Random Number Conversion and LOCC Conversion via Restricted Storage

Wataru Kumagai, Masahito Hayashi

Abstract—We consider random number conversion (RNC) through random number storage with restricted size. We clarify the relation between the performance of RNC and the size of storage in the framework of first- and second-order asymptotics, and derive their rate regions. Then, we show that the results for RNC with restricted storage recover those for conventional RNC without storage in the limit of storage size. As an application to quantum information theory, we analyze LOCC conversion via entanglement storage with restricted size. Moreover, we derive the optimal LOCC compression rate under a constraint of the accuracy of conversion.

Index Terms—Random number conversion, LOCC conversion, Compression rate, Entanglement, Second-order asymptotics.

I. INTRODUCTION

Random number conversion (RNC) is a fundamental topic in information theory [20], and its asymptotic behavior has been well studied in the context of not only the first-order asymptotics but also the second-order asymptotics [6], [16], [11]. In a realistic situation, we often use this conversion via a storage with a limited size, like a hard disk. In this case, first, we convert the initial random number to another random number in a storage with a limited size, which is called random number storage or simply storage. Second, we convert the random number in the storage to the desired random number. Here, we have to consider the trade-off between the accuracy of the conversion and the size of the storage when the target random variable is fixed. This process can be regarded as RNC with randomness compression. When the size of media for the conversion is limited, it is natural to consider this problem.

In this paper, we consider this problem when the initial and the target random variables are given as multiple copies of respective random variables. That is, the initial distribution is given as the \( n \)-fold independent and identical distribution (i.i.d.) of a distribution \( P \) and the target distribution is given as the \( n \)-fold i.i.d. of another distribution \( Q \). In this case, as the first step, we convert the \( n \)-fold i.i.d. of \( P \) to a probability distribution on the random number storage whose cardinality is limited. Then, as the second step, we approximately convert the distribution on the storage to an i.i.d. of \( Q \). In the problem, since there is a freedom of the required number of copies of \( Q \) in the target distribution, we have to take care of the trade-off among three factors, the accuracy of the conversion, the size of the storage, and the required number of copies of \( Q \) in the output distribution. For simplicity, we fix the accuracy of the conversion, and investigate the trade-off between the size of the storage and the required number of copies of \( Q \) in the output distribution. We call this problem RNC via restricted storage. In particular, when \( P = Q \), this problem can be regarded as random number compression to the given storage.

One of our main purposes is to derive the maximum conversion rate under the situation where the rate of storage size is properly limited. If the size of storage is small, the maximum number of convertible copies from \( P^n \) to \( Q \) should also be small since the conversion has to once pass through the small storage. Thus, the allowable size of storage closely relates with the conversion rate of RNC via restricted storage under the accuracy constraint for conversion. In this paper, we focus on the rates for the allowable size of storage and the possible number of copies of target distribution, and investigate the regions of the first-order and the second-order rates. The existing studies [18], [22] derived the region of the first-order and the second-order rates in different problems. Our problem is different from their results in the description of the solution as follows. In their problems, there is a trade-off even in the first-order rates. However, as is shown in this paper, the region of the first-order rates can be characterized by only one optimal point, i.e., there is no trade-off for the first order rates. This region does not depend on the accuracy constraint of conversion. This fact can be found by a combination of simple observations, and hence, it is enough to consider the region of the second-order rates at the optimal point with the first order rate in our problem while they describe the region of rates as the sum of the first order and the second orders [18], [22].

RNC via restricted storage makes sense in a natural setting when the conversion of distributions is given by a deterministic map between the initial and the target probability spaces. In fact, we can derive the same result when we allow any conversion satisfying the majorization condition as our operation of the conversion of the probability distributions.
although this condition does not naturally have its operational meaning. However, our result with the majorization condition can be applied to LOCC conversion via restricted storage for pure states in quantum information theory because LOCC conversion of entangled state can be characterized by the majorization condition \[14\]. In the extension to LOCC conversion of entangled states, it is assumed that an initial i.i.d. pure entangled state is once transformed into a bipartite system called *entanglement storage* with smaller dimension by LOCC and then transformed again to approximate a target i.i.d. pure state by LOCC. In particular, when the target pure entangled state is the same as the original pure entangled state, this problem can be regarded as LOCC compression of entangled states into the given entanglement storage. Since the storage to keep the entangled states is a limited resource, the analysis for LOCC compression is expected to be useful to store entanglement in small quantum system.

To treat the asymptotic behavior of RNC and LOCC conversion, we focus on its mathematical structure called deterministic conversion and majorization conversion. The deterministic conversion is conventionally used in the context of RNC in classical information theory. On the other hand, it is well-known that LOCC convertibility between pure entangled states can be translated to majorization relation between two probability distributions which consist of the squared Schmidt coefficients of the states \[14\], \[21\], and thus, LOCC conversion for pure state is mathematically equivalent to majorization conversion for probability distributions. The asymptotic behavior of LOCC conversion has been intensively studied \[2\], \[3\], \[4\], \[5\], \[6\], \[7\], \[11\]. Then, it is shown that the accuracy of majorization conversion and deterministic conversion asymptotically coincide with each other by dividing the problem into the uniform case (i.e. either an initial or a target distribution is uniform) and the non-uniform case (i.e. both initial and target distributions are non-uniform).

The paper is organized as follows. In Section II, we introduce two kinds of approximate conversion methods called deterministic conversion and majorization conversion, respectively. Then, we formulate random number conversion (RNC) via restricted storage as approximate conversion through a set with restricted size. To begin with, we define the accuracy for the approximate conversion, and then, introduce the performance of RNC as the maximum conversion number for a target i.i.d. distribution which can be approximated from an initial i.i.d. distribution. After that, we give basic relations between the performances of deterministic and majorization conversions and some properties for those in non-asymptotic setting. In Section III we proceed to asymptotic analysis for RNC via restricted storage. Then, we show the relation between the rates of the maximum conversion number and storage size and draw various rate regions in both frameworks of first and second-order asymptotic theory. In Section IV we see the relation with conventional RNC without restriction for storage size. Then, we observe that the performance of RNC via restricted storage converges to that of conventional RNC when the second-order rate of storage size tends to infinity. In Section V we consider LOCC conversion via entanglement storage for quantum pure states. Using the results for RNC, we derive the asymptotic performance of optimal LOCC conversion. In particular, optimal LOCC compression rate is derived. In Section VI we give technical details of Theorems, Propositions and Lemmas. In Section VII we state the conclusion of the paper.

II. NON-ASYMPTOTICS FOR RANDOM NUMBER CONVERSION VIA RESTRICTED STORAGE

We introduce two kinds of approximate conversion methods called deterministic conversions and majorization conversions. Then, to analyze the performance of random number conversion via restricted storage for the conversions, we define the maximum convertible number of copies of target distribution under constrains for storage size and accuracy.

A. Deterministic Conversion

In this subsection, as is illustrated in Fig. I we consider approximate conversion problems when the conversion is routed through a storage with limited size \(N\).

First of all, we introduce a deterministic conversion. For a probability distribution \(P\) on a finite set \(\mathcal{X}\) and a map \(W : \mathcal{X} \rightarrow \mathcal{Y}\), we define the probability distribution \(W(P)\) on \(\mathcal{Y}\) by

\[
W(P)(y) := \sum_{x \in W^{-1}(y)} P(x).
\]

That is, \(W(P)\) is the distribution transformed by the deterministic conversion \(W\).

In order to treat the quality of conversion, we introduce the fidelity (or the Bhattacharyya coefficient) \(F\) between two probability distributions over the same discrete set \(\mathcal{Y}\) as

\[
F(Q, Q') := \sum_{y \in \mathcal{Y}} \sqrt{Q(y)} \sqrt{Q'(y)}.
\]

This value \(F\) represents how close two probability distributions are and relates to the Hellinger distance \(d_H\) as \(d_H(Q, Q') = \sqrt{1 - F(Q, Q')}\) \[19\]. Then, we define the maximal fidelity \(\mathcal{F}\) from \(P\) on \(\mathcal{X}\) to \(Q\) on \(\mathcal{Y}\) among deterministic conversions by

\[
\mathcal{F}(P \rightarrow Q) := \max\{F(W(P), Q) | W : \mathcal{X} \rightarrow \mathcal{Y}\}.
\]

Moreover, when the size of the storage is limited, the maximal fidelity via restricted storage with size \(N\) is defined by

\[
\mathcal{F}(P \rightarrow Q | N) := \max\left\{F(W' \circ W(P), Q) \mid W : \mathcal{X} \rightarrow \mathbb{N}_N, W' : \mathbb{N}_N \rightarrow \mathcal{Y}\right\},
\]

where \(\mathbb{N}_N := \{1, \ldots, N\}\).

When confidence coefficient \(0 < \nu < 1\) is fixed, we define the maximal convertible number \(L\) of \(Q^L\) which can be approximated from \(P\) by deterministic conversions as

\[
L^\nu(P, Q | \nu) := \max\{L | F(W(P), Q^L) \geq \nu, W : \mathcal{X} \rightarrow \mathcal{Y}^L\}.
\]
Moreover, when the size of the storage is limited, the maximal number from $P$ to $Q$ via restricted storage with size $N$ is defined by

$$L^P(P,Q|\nu,N) := \max\left\{L \mid W : \mathcal{X} \rightarrow \mathbb{N}_N, W' : \mathbb{N}_N \rightarrow \mathcal{Y}, F(W') = F(W(P), Q^L) \geq \nu \right\}. $$

Then the above values can be rewritten as

$$L^D(P,Q|\nu) = \max\{L|F^D(P \rightarrow Q^D) \geq \nu\}, \quad (5)$$

$$L^D(P,Q|\nu,N) = \max\{L|F^D(P \rightarrow Q^D|N) \geq \nu\}. \quad (6)$$

In particular, when the source distribution is $n$-fold i.i.d. of $P$, we define

$$L^D_n(P,Q|\nu) := L^D(P^n,Q|\nu),$$

$$L^D_n(P,Q|\nu,N) := L^D(P^n,Q|\nu,N).$$

One of main issues of this paper is the asymptotic expansion of $L^D_n(P,Q|\nu,N)$ up to the order $\sqrt{n}$.

B. Majorization Conversion

In order to relax the condition for conversion, we introduce the concept of majorization. For a probability distribution $P$ on a finite set, let $P_l$ be a sequence $\{P_l\}_{i=1}^{|X|}$ and $P_l$ is the $i$-th element of $\{P(x)\}_{x \in X}$ sorted in decreasing order for $1 \leq i \leq |X|$. When probability distributions $P$ and $Q$ satisfy $\sum_{i=1}^{|X|} P_l^i \leq \sum_{i=1}^{|X|} Q_l^i$ for any $l$, it is said that $P$ is majorized by $Q$ and written as $P \prec Q$. Here, note that the sets where $P$ and $Q$ are defined do not necessarily coincide with each other. The majorization relation is a partial order on a set of probability distributions in which each distribution is defined on a finite set $[1]$. For an example, for a probability distribution $P$ on a finite set $X$ and a map $W : \mathcal{X} \rightarrow \mathcal{Y}$, we have the majorization relation $P \prec W(P)$. For another example, we denote the uniform distribution by $U_l$ whose support size is $l$. When the support size of a probability distribution $P$ is at most $l$, we have $U_l \prec P$. When $P \prec P'$, we call the conversion from $P$ to $P'$ a majorization conversion.

Then, we introduce the maximal fidelity among the majorization conversions as

$$F^M(P \rightarrow Q) := \max_{P'} \{F(P',Q)|P \prec P' \in \mathcal{P}(\mathcal{Y})\} \quad (7)$$

where $P$ and $Q$ are probability distribution on $X$ and $Y$, respectively, and $\mathcal{P}(\mathcal{Y})$ is the set of all probability distributions on $\mathcal{Y}$. Moreover, when the size of the storage is limited, the maximal fidelity via restricted storage with size $N$ is given by

$$F^M(P \rightarrow Q|N) := \max\left\{F(P',Q) \mid P \prec P' \in \mathcal{P}(\mathbb{N}_N) \right\}. $$

Then, it obviously satisfies

$$F^M(P \rightarrow Q|N) \leq \sum_{i=1}^{|X|} Q_l^i. \quad (8)$$

by the monotonicity of the fidelity.

Similar to the deterministic conversion, when confidence coefficient $0 < \nu < 1$ is fixed, we define the maximal convertible number $L$ of $Q^D$ which can be approximated from $P$ by majorization conversions as

$$L^M(P,Q|\nu,N) = \max\{L|F^M(P \rightarrow Q^D|N) \geq \nu\}. $$

Moreover, when the size of the storage is limited, the maximal number from $P$ to $Q$ via restricted storage with size $N$ is defined by

$$L^M_n(P,Q|\nu,N) = \max\{L|P \prec P' \prec P'' \in \mathcal{P}(\mathbb{N}_N), F(P'',Q) \geq \nu\}. \quad (9)$$

Then the above values can be rewritten as

$$L^M(P,Q|\nu) = \max\{L|F^M(P \rightarrow Q^D) \geq \nu\}, \quad (10)$$

$$L^M(P,Q|\nu,N) = \max\{L|F^M(P \rightarrow Q^D|N) \geq \nu\}. \quad (10)$$

In particular, when the source distribution is $n$-fold i.i.d. of $P$, we define

$$L^M_n(P,Q|\nu) := L^M(P^n,Q|\nu),$$

$$L^M_n(P,Q|\nu,N) := L^M(P^n,Q|\nu,N).$$

One of main issues of this paper is the asymptotic expansion of $L^M_n(P,Q|\nu,N)$ up to the order $\sqrt{n}$. This quantity plays an important role in quantum information theory.

C. Basic Properties of Conversions

To begin with, we summarize some properties about max-}

imum fidelity of deterministic and majorization conversion. Since $P \prec W(P)$ for a map $W : \mathcal{X} \rightarrow \mathcal{Y}$, we have the relations

$$F^D(P \rightarrow Q) \leq F^M(P \rightarrow Q), \quad (11)$$

$$F^D(P \rightarrow Q|N) \leq F^M(P \rightarrow Q|N). \quad (12)$$

The following lemmas hold for the uniform distribution $U_l$ in non-asymptotic settings.

**Lemma 1:** [1] For a probability distribution $P$ and a natural number $l$, let $C_l(P)$ be defined on a finite set $X$ as follows

$$C_l(P)(j) := \left\{ \frac{\sum_{i=j}^{l+j} P^i(j)}{l-j} \right\} \quad (13)$$

where $|X|$ represents the cardinality of the set $X$ and $J_{P,l}$

$$:= \max\{0\} \cup \left\{ 1 \leq j \leq l-1 \mid \frac{\sum_{i=j+1}^{l+j} P^i(j)}{l-j} < P^l(j) \right\}. \quad (14)$$

Then, the following holds:

$$F^M(P \rightarrow U_l) = F^M(C_l(P),U_l)$$

$$= \sqrt{\frac{1}{l} \left( \sum_{j=1}^{J_{P,l}} P^i(j) \right) + \left( l - J_{P,l} \right) \sum_{i=j}^{l+j} P^i(j) \right)^{1/2}}. \quad (15)$$
In addition, the following lemma holds.

**Lemma 2:** For probability distributions $P$ and $Q$ on a finite set and a natural number $l$,

$$F^M(P \to Q|l) = F^M(C_l(P) \to Q),$$

where $C_l(P)$ was defined in ([13]). We provide the proof of Lemma 2 in Appendix VI-A. Note that $C_l(P)$ is determined by the source distribution $P$ and does not depend on the target distribution $Q$ in Lemma 2. This fact is essential in the asymptotics for $F^M(P \to Q|l)$.

Next, we summarize some properties about maximum convertible number of two conversion. From (11) and (12), we have

$$L_n^M(P, Q|\nu) \geq L_n^D(P, Q|\nu),$$

$$L_n^M(P, Q|\nu, N) \geq L_n^D(P, Q|\nu, N).$$

One of main issues of this paper is to derive asymptotic behaviors of $L_n^M(P, Q|\nu, N)$ and $L_n^D(P, Q|\nu, N)$ as stated above. Fortunately, when either the source distribution $P$ or the target distribution $Q$ is a uniform distribution, their asymptotic behaviors are evaluated by direct conversions without storage in the following way.

**Proposition 3:**

$$L_n^M(U_i, Q|\nu, l^m) \geq L_{\min\{n,m\}}^D(U_i, Q|\nu),$$

$$L_n^M(U_i, Q|\nu, l^m) = L_{\min\{n,m\}}^M(U_i, Q|\nu).$$

**Proposition 4:** When $m \geq L_n^D(P, U_i|\nu)$,

$$L_n^D(P, U_i|\nu, l^m) = L_n^D(P, U_i|\nu).$$

Otherwise,

$$m \leq L_n^D(P, U_i|\nu, l^m) \leq m - 2 \log_2 \nu.$$ (21)

Similarly, when $m \geq L_n^M(P, U_i|\nu)$,

$$L_n^M(P, U_i|\nu, l^m) = L_n^M(P, U_i|\nu).$$

Otherwise,

$$m \leq L_n^M(P, U_i|\nu, l^m) \leq m - 2 \log_2 \nu.$$ (23)

We provide the proof of Lemma 3 and 4 in Appendices VI-B and VI-C, respectively.

III. ASYMPTOTICS FOR RANDOM NUMBER CONVERSION VIA RESTRICTED STORAGE

We clarify the relation between rate of size of restricted storage and the number of copies of target distribution.

A. First-Order Rate Region

To begin with, we analyze the first-order asymptotic behavior of sizes of storage and target distribution. In order to treat the asymptotic relation between them, we define the rate region as follows.

**Definition 5:** For $i = D$ and $M$,

$$R_{P,Q}^{1,M}(\nu) := \left\{ (s_1, t_1) \mid \liminf_{n \to \infty} F_i^n(P^n \to Q^{l_1 n}|2^{s_1 n}) \geq \nu \right\},$$

where $\nu$ is essential in the asymptotics for $R_{P,Q}^{1,D}(\nu)$.

We say that a rate pair $(s_1, t_1)$ is $\nu$-achievable by deterministic conversions or majorization conversions when $(s_1, t_1) \in R_{P,Q}^{1,D}(\nu)$ or $R_{P,Q}^{1,M}(\nu)$.

**Theorem 6:** For $\nu \in (0, 1)$, we have

$$R_{P,Q}^{1,D}(\nu) = R_{P,Q}^{1,M}(\nu) = \left\{ (s_1, t_1) \mid 0 \leq s_1, 0 \leq t_1 \leq \frac{\min\{H(P), s_1\}}{H(Q)} \right\},$$

where $H(P)$ and $H(Q)$ are the Shannon entropy of $P$ and $Q$, respectively.

We give the proof of Theorem 6 in Appendix VI-D From Theorem 6 and $R_{P,Q}^{1,D}(\nu)$ and $R_{P,Q}^{1,M}(\nu)$ coincide with each other and do not depend on $\nu \in (0, 1)$. In the following, we denote the rate regions by $R_{P,Q}$ simply. The rate region is illustrated as Fig. 2.

Here, larger $t_1$ and smaller $s_1$ give a better performance. Hence, we say that the rate pair $(s_1, t_1)$ is better $(s_1', t_1')$ when $t_1 \geq t_1'$ and $s_1 \leq s_1'$. We define the set of admissible rate pairs as follows.

**Definition 7:**

$$A_{P,Q}^{l_1} := \left\{ (s_1, t_1) \in R_{P,Q} \mid \text{no achievable rate pair is better than } (s_1, t_1) \text{ except for itself.} \right\}$$

Due to Theorem 6 the set of admissible rate pairs is given as follows.

**Corollary 8:**

$$A_{P,Q}^{l_1} = \left\{ \left( s_1, \frac{s_1}{H(Q)} \right) \mid 0 \leq s_1 \leq H(P) \right\}.$$

The set of admissible rate pairs are illustrated as the thick line in Fig. 2. We call $(H(P), H(Q))$ in the set of admissible rate pairs the extreme rate pair. In later discussion, we separately treat the problem according to whether an admissible rate pair is the extreme rate pair or not.

B. Second-Order Rate Region
Fig. 3. The flow chart for second-order rate regions. Let us consider the conversion from $P^n$ via storage with size $2^{n s_1 + s_2 + 2 \sqrt{n}}$ to $Q^{s_1 + s_2 \sqrt{n}}$. The form of second-order rate region depends on the admissibility and the extremality of a first-order rate pair $(s_1, t_1)$, the uniformity of probability distribution $P$ or $Q$, and the value of $C_{P,Q}$ defined in (32).

Next, we analyze the second-order asymptotic behavior of sizes of storage and target distribution. For simplicity, we employ the following abbreviate notations for $i = D$ and $M$:

$$F_{P,Q,s_1,t_1,s_2}(t_2) := \lim_{n \to \infty} F_i^n \left( P^n \to Q^{s_1 + s_2 \sqrt{n}} \right) .$$

In order to treat the asymptotic relation between them, we define the rate region as follows.

**Definition 9:** For $i = D$ and $M$,

$$\mathcal{R}_{P,Q}^{2,i}(s_1,t_1,\nu) := \left\{ (s_2,t_2) \mid F_{P,Q,s_1,t_1,s_2}(t_2) \geq \nu \right\} .$$

Our purpose is to describe the above second-order rate regions. Then, it is enough to derive a computable form of the limit of the maximum fidelity $F_{P,Q,s_1,t_1,s_2}(t_2)$ for $i = D$ and $M$ by Definition 27. Actually, the asymptotics of the maximum fidelity is reduced to a maximization problem of continuous fidelity with a fixed normal distribution.

Here, we have the following lemma.

**Lemma 10:** Let $P$ and $Q$ be arbitrary probability distributions on finite sets. Then, there is a function $F_{P,Q,s_1,t_1,s_2} : \mathbb{R} \to [0,1]$ which is continuous and strictly monotonically decreasing on $F_{P,Q,s_1,t_1,s_2}^{-1}((0,1))$ and

$$F_{P,Q,s_1,t_1,s_2}(t_2) = F_{P,Q,s_1,t_1,s_2}^D(t_2) = F_{P,Q,s_1,t_1,s_2}^M(t_2) \quad (26)$$

for any $t_2 \in \mathbb{R}$.

Then, the following theorem is obtained by Lemma 10.

**Theorem 11:** Let $P$ and $Q$ be arbitrary probability distributions on finite sets. For arbitrary $s_1 > 0$, $s_2 \in \mathbb{R}$ and $\nu \in (0,1)$,

$$L_{P,Q}(\nu, 2^{s_1 + s_2 \sqrt{n}}) \approx L_{P,Q}^D(\nu, 2^{s_1 + s_2 \sqrt{n}}) \approx L_{P,Q}^M(\nu, 2^{s_1 + s_2 \sqrt{n}}) \cong \frac{\min \{ H(P), s_1 \}}{H(Q)} \sum \frac{1}{n} F_{P,Q,s_1,t_1,s_2}^{-1}(\nu) \sqrt{n}, \quad (27)$$

where $\cong$ means that the difference between RHS and LHS of $\cong$ is of $o(\sqrt{n})$.

Moreover, Theorem 11 implies the following theorem about second-order rate regions.

**Theorem 12:** Let $P$ and $Q$ be arbitrary probability distributions on finite sets. For $0 < s_1 \leq H(P)$, $s_2 \in \mathbb{R}$ and $\nu \in (0,1)$,

$$\mathcal{R}_{P,Q}^{2,D}(s_1,\nu) \approx \mathcal{R}_{P,Q}^{2,M}(s_1,\nu) \approx \mathcal{R}_{P,Q}^{2,i}(s_1,\nu) \approx \left\{ (s_2,t_2) \mid t_2 \leq F_{P,Q,s_1,t_1,s_2}^{-1}(\nu) \right\} .$$

In the following subsections, we prove Lemma 10 by dividing the problem into several cases and derive a concrete formula of $F_{P,Q,s_1,t_1,s_2}$ for each case. Then, since the value of $F_{P,Q,s_1,t_1,s_2}(\nu)$ is computable, we can explicitly show the form of each second-order region.

**C. Second-Order Asymptotics: Non-Extreme Case**

We derive the second-order rate region in the following. To treat the problem, we divide it into some cases as in Fig. 3. We say that a second-order rate pair $(s_2,t_2)$ is $(s_1,t_1,\nu)$-achievable by deterministic conversions or majorization conversions when $(s_2,t_2) \in \mathcal{R}_{P,Q}^{2,D}(s_1,t_1,\nu)$ or $\mathcal{R}_{P,Q}^{2,M}(s_1,t_1,\nu)$.

**Lemma 13:** When $(s_1,t_1)$ is a non-extreme admissible rate pair, the function

$$F_{P,Q,s_1,t_1,s_2}(t_2) = \Phi \left( \frac{H(Q)}{V(Q)} s_1 - H(Q) t_2 \right) \quad (28)$$

is continuous and strictly monotonically decreasing on $F_{P,Q,s_1,t_1,s_2}^{-1}((0,1))$ and satisfies (20), where $V(Q) := \sum_{x \in X} Q(x)(-\log Q(x) - H(Q))^2$,

and $\Phi$ is the cumulative distribution function of the standard normal distribution.

We give the proof of Lemma 13 in Appendix IX-A. When $(s_1,t_1)$ is a non-extreme admissible rate pair, from Theorem 12 and Lemma 13 the second-order rate region is given by

$$\mathcal{R}_{P,Q}^{2,D}(s_1,t_1,\nu) = \mathcal{R}_{P,Q}^{2,M}(s_1,t_1,\nu) \quad (29)$$

and is illustrated as Fig. 3.

**D. Second-Order Asymptotics: Uniform Cases**

The remaining problem is to identify the second-order rate region at the extreme rate pair. Hence, we fix as $s_1 = H(P)$ and $t_1 = \frac{H(P)}{H(Q)}$ and denote as

$$F_{P,Q,s_1,t_1,s_2}(t_2) := F_{P,Q,H(P),H(P),s_1,t_1,s_2}(t_2), \quad (30)$$

$$\mathcal{R}_{P,Q}^{2,i}(\nu) := \mathcal{R}_{P,Q}^{2,i} \left( H(P), H(P), H(Q), \nu \right) . \quad (31)$$

for $i = D$ and $M$ in the following subsections.

When $P$ or $Q$ is a uniform distribution $U_l$ with size $l$, the asymptotics is reduced to the problem of resolvability.
Theorem 12 and Lemma 14, the second-order rate region is obtained as follows.

When \((s_1, t_1)\) is an admissible and non-extreme first-order rate pair.

Fig. 5. The relation between a permissible accuracy and a second-order rate of the number of copies of a target distribution.

Fig. 6. The second-order rate region \(\mathcal{R}_{P,Q}^{2,D}(s_1, t_1, \nu)\) and \(\mathcal{R}_{P,Q}^{2,M}(s_1, t_1, \nu)\) when \((s_2, t_2)\) is an extreme first-order rate pair.

Fig. 7. The second-order rate region \(\mathcal{R}_{P,U_1}^{2,D}(s_1, t_1, \nu)\) and \(\mathcal{R}_{P,U_1}^{2,M}(s_1, t_1, \nu)\) when \((s_2, t_2)\) is an extreme first-order rate pair.

**Lemma 15:** When \(P\) is a non-uniform distribution and \(Q = U_1\), the function

\[
F_{P,U_1,s_2}(t_2) = \Phi \left( \sqrt{\frac{H(Q)}{V(Q) s_1}} s_2 \right)
\]

is continuous and strictly monotonically decreasing on \(F_{P,Q,s_1,t_1,s_2}((0, 1))\) and satisfies (36).

We give the proof of Lemma 15 in Appendix VI-G. When \(Q = U_1\) and \((s_1, t_1)\) is the extreme rate pair \((H(P), B(P))\), from Theorem 12 and Lemma 14 the second-order rate region is given by

\[
\mathcal{R}_{P,U_1}^{2,D}(\nu) = \mathcal{R}_{P,U_1}^{2,M}(\nu)
\]

\[
= \left\{ (s_2, t_2) \mid t_2 \leq \frac{\min \{s_2, 0\} \log l - \sqrt{V(Q) \log l \Phi^{-1}(s_2^2)}}{H(Q)} \right\}
\]

(34)

and is illustrated as Fig. 6.
In later subsections, we treat the case when both \( P \) and \( Q \) are non-uniform distributions and \((s_1,t_1)\) is the extreme rate pair \((H(P),H(Q))\). Then we divide the problem into three cases according to the value
\[
C_{P,Q} := \frac{H(P)}{V(P)} \left( \frac{H(Q)}{V(Q)} \right)^{-1}.
\]
(37)

However, since a certain common structure underlies in those cases, we introduce it in this subsection.

To explain it, we prepare some notations. We define two cumulative normal distributions for non-uniform probability distributions \( P, Q \) and a constant \( t_2 \in \mathbb{R} \) as
\[
\Phi_p(x) := \Phi \left( \frac{x}{\sqrt{\Phi(P)}} \right), \quad \Phi_{P,Q,t_2}(x) := \Phi \left( \frac{x-t_2H(Q)}{\sqrt{\Phi(P)\Phi(Q)}} \right).
\]
(38) (39)

We denote their probability density functions by \( N_P := \frac{d\Phi_p}{dx} \) and \( N_{P,Q,t_2} := \frac{d\Phi_{P,Q,t_2}}{dx} \). Then, we introduce continuous fidelity for probability density functions \( p \) and \( q \) on \( \mathbb{R} \) as
\[
F(p,q) := \int_{\mathbb{R}} \sqrt{p(x)q(x)} \, dx,
\]
(40)

and the maximal fidelity
\[
F_{P,Q,s_2}(t_2) := \max_A F(left(\frac{dA}{dx},N_{P,Q,t_2})right)
\]
(41)

where the maximization is taken over functions \( A \) on \( \mathbb{R} \) satisfying the following conditions:

\begin{enumerate}
  \item Piecewise continuous differentiable.
  \item Monotone increasing.
  \item Inequality constraint: \( \Phi_P \leq A \leq 1 \).
  \item Boundary conditions: \( A(x) = 0, A(s_2) = 1 \).
\end{enumerate}

Here, note that \( \frac{dA}{dx} \) in (41) become probability density functions on \( \mathbb{R} \). Then, the following lemma holds.

**Lemma 16:** For non-uniform distributions \( P \) and \( Q \),
\[
F_{P,Q,s_2}(t_2) \geq F_{P,Q,s_2}(t_2),
\]
(42)

We give the proof of Lemma 16 in Appendix VI-H. Explicitly deriving the function \( A_{s_2,t_2} \) which attains the maximum in RHS of (41) under the conditions (C1)-(C4), the following inequality will be proven in Lemmas 18, 21 and 23 according to the value of \( C_{P,Q} \).
\[
F_{P,Q,s_2}(t_2) \leq F \left( \frac{dA_{s_2,t_2}}{dx},N_{P,Q,t_2} \right) = F_{P,Q,s_2}(t_2).
\]
(43) (44)

Then, we have the equation
\[
F_{P,Q,s_2}(t_2) = F_{P,Q,s_2}(t_2) = F_{P,Q,s_2}(t_2) = F \left( \frac{dA_{s_2,t_2}}{dx},N_{P,Q,t_2} \right)
\]
(45) (46)

from (12), (42) and (43). Since the explicit value of RHS in (46) is given in (49), (55) and (59), we can determine the second-order rate region according to the value of \( C_{P,Q} \).

From Theorem 11 to derive the second-order rate region, we can reduce the problem to the maximization of continuous fidelity with a fixed normal distribution and explicitly calculate the value depending the value of \( C_{P,Q} \).

**F. Second-Order Asymptotics: Non-Uniform Case with \( C_{P,Q} = 1 \)**

To begin with, we treat the case when \( C_{P,Q} = 1 \). We prepare a lemma to derive the maximum fidelity in Lemma 16.

**Lemma 17:** Let \( P \) and \( Q \) be any non-uniform probability distributions on finite sets and \( C_{P,Q} = 1 \). When \( t_2 > 0 \), the equation with respect to \( x \)
\[
\frac{1 - \Phi_P(x)}{\Phi_{P,Q,t_2}(s_2)} - \Phi_{P,Q,t_2}(x) = \frac{N_P(x)}{N_{P,Q,t_2}(x)}
\]
(47)

has the unique solution \( \beta = \beta_{P,Q,s_2,t_2} \).

We give the proof of Lemma 17 in Appendix VI-J. We define the function \( A_{1,s_2,t_2} : \mathbb{R} \rightarrow [0,1] \) as
\[
A_{1,s_2,t_2}(x) = \left\{ \begin{array}{ll}
\frac{\Phi_{P,Q,t_2}(s_2)}{\Phi_P(x)} & \text{if } t_2 \leq 0, x \leq s_2 \\
\Phi_P(x) & \text{if } t_2 > 0, x \leq \beta \\
\Phi_P(\beta) + \frac{N_P(\beta)}{N_{P,Q,t_2}(\beta)} \Phi_{P,Q,t_2}(x) & \text{if } t_2 > 0, \beta \leq x \leq s_2 \\
1 & \text{if } s_2 \leq x.
\end{array} \right.
\]
(48)

and using it, we define the function \( F_{P,Q,s_2} : \mathbb{R} \rightarrow [0,1] \) as
\[
F_{P,Q,s_2}(t_2) = F \left( \frac{dA_{1,s_2,t_2}}{dx},N_{P,Q,t_2} \right)
\]
(49)

Then we have the following lemma, and it implies that \( A_{1,s_2,t_2} \) attains the maximum in (42).

**Lemma 18:** When \( P \) and \( Q \) are non-uniform probability distributions on finite sets with \( C_{P,Q} = 1 \), the function \( F_{P,Q,s_2} \) in (49) is continuous and strictly monotonically decreasing on \( F_{P,Q,s_1,s_2}(0,1) \) and satisfies (26).

We give the proof of Lemma 18 in Appendix VI-K. The positional relation of the functions \( \Phi_P, \Phi_{P,Q,t_2} \) and \( A_{1,s_2,t_2} \) shown in Fig 8. In particular, we have Theorem 11 for \( C_{P,Q} = 1 \). Then, the second-order rate region is illustrated as Fig 9.

As a special case, we consider regenerate a random number from \( P^n \) after compression of a random number from \( P^n \) into storage with size \( 2H(P)n + s_2 \sqrt{n} \). Note that the purpose of the process is not to recover the initial random number but to regenerate a random number form \( P^n \). That is, the process itself differs from the data compression. The process corresponds to the case when \( Q = P \) and \( t_2 = 0 \). Then, the accuracy of regeneration is given by Lemma 16 and 18 and described as follows.

**Corollary 19:** Let \( P \) be any non-uniform probability distribution on a finite set. Then,
\[
F_{P,s_2}(0) = \Phi_P(s_2).
\]
(50)
Lemma 16: Let \( C_{P,Q} = 1 \), \( V(P) = H(Q) = 1 \), \( s_2 = 0.7 \) and \( t_2 = 1 \). The dashed, the normal and the thick lines show \( \Phi_P, \Phi_{P,Q,t_2} \) and \( A_{1,s_2,t_2} \), respectively. The limit of the maximal fidelity in Theorem 18 coincides with the fidelity between \( A_{s_2,t_2} \) and \( N_{P,Q,t_2} \).

Second-Order Asymptotics: Non-Uniform Case with \( C_{P,Q} > 1 \)

Next, we treat the case when \( C_{P,Q} > 1 \). We prepare a lemma to derive the maximum fidelity in Lemma 16.

Lemma 20: Let \( P \) and \( Q \) be any non-uniform probability distributions on finite sets and \( C_{P,Q} > 1 \). The equation with respect to \( x \)

\[
\Phi_P(x) = \frac{N_P(x)}{N_{P,Q,t_2}(x)}
\]

has the unique solution \( \alpha = \alpha_{P,Q,s_2,t_2} \in \mathbb{R} \). Moreover, for \( s_2 > \Phi_P^{-1}(\frac{N_P(x)}{N_{P,Q,t_2}(x)}) \), the equation with respect to \( x \)

\[
1 - \Phi_P(x) \frac{N_P(x)}{N_{P,Q,t_2}(s_2)} = \frac{N_P(x)}{N_{P,Q,t_2}(x)}
\]

has two solutions and only the larger solution \( \beta = \beta_{P,Q,s_2,t_2} \) in two solutions is larger than \( \alpha \).

We give the proof of Lemma 20 in Appendix VI-L. When \( s_2 \leq \Phi_P^{-1}(\frac{N_P(x)}{N_{P,Q,t_2}(x)}) \), we define a function \( A_{s_2,t_2} : \mathbb{R} \rightarrow [0, 1] \) as

\[
A_{s_2,t_2}(x) = \begin{cases} 
\frac{N_P(x)}{N_{P,Q,t_2}(x)} & \text{if } x \leq s_2 \\
1 & \text{if } s_2 \leq x.
\end{cases}
\]

On the other hand, when \( s_2 \geq \Phi_P^{-1}(\frac{N_P(x)}{N_{P,Q,t_2}(x)}) \), we define a function \( A_{s_2,t_2} : \mathbb{R} \rightarrow [0, 1] \) as

\[
A_{s_2,t_2}(x) = \begin{cases} 
\frac{\Phi_P(x)}{\Phi_{P,Q,t_2}(\alpha)} \Phi_{P,Q,t_2}(x) & \text{if } x \leq \alpha \\
\Phi_P(x) & \text{if } \alpha \leq x \leq \beta \\
\Phi_P(\beta) + \frac{N_P(\beta)}{N_{P,Q,t_2}(\beta)} (\Phi_{P,Q,t_2}(x) - \Phi_{P,Q,t_2}(\beta)) & \text{if } \beta \leq x \leq s_2 \\
1 & \text{if } s_2 \leq x.
\end{cases}
\]

and using it, we define the function \( F_{P,Q,s_2} : \mathbb{R} \rightarrow [0, 1] \) as

\[
F_{P,Q,s_2} = \int_{\Phi_{P,Q,s_2}(\alpha)}^{\Phi_{P,Q,s_2}(x)} \frac{N_P(s)}{N_{P,Q,s_2}(s)} ds
\]

where

\[
I_{P,Q,t_2}(x) := \int_{-\infty}^{x} \sqrt{N_P(s) N_{P,Q,t_2}(s)} ds
\]

Then we have the following lemma, and it implies that \( A_{s_2,t_2} \) attains the maximum in (42).

Lemma 21: When \( P \) and \( Q \) are non-uniform probability distributions on finite sets with \( C_{P,Q} > 1 \), the function \( F_{P,Q,s_2} \) in (55) is continuous and strictly monotonically decreasing on \( F_{P,Q,s_2}^{-1}((0,1)) \) and satisfies (26).

We give the proof of Lemma 21 in Appendix VI-M. The positional relation of the functions \( \Phi_P, \Phi_{P,Q,t_2} \) and \( A_{s_2,t_2} \) is shown in Fig. 11. Similarly, the positional relation of the functions \( \Phi_P, \Phi_{P,Q,t_2} \) and \( A_{s_2,t_2} \) is shown in Fig. 11. In particular, we have Theorem 11 for \( C_{P,Q} > 1 \). Then, the second-order rate region is illustrated as Fig. 12.

Second-Order Asymptotics: Non-Uniform Case with \( C_{P,Q} < 1 \)

Next, we treat the case when \( C_{P,Q} < 1 \). We prepare a lemma to derive the maximum fidelity in Lemma 16.
Lemma 22: Let $P$ and $Q$ be any non-uniform probability distributions on a finite set and $C_{P,Q} < 1$. Then, the equation with respect to $x$

$$1 - \Phi_P(x) = \frac{N_P(x)}{N_{P,Q,t_2}(x)} \quad (57)$$

has the unique solution $\beta = \beta_{P,Q,s_2,t_2} \in \mathbb{R}$.

We give the proof of Lemma 22 in Appendix VI-N. Note that the solutions of the equation (52) and (57) do not coincide with each other because the relation between $H(P)$ and $H(Q)$ is different in those equations.

Then, we define a function $A_{s_2,t_2}: \mathbb{R} \to [0, 1]$ as

$$A_{s_2,t_2}(x) = \begin{cases} 
\Phi_P(x) & \text{if } x \leq \beta \\
\Phi_P(\beta) + \frac{N_P(\beta)}{N_{P,Q,t_2}(\beta)}(\Phi_P(x) - \Phi_P(t_2(\beta))) & \text{if } \beta \leq x \leq s_2 \\
1 & \text{if } s_2 \leq x,
\end{cases} \quad (58)$$

and using it, we define the function $F_{P,Q,s_2}: \mathbb{R} \to [0, 1]$ as

$$F_{P,Q,s_2}(t_2) = F\left(\frac{dA_{s_2,t_2}}{dx}, N_{P,Q,t_2}\right)$$

$$= I_{P,Q,t_2}(\beta) + \sqrt{1 - \Phi_P(\beta)} \sqrt{\Phi_P(x) - \Phi_P(t_2(\beta))}(59)$$

Then we have the following lemma, and it implies that $A_{s_2,t_2}$ attains the maximum in (42).

Lemma 23: When $P$ and $Q$ are non-uniform probability distributions on finite sets with $C_{P,Q} < 1$, the function $F_{P,Q,s_2}$ in (59) is continuous and strictly monotonically decreasing on $F_{P,Q,s_1,t_2}(0, 1))$ and satisfies (20).

We give the proof of Lemma 23 in Appendix VI-L. In particular, we have Theorem 11 for $C_{P,Q} < 1$. Then, the second-order rate region is illustrated as Fig. 14.

IV. RELATION WITH CONVENTIONAL RNC

We have treated RNC via restricted storage. On the other hand, in the previous paper [11], we treated random number
conversion without restriction of storage. Here, it is expected that the results in this paper approach to that in the previous paper as the size of storage gets larger. In the following, we describe it by asymptotic maximum fidelity of RNC.

When the first-order rate of the size of storage is the entropy of the source distribution, asymptotic maximal fidelity in RNC with restricted storage is given as

\[ F_{P,Q,s_2}(t_2) = F_{P,Q}^D(s_2,t_2) = F_{P,Q}^M(s_2,t_2). \]  (60)

On the other hand, asymptotic maximal fidelity in RNC without restricted storage is given as follows shown in [11]

\[
F_{P,Q}(t_2) := \lim_{n \to \infty} F^D(P^n \to Q^{\frac{H(P)}{\log_2 n}n + t_2 \sqrt{n} \log_2 n})
= \lim_{n \to \infty} F^M(P^n \to Q^{\frac{H(P)}{\log_2 n}n + t_2 \sqrt{n} \log_2 n}). \]  (61)

Then, the following proposition holds.

**Proposition 24:**

\[ \lim_{s_2 \to \infty} F_{P,Q,s_2}(t_2) = F_{P,Q}(t_2). \]  (62)

We give the proof of Proposition 24 in Appendix VI-P. Fig. 15 represents the graph of the ratio \( F_{P,Q,s_2}(t_2)/F_{P,Q}(t_2) \) with respect to \( s_2 \in \mathbb{R} \) when \( C_{P,Q} = 1 \). We can read off that the value of \( F_{P,Q,s_2}(t_2) \) converges to that of \( F_{P,Q}(t_2) \) for each \( t_2 \in \mathbb{R} \) when \( s_2 \) goes to infinity. From Proposition 24, the existence of storage does not affect the accuracy (i.e. the asymptotic maximum fidelity) of RNC via restricted storage as long as the second-order rate is large enough even when the first-order rate strictly achieves the optimal value. In particular, when \( s_2 \) tends to infinity, the second order asymptotic expansion in Theorem 11 recovers Theorem 3 of [11] for RNC without restricted storage.

**V. APPLICATION TO QUANTUM INFORMATION THEORY**

In this section, we provide an application of RNC via restricted storage for quantum information theory.

**A. LOCC Conversion via Restricted Storage**

When two distant parties perform some quantum protocol using a specific suitable entangled state (e.g. quantum teleportation, superdense coding, channel estimation), those parties need to prepare the entangled state. Then, they virtually have entanglement storage with finite size to temporarily preserve entangled states. Here, we consider the situation that they convert an entangled state into the storage and produce the desired entangled state from the converted state after decision of a quantum protocol performed. Since two parties are distant form each other, quantum operations which they can perform are limited to LOCC. We call such a procedure LOCC conversion via restricted storage and it consists of two parts as follows. In the first part, an initial state is converted into the storage by LOCC. In the second part, the converted state is converted again to approximate a target state by LOCC.

In the following, we assume that a initial state and a target state are pure and i.i.d. states with the form \( \psi^\otimes n \) and \( \phi^{\otimes t_1 + t_2 \sqrt{n}} \). Besides, we assume that the dimension of state system has the fixed first order coefficient \( s_1 = S_\psi \) as \( 2^{S_\psi + s_2 \sqrt{n}} \), where, for a bipartite system \( \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \), we define the dimension \( d(\mathcal{H}) \) by \( \min \dim \mathcal{H}_i \). Because, if the fixed first order rate \( s_1 \) is strictly larger than \( S_\psi \), the initial state \( \psi^\otimes n \) can be recovered from the converted state under the condition that the error asymptotically goes to 0 by LOCC. Thus, the conversion problem with storage is reduced to the direct conversion from \( \psi^\otimes n \) to \( \phi^{\otimes t_1 + t_2 \sqrt{n}} \). On the other hand, if the fixed first order coefficient is strictly less than \( S_\psi \), \( \psi^\otimes n \) can be converted to the maximally entangled state \( \phi^\otimes t_1 + t_2 \sqrt{n} \) for any \( s_2 \) by LOCC. Since an arbitrary state on a bipartite system \( \mathcal{H} \) is converted from the maximally entangled state with the size \( d(\mathcal{H}) \) by LOCC, the conversion problem with storage is reduced to the direct conversion from the maximally entangled state to \( \phi^\otimes t_1 + t_2 \sqrt{n} \). Second-order asymptotics for direct conversion of LOCC including entanglement concentration was already discussed in [11].

To treat the rate of LOCC conversion via restricted storage,
we first introduce its accuracy defined by fidelity $F$ as follows

$$F^Q(\psi \to \phi | N) := \max \left\{ F(\Gamma' \circ \Gamma(\psi), \phi) : \Gamma : \mathcal{H} \to (\mathbb{C}^N)^{\otimes 2}, \Gamma' : (\mathbb{C}^N)^{\otimes 2} \to \mathcal{H}' \right\},$$

where $\psi$ and $\phi$ are quantum states on bipartite systems $\mathcal{H}$ and $\mathcal{H}'$ respectively, and the maximum is taken over pairs $(\Gamma, \Gamma')$ of LOCC conversions. Then, the following lemma holds.

**Lemma 25:**

$$F^Q(\psi \to \phi | N) = F^{\mathcal{M}}(P_{\psi} \to P_{\phi} | N) \quad (63)$$

We give the proof of Lemma 25 in Appendix VI-Q. Here, we note that a converted state by LOCC in storage is not necessarily a pure state. However, in the optimal process, we can assume that the converted state by LOCC in storage is pure from the proof of Lemma 25.

Here, we define the asymptotic behavior of the maximal recovery number by LOCC as

$$L_n(\psi, \phi | \nu, s_2) := \max_{\Gamma_1, \Gamma_2: \text{LOCC}} \left\{ M : \mathbb{N} | F(\Gamma_2 \circ \Gamma_1(\psi^{\otimes n}), \phi^{\otimes M}) \geq \nu \right\}$$

where $\Gamma_1 : \mathcal{S}(\mathcal{H}_{AB}^{\otimes n}) \to \mathcal{S}(\mathcal{H}_n)$ and $\Gamma_2 : \mathcal{S}(\mathcal{H}_n) \to \mathcal{S}(\mathcal{H}_{AB}^{\otimes M})$ are LOCC, and $d(\mathcal{H}_n) = 2^{S_n + \nu s_2 \sqrt{\pi}}$. Then, the following second-order asymptotic expansion holds from Lemma 25 and Theorem 11.

**Theorem 26:**

$$L_n(\psi, \phi | \nu, s_2) \approx \frac{S_{\psi} + F^{-1}_{P_{\psi},P_{\phi},s_2}(\nu) \sqrt{n}}{S_{\phi}}. \quad (64)$$

Moreover, the concrete form of $F_{P_{\psi},P_{\phi},s_2}$ is given by the results of Section III.

For simplicity, we employ the following abbreviate notation:

$$F^Q_{\psi,\phi,s_1,t_1,t_2}(t_2) := \liminf_{n \to \infty} F^Q(\psi^{\otimes n} \to \phi^{\otimes n + t_2}, \sqrt{2^{S_1 + t_2 \sqrt{\pi}}}).$$

In order to treat the asymptotic relation between the second-order rates of storage and target entangled state, we define the rate region as follows.

**Definition 27:**

$$\mathcal{R}^2_{\psi,\phi}(s_1,t_1,\nu) := \left\{ (s_2,t_2) : F^Q_{\psi,\phi,s_1,t_1,t_2}(t_2) \geq \nu \right\}.$$

Then, Lemma 25 and Theorem 12 implies the following theorem about second-order rate regions.

**Theorem 28:** Let $\psi$ and $\phi$ be pure entangled states on finite dimensional bipartite quantum systems. For $0 < s_1 \leq S_{\psi}$, $s_2 \in \mathbb{R}$ and $\nu \in (0, 1)$,

$$\mathcal{R}^2_{\psi,\phi}(s_1,s_2,\nu) = \left\{ (s_2,t_2) : t_2 \leq F^Q_{\psi,\phi,s_1,s_2}(\nu) \right\}.$$

**B. Entangled State Compression by LOCC**

In particular, when $\phi = \psi$, LOCC conversion via restricted entanglement storage is regarded as a compression process for entangled states. There already exist some studies about LOCC compression for entangled states. In particular, Schumacher [17] derived the optimal first-order rate of LOCC compression for entangled states in the framework of the first-order asymptotics. However, those have not treated the second-order asymptotics and thus the accuracy (or the success probability) of optimal LOCC compression. When the size (i.e. dimension) of storage has the optimal first-order compression rate $S_{\psi}$, the difference of the number of copies between the initial state and the recovered state is described with respect to the second-order rate $s_2$ of the size of storage as

$$n - L_n(\psi, \psi | \nu, s_2) \approx -F^{-1}_{P_{\psi},P_{\phi},s_2}(\nu) \sqrt{n}, \quad (65)$$

where the concrete form of $F_{P_{\psi},P_{\phi},s_2}$ was given in [49]. The formula (65) relates with the irreversibility of entanglement concentration [10]. That is, when $s_2$ is smaller than $\Phi^{-1}_{P_{\psi}^1}(\nu^2)$ for a required accuracy $\nu$, RHS in (65) is positive from Corollary 19 and represents the loss which inevitably occurs even in the optimal compression process. Moreover, from Lemma 1 and the proof of Lemma 25, LOCC conversion in the optimal compression coincides with LOCC conversion used in the optimal entanglement concentration. In addition, (65) also relates with LOCC cloning [11]. That is, when $s_2$ is larger than $\Phi^{-1}_{P_{\psi}^1}(\nu^2)$, RHS in (65) is negative from Corollary 19 and it represents that the number of copies of the recovered state after the compression process exceeds that of the initial state under the accuracy constraint. While we argued about approximate LOCC cloning without entanglement storage (or with infinite storage) in [11], the above fact says that approximate LOCC cloning can be realized even when there is entanglement storage with the tight first-order rate $S_{\psi}$ as long as the second-order rate of the size of storage is large enough.
VI. PROOFS OF THEOREMS, PROPOSITIONS AND LEMMAS

A. Proof of Lemma 2

Let $P' = (P'(L), ..., P'(L))$ be an arbitrary probability distribution such that $P < P'$. To prove Lemma 2 it is enough to prove that $P_k < P'$. Here, we use the inductive method. When $L = 1$, then Lemma 2 obviously holds for any probability distribution $P$. Let us assume that Lemma 2 holds for any $P$ when $L = k - 1$. In the following, we show that Lemma 2 holds for any $P$ when $L = k$. When $J_{P,k} = 1$, $P_L$ equals $U_i$ and satisfies $P_k = U_k < P$. Let $J_{P,k} \geq 2$ in the following. Then, $P_k(1) = P(1)$.

When $P'(1) = P(1)$, $P'|_{(2,...,|X|)} < P'|_{(2,...,L)}$ holds since $P < P'$. By the assumption of the inductive method, $\frac{1}{C}P_k|_{(2,...,|X|)} < \frac{1}{C}P|_{(2,...,L)}$, where $C = \sum |X| P_k(i)$ and $C' = \sum |X| P'(i)$ are normalizing constants. Thus, it follows that $P_k(1) = P(1)$.

When $P'(1) > P(1)$, let $l_0 := \arg\max\{l \in \{1, ..., L\} | P'(1) = P'(l)\}$ and $\omega := \sum_{i=1}^{l_0} (P'(l) - P(1))$. Moreover, we define the set $K$ by $\{l \in \{1, ..., L\} | P'(l) < P(l)\} = \{l_i, ..., l_{m}\}$ where $l_i \leq l_{i+1}$ and determine $r_0 \in K$ by the condition

$$\sum_{i=1}^{r_0-1} (P(l_i) - P'(l_i)) < \omega \leq \sum_{i=1}^{r_0} (P(l_i) - P'(l_i)).$$

By using those notations, we set a probability distribution $Q'$ by

$$Q'(l) = \begin{cases} P(1) & \text{if } 1 \leq l \leq l_0 \\ P(l) - \epsilon & \text{if } l = l_1, ..., l_{r_0-1} \\ P'(l_{r_0}) + \omega - \sum_{i=1}^{l_0} (P(l_i) - P'(l_i)) & \text{if } l = l_{r_0} \\ P'(l) & \text{otherwise}. \end{cases}$$

Then, $Q'$ satisfies $P < Q' < P'$ and $Q'(1) = P(1)$. As the same way as the case $P'(1) = P(1)$, $P_k < Q'$ holds. Since $Q' < P'$, $P_k < P'$ is derived.

B. Proof of Proposition 3

Let $m \geq n$. Then, the size of storage is greater than or equal to the size of support of the source distribution $U_i^n$, and thus the performances of deterministic (or majorization) conversions via storage and that without storage coincide with each other. Thus, we have

$$L_n^D(U_i, Q|\nu, l^m) = L_n^D(U_i, Q|\nu),$$

$$L_n^M(U_i, Q|\nu, l^m) = L_n^M(U_i, Q|\nu).$$

Next, let $m \leq n$. Then, $U_i^n$ on the storage with size $l^m$ can be converted from $U_i^n$ by deterministic and majorization conversion. Thus, we have

$$L_n^D(U_i, Q|\nu, l^m) \geq L_m^D(U_i, Q|\nu),$$

$$L_n^M(U_i, Q|\nu, l^m) \geq L_m^M(U_i, Q|\nu).$$

Moreover, since any probability distribution on a set with size $l^m$ can be converted from $U_i^n$ by majorization conversion. Therefore we have

$$L_n^M(U_i, Q|\nu, l^m) \leq L_m^M(U_i, Q|\nu).$$

C. Proof of Proposition 2

When $m \geq L_n^P(P, U_i|\nu)$, the equation

$$L_n^P(P, U_i|\nu, l^m) = L_n^P(P, U_i|\nu)$$

obviously holds by the definition. Similarly, when $m \geq L_n^M(P, U_i|\nu)$,

$$L_n^M(P, U_i|\nu, l^m) = L_n^M(P, U_i|\nu)$$

obviously holds by the definition.

Let $m \leq L_n^M(P, U_i|\nu)$. Since any probability distribution on a set with size $l^m$ can be converted from $U_i^n$ by majorization conversion, we obtain

$$L_n^M(P, U_i|\nu, l^m) \leq L_n^M(U_i^n, U_i|\nu) \leq m - 2 \log_2 \nu.$$  (75)

Moreover, when $m \leq L_n^P(P, U_i|\nu)$, from $L_n^P(P, U_i|\nu) \leq L_n^M(P, U_i|\nu)$, we have $m \leq L_n^M(P, U_i|\nu)$.

Thus,

$$L_n^P(P, U_i|\nu, l^m) \leq L_n^M(P, U_i|\nu, l^m) \leq m - 2 \log_2 \nu.$$  (76)

D. Proof of Theorem 6

First, we prove the direct part. Let $s_1 \geq H(P)$. From the results about the asymptotic maximal fidelity in [11], when $\epsilon$ is in $(0, 1/2)$,

$$\lim_{n \to \infty} F^n (P^n \to Q^n_H(P^n, n^{-1/2+\epsilon}) | s_1^n) = 1.$$  

Next, let $s_1 < H(P)$. Then,

$$\lim_{n \to \infty} F^n (P^n \to Q^n_H(P^n, n^{-1/2+\epsilon}) | s_1^n) = 0.$$  

Thus, a first-order achievable rate $t_1$ satisfies $t_1 \geq \frac{H(P)}{\pi(\epsilon)}$. Then, we prove the converse part. Let $s_1 \geq H(P)$. From the results about the asymptotic maximal fidelity in [11], when $\epsilon$ is in $(0, 1/2)$,

$$\lim_{n \to \infty} F^n (P^n \to Q^n_H(P^n, n^{-1/2+\epsilon}) | s_1^n) = 0.$$  

Next, let $s_1 < H(P)$. Then,

$$\lim_{n \to \infty} F^n (P^n \to Q^n_H(P^n, n^{-1/2+\epsilon}) | s_1^n) = 0.$$  

Thus, a first-order achievable rate $t_1$ satisfies $t_1 \leq \frac{H(P)}{\pi(\epsilon)}$.  

\[ \]
E. Proof of Lemma 13

The function $F_{P,Q,s_1,n,\frac{1}{\log t},s_2}$ in (28) is obviously continuous and strictly monotonically decreasing on $F_{P,Q,s_1,n,\frac{1}{\log t},s_2}((0,1))$.

We first prove the direct part. Since $s_1 < H(P)$, the initial distribution can be converted to the uniform distribution with size $2^{s_1 n}$ under the condition that asymptotic fidelity is 1 [11]. Thus, we have

$$F_{P,Q,s_1,n,\frac{1}{\log t},s_2}^D(t_2) \geq F^D(U_2^{s_1 n} \rightarrow Q^{\frac{1}{\log t} n + t_2 \sqrt{n}}) = F_{P,Q,s_1,n,\frac{1}{\log t},s_2}^D(t_2).$$

Next, we first prove the converse part. Since an arbitrary probability distribution on $\mathbb{N}_{2^{s_1 n}}$ can be converted from the uniform distribution with size $2^{s_1 n}$ by majorization conversion. Thus, we have

$$F_{P,Q,s_1,n,\frac{1}{\log t},s_2}^M(t_2) \leq F^M(U_2^{s_1 n} \rightarrow Q^{\frac{1}{\log t} n + t_2 \sqrt{n}}) = F_{P,Q,s_1,n,\frac{1}{\log t},s_2}^M(t_2).$$

From [11], [71] and [78], we obtain (26). ■

F. Proof of Lemma 14

The function $F_{U_1,Q,s_2}$ in (33) is obviously continuous and strictly monotonically decreasing on $F_{U_1,Q,s_2}((0,1))$.

We first prove the direct part. Let $s_2 \geq 0$. Since the size of storage is greater than the size of support of $U_1^n$, $U_1^n$ can be converted to $U_1^n$ itself in storage. Thus, we have

$$F_{U_1,Q,s_2}^D(t_2) \geq F^D(U_1^n \rightarrow Q^{\frac{1}{\log t} n + t_2 \sqrt{n}}) = F_{U_1,Q,s_2}^D(t_2).$$

Next, let $s_2 < 0$. $U_1^n$ can be converted to $U_2^{(\log t)n + s_2 \sqrt{n}}$ under the condition that asymptotic fidelity is 1. Thus, we have

$$F_{U_1,Q,s_2}^D(t_2) \geq F^D(U_2^{(\log t)n + s_2 \sqrt{n}} \rightarrow Q^{\frac{1}{\log t} n + t_2 \sqrt{n}}) = F_{U_1,Q,s_2}^D(t_2).$$

Then, we prove the converse part. Let $s_2 \geq 0$. Then, the following inequality obviously holds

$$F_{U_1,Q,s_2}^M(t_2) \leq F^M(U_1^n \rightarrow Q^{\frac{1}{\log t} n + t_2 \sqrt{n}}) = F_{U_1,Q,s_2}^M(t_2).$$

Next, let $s_2 < 0$. Since an arbitrary probability distribution on $\mathbb{N}_{(\log t)n + s_2 \sqrt{n}}$ can be converted from the uniform distribution with size $2^{(\log t)n + s_2 \sqrt{n}}$ by majorization conversion. Thus, we have

$$F_{U_1,Q,s_2}^M(t_2) \leq F^M(U_2^{(\log t)n + s_2 \sqrt{n}} \rightarrow Q^{\frac{1}{\log t} n + t_2 \sqrt{n}}) = F_{U_1,Q,s_2}^M(t_2).$$

From [11], [71], [80], [81] and [82], we obtain (26). ■

G. Proof of Lemma 15

The function $F_{P,U_1,s_2}$ in (35) is obviously continuous and strictly monotonically decreasing on $F_{P,U_1,s_2}((0,1))$.

We first prove the direct part. Let $(\log t)t_2 \leq s_2$. Since the size of storage is greater than the size of support of $U_1^{\frac{H(P)}{\log t} n + t_2 \sqrt{n}}$, we do not have to care the existence of storage and have

$$F_{P,U_1,s_2}^D(t_2) \leq F^D(P^n \rightarrow U_1^{\frac{H(P)}{\log t} n + t_2 \sqrt{n}}) = F^D(P^n \rightarrow U_2^{H(P)n + (\log l)t_2 \sqrt{n}}) = F_{P,U_1,s_2}. \quad (83)$$

When $(\log l)t_2 > s_2$, the direct part is obvious. Next, we prove the converse part. Let $(\log l)t_2 \leq s_2$. Then, the following inequality obviously holds

$$F_{P,U_1,s_2}^M(t_2) \leq F^M(P^n \rightarrow U_1^{\frac{H(P)}{\log t} n + t_2 \sqrt{n}}) = F^D(P^n \rightarrow U_2^{H(P)n + (\log l)t_2 \sqrt{n}}) = F_{P,U_1,s_2}. \quad (84)$$

Let $(\log l)t_2 > s_2$. Since an arbitrary probability distribution on $\mathbb{N}_{\frac{H(P)}{\log t} n + t_2 \sqrt{n}}$ can be converted from the uniform distribution with size $2^{\frac{H(P)}{\log t} n + s_2 \sqrt{n}}$ by majorization conversion. Thus, we have

$$F_{P,U_1,s_2}^M(t_2) \leq F^M(U_2^{(\log l)n + s_2 \sqrt{n}} \rightarrow U_2^{H(P)n + (\log l)t_2 \sqrt{n}}) = F_{P,U_1,s_2}. \quad (85)$$

From [11], [83], [84] and [85], we obtain (26). ■

H. Proof of Lemma 16

We also consider the following condition (C1’) Continuous differentiable.

That is, a function satisfying (C1’) is differentiable all over $\mathbb{R}$ unlike (C1). Let $\epsilon > 0$ and $t_2 \in \mathbb{R}$. When a function $A : \mathbb{R} \rightarrow [0,1]$ satisfies (C1), (C2), (C3) and (C4), there exists a function $A’ : \mathbb{R} \rightarrow [0,1]$ such that $A'$ satisfies (C1’), (C2), (C3), (C4) and

$$F \left( \frac{dA}{dx}N_{P,Q,t_2} \right) \geq F \left( \frac{dA}{dx}N_{P,Q,t_2} \right) - \epsilon. \quad (86)$$

From the proof of Lemma 9 in [11], there exists a sequence of deterministic maps $W_n$ such that

$$\liminf_{n \rightarrow \infty} F(W_n(P^\frac{1}{n}), Q^{\frac{H(P)}{\log t} n + t_2 \sqrt{n}}) \geq F \left( \frac{dA}{dx}N_{P,Q,t_2} \right) - \epsilon. \quad (87)$$

Moreover, from the condition $A’(s_2) = 1$ in (C4), we can take $W_n$ as a deterministic map such that the size of image of $W_n$ is less than $2^{\frac{H(P)}{\log t} n + s_2 \sqrt{n}}$. Thus,

$$F_{P,Q,s_2}^D(t_2) \geq \liminf_{n \rightarrow \infty} F(W_n(P^\frac{1}{n}), Q^{\frac{H(P)}{\log t} n + t_2 \sqrt{n}}) \geq F \left( \frac{dA}{dx}N_{P,Q,t_2} \right) - \epsilon. \quad (88)$$
Since $\epsilon > 0$ is arbitrary, the proof is completed. \hfill \blacksquare

I. Lemmas for Converse Part

To prove the converse part of later lemmas, we prepare two lemmas. The following lemma is given as Lemma 25 of [11].

**Lemma 29:** Let $a = \{a_i\}_{i=0}^{n} = \{b_i\}_{i=0}^{n}$ be probability distributions and satisfy $\sum \frac{a_i}{b_i} > 0$. When $c = \{c_i\}_{i=0}^{n}$ is a probability distribution and satisfies

$$
\sum_{i=0}^{k} a_i \leq \sum_{i=0}^{k} c_i \quad (k = 0, 1, ..., I)
$$

(89)

the following holds:

$$
\sum_{i=0}^{I} \sqrt{a_i} \sqrt{b_i} \geq \sum_{i=0}^{I} \sqrt{c_i} \sqrt{b_i}.
$$

(90)

Moreover, the equation holds for $c$ if and only if $c = a$.

The following is a modified version of Lemma 26 of [11].

**Lemma 30:** Assume that real numbers $v \leq v'$ satisfy the following condition (\ast).

\(\ast\) There exist $u$ and $u'$ which satisfy the following three conditions:

(I) $u \leq v \leq v' \leq u'$ and $v' \leq s_2$,

(II) $\Phi_P(v) = \frac{N_P(u)}{N_P(u')}$ and

$$
\frac{1 - \Phi_P(v')}{\Phi_P(u') - \Phi_P(u')} = \frac{N_P(u')}{N_P(u)}.
$$

(91)

(III) $N_P(x)$ is monotonically decreasing on $(u, u')$.

Then the following inequality holds

$$
F_{P,Q,s_2}(t_2) \leq \sqrt{\Phi_P(v)\Phi_P(u')} + \int_{v}^{v'} \sqrt{N_P(x)} \sqrt{N_P(u') - N_P(v')} dx
$$

+ $\sqrt{1 - \Phi_P(v')} \Phi_P(u') - \Phi_P(u')$.

(92)

**Proof:** We set as

$$
S_P^n(x) := \{1, 2, ..., [2^{H(P) + x/\sqrt{n}}]\}
$$

$$
S_P^n(x, x') := S_P^n(x') \setminus S_P^n(x).
$$

Let $P_n'$ be a probability distribution on $S_P^n(x)$ such that $P_n' > P_n$. When we set a sequence $\{x_i\}_{i=0}^{n}$ as $x_i := v + \frac{\sqrt{n}}{i}$, we have the following by the monotonicity of the fidelity

$$
F(P_n', P_n) \leq \sqrt{\frac{H(P) + x/\sqrt{n}}{\frac{H(P) + x/\sqrt{n}}{2}}} \sqrt{\frac{H(P) + x/\sqrt{n}}{2}}
$$

+ $\sum_{i=0}^{k} \sqrt{P_n'(S_{n}(x_{i-1}, x_i))} \sqrt{H(P) + x/\sqrt{n}} \sqrt{S_{n}(x_{i-1}, x_i)}$

$$
\times \sqrt{\frac{H(P) + x/\sqrt{n}}{2}} \sqrt{\frac{H(P) + x/\sqrt{n}}{2}} \sqrt{S_{n}(x_i)}
$$

$$
+ \sqrt{1 - P_n'(S_{n}(s_2))} \sqrt{1 - \frac{H(P) + x/\sqrt{n}}{2}} \sqrt{S_{n}(s_2)}
$$

(93)

Here, we denote the right hand side of (93) by $R_I(n)$. Then, we can choose a subsequence $\{n_i\} \subset \{n\}$ such that

$$
\lim_{l \to \infty} R_I(n_l) = \lim_{n \to \infty} R_I(n)
$$

and the limits

$$
c_0 := \lim_{l \to \infty} P_{n_l}'(S_{n_l}(x_0'))
$$

$$
c_1 := \lim_{l \to \infty} P_{n_l}'(S_{n_l}(x_{l-1}', x_l'))
$$

$$
c_{I+1} := \lim_{l \to \infty} \{P_{n_l}'(S_{n_l}(s_2')) - P_{n_l}'(S_{n_l}(x_l'))\}
$$

$$
c_{I+2} := 0
$$

exist for $i = 1, ..., I$. Hence, we obtain

$$
\lim \sup_{n \to \infty} F(P_n', Q_n) \leq \lim \sup_{n \to \infty} R_I(n)
$$

$$
= \sqrt{c_0} \sqrt{\Phi_P(x_0')}
$$

+ $\sum_{i=1}^{I} \sqrt{c_i} \sqrt{\Phi_P(x_i') - \Phi_P(x_{i-1}')}$

$$
+ \sqrt{c_{I+2}} \sqrt{\Phi_P(s_2') - \Phi_P(x_1')},
$$

(94)

where we used Lemma 22 of [11] in the last equality. When we set as

$$
a_0 := \Phi_P(x_0')
$$

$$
a_1 := \Phi_P(x_1') - \Phi_P(x_{i-1}')
$$

$$
a_{I+1} := 1 - \Phi_P(x_I')
$$

$$
a_{I+2} := 0
$$

$$
b_0 := \Phi_P(x_0')
$$

$$
b_i := \Phi_P(x_i') - \Phi_P(x_{i-1}')
$$

$$
b_{I+1} := \Phi_P(s_2') - \Phi_P(x_1')
$$

$$
b_{I+2} := 0
$$

for 1, ..., I, those satisfy the assumptions of Lemma 29 as follows. First, $a_0/b_0 = N_P(u)/N_P(u)$ and $a_{I+1}/b_{I+1} = N_P(u')/N_P(u')$ hold by the assumption (II). Moreover, there exist $z_i \in [x_{i-1}', x_i']$ for $i = 1, ..., I$ such that $a_i/b_i = N_P(z_i)/N_P(z_i)$ for $i = 1, ..., I$ due to the mean value theorem. Then $z_i \in (u, u')$ holds because of the condition $v = x_i' \leq x_{i-1}' \leq z_i \leq x_i' \leq x'_l = v'$ and the assumption (I). Since $N_P(x) / N_P(Q_n(x))$ is monotonically decreasing on $(u, u')$ by the assumption (III), we have $a_i/b_i \geq a_i/b_i$ for $i = 1, ..., I + 1$. Moreover,

$$
\sum_{i=0}^{k} a_i = \Phi(x_k')
$$

$$
= \lim_{l \to \infty} P_n'(S_{n_l}(x_k'))
$$

$$
\leq \lim_{l \to \infty} P_{n_l}'(S_{n_l}(x_k'))
$$

$$
= \sum_{i=0}^{k} c_i
$$

(95)
holds for $k = 0, 1, \ldots, I$ since $P^n < P'_n$, and $\sum_{i=0}^{I+1} a_i = 1 = \sum_{i=0}^{I+1} c_i$ holds.

From the above discussion, we can use Lemma 29. Therefore, the following hold:

$$
\limsup_{n \to \infty} F(P_n^{I_1}, Q_n^{I_1}) \\
\leq \sqrt{c_0} \frac{1}{\Phi_{P,Q,b}(x_i^1)} \\
+ \sum_{i=1}^{I} \sqrt{c_i} \frac{1}{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
+ \sqrt{c_0} \frac{1}{\Phi_{P,Q,b}(s_2) - \Phi_{P,Q,b}(x_i^1)} \\
\leq \frac{\Phi_P(v)}{\sqrt{\Phi_{P,Q,b}(v)}} \\
+ \sum_{i=1}^{I} \frac{\Phi_P(x_i^1) - \Phi_P(x_i^1)}{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
\times \sqrt{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
+ \sqrt{1 - \Phi_P(v')} \frac{1}{\Phi_{P,Q,b}(s_2) - \Phi_{P,Q,b}(v')} \\
= \int_{v'} \sqrt{N_P(x)} \sqrt{N_{P,Q,b}(x)} dx,
$$

where we used $x_i^1 = v$ and $x_i^1 = v'$. Since

$$
\lim_{l \to \infty} \sum_{i=1}^{I} \frac{\Phi_P(x_i^1) - \Phi_P(x_i^1)}{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
\times \sqrt{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
\times \sqrt{1 - \Phi_P(v')} \frac{1}{\Phi_{P,Q,b}(s_2) - \Phi_{P,Q,b}(v')} \\
= \int_{v'} \sqrt{N_P(x)} \sqrt{N_{P,Q,b}(x)} dx,
$$

we obtain

$$
\limsup_{n \to \infty} F(P_n^{I_1}, Q_n^{I_1}) \\
\leq \sqrt{c_0} \frac{1}{\Phi_{P,Q,b}(x_i^1)} \\
+ \sum_{i=1}^{I} \sqrt{c_i} \frac{1}{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
+ \sqrt{c_0} \frac{1}{\Phi_{P,Q,b}(s_2) - \Phi_{P,Q,b}(x_i^1)} \\
\leq \frac{\Phi_P(v)}{\sqrt{\Phi_{P,Q,b}(v)}} \\
+ \sum_{i=1}^{I} \frac{\Phi_P(x_i^1) - \Phi_P(x_i^1)}{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
\times \sqrt{\Phi_{P,Q,b}(x_i^1) - \Phi_{P,Q,b}(x_i^1)} \\
+ \sqrt{1 - \Phi_P(v')} \frac{1}{\Phi_{P,Q,b}(s_2) - \Phi_{P,Q,b}(v')}.
$$

J. Proof of Lemma 17

Here, the existence of the solution is equivalent to the existence of the zero point of the function

$$
f(x) := \Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(x) \\
- (1 - \Phi_P(x)) \frac{N_{P,Q,t_2}(x)}{N_P(x)}. \tag{97}
$$

Since

$$
\frac{df}{dx}(x) = - \frac{d}{dx} \left( \frac{N_{P,Q,t_2}}{N_P} \right)(x)(1 - \Phi_P(x)) \\
= - \frac{iH(Q)}{V(P)} \exp \left( \frac{iH(Q)x - (iH(Q))^2}{V(P)} \right)
$$

the function $f$ is strictly monotonically decreasing. Moreover, since

$$
\lim_{x \to -\infty} f(x) = \Phi_{P,Q,t_2}(s_2) > 0, \\
\lim_{x \to s_2} f(x) = -(1 - \Phi_P(s_2)) \frac{N_{P,Q,t_2}}{N_P}(s_2) < 0.
$$

Thus, the function $f$ has the unique zero point $\beta$ due to the intermediate value theorem.

K. Proof of Lemma 18

Since the direct part is given by Lemma 16 we prove the converse part.

First, we treat the case when $t_2 \leq 0$. From (8),

$$
F_{P,Q,s_2}(t_2) \leq \liminf_{n \to \infty} \frac{Q(P,Q,s_2) - \sqrt{M(P)}}{\sqrt{P(Q,s_2)}},
$$

where we used Lemma 22 of (11) in the last equality.

Next, we treat the case when $t_2 > 0$. Here, we use Lemma 30. For any $v \in \mathbb{R}$, the existence of $u$ such that $u \leq v$ and

$$
\frac{\Phi_P(v)}{\Phi_{P,Q,t_2}(v)} = \frac{N_P(u)}{N_{P,Q,t_2}(u)}, \tag{98}
$$

can be easily verified by the mean value theorem as was shown in the proof of Lemma 11 of (11). Moreover, when we take as $u' = v' = \beta$, then $\beta \leq s_2$ and

$$
\frac{1}{\Phi_{P,Q,t_2}(s_2)} - \frac{1}{\Phi_{P,Q,t_2}(\beta)} = \frac{N_P(\beta)}{N_{P,Q,t_2}(\beta)} \tag{99}
$$

hold by Lemma 17. From Lemma 27 of (11), $P_{N_{P,Q,t_2}(u)}$ is monotonically decreasing on $\mathbb{R}$, and thus (III) holds for any $u$ and $u'$. Taking the limit $v \to -\infty$ in (22), we have the following inequality

$$
F_{P,Q,s_2}(t_2) \leq \int_{-\infty}^{\beta} \sqrt{N_P(x)} \sqrt{N_{P,Q,b}(x)} dx \\
+ \sqrt{1 - \Phi_P(v')} \frac{1}{\Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(\beta)}. \tag{100}
$$

Since

$$
\int_{-\infty}^{\beta} \sqrt{N_P(x)} \sqrt{N_{P,Q,b}(x)} dx \\
= \frac{\Phi_P(\beta - \frac{D_{P,Q,t_2}}{2})}{\sqrt{\Phi_P(\beta)}} e^{-\frac{(D_{P,Q,t_2})^2}{2}}, \tag{101}
$$

the proof is completed.

L. Proof of Lemma 20

There exists the unique solution of (51) with respect to $x$ in Lemma 12 of (11). Next, we show that there are two solutions $\beta' \leq \beta$ for the equation (52) and $\beta$ satisfies $\beta > \alpha$ under the condition $s_2 > \Phi_{P,Q,t_2} \left( \frac{\Phi_{P,Q,t_2}(s_2)}{\Phi_P(x)} \right)$. Here, the existence of
the solutions is equivalent to the existence of the zero points of the function
\[ f(x) := \Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(x) - (1 - \Phi_P(x)) \frac{N_{P,Q,t_2}(x)}{N_P(x)}. \]  
(102)
Since
\[ \frac{df}{dx} = - \frac{d}{dx} \left( \frac{N_{P,Q,t_2}}{N_P} \right) (1 - \Phi_P), \]  
(103)
the function \( f \) is strictly monotonically increasing when \( x < \arg\min (N_P/N_{P,Q,t_2}) \) and is strictly monotonically decreasing \( x > \arg\min (N_P/N_{P,Q,t_2}) \). Here, by the definition of \( \alpha \) and the condition \( s_2 > \Phi_{P,Q,t_2}^{-1} \left( \frac{\Phi_{P,Q,t_2}(\alpha)}{\Phi_P(\alpha)} \right) \), we obtain the following inequality:
\[ f(\alpha) = \Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(\alpha) - (1 - \Phi_P(\alpha)) \frac{\Phi_{P,Q,t_2}(\alpha)}{\Phi_P(\alpha)} > 0. \]  
(104)
Moreover, since
\[ \lim_{x \to -\infty} f(x) = -\infty, \]  
(105)
and
\[ \lim_{x \to \infty} f(x) = \lim_{x \to \infty} (\Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(x)) = - (1 - \Phi_{P,Q,t_2}(s_2)) < 0, \]  
(107)
the function \( f \) has two zero points \( \beta' < \beta \) and \( \beta > \alpha \) due to the intermediate value theorem. 

\section{M. Proof of Lemma 22}

Since the direct part is given by Lemma 16, we prove the converse part. At first, we treat the case when \( s_2 \leq \Phi_{P,Q,t_2}^{-1} \left( \frac{\Phi_{P,Q,t_2}(\alpha)}{\Phi_P(\alpha)} \right) \). For an arbitrary sequence \( \{P'_n\} \) of probability distributions which satisfies \( P'_n > P_n^{u(x)} \), the monotonicity of the fidelity follows
\[ F(P'_n, Q_n) \leq \sqrt{P'_n(S''_n(s_2)) \sqrt{Q_n(S''_n(s_2))}} + \sqrt{P'_n(S''_n(s_2, \infty)) \sqrt{Q_n(S''_n(s_2, \infty))}}. \]  
(108)
Since
\[ \limsup_{n \to \infty} P'_n(S''_n(s_2, \infty)) = 0, \]  
(109)
we obtain
\[ \limsup_{n \to \infty} F(P'_n, Q_n) \leq \sqrt{\Phi_{P,Q,t_2}(s_2)}. \]  
(110)
Next, we treat the case when \( s_2 > \Phi_{P,Q,t_2}^{-1} \left( \frac{\Phi_{P,Q,t_2}(\alpha)}{\Phi_P(\alpha)} \right) \).

Here, we use Lemma 20. By Lemma 20, \( \alpha \) satisfies
\[ \frac{\Phi_P(\alpha)}{\Phi_{P,Q,t_2}(\alpha)} = \frac{N_{P}(\alpha)}{N_{P,Q,t_2}(\alpha)}, \]  
(111)
and \( \beta \) satisfies
\[ \frac{1 - \Phi_P(\beta)}{\Phi_{P,Q,t_2}(s_2)} - \frac{1 - \Phi_P(\beta)}{\Phi_{P,Q,t_2}(\beta)} = \frac{N_P(\beta)}{N_{P,Q,t_2}(\beta)}, \]  
(112)
When we take as \( u = u' = \alpha \) and \( v = \beta' = \beta \) in Lemma 20, those satisfy (I) and (II). Moreover, from Lemma 27 of 11, \( \frac{N_{P}(u)}{N_{P,Q,t_2}(u)} \) is monotonically decreasing on \( \left( -\frac{kH(Q)(u)}{1 - C_{P,Q}}, \infty \right) \). Since \( \frac{kH(Q)}{1 - C_{P,Q}} \leq \alpha \leq \beta \), (III) holds. Thus, we have the following inequality
\[ F_{P,Q,s_2}^M(t_2) \leq \sqrt{\Phi_P(\beta) \Phi_{P,Q,t_2}(\alpha) + (I_{P,Q,t_2}(\beta) - I_{P,Q,t_2}(\alpha))} + \sqrt{1 - \Phi_P(\beta)} \sqrt{\Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(\beta)}, \]  
and thus, the proof is completed. 

\section{N. Proof of Lemma 23}

We show that there is the unique solution \( \beta \) of the equation (57) with respect to \( x \). Here, the unique solution is equivalent to the existence of the unique zero point of the function
\[ f(x) := \Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(x) - (1 - \Phi_P(x)) \frac{N_{P,Q,t_2}(x)}{N_P(x)}. \]  
(113)
Since
\[ \frac{df}{dx} = - \frac{d}{dx} \left( \frac{N_{P,Q,t_2}}{N_P} \right) (1 - \Phi_P), \]  
(114)
the function \( f \) is strictly monotonically decreasing when \( x < \arg\min (N_P/N_{P,Q,t_2}) \) and is strictly monotonically increasing \( x > \arg\min (N_P/N_{P,Q,t_2}) \). Since
\[ \lim_{x \to -\infty} f(x) = \Phi_{P,Q,t_2}(s_2) > 0, \]  
\[ \lim_{x \to \infty} f(x) = - (1 - \Phi_{P,Q,t_2}(s_2)) < 0, \]  
(115)
the function \( f \) has the unique zero point \( \beta \) due to the intermediate value theorem. 

\section{O. Proof of Lemma 23}

Since the direct part is given by Lemma 16, we prove the converse part. Here, we use Lemma 20. For any \( v \in \mathbb{R} \), the existence of \( u \) such that \( u \leq v \) and
\[ \frac{\Phi_P(v)}{\Phi_{P,Q,t_2}(v)} = \frac{N_{P}(u)}{N_{P,Q,t_2}(u)} \]  
(116)
can be easily verified by the mean value theorem as was shown in the proof of Lemma 11 of 11. Moreover, when we take as \( u' = v' = \beta \), then \( \beta \leq s_2 \) and
\[ \frac{1 - \Phi_P(\beta)}{\Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(\beta)} = \frac{N_P(\beta)}{N_{P,Q,t_2}(\beta)}, \]  
(117)
hold by Lemma 22. From Lemma 27 of 11, \( \frac{N_{P}(u)}{N_{P,Q,t_2}(u)} \) is monotonically decreasing on \( (-\infty, \frac{kH(Q)}{1 - C_{P,Q}}) \). Since \( \beta \leq \frac{kH(Q)}{1 - C_{P,Q}} \), thus (III) holds. Taking the limit \( v \to -\infty \) in (92), we have the following inequality
\[ F_{P,Q,s_2}^M(t_2) \leq \int_{-\infty}^{\beta} \sqrt{N_P(x)N_{P,Q,b}(x)}dx + \sqrt{1 - \Phi_P(\beta)} \sqrt{\Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(\beta)} \]  
+ \sqrt{1 - \Phi_P(\beta)} \sqrt{\Phi_{P,Q,t_2}(s_2) - \Phi_{P,Q,t_2}(\beta)} \]  
= I_{P,Q,t_2}(\beta).
and thus, the proof is completed.

**P. Proof of Lemma 24**

To begin with, we treat the case when $C_{P,Q} = 1$. Then, the value in (60) coincides with $F_{P,Q,s_2}(t_2)$ in (125), and thus, the optimal operation does not depend on

$$\Gamma : S(\mathcal{H}_{AB}) \rightarrow S((\mathbb{C}^N)^{\otimes 2}),$$

where

$$\begin{align*}
\Gamma & = \Gamma \circ \Gamma (\psi), \\
\Gamma & : S(\mathcal{H}_{AB}) \rightarrow S((\mathbb{C}^N)^{\otimes 2}),
\end{align*}$$

is attainable in the second step. Here,

$$\psi_{t_2} = \psi_{t_2}(\alpha_{t_2})$$

coincides with (120), which satisfies (121) for $P = P \psi$ and $L = N$.

For any LOCC map $\Gamma : S(\mathcal{H}_{AB}) \rightarrow S((\mathbb{C}^N)^{\otimes 2})$, there exists a LOCC map $\tilde{\Gamma} : S((\mathbb{C}^N)^{\otimes 2}) \rightarrow S((\mathbb{C}^N)^{\otimes 2})$ such that $\Gamma(\psi) = \tilde{\Gamma} \circ \Gamma (\psi)$.

**Proof:**

Because of Nielsen’s theorem ([14]), there exists a LOCC map $\Gamma$ which satisfies (I). Next, we prove that such $\Gamma$ satisfies (II). Let a LOCC map $\Gamma : S(\mathcal{H}_{AB}) \rightarrow S((\mathbb{C}^N)^{\otimes 2})$ output a state $\eta_j$ with probability $q_j$. Then, because of Jonathan-Plenio’s theorem ([9]),

$$\sum_{i=1}^{l} P_i(i) \leq \sum_{i=1}^{l} q_j P^{i\eta_j}_j(i)$$

holds for any $l = 1, ..., N$. Since $C(P_i)(i) = P^i$, we have

$$\sum_{i=1}^{l} C(P_i)(i) \leq \sum_{i=1}^{l} q_j P^{i\eta_j}_j(i)$$

for any $l = 1, ..., N$. Moreover, (123) holds for any $l = J_{P,N} + 1, ..., N$. If it does not hold, it implies a contradiction as follows. Then, there are the minimum numbers $k_0, l_0 \in \{J_{P,N} + 1, ..., N\}$ such that

$$\sum_{i=1}^{k_0} C(P_i)(i) = \sum_{i=1}^{k_0} q_j P^{i\eta_j}_j(i)$$

and $k_0 \geq l_0$. Moreover, the inequality (125) holds for any $l \geq l_0$ because $\sum_{i=1}^{k_0} q_j P^{i\eta_j}_j(l)$ is monotonically decreasing with respect to $l$. Thus, we have the following contradiction.

$$1 = \sum_{i=1}^{k_0} C(P_i)(i) + \sum_{i=k_0+1}^{N} C(P_i)(i)$$

As proved above, (123) holds for any $l = 1, ..., N$, and thus, we obtain (II) because of Jonathan-Plenio’s theorem ([9]).

From Lemma 31, we have

$$F^Q(\psi \rightarrow \phi | N) = F^Q(\psi_N \rightarrow \phi)$$

Thus, the proof is completed.

**VII. Conclusion**

We have considered RNC with restricted storage. The problem can be divided into various cases as was shown in Fig. 3 and we derived the corresponding rate regions for each case. In particular, we first showed the first-order rate region as in Fig. 2 and described the line which consists of admissible rate pairs. Unless the first-order rate pair is not admissible,
the second-order asymptotics is not needed. On the other hand, when the first-order rate pair is admissible, we need to consider trade-off of second-order rates under an accuracy constraint. Here, we emphasize that the form of the second-order rate regions strongly depend on extremality of the first-order rate pairs, uniformity of source and target distributions and the value of $C_{P, Q}$. Then, we applied the results for probability distributions to an LOCC compression problem of pure states in quantum information theory. In particular, we did not assumed that an initial state $\psi$ and a target state $\phi$ are the same states although those states are assumed to be the same in conventional state compression problems. It is thought that the analysis in this paper can be applied to store entangled states into entanglement storage.

We refer some future studies. First, probability distributions (or quantum states) were assumed to be i.i.d. in this paper. To treat information sources with classical (or quantum) correlation, the extension from an i.i.d. sequence to general one is thought as a problem to be solved [13]. Second, we analyzed only the asymptotic performance of random number conversion and LOCC conversion. On the other hand, what we can operate has only finite size. Therefore, it is expected that approximate conversion problems are analyzed in finite setting. Third, since only pure states were treated in quantum information setting although mixed entangled states can be appear in practice, the extension from pure states to mixed states is though to be important. Finally, we have shown that the problem of RNC via restricted storage has a non-trivial trade-off relation described by the second-order rate region although trade-off relation in the first-order rate region is quite simple. As is suggested by the results, when two kinds of first-order rates in an information theoretical problem simply and straightforward relate with each other, there is a possibility that the rate region has a non-trivial trade-off relation in the second order asymptotics. We can conclude that consideration of the second order asymptotics might bring a new trade-off relation in various information theoretical problems.

ACKNOWLEDGMENT

WK acknowledges support from Grant-in-Aid for JSPS Fellows No. 233283. MH is partially supported by a MEXT Grant-in-Aid for Scientific Research (A) No. 23246071 and the National Institute of Information and Communication Technology (NICT), Japan. The Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

REFERENCES

[1] B. C. Arnold, Majorization and the Lorenz Order: A Brief Introduction, Springer-Verlag. (1986).
[2] C. H. Bennett, H. J. Bernstein, S. Popescu, B. Schumacher, Phys. Rev. A. 53, 2046, (1996).
[3] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, A. V. Thapliyal, Phys. Rev. A 63, 012307 (2001).
[4] A. W. Harrow, H. K. Lo, IEEE Trans. Inform. Theory, 50(2), 319, (2004).
[5] M. Hayashi, IEEE Trans. Inform. Theory, 52, 1904-1921, (2006).
[6] M. Hayashi, IEEE Trans. Inform. Theory, 54, 4619–4637, (2008).
[7] M. Hayashi, M. Koashi, K. Matsumoto, F. Morikoshi, A. Winter, J. Phys. A: Math. Gen. 36, 527 (2003).
[8] P. Hayden, A. Winter, Phys. Rev. A, 67, 012326, (2003).
[9] D. Jonathan, M. B. Plenio, Phys. Rev. Lett. 83, 1455 (1999).
[10] W. Kumagai, M. Hayashi, Phys. Rev. Lett. 111(13), 130407, (2013).
[11] W. Kumagai, M. Hayashi, arXiv:1306.4166 (2013).
[12] A. W. Marshall, I. Olkin, Inequalities: Theory of Majorization and Its Applications. Academic Press, New York, (1979).
[13] K. Modi, T. Paterek, W. Son, V. Vedral, and M. Williamson, Phys. Rev. Lett. 104, 080501, (2010).
[14] M. A. Nielsens, Phys. Rev. Lett. 83, 436 (1999).
[15] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, (2000).
[16] R. Nomura, T. S. Han, IEEE Trans. Inform. Theory, 59, 1-16, (2013).
[17] B. Schumacher, Phys. Rev. A, 51(4), 2738, (1995).
[18] V. Y. Tan, O. Kosut, 2012 46th CISS, 1-6, (2012).
[19] A. W. Van der Vaart. Asymptotic Statistics, Cambridge University Press, (1998).
[20] S. Vemuri, S. Verdú, IEEE Trans. Inform. Theory, 41, 1322-1332, (1995).
[21] G. Vidal, D. Jonathan, M. A. Nielsen, Phys. Rev. A 62, 012304, (2000).
[22] S. Watanabe, S. Kuzuoka, V. Y. Tan, arXiv:1301.6467, (2013).
