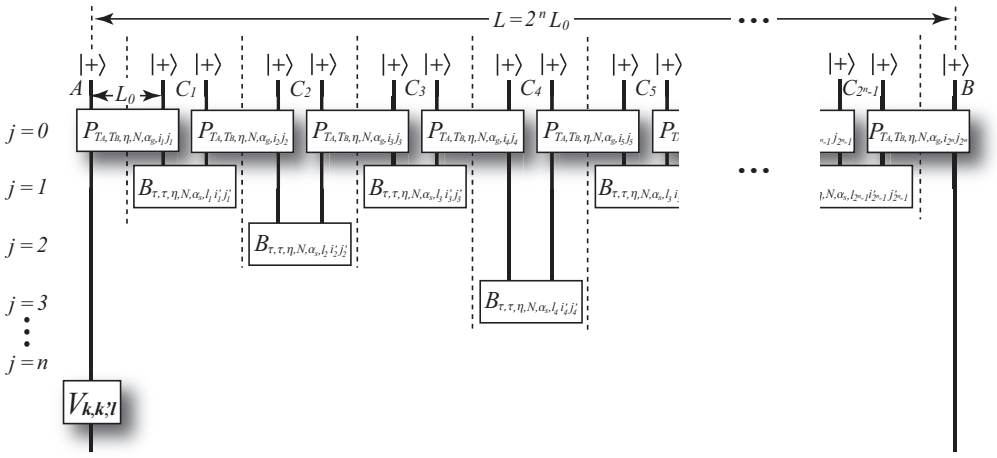

Fig. 6.1. Quantum repeaters based on the entanglement generation and the entanglement connection. $\boldsymbol{k} := (k(i_1, j_1), k(i_2, j_2), \ldots, k(i_{2^n}, j_{2^n}))$, $\boldsymbol{k}' := (k(i'_1, j'_1), k(i'_2, j'_2), \ldots, k(i'_{2^n-1}, j'_{2^n-1}))$, and $\boldsymbol{l} := (l_1, l_2, \ldots, l_{2^n-1})$, where $k(i, j)$ is one defined by Eq. (5.39). $\hat{V}_{\boldsymbol{k},\boldsymbol{k}',\boldsymbol{l}}$ is a unitary operation to transform the state obtained in the success cases into a standard state $F|\Phi^+\rangle\langle\Phi^+|_{AB} + (1-F)|\Phi^-\rangle\langle\Phi^-|_{AB}$.

6.2.1 The repeaters with photon-number-resolving detectors ($N = \infty$)

Here we suppose that the RNPM protocols use photon-number-resolving detectors, i.e., $N = \infty$. In this case, entanglement generation succeeds with $P_s^{(0)} = 1 - r(\alpha_g)$, and the jth entanglement connection succeeds with $P_s^{(j)} = 1 - r(\alpha_s)$. Hence, we have

$$\frac{1}{\prod_{j=0,\ldots,n} P_s^{(j)}} = \frac{1}{[1-r(\alpha_g)][1-r(\alpha_s)]^n} = \frac{1}{[1-r(\alpha_g)][1-r(\alpha_s)]^n}. \tag{6.8}$$

On the other hand, since $N = \infty$ implies $\Lambda^k_{2t(N,\alpha_g)-1} = \Lambda^k_{2t(N,\alpha_s)-1} = I$ for any k, Fig. 6.2 shows that, by a suitable choice of the unitary operation $\hat{V}_{\boldsymbol{k}',\boldsymbol{k},\boldsymbol{l}}$, the protocol returns an entangled state in the form of

$$F|\Phi^+\rangle\langle\Phi^+|_{AB} + (1-F)|\Phi^-\rangle\langle\Phi^-|_{AB}, \tag{6.9}$$

with

$$\begin{aligned} F =& \frac{1 + r^{2^n}(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha_g) r^{2^n}(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha_g) r^{2(2^n-1)}(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha_s)}{2} \\ =& \frac{1 + r^{2^n\left(\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta}\right)}(\alpha_g) r^{(2^n-1)\left(\frac{2-2\tau\eta}{\tau\eta}\right)}(\alpha_s)}{2}. \end{aligned} \tag{6.10}$$

In order to clarify the relation between T and F, we introduce parameters defined by

$$\begin{aligned} f_g :=& r^{2^n\left(\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta}\right)}(\alpha_g), \\ f_s :=& r^{(2^n-1)\left(\frac{2-2\tau\eta}{\tau\eta}\right)}(\alpha_s). \end{aligned} \tag{6.11}$$

By these parameters, Eqs. (6.10) and (6.14) are rewritten as

$$2F - 1 = f_g f_s, \tag{6.12}$$

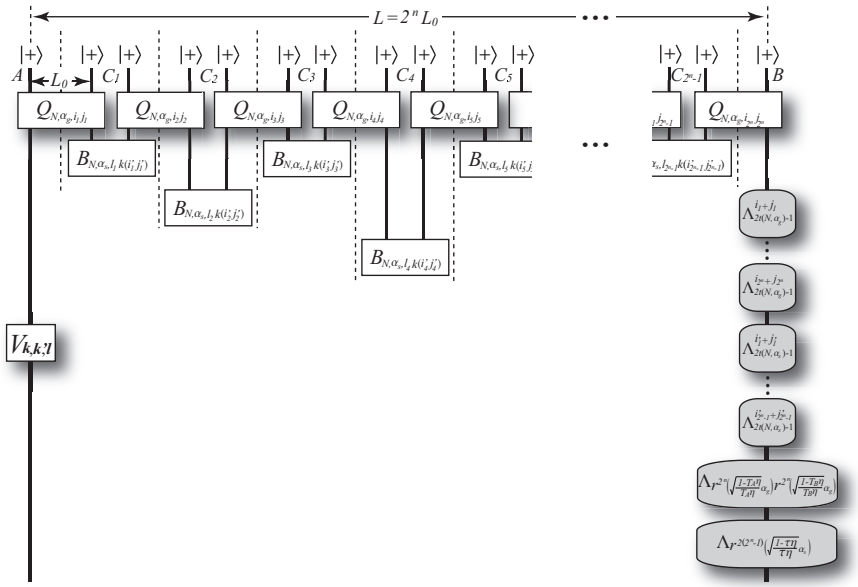

Fig. 6.2. An imaginary protocol equivalent to Fig. 6.1 in the case of $i_1+j_1,\ldots,i_{2^n}+j_{2^n},i_1'+j_1',\ldots,i_{2^n-1}'+j_{2^n-1}'>0$.

and

$$
\begin{aligned}
T =& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{1}{\left(1-f_g^{\frac{1}{2^n}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta}}\right)\left(1-f_s^{\frac{1}{2^n-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)}\right)^n} \\
=& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{1}{\left[1-\exp\left(\frac{\ln f_g}{2^n}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta}\right)\right]\left[1-\exp\left(\frac{\ln f_s}{2^n-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)\right)\right]^n} \\
=& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{2^n}{\ln f_g}\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta} g\left(\frac{\ln f_g}{2^n}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta}\right) \\
& \times\left[\frac{2^n-1}{\ln f_s}\left(\frac{2-2\tau\eta}{\tau\eta}\right) g\left(\frac{\ln f_s}{2^n-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)\right)\right]^n \\
=& \frac{L_0}{c}\left(\frac{3}{2}\right)^{\log_2(L/L_0)} \frac{(L/L_0)}{\ln f_g}\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta} g\left(\frac{\ln f_g}{(L/L_0)}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta}\right) \\
& \times\left[\frac{(L/L_0)-1}{\ln f_s}\left(\frac{2-2\tau\eta}{\tau\eta}\right) g\left(\frac{\ln f_s}{(L/L_0)-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)\right)\right]^{\log_2(L/L_0)},
\end{aligned}
\tag{6.13}
$$

with $g(x) := x/(1-e^x)$. Because $g(x)\to 1$ in the limit of $x\to 0$, Eq. (6.13) shows that T increases sub-exponentially with L. In fact, the minimum time to generate entanglement of Eq. (6.9) over distance L is determined by minimizing T of Eq. (6.13) for parameters f_g and f_s satisfying Eq. (6.12) and for parameter n. Figure 6.3 indicates the minimum time T for given distance L and fidelity F.

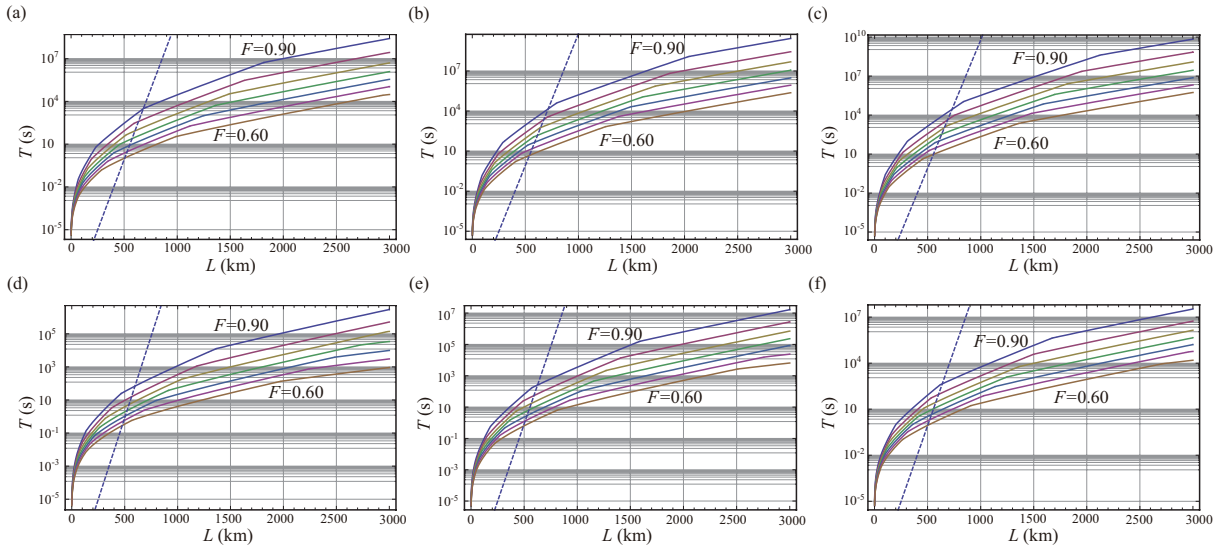

Fig. 6.3. The minimum time T needed to generate entanglement with $0.60 \leq F \leq 0.90$ in increments of 0.05 over distance L under the use of detectors with $N = \infty$; (a) $l_A = L_0/2$, $\tau = 0.98$, and $\eta = 0.95$; (b) $l_A = L_0/2$, $\tau = 0.98$, and $\eta = 0.90$; (c) $l_A = L_0/2$, $\tau = 0.95$, and $\eta = 0.90$; (d) $l_A = L_0$, $\tau = 0.98$, and $\eta = 0.95$; (e) $l_A = L_0$, $\tau = 0.98$, and $\eta = 0.90$; (f) $l_A = L_0$, $\tau = 0.95$, and $\eta = 0.90$. We assume $c = 2 \times 10^8$ m/s, $L_{\rm att} = 22$ km. The dashed line indicates $1/(f\eta e^{-L/L_{\rm att}})$ with $f = 10$ GHz, which is the direct transmission time of the photon from 10 GHz single photon source.

6.2.2 The repeaters with single photon detectors ($N = 1$)

Here we suppose that the RNPM protocols use single-photon detectors, i.e., $N = 1$. For simplicity, we regard, as the success cases, only the events where one of single photon detectors in the RNPM protocol announces the arrival of a single photon. Then, entanglement generation succeeds with $P_s^{(0)} = |\langle 1|\beta(\alpha_g)\rangle|^2 = -r(\alpha_g)\ln r(\alpha_g)$, and the jth entanglement connection succeeds with $P_s^{(j)} = -r(\alpha_s)\ln r(\alpha_s)$. Hence, we have

$$\frac{1}{\prod_{j=0,\ldots,n} P_s^{(j)}} = \frac{1}{[-r(\alpha_g)\ln r(\alpha_g)][-r(\alpha_s)\ln r(\alpha_s)]^n}. \tag{6.14}$$

On the other hand, since $\Lambda^1_{2t(1,\alpha_g)-1} = I$ and $\Lambda^1_{2t(1,\alpha_s)-1} = I$, Fig. 6.2 shows that, by a suitable choice of the unitary operation $\hat{V}_{\boldsymbol{k}',\boldsymbol{k},\boldsymbol{l}}$, the protocol returns an entangled state in the form of

$$F|\Phi^+\rangle\langle\Phi^+|_{AB} + (1-F)|\Phi^-\rangle\langle\Phi^-|_{AB}, \tag{6.15}$$

with

$$\begin{aligned} F &= \frac{1 + r^{2^n}(\sqrt{(1-T_A\eta)/(T_A\eta)}\alpha_g) r^{2^n}(\sqrt{(1-T_B\eta)/(T_B\eta)}\alpha_g) r^{2(2^n-1)}(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha_s)}{2} \\ &= \frac{1 + r^{2^n\left(\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta}\right)}(\alpha_g) r^{(2^n-1)\left(\frac{2-2\tau\eta}{\tau\eta}\right)}(\alpha_s)}{2}. \end{aligned} \tag{6.16}$$

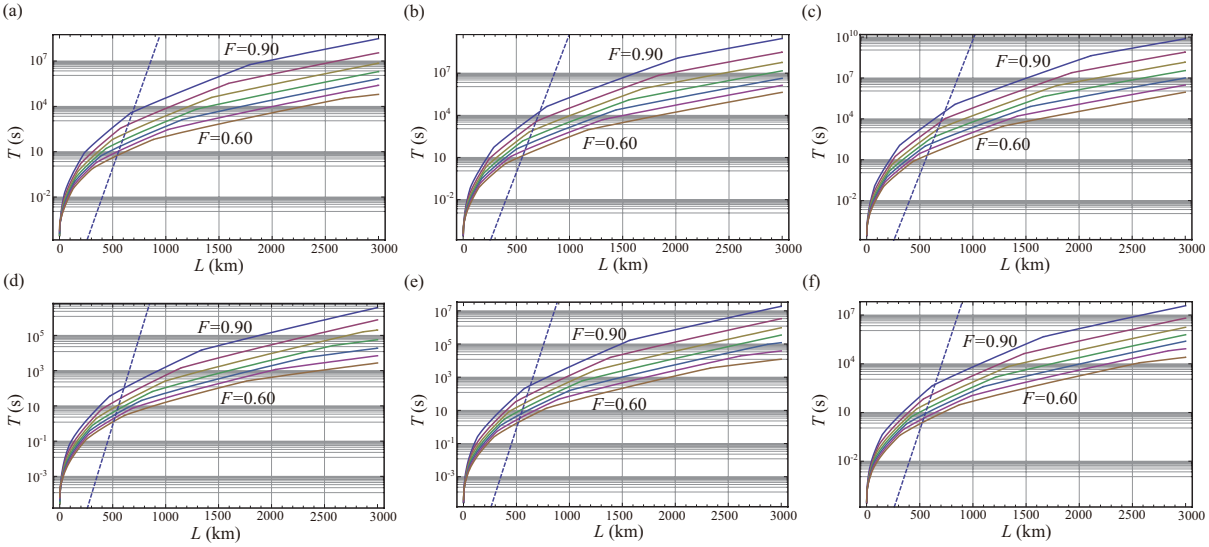

Fig. 6.4. The minimum time T needed to generate entanglement with $0.60 \leq F \leq 0.90$ in increments of 0.05 over distance L under the use of detectors with $N = 1$; (a) $l_A = L_0/2$, $\tau = 0.98$, and $\eta = 0.95$; (b) $l_A = L_0/2$, $\tau = 0.98$, and $\eta = 0.90$; (c) $l_A = L_0/2$, $\tau = 0.95$, and $\eta = 0.90$; (d) $l_A = L_0$, $\tau = 0.98$, and $\eta = 0.95$; (e) $l_A = L_0$, $\tau = 0.98$, and $\eta = 0.90$; (f) $l_A = L_0$, $\tau = 0.95$, and $\eta = 0.90$. We assume $c = 2 \times 10^8$ m/s, $L_{\rm att} = 22$ km. The dashed line indicates $1/(f\eta e^{-L/L_{\rm att}})$ with $f = 10$ GHz, which is the direct transmission time of the photon from 10 GHz single photon source.

In order to clarify the relation between T and F, we introduce parameters defined by

$$\begin{aligned} f_g :=& r^{2^n\left(\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta}\right)}(\alpha_g), \\ f_s :=& r^{(2^n-1)\left(\frac{2-2\tau\eta}{\tau\eta}\right)}(\alpha_s). \end{aligned} \tag{6.17}$$

By these parameters, Eqs. (6.16) and (6.14) are rewritten as

$$2F - 1 = f_g f_s, \tag{6.18}$$

and

$$\begin{aligned} T =& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{1}{\left(\frac{-1}{2^n}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta} f_g^{\frac{1}{2^n}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta}} \ln f_g\right)\left(\frac{-1}{2^n-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right) f_s^{\frac{1}{2^n-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)} \ln f_s\right)^n} \\ =& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{2^n}{(-\ln f_g)}\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta} f_g^{-\frac{1}{2^n}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta}} \\ & \times \left[\frac{2^n-1}{(-\ln f_s)}\left(\frac{2-2\tau\eta}{\tau\eta}\right) f_s^{-\frac{1}{2^n-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)}\right]^n \\ =& \frac{L_0}{c}\left(\frac{3}{2}\right)^{\log_2(L/L_0)} \frac{(L/L_0)}{(-\ln f_g)}\frac{T_A+T_B-2T_AT_B\eta}{T_AT_B\eta} f_g^{-\frac{1}{(L/L_0)}\frac{T_AT_B\eta}{T_A+T_B-2T_AT_B\eta}} \\ & \times \left[\frac{(L/L_0)-1}{(-\ln f_s)}\left(\frac{2-2\tau\eta}{\tau\eta}\right) f_s^{-\frac{1}{(L/L_0)-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)}\right]^{\log_2(L/L_0)}. \end{aligned} \tag{6.19}$$

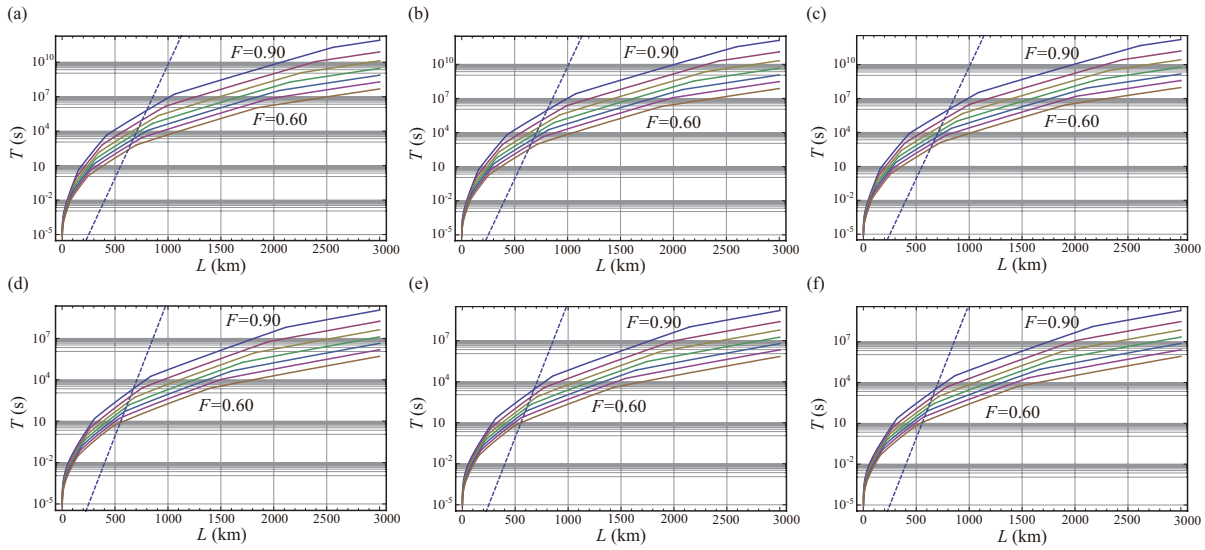

Fig. 6.5. The minimum time T needed to generate entanglement with $0.60 \leq F \leq 0.90$ in increments of 0.05 over distance L under the use of detectors with $N = 0$; (a) $l_A = L_0/2$, $\tau = 0.98$, and $\eta = 0.95$; (b) $l_A = L_0/2$, $\tau = 0.98$, and $\eta = 0.90$; (c) $l_A = L_0/2$, $\tau = 0.95$, and $\eta = 0.90$; (d) $l_A = L_0$, $\tau = 0.98$, and $\eta = 0.95$; (e) $l_A = L_0$, $\tau = 0.98$, and $\eta = 0.90$; (f) $l_A = L_0$, $\tau = 0.95$, and $\eta = 0.90$. We assume $c = 2 \times 10^8$ m/s, $L_{\rm att} = 22$ km. The dashed line indicates $1/(f\eta e^{-L/L_{\rm att}})$ with $f = 10$ GHz, which is the direct transmission time of the photon from 10 GHz single photon source.

Since $f_g^{-\frac{1}{(L/L_0)}\frac{T_A T_B \eta}{T_A+T_B-2T_A T_B\eta}} \to 1$ and $f_s^{-\frac{1}{(L/L_0)-1}\left(\frac{\tau\eta}{2-2\tau\eta}\right)} \to 1$ in the limit of $L \to \infty$, Eq. (6.19) shows that T increases sub-exponentially with L. In practice, the minimum time to generate entanglement of Eq. (6.15) over distance L is determined by minimizing T of Eq. (6.19) for parameters f_g and f_s satisfying Eq. (6.18) and for parameter n. Figure 6.4 indicates the minimum time T for given distance L and fidelity F.

6.2.3 The repeaters with threshold detectors ($N = 0$)

Here we suppose that the RNPM protocols use threshold detectors, i.e., $N = 0$. In this case, entanglement generation succeeds with $P_s^{(0)} = 1 - r(\alpha_g)$, and the jth entanglement connection succeeds with $P_s^{(j)} = 1 - r(\alpha_s)$. Hence, we have

$$\frac{1}{\prod_{j=0,\ldots,n} P_s^{(j)}} = \frac{1}{[1-r(\alpha_g)][1-r(\alpha_s)]^n} = \frac{1}{[1-r(\alpha_g)][1-r(\alpha_s)]^n}. \tag{6.20}$$

From $t_e(0,\alpha) = (1 - e^{-|\beta(\alpha)|^2})/2$, we have

$$2t(0,\alpha) - 1 = 2[1 - t_e(0,\alpha)] - 1 = e^{-|\beta(\alpha)|^2} = r(\alpha). \tag{6.21}$$

Hence, $\Lambda^k_{2t(0,\alpha_g)-1} = \Lambda_{r(\alpha_g)}$ and $\Lambda^k_{2t(0,\alpha_s)-1} = \Lambda_{r(\alpha_s)}$ hold for $k \geq 1$, implying that the protocol returns an entangled state in the form of

$$F|\Phi^+\rangle\langle\Phi^+|_{AB} + (1-F)|\Phi^-\rangle\langle\Phi^-|_{AB}, \tag{6.22}$$

with

$$F = \frac{1 + r^{2^n\left(\frac{T_A+T_B-T_AT_B\eta}{T_AT_B\eta}\right)}(\alpha_g) r^{(2^n-1)\left(\frac{2-\tau\eta}{\tau\eta}\right)}(\alpha_s)}{2}. \tag{6.23}$$

In order to clarify the relation between T and F, we introduce parameters defined by

$$\begin{aligned} f_g :=& r^{2^n\left(\frac{T_A+T_B-T_AT_B\eta}{T_AT_B\eta}\right)}(\alpha_g), \\ f_s :=& r^{(2^n-1)\left(\frac{2-\tau\eta}{\tau\eta}\right)}(\alpha_s). \end{aligned} \tag{6.24}$$

By these parameters, Eqs. (6.23) and (6.20) are rewritten as

$$2F - 1 = f_g f_s, \tag{6.25}$$

and

$$\begin{aligned} T =& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{1}{\left(1 - f_g^{\frac{1}{2^n}\frac{T_AT_B\eta}{T_A+T_B-T_AT_B\eta}}\right)\left(1 - f_s^{\frac{1}{2^n-1}\left(\frac{\tau\eta}{2-\tau\eta}\right)}\right)^n} \\ =& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{1}{\left[1 - \exp\left(\frac{\ln f_g}{2^n}\frac{T_AT_B\eta}{T_A+T_B-T_AT_B\eta}\right)\right]\left[1 - \exp\left(\frac{\ln f_s}{2^n-1}\left(\frac{\tau\eta}{2-\tau\eta}\right)\right)\right]^n} \\ =& \frac{L_0}{c}\left(\frac{3}{2}\right)^n \frac{2^n}{\ln f_g}\frac{T_A+T_B-T_AT_B\eta}{T_AT_B\eta} g\left(\frac{\ln f_g}{2^n}\frac{T_AT_B\eta}{T_A+T_B-T_AT_B\eta}\right) \\ & \times \left[\frac{2^n-1}{\ln f_s}\left(\frac{2-\tau\eta}{\tau\eta}\right) g\left(\frac{\ln f_s}{2^n-1}\left(\frac{\tau\eta}{2-\tau\eta}\right)\right)\right]^n \\ =& \frac{L_0}{c}\left(\frac{3}{2}\right)^{\log_2(L/L_0)} \frac{(L/L_0)}{\ln f_g}\frac{T_A+T_B-T_AT_B\eta}{T_AT_B\eta} g\left(\frac{\ln f_g}{(L/L_0)}\frac{T_AT_B\eta}{T_A+T_B-T_AT_B\eta}\right) \\ & \times \left[\frac{(L/L_0)-1}{\ln f_s}\left(\frac{2-\tau\eta}{\tau\eta}\right) g\left(\frac{\ln f_s}{(L/L_0)-1}\left(\frac{\tau\eta}{2-\tau\eta}\right)\right)\right]^{\log_2(L/L_0)}, \end{aligned} \tag{6.26}$$

with $g(x) := x/(1 - e^x)$. Because $g(x) \to 1$ in the limit of $x \to 0$, Eq. (6.26) shows that T increases sub-exponentially with L. Actually, the minimum time to generate entanglement of Eq. (6.22) over distance L is determined by minimizing T of Eq. (6.26) for parameters f_g and f_s satisfying Eq. (6.25) and for parameter n. Figure 6.5 indicates the minimum time T for given distance L and fidelity F.

6.2.4 Summary

In this section, we have shown that long-distance quantum communication is efficiently implementable only by the RNPM protocols. In particular, the time needed to generate an entangled pair increases only sub-exponentially with the distance, irrespectively of the types of the used photon detectors. This sub-exponential increase of the time ensures that the quantum repeater protocols are more efficient than quantum communication based on the direct transmission of photons for long distances. These facts can be also represented by Figs. 6.3-6.5†. As can be seen by comparing Fig. 6.3 with Fig. 6.4, the protocol based on single photon detectors ($N = 1$) has

† Note that the repetition rate of the single photon source assumed in those figures, i.e., 10 GHz, is a very ambitious value [36].

the performance comparable with one based on photon-number-resolving detectors ($N = \infty$). On the other hand, from Figs. 6.4 and 6.5, the protocol based on threshold detectors ($N = 0$) is rather inferior to one based on single photon detectors, but even the protocol with $N = 0$ exceeds quantum communication based on the direct transmission of photons in efficiencies for distances $L \gtrsim 900$ km. In addition, from Figs. 6.3-6.5, the performance of the repeater protocol with $l_A = L_0/2$ is rather superior to one with $l_A = L_0$.

The repeater protocol used here has two favorable properties: (i) It is sufficient that each repeater at a node has two quantum memories at least; (ii) As long as the error of the detectors comes from non-unity quantum efficiencies, the generated entanglement includes only one type of error (see Eqs. (6.9), (6.15), and (6.22)). Property (ii) implies that the obtained entanglement is of good quality. In fact, for the state with fidelity F, the formula of unconditionally secure key rate of the entanglement-based quantum key distribution protocol is proportional to $1 - h(F)$ with the binary entropy function $h(x) := -x \log_2 x - (1-x)\log_2(1-x)$, which implies that the secret key is distillable for any $F > 1/2$. Therefore, the quantum repeater protocol presented here is realistic and efficient for achieving long-distance quantum communication.

6.3 Quantum repeaters based on the nested purification protocol

As seen in the previous section, by a quantum repeater protocol that utilizes only entanglement generation and entanglement connection, we can overcome the photon loss of the transmission channel. However, in practice, other types of noises may be caused by imperfection of physical devices such as quantum memories. To beat such additional errors, we will need entanglement distillation. Actually, entanglement distillation will be also useful for the satellite-based quantum communication. In the satellite-based quantum communication, a ground station tries to accomplish quantum communication with another ground station by exchanging photons between a satellite and the ground stations in the night. If one of the ground stations is in the day, the satellite needs to store quantum information of the photons in quantum memories until the station becomes in the night, but, in general, quantum memories have several types of noises, which implies that such satellite-based quantum communication will also need entanglement distillation.

In this section, we show that the recurrence method based on the RNPM protocols works. In addition, by the recurrence method, we can also implement the *nested-purification repeater protocol* [28, 29] whose cost scales as the distance only polynomially.

6.3.1 The realistic recurrence method on Werner states

Here we show that the recurrence method based on the RNPM protocols can work for Werner states. This fact ensures that the method has the possibility to recover entangled states with multiple types of error, because any bipartite state can be converted into a Werner state.

Suppose that Alice and Bob share a system in Werner states $\hat{\rho}_W^{A_1B_1} \otimes \hat{\rho}_W^{A_2B_2}$ of Eq. (2.53), and apply the realistic parity check measurements $\{\hat{R}^{A_1A_2\to A_2}_{\tau,\tau,\eta,N,\alpha_d,ij} \otimes \hat{R}^{B_1B_2\to B_2}_{\tau,\tau,\eta,N,\alpha_d,lm}\}_{i,j,l,m=0,\ldots,N+1}$ on it. According to Sec. 6.1.3, in the case of $i + j > 0$ and $l + m > 0$, the left state has the fidelity

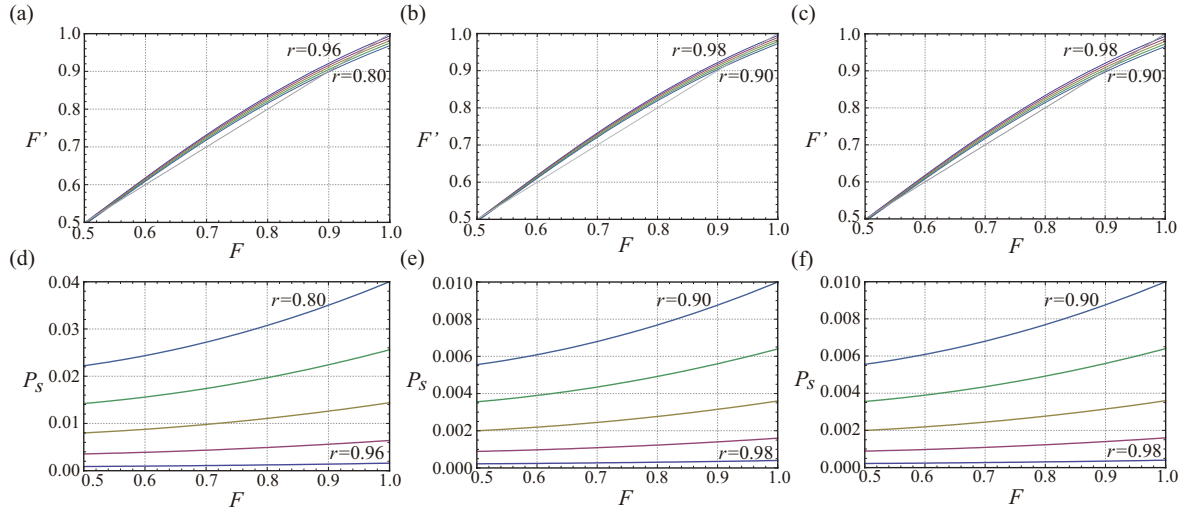

Fig. 6.6. The efficiencies of the recurrence method based on the RNPM protocols with $N = \infty$ as a function of fidelity F of the Werner state to Bell state $|\Phi^+\rangle$: (a) the fidelity F' of the left qubits to a Bell state and (d) the success probability P_s, for $\eta = 0.98$, $\tau = 0.95$, and $r(\alpha_d) = 0.96, 0.92, 0.88, 0.84, 0.80$; (b) the fidelity F' of the left qubits to Bell state $|\Phi^+\rangle$ and (e) the success probability P_s, for $\eta = 0.98$, $\tau = 0.90$, and $r(\alpha_d) = 0.98, 0.96, 0.94, 0.92, 0.90$; (c) the fidelity F' of the left qubits to Bell state $|\Phi^+\rangle$ and (f) the success probability P_s, for $\eta = 0.95$, $\tau = 0.90$, and $r(\alpha_d) = 0.98, 0.96, 0.94, 0.92, 0.90$.

described by

$$F'(F) := \langle\Phi^+|\Lambda^{A_2}_{r^2(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha_d)}\Lambda^{i+j,A_2}_{2t(N,\alpha_d)-1} \otimes \Lambda^{B_2}_{r^2(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha_d)}\Lambda^{l+m,B_2}_{2t(N,\alpha_d)-1}(\hat{\sigma}_W^{A_2B_2})|\Phi^+\rangle$$

$$= \begin{cases} \frac{1+r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)}{2}\frac{10F^2-2F+1}{8F^2-4F+5} + \frac{1-r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)}{2}\frac{6F(1-F)}{8F^2-4F+5}, \\ \qquad (0 < i+j \le N,\ 0 < l+m \le N), \\ \frac{1+r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)(2t(N,\alpha_d)-1)}{2}\frac{10F^2-2F+1}{8F^2-4F+5} + \frac{1-r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)(2t(N,\alpha_d)-1)}{2}\frac{6F(1-F)}{8F^2-4F+5}, \\ \qquad (i+j = N+1,\ 0 < l+m \le N), \\ \frac{1+r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)(2t(N,\alpha_d)-1)}{2}\frac{10F^2-2F+1}{8F^2-4F+5} + \frac{1-r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)(2t(N,\alpha_d)-1)}{2}\frac{6F(1-F)}{8F^2-4F+5}, \\ \qquad (0 < i+j \le N,\ l+m = N+1), \\ \frac{1+r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)(2t(N,\alpha_d)-1)^2}{2}\frac{10F^2-2F+1}{8F^2-4F+5} + \frac{1-r^4\left(\frac{1-\tau\eta}{\tau\eta}\right)(\alpha_d)(2t(N,\alpha_d)-1)^2}{2}\frac{6F(1-F)}{8F^2-4F+5}, \\ \qquad (i+j = N+1,\ l+m = N+1), \end{cases} \tag{6.27}$$

where $\hat{\sigma}_W^{A_2B_2}$ is the state defined by Eq. (2.54). This state may be converted to a Werner state with the fidelity F' before being fed to the subsequent operations such as the entanglement distillation or the entanglement connection. In Fig. 6.6 (Fig. 6.8), assuming the use of photon detectors with $N = \infty$ ($N = 0$), we depict the efficiencies of this recurrence method. In these cases, the success probability is described by Eq. (6.5), namely by

$$[1 - r(\alpha_d)]^2 P^d_{s,W} = \frac{[1 - r(\alpha_d)]^2(8F^2 - 4F + 5)}{9}, \tag{6.28}$$

where we used Eq. (2.55). In Fig. 6.7, we show the efficiencies of the recurrence method based

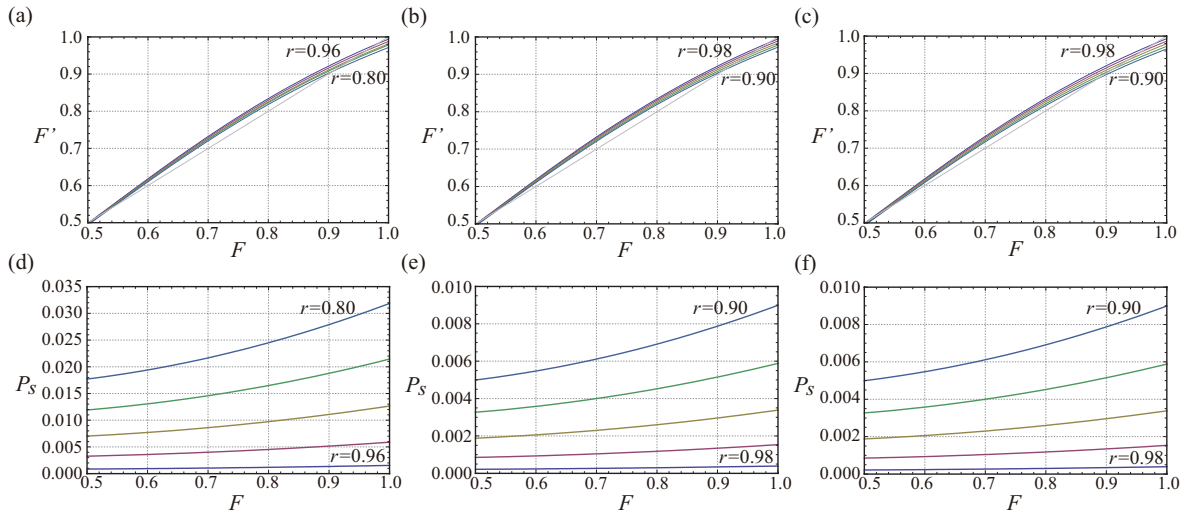

Fig. 6.7. The efficiencies of the recurrence method based on the RNPM protocols with $N = 1$ as a function of fidelity F of the Werner state to Bell state $|\Phi^+\rangle$: (a) the fidelity F' of the left qubits to a Bell state and (d) the success probability P_s, for $\eta = 0.98$, $\tau = 0.95$, and $r(\alpha_d) = 0.96, 0.92, 0.88, 0.84, 0.80$; (b) the fidelity F' of the left qubits to Bell state $|\Phi^+\rangle$ and (e) the success probability P_s, for $\eta = 0.98$, $\tau = 0.90$, and $r(\alpha_d) = 0.98, 0.96, 0.94, 0.92, 0.90$; (c) the fidelity F' of the left qubits to Bell state $|\Phi^+\rangle$ and (f) the success probability P_s, for $\eta = 0.95$, $\tau = 0.90$, and $r(\alpha_d) = 0.98, 0.96, 0.94, 0.92, 0.90$.

on photon detectors with $N = 1$, regarding the event of $i + j = 1$ and $l + m = 1$ as the only success case. In this case, the success probability is

$$[-r(\alpha_d)\ln r(\alpha_d)]^2 P_{s,W}^d = \frac{[-r(\alpha_d)\ln r(\alpha_d)]^2(8F^2 - 4F + 5)}{9}. \tag{6.29}$$

Figures 6.6, 6.7, and 6.8 suggest the existence of two threshold fidelities $F_{\min}$ and $F_{\max}$ such that

$$\begin{aligned} &F'(F_{\min}) = F_{\min}, \\ &F'(F_{\max}) = F_{\max}, \\ &F'(F) > F, \ (F_{\min} < F < F_{\max}). \end{aligned} \tag{6.30}$$

The threshold fidelities are controllable by choosing amplitude α_d. In particular, for sufficiently small α_d, i.e., $r(\alpha_d) \simeq 1$, $F'(F)$ comes closer to the ideal relation of Fig. 2.5. Therefore, by properly selecting amplitude α_d, the recurrence method based on the realistic RNPM protocol can distill an almost Bell pair.

6.3.2 Entanglement connection of Werner states by the realistic RNPM protocol

In order to see that a longer entangled pair can be obtained by connecting entangled states with multiple types of error, here we consider entanglement connections of Werner states by the realistic RNPM protocols. Let us consider the protocol of Fig. 6.9 (a) to connect 2^n pairs in Werner states of Eq. (2.53). We start with noting an equivalence in Fig. 6.9 that is similar to the equivalence between Figs. 6.1 and 6.2. The equivalence is shown by the combination of Fig. A2.2 and the fact that entanglement connection of Bell diagonal states returns a Bell diagonal state (see Sec. 6.1.2.1). Fig. 6.9 (b) suggests that the success of all the realistic Bell measurements

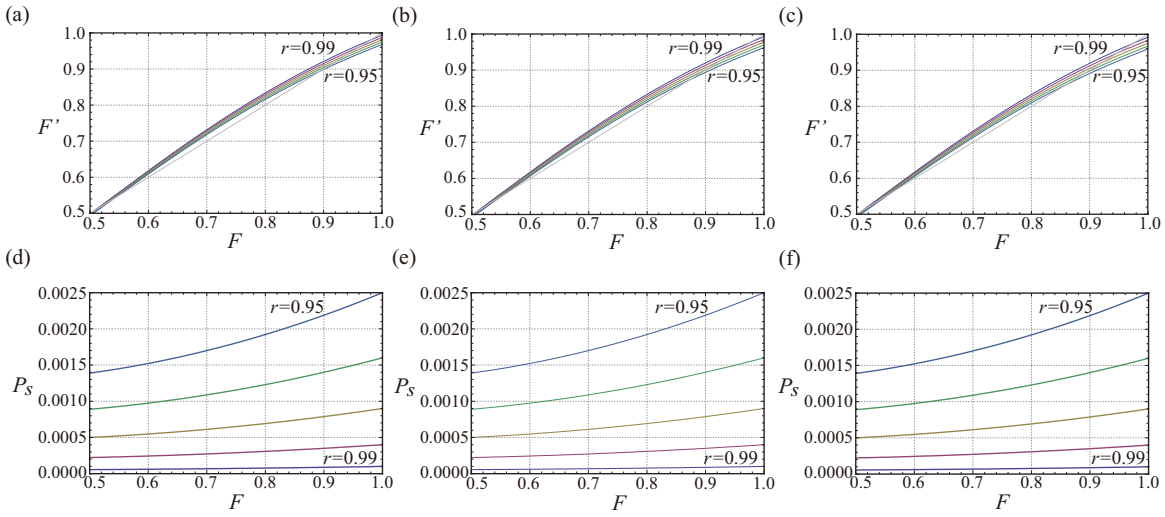

Fig. 6.8. The efficiencies of the recurrence method based on the RNPM protocols with $N = 0$ as a function of fidelity F of the Werner state to Bell state $|\Phi^+\rangle$: (a) the fidelity F' of the left qubits to Bell state $|\Phi^+\rangle$ and (d) the success probability P_s, for $\eta = 0.98$, $\tau = 0.95$, and $r(\alpha_d) = 0.99, 0.98, 0.97, 0.96, 0.95$; (b) the fidelity F' of the left qubits to Bell state $|\Phi^+\rangle$ and (e) the success probability P_s, for $\eta = 0.98$, $\tau = 0.90$, and $r(\alpha_d) = 0.99, 0.98, 0.97, 0.96, 0.95$; (c) the fidelity F' of the left qubits to Bell state $|\Phi^+\rangle$ and (f) the success probability P_s, for $\eta = 0.95$, $\tau = 0.90$, and $r(\alpha_d) = 0.99, 0.98, 0.97, 0.96, 0.95$.

means the connections of Werner states by ideal Bell measurements followed by a phase-flip channel on system B. The state connected by the ideal Bell measurement is Werner state

$$\begin{aligned}\hat{\sigma}_W^{AB} =& \frac{1}{4}\left[1 + 3\left(\frac{4F-1}{3}\right)^{2^n}\right]|\Phi^+\rangle\langle\Phi^+|_{AB} \\ &+ \frac{1}{4}\left[1 - \left(\frac{4F-1}{3}\right)^{2^n}\right](|\Psi^+\rangle\langle\Psi^+|_{AB} + |\Phi^-\rangle\langle\Phi^-|_{AB} + |\Psi^-\rangle\langle\Psi^-|_{AB}).\end{aligned} \tag{6.31}$$

Since this state receives the phase-flip channel as the penalty of imperfections of RNPM protocols, the final state is described by

$$\Lambda^B_{r^{2(2^n-1)}(\sqrt{(1-\tau\eta)/(\tau\eta)}\alpha_s)}\Lambda^{i'_1+j'_1,B}_{2t(N,\alpha_s)-1}\cdots\Lambda^{i'_{2^n-1}+j'_{2^n-1},B}_{2t(N,\alpha_s)-1}(\hat{\sigma}_W^{AB}). \tag{6.32}$$

On being transformed into a Werner state, this state will be sent to the distillation stage.

6.3.3 Nested-purification repeater protocol

Here we provide the idea of the nested-purification repeater protocol [28, 29]. Since this protocol relies on entanglement distillation, it requires a lot of quantum memories. But, the protocol has an advantage that the protocol can enable long-distance quantum communication even if physical apparatuses have various types of error.

We use an entanglement distillation protocol with thresholds $\{F_{\max}, F_{\min}\}$ satisfying Eq. (6.30). Suppose that the channel with distance L is divided to $N = k^l$ $(k, l \in \boldsymbol{N})$ smaller segments, and the segments have entangled pairs with high fidelity $F_{\rm in}(< F_{\max})$ to a Bell state. $j \times k$ adjacent entangled pairs with distance L/k^m $(m = l, l-1, \ldots, 2, 1)$ are regarded as a bundle

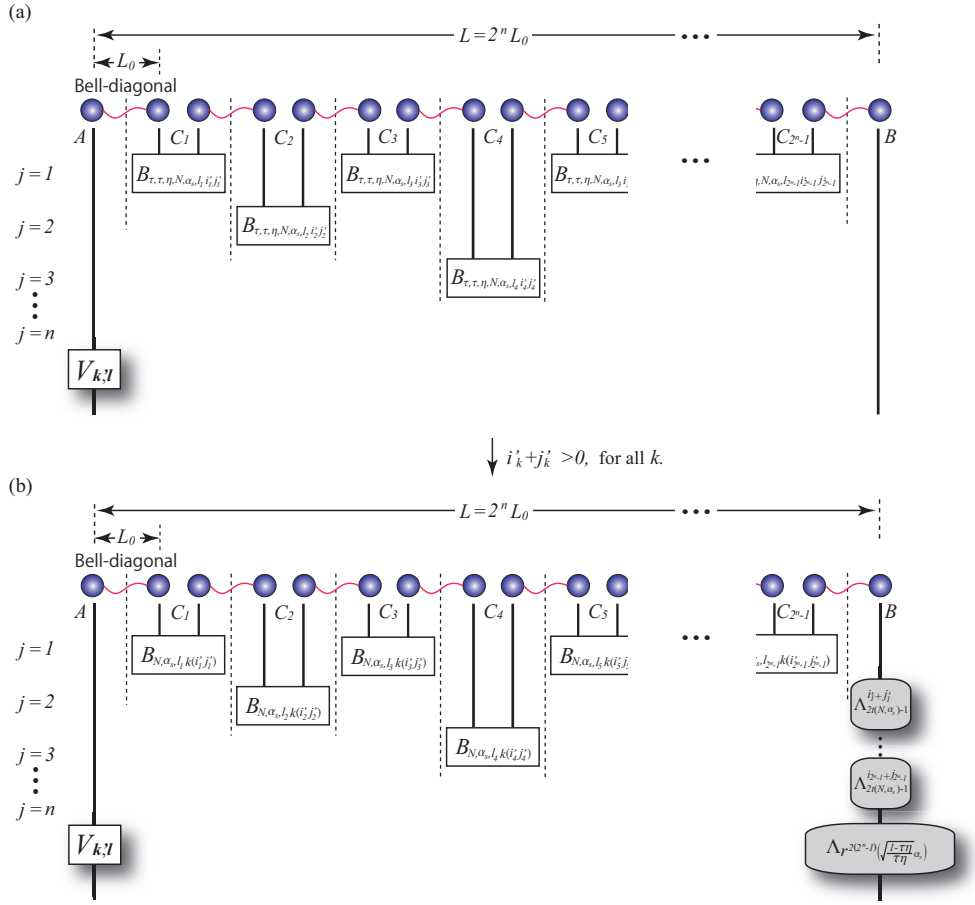

Fig. 6.9. Entanglement connection of Bell diagonal states. $\boldsymbol{k'} := (k(i'_1, j'_1), k(i'_2, j'_2), \ldots, k(i'_{2^n-1}, j'_{2^n-1}))$, and $\boldsymbol{l} := (l_1, l_2, \ldots, l_{2^n-1})$, where $k(i, j)$ is one defined by Eq. (5.39). $\hat{V}_{\boldsymbol{k'},\boldsymbol{l}}$ is a unitary operation to transform the state obtained in the success cases into a standard state of Eq. (6.32). The equivalence between (a) and (b) holds when all the realistic Bell measurements succeed.

(see Fig. 6.10). The pairs of a bundle are converted to entangled pairs with fidelity $F_{\rm out}(> F_{\rm min})$ and with distance L/k^{m-1} by the entanglement connections, and are further converted to an entangled pair with fidelity $F_{\rm in}$ and with distance L/k^{m-1} by the entanglement distillations. j is chosen to be large enough to make this two-step process succeed with almost unity probability. In other words, the working principle of this strategy is based on a 'purification loop' transforming the bundle into a pair according to

$$(L/k^m, F_{\rm in}) \stackrel{\rm Connection}{\longrightarrow} (L/k^{m-1}, F_{\rm out}) \stackrel{\rm Distillation}{\longrightarrow} (L/k^{m-1}, F_{\rm in}). \tag{6.33}$$

The purification loop is repeated l times, namely it is continued until generating an entangled pair with distance L and fidelity $F_{\rm in}$. Then, the total number R of elementary entangled pairs is described as $(kj)^l$, namely

$$R = (kj)^l = k^l k^{\log_k j^l} = N^{1+\log_k j}. \tag{6.34}$$

Here note that j depends only on the efficiencies of the entanglement distillation and the entanglement connection of k neighboring pairs. This implies that j is independent of l. On the other

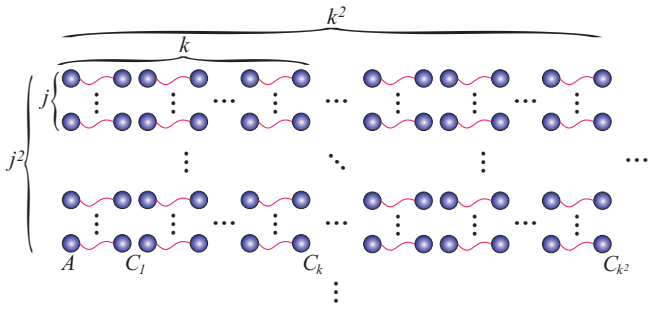

Fig. 6.10. Nested purification with an array of elementary Bell pairs.

hand, N can be changed by selecting parameter l with k fixed. Therefore, Eq. (6.34) shows that the total number R of elementary entangled pairs grows polynomially with the number N of the segments.

Since this repeater protocol is based on recursive use of a purification loop, we need to show that a purification loop is constructible. In Fig. 6.11, as examples, we show that such a purification loop can be made by entanglement distillation and entanglement connection in Sec. 6.3.1 and 6.3.2. There, we assume the RNPM protocols with photon detectors with $N = \infty$ or $N = 1$ in (a)-(c) of Fig. 6.11, and ones with photon detectors with $N = 0$ in (d)-(f) of Fig. 6.11. Without taking optimization, we chose parameters, α_d, α_s, and k, but, in practice, we will need to optimize the parameters for minimizing the cost j.

6.3.4 Summary

In this section, we showed that the recurrence method based on the realistic RNPM protocol works against Werner states. This enables us to distill an almost Bell pair even from entangled states with multiple types of errors. Moreover, the achievability of such an entanglement distillation makes it possible to implement the nested purification repeater protocol. Since the resources needed to this protocol increase with the communication distance only polynomially, the protocol would achieve efficient long-distance quantum communication even in the cases where the entanglement obtained by an entanglement generation protocol inevitably receives multiple types of errors.

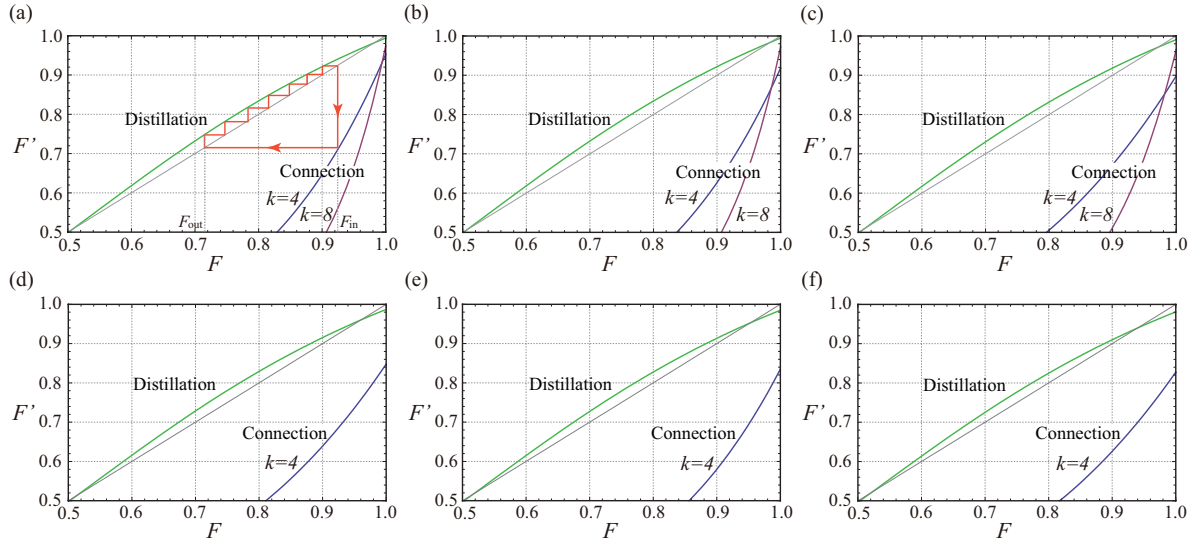

Fig. 6.11. The purification loop for entanglement connection and entanglement distillation based on the realistic RNPM protocols, which are described in Secs. 6.3.1 and 6.3.2. In the case where the single photon detectors ($N = 1$) are used, the detections of single photons are regarded as only success cases of the RNPM protocols. In Fig. (a), we describe a purification loop as an example. (a) $\tau = 0.98$, $\eta = 0.95$, $r(\alpha_d) = 0.96$, $r(\alpha_s) = 0.80$ for $k = 4$, $r(\alpha_s) = 0.95$ for $k = 8$, and $N = 1, \infty$; (b) $\tau = 0.98$, $\eta = 0.90$, $r(\alpha_d) = 0.98$, $r(\alpha_s) = 0.80$ for $k = 4$, $r(\alpha_s) = 0.97$ for $k = 8$, and $N = 1, \infty$; (c) $\eta = 0.95$, $\tau = 0.90$, $r(\alpha_d) = 0.98$, $r(\alpha_s) = 0.80$ for $k = 4$, $r(\alpha_s) = 0.97$ for $k = 8$, and $N = 1, \infty$; (d) $\tau = 0.98$, $\eta = 0.95$, $r(\alpha_d) = 0.98$, $r(\alpha_s) = 0.90$, $N = 0$, and $k = 4$; (e) $\tau = 0.98$, $\eta = 0.90$, $r(\alpha_d) = 0.98$, $r(\alpha_s) = 0.90$, $N = 0$, and $k = 4$; (f) $\tau = 0.95$, $\eta = 0.90$, $r(\alpha_d) = 0.98$, $r(\alpha_s) = 0.90$, $N = 0$, and $k = 4$.

7
Conclusion

In this thesis, we have provided a two-probe entanglement generation protocol, and we have shown that the two-probe protocol can achieve the theoretical limit of performance among all the protocols to generate entanglement with only one type of error by exchanging photons over a lossy channel. We further show that the two-probe protocol acts not only as an entanglement generation scheme but also as the remote nondestructive parity measurement (RNPM). Since the RNPM plays the role of a module for accomplishing the Bell measurement and the parity check measurement, the RNPM has the possibility to accomplish all the primitive operations needed for quantum repeater protocols, namely, entanglement generation, entanglement connection, and entanglement distillation. Actually, because of the loss of photons used as the carrier of quantum information, the protocol merely probabilistically implements RNPM with phase error, and hence, it was unclear whether the protocol dubbed 'RNPM protocol' is powerful enough to achieve long-distance quantum communication efficiently. However, as shown in Chapter 6, the RNPM protocol enables long-distance quantum communication with communication time increasing only sub-exponentially with the channel length. Therefore, the RNPM protocol is a promising candidate of a single module for long-distance quantum communication.

We mention several possibilities of future developments of the RNPM protocol. As shown in Chapter 5, the RNPM further acts as a module for isometry $\hat{C}_Z^{AB}|+\rangle_A$ and CZ gate $\hat{C}_Z^{AB}$. These operations are known to be essential for generating graph states that are the resources for the measurement-based quantum computation. Hence, it is clear that the ideal RNPM protocol can efficiently generate graph states. However, the realistic RNPM protocols will inevitably receive phase error because of the photon loss. Therefore, we will need to clarify how efficient RNPM protocols are required for efficiently composing the graph states. Even for experimentalists, the finding of the RNPM protocol is important. In fact, as noted in Preface or Sec. 2.5.2, the interaction with an optical pulse can be realizable by various quantum memories. Hence, the RNPM protocol can be also achievable by them. We expect that experimental efforts on the development of the RNPM protocol will be reported. Finally, we stress that this thesis has only just begun to grasp the full implications of the RNPM protocol: unexpected progresses of the RNPM protocol would appear in near future.

Appendix 1

RNPM protocol with photon detectors with a threshold and dark counts

We consider the effect of the dark counts occurring in the detectors. The POVM elements of a detector with mean dark count ν can be described by

$$\hat{E}_m = \sum_{k=0}^{m} \frac{e^{-\nu}\nu^{m-k}}{(m-k)!}|k\rangle\langle k|. \tag{1.1}$$

Suppose that the used two detectors show dark counts rates ν_a and ν_b. Then, for an input state $\hat{\rho}^{AB}$, we have

$$\begin{aligned}
&\Gamma_{mn,\alpha}(\hat{\rho}^{AB}) \\
&:= \mathrm{Tr}_{ab}\left\{\hat{E}_m^a \hat{E}_n^b \left[\hat{Z}^A_{\phi(\alpha)}\hat{Z}^B_{\phi(\alpha)}\hat{V}_\alpha^{ab}\hat{U}_\theta^{Aa}\hat{U}_\theta^{Bb}(\hat{\rho}^{AB}\otimes|\alpha\rangle\langle\alpha|_a\otimes|\alpha\rangle\langle\alpha|_b)\hat{U}_\theta^{Bb\dagger}\hat{U}_\theta^{Aa\dagger}\hat{V}_\alpha^{ab\dagger}\hat{Z}^{B\dagger}_{\phi(\alpha)}\hat{Z}^{A\dagger}_{\phi(\alpha)}\right]\right\} \\
&= \sum_{k=0}^{m}\sum_{l=0}^{n}\frac{e^{-\nu_a}\nu_a^{m-k}}{(m-k)!}\frac{e^{-\nu_b}\nu_b^{n-l}}{(n-l)!}\hat{M}^{AB}_{\alpha,kl}\hat{\rho}^{AB}\hat{M}^{AB\dagger}_{\alpha,kl},
\end{aligned} \tag{1.2}$$

where note that

$$\begin{aligned}
\hat{M}_{\alpha,mn} =& \delta_{m0}\langle n|\beta(\alpha)\rangle(|00\rangle\langle 00|_{AB} + (-1)^n|11\rangle\langle 11|_{AB}) \\
&+ \delta_{n0}\langle m|\beta(\alpha)\rangle((-1)^m|01\rangle\langle 01|_{AB} + |10\rangle\langle 10|_{AB}) \\
=& \delta_{m0}\langle n|\beta(\alpha)\rangle(\hat{Z}^B)^n\hat{P}^{AB}_{\Phi} + \delta_{n0}\langle m|\beta(\alpha)\rangle(\hat{Z}^B)^m\hat{P}^{AB}_{\Psi}.
\end{aligned} \tag{1.3}$$

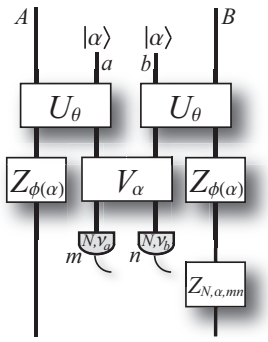

Fig. A1.1. RNPM protocol with photon detectors with threshold N and mean dark count ν.

For $m, n > 0$, this means

$$\begin{aligned}
\Gamma_{0n,\alpha}(\hat{\rho}^{AB}) &= e^{-\nu_a-\nu_b}\left(\frac{\nu_b^n}{n!}|\langle 0|\beta(\alpha)\rangle|^2\hat{\rho}^{AB} + \sum_{l=1}^{n}\frac{\nu_b^{n-l}}{(n-l)!}|\langle l|\beta(\alpha)\rangle|^2(\hat{Z}^B)^l\hat{P}_\Phi^{AB}\hat{\rho}^{AB}\hat{P}_\Phi^{AB}(\hat{Z}^B)^l\right),\\
&= e^{-\nu_a-\nu_b}\left[\frac{\nu_b^n}{n!}|\langle 0|\beta(\alpha)\rangle|^2\hat{\rho}^{AB} + \left(\sum_{l=1}^{\lceil\frac{n-1}{2}\rceil}\frac{\nu_b^{n-2l}}{(n-2l)!}|\langle 2l|\beta(\alpha)\rangle|^2\right)\hat{P}_\Phi^{AB}\hat{\rho}^{AB}\hat{P}_\Phi^{AB}\right.\\
&\qquad\left. + \left(\sum_{l=1}^{\lceil\frac{n}{2}\rceil}\frac{\nu_b^{n-2l+1}}{(n-2l+1)!}|\langle 2l-1|\beta(\alpha)\rangle|^2\right)\hat{Z}^B\hat{P}_\Phi^{AB}\hat{\rho}^{AB}\hat{P}_\Phi^{AB}\hat{Z}^B\right]\\
\Gamma_{m0,\alpha}(\hat{\rho}^{AB}) &= e^{-\nu_a-\nu_b}\left(\frac{\nu_a^m}{m!}|\langle 0|\beta(\alpha)\rangle|^2\hat{\rho}^{AB} + \sum_{k=1}^{m}\frac{\nu_a^{m-k}}{(m-k)!}|\langle k|\beta(\alpha)\rangle|^2(\hat{Z}^B)^k\hat{P}_\Psi^{AB}\hat{\rho}^{AB}\hat{P}_\Psi^{AB}(\hat{Z}^B)^k\right)\\
&= e^{-\nu_a-\nu_b}\left[\frac{\nu_a^m}{m!}|\langle 0|\beta(\alpha)\rangle|^2\hat{\rho}^{AB} + \left(\sum_{k=1}^{\lceil\frac{m-1}{2}\rceil}\frac{\nu_a^{m-2k}}{(m-2k)!}|\langle 2k|\beta(\alpha)\rangle|^2\right)\hat{P}_\Psi^{AB}\hat{\rho}^{AB}\hat{P}_\Psi^{AB}\right.\\
&\qquad\left. + \left(\sum_{k=1}^{\lceil\frac{m}{2}\rceil}\frac{\nu_a^{m-2k+1}}{(m-2k+1)!}|\langle 2k-1|\beta(\alpha)\rangle|^2\right)\hat{Z}^B\hat{P}_\Psi^{AB}\hat{\rho}^{AB}\hat{P}_\Psi^{AB}\hat{Z}^B\right]\\
\Gamma_{00,\alpha}(\hat{\rho}^{AB}) &= e^{-\nu_a-\nu_b}|\langle 0|\beta(\alpha)\rangle|^2\hat{\rho}^{AB},
\end{aligned} \tag{1.4}$$

where $\lceil x\rceil$ is the smallest integer $\geq x$. These relations are reduced to

$$\begin{aligned}
\Gamma_{0n,\alpha}(\hat{\rho}^{AB}) &= \frac{e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}}{n!}\left[\nu_b^n\hat{\rho}^{AB} + \frac{(\nu_b+|\beta(\alpha)|^2)^n + (\nu_b-|\beta(\alpha)|^2)^n - 2\nu_b^n}{2}\hat{P}_\Phi^{AB}\hat{\rho}^{AB}\hat{P}_\Phi^{AB}\right.\\
&\qquad\left. + \frac{(\nu_b+|\beta(\alpha)|^2)^n - (\nu_b-|\beta(\alpha)|^2)^n}{2}\hat{Z}^B\hat{P}_\Phi^{AB}\hat{\rho}^{AB}\hat{P}_\Phi^{AB}\hat{Z}^B\right],\\
\Gamma_{m0,\alpha}(\hat{\rho}^{AB}) &= \frac{e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}}{m!}\left[\nu_a^m\hat{\rho}^{AB} + \frac{(\nu_a+|\beta(\alpha)|^2)^m + (\nu_a-|\beta(\alpha)|^2)^m - 2\nu_a^m}{2}\hat{P}_\Psi^{AB}\hat{\rho}^{AB}\hat{P}_\Psi^{AB}\right.\\
&\qquad\left. + \frac{(\nu_a+|\beta(\alpha)|^2)^m - (\nu_a-|\beta(\alpha)|^2)^m}{2}\hat{Z}^B\hat{P}_\Psi^{AB}\hat{\rho}^{AB}\hat{P}_\Psi^{AB}\hat{Z}^B\right],\\
\Gamma_{00,\alpha}(\hat{\rho}^{AB}) &= e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}\hat{\rho}^{AB},
\end{aligned} \tag{1.5}$$

because

$$\begin{aligned}
&\left(\sum_{l=1}^{\lceil\frac{n-1}{2}\rceil}\frac{\nu_b^{n-2l}}{(n-2l)!}|\langle 2l|\beta(\alpha)\rangle|^2\right) \pm \left(\sum_{l=1}^{\lceil\frac{n}{2}\rceil}\frac{\nu_b^{n-2l+1}}{(n-2l+1)!}|\langle 2l-1|\beta(\alpha)\rangle|^2\right)\\
&\quad= e^{-|\beta(\alpha)|^2}\left(\sum_{l=1}^{\lceil\frac{n-1}{2}\rceil}\frac{\nu_b^{n-2l}}{(n-2l)!}\frac{|\beta(\alpha)|^{4l}}{(2l)!}\right) + e^{-|\beta(\alpha)|^2}\left(\sum_{l=1}^{\lceil\frac{n}{2}\rceil}\frac{\nu_b^{n-2l+1}}{(n-2l+1)!}\frac{(\pm|\beta(\alpha)|^2)^{(2l-1)}}{(2l-1)!}\right)\\
&\quad= e^{-|\beta(\alpha)|^2}\left(\sum_{l=1}^{n}\frac{\nu_b^{n-l}}{(n-l)!}\frac{(\pm|\beta(\alpha)|^2)^l}{l!}\right) = \frac{e^{-|\beta(\alpha)|^2}}{n!}\left[(\nu_b\pm|\beta(\alpha)|^2)^n - \nu_b^n\right],
\end{aligned} \tag{1.6}$$

and $|\langle n|\beta(\alpha)\rangle|^2 = (e^{-|\beta(\alpha)|^2}|\beta(\alpha)|^{2n})/(n!)$. These equations give

$$\begin{aligned}
P_{0n,\alpha}(\hat{\rho}^{AB}) :=& \mathrm{Tr}[\Gamma_{0n,\alpha}(\hat{\rho}^{AB})] = \frac{e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}}{n!}\left\{\nu_b^n + \left[(\nu_b+|\beta(\alpha)|^2)^n - \nu_b^n\right]\mathrm{Tr}[\hat{P}_{\Phi}^{AB}\hat{\rho}^{AB}]\right\},\\
P_{0n,\alpha}(\hat{\rho}^{AB}) :=& \mathrm{Tr}[\Gamma_{0n,\alpha}(\hat{\rho}^{AB})] = \frac{e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}}{m!}\left\{\nu_a^m + \left[(\nu_a+|\beta(\alpha)|^2)^m - \nu_a^m\right]\mathrm{Tr}[\hat{P}_{\Psi}^{AB}\hat{\rho}^{AB}]\right\},\\
P_{00,\alpha}(\hat{\rho}^{AB}) :=& \mathrm{Tr}[\Gamma_{00,\alpha}(\hat{\rho}^{AB})] = e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}.
\end{aligned} \tag{1.7}$$

Thus, the measurement transforms state $\hat{\rho}^{AB}$ into unnormalized states according to

$$\hat{\rho}^{AB} \longrightarrow \begin{cases}
(\hat{Z}^B)^n\Gamma_{0n,\alpha}(\hat{\rho}^{AB})(\hat{Z}^B)^n, & (m=0, 0<n\leq N),\\
\hat{Z}^B_{N,\alpha,0n}\left(\sum_{n>N}\Gamma_{0n,\alpha}(\hat{\rho}^{AB})\right)\hat{Z}^B_{N,\alpha,0n}, & (m=0, n=N+1),\\
(\hat{Z}^B)^m\Gamma_{m0,\alpha}(\hat{\rho}^{AB})(\hat{Z}^B)^m, & (0<m\leq N, n=0),\\
\hat{Z}^B_{N,\alpha,m0}\left(\sum_{m>N}\Gamma_{m0,\alpha}(\hat{\rho}^{AB})\right)\hat{Z}^B_{N,\alpha,m0}, & (m=N+1, n=0),\\
\Gamma_{00,\alpha}(\hat{\rho}^{AB}), & (m=n=0),\\
\text{states to be discarded,} & (m>0, n>0).
\end{cases} \tag{1.8}$$

In the cases of $m, n = 1$ and $N \geq 1$, $\Gamma_{0n,\alpha}(\hat{\rho}^{AB})$ and $\Gamma_{m0,\alpha}(\hat{\rho}^{AB})$ are reduced into

$$\frac{\hat{Z}^B\Gamma_{01,\alpha}(\hat{\rho}^{AB})\hat{Z}^B}{P_{01,\alpha}(\hat{\rho}^{AB})} = \frac{\nu_b\hat{\rho}^{AB} + |\beta(\alpha)|^2\hat{P}_{\Phi}^{AB}\hat{\rho}^{AB}\hat{P}_{\Phi}^{AB}}{\nu_b + |\beta(\alpha)|^2\mathrm{Tr}[\hat{P}_{\Phi}^{AB}\hat{\rho}^{AB}]}, \tag{1.9}$$

$$\frac{\hat{Z}^B\Gamma_{10,\alpha}(\hat{\rho}^{AB})\hat{Z}^B}{P_{10,\alpha}(\hat{\rho}^{AB})} = \frac{\nu_a\hat{\rho}^{AB} + |\beta(\alpha)|^2\hat{P}_{\Psi}^{AB}\hat{\rho}^{AB}\hat{P}_{\Psi}^{AB}}{\nu_a + |\beta(\alpha)|^2\mathrm{Tr}[\hat{P}_{\Psi}^{AB}\hat{\rho}^{AB}]}. \tag{1.10}$$

The probabilities are described by

$$P_{01,\alpha}(\hat{\rho}^{AB}) = e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}\left\{\nu_b + |\beta(\alpha)|^2\mathrm{Tr}[\hat{P}_{\Phi}^{AB}\hat{\rho}^{AB}]\right\}, \tag{1.11}$$

$$P_{10,\alpha}(\hat{\rho}^{AB}) = e^{-\nu_a-\nu_b-|\beta(\alpha)|^2}\left\{\nu_a + |\beta(\alpha)|^2\mathrm{Tr}[\hat{P}_{\Psi}^{AB}\hat{\rho}^{AB}]\right\}. \tag{1.12}$$

In the cases of $N = 0$, the successful output states are

$$\begin{aligned}
&\frac{\hat{Z}^B[\sum_{n=1}^{\infty}\Gamma_{0n,\alpha}(\hat{\rho}^{AB})]\hat{Z}^B}{\sum_{n=1}^{\infty}P_{0n,\alpha}(\hat{\rho}^{AB})}\\
&= \frac{(1-e^{-\nu_b})\hat{Z}^B\hat{\rho}^{AB}\hat{Z}^B + [\cosh(|\beta(\alpha)|^2)-1]\hat{Z}^B\hat{P}_{\Phi}^{AB}\hat{\rho}^{AB}\hat{P}_{\Phi}^{AB}\hat{Z}^B + \sinh(|\beta(\alpha)|^2)\hat{P}_{\Phi}^{AB}\hat{\rho}^{AB}\hat{P}_{\Phi}^{AB}}{1-e^{-\nu_b} + (e^{|\beta(\alpha)|^2}-1)\mathrm{Tr}[\hat{P}_{\Phi}^{AB}\hat{\rho}^{AB}]},
\end{aligned} \tag{1.13}$$

and

$$\begin{aligned}
&\frac{\hat{Z}^B[\sum_{m=1}^{\infty}\Gamma_{m0,\alpha}(\hat{\rho}^{AB})]\hat{Z}^B}{\sum_{m=1}^{\infty}P_{m0,\alpha}(\hat{\rho}^{AB})}\\
&= \frac{(1-e^{-\nu_a})\hat{Z}^B\hat{\rho}^{AB}\hat{Z}^B + [\cosh(|\beta(\alpha)|^2)-1]\hat{Z}^B\hat{P}_{\Psi}^{AB}\hat{\rho}^{AB}\hat{P}_{\Phi}^{AB}\hat{Z}^B + \sinh(|\beta(\alpha)|^2)\hat{P}_{\Psi}^{AB}\hat{\rho}^{AB}\hat{P}_{\Psi}^{AB}}{1-e^{-\nu_a} + (e^{|\beta(\alpha)|^2}-1)\mathrm{Tr}[\hat{P}_{\Psi}^{AB}\hat{\rho}^{AB}]}.
\end{aligned} \tag{1.14}$$

The success probabilities are

$$\sum_{n=1}^{\infty} P_{0n,\alpha}(\hat{\rho}^{AB}) = e^{-\nu_a - |\beta(\alpha)|^2} \left\{ 1 - e^{-\nu_b} + (e^{|\beta(\alpha)|^2} - 1) \mathrm{Tr}[\hat{P}_{\Phi}^{AB} \hat{\rho}^{AB}] \right\}, \tag{1.15}$$

$$\sum_{m=1}^{\infty} P_{m0,\alpha}(\hat{\rho}^{AB}) = e^{-\nu_b - |\beta(\alpha)|^2} \left\{ 1 - e^{-\nu_a} + (e^{|\beta(\alpha)|^2} - 1) \mathrm{Tr}[\hat{P}_{\Psi}^{AB} \hat{\rho}^{AB}] \right\}. \tag{1.16}$$

Appendix 2
Elementary relations on Bell states

A2.1 $\hat{X}^A \otimes \hat{X}^B$-basis and Bell states

$$
\begin{aligned}
|++\rangle_{AB} =& \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{AB} + |\Psi^+\rangle_{AB}), \;\; |+-\rangle_{AB} = \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{AB} - |\Psi^-\rangle_{AB}), \\
|-+\rangle_{AB} =& \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{AB} + |\Psi^-\rangle_{AB}), \;\; |--\rangle_{AB} = \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{AB} - |\Psi^+\rangle_{AB}).
\end{aligned}
\tag{2.1}
$$

A2.2 Bell bases of four qubits

$$
\begin{aligned}
|\Phi^\pm\rangle_{A_1B_1}|\Phi^\pm\rangle_{A_2B_2} &= \frac{1}{2}(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} + |\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2} \\
&\qquad \pm |\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} \pm |\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}), \\
|\Phi^\pm\rangle_{A_1B_1}|\Phi^\mp\rangle_{A_2B_2} &= \frac{1}{2}(|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2} + |\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} \\
&\qquad \mp |\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} \mp |\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}), \\
|\Phi^\pm\rangle_{A_1B_1}|\Psi^\pm\rangle_{A_2B_2} &= \frac{1}{2}(|\Phi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} + |\Phi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} \\
&\qquad \pm |\Psi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} \pm |\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}), \\
|\Phi^\pm\rangle_{A_1B_1}|\Psi^\mp\rangle_{A_2B_2} &= \frac{1}{2}(|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} + |\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} \\
&\qquad \mp |\Psi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2} \mp |\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}), \\
|\Psi^\pm\rangle_{A_1B_1}|\Phi^\pm\rangle_{A_2B_2} &= \frac{1}{2}(|\Phi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} - |\Phi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} \\
&\qquad \pm |\Psi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} \mp |\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}), \\
|\Psi^\pm\rangle_{A_1B_1}|\Phi^\mp\rangle_{A_2B_2} &= \frac{1}{2}(-|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} + |\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} \\
&\qquad \pm |\Psi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2} \mp |\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}), \\
|\Psi^\pm\rangle_{A_1B_1}|\Psi^\pm\rangle_{A_2B_2} &= \frac{1}{2}(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} - |\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2} \\
&\qquad \pm |\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} \mp |\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}), \\
|\Psi^\pm\rangle_{A_1B_1}|\Psi^\mp\rangle_{A_2B_2} &= \frac{1}{2}(-|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2} + |\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} \\
&\qquad \pm |\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2} \mp |\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}).
\end{aligned}
\tag{2.2}
$$

A2.3 Bell measurement

$$\hat{1}^{AB} \otimes \hat{B}_{00}^{C_1C_2} = {}_{C_1C_2}\langle\Phi^+|$$
$$= \frac{1}{2}|\Phi^+\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Phi^+|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Psi^+|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Psi^-|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^+\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Psi^+|_{BC_2} - \langle\Phi^-|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Phi^+|_{BC_2} - \langle\Psi^-|_{AC_1}\langle\Phi^-|_{BC_2})$$
$$+ \frac{1}{2}|\Phi^-\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Phi^+|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Psi^+|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^-\rangle_{AB}(-\langle\Phi^+|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Psi^+|_{BC_2} - \langle\Psi^+|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Phi^+|_{BC_2}), \tag{2.3}$$

$$\hat{1}^{AB} \otimes \hat{B}_{01}^{C_1C_2} = {}_{C_1C_2}\langle\Psi^+| = {}_{C_1C_2}\langle\Phi^+|\hat{X}^{C_2}$$
$$= \frac{1}{2}|\Phi^+\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Psi^+|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Phi^+|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Phi^-|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^+\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Phi^+|_{BC_2} - \langle\Phi^-|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Psi^+|_{BC_2} - \langle\Psi^-|_{AC_1}\langle\Psi^-|_{BC_2})$$
$$+ \frac{1}{2}|\Phi^-\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Psi^+|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Phi^+|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^-\rangle_{AB}(-\langle\Phi^+|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Phi^+|_{BC_2} - \langle\Psi^+|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Psi^+|_{BC_2}), \tag{2.4}$$

$$\hat{1}^{AB} \otimes \hat{B}_{10}^{C_1C_2} = {}_{C_1C_2}\langle\Phi^-| = {}_{C_1C_2}\langle\Phi^+|\hat{Z}^{C_2}$$
$$= \frac{1}{2}|\Phi^+\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Phi^+|_{BC_2} - \langle\Psi^+|_{AC_1}\langle\Psi^-|_{BC_2} - \langle\Psi^-|_{AC_1}\langle\Psi^+|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^+\rangle_{AB}(-\langle\Phi^+|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Psi^+|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Phi^-|_{BC_2} - \langle\Psi^-|_{AC_1}\langle\Phi^+|_{BC_2})$$
$$+ \frac{1}{2}|\Phi^-\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Phi^+|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Phi^-|_{BC_2} - \langle\Psi^+|_{AC_1}\langle\Psi^+|_{BC_2} - \langle\Psi^-|_{AC_1}\langle\Psi^-|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^-\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Psi^+|_{BC_2} - \langle\Phi^-|_{AC_1}\langle\Psi^-|_{BC_2} - \langle\Psi^+|_{AC_1}\langle\Phi^+|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Phi^-|_{BC_2}), \tag{2.5}$$

$$\hat{1}^{AB} \otimes \hat{B}_{11}^{C_1C_2} = -{}_{C_1C_2}\langle\Psi^-| = {}_{C_1C_2}\langle\Phi^+|\hat{X}^{C_2}\hat{Z}^{C_2}$$
$$= \frac{1}{2}|\Phi^+\rangle_{AB}(-\langle\Phi^+|_{AC_1}\langle\Psi^-|_{BC_2} - \langle\Phi^-|_{AC_1}\langle\Psi^+|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Phi^+|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^+\rangle_{AB}(\langle\Phi^+|_{AC_1}\langle\Phi^-|_{BC_2} - \langle\Phi^-|_{AC_1}\langle\Phi^+|_{BC_2} - \langle\Psi^+|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Psi^+|_{BC_2})$$
$$+ \frac{1}{2}|\Phi^-\rangle_{AB}(-\langle\Phi^+|_{AC_1}\langle\Psi^+|_{BC_2} - \langle\Phi^-|_{AC_1}\langle\Psi^-|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Phi^+|_{BC_2} + \langle\Psi^-|_{AC_1}\langle\Phi^-|_{BC_2})$$
$$+ \frac{1}{2}|\Psi^-\rangle_{AB}(-\langle\Phi^+|_{AC_1}\langle\Phi^+|_{BC_2} + \langle\Phi^-|_{AC_1}\langle\Phi^-|_{BC_2} + \langle\Psi^+|_{AC_1}\langle\Psi^+|_{BC_2} - \langle\Psi^-|_{AC_1}\langle\Psi^-|_{BC_2}). \tag{2.6}$$

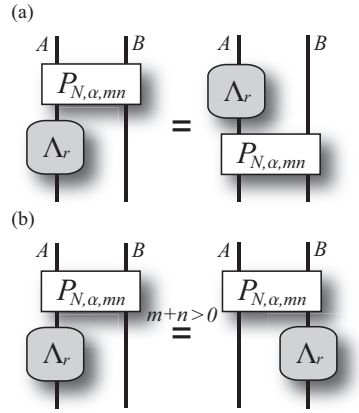

Fig. A2.1. Equivalences on the nondestructive parity measurement followed by the phase-flip channel.

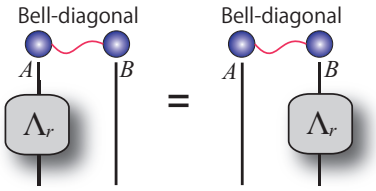

Fig. A2.2. Equivalence on a phase-flip channel on a Bell-diagonal state.

A2.4 Equivalences on the nondestructive parity measurement followed by the phase-flip channel

Here we show the equivalences in Fig. A2.1. The equivalence in Fig. A2.1a is shown from

$$\begin{aligned} \hat{Z}^A \hat{P}_{\Phi}^{AB} &= \hat{P}_{\Phi}^{AB} \hat{Z}^A, \\ \hat{Z}^A \hat{P}_{\Psi}^{AB} &= \hat{P}_{\Psi}^{AB} \hat{Z}^A. \end{aligned} \tag{2.7}$$

The equivalence in Fig. A2.1a is also proven from

$$\begin{aligned} \hat{Z}^A \hat{P}_{\Phi}^{AB} &= \hat{Z}^B \hat{P}_{\Phi}^{AB}, \\ \hat{Z}^A \hat{P}_{\Psi}^{AB} &= -\hat{Z}^B \hat{P}_{\Psi}^{AB}. \end{aligned} \tag{2.8}$$

A2.5 Phase-flip channel on Bell-diagonal states

The equivalence in Fig. A2.1 is confirmed from

$$\begin{aligned} \hat{Z}^A |\Phi^{\pm}\rangle_{AB} &= \hat{Z}^B |\Phi^{\pm}\rangle_{AB}, \\ \hat{Z}^A |\Psi^{\pm}\rangle_{AB} &= -\hat{Z}^B |\Psi^{\pm}\rangle_{AB}. \end{aligned} \tag{2.9}$$

List of publications

- Koji Azuma, Naoya Sota, Ryo Namiki, Şahin Kaya Özdemir, Takashi Yamamoto, Masato Koashi, and Nobuyuki Imoto, Optimal entanglement generation for efficient hybrid quantum repeaters. Phys. Rev. A **80**, 060303 (R) (2009).

- Koji Azuma, Naoya Sota, Masato Koashi, and Nobuyuki Imoto, Tight bound on coherent-state-based entanglement generation over lossy channels. arXiv:0908.2735 [Phys. Rev. A (to be published)].

- Koji Azuma, Hitoshi Takeda, Masato Koashi, and Nobuyuki Imoto, Quantum repeaters built on a single module: Remote nondestructive parity measurement. In preparation.

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. **47**, 777 (1935).

[2] E. Schrodinger, Die gegenwartige Situation in der Quantenmechanik. Naturwissenschaften **23**, 807 (1935).

[3] J. S. Bell, On the Einstein Podolsky Rosen Paradox. Physics (Long Island City, N.Y.) **1**, 195 (1964).

[4] R. Horodecki, P. Horodecki,M. Horodecki, and K. Horodecki, Quantum entanglement. Rev. Mod. Phys. **81**, 865 (2009).

[5] P. Shor, Algorithms for quantum computation: Discrete logarithms and factoring. Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124.

[6] Y. Manin, Computable and Uncomputable (Sovetkoye Radio, Moscow 1980).

[7] R. P. Feynman, Simulating physics with computers. Int. J. Theor. Phys. **21**, 467 (1982).

[8] L. K. Grover, Quantum Computers Can Search Arbitrarily Large Databases by a Single Query. Phys. Rev. Lett. **79**, 4709 (1997).

[9] C. H. Bennett and G. Brassard, Public Key Distribution and Coin Tossing. In Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing 175–179 (IEEE, New York, 1984).

[10] A. K. Ekert, Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991).

[11] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**, 557 (1992).

[12] C. H. Bennett, Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121 (1992).

[13] D. Mayers, Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. Lect. Notes Comput. Sci. **1109**, 343 (1996).

[14] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**, 2050 (1999).

[15] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441 (2000).

[16] K. Tamaki, M. Koashi, and N. Imoto, Secure Key Distribution Based on Two Nonorthogonal States. Phys. Rev. Lett. **90**, 167904 (2003).

[17] M. Koashi, Simple security proof of quantum key distribution via uncertainty principle. arXiv:quant-ph/0505108.

[18] M. Koashi, Complementarity, distillable secret key, and distillable entanglement. arXiv:0704.3661.

[19] L. K. Grover, Quantum Telecomputation. arXiv:quant-ph/9704012.

[20] S. Foletti, H. Bluhm, D. Mahalu, V. Umansky, and A. Yacoby, Universal quantum control of two-electron spin quantum bits using dynamic nuclear polarization. Nat. Phys. **5**, 903 (2009).

[21] L. DiCarlo, J. M. Chow, J. M. Gambetta, L. S. Bishop, B. R. Johnson, D. I. Schuster, J. Majer, A. Blais, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, Demonstration of two-qubit algorithms with a superconducting quantum processor. Nature **460**, 240 (2009).

[22] M. Riebe, T. Monz, K. Kim, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, Deterministic entanglement swapping with an ion-trap quantum computer. Nat. Physics **4**, 839, (2008).

[23] J. Benhelm, G. Kirchmair, C. F. Roos, and R. Blatt, Towards fault-tolerant quantum computing with trapped ions. Nat. Physics **4**, 463 (2008).

[24] R. Prevedel, P. Walther, F. Tiefenbacher, P. Bohi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger, High-speed linear optics quantum computing using active feed-forward. Nature **445**, 65 (2007).
[25] Y. Tokunaga, S. Kuwashiro, T. Yamamoto, M. Koashi, and N. Imoto, Generation of High-Fidelity Four-Photon Cluster State and Quantum-Domain Demonstration of One-Way Quantum Computing. Phys. Rev. Lett. **100**, 210501 (2008).
[26] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nat. Photonics **1**, 343 (2007).
[27] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, High-fidelity transmission of entanglement over a high-loss free-space channel. Nat. Physics **5**, 389 (2009).
[28] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. Phys. Rev. Lett. **81**, 5932 (1998).
[29] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Quantum repeaters based on entanglement purification. Phys. Rev. A **59**, 169 (1999).
[30] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895 (1993).
[31] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics. Nature **414**, 413 (2001).
[32] B. Zhao, Z-B. Chen, Y-A. Chen, J. Schmiedmayer, and J-W. Pan, Robust Creation of Entanglement between Remote Memory Qubits. Phys. Rev. Lett. **98**, 240502 (2007).
[33] Z-B. Chen, B. Zhao, Y-A. Chen, J. Schmiedmayer, and J-W. Pan, Fault-tolerant quantum repeater with atomic ensembles and linear optics. Phys. Rev. A **76**, 022329 (2007).
[34] L. Jiang, J. M. Taylor, and M. D. Lukin, Fast and robust approach to long-distance quantum communication with atomic ensembles. Phys. Rev. A **76**, 012301 (2007).
[35] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, Quantum Repeaters with Photon Pair Sources and Multimode Memories. Phys. Rev. Lett. **98**, 190503 (2007).
[36] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics. arXiv:0906.2699.
[37] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Fault-Tolerant Quantum Communication Based on Solid-State Photon Emitters. Phys. Rev. Lett. **96**, 070504 (2006).
[38] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters. Phys. Rev. A **72**, 052330 (2005).
[39] N. Sangouard, R. Dubessy, and C. Simon, Quantum repeaters based on single trapped ions. Phys. Rev. A **79**, 042340 (2009).
[40] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Hybrid Quantum Repeater Using Bright Coherent Light. Phys. Rev. Lett. **96**, 240501 (2006).
[41] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, Hybrid quantum repeater based on dispersive CQED interactions between matter qubits and bright coherent light. New J. Phys. **8**, 184 (2006).
[42] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Quantum repeaters using coherent-state communication. Phys. Rev. A **78**, 062319 (2008).
[43] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, High-Bandwidth Hybrid Quantum Repeater. Phys. Rev. Lett. **101**, 040502 (2008).
[44] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn, Quantum computation by communication. New J. Phys. **8**, 30 (2006).
[45] P. van Loock, W. J. Munro, K. Nemoto, T. P. Spiller, T. D. Ladd, S. L. Braunstein, and G. J. Milburn, Hybrid quantum computation in quantum optics. Phys. Rev. A **78**, 022303 (2008).
[46] S. G. R. Louis, W. J. Munro, T. P. Spiller, and K. Nemoto, Loss in hybrid qubit-bus couplings and gates. Phys. Rev. A **78**, 022326 (2008).
[47] H. J. Briegel and R. Raussendorf, Persistent Entanglement in Arrays of Interacting Particles. Phys. Rev. Lett. **86**, 910 (2000).
[48] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer. Phys. Rev. Lett. **86**, 5188 (2000).
[49] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster state. Phys. Rev. A **68**, 022312 (2003).

[50] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, UK, 2000).
[51] J. Preskill, URL: http://www.theory.caltech.edu/people/preskill/ph229/
[52] R. A. Horn and C. R. Johnson, Matrix Analysis (Cambridge Univ. Press, Cambridge, 1990).
[53] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned. Nature (London) **299**, 802 (1982).
[54] D. Dieks, Communication by EPR devices. Phys. Lett. **92A**, 271 (1982).
[55] H. P. Yuen, Amplification of quantum states and noiseless photon amplifiers. Phys. Lett. **113A**, 405 (1986).
[56] L. M. Duan and G. C. Guo, Probabilistic Cloning and Identification of Linearly Independent Quantum States. Phys. Rev. Lett. **80**, 4999 (1998).
[57] D. Dieks, Overlap and distinguishability of quantum states. Phys. Lett. A **126**, 303 (1988).
[58] I. D. Ivanovic, How to differentiate between non-orthogonal states. Phys. Lett. A **123**, 257 (1987).
[59] A. Peres, How to differentiate between non-orthogonal states. Phys. Lett. A **128**, 19 (1988).
[60] G. Jaeger and A. Shimony, Optimal distinction between two non-orthogonal quantum states. Phys. Lett. A **197**, 83 (1995).
[61] R. Jozsa, Fidelity for mixed quantum states. J. Mod. Opt. **41**, 2315, (1994).
[62] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Event-ready-detectors" Bell experiment via entanglement swapping. Phys. Rev. Lett. **71**, 4287 (1993).
[63] G. Vidal, Entanglement monotones. J. Mod. Opt. **47**, 355 (2000).
[64] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**, 3824 (1996).
[65] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. Phys. Rev. Lett. **76**, 722 (1996).
[66] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. Phys. Rev. Lett. **77**, 2818 (1996).
[67] C. Macchiavello, On the analytical convergence of the QPA procedure. Phys. Lett. A **246**, 385 (1998).
[68] L. Mandel and E. Wolf, Optical Coherence and Quantum Optics (Cambridge Univ. Press, 1995).
[69] M. O. Scully and M. S. Zubairy, Quantum optics (Cambridge Univ. Press, Cambridge, 1997).
[70] W. P. Schleich, Quantum Optics in Phase Space (Wiley-VCH, Berlin, 2001).
[71] M. Sargent III and P. Horwitz, Three-level Rabi flopping. Phys. Rev. A **13**, 1962 (1976).
[72] A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kaurova, O. Minaeva, G. Gol'tsman, K. G. Lagoudakis, M. Benkhaoul, F. Levy, and A. Fiore, Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths. Nat. Photonics **2**, 302 (2008).
[73] C. Gobby, Z. L. Yuan, and A. J. Shields, Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. **84**, 3762 (2004).
[74] D. E. Browne and T. Rudolph, Resource-Efficient Linear Optical Quantum Computation. Phys. Rev. Lett. **95**, 010501 (2005).
[75] L.-M. Duan and R. Raussendorf, Efficient Quantum Computation with Probabilistic Quantum Gates. Phys. Rev. Lett. **95**, 080503 (2005).

Index