General formulas for fixed-length quantum entanglement concentration

Masahito Hayashi

Abstract—General formulas of entanglement concentration are derived by using an information-spectrum approach for the i.i.d. sequences and the general sequences of partially entangled pure states. That is, we derive general relations between the performance of the entanglement concentration and the eigenvalues of the partially traced state. The achievable rates with constant constraints and those with exponential constraints can be calculated from these formulas.

Index Terms—Information spectrum, Entanglement concentration, Exponents, Maximally entangled state

I. INTRODUCTION

ARIOUS quantum information processings are proposed, many of which require maximally entangled states as resources, *e.g.*, quantum teleportation and dense coding *etc*[2], [1], [3]. Hence, it is often desired to generate maximally entangled states. However, the realized state is not necessarily a maximally entangled state. Thus, entanglement concentration is used for producing maximally entangled states (MES) from partially entangled pure states only by local operation and classical communication (LOCC), while entanglement distillation is used for producing them from partially entangled mixed states by LOCC. Therefore, entanglement concentration is an important issue in the field of quantum information.

In information theory, we often assume that the system is prepared as the independent and identical multiple copies of the given state. Such a condition is called independently and identically distributed (i.i.d.) condition. Under this condition, Bennett *et al.*[6] showed that the amount of entanglement of a partially entangled pure state $|\Phi\rangle\langle\Phi|$ is described by the entropy $H(\rho)$ of its partial traced state $\rho := \text{Tr}_{\mathcal{H}_B} |\Phi\rangle\langle\Phi|$, which is called the reduced density matrix. That is, they proved that an MES with size $2^{nH(\rho)}$ can be asymptotically produced from *n* identical copies of the state $|\Phi\rangle\langle\Phi|$ with a high enough probability. Furthermore, independently of the form of $|\Phi\rangle\langle\Phi|$, Hayashi and Matsumoto constructed a protocol satisfying the above property, which is called universal [7].

However, in the correlated physical system, the state of the total system cannot be regarded as independent and identical copies of a given state. In such a case, we have to treat general partial entangled pure state between two distinct parties. Indeed, this model is not so unnatural because the state on the total system is pure when this system is isolated from the other system. In this paper, as a general asymptotic method to treat this model asymptotically, we focus on the information spectrum method and apply it to entanglement concentration. The information spectrum method has been developed by Han and Verdú [9] for discussing general sequence of information sources/channels, and been established as a unified method to information theory in Han's textbook[13]. Indeed, this method has been applied to quantum information theory, for example, to quantum hypothesis testing[14] and quantum channel coding[15]. In this paper, we apply this method to entanglement concentration, and characterize the asymptotic production rate of a general sequence of partially entangled pure states without any assumption. The information spectrum method used in this paper is slightly different from the original Han-Verdú's method, and is close to Nagaoka-Hayashi's method[14].

1

In the derivation of our general asymptotic formulas, we essentially use the majorization method established by Nielsen[4]. Based on this method, he developed a necessary and sufficient condition for the possibility of transforming from a partially entangled pure state $|\Phi_1\rangle\langle\Phi_1|$ to another entangled pure state $|\Phi_2\rangle\langle\Phi_2|$ by using LOCC between the two parties \mathcal{H}_A and \mathcal{H}_B . This condition is characterized only by the eigenvalues of their reduced densities $\rho_i :=$ $\mathrm{Tr}_{\mathcal{H}_B} |\Phi_i\rangle\langle\Phi_i|, (i = 1, 2).$

Moreover, even in the i.i.d. case, the knowledge of the asymptotic production rate is not sufficient for estimating the production rate of MES for a given finite number of copies. In channel coding or source coding, for this analysis, we usually focus on the error exponents, *i.e.*, the exponential rate of error probability because the error goes to 0 exponentially when we choose our code suitably. In entanglement concentration, when we fix the production rate to a constant number less than the entropy rate, the optimal failure probability goes to 0 exponentially. Hence, based on its exponential rate (failure exponent), we can roughly estimate the failure probability for a given finite number of copies. As preceding researches, Hayashi et al.[8] derived the failure exponent of entanglement concentration in the i.i.d. case based on the method of types, and Hayashi and Matsumoto [7] did that of their universal entanglement concentration protocol. In this paper, we calculate the failure exponent of entanglement concentration in a more general setting.

In most problems in information theory, in the i.i.d. case, the correct (or success) probability exponentially goes to 0 when the rate is strictly better than the optimal rate. This exponential rate is called the correct (or success) exponent, and is one of famouse issues in information theory. Hayashi *et al.*[8] and Hayashi and Matsumoto [7] treated the success

M. Hayashi was with Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN. 2-1 Hirosawa, Wako, Saitama, 351-0198, Japan. Now, he is with Quantum Computation and Information Project, Japan Science and Technology Agency. 201 Daini Hongo White Bldg. 5-28-3, Hongo, Bunkyo-ku, Tokyo 113-0033, Japan. (e-mail masahito@qci.jst.go.jp)

exponent of entanglement concentration in the i.i.d. case. This paper proceed to the general sequence of partially entangled pure states.

One may think that such an exponential treatment is not essential. It is, however, more difficult to obtain the error and correct exponents asymptotically and tightly than the asymptotical optimal production rate. Hence, in order to derive these tight bounds of both exponents, we need better and more simple non-asymptotic evaluations. That is, such a nonasymptotic evaluation should be a better and more simple approximation for the optimal value. Therefore, even though the optimal correct exponent is useless, the non-asymptotic evaluations used for its derivation is quite useful.

Furthermore, the optimal rates with exponential constraint are characterized by Rényi entropy in the i.i.d. case. In this paper, we derive the same formulas under a weak assumption for the Rényi entropy. Using these formulas, we characterize the optimal rates based on the partition function.

Finally, we have to explain our formulation of entanglement concentration. There are two formulations in source coding. One is fixed length, in which the coding length is fixed, *i.e.*, is independent of the input data. The other is variable-length, in which the coding length is variable, *i.e.*, depends on the input data. Similarly to source coding, we can consider two similar formulations in entanglement concentration. In Bennett *et al.*[6]'s protocol and Hayashi and Matsumoto[7]'s protocol, a local measurement is required as the first step, and the length of the MSE generated finally depends on the data of this local measurement. Hence, their protocol is a variable-length entanglement concentration.

On the other hand, based on Nielsen's result[4], Hayashi et al.[8] discussed entanglement concentration protocols producing the MES with the fixed size. Hence, such protocols are called fixed-length entanglement concentration, which are classified into two formulations as follows. In the first formulation, we produce, without a failure, an approximately MES from a partially entangled pure state. Its performance is represented by the size of the MES and the fidelity between the appropriate MES and the final state. This kind of entanglement concentration is called deterministic fixed-length entanglement concentration (DFLEC). In the other formulation, we produce an MES itself, allowing a failure probability, from a partially entangled pure state. The performance of this protocol is evaluated by the size of the MES and the failure probability. This protocol is called a probabilistic fixed-length entanglement concentration (PFLEC). Hayashi et al.[8] treated these two formulations in the i.i.d. case. In this paper, we discuss them in a more general model.

This paper is organized as follows. In section II, we give the mathematical definitions of the optimal rates with respective conditions, (constant constraint, exponetial constraint) for the genereal sequence of partially entangled pure state in two formulations of FLEC. As the main results, characterizations of these quantities are given based on information spectrum. That is, we discover a general relation between the performance of entanglement concentration and the eigenvalues of the reduced density (partially traced state). In section III, the optimal rates of FLECs are characterized by the Rényi entropy.

In section IV, we apply these formulas to the case when the reduced density is given as a thermal state. In section V, the performances of the two FLEC types in a non-asymptotic case are characterized by applications of Nielsen's result [4] and Lo and Popescu's results[17]. In section VI, the main result is verified by applying several lemmas described in section V to an asymptotic case. In section VII, the relation between entanglement concentration and random number generation is discussed. The appendix A summarizes relations for the quantum analogue of the information spectrums based on the original definition[14], which are necessary for verifying the main result.

II. MAIN RESULTS

When the two distinct parties, Alice and Bob, have their respective systems \mathcal{H}_A and \mathcal{H}_B , the total system is described by the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$. In quantum information, as is mentioned in section I, one of main issues is the characterization of entanglement between these distinct parties. If the state on total syste is a pure state $\Phi \in \mathcal{H}_A \otimes \mathcal{H}_B$, it is known that its entanglement between two parties can be characterized by the reduced density (partially traced state) $\rho := \operatorname{Tr}_B |\Phi\rangle \langle \Phi|$. In particular, if the reduced density ρ is the completely mixed state $\frac{1}{d_A}I$, it is called maximally entagled, where d_A denotes the dimension of the system \mathcal{H}_A . Hence, if the pure state $\Psi \in \mathcal{H}_A \otimes \mathcal{H}_B$ is maximally entagled, there exist completely orthogonal basis $\{e_i\}$ and $\{e'_i\}$ on \mathcal{H}_A and \mathcal{H}_B , respectively such that

$$\Psi = \sqrt{\frac{1}{d_A}} \sum_{i=1}^{d_A} e_i \otimes e'_i.$$

While any quantum operation is mathematically described by trace-preserving completely positive (TP-CP) map, in the entanglement concentration of the initial pure state Φ on distinct two parties \mathcal{H}_A and \mathcal{H}_B , our operation is often restricted to a quantum operation with an LOCC implementation between \mathcal{H}_A and \mathcal{H}_B . Hence, a deterministic fixed-length entanglement concentration (DFLEC) is an LOCC quantum operation Ctogether with a maximally entangled state Ψ , on a subspace $\mathcal{H}'_A \otimes \mathcal{H}'_B$, *i.e.*, it is described as (C, Ψ) . Since this protocol (C, Ψ) transforms the initial pure state $|\Phi\rangle\langle\Phi|$ to the final state $C(\Phi) := C(|\Phi\rangle\langle\Phi|)$, its performance is evaluated by the fidelity $\langle\Psi|C(\Phi)|\Psi\rangle$ and the size $L(\Psi)$ of Ψ , which equals $H(\operatorname{Tr}_B |\Psi\rangle\langle\Psi|)$.

For a rigid analysis of the probabilistic fixed-length entanglement concentration, we have to discuss a measuring operation that describes a quantum measurement with the final state as well as the probability distribution of the measured data. The measuring operation is given as a CP map valued measure $I = \{I_i\}_i$ whose sum is a TP-CP map; *i.e.*, every I_i is a CP map, and $\sum_i I_i$ is a TP-CP map. It is often called an instrument. When we perform a quantum measurement corresponding to $I = \{I_i\}_i$ on the system with a state ρ , we obtain the measured data *i* and the final state $\frac{1}{\operatorname{Tr} I_i(\rho)} I_i(\rho)$ with the probability $\operatorname{Tr} I_i(\rho)$. Hence, a probabilistic fixed-length entanglement concentration (PFLEC) of an initial pure state $\Phi \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a two-valued instruments $I = \{I_0, I_1\}$ with an LOCC implementation satisfying that $I_1(\Phi)/\operatorname{Tr} I_1(\Phi)$ is a maximally entangled state $|\Psi\rangle\langle\Psi|$ on a subspace $\mathcal{H}'_A \otimes \mathcal{H}'_B$, where $I_i(|\Phi\rangle\langle\Phi|)$ is abbreviated to $I_i(\Phi)$. That is, the event 1 corresponds to success, and the event 0 does to failure. Thus, its performance is characterized by the failure probability $\operatorname{Tr} I_0(\Phi)$ and the size $L(I) := L(\Psi)$ of the final maximally entangled state.

Here, we briefly discuss the relation between two kinds of fixed-length entanglement concentrations. For any PFLEC $I = \{I_0, I_1\}$ of Φ , the pair $(I_1 + I_0, I_1(\Phi) / \operatorname{Tr} I_1(\Phi))$ becomes a DFLEC and its fidelity between the final state and the desired maximally entangled state $I_1(\Phi) / \operatorname{Tr} I_1(\Phi)$ is greater than the success probability of the DFLEC $I = \{I_0, I_1\}$:

$$\operatorname{Tr}\left[(I_1+I_0)(\Phi)\frac{I_1(\Phi)}{\operatorname{Tr}I_1(\Phi)}\right] \ge \operatorname{Tr}I_1(\Phi).$$
(1)

That is, for any a given PFLEC protocol, there exists a DFLEC protocol whose performance is better than the given PFLEC protocol.

In the quantum system, if n systems are prepared identically to the system $\mathcal{H}_A \otimes \mathcal{H}_B$, the total system is described by $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$. If the state of every system $\mathcal{H}_A \otimes \mathcal{H}_B$ is the pure state Φ and if each system is independently prepared, the state of the total system is written by the tensor product pure state $\Phi^{\otimes n}$. Such a case is called the i.i.d. case. However, even if the state of each system coincides with each other, if they are not independent of each other, the state of total system is not a tensor product state. In order to treat such a general case, we focus on a general sequence of the pair of the joint system with distinct two parties $\mathcal{H}_{A,n}$ and $\mathcal{H}_{B,n}$ and the partially entangled pure state $\Phi_n \in \mathcal{H}_{A,n} \otimes \mathcal{H}_{B,n}$ with an asymptotic situation. Note that, in this notation, the space $\mathcal{H}_{A,n}$ and $\mathcal{H}_{B,n}$ are generalizations of $\mathcal{H}_A^{\otimes n}$ and $\mathcal{H}_B^{\otimes n}$, and Φ_n is a generalization of the *n*-tensor product vector $\Phi^{\otimes n}$.

In order to discuss the asymptotic optimal performance in such a general case, we optimize the production rate of MES with three asymptotic constraints for the failure probability or fidelity. Concerning the PFLEC, we focus on the following conditions:

- Constant constraint: The asymptotic failure probability is less than a fixed constant.
- Exponential constraint for the failure probability: When we choose a good DFLEC protocol, failure probability goes to 0 exponentially. Hence, as another criterion, we restrict our DFLEC satisfying that the exponent of failure probability is greater than a fixed exponent.
- Exponential constraint for the success probability: If we choose a bad DFLEC, the success probability goes to 0 exponentially. Among such PFLEC protocols, if this exponent, *i.e.*, the success exponent, is greater, the protocol is worse. Hence, we can consider the optimization of the production rate of MES with the constraint that the success exponent is less than a fixed exponent.

Thus, concerning PFLEC, we focus on the following values:

$$B_P(\epsilon) := \sup_{\{I^n\}} \left\{ \underline{\lim} \frac{\log L(I^n)}{n} \Big| \overline{\lim} I_0^n(\Phi_n) \le \epsilon \right\}$$
$$B_{e,P}(r) := \sup_{\{I^n\}} \left\{ \underline{\lim} \frac{\log L(I^n)}{n} \Big| \underline{\lim} \frac{-1}{n} \log \operatorname{Tr} I_0^n(\Phi_n) \ge r \right\}$$
$$B_{e,P}^*(r) := \sup_{\{I^n\}} \left\{ \underline{\lim} \frac{\log L(I^n)}{n} \Big| \overline{\lim} \frac{-1}{n} \log \operatorname{Tr} I_1^n(\Phi_n) \le r \right\}.$$

In the DFLEC case, we obtain several criteria by replacing the success probability in the above discussion by the fidelity. That is, we can define the following values:

$$B_D(\epsilon) := \sup_{\{(C^n, \Psi_n)\}} \left\{ \underbrace{\lim \frac{1}{n} \log L(\Psi_n)}_{\lim \langle \Psi_n | C^n(\Phi_n) | \Psi_n \rangle \ge 1 - \epsilon} \right\}$$
$$B_{e,D}(r) := \sup_{\{(C^n, \Psi_n)\}} \left\{ \underbrace{\lim \frac{1}{n} \log L(\Psi_n)}_{\lim \frac{1}{n} \log (1 - \langle \Psi_n | C^n(\Phi_n) | \Psi_n \rangle) \ge r} \right\}$$
$$B_{e,D}^*(r) := \sup_{\{(C^n, \Psi_n)\}} \left\{ \underbrace{\lim \frac{1}{n} \log L(\Psi_n)}_{\lim \frac{1}{n} \log L(\Psi_n)} \right|$$
$$\frac{1}{\lim \frac{-1}{n} \log \langle \Psi_n | C^n(\Phi_n) | \Psi_n \rangle \le r} \right\}.$$

Hence, it is trivial from (1) that

$$B_1(\epsilon) \ge B_2(\epsilon), \quad B_{e,D}(r) \ge B_{e,2}(r), \quad B_{e,D}^*(r) \ge B_{e,2}^*(r).$$
(2)

In this paper, we treat a quantum analogue of information spectrums to analyze the above values. For such an analysis, we need the following definitions. For a self-adjoint operator X, we can denote the projection $\sum_{x_i \ge c} E_i$ by $\{X \ge c\}$, where the spectral decomposition is given by $X = \sum_i x_i E_i$. We can define the projections $\{X > c\}, \{X < C\}, \{X \le c\}, etc.$ in a similar manner. Let ρ_n be the reduced density $\operatorname{Tr}_{\mathcal{H}_{B,n}} |\phi_n\rangle \langle \phi_n|$ and define

$$K(a) := \overline{\lim} \operatorname{Tr} \rho_n \{ \rho_n - e^{-na} \ge 0 \}$$

$$\underline{\zeta}^c(a) := \underline{\lim} \frac{-1}{n} \log \operatorname{Tr} \rho_n \{ \rho_n - e^{-na} > 0 \}.$$

When the limit

$$\lim \frac{-1}{n} \log \operatorname{Tr} \rho_n \{ \rho_n - e^{-na} < 0 \}$$
(3)

exists, we denote it by $\zeta(a)$. These definitions can also be written as

$$K(a) = \overline{\lim} p_n \left\{ \frac{-1}{n} \log p_{n,i} \le a \right\}$$
(4)

$$\underline{\zeta}^{c}(a) = \underline{\lim} \, \frac{-1}{n} \log p_n \left\{ \frac{-1}{n} \log p_{n,i} \le a \right\}$$
(5)

$$\zeta(a) = \lim \frac{-1}{n} \log p_n \left\{ \frac{-1}{n} \log p_{n,i} > a \right\}, \qquad (6)$$

where every $p_{n,i}$ is an eigenvalue of ρ_n and can be regarded as a probability distribution. Hence, the quantity $K(a), \underline{\zeta}^c(a)$, and $\zeta(a)$ denotes the degree of concentration of the e^{na} dimensional subspace. Note that the function $\zeta^c(a)$ decreases monotonically, while the function $\zeta(a)$ increases monotonically. Indeed, in the classical case, the value K(a) gives the asymptotic performances of fixed-length source coding[12] and uniform random number generation[19], [13] with asymptotic constant constraint. Moreover, the quantities $\underline{\zeta}^c(a)$ and $\zeta(a)$ gives the asymptotic optimal performance of source coding with the exponential constraint[12] and that of simulation of random process with KL divergence criterion[18]. As is mentioned in section VII, $\zeta(a)$ gives the asymptotic optimal performance of intrinsic randomness with KL divergence criterion[22].

As is mentioned in the following main theorem, the optimal production rate of MES can be characterized by how densely the eigen values of the reduced density matrix concentrate a small space.

Theorem 1: Without any assumption, for every $\epsilon \in [0, 1]$ we have

$$B_D(\epsilon) = B_P(\epsilon) = \sup_R \{R | K(R) \le \epsilon\}$$

$$B_{e,D}(r) = B_{e,P}(r) = \sup_R \{R | \underline{\zeta}^c(R) \ge r\}.$$

When the limit (3) exists and there exists a real number *a* such that $\zeta(a) \leq \underline{\zeta}^{c}(a)$, we have

$$B_{e,D}^{*}(r) = \sup_{a} \left\{ a - r \left| \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \right| a' \le a \right\} + \frac{a}{2} \le r \right\}$$
$$= \sup_{a} \left\{ \frac{a}{2} - \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \right| a' \le a \right\} \right|$$
$$\inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \right| a' \le a \right\} + \frac{a}{2} \le r \right\}$$
$$B_{e,P}^{*}(r) = \sup\{a - \zeta(a) | \zeta(a) \le r\}.$$

This theorem is proved in section VI after preparing the appropriate discussion.

Remark 1: As is mentioned in Nagaoka and Hayashi[14] the quantum versions of $K(a), \underline{\zeta}^c(a)$, and $\zeta(a)$ give the asymptotic performances of fixed-length source coding. In particular, the optimal rate with the constraint for the constant error exponent is given as

$$\sup_{a} \{a - \zeta(a) | \zeta(a) < r\},\tag{7}$$

which is almost similar to $B^*_{e,P}(r)$. For a proof only of the classical case, see Han [12]. For a proof in the classical and quantum case, see Nagaoka and Hayashi [14].

III. ASYMPTOTIC FORMULAS BASED ON RÉNYI ENTROPY

In the classical and quantum fixed-length source coding of i.i.d. information source, it is known that the optimal rate with the constant constraint for error exponent is described by the Rényi entropy $\psi(s) := \log \sum_i p_i^s$ [21]. Concerning FLEC of the i.i.d. source, as is described in Theorem 2, Hayashi *et al.*[8] showed that this kinds of optimal rates can be described by the Rényi entropy. In this section, using Theorem 1, we derive the same formula in a more general setting.

Theorem 2: Hayashi et al.[8] When $\rho_n = \rho^{\otimes n}$, the relations

$$B_D(\epsilon) = B_P(\epsilon) = H(\rho), \quad \forall \epsilon \text{ such that } 1 > \epsilon \ge 0$$
 (8)

$$B_{e,D}(r) = B_{e,P}(r) = \sup_{s \ge 1} \frac{r + \psi(s)}{1 - s}$$
(9)

$$B_{e,P}^{*}(r) = \min_{0 \le s \le 1} \frac{sr + \psi(s)}{1 - s}$$
(10)

$$B_{e,D}^*(r) = \begin{cases} \min_{\substack{0 \le s \le 1}} \frac{sr + \psi(s)}{1-s} & \text{if } r \le -\frac{1}{2}\psi'\left(\frac{1}{2}\right) - \psi\left(\frac{1}{2}\right) \\ 2\psi\left(\frac{1}{2}\right) + r & \text{otherwise} \end{cases}$$
(11)

hold, where

$$H(\rho) := -\operatorname{Tr} \rho \log \rho, \quad \psi(s) := \log \operatorname{Tr} \rho^s.$$

In particular, the above formulas of some special cases are written as

$$B_{e,D}(r) = B_{e,P}(r) = H_{\infty} \text{ if } r \ge H_{\infty} = \lim_{s \to \infty} -\psi'(s)$$
$$B_{e,P}^{*}(r) = \psi(0) \text{ if } r \ge -\psi'(0) - \psi(0),$$

where

$$H_{\infty} := \lim_{s \to \infty} \frac{-\psi(s)}{s}.$$

The following is the generalization of the above theorem.

Theorem 3: Letting $\psi_n(s) := \log \operatorname{Tr} \rho_n^s$, we assume that the limit $\overline{\psi}(s) := \lim_n \frac{\psi_n(s)}{\overline{\psi}'(s)}$ exists and that its first and second derivatives $\overline{\psi}'(s)$ and $\overline{\psi}''(s)$ exist for $s \in (0,1) \cup (1,\infty)$. Then,

$$\overline{H}_{-} \le B_{D}(\epsilon) = B_{P}(\epsilon) \le \overline{H}_{+}$$
(12)

$$B_{e,D}(r) = B_{e,P}(r) = \sup_{s \ge 1} \frac{r + \psi(s)}{1 - s}$$
(13)

$$B_{e,P}^{*}(r) = \min_{0 \le s \le 1} \frac{sr + \psi(s)}{1 - s}$$
(14)

$$B_{e,D}^{*}(r) = \begin{cases} \min_{\substack{0 \le s \le 1 \\ 2\overline{\psi}\left(\frac{1}{2}\right) + r}} & \text{if } r \le -\frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right) - \overline{\psi}\left(\frac{1}{2}\right) \\ \text{otherwise,} \end{cases}$$
(15)

where

$$\overline{H}_{-} := -\overline{\psi}'(1+0), \quad \overline{H}_{+} := -\overline{\psi}'(1-0)$$

In particular, we have

$$B_{e,D}(r) = B_{e,P}(r) = \overline{H}_{\infty} \text{ if } r \ge \overline{H}_{\infty} = \lim_{s \to \infty} -\overline{\psi}'(s)$$
$$B_{e,P}^*(r) = \overline{\psi}(0) \text{ if } r \ge -\overline{\psi}'(+0) - \overline{\psi}(0),$$

where $\overline{H}_{\infty} := \lim_{s \to \infty} \frac{-\overline{\psi}(s)}{s}$.

The equations (9), (10), and (11) follow from the equations (13), (14), and (15). The equation (8) follows from the equation (12). Hence, Theorem 3 can be regarded as a generalization of Theorem 2. Since Hayashi *et al.* [8]used the method of type, they proved Theorem 2 only in the finite-dimensional case. Hence, its infinite-dimensional case is proved by this paper first time.

Remark 2: Under the same assumption as Theorem 3, we can similarly prove that

$$\sup_{a} \{a - \zeta(a) | \zeta(a) < r\} = \min_{0 \le s \le 1} \frac{sr + \psi(s)}{1 - s}$$

which gives the optimal rate with the constant constraint for error exponent in the fixed-length source coding.

Proof: As is discussed in Appendix B, Gärtner-Ellis theorem [20] yields that

$$\zeta(a) = \begin{cases} 0 & \text{if } a \le \overline{H}_+ \\ \sup_{0 \le s \le 1} (1-s)a - \overline{\psi}(s) > 0 & \text{if } \overline{H}_+ < a < -\overline{\psi}'(0) \end{cases}$$
(16)

$$\underline{\zeta}^{c}(a) = \begin{cases} 0 & \text{if } \overline{H}_{-} \leq a \\ \sup(1-s)a - \overline{\psi}(s) > 0 & \text{if } \overline{H}_{\infty} < a < \overline{H}_{-} \\ \sum_{s \geq 1} \infty & \text{if } a < \overline{H}_{\infty}. \end{cases}$$
(17)

Note that

$$\zeta(-\overline{\psi}'(+0) - 0) = -\overline{\psi}'(+0) - \overline{\psi}(0) \tag{18}$$

$$\underline{\zeta}^c(\overline{H}_{\infty}+0) = \overline{H}_{\infty}.$$
(19)

Moreover, it follows from the discussion in Appendix B that $\overline{\psi}(s)$ is convex. Since $\overline{\psi}''(s)$ exists for $s \in (0,1) \cup (1,\infty)$, we have

$$\overline{\psi}''(s) \ge 0 \quad s \in (0,1) \cup (1,\infty). \tag{20}$$

For any real number a satisfying $\overline{H}_{\infty} \leq a \leq -\overline{\psi}'(+0)$, we define s(a) by

$$a = -\overline{\psi}'(s(a)). \tag{21}$$

Hence, equations (16) and (17) yield that

$$\zeta(a) = \begin{cases} 0 & \text{if } a \le \overline{H}_+ \\ (1 - s(a))a - \overline{\psi}(s(a)) & \text{if } \overline{H}_+ < a < -\overline{\psi}'(0) \end{cases}$$
(22)

$$\underline{\zeta}^{c}(a) = \begin{cases} 0 & \text{if } \overline{H}_{-} \leq a \\ (1 - s(a))a - \overline{\psi}(s(a)) & \text{if } \overline{H}_{\infty} < a < \overline{H}_{-} \\ \infty & \text{if } a < \overline{H}_{\infty}. \end{cases}$$
(23)

First, we prove (13) for the case in which $r < \overline{H}_{\infty}$. In this case, we can define a_r and s_r by $\underline{\zeta}^c(a_r) = r$ and $s_r := s(a_r)$. Thus, we have

$$(1 - s_r)a_r - \overline{\psi}(s_r) = r \tag{24}$$

$$-(1-s_r)\overline{\psi}'(s_r) - \overline{\psi}(s_r) = r.$$
 (25)

Using (24), we can calculate $B_{e,D}(r)$ and $B_{e,P}(r)$ as

$$B_{e,D}(r) = B_{e,P}(r) = a_r = \frac{r + \psi(s_r)}{1 - s_r}.$$

The derivative of the function $f_1(s) := \frac{r + \overline{\psi}(s)}{1-s} (s \ge 1)$ is given by

$$f_1'(s) = \frac{\overline{\psi}'(s)(1-s) + r + \overline{\psi}(s)}{(1-s)^2}.$$

From (25), the equation $f_1(s_r)' = 0$ holds. The derivative of the numerator of $f'_1(s)$ is

$$\left(\overline{\psi}'(s)(1-s)+r+\overline{\psi}(s)\right)'=\overline{\psi}''(s)(1-s)\leq 0,$$

the final inequality inequality follows from (20). Therefore, $B_{e,D}(r) = B_{e,P}(r) = f_1(s_r) = \max_{s>1} f_1(s).$

Next, we prove (13) for the case in which $r \ge \overline{H}_{\infty}$. From (17), if $a > \overline{H}_{\infty}$, then $\underline{\zeta}^{c}(a) < r$. Otherwise, $\underline{\zeta}^{c}(a) \ge r$. Thus, $B_{e,D}(r) = B_{e,P}(r) = \overline{H}_{\infty}$. Since the numerator of $f'_{1}(s)$ equals

$$r + \overline{\psi}'(s)(1-s) + \overline{\psi}(s) = r - \underline{\zeta}^c(-\overline{\psi}'(s)) > 0,$$

we obtain $f'_1(s) > 0$. Therefore,

$$\sup_{s \ge 1} \frac{r + \psi(s)}{1 - s} = \lim_{s \to \infty} \frac{r + \psi(s)}{1 - s} = \overline{H}_{\infty}.$$

Proceeding to (14) for the case in which $r < -\overline{\psi}'(+0) - \overline{\psi}(0)$, we define a_r and s_r by $\zeta(a_r) = r$ and $s_r := s(a_r)$. Thus, we have

$$(1 - s_r)a_r - \overline{\psi}(s_r) = r \tag{26}$$

$$-(1-s_r)\overline{\psi}'(s_r) - \overline{\psi}(s_r) = r.$$
(27)

Using (26), we can calculate $B^*_{e,P}(r)$:

$$B_{e,P}^{*}(r) = a_r - r = \frac{s_r r + \overline{\psi}(s_r)}{1 - s_r}.$$

The derivative of the function $f_2(s) := \frac{sr + \overline{\psi}(s)}{1-s} (0 < s < 1)$ is given by

$$f'_2(s) = rac{\overline{\psi}'(s)(1-s) + r + \overline{\psi}(s)}{(1-s)^2}.$$

From (27), the equation $f_2(s_r)' = 0$ holds. The derivative of the numerator of $f'_2(s)$ is given by

$$\left(\overline{\psi}'(s)(1-s) + r + \overline{\psi}(s)\right)' = \overline{\psi}''(s)(1-s) \ge 0$$

because of (20). Therefore, $B_{e,P}^*(r) = f_2(s_r) = \min_{s \ge 1} f_2(s)$.

Next, we prove (14) for the case in which $r \ge -\overline{\psi}'(+0) - \overline{\psi}(0)$. If $a < -\overline{\psi}'(+0)$, then $\zeta(a) < r$. Otherwise, $\zeta(a) > r$. Thus, it follows from (18) that $B^*_{e,P}(r) = \lim_{\epsilon \to +0} (-\overline{\psi}'(+0) - \epsilon) - \zeta(-\overline{\psi}'(+0) - \epsilon) = -\overline{\psi}'(+0) - (-\overline{\psi}'(+0) - \overline{\psi}(0)) = \overline{\psi}(0)$. Since the numerator of $f'_2(s)$ is

$$r + \overline{\psi}'(s)(1-s) + \overline{\psi}(s) = r - \underline{\zeta}^c(-\overline{\psi}'(s)) > 0,$$

then $f'_2(s) > 0$. Therefore,

$$\min_{0 \le s \le 1} \frac{sr + \psi(s)}{1 - s} = \lim_{s \to 0} \frac{sr + \psi(s)}{1 - s} = \overline{\psi}(0).$$

Next, we prove (15). We can calculate the derivative of $\zeta(a)-\frac{a}{2}$ as

$$\left(\zeta(a) - \frac{a}{2}\right)' = 1 - s(a) - s'(a)a - \overline{\psi}'(s(a))s'(a) - \frac{1}{2}$$
$$= 1 - s(a) - s'(a)a + s'(a)a - \frac{1}{2} = \frac{1}{2} - s(a).$$

This derivative is 0 if and only if $s(a) = \frac{1}{2}$, *i.e.*, $a = -\overline{\psi}'(\frac{1}{2})$. The second derivative is calculated as

$$\left(\zeta(a) - \frac{a}{2}\right)'' = -s'(a) = \frac{1}{\overline{\psi}''(s(a))} > 0,$$
 (28)

where the final equation follows from $1 = \overline{\psi}''(s(a))s'(a)$ which can be derived from (21). Thus, the function $a \mapsto \zeta(a) - \frac{a}{2}$ is strictly convex, and its minimum value equals $\zeta\left(-\overline{\psi}'\left(\frac{1}{2}\right)\right) + \frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right)$, which is attained at $a = -\overline{\psi}'\left(\frac{1}{2}\right)$. Hence, we have

$$\inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \le a \right\} = \left\{ \begin{array}{cc} \zeta(a) - \frac{a}{2} & \text{if } a \le -\overline{\psi}'\left(\frac{1}{2}\right) \\ -\overline{\psi}\left(\frac{1}{2}\right) & \text{if } a > -\overline{\psi}'\left(\frac{1}{2}\right) \end{array} \right.$$

where we use the equation $\zeta \left(-\overline{\psi}'\left(\frac{1}{2}\right)\right) = -\overline{\psi}\left(\frac{1}{2}\right) - \frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right)$, which follows from (22). Since $\zeta(-\overline{\psi}'(1/2)) = -\overline{\psi}\left(\frac{1}{2}\right) - \frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right)$, we have

$$\sup_{a \leq -\overline{\psi}'(1/2)} \{a - r | \zeta(a) \leq r\}$$
$$= \begin{cases} a_r - r & \text{if } r \leq -\overline{\psi}\left(\frac{1}{2}\right) - \frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right) \\ -\overline{\psi}'(1/2) - r & \text{if } r > -\overline{\psi}\left(\frac{1}{2}\right) - \frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right). \end{cases}$$

Remember that a_r is defined such that $\zeta(a_r) = r$. Moreover, we have

$$\sup_{a>-\overline{\psi}'(1/2)} \left\{ a - r \left| -\overline{\psi}\left(\frac{1}{2}\right) + \frac{a}{2} \le r \right\} \right.$$
$$= \left\{ \begin{array}{l} 0 & \text{if } r \le -\overline{\psi}\left(\frac{1}{2}\right) - \frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right) \\ 2\overline{\psi}\left(\frac{1}{2}\right) + r & \text{if } r > -\overline{\psi}\left(\frac{1}{2}\right) - \frac{1}{2}\overline{\psi}'\left(\frac{1}{2}\right). \end{array} \right.$$

Therefore,

Using a discussin similar to (14), we can show (15).

IV. CORRELATED SYSTEM

In this section, we consider the application of Theorem 3 to correlated systems. As an example, the initial state is assumed to be a ground state with the Hamiltonian $\sum_i H_i + H_{i,i+1}$ on the system $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$, where H_i is the Hamiltonian of the *i*-th joint system between A and B, and $H_{i,i+1}$ is its interaction term between the *i*-th and *i* + 1-th systems. However, it is not so easy to calculate $\overline{\psi}(s)$ in this case. Hence, we focus on a more ideal case.

Assume that the total system $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ is isolated from other systems. We also assume that the system $\mathcal{H}_B^{\otimes n}$ is sufficiently large, and the interaction between the system $\mathcal{H}_A^{\otimes n}$ and the system $\mathcal{H}_B^{\otimes n}$ is ideal so that the system $\mathcal{H}_B^{\otimes n}$ can be regarded as the heat bath of the system $\mathcal{H}_A^{\otimes n}$. Now, we suppose that the Hamiltonian $\sum_i H_{A,i} + H_{A,i,i+1}$ on the system $\mathcal{H}_A^{\otimes n}$. Hence, the state of the total system is pure, and the reduced density on A is the thermal state with the Hamiltonian $\sum_i H_{A,i} + H_{A,i,i+1}$. Now, we define the partition function as

$$\Xi(\beta) := \lim \frac{1}{n} \log \operatorname{Tr} \exp(\beta \sum_{i} H_{A,i} + H_{A,i,i+1}).$$
(29)

Thus, when the inverse temperature is β_0 and the partition function is continuous and differentiable, the $\overline{\psi}(s)$ can be calculated as

$$\overline{\psi}(s) = \lim \frac{1}{n} \log \operatorname{Tr} \left(\frac{\exp(\beta_0 \sum_i H_{A,i} + H_{A,i,i+1})}{\operatorname{Tr} \exp(\beta_0 \sum_i H_{A,i} + H_{A,i,i+1})} \right)^s$$
$$= \lim \frac{1}{n} \log \operatorname{Tr} \exp(s\beta_0 \sum_i H_{A,i} + H_{A,i,i+1}) - s\Xi(\beta_0)$$
$$= \Xi(s\beta_0) - s\Xi(\beta_0).$$

Hence,

$$B_{D}(\epsilon) = B_{P}(\epsilon) = -\beta_{0}\Xi'(\beta_{0}) + \Xi(\beta_{0})$$

$$B_{e,D}(r) = B_{e,P}(r) = \sup_{s \ge 1} \frac{r + \Xi(s\beta_{0}) - s\Xi(\beta_{0})}{1 - s}$$

$$B_{e,P}^{*}(r) = \min_{0 \le s \le 1} \frac{sr + \Xi(s\beta_{0}) - s\Xi(\beta_{0})}{1 - s}$$

$$B_{e,D}^{*}(r) = \begin{cases} \min_{0 \le s \le 1} \frac{sr + \Xi(s\beta_{0}) - s\Xi(\beta_{0})}{1 - s} & \text{if } r \le r_{1/2} \\ 2\Xi\left(\frac{\beta_{0}}{2}\right) - \Xi(\beta_{0}) + r & \text{otherwise,} \end{cases}$$

where

$$r_{1/2} := -\frac{\beta_0}{2} \Xi'\left(\frac{\beta_0}{2}\right) + \Xi(\beta_0) - \Xi\left(\frac{\beta_0}{2}\right)$$

Note that the above formulas are based only on the partition function. Hence, it is expected to apply them to other cases. Moreover, we can derive similar formulas concerning classical and quantum fixed-length source coding.

V. NON-ASYMPTOTIC THEORY

In order to derive general asymptotic formulas based on the quantum information spectrums, we need to prepare approximate formulas for non-asymptotic setting based on the form of the reduced density ρ . For this purpose, we focus on majorization, because it gives a necessary and sufficient condition for the possibility of transforming from a partially entangled pure state $|\Phi_1\rangle\langle\Phi_1|$ to another entangled pure state $|\Phi_2\rangle\langle\Phi_2|$ by using LOCC between the two parties \mathcal{H}_A and $\mathcal{H}_B[4]$. Suppose that $p = (p_1, \ldots, p_d)$ and $q = (q_1, \ldots, q_d)$ are probability distributions. The probability p majorizes q, (equivalently q is majorized by p), written $p \succeq q$, if for each k in the range

$$\sum_{j=1}^k p_j^\downarrow \geq \sum_{j=1}^k q_j^\downarrow.$$

The elements indicated by \downarrow are taken in descending order; for example, p_1^{\downarrow} is the largest element in (p_1, \ldots, p_d) . The majorization relation is a partial order. To discuss entanglement transformation, we need to treat probability distributions consisting of eigenvalues of a reduced density ρ . The reduced density ρ majorizes another reduced density σ written $\rho \succeq \sigma$, if the probability distribution $p(\rho)$ consisting of eigenvalues of a reduced density ρ majorizes the probability distribution $p(\sigma)$ defined by the other reduced density σ . In particular, the reduced density ρ strongly majorizes another reduced density σ , written $\rho \succ \sigma$, if $p(\rho) \succeq p(\sigma)$ and if the eigenvector corresponding to $p(\sigma)_j^{\downarrow}$ coincides with the eigenvector corresponding to $p(\sigma)_j^{\downarrow}$. That is, this condition requires that there exists a common basis diagonalizing ρ and σ . For more information about majorization, please see Bhatia's text book[16]. Using these notations, we can describe Nielsen's condition for LOCC transformation as follows.

Lemma 4: Nielsen[4] We can transform an entangled state Φ to another entangled state Ψ by LOCC if and only if $\sigma \succeq \rho$, where ρ (σ) is the reduced density (partially traced state) of Φ (Ψ), respectively.

Therefore, by using the above Nielsen's Lemma, the optimal performance of DFLEC, *i.e.*, the maximum fidelity can be evaluated based on majorization as follows.

Lemma 5: Let σ be the reduced density of a given pure state Ψ , and ρ be the reduced density of the given initial pure state Φ . Then, we have

$$\max_{C} \langle \Psi | C(\Phi) | \Psi \rangle = \max_{\rho' \succeq \rho} \max_{U: \text{unitary}} \left(\operatorname{Tr} \sqrt{\rho'} \sqrt{\sigma} U \right)^2, \quad (30)$$

where the quantum operation C runs over all quantum operations with LOCC in the maximum of LHS. If Ψ is a maximally entangled state with the size L, *i.e.*, the operator $T := L\sigma$ is a projection with the rank L, then the relation

$$\max_{\rho' \succeq \rho} \max_{U:\text{unitary}} \left(\operatorname{Tr} \sqrt{\rho'} \sqrt{\sigma} U \right)^2 = \max_{\rho' \succeq \rho} \frac{\left(\operatorname{Tr} \sqrt{\rho'} T \right)^2}{L} \quad (31)$$

holds.

Proof: For any pure state Ψ , Φ , we have

$$\langle \Psi | \Phi \rangle = \operatorname{Tr}_{\mathcal{H}_A} \sqrt{\rho} \sqrt{\sigma} U_2^* U_1,$$

where two unitaries U_1 and U_2 are defined as

$$U_1 \rho U_1^* = \operatorname{Tr}_{\mathcal{H}_A} |\Phi\rangle \langle \Phi|, \quad U_2 \sigma U_2^* = \operatorname{Tr}_{\mathcal{H}_A} |\Psi\rangle \langle \Psi|.$$

Using Lemma 4, we can prove (30). Next, we choose normalized basis $\{e_i\}_{i=1}^L$ and $\{f_i\}_{i=1}^L$ as

$$T = \sum_{i=1}^{L} |e_i\rangle \langle e_i|, \quad f_i := U^* e_i.$$

Using Schwartz inequality twice, we have

$$\operatorname{Tr} \sqrt{\rho'} TU = \sum_{i=1}^{L} \langle f_i | \sqrt{\rho'} | e_i \rangle$$
$$\leq \sum_{i=1}^{L} \sqrt{\langle f_i | \sqrt{\rho'} | f_i \rangle} \sqrt{\langle e_i | \sqrt{\rho'} | e_i \rangle}$$
$$\leq \sqrt{\sum_{i=1}^{L} \langle f_i | \sqrt{\rho'} | f_i \rangle} \sqrt{\sum_{i=1}^{L} \langle e_i | \sqrt{\rho'} | e_i \rangle}.$$

Since

$$\sum_{i=1}^{L} \langle f_i | \sqrt{\rho'} | f_i \rangle, \sum_{i=1}^{L} \langle e_i | \sqrt{\rho'} | e_i \rangle \le \max_{V: \text{unitary}} \operatorname{Tr} V \sqrt{\rho'} V^* T,$$

we obtain

$$\max_{U,V:\text{unitary}} \operatorname{Tr} V \sqrt{\rho'} V^* T U = \max_{V:\text{unitary}} \operatorname{Tr} V \sqrt{\rho'} V^* T.$$

Therefore, the equation

$$\max_{\rho' \succeq \rho} \max_{U: \text{unitary}} \operatorname{Tr} \sqrt{\rho'} T U = \max_{\rho' \succeq \rho} \operatorname{Tr} \sqrt{\rho'} T$$
(32)

holds because $U\rho U^* \succeq \rho$. Equations (30) and (32) guarantee (31).

However, it is not easy to directly connect the above lemma to the information spectrum. Hence, we prepare the following lemma for the evaluation of the RHS of (31). This lemma plays an important role in the converse part of the main theorem.

Lemma 6: When a projection T and an integer M satisfy $\operatorname{Tr} T \geq M$, and the two reduced densities ρ' and ρ satisfy $\rho' \succeq \rho$, the inequality

$$\operatorname{Tr} \sqrt{\rho' T} \leq \sqrt{\operatorname{Tr} \left\{ \rho \geq \frac{1}{M} \right\}} \sqrt{\operatorname{Tr} \rho \left\{ \rho \geq \frac{1}{M} \right\}} + \sqrt{\operatorname{Tr} T - \operatorname{Tr} \left\{ \rho \geq \frac{1}{M} \right\}} \sqrt{\operatorname{Tr} \rho \left\{ \rho < \frac{1}{M} \right\}}$$
(33)

holds.

Proof: Assume that $\operatorname{Tr} T = N(\geq M)$. Without loss of generality, we can assume that $\rho' \succeq \rho$. Let us diagonalize ρ and ρ' as $\rho = \sum_i s_i |e_i\rangle \langle e_i|$ and $\rho' = \sum_i s'_i |f_i\rangle \langle f_i|$, where $s_i \geq s_{i+1}, s'_i \geq s'_{i+1}$. The inequality $\operatorname{Tr} \sqrt{\rho'T} \leq \sum_{i=1}^N \sqrt{s'_i}$ holds. We define the probability distribution $\{s_{i,N}\}$ and i_N as

$$\{s_{i,N}\} := \arg \max_{\{s'_i\}} \left\{ \sum_{i=1}^N \sqrt{s'_i} \middle| \{s'_i\} \succeq \{s_i\} \right\}, \\ s_{i_N} \ge \frac{1}{N} > s_{i_N+1}.$$

Similarly to i_N , we can define i_M . Since the function $x \mapsto \sqrt{x}$ is concave, we can prove that $s_i = s_{i,N}$ for $i \leq i_N$. Since $i_M \leq i_N$,

$$\sum_{i=1}^{i_M} \sqrt{s_{i,N}} = \sum_{i=1}^{i_M} \sqrt{s_i}$$

$$\leq \sqrt{i_M} \sqrt{\sum_{i=1}^{i_N} s_i} = \sqrt{\operatorname{Tr}\left\{\rho \ge \frac{1}{M}\right\}} \sqrt{\operatorname{Tr}\rho\left\{\rho \ge \frac{1}{M}\right\}}$$

$$\sum_{i=i_M+1}^{N} \sqrt{s_{i,N}} \le \sqrt{N - i_M} \sqrt{\sum_{i=i_M+1}^{N} s_{i,N}}$$

$$= \sqrt{N - i_M} \sqrt{1 - \sum_{i=1}^{i_M} s_i}$$

$$= \sqrt{\operatorname{Tr}T - \operatorname{Tr}\left\{\rho \ge \frac{1}{M}\right\}} \sqrt{\operatorname{Tr}\rho\left\{\rho < \frac{1}{M}\right\}}.$$

8

Thus, we obtain (33).

In order to treat PFLEC, we have to consider a measuring operation with LOCC. Lo and Popescu characterize a projection valued measure $\{P_{\omega}\}$ (Every P_{ω} is a projection, and $\sum_{\omega} P_{\omega}$ is the identity.) on the system *B* as follows.

Lemma 7: Lo and Popescu[17] For any projection valued measure $\{P_{\omega,B}\}$ on the system B, there exist a projection valued measure $\{P_{\omega,A}\}$ on the system A and local unitaries $U_{\omega,A}$ and $U_{\omega,B}$ such that

 $(I \otimes P_{\omega,B}) |\Phi\rangle = (U_{\omega,A} \otimes U_{\omega,B}) (P_{\omega,A} \otimes I) |\Phi\rangle.$ (34) That is, if the initial pure state is known, the operation corresponding to any projection valued measurement on *B* can be replaced by a projection valued measurement on *A* and local unitaries on *A* and *B* based on measuring data. However, we have to treat a general measuring operation with LOCC. The above Lo and Popescu's result can be generalized as follows.

Lemma 8: Given a measuring operation $I = \{I_{\omega}\}$ with LOCC on a tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$ and a pure state $|\Phi\rangle\langle\Phi|$ on the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$, there exist a POVM $\{M_{\omega}\}$ (Every M_{ω} is a positive operator, and $\sum_{\omega} M_{\omega}$ is the identity.) and the quantum operation C_{ω} with LOCC, such that

$$I_{\omega}(\Phi) = C_{\omega}(\sqrt{M_{\omega}} \otimes I | \Phi \rangle \langle \Phi | \sqrt{M_{\omega}} \otimes I), \quad \forall \omega.$$
 (35)

Proof: It is known that any measuring operation $I_B = \{I_{\omega,B}\}$ on the system B can be described by the projection valued measure $\{P_{\omega,B}\}$ on an extended space $\mathcal{H}'_B \supset \mathcal{H}_B$ and quantum operations $C_{\omega,B}$ on B such that

$$I_{\omega,B}(\rho) = C_{\omega,B}(P_{\omega,B}\rho P_{\omega,B}).$$

Applying (34), we have

$$(I_{\omega,B} \otimes I)(\Phi) = (I \otimes C_{\omega,B}) \Big((U_{\omega,A} \otimes U_{\omega,B}) (P_{\omega,A} \otimes I) |\Phi\rangle \langle \Phi| \\ (P_{\omega,A} \otimes I) (U_{\omega,A} \otimes U_{\omega,B})^* \Big).$$

Hence, any operation on *B* can be described by the combination of the projection measurement $\{P_{\omega,A}\}_{\omega}$ on *A* and local operations based only on the measuring data of $\{P_{\omega,A}\}_{\omega}$.

Now, we focus on a measurement operation $I' = \{I'_{\omega}\}_{\omega}$ on a tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$ consisting of LOCC and a pure state $|\Phi\rangle\langle\Phi|$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ satisfying the condition (A): the set $\Omega = \{\omega\}$ consists of all sent classical informations.

Then, there exist the projection valued measure $\{P_{\omega,B}\}_{\omega}$ on an extended space $\mathcal{H}'_B \supset \mathcal{H}_B$ and quantum operations $C_{\omega,A}$ and $C_{\omega,B}$ such that

$$I'_{\omega}(\Phi) = (C_{\omega,A} \otimes C_{\omega,B}) \Big((P_{\omega,A} \otimes I) |\Phi\rangle \langle \Phi| (P_{\omega,A} \otimes I) \Big).$$

Even if the measurement operation $I = \{I_k\}_k$ with LOCC does not satisfies the condition (A), there exist a measurement LOCC operation $I' = \{I'_{\omega}\}_{\omega \in \Omega}$ with subset $\Omega_k \subset \Omega$ satisfying the condition (A) such that

$$I_k = \sum_{\omega \in \Omega_k} I'_{\omega}.$$
 (36)



Fig. 1. Illustration of h(x)

Hence, we have

$$I_k(\Phi) = \sum_{\omega \in \Omega_k} (C_{\omega,A} \otimes C_{\omega,B}) \Big((P_{\omega,A} \otimes I) |\Phi\rangle \langle \Phi | (P_{\omega,A} \otimes I) \Big).$$

That is, there exist a projection valued measure $\{P_{k,A}\}$ on an extended space $\mathcal{H}'_A \supset \mathcal{H}_A$ and LOCC operations C_k such that

$$I_k(\Phi) = C_k((\tilde{P}_{k,A} \otimes I) | \Phi \rangle \langle \Phi | (\tilde{P}_{k,A} \otimes I)).$$

Since the projection $P_{\mathcal{H}_A}$ to \mathcal{H}_A satisfies that $P_{\mathcal{H}_A}\tilde{P}_{k,A}P_{\mathcal{H}_A} = (\tilde{P}_{k,A}P_{\mathcal{H}_A})^*\tilde{P}_{k,A}P_{\mathcal{H}_A}$, there exists a unitary $\tilde{U}_{k,A}$ such that

$$\tilde{P}_{k,A}P_{\mathcal{H}_A} = \sqrt{M_k^A} := \tilde{U}_{k,A}P_{\mathcal{H}_A}\tilde{P}_{k,A}P_{\mathcal{H}_A}.$$

Hence, we obtain

$$I_{k}(\Phi) = C_{k} \left((\tilde{U}_{k,A} \otimes I) (\sqrt{M_{k}^{A}} \otimes I) | \Phi \rangle \langle \Phi | (\sqrt{M_{k}^{A}} \otimes I) (\tilde{U}_{k,A} \otimes I)^{*} \right)$$

Therefore, the proof is completed.

In order to use the information spectrum method, one may characterize the optimal failure probability based on Tr $\rho \{\rho - x \ge 0\}$ for the reduced density ρ of the initial state. However, it is difficult. Hence, we focus on $h(x) := \text{Tr}(\rho - x) \{\rho - x \ge 0\}$ instead of Tr $\rho \{\rho - x \ge 0\}$. Suppose that we wish to reduce all eigenvalues of the reduced density ρ to be no greater than x. This incurs a probability of failure given by h(x). Upon success we obtain a normalized state whose largest eigenvalue is not greater than x/(1 - h(x)), which is majorized by a maximally entangled state of the dimension $\lfloor (1 - h(x))/x \rfloor$. It turns out that this method is optimal among PFLECs as follows.

Lemma 9: The bound on the performance of PFLEC based on Φ is evaluated by using the function h(x), as follows:

$$\max_{I = \{I_0, I_1\}: \text{ PFLEC of } \Phi} \{L(I) | \operatorname{Tr} I_0(\Phi) \le h(x)\}$$
$$= \left\lfloor \frac{1}{x} (1 - h(x)) \right\rfloor, \tag{37}$$

where |x| denotes the maximum integer n satisfying $n \le x$.

Proof: From Lemma 8, for any PFLEC *I*, there exist two quantum operations C_0 and C_1 with LOCC and a positive operator *P* such that $0 \le P \le I$ and

$$\operatorname{Tr} I_0(\Phi) = \operatorname{Tr}(I - P)\rho$$

$$\operatorname{Tr} I_1(\Phi) = \operatorname{Tr} P\rho$$

$$I_1(\Phi) = C_1((\sqrt{I - P} \otimes I)|\Phi\rangle \langle \Phi|(\sqrt{I - P} \otimes I))$$

$$I_0(\Phi) = C_0((\sqrt{P} \otimes I)|\Phi\rangle \langle \Phi|(\sqrt{P} \otimes I)).$$

Hence, we obtain the following equations for the following reasons.

$$\min_{\substack{I = \{I_0, I_1\}: \text{PFLEC of } \Phi \\ I = \min_{\substack{I \ge P \ge 0 \text{ on } \mathcal{H}}} \{ \operatorname{Tr} \rho(I - P) | x - \sqrt{P} \rho \sqrt{P} \ge 0 \}} \left\{ 138 \right\}$$

$$= \min_{I \ge P \ge 0 \text{ on } \mathcal{H}} \{ \operatorname{Tr}(\rho - \sqrt{\rho} P \sqrt{\rho}) | x - \sqrt{\rho} P \sqrt{\rho} \ge 0 \}$$
(39)

$$= \min_{\sigma \text{ on } \mathcal{H}} \{ 1 - \operatorname{Tr} \sigma | x - \sigma \ge 0, \rho \ge \sigma \}$$
(40)

$$= \min_{\sigma \text{ on } \mathcal{H}} \left\{ 1 - \sum_{i} \langle e_i | \sigma | e_i \rangle \left| \langle e_i | \sigma | e_i \rangle \le s_i, x \right\}$$
(41)

$$= 1 - \sum_{i:s_i \le x} s_i - \sum_{i:s_i > x} x = \operatorname{Tr}(\rho - x) \{\rho - x \ge 0\} = h(x)$$
(42)

where we diagonalize ρ as $\rho = \sum_{i} s_i |e_i\rangle \langle e_i|$ in (41). From Lemma 4, there exists a quantum operation C_1 with LOCC that transforms the state $\frac{1}{\operatorname{Tr} P\rho}(P \otimes I) |\Phi\rangle \langle \Phi|(P \otimes I)$ to a maximally entangled state with the size L if and only if $\frac{\operatorname{Tr} I_1(\Phi)}{L} \geq P\rho P$. Thus, from Lemma 8, we obtain (38). In general, for any bounded operator A, there exists a unitary operator U such that $AA^* = UA^*AU^*$. Thus, the condition $x - P\rho P \geq 0$ is equivalent with the condition $x - \sqrt{\rho}P\sqrt{\rho} \geq 0$. We obtain (39). Replacing $\sqrt{\rho}P\sqrt{\rho}$ by σ , we obtain (40).

Equation (42) implies

$$\max_{I=\{I_0,I_1\}: \text{ PFLEC of } \Phi} \left\{ L(I) | \operatorname{Tr} I_0(\Phi) \le h(x) \right\}$$
$$= \max_{x'} \left\{ \frac{1}{x'} (1 - h(x')) \middle| \begin{array}{c} \frac{1}{x'} (1 - h(x')) \text{ is an integer,} \\ h(x') \le h(x) \end{array} \right\}$$
$$= \left\lfloor \frac{1}{x} (1 - h(x)) \right\rfloor,$$

where the second equation follows from the fact that the function h(x) strictly monotonically decreases and is continuous.

VI. ASYMPTOTIC THEORY

In this section, based on non-asymptotic formulas given in section V, we prove our main theorem. For this purpose, we need to prepare the finite-version of the information-spectrum quantities for a projection operator T_n and a reduced density

 σ_n on $\mathcal{H}_{A,n}$ as follows.

$$\begin{split} \zeta_n(T_n|\sigma_n) &:= -\frac{1}{n}\log\operatorname{Tr}\sigma_n T_n,\\ \zeta_{n,1/2}(T_n|\sigma_n) &:= -\frac{1}{n}\log\operatorname{Tr}\sqrt{\sigma_n}T_n,\\ \eta_n(T_n) &:= -\frac{1}{n}\log\operatorname{Tr}(I - T_n),\\ \zeta_n^c(T_n|\sigma_n) &:= -\frac{1}{n}\log\operatorname{Tr}\sigma_n(I - T_n),\\ \zeta_{n,1/2}^c(T_n|\sigma_n) &:= -\frac{1}{n}\log\operatorname{Tr}\sqrt{\sigma_n}(I - T_n). \end{split}$$

As the limiting version, we define

$$\begin{split} \overline{\zeta}(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\zeta_n(T_n|\sigma_n),\\ \underline{\zeta}(\vec{T}|\vec{\sigma}) &:= \underline{\lim}\,\zeta_n(T_n|\sigma_n),\\ \overline{\zeta}_{1/2}(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\zeta_n(T_n|\sigma_n),\\ \underline{\zeta}_{1/2}(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\zeta_n(T_n|\sigma_n),\\ \underline{\gamma}(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\gamma_n(T_n|\sigma_n),\\ \underline{\eta}(\vec{T}|\vec{\sigma}) &:= \underline{\lim}\,\eta_n(T_n|\sigma_n),\\ \underline{\zeta}_c^c(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\zeta_n^c(T_n|\sigma_n),\\ \underline{\zeta}_{1/2}^c(\vec{T}|\vec{\sigma}) &:= \underline{\lim}\,\zeta_n^c(T_n|\sigma_n),\\ \underline{\zeta}_{1/2}^c(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\zeta_n^c(T_n|\sigma_n),\\ \underline{\zeta}_{1/2}^c(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\zeta_{n,1/2}^c(T_n|\sigma_n),\\ \underline{\zeta}_{1/2}^c(\vec{T}|\vec{\sigma}) &:= \overline{\lim}\,\zeta_{n,1/2}^c(T_n|\sigma_n), \end{split}$$

for sequences $\vec{\sigma} = \{\sigma_n\}$ and $\vec{T} = \{T_n\}$. For the projection $S_n(a) := \{\rho_n < e^{-na}\}$, we simplify $\zeta_n(S_n(a)|\sigma_n), \zeta_{n,1/2}(S_n(a)|\sigma_n), \eta_n(S_n(a)), \zeta_n^c(S_n(a)|\sigma_n),$ and $\zeta_{n,1/2}^c(S_n(a)|\sigma_n)$ to $\zeta_n(a|\sigma_n), \zeta_{n,1/2}(a|\sigma_n),$ $\eta_n(a), \zeta_n^c(a|\sigma_n),$ and $\zeta_{n,1/2}^c(a|\sigma_n)$. We can similarly define $\overline{\zeta}(a|\vec{\sigma}), \underline{\zeta}(a|\vec{\sigma}), \overline{\zeta}_{1/2}(a|\vec{\sigma}), \underline{\zeta}_{1/2}(a|\vec{\sigma}), \overline{\eta}(a|\vec{\sigma}), \underline{\eta}(a|\vec{\sigma}),$ $\overline{\zeta}^c(a|\vec{\sigma}), \underline{\zeta}^c(a|\vec{\sigma}), \overline{\zeta}_{1/2}^c(a|\vec{\sigma}),$ and $\underline{\zeta}_{1/2}^c(a|\vec{\sigma})$. Using these values, we can characterize the RHSs of (31), (33) and (37). In particular, when a sequence $\vec{\sigma}$ equals the sequence $\vec{\rho} = \{\rho_n\}$ of the reduced density of the given state, we omit $\vec{\rho}$ in the above values.

Moreover, to discuss the asymptotic theory, we need to define the concept "majorization" in regard to sequences of reduced densities. The sequence of reduced densities $\vec{\sigma} = \{\sigma_n\}$ majorizes (strongly majorizes) another one $\vec{\sigma'} = \{\sigma'_n\}$, written $\vec{\sigma} \succeq \vec{\sigma'}$ ($\vec{\sigma} \succ \vec{\sigma'}$) if $\sigma_n \succeq \sigma'_n$ ($\sigma_n \succ \sigma'_n$), respectively. In the following, we proceed to the proof of our main

theorem. Before it, we should remark that in an asymptotic case, we can neglect the gap between $\lfloor L_n \rfloor$ and L_n because L_n is large enough.

Lemma 10: Without any assumption, the equations

$$B_1(\epsilon) = B_2(\epsilon) = \sup_R \{R | K(R) \le \epsilon\}.$$

hold for every $\epsilon \in [0, 1]$.

Proof: From the definition, the inequality $B_1(\epsilon) \ge B_2(\epsilon)$ is trivial. We only need to prove the two inequalities

$$B_2(\epsilon) \ge \sup_R \{R | K(R) \le \epsilon\}$$
(43)

$$B_1(\epsilon) \le \sup_R \{R | K(R) \le \epsilon\}.$$
(44)

Let R be a real number satisfying

$$K(R) \le \epsilon. \tag{45}$$

From Lemma 9, there exists a PFLEC I^n such that $\operatorname{Tr} I_0^n(\Phi_n) = h_n(e^{-nR})$ and $L_n = e^{nR}(1-h_n(e^{-nR}))$, where $h_n(x) := \operatorname{Tr}(\rho_n - x)\{\rho_n - x \ge 0\}$. From (45), we have

$$\lim \frac{1}{n} \log L_n = R,$$

$$\overline{\lim} \operatorname{Tr} I_0^n(\Phi_n) \leq \overline{\lim} \operatorname{Tr} \rho_n \{ \rho_n - e^{-nR} \geq 0 \}$$
$$= K(R) \leq \epsilon.$$

We have now obtained the direct part (43).

Next, we proceed to the converse part (44). Let I^n be a DFLEC satisfying $\underline{\lim} \langle \Psi_n | C^n(\Phi_n) | \Psi_n \rangle \ge 1 - \epsilon$. For any $R < \underline{\lim} \frac{1}{n} \log L_n$, we have

$$\lim \frac{e^{nR}}{L_n} = 0.$$

From Lemma 6, for any T_n satisfying $\operatorname{Tr} T_n = L_n$, we have

$$\frac{(\operatorname{Tr}\sqrt{\rho_n'T_n})^2}{L_n} \leq \frac{1}{L_n} \left(\sqrt{\operatorname{Tr}\{\rho_n \ge e^{-nR}\}}\sqrt{\operatorname{Tr}\rho_n\{\rho_n \ge e^{-nR}\}} + \sqrt{L_n - \operatorname{Tr}\{\rho_n \ge e^{-nR}\}}\sqrt{\operatorname{Tr}\rho_n\{\rho_n < e^{-nR}\}}\right)^2 = \left(\sqrt{\frac{\operatorname{Tr}\{\rho_n \ge e^{-nR}\}}{L_n}}\sqrt{\operatorname{Tr}\rho_n\{\rho_n \ge e^{-nR}\}} + \sqrt{1 - \frac{\operatorname{Tr}\{\rho_n \ge e^{-nR}\}}{L_n}}\sqrt{\operatorname{Tr}\rho_n\{\rho_n < e^{-nR}\}}\right)^2.$$

Since $\lim \frac{\operatorname{Tr}\{\rho_n \ge e^{-nR}\}}{L_n} \le \lim \frac{e^{nR}}{L_n} = 0$,

$$1 - \epsilon \leq \underline{\lim} \frac{(\operatorname{Tr} \sqrt{\rho_n} T_n)^2}{L_n} \leq \underline{\lim} \operatorname{Tr} \rho_n \{ \rho_n < e^{-nR} \}$$
$$= 1 - K(R).$$

Thus, we obtain (44).

Lemma 11: We have

$$B_{e,D}(r) = B_{e,P}(r) = \sup_{\Sigma} \{ R | \underline{\zeta}^c(R) \ge r \}.$$

Proof: Since $B_{e,D}(r) \ge B_{e,P}^{R}(r)$, we only need to prove the inequalities

$$B_{e,D}(r) \le \sup_{R} \{ R | \underline{\zeta}^c(R) \ge r \}$$
(46)

$$B_{e,P}(r) \ge \sup_{R} \{ R | \underline{\zeta}^{c}(R) \ge r \}.$$
(47)

First, we prove the direct part (47). Assume that $\underline{\zeta}^{c}(R) \geq r > 0$. From Lemma 9, for any R, there exists a PFLEC I^{n} with the size $e^{nR}(1 - (1 - t_{n}(R))e^{-n\zeta_{n}^{c}(R)}))$ such that

Tr
$$I_0^n(\Phi_n) = (1 - t_n(R))e^{-n\zeta_n^c(R)},$$

where

$$t_n(R) := \frac{e^{-nR} \operatorname{Tr}\{\rho_n \ge e^{-nR}\}}{\operatorname{Tr}\rho_n\{\rho_n \ge e^{-nR}\}}.$$

Since $\zeta^c(R) > 0$, we have $0 \leq (1 - t_n(R))e^{-n\zeta_n^c(R)} \leq e^{-n\zeta_n^c(R)} \to 0$. Thus, we have the following relations

$$\lim \frac{1}{n} \log e^{nR} (1 - (1 - t_n(R))e^{-n\zeta_n^c(R)})) = R$$
$$\underline{\lim} \frac{-1}{n} \log \operatorname{Tr} I_0^n(\Phi_n) \ge \underline{\zeta}^c(R) \ge r,$$

which imply the inequality (47).

Next, we proceed to the converse part (46). Assume that the DFLEC (C^n, Ψ_n) satisfies

$$\underline{\lim} \frac{1}{n} \log \left(1 - \langle \Psi_n | C^n(\Phi_n) | \Psi_n \rangle \right) \ge r.$$
(48)

We define the projection T_n and the reduced density ρ'_n as

$$T_n := L_n \operatorname{Tr}_{\mathcal{H}_B} |\Psi_n\rangle \langle \Psi_n|, \quad \rho'_n := \operatorname{argmax}_{\rho' \succeq \rho_n} \frac{\left(\operatorname{Tr} \sqrt{\rho'} T_n\right)^2}{L_n}$$

Then, Lemma 5 and (48) yields that

$$\underline{\lim} \frac{1}{n} \log \left(1 - \frac{(\operatorname{Tr} \sqrt{\rho'_n} T_n)^2}{L_n} \right) \ge r.$$

For any $R' < R_0 := \underline{\lim} \frac{1}{n} \log L_n$, there exists an integer N such that $R_n := \frac{1}{n} \log L_n > R'$ for $\forall n \ge N$. When a projection T_n satisfies that $\operatorname{Tr} T_n = L_n$, Lemma 6 implies that

$$\frac{(\operatorname{Tr}\sqrt{\rho_{n}'T_{n}})^{2}}{L_{n}} \leq \frac{1}{L_{n}} \left(\sqrt{\operatorname{Tr}\{\rho_{n} \ge e^{nR'}\}} \sqrt{\operatorname{Tr}\rho_{n}\{\rho_{n} \ge e^{nR'}\}} + \sqrt{L_{n} - \operatorname{Tr}\{\rho_{n} \ge e^{nR'}\}} \sqrt{\operatorname{Tr}\rho_{n}\{\rho_{n} < e^{nR'}\}} \right)^{2} \leq \left(e^{-\frac{n}{2}(\eta_{n}(R') + \zeta_{n}^{c}(R') + R_{n})} + \sqrt{1 - e^{-n(\eta_{n}(R') + R_{n})}} \sqrt{1 - e^{-n\zeta_{n}^{c}(R')}} \right)^{2} \\ \cong \left(1 - \frac{1}{2} \left(e^{-n(\eta_{n}(R') + R_{n})} + e^{-n\zeta_{n}^{c}(R')} \right) + e^{-\frac{n}{2}(\eta_{n}(R') + \zeta_{n}^{c}(R') + R_{n})} \right)^{2} \\ = \left(1 - \frac{1}{2} \left(e^{-\frac{n}{2}\zeta_{n}^{c}(R')} - e^{-\frac{n}{2}(\eta_{n}(R') + R_{n})} \right)^{2} \right)^{2}. \quad (49)$$

Since $e^{-\frac{n}{2}(\eta_n(R')+R_n)} \leq e^{-\frac{n}{2}(R_n-R')}e^{-\frac{n}{2}(\eta_n(R')+R')} \leq e^{-\frac{n}{2}\zeta_n^c(R')} \leq e^{-\frac{n}{2}\zeta_n^c(R')}$, we have

$$\left(e^{-\frac{n}{2}\zeta_n^c(R')} - e^{-\frac{n}{2}(\eta_n(R') + R_n)} \right)^{\frac{1}{2}} \ge (1 - e^{-\frac{n}{2}(R_n - R')})^2 e^{-n\zeta_n^c(R')}.$$

Thus,

$$\left(1 - \frac{1}{2} \left(e^{-\frac{n}{2}(\eta_n(R') + R_n)} - e^{-\frac{n}{2}\zeta_n^c(R')}\right)^2\right)^2 \le \left(1 - \frac{1}{2}(1 - e^{-\frac{n}{2}(R_n - R')})^2 e^{-n\zeta_n^c(R')}\right)^2.$$
(50)

Since $\lim_{n \to \infty} (1 - e^{-\frac{n}{2}(R_n - R')})^2 = 1$, it follows from (49) and (50) that

$$\underline{\zeta}^{c}(R') \geq \underline{\lim} \, \frac{1}{n} \log \left(1 - \frac{(\operatorname{Tr} \sqrt{\rho'_{n}} T_{n})^{2}}{L_{n}} \right) \geq r.$$

Since R' is an arbitrary real number satisfying $R' < R_0$, the relation $R_0 \le \sup_R \{R \mid \underline{\zeta}^c(R) \ge r\}$ holds. Therefore, we obtain (46).

Lemma 12: When $\overline{\zeta}(a) = \underline{\zeta}(a) =: \zeta(a)$ and there exists a real number a such that $\zeta(a) \leq \underline{\zeta}^c(a)$,

$$B_{e,P}^*(r)$$

$$= \sup_{a} \{a - \min\{\zeta(a), a + \overline{\eta}(a)\} | \min\{\zeta(a), a + \overline{\eta}(a)\} \le r\}$$

$$= \inf_{a} \{a - \min\{\zeta(a), a + \overline{\eta}(a)\} | \min\{\zeta(a), a + \overline{\eta}(a)\} > r\}$$

$$= \inf_{a} \{a - \zeta(a) | \zeta(a) \le r\}.$$

Proof: First, we prove the direct part. Consider a PFLEC I^n satisfying

$$L_n = \frac{1 - h_n(e^{-na})}{e^{-na}}$$

Tr $I_0^n(\Phi_n) = h_n(e^{-na}).$

Thus, we have

$$\underline{\lim} \frac{1}{n} \log L_n = a - \min\{\zeta(a), a + \overline{\eta}(a)\}$$
$$\overline{\lim} \frac{-1}{n} \log (\operatorname{Tr} I_1^n(\Phi_n)) = \min\{\zeta(a), a + \overline{\eta}(a)\}.$$

Therefore, we have

$$B_{e,P}^{*}(r)$$

$$\geq \sup_{a} \{a - \min\{\zeta(a), a + \overline{\eta}(a)\} | \min\{\zeta(a), a + \overline{\eta}(a)\} \leq r\}$$

$$= \max \left\{ \sup_{a} \{a - \zeta(a) | \zeta(a) \leq r\}, \sup_{a} \{-\overline{\eta}(a) | a + \overline{\eta}(a) \leq r\} \right\}$$

$$= \sup_{a} \{a - \zeta(a) | \zeta(a) \leq r\},$$

where the final equation is derived by Lemma 15 as follows. Using Lemma 15, we have $\sup_a \{a - \zeta(a) | \zeta(a) \le r\} \ge \sup_a \{-\underline{\eta}(a) | a + \underline{\eta}(a) \le r\} \ge \sup_a \{-\overline{\eta}(a) | a + \overline{\eta}(a) \le r\}.$

Next, we proceed to the converse part. Let $\{I^n\}$ be a sequence of PFLECs such that $r \ge \overline{\lim \frac{-1}{n} \log(1-\epsilon_n)}$, where $\epsilon_n := \operatorname{Tr} I_0^n(\Phi_n)$. In the following, we focus on $\underline{\lim \frac{1}{n} \log L_n}$. Let a be a real number satisfying

$$\overline{\lim} \, \frac{-1}{n} \log(1 - \epsilon_n) \le r \le \min\{\zeta(a), a + \overline{\eta}(a)\}.$$
(51)

Since

$$\overline{\lim} \frac{-1}{n} \log \left(\operatorname{Tr} \rho_n \{ \rho_n \le e^{-na} \} + e^{-na} \operatorname{Tr} \{ \rho_n > e^{-na} \} \right)$$
$$= \min\{ \zeta(a), a + \overline{\eta}(a) \},$$

there exists an integer N such that

$$\operatorname{Tr} \rho_n \{ \rho_n \le e^{-na} \} + e^{-na} \operatorname{Tr} \{ \rho_n > e^{-na} \}$$
$$> 1 - h_n (e^{-na}), \quad \forall n > N.$$

Lemma 9 guarantees that

$$e^{na} \left(\operatorname{Tr} \rho_n \{ \rho_n \le e^{-na} \} + e^{-na} \operatorname{Tr} \{ \rho_n > e^{-na} \} \right)$$

= $\frac{1 - h_n(e^{-na})}{e^{-na}} \ge L_n.$ (52)

Taking the limit of the exponent, we have

$$\underline{\lim} \frac{1}{n} \log L_n \le a - \min\{\zeta(a), a + \overline{\eta}(a)\}.$$

From (51), we have

$$B^*_{e,P}(r) \leq \inf_{a} \{a - \min\{\zeta(a), a + \overline{\eta}(a)\} | \min\{\zeta(a), a + \overline{\eta}(a)\} \geq r\}.$$

It follows from (70) that the function $a \mapsto \min{\{\zeta(a), a + \overline{\eta}(a)\}}$ is continuous. Thus,

$$\inf_{a} \{a - \min\{\zeta(a), a + \overline{\eta}(a)\} | \min\{\zeta(a), a + \overline{\eta}(a)\} \ge r\}$$
$$= \sup_{a} \{a - \min\{\zeta(a), a + \overline{\eta}(a)\} | \min\{\zeta(a), a + \overline{\eta}(a)\} \le r\}.$$

The proof is now completed.

Lemma 13: When $\overline{\zeta}(a) = \underline{\zeta}(a) =: \zeta(a)$ and there exists a real number a such that $\zeta(a) \leq \zeta^c(a)$,

$$B^*_{e,D}(r) = \sup_{\vec{\rho'} \succeq \vec{\rho}} \sup_{\vec{T}} \{-\underline{\lim} \eta_n(T_n) | \overline{\lim} 2\zeta^c_{n,1/2}(T_n | \rho'_n) - \eta(T_n) \le r\}$$
(53)

$$= \sup_{\vec{\mathcal{T}}} \{-\underline{\lim} \eta_n(T_n) | \overline{\lim} 2\zeta_{n,1/2}^c(T_n) - \eta(T_n) \le r\}$$
(54)

$$= \sup_{a} \left\{ a - r \left| \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \right| a' \le a \right\} + \frac{a}{2} \le r \right\}$$
(55)
$$= \sup_{a} \left\{ \frac{a}{2} - \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \right| a' \le a \right\} \right|$$
$$\inf_{a'} \left\{ \left| \zeta(a') - \frac{a'}{2} \right| a' \le a \right\} + \frac{a}{2} \le r \right\}.$$
(56)

Proof: Equation (53) follows from (31). Since the function $a \mapsto \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \leq a \right\}$ is continuous and decreases monotonically and the function $a \mapsto \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \leq a \right\} + \frac{a}{2}$ is continuous and increases monotonically, equation (56) holds. First, we prove the direct part:

$$\sup_{\vec{T}} \left\{ -\underline{\lim} \eta_n(T_n) \middle| \lim 2\zeta_{n,1/2}^c(T_n) - \eta(T_n) \le r \right\}$$

$$\geq \sup_{a} \left\{ \frac{a}{2} - \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \le a \right\} \middle|$$

$$\inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \le a \right\} + \frac{a}{2} \le r \right\}. \quad (57)$$

As we prove later, we can choose a projection $T_n(a, R)$ such that

$$\eta_n(T_n(a,R)) = -R,\tag{58}$$

$$\zeta_{n,1/2}^c(T_n(a,R)) \le \max\left\{\zeta_{n,1/2}^c(a), -R + \frac{a}{2}\right\}.$$
 (59)

When $\eta_n(a) \ge -R$, the projection $T_n(a, R) := \{\rho_n - e^{-na} \ge 0\}$ satisfies (59). Otherwise, the projection $T_n(a, R) := \{\rho_n - e^{-na} \ge 0\} + (\{\rho_n - e^{-na} < 0\} - \tilde{T}_n(a, R))$ satisfies (59), where $\tilde{T}_n(a, R)$ is constructed as follows: We choose $m := e^{nR}$ normalized eigenvectors $\{e'_i\}_{i=1}^m$ of $\{\rho_n - e^{-na} < 0\}\rho_n$ in descending order concerning the eigenvalue, and define the projection $\tilde{T}_n(a, R)$ by $\sum_{i=1}^m |e'_i\rangle\langle e'_i|$. The choice of $\{e'_i\}_{i=1}^m$ and the relation $e^{nR} = \text{Tr}\{\rho_n - e^{-na} < 0\}e^{-n(-R-\eta_n(a))}$ guarantees

$$\operatorname{Tr}\sqrt{\rho_n}\{\rho_n - e^{-na} < 0\}e^{-n(-R-\eta_n(a))} \le \operatorname{Tr}\sqrt{\rho_n}\tilde{T}_n(a, R).$$
(60)

Then, we can check the condition (59) as follows:

$$\eta_n(T_n(a, R)) = \frac{-1}{n} \log \operatorname{Tr}(I - T_n(a, R))$$

= $\frac{-1}{n} \log \operatorname{Tr} \tilde{T}_n(a, R) = \frac{-1}{n} \log e^{nR} = -R,$
 $\zeta_{n,1/2}^c(T_n(a, R)) = \frac{-1}{n} \log \operatorname{Tr} \sqrt{\rho_n} \tilde{T}_n(a, R)$
 $\leq \frac{-1}{n} \log \operatorname{Tr} \sqrt{\rho_n} \{\rho_n - e^{-na} < 0\} e^{-n(-R - \eta_n(a))}$
= $\zeta_{n,1/2}^c(a) - R - \eta_n(a) \leq -R + \frac{a}{2}.$

Now, we apply Lemma 17 to the case $\rho_n = \rho_n, \sigma_n = \sqrt{\rho_n}$. Since

$$\{\rho_n - e^{na}\sigma_n > 0\} = \{\rho_n - e^{na}\sqrt{\rho_n} > 0\} = \{\sqrt{\rho_n} - e^{na} > 0\} = \{\rho_n - e^{2na} > 0\},\$$

we have

$$\underline{\eta}(a) = \underline{\zeta}_{1/2}^c(2a|\vec{\rho}), \quad \underline{\zeta}(a) = \underline{\zeta}(2a|\vec{\rho}). \tag{61}$$

From Lemma 17, the maximum a_r of

$$\left\{ a \left| \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \right| a' \le a \right\} + \frac{a}{2} = r \right\}$$

exists. We define R by

$$R := \frac{a_r}{2} - \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \le a_r \right\}.$$

Then, R equals to the right hand side of (57), and we have

$$\overline{\lim} 2\zeta_{n,1/2}^c(T_n(a_k, R)) - \eta(T_n(a_k, R))$$

$$\leq 2\max\left\{\overline{\zeta}_{1/2}(a_r + 1/k), -R + \frac{a_r + 1/k}{2}\right\}$$

$$\leq r + 1/k,$$

where $a_k := a_r + 1/k$ and k is a fixed integer, and the last inequality follows from (84) in Lemma 17 in Appendix A. We define N_k as the minimum integer satisfying

$$2\zeta_{n,1/2}^{c}(T_{n}(a_{k},R)) - \eta(T_{n}(a_{k},R)) \le r + \frac{2}{k}, \quad \forall n \ge N_{k}.$$

For the sequence $b_n := \min_k \{a_k | n \ge N_k\}$, we have

$$\overline{\lim} \, 2\zeta_{n,1/2}^c(T_n(b_n, R)) - \eta(T_n(b_n, R)) \le r.$$
 (62)

Inequality (57) follows from (62) and the first equation of (59).

Next, we prove the converse part. Assume that $\{(T_n, \rho'_n)\}$ satisfies $\overline{\lim}_{n\to\infty} 2\zeta_{n,1/2}^c(T_n|\rho'_n) - \eta(T_n) \leq r$. There exists a subsequence $\{n_k\}$ such that $\lim \eta_{n_k}(T_{n_k}) = -R_0 :=$ $\underline{\lim} \eta_n(T_n)$. Focusing on the projection $\{\rho'_n - e^{-na} \ge 0\} =$ $\sqrt{\frac{1}{\rho'_n} - e^{-na/2}} \ge 0$, we have

$$\operatorname{Tr} \sqrt{\rho'_n} \{ \rho'_n - e^{-na} \ge 0 \} - e^{na/2} \operatorname{Tr} \{ \rho'_n - e^{-na} \ge 0 \}$$

$$\ge \operatorname{Tr} \sqrt{\rho'_n} (I - T_n) - e^{na/2} \operatorname{Tr} (I - T_n),$$

which implies

$$\operatorname{Tr} \sqrt{\rho'_n} \{ \rho'_n - e^{-na} \ge 0 \} + e^{na/2} \operatorname{Tr} (I - T_n)$$
$$\ge \operatorname{Tr} \sqrt{\rho'_n} (I - T_n).$$

Taking the limit $k \to \infty$, we have

$$\min\left\{\overline{\lim_{k\to\infty}\zeta_{n_k,1/2}^c(a|\rho'_{n_k}),\frac{a}{2}-R_0}\right\} \le \overline{\lim_{k\to\infty}\zeta_{n_k,1/2}^c(T_{n_k}|\rho'_{n_k})}$$

Now, we apply Lemma 14 to the case $\rho_n = \rho'_n, \sigma = \sqrt{\rho'_n}$. In this case, similarly to (61), we have

$$\underline{\eta}(a) = \underline{\zeta}_{1/2}^c (2a|\vec{\rho'}), \quad \underline{\zeta}(a) = \underline{\zeta}(2a|\vec{\rho'}).$$

Hence, (74) yields that

$$\begin{split} & \overline{\lim_{k \to \infty}} \zeta_{n_k, 1/2}^c(a | \rho'_{n_k}) \geq \underline{\zeta}_{1/2}^c(a | \vec{\rho'}) \\ & \geq \inf_{a'} \left\{ \left. \underline{\zeta}(a' | \vec{\rho'}) - \frac{a'}{2} \right| a' \leq a \right\}. \end{split}$$

Since $\rho'_n \succeq \rho_n$, we have $\zeta(a' | \vec{\rho'}) \ge \zeta(a') = \zeta(a')$, *i.e.*,

$$\inf_{a'} \left\{ \left| \underline{\zeta}(a'|\vec{\rho'}) - \frac{a'}{2} \right| a' \le a \right\} \ge \inf_{a'} \left\{ \left| \zeta(a') - \frac{a'}{2} \right| a' \le a \right\}.$$
Thus

Thus.

$$r \geq \overline{\lim_{n \to \infty}} 2\zeta_{n,1/2}^{c}(T_{n}|\rho_{n}') - \eta(T_{n})$$

$$\geq \overline{\lim_{k \to \infty}} 2\zeta_{n_{k},1/2}^{c}(T_{n_{k}}|\rho_{n_{k}}') - \eta(T_{n_{k}})$$

$$\geq 2\min\left\{\overline{\lim_{k \to \infty}} \zeta_{n_{k},1/2}^{c}(a|\rho_{n_{k}}'), \frac{a}{2} - R_{0}\right\} + R_{0}$$

$$\geq 2\min\left\{\inf\left\{\zeta(a') - \frac{a'}{2} \middle| a' \leq a\right\}, \frac{a}{2} - R_{0}\right\} + R_{0}.$$
(63)

Since the function $a \mapsto \frac{a}{2} - \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \leq a \right\}$ is continuous, there exists a real number a such that

$$R_0 = \frac{a}{2} - \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \le a \right\}$$

Using (63), we have

Ì

$$\geq \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \leq a \right\} + \frac{a}{2},$$

which implies

$$R_0 \leq \sup_a \left\{ \frac{a}{2} - \inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \leq a \right\} \right|$$
$$\inf_{a'} \left\{ \zeta(a') - \frac{a'}{2} \middle| a' \leq a \right\} + \frac{a}{2} \leq r \right\}.$$

The proof is now completed.

VII. RELATION TO RANDOM NUMBER GENERATION

As a related problem, it is known to transform from a given known probability distribution p to a desired probability distribution q. If it is possible, the majorization relation $q \succeq p$ holds. However, even if the majorization relation $q \succeq p$ holds, this transformation is not necessarily available. Hence, if the two entangled pure states Φ_1 and Φ_2 have Schmidt coefficients corresponding to p and q, the Quantum LOCC operation transforming from Φ_1 to Φ_2 is easier than transform from p to q.

In particular, when the desired distribution is the uniform distribution, this problem is called intrinsic randomness. In this problem, our operation of intrinsic randomness is described by the map ψ from the original space Ω to $\mathcal{M} = \{1, \ldots, M\}$. When the initial distribution is p and the uniform distribution is described by p_M on \mathcal{M} , one of criteria of its quality is the half of the square of Hellinger distance between $p \circ \psi^{-1}$ and p_M :

$$\varepsilon(\psi, p) := 1 - \sum_{i=1}^{M} \sqrt{\frac{\sum_{\omega \in \psi^{-1}(i)} p_{\omega}}{M}}.$$
 (64)

In this case, we describe the size of its target uniform distribution ψ by $M(\psi)$. Hence, for a sequence of the initial distributions $\{p_n\}$, we can define the optimal rates

$$B_{H}(\epsilon) := \sup_{\{\psi_{n}\}} \left\{ \underbrace{\lim \frac{\log M(\psi_{n})}{n}}_{\{\psi_{n}\}} \left| \underbrace{\lim \varepsilon(\psi_{n}, p_{n}) \leq \epsilon}_{\{\psi_{n}\}} \right\} \right\}$$
$$B_{e,H}(r) := \sup_{\{\psi_{n}\}} \left\{ \underbrace{\lim \frac{\log M(\psi_{n})}{n}}_{\{\psi_{n}\}} \left| \underbrace{\lim \frac{\log M(\psi_{n})}{n}}_{n} \right| \right.$$
$$\left. \underbrace{\lim \frac{\log M(\psi_{n})}{n}}_{\{\psi_{n}\}} \right|_{\{\psi_{n}\}} \left\{ \underbrace{\lim \frac{\log M(\psi_{n})}{n}}_{\{\psi_{n}\}} \right|_{\{\psi_{n}\}} \left\{ \underbrace{\lim \frac{\log M(\psi_{n})}{n}}_{\{\psi_{n}\}} \right\}$$

The variational distance version with the constant constraint has been discussed by Vembu & Verdú [19] and Han [13].

Let Φ_n be the entangled pure state with the Schmidt coefficient corresponding to p_n . When C_n is the quantum LOCC operation corresponding to ψ_n and Ψ_n is the maximally entangled state with the size $M(\psi_n)$, we have

$$1 - \varepsilon(\psi_n, p_n) = \sqrt{\langle \Psi_n | C_n(\Phi_n) | \Psi_n \rangle}, \tag{65}$$

i.e.,

$$2\varepsilon(\psi_n, p_n) - \varepsilon(\psi_n, p_n)^2 = 1 - \langle \Psi_n | C_n(\Phi_n) | \Psi_n \rangle.$$
 (66)

Hence, comparing the entanglement concentration with the initial entangled state Φ_n and the intrinsic randomness with the initial distribution p_n , (66) yields that

$$B_H(\epsilon) \le B_D(2\epsilon - \epsilon^2).$$

Since

$$\varepsilon(\psi_n, p_n) \le 1 - \langle \Psi_n | C_n(\Phi_n) | \Psi_n \rangle \le 2\varepsilon(\psi_n, p_n),$$

the inequality

$$B_{e,H}(r) \le B_{e,D}(r)$$

holds. Moreover, the equation (65) yields that

$$B_{e,H}^{*}(r) \le B_{e,D}^{*}(2r).$$

When we adopt the KL divergence criterion:

$$D(p_M \| p \circ \psi^{-1}) := \log M + \sum_{i=1}^M \frac{1}{M} \log \left(\sum_{\omega \in \psi^{-1}(i)} p_\omega \right),$$

we focus on the following value:

As is shown Hayashi[22], the relation

$$B_{KL}(\epsilon) = \sup_{a} \{a - \zeta(a) | \zeta(a) < \epsilon\}$$

holds. When $\zeta(a)$ is continuous,

$$B_{KL}(\epsilon) = B_{e,P}^*(\epsilon). \tag{67}$$

In particular, if the limit of Rényi entropy is differentiable,

$$B_{KL}(\epsilon) \ge B_{e,H}^*(\epsilon/2) \tag{68}$$

when $\epsilon \leq -\frac{1}{2}\overline{\psi}'(\frac{1}{2}) - \overline{\psi}(\frac{1}{2})$. The above relation is an interesting relation between Hellinger criterion and KL divergence criterion.

VIII. CONCLUDING REMARKS

We derive asymptotic bounds based on several formulations from Lemma 5, 6, and 9. Since these bounds are tight in a general source, the evaluations given in Lemma 5, 6, and 9 are useful in a non asymptotic case as well as in an asymptotic case. Even if the class of DFLEC is wider than that of PFLEC, their asymptotic performances are almost equivalent. A difference appears only between $B_{e,D}^*(r)$ and $B^*_{e,P}(r)$. For example, when the limit of Rényi entropy $\psi(s)$ is differentiable, $B^*_{e,D}(r)$ is larger than $B^*_{e,P}(r)$ if and only if r is greater than $-\frac{1}{2}\overline{\psi}'(\frac{1}{2})-\overline{\psi}(\frac{1}{2})$. From (54) of Lemma 13, the bound $B_{e,D}^*(r)$ can be attained without an LOCC, *i.e.*, the original reduced density ρ_n is close enough to an appropriate MES only in regard to $B_{e,D}^*(r)$. As a byproduct, in Appendix A, we establish several general relations between informationspectrum quantities.

APPENDIX

A. General relations for information spectrums

Here, we prove some lemmas required by our proof. In this section, we treat information-spectrum quantities with more general definitions, which are given in Nagaoka and Hayashi[14]. This is because we need such a general treatment in our proof of Lemma 13.

For the two sequences $\{\rho_n\}$ and $\{\sigma_n\}$ of trace class positive semidefinite operators, we discuss how to characterize an information-spectrum quantity $\underline{\eta}(a) := \underline{\lim} \frac{-1}{n} \log \operatorname{Tr} \sigma_n \{ \rho_n$ $e^{-na}\sigma_n > 0$ by using two other information-spectrum quantities $\underline{\zeta}(a) := \underline{\lim} \frac{-1}{n} \log \operatorname{Tr} \rho_n \{\rho_n - e^{-na}\sigma_n \leq 0\}$ and $\underline{\zeta}^c(a) := \underline{\lim} \frac{-1}{n} \log \operatorname{Tr} \rho_n \{\rho_n - e^{-na}\sigma_n > 0\}.$ As discussed later, when $\overline{\zeta}(a) := \underline{\lim} \frac{-1}{n} \log \operatorname{Tr} \rho_n \{\rho_n - e^{-na}\sigma_n > 0\}.$ $e^{-na}\sigma_n \leq 0$ equals $\zeta(a)$ for any a, we can use the same method to characterize another information spectrum $\overline{\eta}(a) :=$ $\overline{\lim} \frac{-1}{n} \log \operatorname{Tr} \sigma_n \{ \rho_n - e^{-na} \sigma_n > 0 \}$. As was proven by Nagaoka and Hayashi[14], the function $\underline{\zeta}(a)$ increases monotonically, and other functions $\zeta^{c}(a)$ and $\eta(a)$ decrease monotonically [14]. Focusing on the projection $\{\rho_n - e^{-na}\sigma_n \ge 0\},\$ we have

$$\operatorname{Tr}(\rho_n - e^{-na}\sigma_n)\{\rho_n - e^{-na}\sigma_n \ge 0\} \ge 0,$$

which yields to

$$B_{KL}(\epsilon) := \sup_{\{\psi_n\}} \left\{ \underline{\lim} \frac{\log M(\psi_n)}{n} \Big| \overline{\lim} D(p_{M(\psi_n)} \| p \circ \psi_n^{-1}) \le \epsilon \right\} \operatorname{Tr} \rho_n \{\rho_n - e^{-na} \sigma_n \ge 0\} \ge e^{-na} \operatorname{Tr} \sigma_n \{\rho_n - e^{-na} \sigma_n \ge 0\}.$$

Thus, we have

$$\underline{\zeta}^c(a) \le \underline{\eta}(a) + a. \tag{69}$$

Similarly, we can prove

$$\operatorname{Tr}(\rho_n - e^{-na}\sigma_n) \{\rho_n - e^{-na}\sigma_n \ge 0\}$$
$$\ge \operatorname{Tr}(\rho_n - e^{-na}\sigma_n) \{\rho_n - e^{-nb}\sigma_n \ge 0\}.$$

By adding $e^{-na} \operatorname{Tr} \sigma_n$ to both sides, we have

$$\operatorname{Tr} \rho_n \{ \rho_n - e^{-na} \sigma_n \ge 0 \} + e^{-na} \operatorname{Tr} \sigma_n \{ \rho_n - e^{-na} \sigma_n < 0 \}$$
$$\geq \operatorname{Tr} \rho_n \{ \rho_n - e^{-nb} \sigma_n \ge 0 \} + e^{-na} \operatorname{Tr} \sigma_n \{ \rho_n - e^{-nb} \sigma_n < 0 \}$$

Taking the limit $n \to \infty$, we obtain

$$\min\{\underline{\zeta}(a), a + \underline{\eta}(a)\} \ge \min\{\underline{\zeta}(b), a + \underline{\eta}(b)\}$$
(70)

for any *a* and *b*[14]. When $\underline{\zeta}(a) = \overline{\zeta}(a)$ for any *a*, we can replace $\underline{\eta}$ by $\overline{\eta}$. From inequality (70), We can derive the following two formulas;

$$\underline{\eta}(a) + a \ge \underline{\zeta}(b) \text{ if } \underline{\eta}(b) > \underline{\eta}(a) \tag{71}$$

$$\underline{\zeta}(a) \ge a + \underline{\eta}(b) \text{ if } \underline{\zeta}(a) < \underline{\zeta}(b), \tag{72}$$

which play important roles in the following lemmas. As a lower bound of $\eta(a)$, the following lemma holds.

Lemma 14: If there exists a real number a_0 such that $\zeta(a_0) \leq \zeta^c(a_0)$, the relations

$$\underline{\eta}(a) \ge \inf_{a'} \{ \underline{\zeta}(a') - a' | a' < a \}$$
(73)

$$= \inf_{a'} \{ \underline{\zeta}(a') - a' | a' \le a \}$$
(74)

hold.

Proof: From (69), the relations

$$\zeta(a_0) \le \zeta^c(a_0) \le \eta(a_0) + a_0$$

hold. Since $\eta(a_0) \ge \zeta(a_0) - a_0$, we have

$$\underline{\eta}(a_0) \ge \inf_{a'} \{ \underline{\zeta}(a') - a' | a' \le a_0 \}$$

For any $a \le a_0$, the relation $\underline{\zeta}(a) \le \underline{\zeta}^c(a)$ holds. Since $\underline{\zeta}(a - 0) \le \underline{\zeta}(a)$, the equation (74) holds. Similarly, we can prove that a real number $a(\le a_0)$ satisfies (73).

Next, we prove (73) for any $a > a_0$ by the transfinite induction. Assume that the relation (73) holds for any real number *b* satisfying a > b and

$$\underline{\eta}(a) < \inf_{a'} \{ \underline{\zeta}(a') - a' | a' \le a \}.$$
(75)

For any $\epsilon > 0$, we have

$$\underline{\eta}(a) < \inf_{a'} \{ \underline{\zeta}(a') - a' | a' \le a - \epsilon \} \le \underline{\eta}(a - \epsilon).$$

From (71), we have $\underline{\eta}(a) \ge \underline{\zeta}(a-\epsilon) - a$. Since ϵ is arbitrary, we obtain the inequality

$$\underline{\eta}(a) \ge \inf_{a'} \{ \underline{\zeta}(a') - a' | a' < a \}$$

which contradicts assumption (75).

The following lemma is another characterization of the lower bounds of $\eta(a)$.

Lemma 15: We obtain the inequality

$$\sup_{a} \{a - \underline{\zeta}(a) | \underline{\zeta}(a) \le r\} \ge \sup_{a} \{-\underline{\eta}(a) | a + \underline{\eta}(a) \le r\},$$

which is equivalent to another inequality

$$\inf_{a} \{ \underline{\zeta}(a) - a | \underline{\zeta}(a) \le r \} \le \inf_{a} \{ \underline{\eta}(a) | a + \underline{\eta}(a) \le r \}.$$

Proof: We prove it by reduction to absurdity. Assume that there exists a real number a_0 such that

$$a_0 + \underline{\eta}(a_0) \le r,\tag{76}$$

$$-\underline{\eta}(a_0) > \sup_{a} \{ a - \underline{\zeta}(a) | \underline{\zeta}(a) \le r \}.$$
(77)

We will lead contradiction with the two cases, case 1: $a_1 := \inf_a \{a | \eta(a) = \eta(a_0)\} > a_0$, case 2: $a_1 = a_0$.

In case 1, for any real number $\epsilon \in (0, a_0 - a_1)$, the inequality $\eta(a_1 - \epsilon) > \eta(a_1 + \epsilon)$ holds. Using (71), we have

$$\underline{\zeta}(a_1 - \epsilon) \le \underline{\eta}(a_1 + \epsilon) + a_1 + \epsilon = \underline{\eta}(a_0) + a_1 + \epsilon$$
$$\le r + (a_1 - a_0) + \epsilon < r.$$

Thus,

$$\sup_{a} \{a - \underline{\zeta}(a) | \underline{\zeta}(a) \le r\} \ge a_1 - \epsilon - \underline{\zeta}(a_1 - \epsilon)$$
$$\ge a_1 - \epsilon - (a_1 + \epsilon) - \underline{\eta}(a_1 + \epsilon) = -\underline{\eta}(a_0) - 2\epsilon.$$

Taking the limit $\epsilon \to 0$, we obtain $\sup\{a - \underline{\zeta}(a) | \underline{\zeta}(a) \le r\} \ge -\eta(a_0)$, which contradicts (77).

In case 2, the inequality $\eta(a_0) < \underline{\eta}(a_0 - \epsilon)$ holds for $\forall \epsilon > 0$. Using (71), we have $\zeta(a_0 - \epsilon) \leq \overline{\eta(a_0)} + a_0 \leq r$. Thus,

$$\sup_{a} \{a - \underline{\zeta}(a) | \underline{\zeta}(a) \le r\} \ge a_0 - \epsilon - \underline{\zeta}(a_0 - \epsilon)$$
$$\ge a_0 - \epsilon - a_0 - \underline{\eta}(a_0) = -\epsilon - \underline{\eta}(a_0).$$

This also contradicts (77).

Define the sets I and I' as

$$I := \{ a \in \mathbb{R} | \underline{\zeta}(a) > \underline{\zeta}(a-\epsilon) \quad \forall \epsilon > 0 \},$$

$$I' := \{ a \in \mathbb{R} | \underline{\zeta}(a+\epsilon) > \underline{\zeta}(a) \quad \forall \epsilon > 0 \}.$$

As upper bounds of $\eta(a)$, we have the following two lemmas.

Lemma 16: We have two inequalities

$$\underline{\eta}(a) \le \inf_{a \in I} \{ \underline{\zeta}(a') - a' | a' \le a \},\tag{78}$$

$$\underline{\eta}(a) \le \inf_{a \in I'} \{ \underline{\zeta}(a') - a' | a' < a \}.$$
(79)

If $\underline{\zeta}(a) = \overline{\zeta}(a)$ for any real *a*, we have two other inequalities

$$\overline{\eta}(a) \le \inf_{a \in I} \{ \underline{\zeta}(a') - a' | a' \le a \}, \tag{80}$$

$$\overline{\eta}(a) \le \inf_{a \in I'} \{ \underline{\zeta}(a') - a' | a' < a \}.$$
(81)

Proof: First, we prove (78). Let $a' \in I$ be a real number satisfying $a' \leq a$. From (72), we have

$$a' - \epsilon + \underline{\eta}(a') \le \underline{\zeta}(a' - \epsilon), \quad \forall \epsilon > 0.$$

Since $\epsilon > 0$ is arbitrary, we obtain the relation

$$\underline{\eta}(a) \leq \underline{\eta}(a') \leq \underline{\zeta}(a'-0) - a' \leq \underline{\zeta}(a') - a'.$$

From the arbitrariness of a', the above relation implies (78). Similarly, we can prove (80). Next, we prove (79). Let $a' \in I'$ be a real number satisfying a' < a. From (72), we have

$$a' + \underline{\eta}(a' + \epsilon) \le \underline{\zeta}(a').$$

If $\epsilon > 0$ is small enough,

$$\underline{\eta}(a) \le \underline{\eta}(a' + \epsilon) \le \underline{\zeta}(a') - a'.$$

From the arbitrariness of a', the above inequality implies (79). Similarly, we can prove (81).

Lemma 17: Assume that a real number r satisfies that

$$r < \sup_{a} \left\{ \inf_{a'} \left\{ \underline{\zeta}(a') - a' \middle| a' \le a \right\} + a \right\}.$$
(82)

The maximum a_r of

$$\left\{a\left|\inf_{a'}\left\{\underline{\zeta}(a') - a'\right|a' \le a\right\} + a = r\right\}$$
(83)

exists. Moreover, the inequality

$$\underline{\eta}(a_r + \epsilon) \le \inf_a \left\{ \underline{\zeta}(a) - a \, \middle| \, a \le a_r \right\}, \quad \forall \epsilon > 0$$
(84)

holds. When $\zeta(a) = \underline{\zeta}(a)$ for any a, we can replace $\underline{\eta}$ by $\overline{\eta}$ in the above argument.

Proof: Since the function $g : a \mapsto \inf_{a'} \{ \underline{\zeta}(a') - a' | a' \le a \} + a$ is continuous and increases monotonically, it follows from (82) that set (83) is bounded and closed. Thus the maximum of the set (83) exists.

Next, we prove (84). First we assume that

$$\underline{\zeta}(a_r) - a_r \ge \inf_{a'} \left\{ \underline{\zeta}(a') - a' \, \middle| \, a' \le a_r \right\},\tag{85}$$

Since the function g increases monotonically and $a_r + \epsilon$ does not belong to the set (83), the relations

$$\underline{\zeta}(a) < \underline{\zeta}(a_r) = \inf_{a'} \left\{ \underline{\zeta}(a') - a' \middle| a' \le a_r \right\} + a_r = r$$

$$< \inf_{a'} \left\{ \underline{\zeta}(a') - a' \middle| a' \le a_r + \epsilon \right\} + a_r + \epsilon \le \underline{\zeta}(a_r + \epsilon)$$

hold for $a < a_r$. Applying (72) to the case $b = a_r + \epsilon$, we obtain (84).

Second, we assume the opposite inequality

$$\underline{\zeta}(a_r) - a_r < \inf_{a'} \left\{ \underline{\zeta}(a') - a' \, \middle| \, a' \le a_r \right\}. \tag{86}$$

There exists a sequence $\{a_n\}$ such that

$$\frac{\zeta(a_n) - a_n \to \inf_{a'} \left\{ \underline{\zeta}(a') - a' \,\middle|\, a' \le a_r \right\}}{a_n < a_r}$$

From the above relations, there exists an integer N such that $\zeta(a_n) < \zeta(a_r), \quad \forall n \ge N$. Using (72), we have

$$\underline{\eta}(a_r) \leq \underline{\zeta}(a_n) - a_n.$$

Thus, we obtain

$$\underline{\eta}(a_r) \le \inf_{a'} \left\{ \underline{\zeta}(a') - a' \, \middle| \, a' \le a_r \right\},\tag{87}$$

which implies (84).

B. Gärtner-Ellis theorem

Here, for our proof of Theorem 3, we discuss Gärtner-Ellis theorem [20]. Let X_n be a sequence of random variables. Then, the logarithmic moment function is defined as

$$\Lambda_n(t) := \log \mathcal{E}_{X_n} e^{tX_n}$$

where E_{X_n} denotes the expectation concerning the random variable X_n . The logarithmic moment function $\Lambda_n(t)$ is convex.

Theorem 18: Assume that the limit $\Lambda(t) := \lim_{n \to \infty} \frac{\Lambda_n(t)}{n}$ exists. Then, defining the rate function

$$\Lambda^*(R) := \sup_t tR - \Lambda(t), \tag{88}$$

we have

$$\underline{\lim} \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} \ge a \right\} \ge \inf_{R \ge a} \Lambda^*(R) \tag{89}$$

$$\overline{\lim} \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} > a \right\} \le \inf_{R > a} \Lambda^*(R) \tag{90}$$

$$\underbrace{\lim \frac{-1}{n} \log \mathcal{P}_{X_n}}_{n} \left\{ \frac{X_n}{n} \le a \right\} \ge \inf_{R \le a} \Lambda^*(R) \tag{91}$$

$$\overline{\lim} \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} < a \right\} \le \inf_{R < a} \Lambda^*(R).$$
(92)

Using the above theorem, we can show the following theorem. Since the function $\Lambda_n(t)$ is convex, the $\Lambda(t)$ is convex, too. Hence, when we choose the real numbers R_1, R_2, R_3 and R_4 as

$$R_1 := \lim_{t \to \infty} \frac{\Lambda(t)}{t}, \quad R_2 := \lim_{t \to +0} \frac{\Lambda(t)}{t}, \tag{93}$$

$$R_3 := \lim_{t \to -0} \frac{\Lambda(t)}{t}, \quad R_4 := \lim_{t \to -\infty} \frac{\Lambda(t)}{t}, \tag{94}$$

the relations

$$R_4 \le R_3 \le R_2 \le R_1 \tag{95}$$

hold. Thus, as is proven latter, the equations

$$\lim \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} \ge a \right\} = \lim \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} > a \right\}$$
$$= \begin{cases} 0 & \text{if } a \le R_2 \\ \max t R - \Lambda(t) > 0 & \text{if } R_2 < a < R_1 \\ \infty & \text{if } R_1 < a \end{cases}$$
(96)

and

=

$$\lim \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} \le a \right\} = \lim \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} < a \right\}$$
$$= \begin{cases} 0 & \text{if } R_3 \le a \\ \max_{t < 0} tR - \Lambda(t) > 0 & \text{if } R_4 < a < R_3 \\ \infty & \text{if } a < R_4 \end{cases}$$
(97)

hold. Moreover, if the function Λ is differentiable at $t_0 > 0$, and if $R_2 < a < \Lambda'(t_0)$, we have

$$\lim \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} \ge a \right\} = \lim \frac{-1}{n} \log \mathcal{P}_{X_n} \left\{ \frac{X_n}{n} > a \right\}$$
$$= \sup_{t_0 \ge t > 0} tR - \Lambda(t). \tag{98}$$

Proof of (96), (97) and (98): First, we calculated the rate function $\Lambda^*(a)$. When $R_3 \leq a \leq R_2$,

$$\Lambda^*(a) = \sup_t ta - \Lambda(t) = 0a - \Lambda(0) = 0.$$

Assume that $R_2 < a < R_1$. Then, if $\epsilon > 0$ is sufficiently small,

$$\Lambda^*(a) = \sup_t ta - \Lambda(t) \ge \epsilon a - \Lambda(\epsilon) = (a - R_2)\epsilon + R_2\epsilon - \Lambda(\epsilon)$$
$$\cong (a - R_2)\epsilon + R_2\epsilon - \lim_{t \to +0} \frac{\Lambda(t)}{t}\epsilon = (a - R_2)\epsilon > 0.$$

Now, we choose $t_a \neq 0$ such that $t_a a = \Lambda(t_a)$. The convexity of Λ guarantees that

$$\Lambda^*(a) = \sup_{t} ta - \Lambda(t) = \max_{0 \le t \le t_a} ta - \Lambda(t)$$

For a such that $R_2 \leq a' \leq a$, since $t_a \geq t_{a'}$, we have

$$\Lambda^*(a') = \max_{0 \le t \le t_{a'}} ta' - \Lambda(t) = \max_{0 \le t \le t_a} ta' - \Lambda(t).$$

Hence, the function Λ^* is continuous $[R_2, a]$. Thus, the function Λ^* is continuous $[R_2, R_1)$. in addition, when $a > R_1$, $\Lambda^*(a) = \infty$. Hence, when $a < R_1$, we obtain

$$\inf_{R \ge a} \Lambda^*(R) = \inf_{R > a} \Lambda^*(R)$$
$$= \begin{cases} 0 & \text{if } a \le R_2 \\ \max_{t > 0} tR - \Lambda(t) > 0 & \text{if } R_2 < a < R_1 \end{cases}$$

When $a > R_1$,

$$\inf_{R \ge a} \Lambda^*(R) = \inf_{R > a} \Lambda^*(R) = \infty.$$

Therefore, we obtain (96). Similarly, we can prove (97).

Moreover, for a such that $R_2 \leq a < R_1$, we choose $t'_a = \operatorname{argmax}_t ta - \Lambda(t)$. The convexity of Λ guarantees that when $R_2 \leq a' < a$, we have $t'_{a'} \leq t'_a$. Therefore, we prove (98).

Finally, in order prove (16) and (17) in our proof of Theorem 3, we focus on the probability distributions $p_n = \{p_{n,i}\}$, and apply the above discussion to the random variable $-\log p_{n,i}$. Using (96), (97) and (98), we obtain (16) and (17).

References

- C. H. Bennett and S. J. Wiesner, "Communication via one- and twoparticle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, 69, 2881, 1992.
- [2] 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.
- [3] A. Ekert, Phys. Rev. Lett. 67 661, 1991.
- [4] M. A. Nielsen, "Conditions for a Class of Entanglement Transformations," Phys. Rev. Lett., 83, 436, 1999.
- [5] F. Morikoshi and M. Koashi, "Deterministic entanglement concentration," Phys. Rev. A, 64, 022316, 2001.
- [6] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher "Concentrating partial entanglement by local operations," *Phys. Rev. A*, 53, 2046, 1996; LANL eprint quant-ph/9511030.
- [7] M. Hayashi and K. Matsumoto, "Variable length universal entanglement concentration by local operations and its application to teleportation and dense coding," LANL eprint quant-ph/0109028, 2001.
- [8] M. Hayashi, M. Koashi, K. Matsumoto, F. Morikoshi and A. Winter, "Error exponents for entangle concentration," J. Phys. A: Math. and Gen., 36,527-553, (2003); LANL eprint quant-ph/0206097, 2002.
- [9] T.S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Transactions on Information Theory*, vol.39, pp.752–772, 1993.

- [10] S. Verdú and T.S. Han, "A general formula for channel capacity," *IEEE Transactions on Information Theory*, vol.40, pp.1147–1157, 1994.
- [11] T.S. Han, "Hypothesis testing with the general source," *IEEE Transac*tions on Information Theory, vol.46, pp.2415–2427, 2000.
- [12] T.S. Han, "The reliability functions of the general source with fixedlength coding," *IEEE Transactions on Information Theory*, vol.46, pp.2117–2132, 2000.
- [13] T.S. Han, Information-Spectrum Methods in Information Theory, (Baifukan-Press, Tokyo, 1998 (in Japanese), (English Translation: Springer-Verlag, New York).
- [14] H. Nagaoka and M. Hayashi, "An information-spectrum approach to classical and quantum hypothesis testing," LANL eprint quant-ph/0206185, 2002.
- [15] M. Hayashi and H. Nagaoka, "General formulas for capacity of classicalquantum channels," *IEEE Transactions on Information Theory*, Vol.49, No.7, pp.1753–1768 (2003); LANL eprint quant-ph/0206186, 2002.
- [16] R. Bhatia, Matrix analysis, Springer-Verlag, New York, 1997.
- [17] H.-K. Lo and S. Popescu, "Concentrating entanglement by local actions: Beyond mean values," *Phys. Rev. A*, 63, 022301, 2001; LANL eprint quant-ph/9707038.
- [18] Y. Steinberg and S. Verdú, "Simulation of random processes and ratedistortion theory," *IEEE Trans. Inform. Theory*, 42, 63–86 (1996).
- [19] S. Vembu and S. Verdú, "Generating random bits from an arbitrary source: fundamental limits," *IEEE Trans. Inform. Theory*, **41**, 1322-1332 (1995).
- [20] A. Dembo and O. Zeitouni, Large Deviations Techniques and Applications, Springer-Verlag, New York, 1998.
- [21] I. Csiszár and J. Körner, Information Theory, coding theorems for discrete memoryless systems, Academic Press, 1981.
- [22] M. Hayashi, "Second order asymptotics in fixed-length source coding and intrinsic randomness," e-print: cs.IT/0503089.