

“© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.”

# Moderate Deviation Analysis for Classical-Quantum Channels and Quantum Hypothesis Testing

Hao-Chung Cheng<sup>1,2</sup> and Min-Hsiu Hsieh<sup>1</sup>

<sup>1</sup>*Centre for Quantum Software and Information (UTS:QISI),*

*Faculty of Engineering and Information Technology, University of Technology Sydney, Australia*

<sup>2</sup>*Graduate Institute Communication Engineering, National Taiwan University, Taiwan (R.O.C.)*

**ABSTRACT.** In this work, we study the tradeoffs between the error probabilities of classical-quantum channels and the blocklength  $n$  when the transmission rates approach the channel capacity at a rate slower than  $1/\sqrt{n}$ , a research topic known as moderate deviation analysis. We show that the optimal error probability vanishes under this rate convergence. Our main technical contributions are a tight quantum sphere-packing bound, obtained via Chaganty and Sethuraman's concentration inequality in strong large deviation theory, and asymptotic expansions of error-exponent functions. Moderate deviation analysis for quantum hypothesis testing is also established. The converse directly follows from our channel coding result, while the achievability relies on a martingale inequality.

## 1. INTRODUCTION

Investigating the interplay between the transmission rate, blocklength and error probability is one of the core problems in information theory. Based on different ranges of the error probability, the analysis of communication performance roughly falls into the following three categories: (i) *large error probability* or *non-vanishing error probability* regime; (ii) *medium error probability* regime; and (iii) *small error probability* regime. In the non-vanishing error probability regime, the largest transmission rate, given a coding length  $n$  and an error probability no more than  $\epsilon$ , is one of the main research focuses. Strassen [1] first demonstrated that the maximum size of an  $n$ -blocklength code through a discrete memoryless channel (DMC)  $\mathcal{W}$ , denoted by  $M^*(\mathcal{W}^n, \epsilon)$ , yields an asymptotic expansion to the order  $\sqrt{n}$ , and hence this is called *second-order analysis*:

$$\log M^*(\mathcal{W}^n, \epsilon) = nC + \sqrt{nV} \Phi^{-1}(\epsilon) + O(\log n), \quad (1.1)$$

where the quantities  $C$  and  $V$  denote the capacity [2] and the dispersion [3] of the channel, and  $\Phi$  is the cumulative distribution function of a standard normal random variable. Equivalently, Eq. (1.1) yields the following relationship between the optimal decoding error with blocklength  $n$  and rate  $C - A/\sqrt{n}$  for any constant  $A$ :

$$\lim_{n \rightarrow +\infty} \epsilon^*(n, C - A/\sqrt{n}) = \Phi\left(\frac{A}{\sqrt{V}}\right). \quad (1.2)$$

Strassen's result relied on the *Gaussian approximation* or the *central limit theorem (CLT)*. His work was latter refined by Hayashi [4], Polyanskiy *et al.* [3], and extended to quantum channels [5, 6, 7, 8]. The results for higher-order asymptotics are referred to Refs. [9, 10, 11].

In the *small error probability* regime, Shannon [12] introduced the *reliability function*  $E(R)$  as the optimal error exponent:

$$\lim_{n \rightarrow +\infty} -\frac{1}{n} \log \epsilon^*(n, R) = E(R), \quad (1.3)$$

---

*E-mail address:* F99942118@ntu.edu.tw, Min-Hsiu.Hsieh@uts.edu.au.

for rate  $R$  below the channel capacity<sup>1</sup>  $C$ . This seminal work entails the *error exponent analysis* of a broad class of channels [14, 13, 15, 16, 17, 18]. The exponential decay of the error probability in Eq. (1.3) is a consequence of the *large deviation principle* (LDP) [19]. In summary, the errors in Eqs. (1.2) and (1.3), respectively, fall into the CLT regime and large-deviation regime.

Altuğ and Wagner [20, 21] pioneered the study of the medium error probability regime, and investigated the asymptotic behaviour of the optimal decoding error when the coding rate converges to capacity sufficiently slowly. Specifically, they studied under which conditions the error is asymptotically equal to<sup>2</sup>

$$\epsilon^*(n, C - a_n) \sim \Phi\left(\frac{\sqrt{n}a_n}{\sqrt{v}}\right) \sim e^{-\frac{na_n^2}{2v}}, \quad (1.4)$$

where the sequence  $(a_n)_{n \in \mathbb{N}}$  satisfies

$$\begin{aligned} \text{(i)} \quad & \lim_{n \rightarrow +\infty} a_n = 0; \\ \text{(ii)} \quad & \lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty. \end{aligned} \quad (1.5)$$

Evidently, the transmission rate in Eq. (1.4) approaches capacity slower than  $1/\sqrt{n}$ . A DMC with errors satisfying Eq. (1.4) possesses a *moderate deviation property* (MDP) [19, Section 3.7]. The constant  $v$  in Eq. (1.4) equals the channel dispersion  $V$  when both the limit in Eq. (1.2) and MDP hold [22, Theorem 1]. We refer the interested readers to Refs. [22, 24, 21] for further results in classical channel coding. These three approaches—(i), (ii), and (iii)—all have theoretical significance and practical value, and this paper will focus on the medium error probability regime, which is rarely explored in the quantum scenario.

Our main contribution is, for any classical-quantum (c-q) channel with a non-zero dispersion  $V > 0$ ,

$$\lim_{n \rightarrow +\infty} \frac{\log \epsilon^*(n, C - a_n)}{na_n^2} = -\frac{1}{2V}, \quad (1.6)$$

where  $(a_n)_{n \in \mathbb{N}}$  is any sequence satisfying Eq. (1.5). The result in Eq. (1.6) shows that reliable communication over a c-q channel is possible when the transmission rate approaches capacity at the scale slower than  $1/\sqrt{n}$ . Our proof employs techniques from the error exponent analysis (the LDP regime). For the achievability part, we start from Hayashi's upper bound of the average error for c-q channels [27] followed by an asymptotic expansion of the error-exponent function. For the converse, we employ a sharp converse bound based on a strong large deviation inequality (Proposition 7). This bound is more general than the previous result in Ref. [18, Proposition 14], since it allows the transmission rates to depend on the blocklength instead of being fixed. We remark that Altuğ and Wagner's converse proof [21, Theorem 2.2] is not sufficient for proving Eq. (1.6) because their sphere-packing bound is of a weaker form in general c-q channels [18, Theorem 6] (see also [29]). Thus, naively following their converse approach will result in a gap between the achievability and converse results (see Remark 3.1).

As a special case of c-q channel coding, we obtain the moderate deviations for binary quantum hypothesis testing (see Theorems 9 and 10):

$$\lim_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \hat{\alpha}_{\exp\{-n[D(\rho\|\sigma) - a_n]\}}(\rho^{\otimes n} \|\sigma^{\otimes n}) = -\frac{1}{2V(\rho\|\sigma)}, \quad (1.7)$$

where  $\hat{\alpha}_\mu$  denotes the smallest type-I error when the type-II error does not exceed  $\mu$ ;  $D(\rho\|\sigma)$  and  $V(\rho\|\sigma)$  denote the relative entropy and relative variance of  $\rho$  and  $\sigma$ , respectively. The converse part directly follows from the channel coding, and we provide two proofs for the achievability part. The first one comes from Audenaert *et al.*'s error exponent analysis [30], while the second one employs a martingale inequality [24]. We remark that the moderate deviation analysis for classical hypothesis testing was studied by Sason [24], and by Watanabe and Hayashi [25]. Moreover, a recent work by Rouzé and Datta [26] formulated the quantum hypothesis problem into a martingale, which is similar to our approach for proving the achievability.

<sup>1</sup>To the best of our knowledge, the reliability function  $E(R)$  is only known in the high rate regime, i.e. at rates above a *critical rate* (see e.g. [13, p. 160]).

<sup>2</sup>We denote  $f_n \sim g_n$  if and only if  $\lim_{n \rightarrow +\infty} \frac{f_n}{g_n} = 1$ .

Unlike our proof techniques relying on error exponent analysis (the LDP regime), a recent and independent paper [31] obtained the same result, but proceeds from the second-order analysis (the CLT regime). Their achievability proof follows from the one-shot capacity by Wang and Renner [32]; while the converse part generalizes Polyanskiy and Verdú's result [22] (which in turn relies on Strassen's Gaussian approximation [1]) and a powerful inequality in probability [33] to the quantum scenario. We summarize the error behaviors in these three regimes in Table 1.

This paper is organized as follows. We introduce notation and preliminaries in Section 2. Section 3 contains our main result—the moderate deviation analysis for c-q channel coding. In Section 4, we present the moderate deviations for quantum hypothesis testing. Lastly, we conclude this paper in Section 5.

Error Regimes	Concentration Phenomena	Hypothesis Testing	Channel Coding
Large Error	CLT: $\Pr(S_n \geq \sqrt{nx}) \rightarrow 1 - \Phi\left(\frac{x}{\sqrt{v}}\right)$	$\hat{\alpha}_{\exp\{-n[D - \frac{A}{\sqrt{n}}]\}} \rightarrow \Phi\left(\frac{A}{\sqrt{V}}\right)$	$\epsilon^*\left(n, C - \frac{A}{\sqrt{n}}\right) \rightarrow \Phi\left(\frac{A}{\sqrt{V}}\right)$
Medium Error	MDP: $\Pr(S_n \geq na_n x) = e^{-\frac{na_n^2}{2v}x + o(na_n^2)}$	$\hat{\alpha}_{\exp\{-n[D - a_n]\}} = e^{-\frac{na_n^2}{2V} + o(na_n^2)}$	$\epsilon^*(n, C - a_n) = e^{-\frac{na_n^2}{2V} + o(na_n^2)}$
Small Error	LDP: $\Pr(S_n \geq nx) = e^{-n\Lambda^*(x) + o(n)}$	$\hat{\alpha}_{\exp\{-nr\}} = e^{-n\phi(r) + o(n)}$	$\epsilon^*(n, R) = e^{-nE(R) + o(n)}$

TABLE 1. This table compares the asymptotic error behaviors of quantum hypothesis testing and classical-quantum channel coding in three error probability regimes: (i) large error (central limit theorem), (ii) medium error (moderate deviation principle), and (iii) small error (large deviation principle). The quantity  $S_n$  denotes the sum of  $n$  independent and identically distributed random variables with zero mean and variance  $v$ . The exponent  $\Lambda^*$  is the Legendre-Fenchel transform of the normalized cumulant generating function of  $S_n$  [19]. The error  $\hat{\alpha}_{\exp\{-nr\}}$  is defined as the minimum type-I error with the type-II error smaller than  $\exp\{-nr\}$ . The quantities  $D$  and  $V$  in the hypothesis testing column denote the quantum relative entropy and the relative entropy variance, respectively. The optimal error probability with blocklength  $n$  and rate  $R$  is denoted by  $\epsilon^*(n, R)$ . The quantities  $C$  and  $V$  in the channel coding column indicate the channel capacity and the channel dispersion, respectively. The sequence  $(a_n)_{n \in \mathbb{N}}$  satisfies Eq. (1.5). The quantity  $E(R)$  is the reliability function of the channel.

## 2. PRELIMINARIES AND NOTATION

We first introduce necessary notation. Throughout this paper, we consider a Hilbert space  $\mathcal{H}$  with finite dimension  $d$ . The set of density operators (i.e. positive semi-definite operators with unit trace) and non-singular density operators on  $\mathcal{H}$  are defined by  $\mathcal{S}(\mathcal{H})$  and  $\mathcal{S}_{>0}(\mathcal{H})$ , respectively. The identity operator on  $\mathcal{H}$  is denoted by  $\mathbb{1}_{\mathcal{H}}$ , or simply  $\mathbb{1}$  if there is no possibility of confusion. We use  $\text{Tr}[\cdot]$  as the trace function. Let  $\mathbb{N}$ ,  $\mathbb{R}$ , and  $\mathbb{R}_{\geq 0}$  denote the set of integers, real numbers, and non-negative real numbers, respectively. Define  $[n] := \{1, 2, \dots, n\}$  for  $n \in \mathbb{N}$ .

The power of a positive semi-definite operator  $A$  is defined as:  $A^p = \sum_{i: a_i \neq 0} a_i^p P_i$ , where  $(a_i)_i$  and  $(P_i)_i$  are the eigenvalues and eigenprojections of  $A = \sum_i a_i P_i$ . We use  $\text{supp}(A)$  to denote support of the operator  $A$ . We write  $A \ll B$  if  $\text{supp}(A) \subset \text{supp}(B)$ .

**2.1. Quantum Hypothesis Testing and Channel Coding.** Consider a binary hypothesis testing problem whose null and alternative hypotheses are  $\rho \in \mathcal{S}(\mathcal{H})$  and  $\sigma \in \mathcal{S}(\mathcal{H})$ , respectively. The *type-I error* and *type-II error* of the hypothesis testing, for an operator  $0 \leq Q \leq \mathbb{1}$ , are defined as follows:

$$\alpha(Q; \rho) := \text{Tr}[(\mathbb{1} - Q)\rho], \quad (2.1)$$

$$\beta(Q; \sigma) := \text{Tr}[Q\sigma]. \quad (2.2)$$

There is a trade-off relation between these two errors. Thus we can define the minimum type-I error when the type-II error is below  $\mu \in (0, 1)$  as

$$\hat{\alpha}_{\mu}(\rho \parallel \sigma) := \min_{0 \leq Q \leq \mathbb{1}} \{\alpha(Q; \rho) : \beta(Q; \sigma) \leq \mu\}. \quad (2.3)$$

Denote by  $\mathcal{X}$  a finite input alphabet, and let  $\mathcal{P}(\mathcal{X})$  be the set of probability distributions on  $\mathcal{X}$ . For a sequence  $\mathbf{x}^n \in \mathcal{X}^n$ , we denote by

$$P_{\mathbf{x}^n}(x) := \frac{1}{n} \sum_{i=1}^n \mathbf{1}\{x = x_i\}, \quad (2.4)$$

where  $x_i$  is the  $i$ -th element of  $\mathbf{x}^n$ .

A c-q channel  $\mathcal{W}$  maps elements of  $\mathcal{X}$  to the density operators in  $\mathcal{S}(\mathcal{H})$ , i.e.  $\mathcal{W} : x \mapsto W_x$ . We denote the image of the channel  $\mathcal{W}$  by

$$\text{im}(\mathcal{W}) := \{\rho \in \mathcal{S}(\mathcal{H}) \mid \exists x \in \mathcal{X} : \rho = W_x\}, \quad (2.5)$$

and its closure by  $\overline{\text{im}(\mathcal{W})}$ . Without loss of generality, we assume that  $\text{im}(\mathcal{W})$  has full support on the Hilbert space  $\mathcal{H}$  throughout this paper.

Let  $\mathcal{M}$  be a finite alphabetical set with size  $M = |\mathcal{M}|$ . An  $(n\text{-block})$  *encoder* is a map  $f_n : \mathcal{M} \rightarrow \mathcal{X}^n$  that encodes each message  $m \in \mathcal{M}$  to a codeword  $\mathbf{x}^n(m) := x_1(m) \dots x_n(m) \in \mathcal{X}^n$ . The c-q channel then produces an output state  $W_{\mathbf{x}^n(m)}^{\otimes n}$  with the input codeword  $\mathbf{x}^n(m)$ , where

$$W_{\mathbf{x}^n(m)}^{\otimes n} = W_{x_1(m)} \otimes \dots \otimes W_{x_n(m)} \in \mathcal{S}(\mathcal{H}^{\otimes n}). \quad (2.6)$$

The *decoder* is described by a positive operator-valued measurement (POVM)  $\Pi_n = \{\Pi_{n,1}, \dots, \Pi_{n,M}\}$  on  $\mathcal{H}^{\otimes n}$ , where  $\Pi_{n,i} \geq 0$  and  $\sum_{i=1}^M \Pi_{n,i} = \mathbb{1}$ . The pair  $(f_n, \Pi_n) =: \mathcal{C}_n$  is called a *code* with *rate*  $R = \frac{1}{n} \log |\mathcal{M}|$ . The error probability of sending a message  $m$  with the code  $\mathcal{C}_n$  is  $\epsilon_m(\mathcal{W}, \mathcal{C}_n) := 1 - \text{Tr}(\Pi_{n,m} W_{\mathbf{x}^n(m)}^{\otimes n})$ . We use  $\epsilon_{\max}(\mathcal{W}, \mathcal{C}_n) = \max_{m \in \mathcal{M}} \epsilon_m(\mathcal{W}, \mathcal{C}_n)$  and  $\bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) = \frac{1}{M} \sum_{m \in \mathcal{M}} \epsilon_m(\mathcal{W}, \mathcal{C}_n)$  to denote the *maximal* error probability and the *average* error probability, respectively. Denote by  $\epsilon^*(n, R)$  the smallest average error probability among all codes  $\mathcal{C}_n$  with message size  $|\mathcal{M}| = \exp\{nR\}$ .

**2.2. Information Quantities.** For any  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , we define the quantum relative entropy, (Petz's) quantum Rényi divergence [43], and the log-Euclidean Rényi divergence [48, 18], respectively, as follows:

$$D(\rho \parallel \sigma) := \text{Tr}[\rho(\log \rho - \log \sigma)], \quad (2.7)$$

$$D_\alpha(\rho \parallel \sigma) := \frac{1}{\alpha - 1} \log \text{Tr}[\rho^\alpha \sigma^{1-\alpha}], \quad (2.8)$$

$$D_\alpha^b(\rho \parallel \sigma) := \frac{1}{\alpha - 1} \log \text{Tr} \left[ e^{\alpha \log \rho + (1-\alpha) \log \sigma} \right]. \quad (2.9)$$

We define two types of the quantum relative entropy variances [5, 6] by

$$V(\rho \parallel \sigma) := \text{Tr} \left[ \rho (\log \rho - \log \sigma)^2 \right] - D(\rho \parallel \sigma)^2 \quad (2.10)$$

$$\tilde{V}(\rho \parallel \sigma) := \int_0^1 dt \text{Tr} \left[ \rho^{1-t} (\log \rho - \log \sigma) \rho^t (\log \rho - \log \sigma) \right] - D(\rho \parallel \sigma)^2. \quad (2.11)$$

It is well-known that both quantities are non-negative, and

$$V(\rho \parallel \sigma) > 0 \quad \text{implies} \quad D(\rho \parallel \sigma) > 0. \quad (2.12)$$

We define the *conditional quantum relative entropy* of two channels  $\bar{\mathcal{W}}, \mathcal{W}$  and  $P \in \mathcal{P}(\mathcal{X})$  to be

$$D(\bar{\mathcal{W}} \parallel \mathcal{W} | P) := \sum_{x \in \mathcal{X}} P(x) D(\bar{W}_x \parallel W_x). \quad (2.13)$$

Similarly, we define the following conditional entropic quantities for  $\sigma \in \mathcal{S}(\mathcal{H})$  and  $P \in \mathcal{P}(\mathcal{X})$ :

$$D(W\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) D(W_x\|\sigma), \quad (2.14)$$

$$D_\alpha(W\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) D_\alpha(W_x\|\sigma), \quad (2.15)$$

$$V(W\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) V(W_x\|\sigma), \quad (2.16)$$

$$\tilde{V}(W\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) \tilde{V}(W_x\|\sigma). \quad (2.17)$$

The *mutual information* of the channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with a prior distribution  $P \in \mathcal{P}(\mathcal{X})$  is defined by

$$I(P, \mathcal{W}) := D(P \circ \mathcal{W} \| P \otimes P\mathcal{W}) = D(\mathcal{W} \| P\mathcal{W} | P), \quad (2.18)$$

where  $P \circ \mathcal{W} := \sum_{x \in \mathcal{X}} P(x) |x\rangle\langle x| \otimes W_x$  and  $P\mathcal{W} := \sum_{x \in \mathcal{X}} P(x) W_x$ . Hence, the (classical) *information capacity* of the channel  $\mathcal{W}$  is

$$C_{\mathcal{W}} := \max_{P \in \mathcal{P}(\mathcal{X})} I(P, \mathcal{W}). \quad (2.19)$$

The *conditional information variance* and the *unconditional information variance* of  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with a prior distribution  $P \in \mathcal{P}(\mathcal{X})$  are defined, respectively, by

$$\begin{aligned} V(P, \mathcal{W}) &:= V(\mathcal{W} \| P\mathcal{W} | P), \\ U(P, \mathcal{W}) &:= V(P \circ \mathcal{W} \| P \otimes P\mathcal{W}). \end{aligned} \quad (2.20)$$

It is known that (see e.g. [3, Lemma 62]) that  $V(P^*, \mathcal{W}) = U(P^*, \mathcal{W})$  for every capacity-achieving distribution  $P^* \in \mathcal{P}(\mathcal{X})$ , i.e.  $I(P^*, \mathcal{W}) = C_{\mathcal{W}}$ . Similarly, we also define the unconditional information variance in terms of  $\tilde{V}(\rho\|\sigma)$ :

$$\tilde{V}(P, \mathcal{W}) := \tilde{V}(\mathcal{W} \| P\mathcal{W} | P). \quad (2.21)$$

The *minimal peripheral information variance* and its variant are defined by

$$V_{\mathcal{W}} := \min_{P \in \mathcal{P}(\mathcal{X}) : I(P, \mathcal{W}) = C_{\mathcal{W}}} V(P, \mathcal{W}), \quad (2.22)$$

$$\tilde{V}_{\mathcal{W}} := \min_{P \in \mathcal{P}(\mathcal{X}) : I(P, \mathcal{W}) = C_{\mathcal{W}}} \tilde{V}(P, \mathcal{W}). \quad (2.23)$$

Furthermore, one can verify that

$$V_{\mathcal{W}} > 0 \quad \text{implies} \quad C_{\mathcal{W}} > 0. \quad (2.24)$$

**2.2.1. Auxiliary functions and their properties.** The auxiliary function of a classical-quantum channel is defined as [35, 36, 37, 38, 39]

$$E_0(s, P) := -\log \text{Tr} \left[ \left( \sum_{x \in \mathcal{X}} P(x) W_x^{1/(1+s)} \right)^{1+s} \right].$$

In this paper, we will require three variants of the above auxiliary function:  $\forall s \geq 0$  and  $\sigma \in \mathcal{S}(\mathcal{H})$ ,

$$\tilde{E}_0(s, P, \sigma) := s D_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \quad (2.25)$$

$$E_h(s, P, \sigma) := s D_{\frac{1}{1+s}}(\mathcal{W} \| \sigma | P), \quad (2.26)$$

$$\tilde{E}_h(s, P, \sigma) := s D_{\frac{1}{1+s}}^b(\mathcal{W} \| \sigma | P), \quad (2.27)$$

where  $D_\alpha$  and  $D_\alpha^b$  are the (Petz's) quantum Rényi divergence and the log-Euclidean Rényi divergence, respectively.

The function  $\tilde{E}_0(s, P, \sigma)$  will play a major role in the achievability part of our main result (see Theorem 4 in Section 3). This quantity yields an upper bound to the average error probability (see [27, Eq. (9)]):

$$\bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \leq 4 \exp \left\{ -n \left[ \max_{0 \leq s \leq 1} \max_{P \in \mathcal{P}(\mathcal{X})} \left\{ -sR + \tilde{E}_0(s, P, P\mathcal{W}) \right\} \right] \right\}. \quad (2.28)$$

Properties of  $E_h$  and  $\tilde{E}_h$  will be crucial in the analysis of the converse part of our main result.

The following proposition summarizes properties of  $\tilde{E}_0(s, P, \sigma)$ . We provide the proof in Appendix A.1.

**Proposition 1** (Properties of  $\tilde{E}_0(s, P, \sigma)$ ). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \text{supp}(P)$ . Then  $\tilde{E}_0(s, P, \sigma)$  defined in Eq. (2.25) enjoys the following properties.*

- (a)  $\tilde{E}_0(s, P, \sigma)$  and its partial derivatives  $\partial \tilde{E}_0(s, P, \sigma)/\partial s$ ,  $\partial^2 \tilde{E}_0(s, P, \sigma)/\partial s^2$ ,  $\partial^3 \tilde{E}_0(s, P, \sigma)/\partial s^3$  are all continuous in  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .
- (b) For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $\tilde{E}_0(s, P, \sigma)$  is concave in  $s \in \mathbb{R}_{\geq 0}$ .
- (c) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \right|_{s=0} = D(P \circ \mathcal{W} \| P \otimes \sigma). \quad (2.29)$$

- (d) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\lim_{s \rightarrow +\infty} \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \leq \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \leq D(P \circ \mathcal{W} \| P \otimes \sigma), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (2.30)$$

- (e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 \tilde{E}_0(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -V(P \circ \mathcal{W} \| P \otimes \sigma). \quad (2.31)$$

Properties of  $E_h(s, P, \sigma)$  are collected in the following proposition. The proof can be found in Appendix A.2.

**Proposition 2** (Properties of  $E_h(s, P, \sigma)$ ). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \text{supp}(P)$ . Then  $E_h(s, P, \sigma)$  defined in Eq. (2.26) enjoys the following properties.*

- (a)  $E_h(s, P, \sigma)$  and its partial derivatives  $\partial E_h(s, P, \sigma)/\partial s$ ,  $\partial^2 E_h(s, P, \sigma)/\partial s^2$ ,  $\partial^3 E_h(s, P, \sigma)/\partial s^3$  are continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .
- (b) For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $E_h(s, P, \sigma)$  is concave in  $s$  for all  $s \in \mathbb{R}_{\geq 0}$ .
- (c) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial E_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W} \| \sigma | P). \quad (2.32)$$

- (d) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\lim_{s \rightarrow +\infty} \frac{\partial E_h(s, P, \sigma)}{\partial s} \leq \frac{\partial E_h(s, P, \sigma)}{\partial s} \leq D(\mathcal{W} \| \sigma | P), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (2.33)$$

- (e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 E_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -V(\mathcal{W} \| \sigma | P). \quad (2.34)$$

Proposition 3 below lists the properties of  $\tilde{E}_h$ , and the proof is provided in Appendix A.3.

**Proposition 3** (Properties of  $\tilde{E}_h(s, P, \sigma)$ ). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \text{supp}(P)$ . Then  $\tilde{E}_h(s, P, \sigma)$  defined in Eq. (2.27) enjoys the following properties.*



- (a)  $\tilde{E}_h(s, P, \sigma)$  and its partial derivatives  $\partial \tilde{E}_h(s, P, \sigma)/\partial s$ ,  $\partial^2 \tilde{E}_h(s, P, \sigma)/\partial s^2$ ,  $\partial^3 \tilde{E}_h(s, P, \sigma)/\partial s^3$  are all continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .
- (b) For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $\tilde{E}_h(s, P, \sigma)$  is concave in  $s$  for all  $s \in \mathbb{R}_{\geq 0}$ .
- (c) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W} \parallel \sigma | P). \quad (2.35)$$

- (d) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\lim_{s \rightarrow +\infty} \frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} \leq \frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} \leq D(\mathcal{W} \parallel \sigma | P), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (2.36)$$

- (e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 \tilde{E}_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -\tilde{V}(\mathcal{W} \parallel \sigma | P). \quad (2.37)$$

**2.2.2. Error Exponents.** Auxiliary functions allow us to concisely define sphere-packing exponent functions of a classical-quantum channel. We will use notation similar to Refs. [40, 28, 18]. Define

$$\tilde{E}_{\text{sp}}(R, P, \sigma) := \min_{\bar{\mathcal{W}}: \mathcal{X} \rightarrow \mathcal{S}_0} \{D(\bar{\mathcal{W}} \parallel \mathcal{W} | P) : D(\bar{\mathcal{W}} \parallel \sigma | P) \leq R\} \quad (2.38)$$

$$= \sup_{s \geq 0} \left\{ \tilde{E}_h(s, P) - sR \right\}, \quad (2.39)$$

$$E_{\text{sp}}^{(2)}(R, P, \sigma) := \sup_{s \geq 0} \{E_h(s, P) - sR\}, \quad (2.40)$$

for all  $R > 0$ ,  $P \in \mathcal{P}(\mathcal{X})$ , and  $\sigma \in \mathcal{S}_{>0}(\mathcal{H})$ . The equality in Eq. (2.39) follows from [18, Theorem 6]. From the definitions in Eqs. (2.38) and (D.9), it is not hard to see that [30]

$$\tilde{E}_{\text{sp}}(R, P, \sigma) = 0, \quad \forall R \geq D(\mathcal{W} \parallel \sigma | P). \quad (2.41)$$

and

$$E_{\text{sp}}^{(2)}(R, P, \sigma) = \begin{cases} +\infty, & R < D_0(\mathcal{W} \parallel \sigma | P), \\ 0, & R \geq D(\mathcal{W} \parallel \sigma | P). \end{cases} \quad (2.42)$$

### 3. MODERATE DEVIATIONS FOR CLASSICAL-QUANTUM CHANNELS

This section presents our main results—the error performance of classical-quantum channels satisfies the moderate deviation property, Eq. (1.4). The achievability part is stated in Theorem 4, and its proof is given in Section 3.1. Our proof strategy employs Hayashi's bound [27] and the properties of the modified auxiliary function (Proposition 1). Theorem 5 contains the converse part, and is proved in Section 3.2. The proof involves a weak sphere-packing bound (Proposition 6), a sharp converse lower bound (Proposition 7), and an approximation of the error-exponent function around capacity (Proposition 8).

Let  $(a_n)_{n \in \mathbb{N}}$  be a sequence of real numbers satisfying

$$\begin{aligned} \text{(i)} \quad & a_n \rightarrow 0, \quad \text{as } n \rightarrow +\infty, \\ \text{(ii)} \quad & a_n \sqrt{n} \rightarrow +\infty, \quad \text{as } n \rightarrow +\infty. \end{aligned} \quad (3.1)$$

**Theorem 4 (Achievability).** *For any  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $V_{\mathcal{W}} > 0$  and any sequence  $(a_n)_{n \geq 1}$  satisfying Eq. (3.1), there exists a sequence of codes  $\{\mathcal{C}_n\}_{n \geq 1}$  with rates  $R_n = C_{\mathcal{W}} - a_n$  so that*

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \leq -\frac{1}{2V_{\mathcal{W}}}. \quad (3.2)$$

The proof is given in Section 3.1.



**Theorem 5 (Converse).** *For any  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $V_{\mathcal{W}} > 0$ , any sequence  $\{a_n\}_{n \geq 1}$  satisfying Eq. (3.1), and any sequence of codes  $\{\mathcal{C}_n\}_{n \geq 1}$  with rates  $R_n = C_{\mathcal{W}} - a_n$ , it holds that*

$$\liminf_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \geq -\frac{1}{2V_{\mathcal{W}}}. \quad (3.3)$$

The proof is given in Section 3.2.

*Remark 3.1.* Altuğ and Wagner [21] proved Theorem 5 for discrete classical channels by a weak sphere-packing bound with the expression of  $\tilde{E}_{\text{sp}}$ . Although such a weak sphere-packing bound indeed holds for c-q channels (see Proposition 6 and Remark B.1 in Appendix B), Proposition 8 in Section 3.2 shows that it will lead to

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \leq -\frac{1}{2\tilde{V}_{\mathcal{W}}}, \quad (3.4)$$

where  $\tilde{V}_{\mathcal{W}}$  is defined in Eq. (2.23). Since  $\tilde{V}(\rho \parallel \sigma) \leq V(\rho \parallel \sigma)$  [42, Theorem 1.2], it holds that  $\tilde{V}_{\mathcal{W}} \leq V_{\mathcal{W}}$  and the equality happens if and only if the channel reduces to classical. Hence, Altuğ and Wagner's method yields a weaker result in quantum regime; namely, a gap between the achievability and the converse. In Section 3.2, we will employ a sharp converse bound from strong large deviation theory to achieve our result, Theorem 5.

**3.1. Proof of Achievability: Theorem 4.** Let  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  satisfy  $V_{\mathcal{W}} > 0$ . Let  $\{a_n\}_{n \geq 1}$  be any sequence of real numbers satisfying Eq. (3.1). Since  $V_{\mathcal{W}} > 0$ , Eq. (2.24) shows that  $C_{\mathcal{W}} > 0$ . Hence, we have  $C_{\mathcal{W}} - a_n > 0$ , for all sufficiently large  $n$ . Fix such an integer  $n$  onwards, Hayashi's upper bound, Eq. (2.28), implies that there exists a code  $\mathcal{C}_n$  with  $R_n = C_{\mathcal{W}} - a_n$  so that

$$\bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \leq 4 \exp \left( -n \left[ \max_{0 \leq s \leq 1} \left\{ \tilde{E}_0(s, P, P\mathcal{W}) - sR_n \right\} \right] \right), \quad (3.5)$$

for all  $P \in \mathcal{P}(\mathcal{X})$ . In the following, we denote by  $\tilde{E}_0(s, P) := \tilde{E}_0(s, P, P\mathcal{W})$  for notational convenience. Simple algebra yields

$$\frac{1}{na_n^2} \log \bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \leq \frac{\log 4}{na_n^2} - \frac{1}{a_n^2} \max_{0 \leq s \leq 1} \left\{ \tilde{E}_0(s, P) - sR_n \right\}, \quad (3.6)$$

for all sufficiently large  $n$  and any  $P \in \mathcal{P}(\mathcal{X})$ .

Let  $\tilde{\mathcal{P}}(\mathcal{X})$  be the set of distributions that achieve the minimum in Eq. (2.22), and let  $\tilde{P} \in \tilde{\mathcal{P}}(\mathcal{X})$ . Note that Ref. [9, Lemma 3] implies that  $\tilde{\mathcal{P}}(\mathcal{X})$  is compact. Applying Taylor's theorem to  $\tilde{E}_0(s, \tilde{P})$  at  $s = 0$  together with Proposition 1 gives

$$\tilde{E}_0(s, \tilde{P}) = sC_{\mathcal{W}} - \frac{s^2}{2}V_{\mathcal{W}} + \frac{s^3}{6} \frac{\partial^3 \tilde{E}_0(s, \tilde{P})}{\partial s^3} \bigg|_{s=\bar{s}}, \quad (3.7)$$

for some  $\bar{s} \in [0, s]$ . Let  $s_n = a_n/V_{\mathcal{W}}$ . Then  $s_n \leq 1$  for all sufficiently large  $n$  by the assumption in Eq. (3.1) and  $V_{\mathcal{W}} > 0$ . For all  $s_n \leq 1$ , Eq. (3.7) yields

$$\max_{0 \leq s \leq 1} \left\{ \tilde{E}_0(s, \tilde{P}) - sR_n \right\} \geq \tilde{E}_0(s_n, \tilde{P}) - s_n R_n \quad (3.8)$$

$$= \frac{a_n}{V_{\mathcal{W}}} (C_{\mathcal{W}} - R_n) - \frac{a_n^2}{2V_{\mathcal{W}}} + \frac{a_n^3}{6V_{\mathcal{W}}^3} \frac{\partial^3 \tilde{E}_0(s, \tilde{P})}{\partial s^3} \bigg|_{s=\bar{s}_n} \quad (3.9)$$

$$= \frac{a_n^2}{2V_{\mathcal{W}}} + \frac{a_n^3}{6V_{\mathcal{W}}^3} \frac{\partial^3 \tilde{E}_0(s, \tilde{P})}{\partial s^3} \bigg|_{s=\bar{s}_n}, \quad (3.10)$$

where  $\bar{s}_n \in [0, s_n]$  and Eq. (3.10) holds since  $R_n = C_{\mathcal{W}} - a_n$ .

Define

$$\Upsilon = \max_{(s,P) \in [0,1] \times \tilde{\mathcal{P}}(\mathcal{X})} \left| \frac{\partial^3 \tilde{E}_0(s, P)}{\partial s^3} \right|, \quad (3.11)$$

which is finite due to the compact set  $[0, 1] \times \tilde{\mathcal{P}}(\mathcal{X})$  and item (a) in Proposition 1. Therefore, Eq. (3.10) implies that

$$\max_{0 \leq s \leq 1} \left\{ \tilde{E}_0(s, \tilde{P}) - sR_n \right\} \geq \frac{a_n^2}{2V_W} + \frac{a_n^3}{6V_W^3} \frac{\partial^3 \tilde{E}_0(s, \tilde{P})}{\partial s^3} \Big|_{s=\bar{s}_n} \quad (3.12)$$

$$\geq \frac{a_n^2}{2V_W} - \frac{a_n^3}{6V_W^3} \left| \frac{\partial^3 \tilde{E}_0(s, \tilde{P})}{\partial s^3} \right|_{s=\bar{s}_n} \quad (3.13)$$

$$\geq \frac{a_n^2}{2V_W} - \frac{a_n^3}{6V_W^3} \Upsilon, \quad (3.14)$$

for all sufficiently large  $n$ .

Substituting Eq. (3.14) into Eq. (3.6) gives

$$\frac{1}{na_n^2} \log \bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \leq \frac{\log 4}{na_n^2} - \frac{1}{2V_W} \left( 1 - \Upsilon \frac{a_n}{3V_W^2} \right). \quad (3.15)$$

Recall Eq. (3.1) and let  $n \rightarrow +\infty$ , which completes the proof:

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \leq -\frac{1}{2V_W}. \quad (3.16)$$

□

**3.2. Proof of Converse: Theorem 5.** Our strategy consists of the following steps. First, we claim that it suffices to prove Eq. (3.3) for the maximal error probability of any code  $\mathcal{C}_n$ , i.e.  $\epsilon_{\max}(\mathcal{W}, \mathcal{C}_n)$ . Recall the standard expurgation method (see e.g. [41, p. 96], [50, Theorem 20], [15, p. 395]): by removing half codewords with highest error probability to arrive at  $\bar{\epsilon}(\mathcal{W}, \mathcal{C}_n) \geq \frac{1}{2} \epsilon_{\max}(\mathcal{W}, \mathcal{C}'_n)$  with  $|\mathcal{C}'_n| = \lceil |\mathcal{C}_n|/2 \rceil \geq \frac{1}{2} \exp\{nR_n\} = \exp\{n(R_n - \frac{1}{n} \log 2)\}$ . Since the induced rate back-off is only  $\frac{1}{n} \log 2 = o(a_n)$ , one might define another sequence  $a'_n := a_n - \frac{1}{n} \log 2$  satisfying Eq. (3.1). Hence, without loss generality, we only need to prove the converse part for  $\epsilon_{\max}$ .

Second, we employ the method of Ref. [18, Lemma 16] to relate the error probability  $\epsilon_{\max}$  to the minimum type-I error:

$$\frac{\log \epsilon_{\max}(\mathcal{W}, \mathcal{C}_n)}{na_n^2} \geq \max_{\sigma^n \in \mathcal{S}(\mathcal{H}^{\otimes n})} \min_{\mathbf{x}^n \in \mathcal{X}^n} \frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \|\sigma^n)}{na_n^2} \quad (3.17)$$

$$\geq \min_{\mathbf{x}^n \in \mathcal{X}^n} \frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \|(P^* \mathcal{W})^{\otimes n})}{na_n^2}, \quad (3.18)$$

where  $P^* \in \mathcal{P}(\mathcal{X})$  is an arbitrary capacity-achieving distribution, i.e.  $I(P^*, \mathcal{W}) = C_W$ .

Third, we divide the set of codewords into two groups. Fix an arbitrary  $\eta \in (0, \frac{1}{2})$ . Let  $A := \max_{\rho \in \mathcal{S}_o} V(\rho \| P^* \mathcal{W})$  and let  $\xi = \sqrt{2A/\eta}$ . Define:

$$\Omega_{\text{good}} := \{\mathbf{x}^n \in \mathcal{X}^n : D(\mathcal{W} \| P^* \mathcal{W} | P_{\mathbf{x}^n}) > R_n\}; \quad (3.19)$$

$$\Omega_{\text{bad}} := \mathcal{X}^n \setminus \Omega_{\text{good}}. \quad (3.20)$$

For the codes in  $\Omega_{\text{bad}}$ , we employ a weak converse bound in Proposition 6, and apply a sharp converse bound, Proposition 7, for  $\Omega_{\text{good}}$ . Furthermore, we can assume  $a_n > 0$  for all sufficiently large  $n \in \mathbb{N}$  owing to the assumption  $\lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty$ . Subsequently, we will consider such  $n$  onwards.

*Proof of Theorem 5.* We start the proof with the case  $\Omega_{\text{bad}}$ , and further consider two different cases:

$$\Omega_{\text{bad}}^{(1)} := \left\{ \mathbf{x}^n \in \mathcal{X}^n : D(\mathcal{W} \| P^* \mathcal{W} | P_{\mathbf{x}^n}) \leq R_n - \frac{2\xi}{\sqrt{n}} \right\}; \quad (3.21)$$

$$\Omega_{\text{bad}}^{(2)} := \left\{ \mathbf{x}^n \in \mathcal{X}^n : R_n - \frac{2\xi}{\sqrt{n}} < D(\mathcal{W} \| P^* \mathcal{W} | P_{\mathbf{x}^n}) \leq R_n \right\}. \quad (3.22)$$

We apply the following weak converse bound with  $\sigma = P^* \mathcal{W}$ , whose proof is provided in Appendix B to further lower bound the right-hand side of Eq. (3.18).

**Proposition 6** (A Weak Converse Bound). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $\mathcal{S}_\circ := \overline{\text{im}(\mathcal{W})}$ , an arbitrary rate  $R \geq 0$ , and  $\sigma \in \mathcal{S}_{>0}(\mathcal{H})$ . For any  $\eta \in (0, \frac{1}{2})$ , let  $N_0 \in \mathbb{N}$  such that for all  $n \geq N_0$ ,*

$$e^{-\xi\sqrt{n}} \leq \frac{\eta}{2}, \quad (3.23)$$

where  $\xi = \sqrt{2A/\eta}$  and  $A := \max_{\rho \in \mathcal{S}_\circ} V(\rho \| \sigma)$ . Then, it holds that for all  $n \geq N_0$ ,

$$\hat{\alpha}_{\exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \| \sigma^{\otimes n}) \geq f(\eta) \exp \left\{ -n \left[ \frac{\tilde{E}_{\text{sp}} \left( R - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, \sigma \right)}{1 - \eta} \right] \right\}, \quad (3.24)$$

where  $f(\eta) = \exp \left\{ -\frac{h(1-\eta)}{1-\eta} \right\}$  and  $h(p) := -p \log p - (1-p) \log(1-p)$  is the binary entropy function.

Let  $\eta$  and  $\xi$  be defined as above, and let  $N_1$  be an integer satisfying Eq. (3.23). Then Eq. (3.24) gives, for all  $n \geq N_1$ ,

$$\frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\frac{\tilde{E}_{\text{sp}} \left( R_n - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, P^* \mathcal{W} \right)}{a_n^2(1-\eta)} + \frac{\log f(\eta)}{na_n^2}. \quad (3.25)$$

Further, Eq. (2.41) implies that for all  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(1)}$ ,

$$\tilde{E}_{\text{sp}} \left( R_n - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, P^* \mathcal{W} \right) = 0. \quad (3.26)$$

Hence, we have for all  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(1)}$ ,

$$\frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq \frac{\log f(\eta)}{na_n^2} \quad (3.27)$$

$$\geq -\frac{1}{2V_{\mathcal{W}}} + \frac{\log f(\eta)}{na_n^2}, \quad (3.28)$$

where the last inequality follows from  $V_{\mathcal{W}} > 0$ . Since  $f(\eta) < +\infty$ , taking the infimum limit of  $n \rightarrow +\infty$  and using Eq. (3.1) give, for all  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(1)}$ ,

$$\liminf_{n \rightarrow +\infty} \frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\frac{1}{2V_{\mathcal{W}}}. \quad (3.29)$$

Next, we move on to  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(2)}$ . In this case,  $\tilde{E}_{\text{sp}}$  in Eq. (3.25) is not equal to zero for any finite  $n$ , we employ Eq. (3.47) in Proposition 8 below with  $\delta_n = a_n + 2\xi/\sqrt{n}$  and  $b_n = a_n$  to arrive at

$$\liminf_{n \rightarrow +\infty} \frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\lim_{n \rightarrow +\infty} \frac{4\xi^2}{n \left( a_n + \frac{2\xi}{\sqrt{n}} \right)^2} \cdot \frac{1}{2\tilde{V}_{\mathcal{W}}(1-\eta)} \quad (3.30)$$

$$= 0 \quad (3.31)$$

$$\geq -\frac{1}{2V_{\mathcal{W}}}, \quad (3.32)$$

where the equality follows since  $\lim_{n \rightarrow +\infty} na_n^2 = +\infty$ .

In the last case of  $\mathbf{x}^n \in \Omega_{\text{good}}$ , we employ a tighter bound, Proposition 7, to lower bound the right-hand side of Eq. (3.18). The proof is delayed to Appendix C.

**Proposition 7** (A Sharp Converse Bound). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and a state  $\sigma \in \mathcal{S}(\mathcal{H})$ . Suppose the sequence  $\mathbf{x}^n \in \mathcal{X}^n$  satisfies*

$$\nu \leq V(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n}) < +\infty \quad (3.33)$$

for some  $\nu > 0$ , and suppose the sequence of rates  $(R_n)_{n \in \mathbb{N}}$  satisfies<sup>3</sup>  $D_0(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n}) < R_n < D(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n})$ . Then, there exists an  $N_0 \in \mathbb{N}$  such that, for all  $n \geq N_0$ ,

$$\hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \parallel \sigma^{\otimes n}) \geq \frac{A}{s_n^* \sqrt{n}} \exp \left\{ -n E_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, \sigma) \right\}, \quad (3.34)$$

where  $c_n = \frac{K \log n}{n}$  and  $A, K > 0$  are finite constants independent of the sequence  $\mathbf{x}^n$ , and

$$s_n^* := \arg \max_{s \geq 0} \{E_h(s, P_{\mathbf{x}^n}, \sigma) - s R_n\}. \quad (3.35)$$

Before applying Proposition 7, we verify that the condition, Eq. (3.33), is satisfied. Define

$$v(\delta) := \min_{P \in \mathcal{P}(\mathcal{X})} \{V(\mathcal{W} \parallel P^* \mathcal{W} | P) : D(\mathcal{W} \parallel P^* \mathcal{W} | P) \geq C_{\mathcal{W}} - \delta\}. \quad (3.36)$$

Note that the map  $\delta \mapsto v(\delta)$  is monotone decreasing and continuous at 0 from above, i.e.  $\lim_{\delta \downarrow 0} v(\delta) = v(0) = V_{\mathcal{W}}$  [7, Lemma 22]. For any  $\kappa \in (0, 1)$ , we can choose a sufficiently small  $\gamma > 0$  independent of the sequence  $\mathbf{x}^n$  such that  $v(\gamma) \geq (1 - \kappa)V_{\mathcal{W}} =: \nu > 0$ . Further, let  $N_2 \in \mathbb{N}$  such that  $a_n \leq \gamma$  for all  $n \geq N_2$ . Then, one finds, for all  $\mathbf{x}^n \in \Omega_{\text{good}}$  and  $n \geq N_2$ ,

$$V(\mathcal{W} \parallel P^* \mathcal{W} | P_{\mathbf{x}^n}) \geq v(\gamma) \geq \nu > 0. \quad (3.37)$$

Moreover, since  $V_{\mathcal{W}} > 0$  implies that  $C_{\mathcal{W}} = \max_{P \in \mathcal{P}(\mathcal{X})} D(\mathcal{W} \parallel P^* \mathcal{W} | P) > \max_{P \in \mathcal{P}} D_0(\mathcal{W} \parallel P^* \mathcal{W} | P)$ , one can choose a sufficiently large  $n$ , say  $N_3 \in \mathbb{N}$ , such that  $R_n > D_0(\mathcal{W} \parallel P^* \mathcal{W} | P_{\mathbf{x}^n})$  for all  $n \geq N_3$ . Now, we have for all  $\mathbf{x}^n \in \Omega_{\text{good}}$  and  $n \geq \max\{N_2, N_3\}$  that

$$\max_{P \in \mathcal{P}(\mathcal{X})} D_0(\mathcal{W} \parallel P^* \mathcal{W} | P) < R_n < D(\mathcal{W} \parallel P^* \mathcal{W} | P_{\mathbf{x}^n}); \quad (3.38)$$

$$0 < \nu \leq V(\mathcal{W} \parallel P^* \mathcal{W} | P_{\mathbf{x}^n}). \quad (3.39)$$

Together with Eqs. (3.18) and (3.37) and letting  $\sigma = P^* \mathcal{W}$ , Proposition 7 yields, for all  $\mathbf{x}^n \in \Omega_{\text{good}}$  and all sufficiently large  $n$ , say  $n \geq N_4 \in \mathbb{N}$ ,

$$\frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \parallel (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\frac{E_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, P^* \mathcal{W})}{a_n^2} - \frac{\log s_n^* \sqrt{n}}{na_n^2} + \frac{\log A}{na_n^2}. \quad (3.40)$$

Recall Eq. (3.48) in Proposition 8 below with  $b_n = 0$  and  $\delta_n = a_n + c_n$  that  $\limsup_{n \rightarrow +\infty} \frac{s_n^*}{a_n + c_n} \leq \frac{1}{V_{\mathcal{W}}}$ . Hence, one can fix an arbitrary  $\zeta > 0$  and there exists an  $N_5 \in \mathbb{N}$  such that  $\frac{s_n^* \sqrt{n}}{(a_n + c_n) \sqrt{n}} \leq \frac{1}{V_{\mathcal{W}}} + \zeta$  for all  $n \geq N_5$ . This then leads to for all sufficiently large  $n \geq \max\{N_2, N_3, N_4, N_5\}$  and all  $\mathbf{x}^n \in \Omega_{\text{good}}$ ,

$$\frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \parallel (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\frac{E_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, P^* \mathcal{W})}{a_n^2} - \frac{\log(a_n + c_n) \sqrt{n}}{na_n^2} + \frac{\log \frac{A}{\frac{1}{V_{\mathcal{W}}} + \zeta}}{na_n^2}. \quad (3.41)$$

Taking  $n \rightarrow +\infty$ , the second and the third terms on the right-hand side of Eq. (3.41) vanish since  $c_n = K \frac{\log n}{n} = o(a_n)$  and the assumption  $\lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty$ .

<sup>3</sup>Note that  $D_0(\mathcal{W} \parallel \sigma | P) = D(\mathcal{W} \parallel \sigma | P)$  implies  $W_x = \sigma$  for all  $x \in \text{supp}(P)$  [46, Corollary 4.1]. This further gives  $V(\mathcal{W} \parallel \sigma | P) = 0$ . However, the assumption in Eq. (3.33) ensures that  $\liminf_{n \in \mathbb{N}} D(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n}) - D_0(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n}) > 0$ . Hence, the intervals  $[D_0(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n}), D(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n})]$  for all  $\mathbf{x}^n$  satisfying Eq. (3.33) are not measure zero.

Next, we apply Eq. (3.46) in Proposition 8 again to bound the error-exponent function  $E_{\text{sp}}^{(2)}$  in Eq. (3.40): for all  $\mathbf{x}^n \in \Omega^{(3)}$

$$\liminf_{n \rightarrow +\infty} \frac{\log \hat{\alpha}_{\exp\{-nR_n\}} (W_{\mathbf{x}^n}^{\otimes n} \| (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq - \limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_{\mathbf{x}^n}, P^* \mathcal{W})}{a_n^2} \quad (3.42)$$

$$= - \limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_{\mathbf{x}^n}, P^* \mathcal{W})}{\delta_n^2} \quad (3.43)$$

$$\geq -\frac{1}{2V_{\mathcal{W}}}. \quad (3.44)$$

Finally, combining Eqs. (3.18), (3.29), (3.32) and (3.44) concludes the desired Eq. (3.3).

**Proposition 8** (Error Exponent around Capacity). *Let  $(b_n)_{n \in \mathbb{N}}$  be a sequence of real numbers with  $\lim_{n \rightarrow +\infty} b_n = 0$  and let  $(\delta_n)_{n \in \mathbb{N}}$  be a sequence of positive numbers with  $\lim_{n \rightarrow +\infty} \delta_n = 0$ . Suppose the sequence of distributions  $(P_n)_{n \in \mathbb{N}}$  satisfies*

$$C_{\mathcal{W}} - \delta_n < D(\mathcal{W} \| P^* \mathcal{W} | P_n) \leq C_{\mathcal{W}} - b_n. \quad (3.45)$$

The following hold:

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W})}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2V_{\mathcal{W}} \delta_n^2}; \quad (3.46)$$

$$\limsup_{n \rightarrow +\infty} \frac{\tilde{E}_{\text{sp}}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W})}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2\tilde{V}_{\mathcal{W}} \delta_n^2}; \quad (3.47)$$

$$\limsup_{n \rightarrow +\infty} \frac{s_n^*}{\delta_n} \leq \frac{1}{V_{\mathcal{W}}}, \quad (3.48)$$

where

$$s_n^* := \arg \max_{s \geq 0} \{E_{\text{h}}(s, P_n, P^* \mathcal{W}) - s(C_{\mathcal{W}} - \delta_n)\}. \quad (3.49)$$

The proof of Proposition 8 is provided in Appendix D. □

#### 4. MODERATE DEVIATIONS FOR QUANTUM HYPOTHESIS TESTING

In this section, we show that a special case of channel coding yields the moderate deviation result for quantum hypothesis testing. The achievability part is given in Theorem 9. In Section 4.1, we provide two proofs. The first proof follows the idea of asymptotic expansions in Theorem 4; however, we will employ Audenaert *et al.*'s quantum Hoeffding bound [30], instead of Hayashi's inequality [27]. The second proof relies on a martingale inequality [24]. The converse part and its proof are provided in Theorem 10 and Section 4.2, respectively.

**Theorem 9** (Achievability). *Let  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  be the density operators with finite relative variance  $V := V(\rho \| \sigma) > 0$ . For any sequence of real numbers  $(a_n)_{n \in \mathbb{N}}$  satisfying Eq. (3.1), there exists a sequence  $r_n := D(\rho \| \sigma) - a_n$  such that*

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \hat{\alpha}_{\exp\{-nr_n\}} (\rho^{\otimes n} \| \sigma^{\otimes n}) \leq -\frac{1}{2V}. \quad (4.1)$$

**Theorem 10** (Converse). *Let  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  be the density operators with non-zero and finite relative variance  $V := V(\rho \| \sigma) > 0$ . For any sequence of real numbers  $\{a_n\}_{n \in \mathbb{N}}$  satisfying Eq. (3.1), there exists a sequence  $r_n := D(\rho \| \sigma) - a_n$  such that*

$$\liminf_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \hat{\alpha}_{\exp\{-nr_n\}} (\rho^{\otimes n} \| \sigma^{\otimes n}) \geq -\frac{1}{2V}. \quad (4.2)$$

**4.1. Proof of Achievability: Theorem 9.** In this section, we present two proofs for Theorem 9. The first one relies on the quantum Hoeffding bound [30] and the Taylor's expansion of the exponent function  $E_h$ .

*The first proof of Theorem 9.* Recall the following achievability of the quantum Hoeffding bound:

**Lemma 11** (Theorem 5, Section 5.5 of [30]). *Let  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ . For any  $r \geq 0$  and any  $n \in \mathbb{N}$ , we have*

$$\hat{\alpha}_{\exp\{-nr\}}(\rho^{\otimes n} \parallel \sigma^{\otimes n}) \leq \exp \left\{ -n \left[ \sup_{0 < \alpha \leq 1} \left\{ \frac{\alpha - 1}{\alpha} (r - D_\alpha(\rho \parallel \sigma)) \right\} \right] \right\}. \quad (4.3)$$

Since  $D(\rho \parallel \sigma) > 0$  (due to Eq. (2.12)), we have

$$r_n := D(\rho \parallel \sigma) - a_n > 0 \quad (4.4)$$

for all sufficiently large  $n$ . Choose such  $n$  onwards, then Eq. (4.3) implies that:

$$\frac{1}{na_n^2} \log \hat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n} \parallel \sigma^{\otimes n}) \leq -\frac{1}{a_n^2} \sup_{0 < \alpha \leq 1} \left\{ \frac{\alpha - 1}{\alpha} (r_n - D_\alpha(\rho \parallel \sigma)) \right\} \quad (4.5)$$

$$= -\frac{1}{a_n^2} \sup_{s \geq 0} \{E_h(s) - sr_n\}, \quad (4.6)$$

where we substitute  $s = \frac{1-\alpha}{\alpha}$  and let

$$E_h(s) := sD_{\frac{1}{1+s}}(\rho \parallel \sigma). \quad (4.7)$$

Taylor's theorem followed by simple calculation yields

$$E_h(s) = sD(\rho \parallel \sigma) - \frac{s^2}{2}V + \frac{s^3}{6} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}} \quad (4.8)$$

for some  $\bar{s} \in [0, s]$  and all  $s \geq 0$ . The above equation is also a simple consequence of items (c) and (e) in Proposition 2. Now let  $s_n = a_n/V$ , for all  $n \in \mathbb{N}$ . Then for all sufficiently large  $n$  and for some  $\bar{s}_n \in [0, s_n]$ , Eq. (4.8) yields

$$\sup_{s \geq 0} \{E_h(s) - sr_n\} \geq E_h(s_n) - s_n r_n \quad (4.9)$$

$$= \frac{a_n}{V} (D(\rho \parallel \sigma) - r_n) - \frac{a_n^2}{2V} + \frac{a_n^3}{6V^3} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}_n} \quad (4.10)$$

$$= \frac{a_n^2}{2V} + \frac{a_n^3}{6V^3} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}_n}, \quad (4.11)$$

where we substitute  $r_n = D(\rho \parallel \sigma) - a_n$  in Eq. (4.11).

Define

$$\Upsilon := \max_{s \in [0, 1]} \left| \frac{\partial^3 E_h(s)}{\partial s^3} \right|, \quad (4.12)$$

which is finite. Therefore, Eq. (4.11) leads to

$$\sup_{s \geq 0} \{E_h(s) - sr_n\} \geq \frac{a_n^2}{2V} + \frac{a_n^3}{6V^3} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}_n} \quad (4.13)$$

$$\geq \frac{a_n^2}{2V} - \frac{a_n^3}{6V^3} \Upsilon \quad (4.14)$$

for all sufficiently large  $n$ . Substituting Eq. (4.14) into Eq. (4.6) yields

$$\frac{1}{na_n^2} \log \hat{\alpha}_{\exp\{-nr_n\}}(\rho \parallel \sigma) \leq -\frac{1}{2V} \left( 1 - \Upsilon \frac{a_n}{3V^2} \right), \quad (4.15)$$

which implies the desired achievability part:

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \hat{\alpha}_{\exp\{-nr_n\}}(\rho \parallel \sigma) \leq -\frac{1}{2V}. \quad (4.16)$$

□

In the following, we give an alternative proof of Theorem 9 by employing a martingale inequality [24].

*The second proof of Theorem 9.* We follow the idea in Ref. [6] to write the eigendecomposition of  $\rho^{\otimes n}$  and  $\sigma^{\otimes n}$ , respectively, as

$$\rho^{\otimes n} = \sum_{x^n} \lambda^n(x^n) |f_{x^n}^n\rangle\langle f_{x^n}^n|; \quad \sigma^{\otimes n} = \sum_{y^n} \gamma^n(y^n) |g_{y^n}^n\rangle\langle g_{y^n}^n|, \quad (4.17)$$

where  $x^n := x_1 x_2 \dots x_n$ ;  $y^n := y_1 y_2 \dots y_n$ ;  $\lambda^n(x^n) = \prod_{i=1}^n \lambda(x_i)$ ;  $\mu^n(y^n) = \prod_{i=1}^n \mu(y_i)$ ;  $|f_{x^n}^n\rangle = |f_{x_1}\rangle \otimes |f_{x_2}\rangle \otimes \dots \otimes |f_{x_n}\rangle$ ; and  $|g_{y^n}^n\rangle = |g_{y_1}\rangle \otimes |g_{y_2}\rangle \otimes \dots \otimes |g_{y_n}\rangle$ . Further, we define a pair of random variables  $(X, Y)$  via the Nussbaum-Szkoła mapping [58], i.e.  $P_{X,Y}(x, y) = \lambda(x) |\gamma_{xy}|^2$ , where  $\gamma_{xy} := \langle g_y | f_x \rangle \in \mathbb{C}$ . It is well-known that

$$D(\rho \| \sigma) = D(\lambda(X) \| \mu(Y)) = \mathbb{E}_{(X,Y)} \left[ \log \frac{\lambda(X)}{\mu(Y)} \right], \quad (4.18)$$

$$V(\rho \| \sigma) = V(\lambda(X) \| \mu(Y)) = \text{Var}_{(X,Y)} \left[ \log \frac{\lambda(X)}{\mu(Y)} \right]. \quad (4.19)$$

Let  $T_n := \exp\{nr_n\}$ . For every sequence  $x^n$ , we define a sub-normalized vector:

$$|\xi_{x^n}^n\rangle := \sum_{y^n: \lambda^n(x^n)/\mu^n(y^n) \geq T_n} \gamma_{x^n y^n}^n |g_{y^n}^n\rangle \quad (4.20)$$

with  $\gamma_{x^n y^n}^n = \prod_{i=1}^n \gamma_{x_i y_i}$  and  $\sum_x |\gamma_{xy}|^2 = \sum_y |\gamma_{xy}|^2 = 1$ . Applying the Gram-Schmidt orthonormalization process on  $\{|\xi_{x^n}^n\rangle\}_{x^n}$  to obtain an orthonormal vectors

$$|\hat{\xi}_{x^n}^n\rangle = \sum_{y^n: \lambda^n(x^n)/\mu^n(y^n) \geq T_n} t_{x^n y^n}^n |g_{y^n}^n\rangle \quad (4.21)$$

for some  $t_{x^n y^n}^n \in \mathbb{C}$  and

$$\sum_{y^n: \lambda^n(x^n)/\mu^n(y^n) \geq T_n} |t_{x^n y^n}^n|^2 = 1. \quad (4.22)$$

We define a test of the hypotheses by

$$Q_n := \sum_{x^n} |\hat{\xi}_{x^n}^n\rangle\langle \hat{\xi}_{x^n}^n|. \quad (4.23)$$

Then, it suffices to show  $\beta(Q_n; \sigma^{\otimes n}) \leq \exp\{-nr_n\}$  and

$$\lim_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \alpha(Q_n; \rho^{\otimes n}) \leq -\frac{1}{2V} \quad (4.24)$$

to complete the proof. The former follows Eqs. (4.17), (4.21), and (4.22):

$$\begin{aligned} \beta(Q_n; \sigma^{\otimes n}) &= \sum_{x^n} \text{Tr} \left[ \sigma^{\otimes n} |\hat{\xi}_{x^n}^n\rangle\langle \hat{\xi}_{x^n}^n| \right] \\ &= \sum_{x^n} \sum_{y^n: \lambda^n(x^n)/\mu^n(y^n) \geq T_n} |t_{x^n y^n}^n|^2 \mu^n(y^n) \\ &\leq \sum_{x^n} \frac{\lambda^n(x^n)}{T_n} = \frac{1}{T_n} = \exp\{-nr_n\}. \end{aligned} \quad (4.25)$$



Likewise, since  $\frac{|\langle \xi_{x^n} \rangle \langle \xi_{x^n} \rangle|}{|\langle \xi_{x^n} | \xi_{x^n} \rangle|^2} \leq Q_n$ , one can verify that

$$\alpha(Q_n; \rho^{\otimes n}) \leq 1 - \sum_{x^n} \lambda^n(x^n) \langle \xi_{x^n}^n | \xi_{x^n}^n \rangle \quad (4.26)$$

$$= \Pr \left\{ \frac{\lambda^n(X^n)}{\mu^n(Y^n)} < T_n \right\} \quad (4.27)$$

$$= \Pr \left\{ \log \frac{\lambda^n(X^n)}{\mu^n(Y^n)} < nr_n \right\}. \quad (4.28)$$

Next, we adopt Sason's approach [24] to construct a martingale sequence  $\{U_k, \mathfrak{M}_k\}_{k=0}^n$ , where  $\mathfrak{M}_k$  denotes the sigma-algebra formed by  $(X_l, Y_l)_{l=1}^k$ ;  $\mathfrak{M}_0 \subseteq \mathfrak{M}_1 \subseteq \dots \subseteq \mathfrak{M}_n$  is the filtration; and

$$U_k := \mathbb{E}_{(X^n, Y^n)} \left[ \log \frac{\lambda^n(X^n)}{\mu^n(Y^n)} \middle| \mathfrak{M}_k \right] \quad (4.29)$$

$$= \sum_{i=1}^k \log \frac{\lambda(X_i)}{\mu(Y_i)} + \sum_{i=k+1}^n \mathbb{E}_{X^n} \left[ \log \frac{\lambda(X_i)}{\mu(Y_i)} \right] \quad (4.30)$$

$$= \sum_{i=1}^k \log \frac{\lambda(X_i)}{\mu(Y_i)} + (n-k)D(\lambda(X) \parallel \mu(Y)). \quad (4.31)$$

In particular, we have

$$U_0 = nD(\lambda(X) \parallel \mu(Y)); \quad U_n = \log \frac{\lambda(X^n)}{\mu(Y^n)} = \sum_{i=1}^n \log \frac{\lambda(X_i)}{\mu(Y_i)}.$$

Hence, it can be verified that:

$$\begin{aligned} U_k - U_{k-1} &= \log \frac{\lambda(X_k)}{\mu(Y_k)} - D(\lambda(X) \parallel \mu(Y)); \\ \mathbb{E}_{X^n} [U_k - U_{k-1} | \mathfrak{M}_{k-1}] &= 0; \\ \mathbb{E}_{X^n} [(U_k - U_{k-1})^2 | \mathfrak{M}_{k-1}] &= V(\lambda(X) \parallel \mu(Y)) = V. \end{aligned}$$

Let

$$b := \max_{(x,y): x=y} \left| \log \frac{\lambda(x)}{\mu(y)} - D(\lambda(X) \parallel \mu(Y)) \right|, \quad (4.32)$$

which is a finite number due to the assumption of the finite-dimensional Hilbert space. Then, we have  $|U_k - U_{k-1}| \leq b$  almost surely for every  $k \in [n]$ . Equipped with the notation above, Eq. (4.28) can be expressed as:

$$\alpha(Q_n; \rho^{\otimes n}) = \Pr \{U_n - U_0 \leq -na_n\}. \quad (4.33)$$

In the following, we borrow the idea from Sason [24] to employ a martingale inequality to upper bound Eq. (4.33).

**Theorem 12** (Refined Azuma's Inequality [24, Theorem 2]). *Let  $(X_k)_{k=1}^n$  be a martingale with respect to the filtration  $(\mathfrak{M}_k)_{k=0}^n$  such that the following requirements are satisfied almost surely: (i)  $\mathbb{E}[X_k | \mathfrak{M}_{k-1}] = 0$ ; (ii)  $\mathbb{E}[X_k^2 | \mathfrak{M}_{k-1}] \leq v$ ; (iii)  $\|X_k\|_\infty \leq b_k$ . For any  $x \geq 0$ ,*

$$\begin{aligned} \Pr \left\{ \sum_{k=1}^n X_k \geq xn \right\} &= \Pr \left\{ \sum_{k=1}^n X_k \leq -xn \right\} \\ &\leq 2 \exp \left\{ -nh \left( \frac{bx + v}{b^2 + v} \parallel \frac{v}{b^2 + v} \right) \right\}, \end{aligned} \quad (4.34)$$

where  $h(p \parallel q) := p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q}$ .

Apply Theorem 12 to Eq. (4.33) with  $x = a_n$ ,  $X_k = U_k - U_{k-1}$  for ever  $k \in [n]$ :

$$\alpha(Q_n; \rho^{\otimes n}) \leq 2 \exp \left\{ -nh \left( \frac{ba_n + V}{b^2 + V} \parallel \frac{V}{b^2 + V} \right) \right\}. \quad (4.35)$$

By using a scalar inequality [24, Lemma 1]:

$$(1 + u) \log(1 + u) \geq u + \frac{u^2}{2} - \frac{u^3}{6}, \quad u \geq 0, \quad (4.36)$$

and the definition of  $h(\cdot \parallel \cdot)$  in Theorem 12, Eq. (4.35) leads to

$$\alpha(Q_n; \rho^{\otimes n}) \leq 2 \exp \left\{ -n \left[ \frac{a_n^2}{2V} \left( 1 - \frac{a_n b}{3V(1 + V/b^2)} \right) \right] \right\}. \quad (4.37)$$

Finally, recall that  $\lim_{n \rightarrow +\infty} a_n = 0$  in Eq. (3.1), then

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \alpha_n(\eta_n) \leq -\frac{1}{2V}.$$

□

**4.2. Proof of Converse: Theorem 10.** The converse part is a direct consequence of the sharp converse Hoeffding bound, Theorem 7.

Let  $\mathcal{X} = \{x\}$  and  $W_x = \rho$ . We apply Theorem 7 with  $r = r_n$  to obtain

$$\hat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n} \parallel \sigma^{\otimes n}) \geq \frac{A}{s_n^* \sqrt{n}} \exp \left\{ -n \left[ \sup_{0 < \alpha \leq 1} \frac{\alpha - 1}{\alpha} (r_n - c_n - D_\alpha(\rho \parallel \sigma)) \right] \right\}, \quad (4.38)$$

for sufficiently large  $n \in \mathbb{N}$  and some constant  $A > 0$ . Here

$$s_n^* := \arg \max_{s \geq 0} \left\{ s D_{\frac{1}{1+s}}(\rho \parallel \sigma) - s r_n \right\}. \quad (4.39)$$

Now let

$$\delta_n := a_n + c_n, \quad \forall n \in \mathbb{N}, \quad (4.40)$$

and invoke Proposition 8 with  $W_x = \rho$ ,  $P(x) = 1$ , and substitute  $P^* \mathcal{W}$  with  $\sigma$  to obtain

$$\limsup_{n \rightarrow +\infty} \frac{\sup_{s \geq 0} \left\{ -s (D(\rho \parallel \sigma) - \delta_n) + s D_{\frac{1}{1+s}}(\rho \parallel \sigma) \right\}}{\delta_n^2} \leq \frac{1}{2V}. \quad (4.41)$$

Moreover, Eq. (3.48) in Proposition 8 gives that  $\lim_{n \rightarrow +\infty} \frac{s_n^*}{\delta_n} = 1/V$ . Combining Eqs. (4.38) and (4.41) concludes our claim:

$$\liminf_{n \rightarrow +\infty} \frac{\log \hat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n} \parallel \sigma^{\otimes n})}{n \delta_n^2} \geq -\frac{1}{2V}. \quad (4.42)$$

## 5. CONCLUSION

A practical question in quantum information theory is that—is it possible for a reliable communication through a c-q channel when the transmission rate approaches capacity in blocklength? In this paper, we propose a moderate deviation analysis for c-q channel and thus give an affirmative answer. Moreover, we also establish the moderate deviations for quantum hypothesis testing.

Our proof strategy is based on a strong large deviation theory [28, 18] and the study of the asymptotic behaviour of the error exponent function. As a result, we successfully bridge the connection between small error regime and the medium error regime. On the other hand, the recent work from the authors [31] also obtains the moderate deviation result via the techniques in the non-vanishing error regime. It is remarkable that both methods from different regimes arrive at the same place, and hence both this work along with Ref. [31] illuminate the whole picture of the three regimes in quantum information theory. □

## ACKNOWLEDGEMENTS

MH is supported by an ARC Future Fellowship under Grant FT140100574. We would like to thank Vincent Tan for introducing us to Altuğ and Wagner's work of moderate deviation analysis. We also thank Christopher Chubb and Marco Tomamichel for the insightful discussions and the useful comments.

## APPENDIX A. PROPERTIES OF AUXILIARY FUNCTIONS

This section contains proofs of Propositions 1 and 2. Most results follow from properties of Petz quantum Rényi divergence [43] (see also [44, 45, 46]).

### A.1. Proof of Proposition 1.

**Proposition 1** (Properties of  $\tilde{E}_0(s, P, \sigma)$ ). *For any classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , the modified auxiliary function  $\tilde{E}_0(s, P, \sigma)$  admits the following properties.*

- (a)  $\tilde{E}_0(s, P, \sigma)$  and its partial derivatives  $\partial \tilde{E}_0(s, P, \sigma) / \partial s$ ,  $\partial^2 \tilde{E}_0(s, P, \sigma) / \partial s^2$ ,  $\partial^3 \tilde{E}_0(s, P, \sigma) / \partial s^3$  are all continuous in  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .
- (b) For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $\tilde{E}_0(s, P, \sigma)$  is concave in  $s \in \mathbb{R}_{\geq 0}$ .
- (c) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \right|_{s=0} = D(P \circ \mathcal{W} \| P \otimes \sigma) \quad (\text{A.1})$$

- (d) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\lim_{s \rightarrow +\infty} \frac{\partial \tilde{E}_0(s, P)}{\partial s} \leq \frac{\partial \tilde{E}_0(s, P)}{\partial s} \leq D(P \circ \mathcal{W} \| P \otimes \sigma), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (\text{A.2})$$

- (e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 \tilde{E}_0(s, P)}{\partial s^2} \right|_{s=0} = -V(P \circ \mathcal{W} \| P \otimes \sigma). \quad (\text{A.3})$$

*Proof of Proposition 1.*

- (1-(a)) The continuity can be proved by the standard approach of functional calculus (see e.g. [44, Lemma III.1] and [45, Section 4.2]). Let  $\tilde{F}(s) := \sum_{x \in \mathcal{X}} P(x) \text{Tr} [W_x^{1-s}(\sigma)^s]$ . Direct calculation shows that

$$\frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} = -\frac{\tilde{F}'(s)}{\tilde{F}(s)}, \quad (\text{A.4})$$

$$\frac{\partial^2 \tilde{E}_0(s, P, \sigma)}{\partial s^2} = -\frac{\tilde{F}''(s)}{\tilde{F}(s)} + \left( \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \right)^2, \quad (\text{A.5})$$

$$\frac{\partial^3 \tilde{E}_0(s, P, \sigma)}{\partial s^3} = -\frac{\tilde{F}'''(s)}{\tilde{F}(s)} + 3 \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \frac{\partial^2 \tilde{E}_0(s, P, \sigma)}{\partial s^2} - \left( \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \right)^3, \quad (\text{A.6})$$

and

$$\tilde{F}'(s) = \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} [-W_x^{1-s} \log(W_x)(\sigma)^s + W_x^{1-s}(\sigma)^s \log(\sigma)], \quad (\text{A.7})$$

$$\begin{aligned} \tilde{F}''(s) = \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} [ & W_x^{1-s} \log^2(W_x)(\sigma)^s - W_x^{1-s} \log(W_x)(\sigma)^s \log(\sigma) \\ & - W_x^{1-s} \log(W_x)(\sigma)^s \log(\sigma) + W_x^{1-s}(\sigma)^s \log^2(\sigma) ], \end{aligned} \quad (\text{A.8})$$

$$\begin{aligned} \tilde{F}'''(s) = \sum_{x \in \mathcal{X}} P(x) \operatorname{Tr} [ & -W_x^{1-s} \log^3(W_x)(\sigma)^s + W_x^{1-s} \log^2(W_x)(\sigma)^s \log(\sigma) \\ & + 2W_x^{1-s} \log^2(W_x)(\sigma)^s \log(\sigma) - 2W_x^{1-s} \log(W_x)(\sigma)^s \log^2(\sigma) \\ & - W_x^{1-s} \log(W_x)(\sigma)^s \log^2(\sigma) + W_x^{1-s}(\sigma)^s \log^3(\sigma) ]. \end{aligned} \quad (\text{A.9})$$

Since the matrix power function is continuous (with respect to the strong topology; see e.g. [47, Theorem 1.19]), we conclude the continuity of the partial derivatives Eqs. (A.4)-(A.6) in item (a).

(1-(b)) The claim follows from the concavity of the map  $s \mapsto sD_{1-s}(\cdot \| \cdot)$  (see e.g. [48, Lemma III.11]).

(1-(c)) The results can be derived from evaluating Eqs. (A.4), (A.5), (A.7), and (A.8) at  $s = 0$ . We provide an alternative proof here. One can verify

$$\left. \frac{\partial \tilde{E}_0(s, P, \sigma)}{\partial s} \right|_{s=0} = D_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) - sD'_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (\text{A.10})$$

$$= D_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (\text{A.11})$$

$$= D(P \circ \mathcal{W} \| P \otimes \sigma). \quad (\text{A.12})$$

(1-(d)) The concavity of the map  $s \mapsto \tilde{E}(s, P, \sigma)$  in item (b) ensures that  $\partial \tilde{E}(s, P, \sigma) / \partial s$  is non-increasing in  $s$ . Along with Eq. (A.12), we conclude Eq. (2.30).

(1-(e)) Following from item (c), one obtain

$$\left. \frac{\partial^2 \tilde{E}_0(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -2D'_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) + sD''_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (\text{A.13})$$

$$= -2D'_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (\text{A.14})$$

$$= -V(P \circ \mathcal{W} \| P \otimes \sigma), \quad (\text{A.15})$$

where the last equality (A.15) follows from the fact  $D'_{1/1+s}(\cdot \| \cdot) \Big|_{s=0} = V(\cdot \| \cdot) / 2$  [45, Theorem 2].

□

## A.2. Proof of Proposition 2.

**Proposition 2** (Properties of  $E_h(s, P, \sigma)$ ). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \operatorname{supp}(P)$ . Then  $E_h(s, P, \sigma)$  defined in Eq. (2.26) enjoys the following properties.*

- (a) *The partial derivatives  $\partial E_h(s, P, \sigma) / \partial s$ ,  $\partial^2 E_h(s, P, \sigma) / \partial s^2$ ,  $\partial^3 E_h(s, P, \sigma) / \partial s^3$ , and  $E_h(s, P)$  are all continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .*
- (b) *For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $E_h(s, P, \sigma)$  is concave in  $s$  for all  $s \in \mathbb{R}_{\geq 0}$ .*
- (c) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\left. \frac{\partial E_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W} \| \sigma | P). \quad (\text{A.16})$$

- (d) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\lim_{s \rightarrow +\infty} \frac{\partial E_h(s, P, \sigma)}{\partial s} \leq \frac{\partial E_h(s, P, \sigma)}{\partial s} \leq D(\mathcal{W} \| \sigma | P), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (\text{A.17})$$

(e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 E_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -V(\mathcal{W} \parallel \sigma | P). \quad (\text{A.18})$$

*Proof Proposition 2.*

(2-(a)) Direct calculation yields that

$$\frac{\partial E_h(s, P, \sigma)}{\partial s} = D_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) - \frac{s}{(1+s)^2} D'_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) \quad (\text{A.19})$$

$$\frac{\partial^2 E_h(s, P, \sigma)}{\partial s^2} = -\frac{2}{(1+s)^3} D'_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) + \frac{s}{(1+s)^4} D''_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) \quad (\text{A.20})$$

$$\begin{aligned} \frac{\partial^3 E_h(s, P, \sigma)}{\partial s^3} &= \frac{6}{(1+s)^4} D'_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) + \frac{3-3s}{(1+s)^5} D''_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) \\ &\quad - \frac{s}{(1+s)^6} D'''_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P). \end{aligned} \quad (\text{A.21})$$

From Eqs. (A.19)-(A.21) and the fact that  $D_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$ ,  $D'_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$ ,  $D''_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$ , and  $D'''_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$  are continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ , we deduce the continuity property in item (a).

(2-(b)) The proof strategy follows closely with [48, Appendix B]. Let  $\psi(\alpha) = \sum_{x \in \mathcal{X}} P(x) \log \text{Tr} [W_x^\alpha \sigma^{1-\alpha}]$ . Since  $\alpha \mapsto \psi(\alpha)$  is convex for all  $\alpha \in (0, 1]$  [48, Lemma III.11], it can be written as the supremum of affine functions, i.e.

$$\psi(\alpha) = \sup_{i \in \mathcal{I}} \{c_i \alpha + d_i\} \quad (\text{A.22})$$

for some index set  $\mathcal{I}$ . Hence,

$$-E_h(s, P, \sigma) = (1+s) \psi \left( \frac{1}{1+s} \right) = \sup_{i \in \mathcal{I}} \{c_i + d_i(1+s)\}. \quad (\text{A.23})$$

The right-hand side of Eq. (A.23), in turn, implies that the map  $s \mapsto E_h(s, P, \sigma)$  is convex for all  $s \in \mathbb{R}_{\geq 0}$ .

(2-(c)) From Eqs. (A.19) and (A.20), one finds

$$\left. \frac{\partial E_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W} \parallel \sigma | P). \quad (\text{A.24})$$

(2-(d)) The concavity of the map  $s \mapsto E_h(s, P, \sigma)$  in item (b) ensures that  $\partial E_h(s, P, \sigma)/\partial s$  is non-increasing in  $s$ . Along with Eq. (A.24) in item (c), we conclude Eq. (2.33).

(2-(e)) Applying  $D'_{1/(1+s)}(\cdot \parallel \cdot)|_{s=0} = V(\cdot \parallel \cdot)/2$  [45, Theorem 2], it holds that

$$\left. \frac{\partial^2 E_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -V(\mathcal{W} \parallel \sigma | P). \quad (\text{A.25})$$

□

### A.3. Proof of Proposition 3.

**Proposition 3** (Properties of  $\tilde{E}_h(s, P, \sigma)$ ). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \text{supp}(P)$ . Then  $\tilde{E}_h(s, P, \sigma)$  defined in Eq. (2.27) enjoys the following properties.*

- (a) *The partial derivatives  $\partial \tilde{E}_h(s, P, \sigma)/\partial s$ ,  $\partial^2 \tilde{E}_h(s, P, \sigma)/\partial s^2$ ,  $\partial^3 \tilde{E}_h(s, P, \sigma)/\partial s^3$ , and  $\tilde{E}_h(s, P, \sigma)$  are all continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .*
- (b) *For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $\tilde{E}_h(s, P, \sigma)$  is concave in  $s$  for all  $s \in \mathbb{R}_{\geq 0}$ .*

(c) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W} \parallel \sigma | P). \quad (\text{A.26})$$

(d) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\lim_{s \rightarrow +\infty} \frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} \leq \frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} \leq D(\mathcal{W} \parallel \sigma | P), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (\text{A.27})$$

(e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 \tilde{E}_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -\tilde{V}(\mathcal{W} \parallel \sigma | P). \quad (\text{A.28})$$

*Proof of Proposition 3.* This proof follows similarly from Proposition 2.

(3-(a)) Direct calculation yields that

$$\frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} = \tilde{D}_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) - \frac{s}{(1+s)^2} \tilde{D}'_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) \quad (\text{A.29})$$

$$\frac{\partial^2 \tilde{E}_h(s, P, \sigma)}{\partial s^2} = -\frac{2}{(1+s)^3} \tilde{D}'_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) + \frac{s}{(1+s)^4} \tilde{D}''_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) \quad (\text{A.30})$$

$$\begin{aligned} \frac{\partial^3 \tilde{E}_h(s, P, \sigma)}{\partial s^3} &= \frac{6}{(1+s)^4} \tilde{D}'_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) + \frac{3-3s}{(1+s)^5} \tilde{D}''_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P) \\ &\quad - \frac{s}{(1+s)^6} \tilde{D}'''_{\frac{1}{1+s}}(\mathcal{W} \parallel \sigma | P). \end{aligned} \quad (\text{A.31})$$

From Eqs. (A.29)-(A.31) and the fact that  $\tilde{D}_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$ ,  $\tilde{D}'_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$ ,  $\tilde{D}''_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$ , and  $\tilde{D}'''_{1/(1+s)}(\mathcal{W} \parallel \sigma | P)$  are continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ , we deduce the continuity property in item (a).

(3-(b)) The proof strategy follows closely with [48, Appendix B]. Let

$$\tilde{\psi}(\alpha) = \sum_{x \in \mathcal{X}} P(x) \log \text{Tr} \left[ e^{\alpha \log W_x + (1-\alpha) \log \sigma} \right]. \quad (\text{A.32})$$

Since  $\alpha \mapsto \tilde{\psi}(\alpha)$  is convex for all  $\alpha \in (0, 1]$  [48, Lemma III.11], it can be written as the supremum of affine functions, i.e.

$$\tilde{\psi}(\alpha) = \sup_{i \in \mathcal{I}} \{c_i \alpha + d_i\} \quad (\text{A.33})$$

for some index set  $\mathcal{I}$ . Hence,

$$-\tilde{E}_h(s, P, \sigma) = (1+s) \tilde{\psi} \left( \frac{1}{1+s} \right) = \sup_{i \in \mathcal{I}} \{c_i + d_i(1+s)\}. \quad (\text{A.34})$$

The right-hand side of Eq. (A.34), in turn, implies that the map  $s \mapsto \tilde{E}_h(s, P, \sigma)$  is convex for all  $s \in \mathbb{R}_{\geq 0}$ .

(3-(c)) From Eqs. (A.29) and (A.30) and recalling [48, Lemma III.4], one finds

$$\left. \frac{\partial \tilde{E}_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W} \parallel \sigma | P). \quad (\text{A.35})$$

(3-(d)) The concavity of the map  $s \mapsto E_h(s, P)$  in item (b) ensures that  $\partial E_h(s, P)/\partial s$  is non-increasing in  $s$ . Along with Eq. (A.35) in item (c), we conclude Eq. (2.36).

(3-(e)) Following similar steps in [45, Proposition 4], it can be verified that

$$\tilde{D}'_\alpha(\rho\|\sigma)\Big|_{\alpha=1} = \lim_{\alpha \uparrow 1} \frac{1}{2} \frac{d^2}{d\alpha^2} \log f(\alpha) = \frac{f(1)f''(1) - (f'(1))^2}{2(f(1))^2}, \quad (\text{A.36})$$

where  $f(\alpha) := \text{Tr} [e^{\alpha \log \rho + (1-\alpha) \log \sigma}]$ . Further, the Fréchet derivative of the exponential (see e.g. [49, Example X.4.2]) gives

$$f'(\alpha) = \text{Tr} [e^{\alpha \log \rho + (1-\alpha) \log \sigma} (\log \rho - \log \sigma)], \quad (\text{A.37})$$

$$f''(\alpha) = \int_0^1 dt \text{Tr} [e^{t(\alpha \log \rho + (1-\alpha) \log \sigma)} (\log \rho - \log \sigma) e^{(1-t)(\alpha \log \rho + (1-\alpha) \log \sigma)} (\log \rho - \log \sigma)], \quad (\text{A.38})$$

Therefore, Eq. (A.36) equals

$$\tilde{D}'_\alpha(\rho\|\sigma)\Big|_{\alpha=1} = \frac{1}{2} \left( \int_0^1 dt \text{Tr} [\rho^{1-t} (\log \rho - \log \sigma) \rho^t (\log \rho - \log \sigma)] - D(\rho\|\sigma)^2 \right) \quad (\text{A.39})$$

$$= \frac{1}{2} \tilde{V}(\rho\|\sigma). \quad (\text{A.40})$$

Finally, combining with Eq. (A.30) yields

$$\left. \frac{\partial^2 \tilde{E}_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -\tilde{V}(W\|\sigma|P). \quad (\text{A.41})$$

□

## APPENDIX B. A WEAK CONVERSE BOUND: PROOF OF PROPOSITION 6

**Proposition 6** (Weak Converse Bound with Polynomial Prefactors). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $\mathcal{S}_o := \text{im}(\mathcal{W})$ , an arbitrary rate  $R \geq 0$ , and  $\sigma \in \mathcal{S}_{>0}(\mathcal{H})$ . For any  $\eta \in (0, \frac{1}{2})$  and  $c > 0$ , let  $N_0 \in \mathbb{N}$  such that for all  $n \geq N_0$ ,*

$$c \cdot e^{-\xi \sqrt{n}} \leq \frac{\eta}{2}, \quad (\text{B.1})$$

where  $\xi = \sqrt{2A/\eta}$  and  $A := \max_{\rho \in \mathcal{S}_o} V(\rho\|\sigma)$ . Then, it holds that for all  $n \geq N_0$ ,

$$\hat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \|\sigma^{\otimes n}) \geq f(\eta) \exp \left\{ -n \left[ \frac{\tilde{E}_{\text{sp}} \left( R - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, \sigma \right)}{1 - \eta} \right] \right\}, \quad (\text{B.2})$$

where  $f(\eta) = \exp \left\{ -\frac{h(1-\eta)}{1-\eta} \right\}$  and  $h(p) := -p \log p - (1-p) \log(1-p)$  is the binary entropy function.

*Remark B.1.* Consider a constant composition code with common type  $P_{\mathbf{x}^n}$  on a finite input alphabet  $\mathcal{X}$ . Recall the definition of the weak sphere-packing exponent [40, 18]:

$$\tilde{E}_{\text{sp}}(R, P_{\mathbf{x}^n}) := \min_{\bar{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})} \left\{ D(\bar{W} \|\mathcal{W}|P_{\mathbf{x}^n}) : I(P_{\mathbf{x}^n}, \bar{W}) \leq R \right\}. \quad (\text{B.3})$$

Proposition 6, along with [18, Lemma 11], establishes a weak sphere-packing bound with polynomial prefactors, which generalizes Altuğ and Wagner's result [21, Lemma 3] to c-q channels: for any  $\eta \in (0, \frac{1}{2})$  and for all sufficiently large  $n$  such that Eq. (B.1) holds, we have

$$\epsilon_{\max}(W, P_{\mathbf{x}^n}) \geq \max_{\sigma \in \mathcal{S}(\mathcal{H})} \hat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \|\sigma^{\otimes n}) \quad (\text{B.4})$$

$$\geq \hat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \|\sigma^*)^{\otimes n} \quad (\text{B.5})$$

$$\geq f(\eta) \exp \left\{ -n \left[ \frac{\tilde{E}_{\text{sp}} \left( R - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n} \right)}{1 - \eta} \right] \right\}, \quad (\text{B.6})$$

where  $\sigma^* := P_{\mathbf{x}^n} \bar{W}^*$  and  $\bar{W}^*$  is an arbitrary minimizer in Eq. (B.3). Moreover, Eq. (B.6) improves the prefactor of Winter's weak sphere-packing bound [40] from the order of subexponential to polynomial.



*Proof of Proposition 6.* Consider an arbitrary sequence  $\mathbf{x}^n \in \mathcal{X}^n$  and a test  $Q_n$  on  $\mathcal{H}^{\otimes n}$ . For two c-q channels  $\bar{W}, W : \mathcal{X} \rightarrow \mathcal{S}_o$ , the data-processing inequality implies that

$$D(\bar{W}_{\mathbf{x}^n}^{\otimes n} \| W_{\mathbf{x}^n}^{\otimes n}) \geq [1 - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})] \log \frac{1 - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})}{1 - \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n})} + \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \log \frac{\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})}{\alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n})} \quad (\text{B.7})$$

$$= -h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})) - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \log \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) - [1 - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})] \log (1 - \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n})) \quad (\text{B.8})$$

$$\geq -\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \log \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) - h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})), \quad (\text{B.9})$$

where the last inequality (B.9) follows since the third term in (B.8) is non-negative. Continuing from Eq. (B.9), we have

$$\alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) \geq \exp \left\{ -\frac{D(\bar{W}_{\mathbf{x}^n}^{\otimes n} \| W_{\mathbf{x}^n}^{\otimes n}) + h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}))}{\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})} \right\} \quad (\text{B.10})$$

$$= \exp \left\{ -\frac{n D(\bar{W} \| W | P_{\mathbf{x}^n}) + h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}))}{\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})} \right\}, \quad (\text{B.11})$$

where Eq. (B.11) follows from the additivity of the relative entropy and the empirical distribution  $P_{\mathbf{x}^n}$ .

The next step is to replace  $\alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n})$  with a lower bound that does not depend on the dummy channel  $\bar{W}$ , provided that  $\bar{W}$  satisfies certain conditions. This can be done using Proposition 13, Wolfowitz's strong converse bound. We delay its proof in Appendix B.1.

**Proposition 13** (Wolfowitz's Strong Converse). *Let  $\mathcal{S}_o \subseteq \mathcal{S}(\mathcal{H})$  be closed and let  $\bar{W} : \mathcal{X} \rightarrow \mathcal{S}_o$  be an arbitrary classical-quantum channel. Consider the binary hypothesis testing:*

$$H_0 : \bar{W}_{\mathbf{x}^n}^{\otimes n}, \quad (\text{B.12})$$

$$H_1 : \sigma^{\otimes n}, \quad (\text{B.13})$$

where  $\mathbf{x}^n \in \mathcal{X}^n$  and  $\sigma \in \mathcal{S}_{>0}(\mathcal{H})$ . For any test  $Q_n$  such that  $\beta(Q_n; \sigma^{\otimes n}) \leq e^{-nR}$  and  $D(\bar{W}_{\mathbf{x}^n}^{\otimes n} \| \sigma | P_{\mathbf{x}^n}) \leq R - 2\kappa$ , it holds that

$$\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) > 1 - \frac{A}{n\kappa^2} - e^{-n\kappa}, \quad (\text{B.14})$$

where  $A := \max_{\rho \in \mathcal{S}_o} V(\rho \| \sigma)$ .

Fix  $0 < \eta < \frac{1}{2}$ , and let  $\xi^2 := \frac{2A}{\eta}$ . Note that  $\xi^2$  is finite because  $A < +\infty$ . For all  $n \geq N_0$ , we have

$$c \cdot e^{-\xi\sqrt{n}} \leq \frac{\eta}{2} \quad (\text{B.15})$$

by assumption in Proposition 6. Choose  $\kappa = \xi/\sqrt{n}$ . For any  $\bar{W} : \mathcal{X} \rightarrow \mathcal{S}_o$  with  $D(\bar{W} \| \sigma | P_{\mathbf{x}^n}) \leq R - \frac{2\xi}{\sqrt{n}}$  and any test  $Q_n$  such that  $\beta(Q_n; \sigma^{\otimes n}) \leq e^{-nR}$ , Proposition 13 gives a lower bound to the type-I error:

$$\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \geq 1 - \frac{A}{n\kappa^2} - e^{-n\kappa} \geq 1 - \eta. \quad (\text{B.16})$$

Hence, combining Eqs. (B.11) and (B.16) yields that, for any  $\beta(Q_n; \sigma^{\otimes n}) \leq ce^{-nR}$ ,

$$\alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) \geq \max_{\bar{W}: D(\bar{W} \| \sigma | P_{\mathbf{x}^n}) \leq R - \frac{2\xi}{\sqrt{n}}} \exp \left\{ -\frac{n D(\bar{W} \| W | P_{\mathbf{x}^n}) + h(1 - \eta)}{1 - \eta} \right\}, \quad (\text{B.17})$$

$$= \exp \left\{ -\frac{h(1 - \eta)}{1 - \eta} \right\} \exp \left\{ -\frac{n \tilde{E}_{\text{sp}} \left( R - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, \sigma \right)}{1 - \eta} \right\}, \quad (\text{B.18})$$

which concludes Proposition 6. □

**B.1. Proof of Wolfowitz's Strong Converse: Proposition 13.** To prove our claim, we first introduce notation for generalized divergences. For any  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , and  $\gamma > 0$ , define the *hockey-stick divergence* by

$$\mathcal{D}_\gamma(\rho\|\sigma) := \text{Tr} [(\rho - \gamma\sigma)_+], \quad (\text{B.19})$$

where  $A_+ := A\{A \geq 0\}$  denotes the self-adjoint matrix contributed only by its positive part. This divergence satisfies the data-processing inequality (DPI):

$$\text{Tr} [(\rho - \gamma\varrho)_+] \geq \text{Tr} [(\mathcal{N}(\rho) - \gamma\mathcal{N}(\varrho))_+], \quad (\text{B.20})$$

for any completely positive and trace-preserving map  $\mathcal{N} : \mathcal{S}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{S}(\mathcal{H}_{\text{out}})$  [51, Lemma 4]. Let

$$\rho_p := p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|, \quad \text{and} \quad \sigma_q := q|0\rangle\langle 0| + (1-q)|1\rangle\langle 1|, \quad (\text{B.21})$$

for  $0 \leq p, q \leq 1$  and some orthonormal basis  $\{|0\rangle, |1\rangle\}$ , and define

$$d_\gamma(p\|q) := \mathcal{D}_\gamma(\rho_p\|\sigma_q). \quad (\text{B.22})$$

Note that the quantity  $d_\gamma(p\|q)$  is independent of the choice of the basis  $\{|0\rangle, |1\rangle\}$ . Now we are ready to prove Proposition 13.

*Proof of Proposition 13.* Fix an arbitrary test  $Q_n$  on  $\mathcal{H}^{\otimes n}$ . For notational convenience, we shorthand  $\rho^n = \bar{W}_{\mathbf{x}^n}^{\otimes n}$ ,  $\tau^n = \sigma^{\otimes n}$ ,  $\alpha = \alpha(Q_n; \rho^n)$  and  $\beta = \beta(Q_n; \tau^n)$ . Further, we assume  $\beta(Q_n; \tau^n) \leq e^{-nR}$ . From the definition of the classical divergence, Eqs. (B.19) and (B.22), and any  $\gamma > 0$ , we find

$$d_\gamma(1 - \alpha\|\beta) = (1 - \alpha - \gamma\beta)_+ + (\alpha - \gamma[1 - \beta])_+ \quad (\text{B.23})$$

$$\geq 1 - \alpha - \gamma\beta \quad (\text{B.24})$$

$$\geq 1 - \alpha - \gamma e^{-nR}. \quad (\text{B.25})$$

On the other hand, DPI and the measurement map  $\text{Tr}[Q_n(\cdot)]|0\rangle\langle 0| + (1 - \text{Tr}[Q_n(\cdot)])|1\rangle\langle 1|$  imply that

$$\mathcal{D}_\gamma(\rho^n\|\tau^n) \geq d_\gamma(\text{Tr}[Q_n\rho^n]\|\text{Tr}[Q_n\tau^n]) = d_\gamma(1 - \alpha\|\beta). \quad (\text{B.26})$$

Hence, Eqs. (B.25) and (B.26) lead to

$$\alpha \geq 1 - \mathcal{D}_\gamma(\rho^n\|\tau^n) - \gamma e^{-nR}. \quad (\text{B.27})$$

Since

$$\mathcal{D}_\gamma(\rho^n\|\tau^n) = \text{Tr} [\{\rho^n - \gamma\tau^n \geq 0\}(\rho^n - \gamma\tau^n)] \quad (\text{B.28})$$

$$\leq \text{Tr} [\{\rho^n - \gamma\tau^n \geq 0\}\rho^n], \quad (\text{B.29})$$

continuing from Eq. (B.27) gives

$$\alpha \geq 1 - \text{Tr} [\{\rho^n - \gamma\tau^n \geq 0\}\rho^n] - \gamma e^{-nR}. \quad (\text{B.30})$$

Next, invoking Lemma 14 below, for all  $\log \gamma > D(\rho^n\|\tau^n)$ , we have

$$\alpha \geq 1 - \frac{V(\rho^n\|\tau^n)}{[\log \gamma - D(\rho^n\|\tau^n)]^2} - \gamma e^{-nR} \quad (\text{B.31})$$

$$= 1 - \frac{V(\bar{W}\|\sigma|P_{\mathbf{x}^n})}{n \left[ \frac{\log \gamma}{n} - D(\bar{W}\|\sigma|P_{\mathbf{x}^n}) \right]^2} - \gamma e^{-nR} \quad (\text{B.32})$$

Finally, recall  $D(\bar{W}\|\sigma|P_{\mathbf{x}^n}) \leq R - 2\kappa$  and  $A := \max_{\rho \in \mathcal{S}_o} V(\rho\|\sigma)$  and choose  $\log \gamma = nD(\bar{W}\|\sigma|P_{\mathbf{x}^n}) + n\kappa$ . Then, Eq. (B.32) yields, for any test  $Q_n$  and  $\beta(Q_n; \sigma^{\otimes n}) \leq e^{-nR}$ ,

$$\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \geq 1 - \frac{V(\bar{W}\|\sigma|P_{\mathbf{x}^n})}{n\kappa^2} - e^{-n\kappa} \quad (\text{B.33})$$

$$\geq 1 - \frac{A}{n\kappa^2} - e^{-n\kappa}, \quad (\text{B.34})$$

which concludes the proof.

**Lemma 14** (Quantum Chebyshev's Inequality [51, Lemma 6]). *Let  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  and assume  $\log \gamma > D(\rho\|\sigma)$ . Then*

$$\mathrm{Tr}[\rho\{\rho - \gamma\sigma \geq 0\}] \leq \frac{V(\rho\|\sigma)}{[\log \gamma - D(\rho\|\sigma)]^2}. \quad (\text{B.35})$$

□

## APPENDIX C. A SHARP CONVERSE BOUND FROM STRONG LARGE DEVIATION

In this section, we provide the proof of Proposition 7. Our technique highly relies on a strong large deviation inequality.

**C.1. A Strong Large Deviation Inequality.** Let  $(X_i)_{i \in \mathbb{N}}$  be a sequence of independent, real-valued random variables with probability measures  $(\mu_i)_{i=1}^n$ . Let  $Z_n := \sum_{i=1}^n X_i$  and let  $\Lambda_n(t) := \log \mathbb{E}[e^{tZ_n}]$ . Define the Legendre-Fenchel transform of  $\frac{1}{n}\Lambda_n(\cdot)$  by:

$$\Lambda_n^*(z) := \sup_{t \in \mathbb{R}} \left\{ zt - \frac{1}{n}\Lambda_n(t) \right\}, \quad \forall z \in \mathbb{R}. \quad (\text{C.1})$$

Let  $(T_n)_{n \in \mathbb{N}}$  be a bounded sequence of real numbers and  $(t_n^*)_{n \in \mathbb{N}}$  be a sequence satisfying for all  $n \in \mathbb{N}$

$$t_n^* \in (0, 1); \quad (\text{C.2})$$

$$T_n = \frac{1}{n}\Lambda_n'(t_n^*); \quad (\text{C.3})$$

$$\Lambda_n^*(T_n) = T_n t_n^* - \frac{1}{n}\Lambda_n(t_n^*). \quad (\text{C.4})$$

With these definitions, we can now state the following sharp concentration inequality for  $\frac{1}{n}Z_n$ :

**Theorem 15** (Chaganty-Sethuraman's Concentration Inequality [52, Theorem 3.3]). *For any  $\eta \in (0, 1)$ , there exists an  $N_0 \in \mathbb{N}$  such that, for all  $n \geq N_0$ ,*

$$\Pr \left\{ \frac{1}{n}Z_n \geq T_n, \right\} \geq \frac{1 - \eta}{t_n^* \sqrt{2\pi n m_{2,n}}} \exp\{-n\Lambda_n^*(T_n)\}, \quad (\text{C.5})$$

where  $m_{2,n} := \frac{1}{n} \sum_{i=1}^n \mathrm{Var}_{\tilde{\mu}_{n,i}}[X_i]$ , and the measure  $\tilde{\mu}_{n,i}$  is defined via

$$\frac{d\tilde{\mu}_{n,i}}{d\mu_i}(y) := \frac{e^{yt_n^*}}{\mathbb{E}[e^{t_n^* X_i}]}. \quad (\text{C.6})$$

*Remark C.1.* Chaganty and Sethuraman in Ref. [52, Theorem 3.3] considered a more general sequence of random variables  $\{Z_n\}_{n \in \mathbb{N}}$ , which are not necessarily the sum of random variables. They proved Theorem 15 provided that the following condition is satisfied: there exists  $\delta_0 > 0$  such that for any  $\delta$  and  $\lambda$  with  $0 < \delta < \delta_0 < \lambda$ ,  $\sup_{\delta < |t| \leq \lambda t_n^*} |\Lambda_n(t_n^* + it)/\Lambda_n(t_n^*)| = o(1/\sqrt{n})$ , where the supremum is defined to be 0 if  $\{t : \delta < |t| \leq \lambda t_n^*\}$  is empty. In the case of  $Z_n$  being a sum of random variables,  $\Lambda_n(t_n^* + it)/\Lambda_n(t_n^*)$  is the product of the characteristic functions of  $\{X_i\}_{i=1}^n$ . Since the supremum of a characteristic function on a compact interval not containing 0 is less than 1, this condition is thus satisfied.

We note that the lower bound in Theorem 15 for the general sequence of random variables  $(X_i)_{i \in \mathbb{N}}$  suffices to establish the converse, Theorem 5. We do not particularly consider the case of lattice valued random variables (see e.g. [52, Theorem 3.5]).

## C.2. Proof of Proposition 7.

**Proposition 7** (A Sharp Converse Bound). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and a state  $\sigma \in \mathcal{S}(\mathcal{H})$ . Suppose the sequence  $\mathbf{x}^n \in \mathcal{X}^n$  satisfies*

$$\nu \leq V(\mathcal{W}\|\sigma|P_{\mathbf{x}^n}) < +\infty \quad (\text{C.7})$$

for some  $\nu > 0$ , and suppose the sequence of rates  $(R_n)_{n \in \mathbb{N}}$  satisfies  $D_0(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n}) < R_n < D(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n})$ . Then, there exists an  $N_0 \in \mathbb{N}$  such that, for all  $n \geq N_0$ ,

$$\hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \parallel \sigma^{\otimes n}) \geq \frac{A}{s_n^* \sqrt{n}} \exp \left\{ -n E_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, \sigma) \right\}, \quad (\text{C.8})$$

where  $c_n = \frac{K \log n}{n}$  and  $A, K > 0$  are finite constants independent of the sequence  $\mathbf{x}^n$ , and

$$s_n^* := \arg \max_{s \geq 0} \{E_h(s, P_{\mathbf{x}^n}, \sigma) - s R_n\}. \quad (\text{C.9})$$

*Proof of Proposition 7.* Let  $\rho^n := W_{\mathbf{x}^n}^{\otimes n}$ ,  $\sigma^n := \sigma^{\otimes n}$ ,  $p^n := \bigotimes_{i=1}^n p_{x_i}$ , and  $q^n := \bigotimes_{i=1}^n q_{x_i}$ , where  $p_{x_i}, q_{x_i}$  are Nussbaum-Szkoła distributions [58] of  $W_{x_i}, \sigma$  for every  $i \in [n]$ . Let  $\tilde{R}_n := R_n - \gamma_n$ , where  $\gamma_n := \frac{\log n}{2n} + \frac{x}{n}$  for some  $x \in \mathbb{R}$ . The choice of  $x$  and the rate back-off term  $\gamma_n$  will become evident later. Let  $N_1 \in \mathbb{N}$  such that  $\tilde{R}_n \geq D_0(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n})$  for all  $n \geq N_1$ . Subsequently, we choose such  $n \geq N_1$  onwards.

Since  $D_\alpha(W_{x_i} \parallel \sigma) = D_\alpha(p_{x_i} \parallel q_{x_i})$ , for  $\alpha \in (0, 1]$ , we use the notation

$$\phi_n(\tilde{R}_n) := E_{\text{sp}}^{(2)}(\tilde{R}_n, P_{\mathbf{x}^n}, \sigma) = \sup_{0 < \alpha \leq 1} \frac{1 - \alpha}{\alpha} \left( \sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) D_\alpha(p_{x_i} \parallel q_{x_i}) - \tilde{R}_n \right), \quad (\text{C.10})$$

where  $P_{\mathbf{x}^n}$  denotes the empirical distribution of  $\mathbf{x}^n = x_1, \dots, x_n$ . Moreover, the condition in Eq. (C.7) implies that  $W_x \ll \sigma$ , for all  $x \in \text{supp}(P_{\mathbf{x}^n})$ , and thus  $p^n \ll q^n$ . Without loss of generality, we let  $q_{x_i}(\omega) = 0, \omega \notin \text{supp}(p_{x_i})$  since they won't contribute to  $\phi_n(\tilde{R}_n)$ .

We apply Nagaoka's argument [59]: for any  $0 \leq Q_n \leq \mathbb{1}$ , choosing  $\delta = \exp\{n\tilde{R}_n - n\phi_n(\tilde{R}_n)\}$  yields:

$$\alpha(Q_n; \rho^n) + \delta \beta(Q_n; \sigma^n) \geq \frac{1}{2} \left( \alpha(\mathcal{U}; p^n) + e^{n\tilde{R}_n - n\phi_n(\tilde{R}_n)} \beta(\mathcal{U}; q^n) \right), \quad (\text{C.11})$$

where

$$\alpha(\mathcal{U}; p^n) := \sum_{\omega \in \mathcal{U}^c} p^n(\omega); \quad \beta(\mathcal{U}; q^n) := \sum_{\omega \in \mathcal{U}} q^n(\omega), \quad (\text{C.12})$$

and

$$\mathcal{U} := \left\{ \omega : p^n(\omega) e^{n\phi_n(\tilde{R}_n)} > q^n(\omega) e^{n\tilde{R}_n} \right\}. \quad (\text{C.13})$$

In the following, we will employ Theorem 15, to further lower bound  $\alpha(\mathcal{U}; p^n)$  and  $\beta(\mathcal{U}; q^n)$ . Before proceeding, we need to introduce some notation. Define the *tilted distributions*, for every  $i \in [n]$  and  $t \in [0, 1]$ , to be

$$\hat{q}_{x_i, t}(\omega) := \frac{p_{x_i}(\omega)^{1-t} q_{x_i}(\omega)^t}{\sum_{\omega \in \text{supp}(p_{x_i})} p_{x_i}(\omega)^{1-t} q_{x_i}(\omega)^t}, \quad \omega \in \text{supp}(p_{x_i}). \quad (\text{C.14})$$

Let

$$\Lambda_{0, x_i}(t) := \log \mathbb{E}_{p_{x_i}} \left[ e^{t \log \frac{q_{x_i}}{p_{x_i}}} \right], \quad \Lambda_{1, x_i}(t) := \log \mathbb{E}_{q_{x_i}} \left[ e^{t \log \frac{p_{x_i}}{q_{x_i}}} \right], \quad (\text{C.15})$$

Since  $p^n$  and  $q^n$  share the same support, it can be verified that the maps  $t \mapsto \Lambda_{j, x_i}(t)$ ,  $j \in \{0, 1\}$  are differential for all  $t \in [0, 1]$ . One can immediately verify the following partial derivatives with respect to  $t$ :

$$\Lambda'_{0, x_i}(t) = \mathbb{E}_{\hat{q}_{x_i, t}} \left[ \log \frac{q_{x_i}}{p_{x_i}} \right], \quad \Lambda'_{1, x_i}(t) = \mathbb{E}_{\hat{q}_{x_i, 1-t}} \left[ \log \frac{p_{x_i}}{q_{x_i}} \right]; \quad (\text{C.16})$$

$$\Lambda''_{0, x_i}(t) = \text{Var}_{\hat{q}_{x_i, t}} \left[ \log \frac{q_{x_i}}{p_{x_i}} \right], \quad \Lambda''_{1, x_i}(t) = \text{Var}_{\hat{q}_{x_i, 1-t}} \left[ \log \frac{p_{x_i}}{q_{x_i}} \right]. \quad (\text{C.17})$$

Note that Eqs. (C.15), (C.16), and (C.17) ensure that

$$\Lambda_{0, x_i}(t) = \Lambda_{1, x_i}(1-t), \quad \Lambda'_{0, x_i}(t) = -\Lambda'_{1, x_i}(1-t), \quad \Lambda''_{0, x_i}(t) = \Lambda''_{1, x_i}(1-t). \quad (\text{C.18})$$

With  $\Lambda_{j,x_i}(t)$  in Eq. (C.15), we can define

$$\Lambda_{j,P_{\mathbf{x}^n}}(t) := \sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) \Lambda_{j,x}(t), \quad j \in \{0, 1\}; \quad (\text{C.19})$$

$$\Lambda_{j,P_{\mathbf{x}^n}}^*(z) := \sup_{t \in \mathbb{R}} \{tz - \Lambda_{j,P_{\mathbf{x}^n}}(t)\}, \quad j \in \{0, 1\}, \quad (\text{C.20})$$

where  $\Lambda_{j,P_{\mathbf{x}^n}}^*(z)$  in Eq. (C.20) are the *Legendre-Fenchel transform* of  $\Lambda_{j,P_{\mathbf{x}^n}}(t)$ . The quantities  $\Lambda_{j,P_{\mathbf{x}^n}}^*(z)$  would appear in the lower bounds of  $\alpha(\mathcal{U}; p^n)$  and  $\beta(\mathcal{U}; q^n)$  obtained by Theorem 15 as shown later.

In the following, we will relate the Legendre-Fenchel transform  $\Lambda_{j,P_n}^*(z)$  to the desired error-exponent function  $\phi_n(\tilde{R}_n)$ . Such a relationship is stated in the following lemma whose proof was presented in [18].

**Lemma 16** ([18, Lemma 17]). *The following holds for all sequences  $\mathbf{x}^n$  satisfying Eq. (C.7) and all  $r \in (D_0(\mathcal{W}||\sigma|P_{\mathbf{x}^n}), D(\mathcal{W}||\sigma|P_{\mathbf{x}^n}))$ :*

- (a)  $\Lambda_{0,P_{\mathbf{x}^n}}''(t) > 0$  for all  $t \in [0, 1]$ .
- (b)  $\Lambda_{0,P_{\mathbf{x}^n}}^*(\phi_n(r) - r) = \phi_n(r)$ .
- (c)  $\Lambda_{1,P_{\mathbf{x}^n}}^*(r - \phi_n(r)) = r$ .
- (d) Let  $s^*$  be the optimizer of  $E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n}, \sigma)$ , c.f. (C.9). The optimizer of  $\Lambda_{0,P_{\mathbf{x}^n}}^*(z)$ , denoted by  $t^*$ , is unique and satisfies  $t^* = \frac{s^*}{1+s^*} \in (0, 1)$  and  $\Lambda_{0,P_{\mathbf{x}^n}}'(t^*) = \phi_n(r) - r$ .

Since the item (d) in Lemma 16 shows that the optimizer  $t$  in Eq. (C.20) always lies in the compact set  $[0, 1]$ , by invoking Eq. (C.18) we define the following quantity:

$$V_{\min}(\nu) := \min_{t \in [0, 1], P_{\mathbf{x}^n} \in \mathcal{P}_\nu(\mathcal{X})} \Lambda_{0,P_n}''(t), \quad (\text{C.21})$$

where  $\mathcal{P}_\nu(\mathcal{X}) := \{P_{\mathbf{x}^n} \in \mathcal{P}(\mathcal{X}) : \nu \leq V(\mathcal{W}||\sigma|P_{\mathbf{x}^n}) < +\infty\}$  is a compact set owing to the continuity of the map  $P \mapsto V(\mathcal{W}||\sigma|P)$ ; see Eq. (2.16).

Further, from the definitions in Eqs, (C.17),  $\Lambda_{0,(\cdot)}''(\cdot)$  is continuous functions in  $[0, 1] \times \mathcal{P}(\mathcal{X})$ . The minimization in the above definitions are well-defined and finite. Further, the quantity  $V_{\min}(\nu)$  is bounded away from zero owing to item (a) in Lemma 16.

Now, we are ready to derive the lower bounds to  $\alpha(\mathcal{U}; p^n)$  and  $\beta(\mathcal{U}; q^n)$ . Fix an arbitrary  $\eta \in (0, 1)$ . Applying Theorem 15 to  $X_i = \log q_i - \log p_i$  with probability measure  $p_i$ , and threshold  $T_n = \tilde{R}_n - \phi_n(\tilde{R}_n)$  gives, for all sufficiently large  $n$ , say  $n \geq N_2 \in \mathbb{N}$ ,

$$\alpha(\mathcal{U}; p^n) := \sum_{\omega \in \mathcal{U}^c} p^n(\omega) \quad (\text{C.22})$$

$$= \Pr \left\{ \frac{1}{n} \sum_{i=1}^n Z_i \geq \tilde{R}_n - \phi_n(\tilde{R}_n) \right\} \quad (\text{C.23})$$

$$\geq \frac{1 - \eta}{t_n^* \sqrt{2\pi n V_{\min}(\nu)}} \exp \left\{ -n \Lambda_{0,P_{\mathbf{x}^n}}^* \left( \phi_n(\tilde{R}_n) - \tilde{R}_n \right) \right\}, \quad (\text{C.24})$$

where

$$t_n^* := \arg \max_{t \in \mathbb{R}} \{tz_n - \Lambda_{0,P_{\mathbf{x}^n}}(t)\} \quad (\text{C.25})$$

Similarly, applying again Theorem 15 to  $X_i = \log p_i - \log q_i$  with probability measure  $= q_i$ , and threshold  $\phi_n(\tilde{R}_n) - \tilde{R}_n$  yields, for all sufficiently large  $n$ , say  $n \geq N_3 \in \mathbb{N}$ ,

$$\beta(\mathcal{U}; q^n) := \sum_{\omega \in \mathcal{U}} q^n(\omega) \quad (\text{C.26})$$

$$= \Pr \left\{ \frac{1}{n} \sum_{i=1}^n Z_i \geq \phi_n(\tilde{R}_n) - \tilde{R}_n \right\} \quad (\text{C.27})$$

$$\geq \frac{1-\eta}{(1-t_n^*)\sqrt{2\pi n V_{\min}(\nu)}} \exp \left\{ -n\Lambda_{1, P_{\mathbf{x}^n}}^* \left( \tilde{R}_n - \phi_n(\tilde{R}_n) \right) \right\} \quad (\text{C.28})$$

$$\geq \frac{1-\eta}{\sqrt{2\pi n V_{\min}(\nu)}} \exp \left\{ -n\Lambda_{1, P_{\mathbf{x}^n}}^* \left( \tilde{R}_n - \phi_n(\tilde{R}_n) \right) \right\}, \quad (\text{C.29})$$

where the term  $1-t_n^*$  in Eq (C.28) comes from the symmetry in Eq. (C.18), and the last inequality (C.29) follows from  $t_n^* \in (0, 1)$  in item (d) of Lemma 16.

Continuing from Eq. (C.24) and item (b) in Lemma 16 gives

$$\alpha(\mathcal{U}; p^n) \geq \frac{1-\eta}{t_n^* \sqrt{2\pi n V_{\min}(\nu)}} \exp\{-n\phi_n(\tilde{R}_n)\}. \quad (\text{C.30})$$

Eq. (C.29) together with item (c) in Lemma 16 yields

$$\beta(\mathcal{U}; q^n) \geq \frac{1-\eta}{\sqrt{2\pi n V_{\min}(\nu)}} \exp\{-n\tilde{R}_n\} = 2 \exp\{-nR_n\}, \quad (\text{C.31})$$

where we choose  $x = \log 2\sqrt{2\pi V_{\min}(\nu)} - \log(1-\eta)$  in the rate back-off  $\gamma_n = \frac{\log n}{2n} + \frac{x}{n}$ . Thus we can bound the left-hand side of Eq. (C.11) from below. If for any test  $0 \leq Q_n \leq \mathbb{1}$  such that

$$\beta(Q_n; \sigma^n) \leq \exp\{-nR_n\}, \quad (\text{C.32})$$

holds, it implies that

$$\alpha(Q_n; \rho^n) \geq \frac{1-\eta}{t_n^* 2\sqrt{2\pi n V_{\min}(\nu)}} \exp\{-n\phi_n(\tilde{R}_n)\}. \quad (\text{C.33})$$

Finally, let  $A := (1-\eta)/(2\sqrt{2\pi V_{\min}(\nu)})$  and choose a constant  $K > 0$  such that for all  $n \geq N_0 := \max\{N_1, N_2, N_3\}$ ,

$$\gamma_n = \frac{\log n}{2n} + \frac{\log 2\sqrt{2\pi V_{\min}(\nu)} - \log(1-\eta)}{n} \leq \frac{K \log n}{n} =: c_n. \quad (\text{C.34})$$

Since the map  $r \mapsto \phi_n(r)$  is monotonically decreasing [30, Section 5], Eqs. (C.32), (C.33), and (C.34) conclude our result: for all  $n \geq N_0$ ,

$$\hat{\alpha}_{\exp\{-nR\}}(\rho^n \| \sigma^n) \geq \frac{A}{t_n^* \sqrt{n}} \exp \left\{ -nE_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, \sigma) \right\} \quad (\text{C.35})$$

$$\geq \frac{A}{s_n^* \sqrt{n}} \exp \left\{ -nE_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, \sigma) \right\}, \quad (\text{C.36})$$

where the last inequality follows from item (d) in Lemma 16:  $t_n^* = s_n^*/(1+s_n^*) \in (0, 1)$ .  $\square$

#### APPENDIX D. PROOF OF PROPOSITION 8

**Proposition 8** (Error Exponent around Capacity). *Let  $(b_n)_{n \in \mathbb{N}}$  be a sequence of real numbers with  $\lim_{n \rightarrow +\infty} b_n = 0$  and let  $(\delta_n)_{n \in \mathbb{N}}$  be a sequence of positive numbers with  $\lim_{n \rightarrow +\infty} \delta_n = 0$ . Suppose the sequence of distributions  $(P_n)_{n \in \mathbb{N}}$  satisfies*

$$C_W - \delta_n < D(W \| P_n^* W | P_n) \leq C_W - b_n. \quad (\text{D.1})$$

The following holds:

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W})}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2V_{\mathcal{W}} \delta_n^2}; \quad (\text{D.2})$$

$$\limsup_{n \rightarrow +\infty} \frac{\tilde{E}_{\text{sp}}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W})}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2\tilde{V}_{\mathcal{W}} \delta_n^2}; \quad (\text{D.3})$$

$$\limsup_{n \rightarrow +\infty} \frac{s_n^*}{\delta_n} \leq \frac{1}{V_{\mathcal{W}}}, \quad (\text{D.4})$$

where

$$s_n^* := \arg \max_{s \geq 0} \{E_{\text{h}}(s, P_n, P^* \mathcal{W}) - s(C_{\mathcal{W}} - \delta_n)\}. \quad (\text{D.5})$$

*Proof of Proposition 8.* We only prove Eqs. (D.2) and (D.4), since Eq. (D.3) follows from the same argument and Proposition 3.

Recall the error-exponent function  $E_{\text{sp}}^{(2)}$ :

$$E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P, P^* \mathcal{W}) = \sup_{s \geq 0} \{-s(C_{\mathcal{W}} - \delta_n) + E_{\text{h}}(s, P, P^* \mathcal{W})\}. \quad (\text{D.6})$$

In the following, we fix  $\sigma = P^* \mathcal{W}$  in the definition of  $E_{\text{h}}$  (Eq. (2.26)) and denote by

$$E_{\text{h}}(s, P) := E_{\text{h}}(s, P, P^* \mathcal{W}) = s D_{\frac{1}{1+s}}(\mathcal{W} \| P^* \mathcal{W} | P). \quad (\text{D.7})$$

for notational convenience. We define a *critical rate* for a c-q channel  $\mathcal{W}$  to be

$$r_{\text{cr}} := \max_{P \in \mathcal{P}(\mathcal{X})} \left. \frac{\partial E_{\text{h}}(s, P)}{\partial s} \right|_{s=1}. \quad (\text{D.8})$$

Let  $N_0$  be the smallest integer such that  $C_{\mathcal{W}} - \delta_n > r_{\text{cr}}$ ,  $\forall n \geq N_0$ . Since the map  $r \mapsto E_{\text{sp}}^{(2)}(r, \cdot, \cdot)$  is non-increasing [30, Section 5], the maximization over  $s$  in Eq. (D.6) can be restricted to the set  $[0, 1]$  for any rate above  $r_{\text{cr}}$ , i.e.,

$$E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W}) = \max_{0 \leq s \leq 1} \{-s(C_{\mathcal{W}} - \delta_n) + E_{\text{h}}(s, P_n)\}. \quad (\text{D.9})$$

For every  $n \in \mathbb{N}$ , let  $s_n^*$  attain the maxima in Eq. (D.9) at a rate of  $C_{\mathcal{W}} - \delta_n \geq 0$ . In the following lemma, we discuss the asymptotic behavior of  $\{s_n^*\}_{n \in \mathbb{N}}$ .

**Lemma 17.** *Let  $s_n^*$  attain the maxima in Eq. (D.9) and  $P_n$  satisfy Eq. (D.1). We have*

- (a) *The limit point of  $\{P_n\}_{n \in \mathbb{N}}$  is capacity achieving.*
- (b)  *$s_n^* > 0$  for all  $n \in \mathbb{N}$  and  $\lim_{n \rightarrow +\infty} s_n^* = 0$ .*

*Proof of Lemma 17.* Let  $\{P_{n_k}\}_{k \geq 1}$  and  $\{s_{n_k}^*\}_{k \geq 1}$  be arbitrary subsequences. Since  $\mathcal{P}(\mathcal{X})$  and  $[0, 1]$  are compact, we may assume that

$$\lim_{k \rightarrow +\infty} P_{n_k} = P_o, \quad \lim_{k \rightarrow \infty} s_{n_k}^* = s_o, \quad (\text{D.10})$$

for some  $P_o \in \mathcal{P}(\mathcal{X})$  and  $s_o \in [0, 1]$ .

(17-(a)) Let  $k \rightarrow +\infty$ . Eq. (D.1) implies that

$$D(\mathcal{W} \| P^* \mathcal{W} | P_o) = C_{\mathcal{W}}, \quad (\text{D.11})$$

which guarantees that  $P_o$  is capacity-achieving by the dual representation of the information radius, see e.g. [61], [9, Theorem 2].

(17-(b)) One can observe from Eq. (D.9) that  $s_n^* = 0$  if and only if  $C_{\mathcal{W}} - \delta_n \geq D(\mathcal{W} \| P^* \mathcal{W} | P_n)$ . However, this violates the assumption in Eq. (D.1). Hence, we have  $s_n^* > 0$  for all  $n \in \mathbb{N}$ .

Since  $P_o$  is capacity achieving, the uniqueness of the divergence center implies that  $P_o \mathcal{W} = P^* \mathcal{W}$ . Item (c) in Proposition 2 shows that

$$\left. \frac{\partial^2 E_{\text{h}}(s, P_o)}{\partial s^2} \right|_{s=0} = -V(\mathcal{W} \| P^* \mathcal{W} | P_o) = -V(P_o, \mathcal{W}) \leq -V_{\mathcal{W}} < 0, \quad (\text{D.12})$$



where the last inequality follows since  $V_W > 0$ . Then, Eq. (D.12) implies that the first-order derivative  $\partial E_h(s, P_o) / \partial s$  is strictly decreasing around  $s = 0$ . Moreover, item (d) in Proposition 2 gives

$$\left. \frac{\partial E_h(s, P_o)}{\partial s} \right|_{s=s_o} \leq D(W \| P^* W | P_o) = C_W, \quad (\text{D.13})$$

This, together with items (b) and (c) in Proposition 2, shows that the first inequality in Eq. (D.13) becomes an equality if and only if  $s_o = 0$ . Since the subsequence was arbitrary, item (b) is shown.  $\square$

Now we are ready to prove this proposition. We start with proving Eq. (D.4). Since  $s \mapsto E_h(s, \cdot)$  is concave from item (b) in Proposition 2, the maximizer  $s_n^*$  must satisfy

$$\left. \frac{\partial E_h(s, P_{n_k})}{\partial s} \right|_{s=s_{n_k}^*} = C_W - \delta_{n_k}. \quad (\text{D.14})$$

Further, item (c) in Proposition 2 gives

$$\left. \frac{\partial E_h(s, P_{n_k}^*)}{\partial s} \right|_{s=0} = D(W \| P^* W | P_{n_k}^*). \quad (\text{D.15})$$

The mean value theorem states that there exists a number  $\hat{s}_{n_k} \in (0, s_{n_k}^*)$ , for each  $k \geq \mathbb{N}$ , such that

$$-\left. \frac{\partial^2 E_h(s, P_{n_k})}{\partial s^2} \right|_{s=\hat{s}_{n_k}} = \frac{D(W \| P^* W | P_{n_k}) - C_W + \delta_{n_k}}{s_{n_k}^*} \quad (\text{D.16})$$

$$\leq \frac{\delta_{n_k}}{s_{n_k}^*}, \quad (\text{D.17})$$

where the last inequality is again due to  $D(W \| P^* W | P_{n_k}^*) \leq C_W$ . When  $k$  approaches infinity, items (a) and (e) in Proposition 2 give

$$\lim_{k \rightarrow +\infty} \left. \frac{\partial^2 E_h(s, P_{n_k})}{\partial s^2} \right|_{s=\hat{s}_{n_k}} = \left. \frac{\partial^2 E_h(s, P_o)}{\partial s^2} \right|_{s=0} = -V(P_o, W) \leq -V_W. \quad (\text{D.18})$$

Combining Eqs. (D.17) and (D.18) leads to

$$\limsup_{k \rightarrow +\infty} \frac{s_{n_k}^*}{\delta_{n_k}} \leq \frac{1}{V_W}. \quad (\text{D.19})$$

Since the subsequence was arbitrary, the above result establishes Eq. (D.4).

Next, for any sufficiently large  $n \geq N_0$ , we apply Taylor's theorem to the map  $s_n^* \mapsto E_h(s_n^*, P_n)$  at the original point to obtain

$$\begin{aligned} & E_{\text{sp}}^{(2)}(C_W - \delta_n, P_n, P^* W) \\ &= -s_n^*(C_W - \delta_n) + E_h(s_n^*, P_n) \end{aligned} \quad (\text{D.20})$$

$$= s_n^*(\delta_n + D(W \| P^* W | P_n) - C_W) - \frac{(s_n^*)^2}{2} V(P_n, W) + \frac{(s_n^*)^3}{6} \left. \frac{\partial^3 E_h(s, P_n)}{\partial s^3} \right|_{s=\bar{s}_n} \quad (\text{D.21})$$

for some  $\bar{s}_n \in [0, s_n^*]$ . Let

$$\Upsilon = \max_{(s, P) \in [0, 1] \times \mathcal{P}(\mathcal{X})} \left| \frac{\partial^3 E_h(s, P)}{\partial s^3} \right|. \quad (\text{D.22})$$

Continuing from Eq. (D.21) gives

$$E_{\text{sp}}^{(2)}(C_W - \delta_n, P_n, P^*W) \leq s_n^*(\delta_n - b_n) - \frac{(s_n^*)^2}{2}V(P_n, W) + \frac{(s_n^*)^3\Upsilon}{6} \quad (\text{D.23})$$

$$\leq \sup_{s \geq 0} \left\{ s(\delta_n - b_n) - \frac{s^2}{2}V(P_n, W) \right\} + \frac{(s_n^*)^3\Upsilon}{6} \quad (\text{D.24})$$

$$= \frac{(\delta_n - b_n)^2}{2V(P_n, W)} + \frac{(s_n^*)^3\Upsilon}{6}, \quad (\text{D.25})$$

where the first line follows from the assumption  $D(W\|P^*W|P_n) \leq C_W - b_n$  in Eq. (D.1) and Eq. (D.22). Finally, Eq. (D.25), along with item (b) in Lemma 17 and Eq. (D.19), implies that

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_W - \delta_n, P_n, P^*W)}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2V(P_n, W)\delta_n^2} \quad (\text{D.26})$$

$$\leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2V_W\delta_n^2}, \quad (\text{D.27})$$

where the last inequality follows from the continuity of  $V(\cdot, W)$  on  $\mathcal{P}(\mathcal{X})$  (Eq. (2.20)); the fact that  $\{P_n\}_{n \in \mathbb{N}}$  is capacity achieving (item (a) in Lemma 17); and the definition of  $V_W$  in Eq. (2.22).  $\square$

## REFERENCES

- [1] V. Strassen, “Asymptotische abschätzungen in Shannon’s informationstheorie,” *Transactions of the Third Prague Conference on Information Theory*, pp. 689–723, 1962.
- [2] C. E. Shannon, “A mathematical theory of communication,” *The Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.
- [3] Y. Polyanskiy, H. V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.
- [4] M. Hayashi, “Information spectrum approach to second-order coding rate in channel coding,” *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 4947–4966, Nov 2009.
- [5] M. Tomamichel and M. Hayashi, “A hierarchy of information quantities for finite block length analysis of quantum tasks,” *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7693–7710, Nov 2013.
- [6] K. Li, “Second-order asymptotics for quantum hypothesis testing,” *The Annals of Statistics*, vol. 42, no. 1, pp. 171–189, Feb 2014.
- [7] M. Tomamichel and V. Y. F. Tan, “Second-order asymptotics for the classical capacity of image-additive quantum channels,” *Communications in Mathematical Physics*, vol. 338, no. 1, pp. 103–137, May 2015.
- [8] M. Tomamichel, M. Berta, and J. M. Renes, “Quantum coding with finite resources,” *Nature Communications*, vol. 7, p. 11419, May 2016.
- [9] M. Tomamichel and V. Y. F. Tan, “A tight upper bound for the third-order asymptotics for most discrete memoryless channels,” *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7041–7051, Nov 2013.
- [10] V. Y. F. Tan, “Asymptotic estimates in information theory with non-vanishing error probabilities,” *Foundations and Trends® in Communications and Information Theory*, vol. 10, no. 4, pp. 1–184, 2014.
- [11] V. Y. F. Tan and M. Tomamichel, “The third-order term in the normal approximation for the AWGN channel,” *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2430–2438, May 2015.
- [12] C. E. Shannon, “Probability of error for optimal codes in a Gaussian channel,” *Bell System Technical Journal*, vol. 38, no. 3, pp. 611–656, May 1959.
- [13] R. Gallager, *Information Theory and Reliable Communication*. Wiley, 1968.
- [14] R. M. Fano, *Transmission of Information, A Statistical Theory of Communications*. The MIT Press, 1961.
- [15] R. E. Blahut, *Principles and practice of information theory*. Addison-Wesley, 1987.

- [16] E. A. Haroutunian, M. E. Haroutunian, and A. N. Harutyunyan, “Reliability criteria in information theory and in statistical hypothesis testing,” *Foundations and Trends® in Communications and Information Theory*, vol. 4, no. 2–3, pp. 97–263, 2007.
- [17] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press (CUP), 2011.
- [18] H.-C. Cheng, M.-H. Hsieh, and M. Tomamichel, “Quantum Sphere-Packing Bounds with Polynomial Prefactors,” [arXiv:1704.05703 \[quant-ph\]](#).
- [19] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*. Springer, 1998.
- [20] Y. Altuğ and A. B. Wagner, “Moderate deviation analysis of channel coding: Discrete memoryless case,” in *2010 IEEE International Symposium on Information Theory*. Jun 2010.
- [21] —, “Moderate deviations in channel coding,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4417–4426, Aug 2014.
- [22] Y. Polyanskiy and S. Verdú, “Channel dispersion and moderate deviations limits for memoryless channels,” in *2010 48th Annual Allerton Conference on Communication, Control, and Computing*. Sep 2010.
- [23] A. Winter, “Coding theorems of quantum information theory,” *PhD Thesis, Universität Bielefeld*, 1999.
- [24] I. Sason, “Moderate deviations analysis of binary hypothesis testing,” in *2012 IEEE International Symposium on Information Theory Proceedings*. Jul 2012.
- [25] S. Watanabe and M. Hayashi, “Finite-length analysis on tail probability for Markov chain and application to simple hypothesis testing,” [arXiv:1401.3801](#).
- [26] C. Rouzé and N. Datta, “Finite blocklength and moderate deviation analysis of hypothesis testing of correlated quantum states and application to classical-quantum channels with memory,” [arXiv:1612.01464](#).
- [27] M. Hayashi, “Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding,” *Physical Review A*, vol. 76, no. 6, dec 2007.
- [28] H.-C. Cheng, M.-H. Hsieh and M. Tomamichel, “Sphere-Packing Bound for Symmetric Classical-Quantum Channels,” [arXiv:1701.02957](#).
- [29] M. Dalai and A. Winter, “Constant compositions in the sphere packing bound for classical-quantum channels,” in *2014 IEEE International Symposium on Information Theory*. Jun 2014.
- [30] K. M. R. Audenaert, M. Nussbaum, A. Szkoła, and F. Verstraete, “Asymptotic error rates in quantum hypothesis testing,” *Communications in Mathematical Physics*, vol. 279, no. 1, pp. 251–283, Feb 2008.
- [31] C. T. Chubb, V. Y. F. Tan, and M. Tomamichel, “Moderate deviation analysis for classical communication over quantum channels,” [arXiv:1701.03114 \[quant-ph\]](#).
- [32] L. Wang and R. Renner, “One-shot classical-quantum capacity and hypothesis testing,” *Physical Review Letters*, vol. 108, no. 20, May 2012.
- [33] L. V. Rozovsky, “Estimate from below for large-deviation probabilities of a sum of independent random variables with finite variances,” *Journal of Mathematical Sciences*, vol. 109, pp. 2192–2209, 2002.
- [34] H. Nagaoka and M. Hayashi, “An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses,” *IEEE Transactions on Information Theory*, vol. 53, no. 2, pp. 534–549, Feb 2007.
- [35] M. V. Burnashev and A. S. Holevo, “On the reliability function for a quantum communication channel,” *Problems of information transmission*, vol. 34, no. 2, pp. 97–107, 1998.
- [36] A. Holevo, “Reliability function of general classical-quantum channel,” *IEEE Transaction on Information Theory*, vol. 46, no. 6, pp. 2256–2261, 2000.
- [37] J. I. Fujii, R. Nakamoto, and K. Yanagi, “Remarks on concavity of the auxiliary function appearing in quantum reliability function in classical-quantum channels,” in *2005 IEEE International Symposium on Information Theory*. Jun 2005.
- [38] J. I. Fujii, R. Nakamoto, and K. Yanagi, “Concavity of the auxiliary function appearing in quantum reliability function,” *IEEE Transaction on Information Theory*, vol. 52, no. 7, pp. 3310–3313, 2006.

- [39] H.-C. Cheng and M.-H. Hsieh, “Concavity of the auxiliary function for classical-quantum channels,” *IEEE Transactions on Information Theory*, vol. 62, no. 10, pp. 5960 – 5965, 2016.
- [40] A. Winter, “Coding theorems of quantum information theory,” 1999, (PhD Thesis, Universität Bielefeld). [arXiv:quant-ph/9907077](#).
- [41] C. Shannon, R. Gallager, and E. Berlekamp, “Lower bounds to error probability for coding on discrete memoryless channels. I,” *Information and Control*, vol. 10, no. 1, pp. 65–103, Jan 1967.
- [42] J.-C. Bourin, “Matrix versions of some classical inequalities,” *Linear Algebra and its Applications*, vol. 446, no. 2–3, pp. 890–907, July 2006.
- [43] D. Petz, “Quasi-entropies for finite quantum systems,” *Reports on Mathematical Physics*, vol. 23, no. 1, pp. 57–65, Feb 1986.
- [44] M. Mosonyi and T. Ogawa, “Two approaches to obtain the strong converse exponent of quantum hypothesis testing for general sequences of quantum states,” *IEEE Transactions on Information Theory*, vol. 61, no. 12, pp. 6975–6994, Dec 2015.
- [45] S. M. Lin and M. Tomamichel, “Investigating properties of a family of quantum rényi divergences,” *Quantum Information Processing*, vol. 14, no. 4, pp. 1501–1512, Feb 2015.
- [46] M. Tomamichel, *Quantum Information Processing with Finite Resources*. Springer International Publishing, 2016.
- [47] N. J. Higham, *Functions of Matrices: Theory and Computation*. SIAM, Jan 2008.
- [48] M. Mosonyi and T. Ogawa, “Strong converse exponent for classical-quantum channel coding,” 2014 [arXiv:1409.3562 \[quant-ph\]](#).
- [49] R. Bhatia, *Matrix Analysis*, Springer New York, 1997.
- [50] R. E. Blahut, “Hypothesis testing and information theory,” *IEEE Transaction on Information Theory*, vol. 20, no. 4, pp. 405–417, Jul 1974.
- [51] N. Sharma and N. A. Warsi, “Fundamental bound on the reliability of quantum information transmission,” *Physical Review Letters*, vol. 110, no. 8, Feb 2013.
- [52] N. R. Chaganty and J. Sethuraman, “Strong Large Deviation and Local Limit Theorems,” *The Annals of Probability*, vol. 21, no. 3, pp. 1671–1690, 1993.
- [53] R. Sibson, “Information radius,” *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 14, no. 2, pp. 149–160, 1969.
- [54] I. Csiszár, “Generalized cutoff rates and Rényi’s information measures,” *IEEE Transactions on Information Theory*, vol. 41, no. 1, pp. 26–34, 1995.
- [55] M. Mosonyi and F. Hiai, “On the quantum Rényi relative entropies and related capacity formulas,” *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2474–2487, Apr 2011.
- [56] M. M. Wilde, A. Winter, and D. Yang, “Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy,” *Communications in Mathematical Physics*, vol. 331, no. 2, pp. 593–622, Jul 2014.
- [57] F. Hiai and D. Petz, *Introduction to Matrix Analysis and Applications*. Springer International Publishing, 2014.
- [58] M. Nussbaum and A. Szkoła, “The Chernoff lower bound for symmetric quantum hypothesis testing,” *Annals of Statistics*, vol. 37, no. 2, pp. 1040–1057, apr 2009.
- [59] H. Nagaoka, “The converse part of the theorem for quantum Hoeffding bound,” 2006 [arXiv:quant-ph/0611289](#).
- [60] Y. Altuğ and A. B. Wagner, “Refinement of the sphere-packing bound: Asymmetric channels,” *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1592–1614, Mar 2014.
- [61] B. Schumacher and M. D. Westmoreland, “Optimal signal ensembles,” *Physical Review A*, vol. 63, no. 2, Jan 2001.
- [62] X. Wang, W. Xie, and R. Duan, “Semidefinite programming strong converse bounds for classical capacity,” [arXiv:1610.06381 \[quant-ph\]](#).