

Distributed Quantum Hypothesis Testing against Product States under Zero-rate Communication Constraints

Sreejith Sreekumar, Mario Berta

Institute for Quantum Information

RWTH Aachen University, Germany

{sreekumar, berta}@physik.rwth-aachen.de

Christoph Hirche

Institute for Information Processing

University of Hanover, Germany

christoph.hirche@gmail.com

Hao-Chung Cheng

Department of Electrical Engineering

National Taiwan University, Taiwan

haochung@ntu.edu.tw

Abstract—The trade-offs between error probabilities in quantum hypothesis testing are by now well-understood in the centralized setting, but much less is known for distributed settings. Here, we study a distributed binary hypothesis testing problem to infer a bipartite quantum state shared between two remote parties, where one of these parties communicates to the tester at zero-rate, while the other party communicates to the tester at zero-rate or higher. As our main contribution, we derive an efficiently computable single-letter formula for the Stein’s exponent of this problem, when the state under the alternative is product. As a key tool for proving the converse direction of our results, we develop a quantum version of the blowing-up lemma which may be of independent interest.

I. INTRODUCTION

Quantum hypothesis testing to discriminate between two quantum states is perhaps the most fundamental and simplest form of inference on a quantum system. The performance of quantum hypothesis testing is well-known and characterized by the Helstrom-Holevo test which achieves the optimal trade-off between the type I and II error probabilities. Moreover, given an arbitrary number of independent and identical (i.i.d.) copies of quantum states, the best asymptotic rate of decay of error probabilities (or error-exponents) in different regimes of interest have also been ascertained [1]–[3]. These error-exponents have simple characterizations in terms of single-letter expressions involving quantum relative entropy [4] and its Rényi generalizations [5]–[9]. However, such expressions depend on the assumption that the tester, who performs the test, has direct access to the i.i.d. copies and can perform the optimal measurement to deduce the true hypothesis. We refer to such a scenario as the *centralized* setting. The situation dramatically changes when the tester has only remote or partial access to the quantum (sub-)systems. In contrast to the centralized setting, the performance of quantum hypothesis testing in such scenarios is much less understood.

Here, we consider a distributed binary hypothesis testing problem (see Figure 1) to discriminate between a bipartite quantum state shared between two parties, Alice (A) and Bob (B), with the following null and alternative hypotheses:

$$H_0 : \text{State on } AB \text{ is } \rho_{AB}, \quad (1a)$$

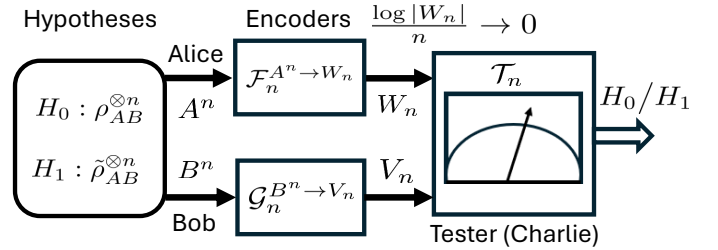


Fig. 1: Distributed quantum hypothesis testing under a zero-rate noiseless communication constraint. At least, one of the parties (Alice here) communicates at zero-rate to the tester (Charlie). The other party (Bob) communicates to Charlie at zero-rate or higher.

$$H_1 : \text{State on } AB \text{ is } \tilde{\rho}_{AB} := \tilde{\rho}_A \otimes \tilde{\rho}_B. \quad (1b)$$

Alice and Bob have access to as many i.i.d. copies of the true state as desired, and are allowed to perform local operations on the associated systems A^n and B^n , respectively. The output of the local operations are communicated to the tester Charlie, who performs the test. In other words, Alice and Bob apply completely positive trace-preserving (CPTP) linear maps (or quantum channels) $\mathcal{F}_n = \mathcal{F}_n^{A^n \rightarrow W_n}$ and $\mathcal{G}_n = \mathcal{G}_n^{B^n \rightarrow V_n}$, respectively, with $|W_n| \wedge |V_n| > 1$, where $|W_n|$ denotes the dimension of system W_n . Alice sends W_n and Bob sends V_n to Charlie over their respective noiseless channels. Let $\sigma_{W_n V_n}$ denote the state of (W_n, V_n) under the null and $\tilde{\sigma}_{W_n V_n}$ denote the state of the same systems under the alternative. Charlie applies a binary outcome POVM $\mathcal{T}_n = \{T_n, I - T_n\}$ on (W_n, V_n) to decide which hypothesis is true. The type I and type II error probabilities achieved by the test \mathcal{T}_n are

$$\alpha_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n) = \text{Tr}[(I - T_n)\sigma_{W_n V_n}],$$

$$\text{and } \beta_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n) = \text{Tr}[T_n \tilde{\sigma}_{W_n V_n}],$$

respectively.

We assume that at least one of the parties communicates at zero-rate to Charlie, which we take to be Alice without

loss of generality (it turns out that the results in this paper do not depend on whether this is Alice or Bob). The zero-rate communication constraint for Alice means that

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log |W_n| \rightarrow 0. \quad (2)$$

We are interested in the characterizing the *Stein's* exponent defined as

$$\theta(\epsilon, \rho_{AB}, \tilde{\rho}_{AB}) := \lim_{n \rightarrow \infty} -\frac{\log \bar{\beta}_n(\epsilon)}{n}, \quad (3)$$

if the above limit exists, where

$$\bar{\beta}_n(\epsilon) := \inf_{\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n} \{\beta_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n) : \alpha_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n) \leq \epsilon\}.$$

Zero-rate communication is practically relevant in scenarios where communication is expensive, e.g., sensor networks or communication in an adversarial environment. For instance, wireless sensor networks powered by batteries used for industrial automation, agriculture, smart cities, environmental monitoring or healthcare have limited energy budgets and typically monitor large amounts of data between successive communication phases with the central controller. Potential quantum applications include tasks in quantum sensing and metrology, which benefit from a spatially distributed network architecture (see e.g. [10]–[12] and references therein). Another pertinent application is covert inference, where zero-rate communication becomes essential to avoid detection by an adversary (see e.g. [13]–[16]).

In contrast to the centralized scenario, design of an optimal hypothesis testing scheme in distributed settings also involves an optimization over all feasible encoders (in addition to the test statistic). In distributed quantum settings, there is an additional complexity arising due to constraints on the kind of operations that could be performed on the system. For instance, such constraints could occur naturally due to restrictions on the set of feasible measurements (e.g., due to geographic separation) or the distributed processing of information post-measurement. This makes the characterization of Stein's exponent more challenging, and, even classically, single-letter expressions are known only in special cases. One such important setting is the zero-rate regime, which partly motivates our study.

As our main contribution, we obtain an efficiently computable single-letter formula for the Stein's exponent when the state under the alternative is the product of its marginals, i.e.,

$$\theta(\epsilon, \rho_{AB}, \tilde{\rho}_A \otimes \tilde{\rho}_B) = D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B), \quad \forall \epsilon \in (0, 1).$$

This characterization extends the analogous classical expression derived in [17] and [18] to the quantum setting. The proof of the above formula as usual involves establishing achievability (lower bound) and a converse (upper bound). For proving achievability, we use quantum-typicality based arguments inspired by [19]. For establishing the upper bound,

we derive a non-asymptotic strong converse¹ via a pinching-based argument [20] in conjunction with a quantum version of the blowing-up lemma [21]–[23] that we develop. The lower and upper bounds match asymptotically and characterize the Stein's exponent in terms of the desired expression.

A. Related Literature

Distributed hypothesis testing with the goal of testing for the joint distribution of data has been an active topic of research in classical information theory and statistics, with the characterization of Stein's exponent and other performance metrics explored in various multi-terminal settings. A multi-letter characterization of the Stein's exponent in a two-terminal setting where the communication happens over a noiseless (positive) rate-limited channel was first established in [24], along with a single-letter formula for testing against independence (i.e. testing a joint distribution vs the product of its marginals). Invoking the blowing-up lemma, a strong converse was also proven under a positivity assumption on the probability distribution under the alternative. Distributed hypothesis testing under a zero-rate noiseless communication constraint was introduced in [17], where a one-bit communication scheme indicating whether the observed sequence at each encoder is typical or not was proposed. Subsequently, the optimality of the one-bit scheme along with a strong converse was established in [18] by leveraging the blowing-up lemma. The trade-off between the type I and type II error-exponents in the same setting under a positive and zero-rate communication constraint was first explored in [25], where inner bounds were established (see also [26], and [27]–[32] for more recent progress and extensions).

In contrast to the above, analogous problems in quantum settings have been much less explored. The only exception that we are aware of is [33], which among other contributions, established a single-letter characterization of the Stein's exponent for testing against independence including a strong converse. Here, we consider the first quantum analogue of the problem studied in [17], [18]. We briefly compare our work with [33]. While [33] treats the positive rate communication constraint for testing against independence, we work in the zero-rate setting allowing arbitrary marginals $\tilde{\rho}_A$ and $\tilde{\rho}_B$. Also, our proofs involve markedly different techniques from those used in [33]. In particular, the converse proof in [33] relies on quantum reverse-hypercontractivity, whereas we employ a novel quantum version of the blowing-up lemma. Moreover, the strong converse in [33] is shown for a classical-quantum state ρ_{AB} , while our proof works for general ρ_{AB} .

B. Notation

Throughout, we consider the setting of a finite dimensional Hilbert space for the systems involved. The set of density operators (or quantum states) on Hilbert space of dimension d , is denoted by \mathcal{S}_d . $\text{Tr}[\cdot]$ signifies the trace operation. The notation \leq denotes the Löwner partial order in the context

¹Strong converse here refers to the optimal Stein's exponent being independent of the constraint, $\epsilon \in (0, 1)$, on the type I error probability.

of operators, i.e., for Hermitian operators H_1, H_2 , $H_1 \leq H_2$ means that $H_2 - H_1$ is positive semi-definite. I denotes the identity operator. For operators L_1, L_2 , $L_1 \ll L_2$ designates that the support of L_1 is contained in that of L_2 . For reals a, b , $a \wedge b := \min\{a, b\}$ and $a \vee b := \max\{a, b\}$. For a finite discrete set \mathcal{X} , a positive operator-valued measure (POVM) indexed by \mathcal{X} is a set $\mathcal{M} = \{M_x\}_{x \in \mathcal{X}}$ such that $M_x \geq 0$ for all x and $\sum_{x \in \mathcal{X}} M_x = I$. Such a POVM induces a measurement channel (quantum to classical channel) specified by

$$\mathcal{M}(\omega) := \sum_{x \in \mathcal{X}} \text{Tr}[M_x \omega] |x\rangle\langle x|.$$

For composite systems, we indicate the labels of the subsystems involved as subscript or superscript wherever convenient, e.g., ρ_{AB} for the state of bipartite system AB . The marginal ω_A (resp. ω_B) of a bipartite linear operator ω_{AB} is defined by taking partial trace with respect to B (resp. A).

II. MAIN RESULT

The next theorem which characterizes the Stein's exponent for the hypothesis test in (1) is our main result.

Theorem 1 (Single-letterization of Stein's exponent) *For any ρ_{AB} , $\tilde{\rho}_{AB} = \tilde{\rho}_A \otimes \tilde{\rho}_B$ and $\epsilon \in (0, 1)$,*

$$\theta(\epsilon, \rho_{AB}, \tilde{\rho}_{AB}) = D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B). \quad (4)$$

Before we prove Theorem 1, we discuss a simple implication of it for testing against independence, in which case $\tilde{\rho}_{AB} = \rho_A \otimes \rho_B$. Note that (4) implies that $\theta(\epsilon, \rho_{AB}, \rho_A \otimes \rho_B) = 0$. To compare this with the performance in the centralized setting, recall that the Stein's exponent in the latter case is equal to the mutual information evaluated with respect to ρ_{AB} (see, e.g., [34], [35] for a composite hypothesis testing version), which is positive except in the trivial case $\rho_{AB} = \rho_A \otimes \rho_B$. Hence, there is a strict gap between the performance under zero-rate and centralized setting as expected.

Proof. First, we show achievability of Stein's exponent given in (4), i.e., we establish that for all $\epsilon \in (0, 1]$,

$$\theta(\epsilon, \rho_{AB}, \tilde{\rho}_{AB}) \geq D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B).$$

Our proof relies on the concept of (relatively) typical projectors considered in [19] (see the full version of our paper [36, Proof of Theorem 2] for an alternative proof). For $\delta > 0$, let $P_{\delta,n}(\rho, \sigma) := \sum_{x^n \in \mathcal{A}_n(\delta, \rho, \sigma)} P_{x^n}$ denote the orthogonal projection considered in [19, Equation 10], where $P_{x^n} = |x^n\rangle\langle x^n|$ for an orthonormal eigenvector $|x^n\rangle$ of $\sigma^{\otimes n}$ and

$$\mathcal{A}_n(\delta, \rho, \sigma) := \left\{ x^n : e^{n(\text{Tr}[\rho \log \sigma] - \delta)} \leq \text{Tr}[\sigma^{\otimes n} P_{x^n}] \leq e^{n(\text{Tr}[\rho \log \sigma] + \delta)} \right\}.$$

Consider

$$\bar{M}_{\delta,n}^{A^n B^n}(\rho_{AB}, \tilde{\rho}_{AB}) = \hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A) \otimes \hat{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B),$$

where

$$\hat{M}_{\delta,n}(\rho, \sigma) = P_{\delta,n}(\rho, \sigma) P_{\delta,n}(\rho, \rho) P_{\delta,n}(\rho, \sigma),$$

for density operators ρ and σ . Alice and Bob first performs local measurements using binary outcome POVMs

$$\mathcal{M}_n^{A^n} = \{M_0^{A^n}, M_1^{A^n}\} := \{\hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A), I_{A^n} - \hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A)\},$$

$$\mathcal{M}_n^{B^n} = \{M_0^{B^n}, M_1^{B^n}\} := \{\hat{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B), I_{B^n} - \hat{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B)\},$$

respectively. The outcomes are sent to Charlie who decides in favour of the null hypothesis if and only if both outcomes are zero. We next evaluate the type I and type II error probability achieved by this one-bit communication scheme. First, note that for any commuting M_1, M_2 such that $0 \leq M_1, M_2 \leq I$ and density operator σ , we have

$$0 \leq \text{Tr}[\sigma(I - M_1)(I - M_2)]$$

$$= 1 - \text{Tr}[\sigma M_1] - \text{Tr}[\sigma M_2] + \text{Tr}[\sigma M_1 M_2]. \quad (5)$$

Applying (5) with $M_1 = \hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A) \otimes I_{B^n}$ and $M_2 = I_{A^n} \otimes \hat{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B)$, the type I success probability converges to one as follows:

$$\begin{aligned} & \text{Tr}[\bar{M}_{\delta,n}^{A^n B^n}(\rho_{AB}, \tilde{\rho}_{AB}) \rho_{AB}^{\otimes n}] \\ & \geq \text{Tr}[(\hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A) \otimes I_{B^n}) \rho_{AB}^{\otimes n}] \\ & \quad + \text{Tr}[(I_{A^n} \otimes \hat{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B)) \rho_{AB}^{\otimes n}] - 1 \\ & = \text{Tr}[\hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A) \rho_A^{\otimes n}] + \text{Tr}[\hat{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B) \rho_B^{\otimes n}] - 1 \\ & \rightarrow 1. \end{aligned}$$

In the above, the inequality follows from (5) and the final step is due to $\text{Tr}[\hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A) \rho_A^{\otimes n}] \rightarrow 1$ and $\text{Tr}[\hat{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B) \rho_B^{\otimes n}] \rightarrow 1$, which in turn follows from [19, Lemma 4(4)] and is a consequence of the weak law of large numbers. Hence, the type I error probability vanishes asymptotically. Moreover, the type II error probability can be upper bounded as

$$\begin{aligned} & \text{Tr}[\bar{M}_{\delta,n}^{A^n B^n}(\rho_{AB}, \tilde{\rho}_{AB}) (\tilde{\rho}_A^{\otimes n} \otimes \tilde{\rho}_B^{\otimes n})] \\ & = \text{Tr}[\hat{M}_{\delta,n}^{A^n}(\rho_A, \tilde{\rho}_A) \tilde{\rho}_A^{\otimes n}] \text{Tr}[\bar{M}_{\delta,n}^{B^n}(\rho_B, \tilde{\rho}_B) \tilde{\rho}_B^{\otimes n}] \\ & \leq e^{-n(D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B) - 4\delta)}, \end{aligned}$$

where the last inequality follows due to [19, Equation 20]. This implies that

$$\theta(\epsilon, \rho_{AB}, \tilde{\rho}_{AB}) \geq D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B) - 4\delta,$$

for all $\epsilon \in (0, 1]$. Since $\delta > 0$ is arbitrary, the claim follows.

Next we show the converse, i.e.,

$$\theta(\epsilon, \rho_{AB}, \tilde{\rho}_{AB}) \leq D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B). \quad (6)$$

First, consider ρ_{AB} is such that $\rho_A \otimes \rho_B \not\ll \tilde{\rho}_A \otimes \tilde{\rho}_B$. This implies that either $\rho_A \not\ll \tilde{\rho}_A$ or $\rho_B \not\ll \tilde{\rho}_B$. In either case, $D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B) = \infty$. Hence, (6) holds trivially. Next, consider that $\rho_A \otimes \rho_B \ll \tilde{\rho}_A \otimes \tilde{\rho}_B$. We will use the following non-asymptotic strong-converse which implies (6).

Lemma 1 (Non-asymptotic strong converse) *Let $\tilde{\rho}_{AB} = \tilde{\rho}_A \otimes \tilde{\rho}_B$, $(r_n)_{n \in \mathbb{N}}$ be a non-negative sequence and $0 \leq \epsilon < 1$. Then*

$$\begin{aligned} & \sup_{(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n): \alpha_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n) \leq \epsilon} -\frac{1}{n} \log \beta_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n) \\ & \leq \max_{\mathcal{M}_n \in \text{PLO}_n} \min_{\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})} \frac{D(\mathcal{M}_n(\hat{\rho}_{AB}^n) \| \mathcal{M}_n(\tilde{\rho}_{AB}^{\otimes n}))}{n(1 - 2e^{-2r_n^2})} \\ & \quad + \frac{2}{n} \log \bar{\gamma}_n(\epsilon_n, r_n) + \frac{1}{n(1 - 2e^{-2r_n^2})}, \end{aligned} \quad (7)$$

where PLO_n is the class of all rank-one local projective measurements, $\epsilon_n = (1 - \epsilon)/|W_n|^2$, $\mathcal{D}_n(\rho_{AB}) := \{\hat{\rho}_{AB}^n : \hat{\rho}_A^n = \rho_A^{\otimes n}, \hat{\rho}_B^n = \rho_B^{\otimes n}\}$,

$$\bar{\gamma}_n(\epsilon_n, r_n) := \frac{2(d_A \vee d_B)^{\lceil l_n(\epsilon_n, r_n) \rceil} \sum_{l=1}^{\lceil l_n(\epsilon_n, r_n) \rceil} \binom{n}{l}}{\epsilon_n (\bar{\mu}_{\min}(\tilde{\rho}_{AB}))^{\lceil l_n(\epsilon_n, r_n) \rceil}}, \quad (8)$$

$$l_n(\epsilon_n, r_n) := \sqrt{n} \left(\sqrt{-0.5 \log(0.5\epsilon_n)} + r_n \right), \quad (9)$$

$$\bar{\mu}_{\min}(\tilde{\rho}_{AB}) := \min_{x, \bar{x} \in \mathcal{X}_+ \times \bar{\mathcal{X}}_+} \langle x\bar{x} | \tilde{\rho}_{AB} | x\bar{x} \rangle, \quad (10)$$

d_A (resp. d_B) is the dimension of the Hilbert space associated with A (resp. B), and $\{|x\rangle\}_{x \in \mathcal{X}_+}$ (resp. $\{|\bar{x}\rangle\}_{\bar{x} \in \bar{\mathcal{X}}_+}$) is the set of orthonormal eigenvectors corresponding to positive eigenvalues in the spectral decomposition of ρ_A (resp. ρ_B).

To prove (6) from (7), we first show that

$$\begin{aligned} & \lim_{n \rightarrow \infty} \max_{\mathcal{M}_n \in \text{PLO}_n} \min_{\substack{\hat{\rho}_{AB}^n \\ \in \mathcal{D}_n(\rho_{AB})}} \frac{D(\mathcal{M}_n(\hat{\rho}_{AB}^n) \| \mathcal{M}_n(\tilde{\rho}_{AB}^{\otimes n}))}{n(1 - 2e^{-2r_n^2})} \\ & = D(\rho_A \| \tilde{\rho}_A) + D(\rho_B \| \tilde{\rho}_B). \end{aligned} \quad (11)$$

To see this, note that for any $\mathcal{M}_n = \mathcal{P}_n^{A^n} \otimes \mathcal{P}_n^{B^n} \in \text{PLO}$ and $\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})$, we have

$$\begin{aligned} & D(\mathcal{M}_n(\hat{\rho}_{AB}^n) \| \mathcal{M}_n(\tilde{\rho}_{AB}^{\otimes n})) \\ & = D(\mathcal{M}_n(\hat{\rho}_{AB}^n) \| \mathcal{M}_n(\hat{\rho}_A^n \otimes \hat{\rho}_B^n)) + D(\mathcal{P}_n^{A^n}(\hat{\rho}_A^n) \| \mathcal{P}_n^{A^n}(\tilde{\rho}_A^{\otimes n})) \\ & \quad + D(\mathcal{P}_n^{B^n}(\hat{\rho}_B^n) \| \mathcal{P}_n^{B^n}(\tilde{\rho}_B^{\otimes n})) \\ & = D(\mathcal{M}_n(\hat{\rho}_{AB}^n) \| \mathcal{M}_n(\hat{\rho}_A^n \otimes \hat{\rho}_B^n)) + D(\mathcal{P}_n^{A^n}(\rho_A^{\otimes n}) \| \mathcal{P}_n^{A^n}(\tilde{\rho}_A^{\otimes n})) \\ & \quad + D(\mathcal{P}_n^{B^n}(\rho_B^{\otimes n}) \| \mathcal{P}_n^{B^n}(\tilde{\rho}_B^{\otimes n})), \end{aligned}$$

where the last equality follows because $\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})$ implies that $\hat{\rho}_A^n = \rho_A^{\otimes n}$ and $\hat{\rho}_B^n = \rho_B^{\otimes n}$. Taking minimum over $\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})$, we obtain

$$\begin{aligned} & \min_{\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})} D(\mathcal{M}_n(\hat{\rho}_{AB}^n) \| \mathcal{M}_n(\tilde{\rho}_{AB}^{\otimes n})) \\ & = D(\mathcal{P}_n^{A^n}(\rho_A^{\otimes n}) \| \mathcal{P}_n^{A^n}(\tilde{\rho}_A^{\otimes n})) + D(\mathcal{P}_n^{B^n}(\rho_B^{\otimes n}) \| \mathcal{P}_n^{B^n}(\tilde{\rho}_B^{\otimes n})), \end{aligned}$$

because relative entropy is non-negative and hence the minimum is achieved by $\hat{\rho}_{AB}^n = \hat{\rho}_A^n \otimes \hat{\rho}_B^n = \rho_A^{\otimes n} \otimes \rho_B^{\otimes n}$. Normalizing by n and maximizing over $\mathcal{M}_n \in \text{PLO}_n$ leads to

$$\begin{aligned} & \max_{\mathcal{M}_n \in \text{PLO}_n} \min_{\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})} \frac{D(\mathcal{M}_n(\hat{\rho}_{AB}^n) \| \mathcal{M}_n(\tilde{\rho}_{AB}^{\otimes n}))}{n} \\ & = \frac{D_{\text{ALL}_n}(\rho_A^{\otimes n} \| \tilde{\rho}_A^{\otimes n})}{n} + \frac{D_{\text{ALL}_n}(\rho_B^{\otimes n} \| \tilde{\rho}_B^{\otimes n})}{n}, \end{aligned}$$

since measured relative entropy with respect to all measurements is same as over all orthogonal rank-one projective measurements [37]. Taking limit $n \rightarrow \infty$ and using $r_n \rightarrow \infty$, (11) follows since for any density operators ρ, σ (see e.g. [38])

$$\lim_{n \rightarrow \infty} \frac{D_{\text{ALL}_n}(\rho^{\otimes n} \| \sigma^{\otimes n})}{n} = D(\rho \| \sigma). \quad (12)$$

Having shown (11), we next choose r_n such that the last two terms in (7) vanishes. The last term converges to zero for any $r_n \rightarrow \infty$. Hence, we only need to ensure that $\log \bar{\gamma}_n(\epsilon_n, r_n)/n \rightarrow 0$ when $\rho_A \otimes \rho_B \ll \tilde{\rho}_{AB}$. Let $r_n = n^{1/3}$. Note that $\rho_A \otimes \rho_B \ll \tilde{\rho}_{AB}$ implies that $\bar{\mu}_{\min}(\tilde{\rho}_{AB}) > 0$. Using $\binom{n}{l} \leq (ne/l)^l$, we have

$$\begin{aligned} \bar{\gamma}_n(\epsilon_n, r_n) & := \frac{2(d_A \vee d_B)^{\lceil l_n(\epsilon_n, r_n) \rceil} \sum_{l=1}^{\lceil l_n(\epsilon_n, r_n) \rceil} \binom{n}{l}}{\epsilon_n (\bar{\mu}_{\min}(\tilde{\rho}_{AB}))^{\lceil l_n(\epsilon_n, r_n) \rceil}} \\ & \leq \frac{2(d_A \vee d_B)^{\lceil l_n(\epsilon_n, r_n) \rceil} \lceil l_n(\epsilon_n, r_n) \rceil (ne)^{\lceil l_n(\epsilon_n, r_n) \rceil}}{\epsilon_n (\bar{\mu}_{\min}(\tilde{\rho}_{AB}))^{\lceil l_n(\epsilon_n, r_n) \rceil}}. \end{aligned}$$

For the given choice of r_n , $l_n(\epsilon_n, r_n) = o(n)$ (see (9)) since $\log |W_n| = o(n)$ due to (2). Moreover, for $\epsilon_n = (1 - \epsilon)/|W_n|^2$, $\log \epsilon_n = o(n)$. Consequently, $\log(\bar{\gamma}_n(\epsilon_n, r_n))/n \rightarrow 0$. From the above, (6) follows from (7) by taking limit superior w.r.t. n , and using (11). \square

Due to space constraints, we will only provide a sketch of the proof of Lemma 1. Full details can be found in [36, Proof of Lemma 13].

1) Sketch of Proof of Lemma 1: A key ingredient of the proof is the following bipartite quantum analogue of the blowing-up lemma [21]–[23], which at a high-level expresses a concentration of measure phenomenon.

Lemma 2 (Bipartite version of quantum blowing-up lemma) *Suppose $0 < \epsilon_n \leq 1$, $0 \leq M_n^{A^n} \times M_n^{B^n} \leq I_{A^n B^n}$, and $\rho_{AB} \in \mathcal{S}_{d_A d_B}$ be such that $\text{Tr}[\rho_A^{\otimes n} M_n^{A^n}] \wedge \text{Tr}[\rho_B^{\otimes n} M_n^{B^n}] \geq \epsilon_n$ for all $n \in \mathbb{N}$. Then, for any $\sigma_{AB} \in \mathcal{S}_{d_A d_B}$ and non-negative sequence $(r_n)_{n \in \mathbb{N}}$, there exists a projector $0 \leq P_n^{A^n} \otimes P_n^{B^n} \leq I_{A^n B^n}$ such that*

$$\text{Tr}[\rho_A^{\otimes n} P_n^{A^n}] \wedge \text{Tr}[\rho_B^{\otimes n} P_n^{B^n}] \geq 1 - e^{-2r_n^2}, \quad (13a)$$

$$\begin{aligned} \text{Tr}[\sigma_{AB}^{\otimes n} (P_n^{A^n} \otimes P_n^{B^n})] & \leq \text{Tr}[(M_n^{A^n} \otimes M_n^{B^n}) \sigma_{AB}^{\otimes n}] \\ & \quad \times \bar{\gamma}_n^2(\epsilon_n, r_n), \end{aligned} \quad (13b)$$

where $\bar{\gamma}_n(\epsilon_n, r_n)$ is as given in (8) with σ_{AB} in place of $\tilde{\rho}_{AB}$.

We omit the proof of Lemma 2, which can be found in [36, Proof of Lemma 15].

Proceeding with the proof of Lemma 1, we may assume without loss of generality that $V_n = B^n$ and $\mathcal{G}_n^{B^n \rightarrow V^n} = \mathcal{I}^{B^n \rightarrow B^n}$. Let $\mathcal{F}_n^{A^n \rightarrow W_n}$ be an arbitrary encoder (CPTP map),

$$\sigma_{W_n B^n} := (\mathcal{F}_n^{A^n \rightarrow W_n} \otimes \mathcal{I}^{B^n \rightarrow B^n})(\rho_{AB}^{\otimes n}),$$

$$\tilde{\sigma}_{W_n B^n} := (\mathcal{F}_n^{A^n \rightarrow W_n} \otimes \mathcal{I}^{B^n \rightarrow B^n})(\tilde{\rho}_{AB}^{\otimes n}),$$

and $\mathcal{T}_n = \{M_{W_n B^n}, I_{W_n B^n} - M_{W_n B^n}\}$ be any binary outcome POVM. Consider the spectral decomposition $\tilde{\sigma}_{W_n} =$

$\sum_{w_n \in \mathcal{W}_n} \lambda_{w_n} P_{w_n}$, where $\{P_{w_n}\}_{w_n \in \mathcal{W}_n}$ is a set of orthogonal rank-one projectors such that $\sum_{w_n \in \mathcal{W}_n} P_{w_n} = I_{W_n}$. Let $\Pi_{W_n}(\cdot)$ denote the pinching map² (see e.g. [38]) w.r.t. these projectors, i.e.,

$$\Pi_{W_n}(\omega) = \sum_{w_n \in \mathcal{W}_n} P_{w_n} \omega P_{w_n}.$$

The key idea behind the proof is to use pinching map to construct a new test $\bar{\mathcal{T}}_n = \{\bar{M}_{W_n B^n}, I_{W_n B^n} - \bar{M}_{W_n B^n}\}$ satisfying two properties. Firstly, $\bar{M}_{W_n B^n}$ can be written as a separable sum, i.e., sum of tensor products of positive operators with the number of terms in the sum scaling at zero-rate with n . Secondly, the pinching operation is such that the error probabilities achieved by $\bar{\mathcal{T}}_n$ are not too different (in the exponent) from those achieved by \mathcal{T}_n . The separable decomposition of $\bar{M}_{W_n B^n}$ enables leveraging the bipartite version of the quantum blowing-up lemma to obtain a new POVM that achieves a vanishing type I error probability with a negligible decrease in the type II error exponent. Then, relating the error probabilities achieved by the modified and original test leads to the desired claim.

Define

$$\begin{aligned} \bar{M}_{W_n B^n} &:= (\Pi_{W_n} \otimes \mathcal{I}^{B^n \rightarrow B^n})(M_{W_n B^n}) \\ &= \sum_{w_n \in \mathcal{W}_n} (P_{w_n} \otimes I_{B^n}) M_{W_n B^n} (P_{w_n} \otimes I_{B^n}). \end{aligned} \quad (14)$$

From the pinching inequality [20], we have

$$\bar{M}_{W_n B^n} \geq \frac{M_{W_n B^n}}{|W_n|}. \quad (15)$$

Then, $\alpha_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n) \leq \epsilon$ and (15) implies

$$\text{Tr}[\sigma_{W_n B^n} \bar{M}_{W_n B^n}] \geq \frac{\text{Tr}[\sigma_{W_n B^n} M_{W_n B^n}]}{|W_n|} \geq \frac{1 - \epsilon}{|W_n|}. \quad (16)$$

Next, observe that $\bar{M}_{W_n B^n}$ can be written as

$$\bar{M}_{W_n B^n} = \sum_{w_n \in \mathcal{W}_n} P_{w_n}^{W_n} \otimes M_{w_n}^{B^n}, \quad (17)$$

for some $\{M_{w_n}^{B^n}\}_{w_n \in \mathcal{W}_n}$ such that $M_{w_n}^{B^n} \geq 0$ for all $w_n \in \mathcal{W}_n$ and $\sum_{w_n \in \mathcal{W}_n} M_{w_n}^{B^n} = M_{B^n}$. This implies that

$$\text{Tr}[\sigma_{W_n B^n} \bar{M}_{W_n B^n}] = \sum_{w_n} \text{Tr}[(M_{w_n}^{A^n} \otimes M_{w_n}^{B^n}) \rho_{AB}^{\otimes n}], \quad (18)$$

where $M_{w_n}^{A^n} := \mathcal{F}_n^{\dagger W_n \rightarrow A^n}(P_{w_n}^{W_n})$ and $\mathcal{F}_n^{\dagger W_n \rightarrow A^n}$ is the adjoint map of $\mathcal{F}_n^{A^n \rightarrow W_n}$. Note that $0 \leq M_{w_n}^{A^n} \leq I_{A^n}$ and $\sum_{w_n \in \mathcal{W}_n} M_{w_n}^{A^n} = I_{A^n}$ since $\mathcal{F}_n^{\dagger W_n \rightarrow A^n}$ is a completely positive unital map, being the adjoint of a CPTP map (see e.g. [38]). From (16) and (18), we obtain

$$\sum_{w_n \in \mathcal{W}_n} \text{Tr}[(M_{w_n}^{A^n} \otimes M_{w_n}^{B^n}) \rho_{AB}^{\otimes n}] \geq \frac{1 - \epsilon}{|W_n|}.$$

²Note that we perform pinching w.r.t. rank-one orthogonal projectors which is slightly different from the usual pinching operation, where the projectors are formed by combining eigenprojections corresponding to same eigenvalues.

Hence, there exists some $w^* \in \mathcal{W}_n$ such that

$$\text{Tr}[\rho_{AB}^{\otimes n} (M_{w^*}^{A^n} \otimes M_{w^*}^{B^n})] \geq \frac{1 - \epsilon}{|W_n|^2}.$$

Since $0 \leq M_{w^*}^{A^n} \leq I_{A^n}$ and $0 \leq M_{w^*}^{B^n} \leq I_{B^n}$,

$$\text{Tr}[\rho_A^{\otimes n} M_{w^*}^{A^n}] \wedge \text{Tr}[\rho_B^{\otimes n} M_{w^*}^{B^n}] \geq \frac{1 - \epsilon}{|W_n|^2}.$$

By Lemma 2, there exists $0 \leq P_n^{+A^n} \leq I_{A^n}$ and $0 \leq P_n^{+B^n} \leq I_{B^n}$ such that

$$\text{Tr}[\rho_A^{\otimes n} P_n^{+A^n}] \wedge \text{Tr}[\rho_B^{\otimes n} P_n^{+B^n}] \geq 1 - e^{-2r_n^2}, \quad (19)$$

$$\begin{aligned} \text{and } \text{Tr}[\hat{\rho}_{AB}^{\otimes n} (P_n^{+A^n} \otimes P_n^{+B^n})] \\ \leq \bar{\gamma}_n^2(\epsilon_n, r_n) \text{Tr}[(M_{w^*}^{A^n} \otimes M_{w^*}^{B^n}) \hat{\rho}_{AB}^{\otimes n}], \end{aligned} \quad (20)$$

where $\bar{\gamma}_n(\epsilon_n, r_n)$ is as defined in (8) with $\epsilon_n := (1 - \epsilon)/|W_n|^2$. Since $\hat{\rho}_A^n = \rho_A^{\otimes n}$ and $\hat{\rho}_B^n = \rho_B^{\otimes n}$ for any $\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})$, we have from (19) that

$$\min_{\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})} \text{Tr}[\hat{\rho}_A^n P_n^{+A^n}] \wedge \text{Tr}[\hat{\rho}_B^n P_n^{+B^n}] \geq 1 - e^{-2r_n^2}.$$

This implies that for any $\hat{\rho}_{AB}^n \in \mathcal{D}_n(\rho_{AB})$,

$$\begin{aligned} \text{Tr}[\hat{\rho}_{AB}^n (P_n^{+A^n} \otimes P_n^{+B^n})] \\ \stackrel{(a)}{\geq} \text{Tr}[\hat{\rho}_{AB}^n (P_n^{+A^n} \otimes I_{B^n})] + \text{Tr}[\hat{\rho}_{AB}^n (I_{A^n} \otimes P_n^{+B^n})] - 1 \\ = \text{Tr}[\hat{\rho}_A^n P_n^{+A^n}] + \text{Tr}[\hat{\rho}_B^n P_n^{+B^n}] - 1 \\ \geq 1 - 2e^{-2r_n^2}, \end{aligned} \quad (21)$$

where (a) used (5). Using (20) and $\Pi_{W_n}(\tilde{\sigma}_{W_n}) = \tilde{\sigma}_{W_n}$, we can further show that

$$\text{Tr}[\hat{\rho}_{AB}^{\otimes n} (P_n^{+A^n} \otimes P_n^{+B^n})] \leq \bar{\gamma}_n^2(\epsilon_n, r_n) \beta_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n).$$

Consider the local POVM $\mathcal{M}_n^+ := \mathcal{M}_+^{A^n} \otimes \mathcal{M}_+^{B^n}$, where $\mathcal{M}_+^{A^n} := \{P_n^{+A^n}, I - P_n^{+A^n}\}$ and $\mathcal{M}_+^{B^n} := \{P_n^{+B^n}, I - P_n^{+B^n}\}$. Using (21) and the above inequality, it is possible via an argument involving the log-sum inequality to relate $\beta_n(\mathcal{F}_n, \mathcal{G}_n, \mathcal{T}_n)$ to $D(\mathcal{M}_n^+(\hat{\rho}_{AB}^n) \| \mathcal{M}_n^+(\rho_{AB}^{\otimes n}))$, eventually leading to (7). Due to space constraints, we omit the details and refer to [36, Proof of Lemma 13].

III. CONCLUDING REMARKS

We derived a single-letter expression for the Stein's exponent of a distributed quantum hypothesis testing problem under zero-rate noiseless communication constraint when the state under the alternative is of product form. When at least one of the parties is constrained to communicate classical information to the tester at zero-rate, a multi-letter characterization of this exponent in terms of max-min optimization of regularized measured relative entropy can be established [36]. Looking ahead, it would be worthwhile to investigate more general instances where an efficiently computable expression for the Stein's exponent can be derived. Also of interest is to explore the trade-offs between the (Hoeffding's) exponents of both the type I and type II error probabilities as well as a computable characterization of the Chernoff's exponent.

REFERENCES

- [1] F. Hiai and D. Petz, “The proper formula for relative entropy and its asymptotics in quantum probability,” *Commun. Math. Phys.*, vol. 143, no. 1, pp. 99–114, 1991.
- [2] M. Nussbaum and A. Szkola, “The Chernoff lower bound for symmetric quantum hypothesis testing,” *Ann. Stat.*, vol. 37, 08 2006.
- [3] K. Audenaert, M. Nussbaum, A. Szkola, and F. Verstraete, “Asymptotic error rates in quantum hypothesis testing,” *Commun. Math. Phys.*, vol. 279, no. 1, pp. 251–283, 2008.
- [4] H. Umegaki, “Conditional expectations in an operator algebra IV (entropy and information),” *Kodai Math. Seminar Rep.*, vol. 14, no. 2, pp. 59–85, 1962.
- [5] A. Rényi, “On measures of entropy and information,” in *Proc. 4th Berkeley Symp. Math. Stat. Probab.*, vol. 1. Berkeley: University of California Press, 1961, pp. 547–561.
- [6] D. Petz, “Quasi-entropies for states of a von Neumann algebra,” *Publ. Res. Inst. Math. Sci.*, vol. 21, no. 4, pp. 787–800, Aug. 1985.
- [7] —, “Quasi-entropies for finite quantum systems,” *Rep. Math. Phys.*, vol. 23, no. 1, pp. 57–65, Feb. 1986.
- [8] M. Müller-Lennert, F. Dupuis, O. Szechr, S. Fehr, and M. Tomamichel, “On quantum Rényi entropies: A new generalization and some properties,” *J. Math. Phys.*, vol. 54, no. 12, 2013.
- [9] 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,” *Commun. Math. Phys.*, vol. 331, pp. 593–622, 2014.
- [10] T. J. Proctor, P. A. Knott, and J. A. Dunningham, “Networked quantum sensing,” *arXiv:1702.04271 [quant-ph]*, 2017.
- [11] C. Zhan and H. Gupta, “Quantum sensor network algorithms for transmitter localization,” in *2023 IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Los Alamitos, CA, USA, Sep. 2023, pp. 659–669.
- [12] M. Rivero-Angeles, “Quantum-based wireless sensor networks: A review and open questions,” *Int. J. Distrib. Sens. Netw.*, vol. 17, Oct. 2021.
- [13] B. A. Bash, D. Goeckel, and D. Towsley, “Limits of reliable communication with low probability of detection on AWGN channels,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, 2013.
- [14] B. Bash, A. Gheorghe, M. Patel, J. Habif, D. Goeckel, D. Towsley, and S. Guha, “Quantum-secure covert communication on bosonic channels,” *Nat. Commun.*, vol. 6, 10 2015.
- [15] L. Wang, G. W. Wornell, and L. Zheng, “Fundamental limits of communication with low probability of detection,” *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.
- [16] M. Bloch, “Covert communication over noisy channels: A resolvability perspective,” *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.
- [17] T. S. Han, “Hypothesis testing with multiterminal data compression,” *IEEE Trans. Inf. Theory*, vol. 33, no. 6, pp. 759–772, Nov. 1987.
- [18] H. M. H. Shalaby and A. Papamarcou, “Multiterminal detection with zero-rate data compression,” *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 254–267, Mar. 1992.
- [19] I. Bjelakovic and R. Siegmund-Schultze, “Quantum Stein’s lemma revisited, inequalities for quantum entropies, and a concavity theorem of Lieb,” *arXiv:quant-ph/0307170v2*, 2012.
- [20] M. Hayashi, “Optimal sequence of quantum measurements in the sense of Stein’s lemma in quantum hypothesis testing,” *J. Phys. A: Math. Gen.*, vol. 35, no. 50, p. 10759, Dec. 2002.
- [21] R. Ahlswede, P. Gacs, and J. Körner, “Bounds on conditional probabilities with applications in multi-user communication,” *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 34(2), pp. 157–177, vol. 34, 01 1976.
- [22] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.
- [23] K. Marton, “A simple proof of the blowing-up lemma (corresp.),” *IEEE Trans. Inf. Theory*, vol. 32, no. 3, pp. 445–446, 1986.
- [24] R. Ahlswede and I. Csiszár, “Hypothesis testing with communication constraints,” *IEEE Trans. Inf. Theory*, vol. 32, no. 4, pp. 533–542, Jul. 1986.
- [25] T. S. Han and K. Kobayashi, “Exponential-type error probabilities for multiterminal hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 2–14, Jan. 1989.
- [26] T. S. Han and S. Amari, “Statistical inference under multiterminal data compression,” *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2300–2324, Oct. 1998.
- [27] W. Zhao and L. Lai, “Distributed testing with zero-rate compression,” in *2015 IEEE Int. Symp. Inf. Theory (ISIT)*, 2015, pp. 2792–2796.
- [28] S. Watanabe, “Neyman-Pearson test for zero-rate multiterminal hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 4923–4939, Jul. 2018.
- [29] S. Sreekumar, A. Cohen, and D. Gündüz, “Privacy-aware distributed hypothesis testing,” *Entropy*, vol. 22, no. 6, Jun. 2020.
- [30] A. Gilani, S. B. Amor, S. Salehkalaibar, and V. Tan, “Distributed hypothesis testing with privacy constraints,” *Entropy*, vol. 21, no. 478, pp. 1–27, May 2019.
- [31] S. Salehkalaibar and V. Y. F. Tan, “Distributed sequential hypothesis testing with zero-rate compression,” in *Proc. 2021 IEEE Inf. Theory Workshop (ITW)*, Kanazawa, Japan, 2021, pp. 1–5.
- [32] X. Xu and S.-L. Huang, “On distributed learning with constant communication bits,” *IEEE J. Sel. Areas Inf. Theory*, vol. 3, no. 1, pp. 125–134, Mar. 2022.
- [33] H.-C. Cheng, N. Datta, and C. Rouzé, “Strong converse bounds in quantum network information theory,” *IEEE Trans. Inf. Theory*, vol. 67, no. 4, pp. 2269–2292, 2021.
- [34] M. Hayashi and M. Tomamichel, “Correlation detection and an operational interpretation of the Rényi mutual information,” *J. Math. Phys.*, vol. 57, no. 10, p. 102201, 10 2016.
- [35] M. Berta, F. Brandao, and C. Hirche, “On composite quantum hypothesis testing,” *Commun. Math. Phys.*, vol. 385, 07 2021.
- [36] S. Sreekumar, C. Hirche, H.-C. Cheng, and M. Berta, “Distributed quantum hypothesis testing under zero-rate communication constraints,” *arXiv:2410.08937v2*, 2024.
- [37] M. Berta, O. Fawzi, and M. Tomamichel, “On variational expressions for quantum relative entropies,” *Lett. Math. Phys.*, vol. 107, no. 12, pp. 2239–2265, Dec. 2015.
- [38] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Springer, 2015.