Discrimination of Quantum States Under Locality Constraints in the Many-Copy Setting

Hao-Chung Cheng, Andreas Winter, Nengkun Yu

1 Department of Electrical Engineering and Graduate Institute of Communication Engineering, National Taiwan University, Taipei 106, Taiwan (R.O.C.). E-mail: haochung.ch@gmail.com
2 Department of Mathematics, National Taiwan University, Taipei 106, Taiwan (R.O.C.)
3 Center for Quantum Science and Engineering, National Taiwan University, Taipei 106, Taiwan (R.O.C.)
4 Physics Division, National Center for Theoretical Sciences, Taipei 10617, Taiwan (R.O.C.)
5 Hon Hai (Foxconn) Quantum Computing Center, New Taipei City 236, Taiwan (R.O.C.)
6 ICREA-Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain. E-mail: andreas.winter@uab.cat
7 Departament de Física, Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, 08193 Barcelona, Spain
8 Computer Science Department, Stony Brook University, New York, NY, USA. E-mail: nengkunyu@gmail.com
9 Centre for Quantum Software and Information and Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW 2007, Australia

Received: 1 August 2021 / Accepted: 14 August 2023
Published online: 14 September 2023 – © The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2023

Abstract: We study quantum hypothesis testing between orthogonal states under restricted local measurements in the many-copy scenario. For testing arbitrary multipartite entangled pure state against its orthogonal complement state via the local operation and classical communication (LOCC) operation, we prove that the optimal average error probability always decays exponentially in the number of copies. Second, we provide a sufficient condition for the LOCC operations to achieve the same performance as the positive-partial-transpose (PPT) operations. We further show that testing a maximally entangled state against its orthogonal complement and testing extremal Werner states both fulfill the above-mentioned condition. Hence, we determine the explicit expressions for the optimal average error probability, the optimal trade-off between the type-I and type-II errors, and the associated Chernoff, Stein, Hoeffding, and strong converse exponents. Then, we show an infinite asymptotic separation between the separable (SEP) and PPT operations by providing a pair of states constructed from an unextendible product basis (UPB). The quantum states can be distinguished perfectly by PPT operations, while the optimal error probability, with SEP operations, admits an exponential lower bound. On the technical side, we prove this result by providing a quantitative version of the well-known statement that the tensor product of UPBs is a UPB.

1. Introduction

Testing whether a system has a specific property is fundamental. In statistics, this problem is called hypothesis testing [1]. It has substantial applications in numerous fields, such as information sciences [2–8], computational learning theory [9–12], property and distribution testing [13–16], and differential privacy [17–21].

The most basic form of hypothesis testing is binary hypothesis testing, i.e., testing a null hypothesis $H_0$ against an alternative hypothesis $H_1$. In quantum computing, the two
hypotheses are modeled by quantum states $\rho_0$ and $\rho_1$, respectively. To distinguish the two quantum states, one has to perform a test $T$, or equivalently, a two-outcome positive-operator valued measure (POVM) measurement $\{T, 1 - T\}$ on the received state, where $0 \leq T \leq 1$ is a quantum observable. Such a test $T$ incurs two types of errors: the type-I error probability $\alpha(T) := \Pr[H_1|H_0] = \text{Tr} [\rho_0 (1 - T)]$, the probability of accepting $H_1$ when $H_0$ is true; and the type-II error probability $\beta(T) := \Pr[H_0|H_1] = \text{Tr} [\rho_1 T]$, the probability of deciding for $H_0$ when actually $H_1$ is true. Subsequently, we simply term $\alpha(T)$ and $\beta(T)$ as the type-I error and the type-II error, respectively. If the prior probabilities of the hypotheses are known, say $p$ and $1 - p$, we measure the performance of the decision scheme by calculating the average (Bayes) error probability. We name this the Bayesian approach, and specifically the symmetric setting, $p = 1 - p = \frac{1}{2}$, when the two hypotheses are equally likely. In most practical situations where the prior probabilities are unknown, the Neyman–Pearson approach is used to analyze the trade-off between the two types of errors. We name this the asymmetric setting.

In the Bayesian setting, the optimal average error probability is defined as

$$P_e(\rho_0, \rho_1; p) := \inf_{0 \leq T \leq 1} \{p \alpha(T) + (1 - p) \beta(T)\}$$

for $p := \Pr[H_0] \in (0, 1)$. Helstrom and Holevo [22] proved a closed-form expression of $P_e$ and showed that the optimal test is achieved by projection onto the positive support of $p \rho_0 - (1 - p) \rho_1$. This measurement can be viewed as a quantum generalization of the classical Neyman–Pearson test, as described in [23–26].

In the present paper, we are concerned with the many-copy and asymptotic behavior of $P_e(\rho_0^\otimes n, \rho_1^\otimes n; p)$, where $n$ identical copies of states are prepared. Then, the celebrated quantum Chernoff theorem [27–29] establishes that

$$\text{Chernoff}(\rho_0, \rho_1) := \lim_{n \to \infty} - \frac{1}{n} \log P_e(\rho_0^\otimes n, \rho_1^\otimes n; p) = - \min_{0 \leq s \leq 1} \log \text{Tr} \left[ \rho_0^{1-s} \rho_1^s \right]. \quad (1)$$

That is, the Chernoff exponent determines the convergence rate of the error probability. Because of this result in the asymptotic setting, we consider all the Bayesian error probabilities $P_e(\rho_0^\otimes n, \rho_1^\otimes n; p)$ as pertaining to the symmetric setting, as long as $p$ does not depend on $n$.

In the asymmetric setting, one aims to study the asymptotic functional dependence between the type-I and type-II errors. In particular, three exponents are the most important. Detailed definitions of exponents will be given in Sect. 2. The Stein exponent characterizes the best (i.e., the largest) exponential decay rate of the type-II error when the type-I error upper is bounded by some $\varepsilon \in (0, 1)$. Quantum Stein’s lemma [30,31] shows that the exponent is given by the quantum relative entropy [32]. Moreover, it is independent of $\varepsilon \in (0, 1)$, which is known as the strong converse property. The Hoeffding exponent and the strong converse exponent, respectively, determine the optimal exponential rate of the type-I error (or the type-I success probability) when the type-II error exponentially decays at the rate below or above the Stein exponent. They are proved to be given by quantities involving Petz’s Rényi divergence [28,29,33,34] and the sandwiched Rényi divergence [35–38]. Other extensions in the large, moderate, and small deviation regimes have been studied in depth by [6–8,39–45].

Small to intermediate scale quantum computers will be available in the near-term future [46,47]. However, such quantum computers will be built in geographically separated laboratories, which means that each lab will perform only local quantum operations,
and mutual classical communication may be available. These operations constitute a restricted class of measurements known as local operations and classical communication (LOCC) [48–51]. Naturally, this leads to the question of how well do LOCC measurements perform in hypothesis testing compared to global measurements? For instance, the above-mentioned quantum Neyman–Pearson test is generally not implementable via LOCC due to quantum entanglement and nonlocality [50,52]. Therefore, the problem of local discrimination and local hypothesis testing recently gained considerable attention in the field of quantum computation and quantum information [53–67]. Unfortunately, only limited results are known due to the complicated mathematical structure of LOCC.

In the present work, our goal is to study the asymptotic behavior of the errors incurred by the restriction to LOCC and derive the above-mentioned four exponents. We also consider other classes of measurements: the positive-partial-transpose operations (PPT) and separable operations (SEP) [68], mainly out of theoretical interest or as a tool to analyze LOCC. It is well-known that strict inclusions hold among them [52], i.e.

\[
\text{LOCC} \subset \text{SEP} \subset \text{PPT} \subset \text{ALL.} \tag{2}
\]

Although hypothesis testing under LOCC has been studied in many papers in the one-shot setting [53–60,62,63,65], the explorations of the asymptotic error behavior are relatively limited [53,55,57]. In this work, we focus on demonstrating an interesting phenomenon in the many-copy setting. Namely, the results show that distinguishing a pair of orthogonal states under LOCC indeed exhibits a fundamental difference from the conventional task using global measurements. By definition of the Chernoff exponent given in Eq. (1) and the inclusions Eq. (2), we have

\[
\text{Chernoff}^{\text{LOCC}} \leq \text{Chernoff}^{\text{SEP}} \leq \text{Chernoff}^{\text{PPT}} \leq \text{Chernoff}^{\text{ALL}} = \min_{0 \leq s \leq 1} \log \text{Tr} \left[ \rho_0^{1-s} \rho_1^s \right]. \tag{3}
\]

Here and subsequently, we put a superscript ‘X’ on \( P_e \) and the Chernoff exponent to highlight the class X measurements allowed. Particularly intriguing examples arise in the context of data hiding [53,69–73] where the underlying states are orthogonal, i.e., \( \text{Tr} [\rho_0 \rho_1] = 0 \). This result implies that Chernoff\(^{\text{ALL}}(\rho_0, \rho_1) = \infty \). However, for a given pair of orthogonal states with entanglement, the problem of whether Chernoff\(^{\text{LOCC}}(\rho_0, \rho_1) \) is finite or not has remained open since the early days of quantum information theory. We know that Chernoff\(^{\text{LOCC}}(\rho_0, \rho_1) \) is nonzero, which can be achieved by implementing local tomography, then applying the classical Chernoff bound. On the other hand, it is unclear if the definition of the Chernoff exponent for a class \( X \in \{ \text{LOCC}, \text{SEP}, \text{PPT} \} \) is faithful, in the sense that the sequence \( \left( -\frac{1}{n} \log P_e^X(\rho_0^\otimes n, \rho_1^\otimes n; p) \right) \) diverges if and only if \( P_e^X(\rho_0^\otimes n, \rho_1^\otimes n; p) = 0 \) for some finite \( n \); cf. [64].\(^1\) Hence, in this work, we study the case of distinguishing an entangled state (possibly on a multipartite system) and its orthogonal complement using restricted classes of POVMs. In particular, we show that the Chernoff bounds in this case is faithful for all the three classes; we remark that no simple expression for a general multipartite entangled state is known.

Although it has been shown that the inclusion relations Eq. (2) are all strict [52], it is not known whether strict inclusion still holds in the many-copy asymptotics. For instance, does any equality hold in Eq. (3)? This question naturally arises since SEP and PPT operations are often exploited to approximate LOCC operations. Hence, one may ask how differently the restricted classes of measurements perform.

\[^1\] In [64], the authors showed that if two quantum operation cannot be perfectly distinguishable with finite uses, then the associated Chernoff exponent is finite.
In this paper, we further show that the (one-way) LOCC operations can achieve the same performance as the PPT operation, even if the states are highly entangled. In this case, the equalities in (2) between LOCC, SEP, and PPT hold. On the other hand, we demonstrate that there is an infinite separation between the SEP and PPT operations, even if there is no entanglement involved in the underlying states. Namely, we construct a pair of states such that Chernoff$_{\text{PPT}} = \infty$, while Chernoff$_{\text{SEP}} \leq -\log \mu < \infty$ for some $\mu > 0$.

Organization of the paper. We summarize our main contributions in Sect. 1.1. In Sect. 1.2, we compare our results with existing works. Section 2 introduces necessary notation and definitions. In Sect. 3, we consider hypothesis testing between arbitrary entangled pure state and its orthogonal complement. In Sect. 4, we study the scenario when LOCC equals PPT POVMs. A special case of testing a maximally entangled state and its orthogonal complement is shown in Sect. 4.1, and testing extremal Werner states is shown in Sect. 4.2. In Sect. 5, we demonstrate an infinite asymptotic separation for the SEP and PPT operations. In closing, we provide discussions and conclusions in Sect. 6. Appendix A includes the case of testing a pure state with equal non-zero Schmidt coefficients.

1.1. Main contributions. This work concerns hypothesis testing between orthogonal states using restricted measurements and the relations between LOCC, SEP, and PPT in the many-copy scenario. Below we list our contributions and findings regarding to these questions.

(I) We study the optimal error probability of distinguishing an arbitrary multipartite entangled pure state $\psi$ and its orthogonal complement $\psi^\perp := \frac{1 - \psi}{D - 1}$ (where $D$ is the dimension of the underlying Hilbert space) in the many-copy scenario.

(i) We prove that the optimal error probability always decays exponentially in the number of copies $n$ (Theorem 1, Sect. 3): There exists constants $0 < a \leq b < \infty$ such that,

$$e^{-nb} \leq P_{\text{LOCC}}^{n} \left( \psi \otimes_{n}, (\psi^\perp) \otimes_{n}; p \right) \leq (1 - p) \cdot e^{-na}, \quad \forall n \in \mathbb{N}.$$ 

Hence, the Chernoff bound is faithful. We remark that the derived error exponent $a$ in the upper bound depends only on the dimension of the underlying Hilbert spaces, and it is tight if $\psi$ is a maximally entangled state. Our key technique proving this result is by establishing an exponential lower bound to the optimal error probability for distinguishing a bipartite entangled state $\psi$ on a bipartite system $\mathbb{C}^{d} \otimes \mathbb{C}^{d}$ against its orthogonal complement $\psi^\perp$ using PPT POVMs (Proposition 4, Sect. 3.1) expressed as:

$$P_{\text{PPT}}^{n} \left( \psi \otimes_{n}, (\psi^\perp) \otimes_{n}; p \right) \geq \min \{1 - p, p\} \cdot r^{n}, \quad \forall n \in \mathbb{N}$$

where $r := \frac{1 - \eta}{\frac{1}{d^{2}} - 1} \in (0, \frac{1}{d^{2}}]$, and $\eta$ denotes the largest squared Schmidt coefficient of $\psi$. The above bound also provides a lower bound to the error probability using LOCC POVMs. Moreover, our approach extends to a strong converse bound in the asymmetric setting. Specifically, the type-I error approaches 1 at the exponential rate $r - \log \frac{1}{r}$ whenever the type-II error decays exponentially at rate $r > \log \frac{1}{r}$, which also implies that the Stein exponent is upper bounded by the quantity $\log \frac{1}{r}$ (i.e., the strong converse property).
(ii) We find a sufficient condition to characterize when the three classes of measurement, LOCC, SEP, and PPT, collapse in either symmetric or asymmetric hypothesis testing (Theorem 7, Sect. 4). Moreover, we show that such a sufficient condition is fulfilled when the underlying pair of states are maximally entangled state $\Phi_1^d := \frac{1}{d} \sum_{i,j=0}^{d-1} |ii\rangle \langle jj|$ on $\mathbb{C}^d \times \mathbb{C}^d$ and its orthogonal complement state $\Phi_1^\perp := (1 - \Phi_1^d)/(d^2 - 1)$. We then explicitly calculate the average error probability (Theorem 8, Sect. 4.1) under an optimal LOCC protocol:

$$
P_{LOCC}^e (\Phi_1^d \otimes^n, (\Phi_1^\perp)^\otimes^n; p) = \min \left\{ (1 - p) \left( \frac{1}{d + 1} \right)^n, p \right\}.
$$

This then immediately gives the Chernoff exponent: $\text{Chernoff}_{LOCC} (\Phi_1^d, \Phi_1^\perp) = \log (d + 1)$. Further, we establish the optimal trade-off between the type-I and type-II errors, i.e., given any type-I error no larger than a constant $\varepsilon$, the minimum type-II error of using a restricted class ‘X’ of measurements, denoted by $\beta_{X}^\varepsilon (\Phi_1^d \otimes^n, (\Phi_1^\perp)^\otimes^n)$, satisfies

$$
\beta_{X}^\varepsilon (\Phi_1^d \otimes^n, (\Phi_1^\perp)^\otimes^n) = \frac{1 - \varepsilon}{(d + 1)^n}.
$$

(4)

With such functional dependence and exact characterization, we then obtain the associated Stein, Hoeffding, and strong converse exponents in Corollaries 10, 11, and 12, respectively. We remark that, in the general cases of testing arbitrary states using restricted measurements, the single-letter formula is unknown even for the Stein exponent. Moreover, the known Stein exponent for the general case only holds at $\varepsilon = 0$, which asserts that the type-I error vanishes asymptotically as the type-II error decays at a rate below the Stein exponent. Nevertheless, it does not provide the strong converse property; namely, the minimum type-I error converges to 1 as the type-II error decays at a rate above the Stein exponent. We refer the reader to Sect. 1.2 for more detailed discussions.

(iii) Our results apply to the case of testing the pure state with uniform nonzero Schmidt coefficients (i.e. $\frac{1}{m} \sum_{i,j=0}^{m-1} |ii\rangle \langle jj|$ for $m \leq d$) and its orthogonal complement (Propositions 22 and 23 of Section A). Lastly, we extend Matthews and Winter’s work [53] to show that testing extremal Werner states [74] also satisfies the above sufficient condition. Therefore, we establish the optimal trade-off between the type-I and type-II errors and the corresponding Stein, Hoeffding, and strong converse exponents (Theorem 13, Sect. 4.2). In Table 1 below, we summarize the established exact characterizations for the exponents in various testing setting.

(II) In Sect. 5, we establish an infinite asymptotic separation between SEP measurements and PPT measurements. Specifically, we consider the null hypothesis to be the uniform mixture of an unextendible product basis (UPB) [76] and the alternative hypothesis to be a state supported on the orthogonal complement of the former. Such a pair of states can be discriminated perfectly by a PPT measurement, while we show that the optimal error probability under SEP measurements possesses an exponential lower bound (Theorem 18 of Sect. 5). Our key technique to establishing this result is introducing a novel quantity, unextendibility, (Definition 19, Sect. 5) to measure how far a UPB is from being an extendible product basis and proving its multiplicativity property under the tensor product (Proposition 20). Accordingly, our result gives a quantitative characterization of when the tensor product of UPBs is still a UPB [77].
1.2. Comparisons to existing results. The Stein exponent for binary quantum hypothesis testing when $\varepsilon = 0$, i.e. $\text{Stein}^X(\rho_0, \rho_1, 0)$, was studied by Brandão et al. [54] and proved to be given by the regularized relative entropy between the measurement outcomes, i.e.

$$\lim_{\varepsilon \to 0} \text{Stein}^X(\rho_0, \rho_1, \varepsilon) = \lim_{n \to \infty} \sup_{M \in X} \frac{D(M(\rho_1^\otimes n)\|M(\rho_0^\otimes n))}{n},$$

where $D$ is the quantum relative entropy [32], and $M$ is any POVM in the class ‘X’, and the precise definition for $\text{Stein}^X(\rho_0, \rho_1, \varepsilon)$ will be introduced later in Sect. 2. First, calculating such a regularized quantity is computationally intractable. Second, it is not known whether the strong converse property holds. Namely, if $\text{Stein}^X(\rho_0, \rho_1, \varepsilon)$ is dependent on $\varepsilon \in (0, 1)$. Hence, in Corollaries 10 and 14, we establish a single-letter formula for testing $\Phi_d$ against $\Phi_d^\perp$, and the completely anti-symmetric Werner state [74] on $\mathbb{C}^d \otimes \mathbb{C}^d$, respectively; and $\tau$ is the completely mixed state of another system (whose dimension is irrelevant here). The parameter $\lambda \in [0, 1]$ is an arbitrary scalar.

### Table 1. Exact characteristics of the Chernoff exponent, Eq. (6), Stein exponent, Eq. (8), Hoeffding exponent, Eq. (9), and strong converse exponent, Eq. (10) under various settings of binary hypothesis testing via LOCC, SEP, and PPT measurements. Namely, the established exponents in the table are all the same for the three classes of the restricted measurements. The states $\Phi_d$, $\Phi_d^\perp$, $\sigma_{a,d}$, and $\sigma_{a,d}$ are the maximally entangled state, its orthogonal complement state, the completely symmetric Werner state and the completely anti-symmetric Werner state [74] on $\mathbb{C}^d \otimes \mathbb{C}^d$, respectively; and $\tau$ is the completely mixed state of another system (whose dimension is irrelevant here). The parameter $\lambda \in [0, 1]$ is an arbitrary scalar.

| Setting | Exponents | Chernoff | Stein | Hoeffding | Strong converse |
|---------|-----------|----------|-------|-----------|-----------------|
| $H_0$ : $\Phi_d^\otimes n$ | $\log(d+1)$ | $\log(d+1)$ | $\infty$ | $r - \log(d+1)$ |
| $H_1$ : $\Phi_d^\perp$ | $\log(d+1)$ | $\infty$ | $\log(d+1)$ | $0$ |
| $H_0$ : $\Phi_d^\perp$ | $\log(d+1)$ | $\log(d+1)$ | $\infty$ | $0$ |
| $H_0$ : $\Phi_d^\perp$ | $\log(d+1)$ | $\log(d+1)$ | $\infty$ | $0$ |
| $H_0$ : $\Phi_d^\perp$ | $\log(d+1)$ | $\log(d+1)$ | $\infty$ | $0$ |
| $H_0$ : $\Phi_d^\perp$ | $\log(d+1)$ | $\log(d+1)$ | $\infty$ | $0$ |
| $H_0$ : $\Phi_d^\perp$ | $\log(d+1)$ | $\log(d+1)$ | $\infty$ | $0$ |
| $H_0$ : $\Phi_d^\perp$ | $\log(d+1)$ | $\log(d+1)$ | $\infty$ | $0$ |

### Example

```latex
\begin{tabular}{|c|c|c|c|}
\hline
Setting & Exponents & Chernoff & Stein & Hoeffding & Strong converse \\
\hline
$H_0$ : $\Phi_d^\otimes n$ & $\log(d+1)$ & $\log(d+1)$ & $\infty$ & $r - \log(d+1)$ \\
$H_1$ : $\Phi_d^\perp$ & $\log(d+1)$ & $\infty$ & $\log(d+1)$ & $0$ \\
$H_0$ : $\Phi_d^\perp$ & $\log(d+1)$ & $\log(d+1)$ & $\infty$ & $0$ \\
$H_0$ : $\Phi_d^\perp$ & $\log(d+1)$ & $\log(d+1)$ & $\infty$ & $0$ \\
$H_0$ : $\Phi_d^\perp$ & $\log(d+1)$ & $\log(d+1)$ & $\infty$ & $0$ \\
$H_0$ : $\Phi_d^\perp$ & $\log(d+1)$ & $\log(d+1)$ & $\infty$ & $0$ \\
$H_0$ : $\Phi_d^\perp$ & $\log(d+1)$ & $\log(d+1)$ & $\infty$ & $0$ \\
$H_0$ : $\Phi_d^\perp$ & $\log(d+1)$ & $\log(d+1)$ & $\infty$ & $0$ \\
\hline
\end{tabular}
```
POVMs, in which solving the latter problem is easier than solving the original one. Then, Ref. [55] extends the analysis of [56] to the many-copy scenario to obtain the Chernoff, Stein, and Hoeffding exponents for several restricted POVMs. For one-way LOCC POVMs, the hypothesis-testing problem is essentially classical, while for SEP POVMs, additional large-deviation-type techniques were used. In particular, the authors proved that the Stein exponent is the same for all three classes of POVMs. In Ref. [57], the results for the Stein exponent are sharpened up to the third-order term. Moreover, the Hoeffding exponents for the two-way LOCC and SEP POVMs coincide. There is a difference in the Hoeffding exponent between the one-way LOCC and two-way LOCC POVMs unless the Schmidt coefficients are uniform.

Below we highlight the differences between our work from Refs. [55–57]. First, since the pair of states for testing in [55–57] are not orthogonal, the faithfulness of the error exponents therein holds trivially. Namely, the discrimination error between an entangled bipartite state and the completely mixed state can not decay super-exponentially. On the other hand, testing orthogonal states in our work becomes highly nontrivial because examples show that more than one copy is required for perfect discrimination. In contrast, two copies suffice for discrimination without mistake (see e.g. [61,62]). Second, the proofs in Refs. [55–57] heavily rely on the equivalence of testing a bipartite pure state against the white noise state to a global hypothesis-testing problem between a classical distribution against the uniform one. Note that the white noise state plays a crucial role here. It is unclear whether such an equivalence still holds generally. As for the first part of this work, we primarily rely on the twirling operation of the hypotheses. Third, Refs. [55–57] concerned hypothesis testing using SEP POVMs and reduced it to a global hypothesis testing with a composite null hypothesis. This work, however, does not directly analyze the SEP POVMs but the PPT POVMs. We remark that a converse bound for testing using SEP POVMs does not necessarily yield a converse bound for testing using PPT POVMs since SEP ⊂ PPT. Moreover, Sect. 5 establishes an infinite separation between SEP and PPT, which seems novel to our knowledge. Lastly, the second-order expansion of the optimal type-II error with type-I no larger than a constant studied in [57] generally resembles the classical case [43,44]. For testing the maximally entangled state against the white noise state, [57, Theorem 4] showed that, for ‘X’ being LOCC or SEP, \( \beta_X^n(\Phi_1^d, (\mathbb{1}_d / d)^\otimes n) = (1 - \varepsilon)/d \), which is similar to ours given in (4) probably because of symmetry of the maximally entangled state. Although we are not concerned with testing against a white noise state in this paper, our analysis of the PPT-distinguishability (Proposition 4 in Sect. 3.1) shows that the above result holds for PPT POVMs as well, which strengthens the result [57, Theorem 4] from SEP to PPT POVMs.

2. Notation and Definitions

Let \( \mathbb{C}^d \) be a \( d \)-dimensional complex Hilbert space. A quantum state (i.e., density operator) on \( \mathbb{C}^d \) is a positive semi-definite operator with unit trace. The operator ‘\( \dagger \)’ denotes complex conjugate and transpose. The trace operation is denoted by \( \text{Tr}[\cdot] \). The symbol \( \mathbb{1}_d \) stands for the identity operator on \( \mathbb{C}^d \), and \( \mathbb{0}_d \) denotes the zero operation on \( \mathbb{C}^d \). If there is no ambiguity, we will drop the subscript for simplicity. For a bounded operator \( M \), we denote by \( |M| := \sqrt{M^\dagger M} \) its absolute value. We use \( \|M\|_\infty \) for the usual operator norm of \( M \) (i.e. the largest of the eigenvalue of \( |M| \)), and \( \|M\|_1 := \text{Tr}[|M|] \) for the trace norm (i.e. the sum of the singular values).
A positive-operator valued measure (POVM) is a set of positive semi-definite operators whose sum equals identity. For any density operator \( \rho \) on \( \mathbb{C}^d \), we use \( \rho^\perp \) to denote the orthogonal complement of \( \rho \), which is defined as the density operator on \( \mathbb{C}^d \) that is maximally mixed on the orthogonal complement of the support of \( \rho \). For example, if \( \rho \) is pure (i.e., a rank-one projection), then \( \rho^\perp = (\mathbb{1}_d - \rho)/(d - 1) \). The maximally entangled state on \( \mathbb{C}^d \otimes \mathbb{C}^d \) is denoted by \( \Phi_d := \frac{1}{d} \sum_{i,j=0}^{d-1} |i\rangle \langle j| \), and \( \Phi_d^\perp := (\mathbb{1} - \Phi_d)/(d^2 - 1) \) is its orthogonal complement. We use \( \tau_d := 1_d/d \) to denote the completely mixed state on \( \mathbb{C}^d \). The operations \( \otimes \) and \( \oplus \) represent the tensor product and direct sum, respectively. We use \( \mathbb{N} \) to denote natural numbers.

For an operator on a bipartite Hilbert space \( \mathcal{H}_c \otimes \mathcal{H}_B \), we use \( \Gamma \) to denote its partial transpose with respect to \( \mathcal{H}_B \), i.e., for some orthonormal basis \( \{|i\rangle_A \otimes |j\rangle_B\}_{i,j} \), we define the partial transpose as

\[
(|i\rangle \langle k|_A \otimes |j\rangle \langle \ell|_B) := |i\rangle \langle k|_A \otimes |\ell\rangle \langle j|_B.
\]

We remark that the partial transpose \( \Gamma \) is an isometry with respect to the Hilbert–Schmidt inner product, i.e., \( \text{Tr}[AB^\Gamma] = \text{Tr}[A^\Gamma B] \) for Hermitian matrices \( A \) and \( B \). We will use this fact throughout the paper.

Given a multipartite system \( \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m \), a (one-way) LOCC POVM \([51]\) is a decision rule based on all the measurement outcomes performed locally on each subsystem. The SEP measurements are defined as

\[
\text{SEP} : = \left\{ \left( E_k^{(1)} \otimes \cdots \otimes E_k^{(m)} \right)_{k} : E_k^{(j)} \geq 0, \sum_k E_k^{(1)} \otimes \cdots \otimes E_k^{(m)} = 1 \right\},
\]

and the PPT POVMs are defined as

\[
\text{PPT} : = \left\{ (E_k)_k \text{ POVM} : \forall 1 \leq j \leq m, \forall k, \left( E_k \right)^\Gamma \geq 0, \text{ where } \Gamma \text{ is partial transpose on } \mathcal{H}_j \right\}.
\]

We remark that for the LOCC measurements, classical post-processing, i.e., a decision rule, at the end is allowed.

Consider a binary hypothesis testing problem as follows:

\[
\begin{align*}
H_0 : & \quad \rho_0^\otimes n, \\
H_1 : & \quad \rho_1^\otimes n, \quad \forall n \in \mathbb{N}.
\end{align*}
\]

Given a test \( T \) where \( (T, \mathbb{1} - T) \) forms a two-outcome POVM, we let \( \alpha_n(T) := \text{Tr} \left[ \rho_0^\otimes n (\mathbb{1} - T) \right] \) and \( \beta_n(T) := \text{Tr} \left[ \sigma^\otimes n T \right] \). In the symmetric case with prior \( 0 < p < 1 \), we define the optimal error probability of the binary hypothesis testing using the class \( X \) of POVMs as:

\[
P^X_e(\rho_0^\otimes n, \rho_1^\otimes n ; p) : = \inf_{T, (\mathbb{1} - T) \in X} \{ p \alpha_n(T_n) + (1 - p) \beta_n(T_n) \}. \tag{5}
\]

The associated Chernoff exponent is expressed as

\[
\text{Chernoff}^X(\rho_0, \rho_1) : = \lim_{n \to \infty} \frac{1}{n} \log P^X_e(\rho_0^\otimes n, \rho_1^\otimes n ; p). \tag{6}
\]

We note that the definition given in Eq. (5) can be naturally extended to multiple hypothesis testing with priors.
Given density matrices $\rho_0$ and $\rho_1$, we use the following definitions:

$$R^X(\rho_0, \rho_1) = \{ (\alpha, \beta) : \exists T, \mathbb{1} - T \in X : \alpha = \text{Tr}[(\mathbb{1} - T)\rho_0], \beta = \text{Tr}[T\rho_1] \},$$

$$\alpha^X_\beta(\rho_0, \rho_1) := \inf \{ \alpha : (\alpha, \beta) \in R^X(\rho_0, \rho_1) \},$$

$$\beta^X_\alpha(\rho_0, \rho_1) := \inf \{ \beta : (\alpha, \beta) \in R^X(\rho_0, \rho_1) \}.$$  \hspace{1cm} (7)

Here, $R^X(\rho_0, \rho_1)$ is sometimes called the hypothesis-testing region, and the trade-off between type-I and type-II errors, $\beta^X_\alpha(\rho_0, \rho_1)$, is termed as the Neyman–Pearson function or the trade-off function (see [1, Section 3.2], [75], [21, Definition 2.1]).

In the asymmetric case, we define the following exponent functions:

$$\text{Stein}^X(\rho_0, \rho_1, \varepsilon) := \lim_{n \to \infty} \sup_{T, (\mathbb{1} - T) \in X} \left\{ -\frac{1}{n} \log \beta_n(T) : \alpha_n(T) \leq \varepsilon \right\}, \forall \varepsilon \in (0, 1);$$

$$\text{Hoeffding}^X(\rho_0, \rho_1, r) := \lim_{n \to \infty} \sup_{T, (\mathbb{1} - T) \in X} \left\{ -\frac{1}{n} \log \alpha_n(T) : -\frac{1}{n} \log \beta_n(T) \geq r \right\}, \forall r > 0;$$

$$\text{SC}^X(\rho_0, \rho_1, r) := \lim_{n \to \infty} \sup_{T, (\mathbb{1} - T) \in X} \left\{ -\frac{1}{n} \log(1 - \alpha_n(T)) : -\frac{1}{n} \log \beta_n(T) \geq r \right\}, \forall r > 0.$$  \hspace{1cm} (8, 9, 10)

3. Testing Arbitrary Entangled Pure States

This section is devoted to proving that the Chernoff bound of testing an arbitrary multipartite entangled pure state against its orthogonal complement using LOCC POVMs is faithful. Namely, the associated optimal error probability decays exponentially in the number of copies (see Theorem 1).

The main technique in establishing this result is to show an exponential lower bound of the optimal error probability using PPT POVMs, as stated in Proposition 4 of Sect. 3.1. Moreover, our technique also extends to provide a strong converse bound to the Stein exponent and a lower bound to the strong converse exponent in the asymmetric setting (Sect. 3.1).

**Theorem 1** (Faithfulness of the Chernoff bound). Let $\psi$ be an arbitrary multipartite entangled pure state on $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_m}$ and $\psi^\perp$ be its orthogonal complement state. The optimal error probability of discriminating them using LOCC POVMs decays exponentially in the number of copies, i.e., for any $0 < p < 1$ there exists $0 < b < \infty$ such that

$$e^{-nb} \leq P_{e}^{\text{LOCC}}(\psi^\otimes n, (\psi^\perp)^\otimes n; p) \leq (1 - p) \left( 1 - \frac{d_{m-1}d_m - \min\{d_{m-1}, d_m\}}{d_1d_2\cdots d_m - 1} \right)^n, \forall n \in \mathbb{N}.$$  \hspace{1cm} (11)

In other words,

$$0 < 1 - \frac{d_{m-1}d_m - \min\{d_{m-1}, d_m\}}{d_1d_2\cdots d_m - 1} \leq \text{Chernoff}^{\text{LOCC}}(\psi, \psi^\perp) \leq b < \infty.$$  \hspace{1cm} (12)
Remark 3.1. The lower bound to $P_{e}^{\text{LOCC}}(\psi \otimes^n, (\psi^\perp) \otimes^n; p)$ relies on the converse bound for the bipartite scenario that will be shortly introduced in Proposition 4 of Sect. 3.1.

Remark 3.2. As we will prove later in Theorem 8 of Sect. 4.1, the upper bound $P_{e}^{\text{LOCC}}(\psi \otimes^n, (\psi^\perp) \otimes^n; p) \leq 1 - \frac{p}{(d+1)^n}$ given in Theorem 1 is tight when $\psi$ is a bipartite maximally entangled on $\mathbb{C}^d \otimes \mathbb{C}^d$.

Proof. We first prove the upper bound. Observe that the pure state $|\psi\rangle$ can be expanded in the computational basis of the first $m-2$ system

$$|\psi\rangle = |0 \cdots 0\rangle|\phi\rangle_{m-1,m} + \sum_{j \neq 0 \cdots 0} |j\rangle|\phi_j\rangle_{m-1,m}. $$

Let $\sum_{i=0}^{d-1} \sqrt{\lambda_i}|ii\rangle$ be the Schmidt decomposition of $|\phi\rangle_{m-1,m}$ for some Schmidt basis $\{|i\rangle_{i=0}^{d-1}\}$, where $d \leq d_{m-1}, d_m$. For each copy, we measure the first $m-2$ systems in the computational basis and the last two systems in the Schmidt basis corresponding to $|\phi\rangle_{m-1,m}$ via an LOCC protocol. The resulting probability distributions of measuring $\psi$ is $P$ and the probability distribution of measuring $\psi^\perp$ is

$$Q = \frac{d_1d_2 \cdots d_m}{d_1d_2 \cdots d_m - 1} U - \frac{1}{d_1d_2 \cdots d_m - 1} P$$

where $U$ is the uniform distribution over $\{0, 1, \ldots, d_1d_2 \cdots d_m - 1\}$, and the support of $P$ is at most $d_1d_2 \cdots d_m + d - d_{m-1}d_m$. Using the classical Chernoff bound we obtain, for all $\alpha \in [0, 1]$,

$$P_{e}^{\text{LOCC}}(\psi \otimes^n, (\psi^\perp) \otimes^n; p) \leq p^\alpha (1 - p)^{1-\alpha} \left( \sum_x (P(x))^\alpha (Q(x))^{1-\alpha} \right)^n \leq (1 - p) \left( 1 - \frac{d_{m-1}d_m - \min\{d_{m-1}, d_m\}}{d_1d_2 \cdots d_m - 1} \right)^n,$$

where we simply chose $\alpha = 0$ in the last line to conclude the upper bound.

For the lower bound, note that any multipartite system can be viewed as a bipartite system by grouping the $m$ parties into two nonempty sets. Since we assume $\psi$ to be multi-party entangled, there exists a bipartition with respect to which $\psi$ is entangled (between the two groups). Hence, LOCC POVMs on the multipartite system are contained in the LOCC POVMs on the associated bipartite system. The minimum error probability of the latter is thus a lower bound on the error probability of the former. Then, it suffices to apply the exponential lower bound to the error probability using LOCC POVMs on a bipartite system to complete the proof, as shown in Proposition 4 later in Sect. 3.1.

Remark 3.3. Let us emphasize that if $\psi$ is not entangled, but rather a product state, then the distribution $P$ is a singleton, and hence the Chernoff exponent becomes $\infty$ by choosing $\alpha = 1/2$. 

\end{document}
3.1. Exponential Strong Converse Bound for Bipartite Pure States. The faithfulness of testing arbitrary multipartite entangled state in Theorem 1 relies on an exponential lower bound to $P_{e}^{\text{LOCC}}$. In this section, we present our main proof technique—an upper bound on the PPT-distinguishability norm—in Lemma 2 below. Then we will show how it gives exponential converse bounds to the error probability using PPT POVMs (Proposition 4), which implies an lower bound for LOCC POVMs.

We define the PPT-distinguishability norm [71] for any Hermitian matrix $H$ as

$$\|H\|_{\text{PPT}} := \sup_{-1 \leq M, M^{\dagger} \leq 1} \text{Tr}[HM].$$  \hspace{1cm} (11)

**Lemma 2** (Upper bound on PPT-distinguishability norm). Let $\rho_0$ and $\rho_1$ be arbitrary bipartite density matrices. Provided that

$$-\rho_1^{\Gamma} \leq t \cdot \rho_0^{\Gamma} \leq \rho_1^{\Gamma}$$ \hspace{1cm} (12)

for some $t \in [0, 1]$, then

$$\|\rho_0^\otimes n - \lambda \rho_1^\otimes n\|_{\text{PPT}} \leq |1 - \lambda t^n| + \lambda(1 - t^n), \quad \forall \lambda \geq 0.$$

**Remark 3.4.** The condition (12) obviously holds for $t = 0$ with any PPT state $\rho_1$, but it would only yield a trivial bound: $\|\rho_0^\otimes n - \lambda \rho_1^\otimes n\|_{\text{PPT}} \leq \|\rho_0^\otimes n - \lambda \rho_1^\otimes n\|_1 \leq 1 + \lambda$.

**Proof.** Our key technique is to succinctly formulate the PPT-distinguishability norm [71] into its dual representation in terms of the Schatten 1-norm. Then, we find a feasible solution to the dual problem to prove our claim. We first derive a dual program to the PPT-distinguishability norm given in (11).

Since there are four linear inequality constraints in the above primal optimization, we write the Lagrangian $L$ by introducing the corresponding dual variables $A, B, C, D \geq 0$ as

$$L = \text{Tr}[HM] + \text{Tr}[A(1 - M)] + \text{Tr}[B(1 + M)] + \text{Tr}[C(1 - M^{\Gamma})] + \text{Tr}[D(1 + M^{\Gamma})]$$

$$= \text{Tr}[A + B + C + D] + \text{Tr}[M(H - A + B - C^{\Gamma} + D^{\Gamma})].$$

To derive the dual program of Eq. (11), we maximize $L$ over all Hermitian matrices $M$ without constraints. Clearly, this is infinite unless $H = A - B + (C - D)^{\Gamma}$. For such a case, the maximum is simply $\text{Tr}[A + B + C + D]$. The dual formulation for the PPT-distinguishability norm is

$$\inf_{A, B, C, D \geq 0} \{ \text{Tr}[A + B + C + D] : H = A - B + (C - D)^{\Gamma} \}.$$

It is easy to see that a strictly feasible solution exists for the dual program; the strong duality holds for the semidefinite program considered here.

Moreover, we can rewrite the above in terms of 1-norm by denoting Hermitian matrices $X = A - B$ and $Y = (C - D)^{\Gamma}$ as follows:

$$\|H\|_{\text{PPT}} = \inf_{X = X^{\dagger}, Y = Y^{\dagger}} \{ \|X\|_1 + \|Y^{\Gamma}\|_1 : H = X + Y \}. \hspace{1cm} (13)$$
This is because the optimal decomposition of the absolute value of a matrix is into its positive and negative parts. That is,
\[
\|X\|_1 = \sup_{-\mathbb{1} \leq M \leq \mathbb{1}} \text{Tr}[MX] = \inf_{A, B \geq 0} \sup_M \{\text{Tr}[MX] + \text{Tr}[A (\mathbb{1} - M)] + \text{Tr}[B (\mathbb{1} + M)]\} = \inf_{A, B \geq 0} \{\text{Tr}[A + B] : X = A - B\}.
\]

Next, we find a feasible solution to the dual program, (13), i.e.
\[
H = \rho_0^\otimes n - \lambda \rho_1^\otimes n, \quad X = (1 - \lambda t^n)\rho_0^\otimes n, \quad Y = \lambda \cdot \left(t^n \rho_0^\otimes n - \rho_1^\otimes n\right).
\]

To obtain an upper bound to the dual program, we calculate:
\[
Y^\Gamma = \lambda \cdot \left((t\rho_0^\Gamma)^\otimes n - (\rho_1^\Gamma)^\otimes n\right) \leq 0,
\]
where the operator inequality follows from the hypothesis (12) and Lemma 3 given below.

Hence, we obtain an upper bound to the dual program:
\[
\|\rho_0^\otimes n - \lambda \rho_1^\otimes n\|_{\text{PPT}} \leq \|X\|_1 + \|Y^\Gamma\|_1 = \text{Tr}[|X|] - \text{Tr}[Y^\Gamma] = \text{Tr}[|X|] - \text{Tr}[Y] = |1 - \lambda t^n| + \lambda(1 - t^n),
\]
concluding the proof. \(\square\)

**Lemma 3.** For self-adjoint operators \(A\) and \(Z\) satisfying \(-A \leq Z \leq A\), then
\[
-A^\otimes n \leq Z^\otimes n \leq A^\otimes n, \quad \forall n \in \mathbb{N}. \tag{14}
\]

**Proof.** First, one can assert that \(A\) is positive semi-definite because \(A \geq -A\) is equivalent to \(2A \geq 0\). Furthermore, both the supports of the positive part of \(Z\) and the negative parts of \(Z\) must be contained in the support of \(A\). Otherwise, the hypothesis \(-A \leq Z \leq A\) cannot be true. Hence, we have
\[
-\mathbb{1} \leq A^{-\frac{1}{2}} Z A^{-\frac{1}{2}} \leq \mathbb{1},
\]
where the inverse of \(A\) is taken on the support of \(A\). Since the eigenvalues of \(A^{-\frac{1}{2}} Z A^{-\frac{1}{2}}\) is bounded in \([-1, 1]\), the eigenvalues of the tensor power are also bounded in \([-1, 1]\) via multiplication. Namely, we obtain
\[
-\mathbb{1}^\otimes n \leq \left(A^{-\frac{1}{2}} Z A^{-\frac{1}{2}}\right)^\otimes n = (A^\otimes n)^{-\frac{1}{2}} Z^\otimes n (A^\otimes n)^{-\frac{1}{2}} \leq \mathbb{1}^\otimes n,
\]
which, in turn, implies the desired inequality in (14). \(\square\)
**Proposition 4** (Exponential lower bounds for PPT POVMs). Let \( \rho_0 \) and \( \rho_1 \) be arbitrary bipartite density matrices. Provided that \((12)\) holds for some \( t \in (0, 1] \), the error probability of testing multi-copies of \( \rho_0 \) and \( \rho_1 \) using LOCC POVMs is lower bounded by

\[
p_{e}^{\text{LOCC}} (\rho_{0}^{\otimes n}, \rho_{1}^{\otimes n}; p) \geq P_{e}^{\text{PPT}} (\rho_{0}^{\otimes n}, \rho_{1}^{\otimes n}; p) \geq \min \{ (1 - p) \cdot t^n, \ p \} \geq \min \{ (1 - p, p) \cdot t^n, \ \forall n \in \mathbb{N} \}
\]

Additionally, for any \( r > \log \frac{1}{T} \), we have

\[
\alpha_{e-nr}^{\text{LOCC}} (\rho_{0}^{\otimes n}, \rho_{1}^{\otimes n}) \geq \alpha_{e-nr}^{\text{PPT}} (\rho_{0}^{\otimes n}, \rho_{1}^{\otimes n}) \geq 1 - e^{-n \left[ r - \log \frac{1}{T} \right]}, \ \forall n \in \mathbb{N},
\]

where the optimal type-I error \( \alpha_{e}^{P} \) is defined in Eq. \((7)\) of Sect. 2.

In particular for the case of \( \rho_0 = \psi \) being a bipartite entangled pure state on \( \mathbb{C}^d \otimes \mathbb{C}^d \) and \( \rho_1 = \psi^\perp := \frac{1-\psi}{d^2-1} \) being its orthogonal complement, then \( t = \frac{1-\eta}{d^2-1} \in (0, \frac{1}{d+1}] \) holds in \((12)\), where \( \eta \) denotes the largest squared Schmidt coefficient of \( \psi \), i.e., \( \eta := \| \text{Tr}_A[\psi] \|_{\infty} \in \left[ \frac{1}{d}, 1 \right] \).

**Remark 3.5.** Proposition 4 applies to testing general bipartite quantum states, albeit we only focus on testing orthogonal states in this paper. Furthermore, as mentioned in Theorem 1, the converse bound for testing bipartite states considered in Proposition 4 implies a converse bound for testing arbitrary multipartite states. Hence, Proposition 4 provides a general method to witness the faithfulness of a Chernoff bound. Later in Sect. 4, we show that Proposition 4 is actually tight for certain scenarios.

**Proof.** We first prove the claim for symmetric hypothesis testing. We apply Lemma 2 with \( \lambda = \frac{1-p}{p} \geq 0 \) to lower bound the error probability under PPT POVM:

\[
P_{e}^{\text{PPT}} (\rho_{0}^{\otimes n}, \rho_{1}^{\otimes n}; p) = \inf_{T, (1-T) \in \text{PPT}} p \text{ Tr} \left[ \psi^{\otimes n} (1 - T) \right] + (1 - p) \text{ Tr} \left[ (\psi^\perp)^{\otimes n} T \right] \\
= \inf_{T, (1-T) \in \text{PPT}} \left[ \frac{1}{2} + \text{ Tr} \left[ (p \rho_{0}^{\otimes n} - (1 - p) \rho_{1}^{\otimes n}) (2T - 1) \right] \right] \\
= \frac{1}{2} \left( 1 - \| p \rho_{0}^{\otimes n} - (1 - p) \rho_{1}^{\otimes n} \|_{\text{PPT}} \right) \\
\geq \frac{1}{2} \left( 1 - | p - (1 - p) \cdot t^n | - (1 - p) \cdot (1 - t^n) \right) \\
= \frac{1}{2} \left( p + (1 - p) t^n - | p - (1 - p) \cdot t^n | \right) \\
= \min \left\{ (1 - p) \cdot t^n, \ p \right\},
\]

yielding the first claim.

For asymmetric hypothesis testing, we assert that, for all \( \mu \geq 0 \),

\[
\alpha_{\mu}^{\text{PPT}} (\rho, \sigma) = \max_{\lambda \geq 0} \left\{ \frac{1}{2} (1 + \lambda - \| \rho - \lambda \sigma \|_{\text{PPT}}) - \lambda \mu \right\}.
\]
This is proved by the following:

\[ \alpha_{PPT}^{\mu} (\rho, \sigma) := \inf_{T \in \text{PPT}} \{ \text{Tr} [\rho (\mathds{1} - T)] : \text{Tr} [\sigma T] \leq \mu \} \]

\[ = \inf_{T \in \text{PPT}} \max_{\lambda \geq 0} \{ \text{Tr} [\rho (\mathds{1} - T)] + \lambda \text{Tr} [\sigma T] - \lambda \mu \} \]

\[ (a) = \max_{\lambda \geq 0} \inf_{T \in \text{PPT}} \frac{1}{2} \left( 1 + \lambda - \text{Tr} [(\rho - \lambda \sigma)(2T - \mathds{1})] - \lambda \mu \right) \]

\[ = \max_{\lambda \geq 0} \inf_{T \in \text{PPT}} \frac{1}{2} \left( 1 + \lambda - \parallel \rho - \lambda \sigma \parallel_{\text{PPT}} - \lambda \mu \right) \] (15)

where in (a) we change the order of inf and max by Sion’s minimax theorem and noting that the objective function is linear in \( \lambda \) and \( T \), respectively; and (b) follows from the PPT-distinguishability norm given in Eq. (11).

Application of Lemma 2 with \( \lambda = t^{-n} \) to (15) leads us to

\[ \alpha_{PPT}^{\exp (-nr)} (\psi^\otimes n, (\psi^\perp)^\otimes n) \geq \frac{1}{2} \left[ 1 + \lambda - |1 - \lambda t^n| - \lambda (1 - t^n) \right] - \lambda e^{-nr} \]

\[ = 1 - t^{-n} e^{-nr}, \]

which shows the second claim.

Lastly, to see \( t = \frac{1 - \eta}{(d^2 - 1) \eta} \in (0, \frac{1}{d+1}] \) holds for (12) with \( \eta = \parallel \text{Tr}_A[\psi] \parallel_{\infty} \in \left[ \frac{1}{d}, 1 \right) \), we verify the following stronger condition:

\[ (\psi^\perp)^\Gamma - t \cdot \parallel \psi^\Gamma \parallel \geq 0, \]

which implies that (12) must be fulfilled. Namely,

\[ (\psi^\perp)^\Gamma - t \cdot \parallel \psi^\Gamma \parallel = \frac{1}{d^2 - 1} \left( 1 - \psi^\Gamma - \frac{1 - \eta}{\eta} \parallel \psi^\Gamma \parallel \right) \]

\[ \geq \frac{1}{d^2 - 1} \left( 1 - \parallel \psi^\Gamma \parallel - \frac{1 - \eta}{\eta} \parallel \psi^\Gamma \parallel \right) \]

\[ = \frac{1}{d^2 - 1} \left( 1 - \frac{1}{\eta} \parallel \psi^\Gamma \parallel \right) \]

\[ \geq 0. \]

Here, the last inequality holds because \( \psi^\Gamma \) has eigenvalues \( \pm \sqrt{\lambda_i \lambda_j} \) for \( i \neq j \) and \( \lambda_i \), where \( \{\lambda_i\}_{1 \leq i \leq d} \) denote the squared Schmidt coefficients of \( \psi \) [62, Lemma 14]; then the eigenvalues of \( \frac{1}{\eta} \parallel \psi^\Gamma \parallel \) are \( \frac{\sqrt{\lambda_i \lambda_j}}{\max_{1 \leq k \leq d} \lambda_k} \leq 1 \). This concludes the proof.

Proposition 4 yields the faithfulness of the Chernoff exponent for distinguishing arbitrary pure bipartite entangled state against its orthogonal complement. Moreover, the type-I error converges to 1 exponentially fast as long as the exponential decay rate of the type-II error exceeds \( \log \frac{1}{t} \). This result gives a strong converse bound for the Stein exponent of distinguishing \( \psi^\otimes n \) against \( (\psi^\perp)^\otimes n \).
Corollary 5 (Strong converse bound for the Stein exponent). Consider any pure bipartite entangled state \( \psi \) on \( \mathbb{C}^d \otimes \mathbb{C}^d \) and its orthogonal complement \( \psi^\perp := \frac{1-\psi}{d^2-1} \). Let 
\[ t := \frac{1-n}{(d^2-1)n} \in (0, \frac{1}{d+1}] \quad \text{and} \quad \eta := \| \text{Tr}_A[\psi] \|_\infty \in [\frac{1}{d}, 1). \]
Then, 
\[
\text{Chernoff}^{\text{LOCC}}(\psi, \psi^\perp) \leq \text{Chernoff}^{\text{PPT}}(\psi, \psi^\perp) \leq \log \frac{1}{t} < \infty;
\]
\[
\text{SCPPT}(\psi, \psi^\perp, r) \geq r - \log \frac{1}{t}, \quad \forall r > \log \frac{1}{t};
\]
\[
\text{Stein}^{\text{PPT}}(\psi^\otimes n, (\psi^\perp)^\otimes n, \varepsilon) \leq \log \frac{1}{t} \in [\log(d+1), \infty), \quad \forall \varepsilon \in (0, 1).
\]

4. Optimal LOCC Protocols for Binary Hypothesis Testing

In Sect. 3, we established exponential lower bounds to the optimal errors using PPT POVMs. This section will show a sufficient condition under which such lower bounds are achievable by (one-way) LOCC POVMs (Theorem 7). Namely, it characterizes a sufficient condition when the three classes, LOCC, SEP, and PPT, collapse for testing orthogonal bipartite states. In Sects. 4.1 and 4.2, we will show that the condition holds for testing a maximally entangled state against its orthogonal complement and testing extremal Werner states. Hence, the corresponding optimal LOCC protocols in symmetric and asymmetric hypothesis testing are obtained.

We start with an achievability result.

Proposition 6 (Achievability). Let \( \rho_0 \) and \( \rho_1 \) be arbitrary orthogonal states, and let \( \Pi_{\rho_i} \) denotes the projection onto the support of \( \rho_i \).

If there exists a \( t \in (0, 1] \) satisfying
\[
\{ M = t \cdot \Pi_{\rho_1} + \Pi_{\rho_0}, \mathbb{1} - M = (1 - t) \cdot \Pi_{\rho_1} \} \in \mathcal{X}, \quad (16)
\]
then, for any \( p \in (0, 1) \) and \( n \in \mathbb{N} \),
\[
P_e^X(\rho_0^\otimes n, \rho_1^\otimes n; p) \leq \min \left\{ (1 - p) \cdot t^n, p \right\},
\]
and, for any \( \alpha \in [0, 1] \),
\[
\beta_\alpha^X(\rho_0^\otimes n, \rho_1^\otimes n) \leq (1 - \alpha) \cdot t^n.
\]

Here, ‘\( \mathcal{X} \)’ means a restricted class of measurements.

Proof. For symmetric hypothesis testing, we choose \( \{ M^\otimes n, \mathbb{1} - M^\otimes n \} \) for testing by the assumption in (16). Note that from (16),
\[
M^\otimes n = \sum_{k=0}^n t^{n-k} \Lambda_k,
\]
where \( \Lambda_k \) denotes the sum of all elements of \( \{ \Pi_{\rho_0}, \Pi_{\rho_1} \}^\otimes n \) that have \( k \) copies of \( \Pi_{\rho_0} \). Then,
\[
P_e^X(\rho_0^\otimes n, \rho_1^\otimes n; p) \leq p \text{Tr}\left[ (\mathbb{1} - M^\otimes n) \rho_0^\otimes n \right] + (1 - p) \text{Tr}\left[ M^\otimes n \rho_1^\otimes n \right]
\[
= p \text{Tr}\left[ (\mathbb{1} - \Lambda_n) \rho_0^\otimes n \right] + (1 - p) \text{Tr}\left[ \Lambda_0 \rho_1^\otimes n \right] \cdot t^n
\[
= (1 - p) \cdot t^n.
\]
On the other hand, if the above upper bound is strictly greater than \( p \), we simply choose measurement \( \{ 0, 1 \} \), i.e., the test always opts for \( H_1 \). This shows the first claim.

Next, we move on to asymmetric hypothesis testing. For every \( \alpha \in [0, 1] \), we choose the test

\[
T_n := (1 - \alpha) \cdot M^{\otimes n} = (1 - \alpha) \cdot \sum_{k=0}^{n} t^{n-k} \Lambda_k.
\]

Observing that \( \text{Tr}[M \rho_0] = 1 \) and \( \text{Tr}[M \rho_1] = t \), we obtain

\[
\alpha_n(T_n) = \text{Tr}[(\mathbb{1} - T_n) \rho_0^{\otimes n}] = 1 - (1 - \alpha) \text{Tr}[\rho_0^{\otimes n} M^{\otimes n}] = \alpha; \quad (17)
\]

\[
\beta_n(T_n) = \text{Tr}[T_n \rho_1^{\otimes n}] = (1 - \alpha) \cdot \text{Tr}[M^{\otimes n} \rho_1^{\otimes n}] = (1 - \alpha) \cdot t^n. \quad (18)
\]

Equations (17) and (18) imply that \( (\alpha, \beta_n(T_n)) \in \mathcal{R}(\rho_0^{\otimes n}, \rho_1^{\otimes n}) \). Hence, we have

\[
\hat{\beta}_n(T_n) = (1 - \alpha) \cdot t^n \quad \text{as desired. This concludes the proof.} \quad \square
\]

Combining Propositions 6 and 4 in Sect. 3.1 and noting \( \text{LOCC} \subset \text{SEP} \subset \text{PPT} \), we obtain the main result of this section, namely, a sufficient condition of achieving the optimal average error probability using \( \text{LOCC} \) protocols in symmetric hypothesis testing and the optimal trade-off in asymmetric hypothesis testing.

**Theorem 7** (A sufficient condition for optimal \( \text{LOCC} \) protocols). Let \( \rho_0 \) and \( \rho_1 \) be arbitrary orthogonal bipartite states. If there exists a \( t \in (0, 1] \) satisfying

\[
\{ M = t \cdot \Pi_{\rho_1} + \Pi_{\rho_0}, \mathbb{1} - M = (1 - t) \cdot \Pi_{\rho_1} \} \in \text{LOCC}, \quad (19a)
\]

\[
-\rho_1^\Gamma \leq t \cdot \rho_0^\Gamma \leq \rho_1^\Gamma, \quad (19b)
\]

then, for any \( n \in \mathbb{N} \),

\[
P_e^{\text{PPT}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = P_e^{\text{SEP}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = P_e^{\text{LOCC}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = \min \left\{ (1 - p) \cdot t^n, p \right\},
\]

and, for any \( \alpha \in [0, 1] \),

\[
\hat{\beta}_n^{\text{PPT}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}) = \hat{\beta}_n^{\text{SEP}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}) = \hat{\beta}_n^{\text{LOCC}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}) = (1 - \alpha) \cdot t^n.
\]

In Sect. 4.1, we will show that \( t = \frac{1}{d+1} \) for testing maximally entangled state against its orthogonal complement, and show that \( t = \frac{d-1}{d+1} \) for testing extremal Werner states in Sect. 4.2.

### 4.1. Testing Maximally Entangled States.

This section aims to test the following hypotheses of maximally entangled state against its orthogonal complement,

\[
\begin{align*}
H_0 : \rho_0^{\otimes n} &= \Phi_d^{\otimes n} \\
H_1 : \rho_1^{\otimes n} &= \left( \frac{\mathbf{1}_d - \Phi_d}{d^2 - 1} \right)^{\otimes n}, \quad \forall n \in \mathbb{N}.
\end{align*}
\]

We establish the optimal average error probability and the optimal trade-off between the two types of errors, type-I and type-II in Theorem 8 below. The Chernoff exponent (Corollary 9) in the symmetric setting, the Stein, Hoeffding, and strong converse exponents (Corollaries 10, 11, and 12) follow immediately.
Theorem 8. Consider the binary hypotheses given in Eq. (20). The following hold for any \( n \in \mathbb{N} \):

\[
P_e^{\text{PPT}}(\rho_0^\otimes n, \rho_1^\otimes n; p) = P_e^{\text{SEP}}(\rho_0^\otimes n, \rho_1^\otimes n; p) = P_e^{\text{LOCC}}(\rho_0^\otimes n, \rho_1^\otimes n; p)
\]

\[
= \min \left\{ (1 - p) \left( \frac{1}{d+1} \right)^n, p \right\},
\]

and, for any \( \alpha \in [0, 1] \),

\[
\beta^{\text{PPT}}_{\alpha}(\rho_0^\otimes n, \rho_1^\otimes n) = \beta^{\text{SEP}}_{\alpha}(\rho_0^\otimes n, \rho_1^\otimes n) = \beta^{\text{LOCC}}_{\alpha}(\rho_0^\otimes n, \rho_1^\otimes n) = 1 - \alpha \frac{d}{d+1}. 
\]

Proof. First, we verify condition (19a) in Theorem 7. For each copy, Alice and Bob measure on the computational basis and compare their measurement outcomes. If they agree, we claim that \( \Phi_1^\otimes n \) is the true hypothesis. We choose such a measurement strategy because the maximally entangled state is likely to give concordant measurement outcomes due to symmetry. Mathematically, this strategy is described by the two-outcome measurement:

\[
\left\{ \sum_{i=0}^{d-1} |ii\rangle\langle ii|, \sum_{i \neq j} |ij\rangle\langle ij| \right\}.
\]

Since the states in the hypotheses are both \( U \otimes U^* \)-invariant (where ‘*’ means the complex conjugate), after the twirling operation, we have the measurement

\[
\left\{ M_d = \Phi_d + \frac{1}{d+1} (\mathbb{1} - \Phi_d), \mathbb{1} - M_d = \frac{d}{d+1} (\mathbb{1} - \Phi_d) \right\}. 
\]

Equivalently, the choice of \( M_d \) is implementable by a (one-way) LOCC protocol, and hence (19a) is satisfied with \( t = \frac{1}{d+1} \).

Next, we verify that

\[
\frac{1}{d+1} |\Phi_d^\Gamma| \leq (\Phi_d^\perp)^\Gamma,
\]

and hence the condition (19b) in Theorem 7 with \( t = \frac{1}{d+1} \) is fulfilled for the sake of completeness, i.e.

\[
\frac{1}{d+1} |\Phi_d^\Gamma| - (\Phi_d^\perp)^\Gamma = \frac{1}{d^2-1} \left( (d-1) |\Phi_d^\Gamma| - (\mathbb{1} - \Phi_d^\Gamma) \right)
\]

\[
\leq \frac{1}{d^2-1} \left( (d-1) |\Phi_d^\Gamma| - \mathbb{1} + |\Phi_d^\Gamma| \right)
\]

\[
= \frac{1}{d^2-1} \left( d |\Phi_d^\Gamma| - \mathbb{1} \right)
\]

\[
= 0,
\]

which concludes the proof.

Remark 4.1. Theorem 8 shows that our result of exponential lower bound for testing arbitrary multipartite entangled pure state against its orthogonal complement given in Proposition 4 of Sect. 3.1 is tight for maximally entangled state \( \Phi_d \).
From the definition in Eq. (6), we obtain our main result for the Chernoff exponents:

**Corollary 9 (Chernoff exponent).** Consider the binary hypothesis given in Eq. (20). For every $0 < p < 1$, we have

$$\text{Chernoff}^{\text{PPT}}(\rho_0, \rho_1) = \text{Chernoff}^{\text{SEP}}(\rho_0, \rho_1) = \text{Chernoff}^{\text{LOCC}}(\rho_0, \rho_1) = \log(d + 1).$$

The optimal trade-off between type-I and type-II errors (Theorem 8) gives the results of the Stein exponent (Corollary 10), the Hoeffding exponent (Corollary 11), and strong converse exponent (Corollary 12) as outlined below.

**Corollary 10 (Stein exponent).** The following Stein exponents hold.

(a) Consider the binary hypothesis testing: $\rho_0 = \Phi_1 d$ and $\rho_1 = \Phi_1 \perp d$. Then,

$$\text{Stein}^{\text{PPT}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{SEP}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{LOCC}}(\rho_0, \rho_1, \varepsilon) = \log(d + 1), \quad \forall \varepsilon \in [0, 1).$$

(b) Consider the binary hypothesis testing: $\rho_0 = \Phi_1 d$ and $\rho_1 = \Phi_1 \perp d$. Then,

$$\text{Stein}^{\text{PPT}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{SEP}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{LOCC}}(\rho_0, \rho_1, \varepsilon) = \infty, \quad \forall \varepsilon \in [0, 1).$$

**Proof.** (a) By Theorem 8, we have, for every $\varepsilon \in [0, 1)$,

$$\text{Stein}^{\text{LOCC}}(\Phi_1 \otimes n, (\Phi_1 \perp d) \otimes n, \varepsilon) = \lim_{n \to \infty} \rho_1^X(n) = \lim_{n \to \infty} \log(d + 1) - \frac{1}{n} \log(1 - \varepsilon) = \log(d + 1)$$

as desired.

(b) For every $\varepsilon \in (0, 1)$, we choose the test $T_n := \mathbb{1} - M_d \otimes n$. From Eqs. (17) and (18), we have

$$\alpha_n(T_n) = \frac{1}{(d + 1)^n}; \quad \beta_n(T_n) = 0.$$

Hence, it follows that $\lim_{n \to 0} \alpha_n(T_n) \leq \varepsilon$, and

$$\text{Stein}^X(\rho_0, \rho_1, \varepsilon) \geq \lim_{n \to \infty} - \frac{1}{n} \log \beta_n(T_n) = \infty.$$

This completes the proof.

**Corollary 11 (Hoeffding exponent).** The following Hoeffding exponents hold.

(a) Consider the binary hypothesis testing: $\rho_0 = \Phi_1 d$ and $\rho_1 = \Phi_1 \perp d$. Then,

$$\text{Hoeffding}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{Hoeffding}^{\text{SEP}}(\rho_0, \rho_1, r)$$

$$= \text{Hoeffding}^{\text{LOCC}}(\rho_0, \rho_1, r)$$

$$= \infty, \quad \forall r \leq \log(d + 1).$$

(b) Consider the binary hypothesis testing: $\rho_0 = \Phi_1 d$ and $\rho_1 = \Phi_1 \perp d$. Then,

$$\text{Hoeffding}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{Hoeffding}^{\text{SEP}}(\rho_0, \rho_1, r) = \text{Hoeffding}^{\text{LOCC}}(\rho_0, \rho_1, r)$$

$$= \log(d + 1), \quad \forall r > 0.$$
Proof. (a) From Theorem 8, we know that if the type-II error is allowed to decay exponentially at the rate of \( \log(d+1) \), then the type-I error is zero for all \( n \). From the definition of the Hoeffding exponent given in Eq. (9), the type-I error is always zero if the type-II error decays slower, which shows that the Hoeffding exponent is infinite.

(b) Fix an arbitrary \( n \). From Theorem 8, Eqs. (17) and (18), choosing the test as \( 1 - (1 - \varepsilon)M_d^{\otimes n} \), it follows that

\[
\alpha_n(T_n) = \frac{1 - \varepsilon}{(d + 1)^n}, \quad \beta_n(T_n) = \varepsilon.
\]

Note that the test is optimal for every \( \varepsilon \in [0, 1) \). Now, letting \( \varepsilon = \exp\{-nr\} \) for any \( r > 0 \), we have \( \alpha_n(T_n) = (1 - \exp\{-nr\}) \). Since this holds for every \( n \), then

\[
\text{Hoeffding}^{\text{LOCC}}(\rho_0, \rho_1, r) = \lim_{n \to \infty} -\frac{1}{n} \log \alpha_n(T_n) = \log(d+1) - \lim_{n \to \infty} \frac{1}{n} \log(1 - \exp\{-nr\}) = \log(d+1),
\]

thereby completing the proof.

\[\Box\]

**Corollary 12** (Strong converse exponent). The following strong converse exponents hold.

(a) Consider the binary hypothesis testing: \( \rho_0 = \Phi_d \) and \( \rho_1 = \Phi_d^\perp \). Then,

\[
\text{SC}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{SC}^{\text{SEP}}(\rho_0, \rho_1, r) = \text{SC}^{\text{LOCC}}(\rho_0, \rho_1, r) = r - \log(d+1), \quad \forall r > \log(d+1).
\]

(b) Consider the binary hypothesis testing: \( \rho_0 = \Phi_d^\perp \) and \( \rho_1 = \Phi_d \). Then,

\[
\text{SC}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{SC}^{\text{SEP}}(\rho_0, \rho_1, r) = \text{SC}^{\text{LOCC}}(\rho_0, \rho_1, r) = 0, \quad \forall r \geq 0.
\]

Proof. (a) By denoting \( \alpha^X_\beta := \inf \{ \alpha : (\alpha, \beta) \in \mathcal{R}^X(\rho_0^{\otimes n}, \rho_1^{\otimes n}) \} \), Theorem 8 implies that

\[
\beta = \frac{1 - \alpha^X_\beta}{(d + 1)^n}.
\]

Letting \( \beta = \exp\{-nr\} \), we have the desired strong converse exponent.

(b) By Corollary 11-(b), the type-I error will exponentially decay when the type-II error exponentially decays at any finite rate \( r \). Therefore, the strong converse exponent is zero for all finite rate \( r \) since \( \lim_{n \to \infty} \frac{1}{n} \log[1 - \frac{1}{(d+1)^r}] = 0 \).

\[\Box\]

We remark that analysis of this section directly applies to the scenario of testing pure states with uniform non-zero Schmidt coefficients. We defer the results to Appendix A (see also Table 1).
4.2. Testing Completely (Anti-)Symmetric Werner States. In this section, we consider testing completely anti-symmetric Werner state $\sigma_{a,d}$ and completely symmetric Werner state $\sigma_{s,d}$ \cite{70,74}:

$$
\begin{cases}
H_0 : \rho_0^\otimes n = \sigma_{a,d}^\otimes n := \left( \frac{2}{d(d+1)} \Pi_{a,d} \right)^\otimes n, \quad \forall n \in \mathbb{N}.
H_1 : \rho_1^\otimes n = \sigma_{s,d}^\otimes n := \left( \frac{2}{d(d+1)} \Pi_{s,d} \right)^\otimes n,
\end{cases}
$$

(22)

Here, $\Pi_{a,d} := \frac{1}{2}(I_d - F_d)$ and $\Pi_{s,d} := \frac{1}{2}(I_d + F_d)$ and are projections onto the anti-symmetric and symmetric subspaces, respectively, and $F_d := \sum_{i,j=0}^{d-1} |i\rangle \langle j| \otimes |j\rangle \langle i|$ is the swap operator between the two $d$-dimensional subsystems. We obtain the following optimal LOCC protocols.

**Theorem 13.** Consider the binary hypotheses given in Eq. (22). The following hold for any $n \in \mathbb{N}$:

$$
P_{e}^{\text{PPT}} (\rho_0^\otimes n, \rho_1^\otimes n ; p) = P_{e}^{\text{SEP}} (\rho_0^\otimes n, \rho_1^\otimes n ; p) = P_{e}^{\text{LOCC}} (\rho_0^\otimes n, \rho_1^\otimes n ; p) = \min \left\{ (1 - p) \left( \frac{d-1}{d+1} \right)^n, p \right\},
$$

and, for any $\alpha \in [0,1]$,

$$
\beta_{\alpha}^{\text{PPT}} (\rho_0^\otimes n, \rho_1^\otimes n) = \beta_{\alpha}^{\text{SEP}} (\rho_0^\otimes n, \rho_1^\otimes n) = \beta_{\alpha}^{\text{LOCC}} (\rho_0^\otimes n, \rho_1^\otimes n) = (1 - \alpha) \cdot \left( \frac{d-1}{d+1} \right)^n.
$$

**Proof.** For verifying the first condition (19a) in Theorem 7, we consider the following (one-way) LOCC protocol for each copy:

$$
\begin{cases}
\sum_{i \neq j}^{d-1} |ij\rangle \langle ij|, \sum_{i=0}^{d-1} |ii\rangle \langle ii|.
\end{cases}
$$

Noting that the states $\sigma_{a,d}$ and $\sigma_{s,d}$ are both $U \otimes U$-invariant, after twirling, we obtain:

$$
\left\{ M_d := \frac{d-1}{d+1} \Pi_{s,d} + \Pi_{a,d}, \quad 1 - M_d = \frac{2}{d+1} \Pi_{a,d} \right\}.
$$

This shows that (19a) holds for $t = \frac{d-1}{d+1}$.

To verify the second condition (19b) with $t = \frac{d-1}{d+1}$, we calculate

$$
\frac{d-1}{d+1} |\sigma_{a,d}| - |\sigma_{s,d}| = \frac{1}{d(d+1)} \left( |I_d^2 - F_d^\Gamma| - |I_d^2 - F_d^\Gamma| \right)
= \frac{1}{d(d+1)} \left( |I_d^2 - d\Phi_d| - |I_d^2 - d\Phi_d| \right)
= - \frac{2}{d(d+1)} \Phi_d
\leq 0.
$$

This guarantees that (19b) must be fulfilled. \qed
Then, the associated Stein, Hoeffding, and the strong converse exponents can be established similarly as in Corollaries 10, 11, and 12. We lists the results below without duplicating the proof (see also Table 1 for a summary).

**Corollary 14** (Stein exponent). The following Stein exponents hold.

(a) Consider the binary hypothesis testing: $\rho_0 = \sigma_{a,d}$ and $\rho_1 = \sigma_{s,d}$. Then,

$$\text{Stein}^{\text{PPT}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{SEP}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{LOCC}}(\rho_0, \rho_1, \varepsilon) = \log \frac{d + 1}{d - 1}, \quad \forall \varepsilon \in [0, 1).$$

(b) Consider the binary hypothesis testing: $\rho_0 = \sigma_{s,d}$ and $\rho_1 = \sigma_{a,d}$. Then,

$$\text{Stein}^{\text{PPT}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{SEP}}(\rho_0, \rho_1, \varepsilon) = \text{Stein}^{\text{LOCC}}(\rho_0, \rho_1, \varepsilon) = \infty, \quad \forall \varepsilon \in [0, 1).$$

**Corollary 15** (Hoeffding exponent). The following Hoeffding exponents hold.

(a) Consider the binary hypothesis testing: $\rho_0 = \sigma_{a,d}$ and $\rho_1 = \sigma_{s,d}$. Then,

$$\text{Hoeffding}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{Hoeffding}^{\text{SEP}}(\rho_0, \rho_1, r) = \text{Hoeffding}^{\text{LOCC}}(\rho_0, \rho_1, r) = \infty, \quad \forall r \leq \log \frac{d + 1}{d - 1}.$$

(b) Consider the binary hypothesis testing: $\rho_0 = \sigma_{s,d}$ and $\rho_1 = \sigma_{a,d}$. Then,

$$\text{Hoeffding}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{Hoeffding}^{\text{SEP}}(\rho_0, \rho_1, r) = \text{Hoeffding}^{\text{LOCC}}(\rho_0, \rho_1, r) = \log \frac{d + 1}{d - 1}, \quad \forall r > 0.$$

**Corollary 16** (Strong converse exponent). The following strong converse exponents hold.

(a) Consider the binary hypothesis testing: $\rho_0 = \sigma_{a,d}$ and $\rho_1 = \sigma_{s,d}$. Then,

$$\text{SCP}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{SCP}^{\text{SEP}}(\rho_0, \rho_1, r) = \text{SCP}^{\text{LOCC}}(\rho_0, \rho_1, r) = r - \log \frac{d + 1}{d - 1}, \quad \forall r > \log \frac{d + 1}{d - 1}.$$

(b) Consider the binary hypothesis testing: $\rho_0 = \sigma_{s,d}$ and $\rho_1 = \sigma_{a,d}$. Then,

$$\text{SCP}^{\text{PPT}}(\rho_0, \rho_1, r) = \text{SCP}^{\text{SEP}}(\rho_0, \rho_1, r) = \text{SCP}^{\text{LOCC}}(\rho_0, \rho_1, r) = 0, \quad \forall r \geq 0.$$

5. Infinite Asymptotic Separation Between SEP POVMs and PPT POVMs

In this section, we prove that there is an infinite asymptotic separation between the optimal average error probabilities using SEP POVMs and PPT POVMs.
Definition 17 (Unextendible product basis [76,77]). Consider two Hilbert spaces, $\mathcal{H}_A$ and $\mathcal{H}_B$. The set $S = \{ |\alpha_i\rangle \otimes |\beta_i\rangle : 1 \leq i \leq N \} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ is called an unextendible product basis\(^2\) (UPB) if it satisfies the following:

\[
\begin{align*}
&\{ |\alpha_i\rangle \otimes |\beta_i\rangle \perp |\alpha_j\rangle \otimes |\beta_j\rangle, \forall i \neq j \}, \\
&\{ |\phi\rangle \otimes |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B : \forall i \in \{1, \ldots, N\}, |\phi\rangle \otimes |\psi\rangle \perp |\alpha_i\rangle \otimes |\beta_i\rangle \} = \{0\}.
\end{align*}
\]

An example of UPB was given in [76, (18)], which consists of five states on $\mathbb{C}^3 \otimes \mathbb{C}^3$:

\[
|\psi_0\rangle = \frac{1}{\sqrt{2}} |0\rangle \otimes (|0\rangle - |1\rangle), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}} |2\rangle \otimes (|1\rangle - |2\rangle),
\]

\[
|\psi_1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \otimes |2\rangle, \quad |\psi_3\rangle = \frac{1}{\sqrt{2}} (|1\rangle - |2\rangle) \otimes |0\rangle,
\]

\[
|\psi_4\rangle = \frac{1}{3} (|0\rangle + |1\rangle + |2\rangle) \otimes (|0\rangle + |1\rangle + |2\rangle).
\]

For a UPB $S = \{ |\alpha_i\rangle \otimes |\beta_i\rangle : 1 \leq i \leq N \} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$, we consider the following binary hypotheses:

\[
\begin{align*}
H_0 & : \rho_0^{\otimes n} := \left[ \frac{1}{N} \left( \sum_{i=1}^{N} |\alpha_i\beta_i\rangle \langle \alpha_i\beta_i| \right) \right]^{\otimes n}, \ n \in \mathbb{N}, \\
H_1 & : \rho_1^{\otimes n},
\end{align*}
\]

(23)

Here, $\rho_1$ is a state in $\mathcal{H}_A \otimes \mathcal{H}_B$ that is orthogonal to $\rho_0$. We show below that the optimal exponential decay rate of using SEP POVMs is strictly worse than that of using PPT POVMs.

Theorem 18 (Separation). There is an infinite asymptotic separation between SEP POVMs and PPT POVMs. That is, for testing the states given in Eq. (23), there exists a $\mu > 0$ such that for every $0 < p < 1$,

\[
\begin{align*}
&P_{\text{SEP}}^{\text{PPT}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = 0, \\
&P_{\text{SEP}}^{\text{SEP}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) \geq \frac{1}{2} \mu_n, \quad \forall n \in \mathbb{N}.
\end{align*}
\]

Consequently, we have that $\text{Chernoff}^{\text{PPT}}(\rho_0, \rho_1) = \infty$, while $\text{Chernoff}^{\text{SEP}}(\rho_0, \rho_1) < \infty$.

The key ingredient to establish Theorem 18 is to introduce a novel quantity that characterizes the “richness” of a product basis:

Definition 19 (Unextendibility). Given a product basis $S = \{ |\alpha_i\rangle \otimes |\beta_i\rangle : 1 \leq i \leq N \} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$, we define the unextendibility of $S$ as

\[
\delta_S := \min_{\rho_A, \rho_B} \max_{1 \leq i \leq N} \langle \alpha_i | \rho_A | \alpha_i \rangle \langle \beta_i | \rho_B | \beta_i \rangle,
\]

(24)

where $\rho_A$ and $\rho_B$ range over all density matrices on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

\(^2\) In this paper we only considered unextendible product bases on a bipartite Hilbert spaces. However, the Definition 17 naturally extends to the multipartite scenario.
Note that the minimum in Eq. (24) is always attained for some ρ_A and ρ_B, since the objective function on the right-hand side is continuous in ρ_A ⊗ ρ_B and the set of product states ρ_A ⊗ ρ_B is compact.

For an unextendible product basis S [77], one immediately has δ_S > 0.

**Proposition 20 (Multiplicativity).** The quantity δ_S is multiplicative. That is,

\[ δ_{S_1 ⊗ S_2} = δ_{S_1} δ_{S_2} \]

for any two product bases S_1 and S_2.

**Remark 5.1.** Note that a product basis S is unextendible if and only if δ_S > 0. Hence, the quantity δ_S indicates how far a UPB is from an extendible product basis. Then Proposition 20 implies that the tensor product of any two UPBs S_1 and S_2 enjoys the property that δ_{S_1 ⊗ S_2} = δ_{S_1} δ_{S_2} > 0. Therefore, this gives a quantitative characterization of the well-known fact that the tensor product of UPBs is also a UPB [77].

**Proof.** Let two product bases be given as

\[ S_1 = \{ |α_i⟩ ⊗ |β_i⟩ : 1 ≤ i ≤ N_1 \} ⊆ H_{A_1} ⊗ H_{B_1} , \]
\[ S_2 = \{ |ψ_j⟩ ⊗ |φ_j⟩ : 1 ≤ j ≤ N_2 \} ⊆ H_{A_2} ⊗ H_{B_2} . \]

From the definition given in Eq. (24), one can directly verify that

\[ δ_{S_1 ⊗ S_2} ≤ δ_{S_1} δ_{S_2} . \]

It remains to prove the direction ≥.

Let ρ_{A_1A_2} on H_{A_1} ⊗ H_{A_2} and ρ_{B_1B_2} on H_{B_1} ⊗ H_{B_2} be the states that attain the minimization in δ_{S_1 ⊗ S_2}, i.e.,

\[ δ_{S_1 ⊗ S_2} = \max_{1 ≤ i ≤ N_1, 1 ≤ j ≤ N_2} \langle α_i | ρ_{A_1A_2} | α_i⟩ \langle β_i | ρ_{B_1B_2} | β_i⟩ . \]  \hspace{1cm} (25)

Further, for any 1 ≤ i ≤ N_1, we let

\[ \langle α_i | ρ_{A_1A_2} | α_i⟩ = λ_i σ_{i,A_2} , \]
\[ \langle β_i | ρ_{B_1B_2} | β_i⟩ = μ_i σ_{i,B_2} , \]

where

\[ λ_i := \text{Tr} [⟨ α_i | ρ_{A_1A_2} | α_i⟩] = ⟨ α_i | ρ_{A_1} | α_i⟩ ≥ 0 , \]
\[ μ_i := \text{Tr} [⟨ β_i | ρ_{B_1B_2} | β_i⟩] = ⟨ β_i | ρ_{B_1} | β_i⟩ ≥ 0 . \]

By the definition of δ_1, there always exists some i_0 such that

\[ λ_{i_0} μ_{i_0} ≥ δ_{S_1} . \]  \hspace{1cm} (26)

By the choice of i_0 for any 1 ≤ j ≤ N_2, we have

\[ \langle α_{i_0} | ψ_j⟩ ⟨ β_{i_0} | φ_j⟩ = λ_{i_0} μ_{i_0} ⟨ ψ_j | σ_{i_0,A_2} | ψ_j⟩ ⟨ φ_j | σ_{i_0,B_2} | φ_j⟩ . \]

By the definition of δ_{S_2}, there exists some j_0 such that

\[ ⟨ ψ_{j_0} | σ_{i_0,A_2} | ψ_{j_0}⟩ ⟨ φ_{j_0} | σ_{i_0,B_2} | φ_{j_0}⟩ ≥ δ_{S_2} . \]  \hspace{1cm} (27)

Combining Eqs. (25), (26), and (27) gives

\[ δ_{S_1 ⊗ S_2} ≥ δ_{S_1} δ_{S_2} , \]

which completes the proof.
Now, we are ready to prove the main result, expressed as Theorem 18 in this section.

**Proof.** (Proof of Theorem 18) Consider the binary hypotheses given in Eq. (23) and let

\[
P = \sum_{i=1}^{N} |\alpha_i \beta_i\rangle \langle \alpha_i \beta_i|, \quad \rho = \frac{1}{N} P.
\]

By construction, both \(P\) and \(\mathbb{1} - P\) are PPT operators [77]. For this reason, the pair of states \((\rho, \sigma)\) can be perfectly distinguished by PPT POVMs. Hence, it remains to show an exponential lower bound to the error probability for distinguishing \((\rho_0^\otimes n, \rho_1^\otimes n)_{n \in \mathbb{N}}\) using SEP POVMs.

Consider uniform prior. Then, we have

\[
P_{e, \text{SEP}}(\rho_0^\otimes n, \rho_1^\otimes n; \frac{1}{2}) = 1 - \sup_{T, (1-T) \in \text{SEP}} \left\{ \frac{1}{2} \text{Tr} \left[ \rho_0^\otimes n (\mathbb{1} - T) \right] + \frac{1}{2} \text{Tr} \left[ \rho_1^\otimes n T \right] \right\}.
\]

The above equation can be written as a primal problem of a semi-definite program as follows:

maximize : \[
\frac{1}{2} \text{Tr} \left[ \rho_0^\otimes n \Pi_0 \right] + \frac{1}{2} \text{Tr} \left[ \rho_1^\otimes n \Pi_1 \right];
\]
subject to : \[
\Pi_0 + \Pi_1 = \mathbb{1},
\]
\[
\Pi_i \in \text{SEP} \quad \forall i \in \{0, 1\}.
\]

To derive its dual problem, we introduce the dual cone to SEP as follows:

\[
\text{SEP}^\ast(A^n \ colon B^n) := \left\{ H : H^\dagger = H, \quad \text{Tr}[\Pi \cdot H] \geq 0, \quad \forall \Pi \in \text{SEP} \right\}.
\]

Such a dual cone is also known as the set of block-positive operators [78, Section 2], i.e.,

\[
\text{SEP}^\ast(A^n \ colon B^n) = \left\{ H : H^\dagger = H, \quad \text{Tr}_{B^n} \left[ H \cdot (\mathbb{1}_{A^n} \otimes |y\rangle \langle y|) \right] \geq 0, \quad \forall |y\rangle \in \mathcal{H}_{B}^\otimes n \right\}.
\]

Then the associated dual problem is:

minimize : \[\text{Tr}[H];\]
subject to : \[H - \frac{1}{2} \rho_0^\otimes n \in \text{SEP}^\ast(A^n \ colon B^n),\]
\[
H - \frac{1}{2} \rho_1^\otimes n \in \text{SEP}^\ast(A^n \ colon B^n),
\]
\[
H = H^\dagger.
\]

By the weak duality, we have

\[
P_{e, \text{SEP}}(\rho_0^\otimes n, \rho_1^\otimes n; \frac{1}{2}) \geq 1 - \inf_{H^\dagger = H} \left\{ \text{Tr}[H] : H - \frac{1}{2} \rho_0^\otimes n, H - \frac{1}{2} \rho_1^\otimes n \in \text{SEP}^\ast(A^n \ colon B^n) \right\}.
\]

(28)
Now, we choose a Hermitian operator $H$ as

$$H = \frac{1}{2} \rho_0^{\otimes n} + \left( \frac{1}{2} - \frac{\mu}{2} \right) \rho_1^{\otimes n},$$

where $\delta_S$ was introduced in Definition 19, and it is clear that $\delta_S \leq 1$. We aim to show that the operator $H$ is a feasible solution to Eq. (28) to complete the proof. First, it is not hard to see that

$$H - \frac{1}{2} \rho_0^{\otimes n} = \left( \frac{1}{2} - \frac{\mu}{2} \right) \rho_1^{\otimes n} \in \text{SEP}^*(A^n : B^n),$$

since positivity implies block-positivity. Second, we have

$$H - \frac{1}{2} \rho_1^{\otimes n} = \frac{1}{2} \left( \rho_0^{\otimes n} - \mu \rho_1^{\otimes n} \right) \geq \frac{1}{2} \left( \rho_0^{\otimes n} - \mu \rho_1^{\otimes n} \right) = \frac{1}{2N^n} \left( P^{\otimes n} - \delta_S^{\otimes n} \right).$$

To show that the quantity $P^{\otimes n} - \delta_S^{\otimes n}$ is block-positive, we will invoke the definition of $\delta_S$ given in Definition 19 and the multiplicativity of $\delta_S$ established in Proposition 20. Note that for all density matrices $\omega_A$ on $\mathcal{H}_A$ and $\omega_B$ on $\mathcal{H}_B$, we have

$$\text{Tr} \left[ P \cdot \omega_A \otimes \omega_B \right] \geq \delta_S > 0.$$ 

Hence, for any $\omega_{A_1 A_2 \ldots A_n} \otimes \omega_{B_1 B_2 \ldots B_n}$,

$$\text{Tr} \left[ P^{\otimes n} \cdot \omega_{A_1 A_2 \ldots A_n} \otimes \omega_{B_1 B_2 \ldots B_n} \right] \geq \delta_S^{\otimes n} = \delta^n_S > 0$$

In other words, $P^{\otimes n} - \delta_S^{\otimes n}$ is block-positive, which proves our claim. \hspace{1cm} \Box

6. Discussions and Conclusions

We studied the hypothesis testing between an entangled pure state against its orthogonal complement in the many-copy scenario. Our two principal motivations for this work are as follows: First, quantum entanglement is a valuable resource in quantum computation and other important quantum information-theoretic protocols. How to distinguish a state which possesses entangled bits is of fundamental significance. Second, whether the Chernoff exponent for pairs of orthogonal states with entanglement under LOCC is faithful (i.e., finite) is a long-standing open problem. This problem is challenging because there is no known simple mathematical structure of LOCC. Moreover, a general state can be entangled in a multipartite quantum system. Without any simple mathematical expression, hypothesis testing using LOCC is more challenging.

In the present paper, we show that the optimal average error probability for testing an arbitrary multipartite entangled pure state against its orthogonal complement decays exponentially in the number of copies, which in turn implies that the associated Chernoff exponent is faithful. In the special case of a maximally entangled state, we explicitly
derive its optimal average error probability in the symmetric setting and show that a single-copy measurement performs as well as the best LOCC protocol. This finding directly leads to an explicit expression of the Chernoff exponent.

In the asymmetric setting, we obtain an optimal trade-off between the type-I error \( \alpha_n \) and the type-II error \( \beta_n \). This allows us to fully characterize their asymptotic properties. The associated Stein’s exponent, namely the optimal exponential rate of \( \beta_n \) when \( \alpha_n \) is at most a constant, is proved. When \( \beta_n \) decays at a rate below or above the Stein exponent, we also establish the optimal exponential rate of \( \alpha_n \) and \( 1 - \alpha_n \), respectively. Our results show that the negative logarithm of the considered error does not diverge, which then guarantees that all the definitions of the four exponents are faithful. In other words, the asymptotic behavior of the errors satisfies the so-called large deviation principle [79]. It is worth mentioning that there is a distinctive difference between the second-order asymptotics under LOCC and those under global measurements. Indeed, this signifies that LOCC has an exceptional structure. To be more specific, we recall the second-order expansion of the optimal exponential rate of type-II error with type-I error no larger than a constant \( \varepsilon \) under global measurements [43,44], i.e.,

\[
D(\rho_0 \parallel \rho_1) + \sqrt{\frac{V(\rho_0 \parallel \rho_1)}{n}} Q^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right),
\]

where \( D \) and \( V \) are the quantum relative entropy and the relative entropy variance, respectively, and \( Q \) is the cumulative distribution function of the standard normal distribution. As described in [44, Section 5], \( V(\rho_0 \parallel \rho_1) = 0 \) implies \( D(\rho_0 \parallel \rho_1) = 0 \) for any pair of quantum states \( \rho_0, \rho_1 \). In other words, the first-order term in Eq. (29) disappears whenever the second-order term vanishes. On the other hand, the obtained result for LOCC in Eq. (4), shows that the optimal exponential rate of type-II error is given by

\[
-\frac{1}{n} \log \beta_n = \log(d + 1) - \log(1 - \varepsilon) - \frac{\log n}{n}.
\]

While the second-order term is missing, the first-order term \( \log(d + 1) \) is strictly positive. Indeed, this result implies that such asymptotic expansion has a different second-order term from that in Eq. (29). In previous work by Hayashi and Owari [55–57], we note that when distinguishing a bipartite pure state and a completely mixed state under LOCC, the asymptotic bounds admit a similar second-order expansion as in Eq. (29) unless the pure state is maximally entangled.

Finally, we establish an infinite asymptotic separation between the SEP and PPT operations in the many-copy scenario. Our result shows that indeed there is a gap between the SEP and PPT operations no matter how many copies of states are provided. Our technique is a multiplicativity property—a quantitative characterization of the tensor product of unextendible product bases. On the other hand, whether there is an infinite separation between the SEP and LOCC operations is a compelling open problem for future work. We believe that our analysis and results might have applications in data hiding or the studies of other important sets of orthogonal states.

**Acknowledgements.** We sincerely thank anonymous reviewers for their insightful suggestions to improve this paper. In particular, the proofs of Theorem 8 and Theorem 13 are greatly simplified, and the hypothesis in Lemma 2 is stated more precisely due to their comments. H.-C. Cheng is supported by the Young Scholar Fellowship (Einstein Program) of the Ministry of Science and Technology, Taiwan (R.O.C.) under Grants NSTC 111-2636-E-002-026, NSTC 112-2636-E-002-009, NSTC 112-2119-M-007-006, NSTC 112-2119-M-001-006, NSTC 112-2124-M-002-003, by the Yushan Young Scholar Program of the Ministry of Education, Taiwan (R.O.C.) under Grants NTU-111V1904-3 and NTU-112V1904-4, and by the research project “Pioneering Research in Forefront Quantum Computing, Learning and Engineering” of National Taiwan University.
under Grant NTC-CC-112L893405.” H.-C. Cheng acknowledges the support from the “Center for Advanced Computing and Imaging in Biomedicine (NTU-112L900702)” through The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan. A. Winter acknowledges financial support by the Spanish MINECO (Projects FIS2016-86681-P and PID2019-107609GB-I00) with the support of FEDER funds, and the Generalitat de Catalunya (Project CIRIT 2017-SGR-1127). N. Yu was supported by ARC Discovery Early Career Researcher Award DE180100156 and ARC Discovery Project DP210102449.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Appendix A. Testing Pure States with Uniform Non-Zero Schmidt Coefficients

In the following, we test pure entangled states with equal positive Schmidt coefficients, i.e.,

\[ \rho_0 := \frac{1}{m} \sum_{i,j=0}^{m-1} |ii\rangle \langle jj| \quad \text{for } m \leq d \]

against its orthogonal complement \((I_{d^2} - \rho_0) / (d^2 - 1)\). Equivalently, such state can be written as a maximally entangled state \(\Phi_m\) on \(\mathbb{C}^m \otimes \mathbb{C}^m\) embedded in a higher dimension Hilbert space \(\mathbb{C}^d \otimes \mathbb{C}^d\). In other words, we consider the binary hypotheses

\[
\begin{align*}
H_0 : \rho_0^{\otimes n} &= (\Phi_m \oplus (I_{d^2-m^2})^{\otimes n})^{\otimes n} \\
H_1 : \rho_1^{\otimes n} &= \frac{(I_{d^2} - \Phi_m \oplus (I_{d^2-m^2})^{\otimes n})}{d^2-1}^{\otimes n}, \quad \forall n.
\end{align*}
\]

We first prove a useful converse bound below, which will be used for our analysis later.

**Lemma 21.** Fix dimensions \(d\) and \(d'\). Let \(\rho\) and \(\sigma\) be density matrices on \(\mathbb{C}^d \otimes \mathbb{C}^d\). Then, for any class of two-outcome POVM, \(X \in \{\text{LOCC, SEP, PPT, ALL}\}\), any \(p, \lambda \in [0, 1]\) and any natural number \(n\), it follows that

\[
P^X_e \left( (\rho \oplus \mathbb{1}_{d^2})^{\otimes n}, (\lambda \sigma \oplus (1 - \lambda) \tau_{d^2})^{\otimes n} ; p \right) \geq P^X_e \left( \rho^{\otimes n}, (\lambda \sigma)^{\otimes n} ; p \right).
\]

**Proof.** Recalling the definition of optimal average error probability for any operators, (possibly sub-normalized), i.e.,

\[
P_e(\rho_0, \rho_1; p) := \inf_T \{ p \alpha(T) + (1 - p) \beta(T) \},
\]

it follows that

\[
P^X_e \left( (\rho \oplus \mathbb{1}_{d^2})^{\otimes n}, (\lambda \rho \perp (1 - \lambda) \tau_{d^2})^{\otimes n} ; p \right)
= \inf_{T_n \in \mathcal{X}} \left\{ p \Tr \left[ (I - T_n) (\rho \oplus \mathbb{1}_{d^2})^{\otimes n} \right] + (1 - p) \Tr \left[ T_n (\lambda \sigma \oplus (1 - \lambda) \tau_{d^2})^{\otimes n} \right] \right\}
\geq \inf_{T_n \in \mathcal{X}} \left\{ p \Tr \left[ (I - T_n) \rho^{\otimes n} \right] + (1 - p) \Tr \left[ T_n (\lambda \sigma)^{\otimes n} \right] \right\}
+ \inf_{G_n \in \mathcal{X}} \left\{ p \Tr \left[ (I - G_n) \mathbb{1}_{d^2} \right] + (1 - p) \Tr \left[ G_n \sum_{k=0}^{n-1} \lambda^k (1 - \lambda)^{1-k} B_k \right] \right\}, \quad (31)
\]
where we have used super-additivity of infimum, and $B_k$ denotes the sum of all elements of $\{\sigma, \tau_{d^2}\}^{\otimes n}$ which have $k$ copies of $\sigma$. Note that the second term in Eq. (31) is zero since one allows to choose the projection $I_{d^2}$ onto the copy of $\tau_{d^2}$ as the POVM. Moreover, this measurement is implementable by all four classes of POVMs. This then completes the proof.

In the following proposition, we consider a more general case compared to Eq. (30) since there are non-unique orthogonal complements in high-dimensional systems.

**Proposition 22.** Consider the hypotheses

\[
\begin{aligned}
H_0 &: \rho_0^{\otimes n} = (\Phi_m \oplus 1_{d^2-m^2})^{\otimes n} \\
H_1 &: \rho_1^{\otimes n} = (\lambda \Phi_m^{\perp} \oplus (1-\lambda) \tau_{d^2-m^2})^{\otimes n}, \quad \forall n.
\end{aligned}
\]

Then, it holds that

\[
P^{\text{PPT}}_c(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = P^{\text{SEP}}_c(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = P^{\text{LOCC}}_c(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p)
= \min \left\{ (1-p) \left( \frac{\lambda}{m+1} \right)^n , p \right\}.
\]

**Proof.** We first prove the achievability, i.e., the “$\geq$” direction. We choose the following POVM:

\[
\begin{aligned}
\left\{(M_m \oplus 1_{d^2-m^2})^{\otimes n}, 1_{d^2} - (M_m \oplus 1_{d^2-m^2})^{\otimes n}\right\}
= \left\{M_m^{\otimes n} \oplus 1_{d^2-m^2}^{\otimes n}, (1_{m^2} - M_m^{\otimes n}) \oplus 1_{d^2-m^2}^{\otimes n}\right\},
\end{aligned}
\]

where $M_m = \Phi_m + \frac{1}{m+1} (1_{m^2} - \Phi_m)$ as in Eq. (21). Then, the average error probability for the chosen LOCC protocol is

\[
P^{\text{LOCC}}_c = p \text{ Tr} \left[ (1_{m^2} - M_m^{\otimes n}) \oplus 1_{d^2-m^2}^{\otimes n} \cdot \Phi_m^{\otimes n} \oplus 1_{d^2-m^2}^{\otimes n} \right]
+ (1-p) \text{ Tr} \left[ M_m^{\otimes n} \oplus 1_{d^2-m^2}^{\otimes n} \cdot (\lambda \Phi_m^{\perp} \oplus (1-\lambda) \tau_{d^2-m^2})^{\otimes n} \right]
= (1-p) \text{ Tr} \left[ M_m^{\otimes n} \left( \lambda \Phi_m^{\perp} \right)^n \right]
= (1-p) \left( \frac{m^2-1}{d^2-1} \right)^n \left( \frac{\lambda}{m+1} \right)^n.
\]

By applying a similar technique to the proof of Proposition 6, we choose $\rho_1^{\otimes n} = \left( \frac{1_{d^2-m^2} - \Phi_m^{\otimes n} \oplus 1_{d^2-m^2}^{\otimes n}}{d^2-1} \right)^{\otimes n}$ whenever $P^{\text{LOCC}}_c > p$. Hence, we complete the proof of achievability.

Next, we move on to prove the converse, i.e., the “$\leq$” direction. Invoking Lemma 21, we have

\[
P^{\text{PPT}}_c(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) \geq P^{\text{PPT}}_c(\Phi^{\otimes n}, (\lambda \Phi_m^{\perp})^{\otimes n}; p).
\]

Following a similar argument in Proposition 6, we obtain the desired result. \qed
Remark A.1. By choosing \( \lambda = \frac{m^2 - 1}{d^2 - 1} \) in Eq. (32), it can be verified that the single copy in the alternative hypothesis \( H_1 \) coincides the canonical orthogonal complement in the alternative hypothesis of Eq. (30), namely \( \frac{1}{d^2 - \Phi_m \oplus O_{d^2 - m^2}} \). This answers the optimal average error probability of binary hypotheses Eq. (30) considered at the beginning of this section, i.e., \( \min \left\{ (1 - p) \left( \frac{m - 1}{d^2 - 1} \right)^n , \ p \right\} \).

The binary hypotheses considered in Eq. (32) have a simple variant (by interchanging \( \Phi_m \) and \( \Phi_m^{\perp} \)), for which we can immediately calculate its optimal average error.

**Proposition 23.** Consider the binary hypotheses

\[
\begin{align*}
H_0 : \rho_0^{\otimes n} &= (\Phi_m^{\perp} \oplus O_{d^2 - m^2})^{\otimes n} , \\
H_1 : \rho_1^{\otimes n} &= (\lambda \Phi_m \oplus (1 - \lambda) \tau_{d^2 - m^2})^{\otimes n} , \ \forall n ,
\end{align*}
\]

where \( \lambda \in [0, 1] \). Then, it holds that

\[
P_e^{\text{PPT}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = P_e^{\text{SEP}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = P_e^{\text{LOCC}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = \min \left\{ p \left( \frac{1}{m + 1} \right)^n , (1 - p) \lambda^n \right\} .
\]

**Proof.** We choose the POVM as

\[
\{ (1_{m^{2n}} - M_m^{\otimes n}) \oplus O_{d^{2n} - m^{2n}} , M_m^{\otimes n} \oplus 1_{d^{2n} - m^{2n}} \} , \quad (33)
\]

where \( M_m = \Phi_m + \frac{1}{m+1} (1_{m^2} - \Phi_m) \), as defined in Eq. (21).

The average error probability for the chosen LOCC protocol is

\[
P_e^{\text{LOCC}} = p \ Tr\left[ M_m^{\otimes n} \oplus 1_{d^{2n} - m^{2n}} \cdot (\Phi_m^{\perp})^{\otimes n} \oplus O_{d^{2n} - m^{2n}} \right] \\
+ (1 - p) \ Tr\left[ (1_{m^{2n}} - M_m^{\otimes n}) \oplus O_{d^{2n} - m^{2n}} \cdot (\lambda \Phi_m \oplus (1 - \lambda) \tau_{d^2 - m^2})^{\otimes n} \right] \\
= p \ Tr\left[ M_m^{\otimes n} (\Phi_m^{\perp})^{\otimes n} \right] + (1 - p) \ Tr\left[ (1_{m^{2n}} - \Phi_m^{\otimes n}) \cdot (\lambda \Phi_m)^{\otimes n} \right] \\
= p \ Tr\left[ M_m^{\otimes n} (\Phi_m^{\perp})^{\otimes n} \right] + (1 - p) \lambda^n \\
= p \left( \frac{1}{m + 1} \right)^n . \quad (34)
\]

On the other hand, we can also choose the POVM as

\[
\{ 1_{m^{2n}} \oplus O_{d^{2n} - m^{2n}} , O_{m^{2n}} \oplus 1_{d^{2n} - m^{2n}} \} . \quad (35)
\]

Then, the corresponding average error probability is

\[
P_e^{\text{LOCC}} = p \ Tr\left[ O_{m^{2n}} \oplus 1_{d^{2n} - m^{2n}} \cdot (\Phi_m^{\perp})^{\otimes n} \oplus O_{d^{2n} - m^{2n}} \right] \\
+ (1 - p) \ Tr\left[ 1_{m^{2n}} \oplus O_{d^{2n} - m^{2n}} \cdot (\lambda \Phi_m \oplus (1 - \lambda) \tau_{d^2 - m^2})^{\otimes n} \right] \\
= (1 - p) \ Tr\left[ 1_{m^{2n}} \cdot (\lambda \Phi_m)^{\otimes n} \right] \\
= (1 - p) \lambda^n . \quad (36)
\]
Since both POVMs chosen in Eqs. (33) and (35) are implementable by LOCC protocols, we minimize the average error probabilities given in Eqs. (34) and (36) to arrive at the “\(\leq\)” direction of our result.

For the other direction, i.e., “\(\geq\)”, we use Lemma 21, to obtain

\[ P^{\text{PPT}}_{\text{LOCC}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) \geq P^{\text{PPT}}_{\text{LOCC}}((\Phi_m^\perp)^{\otimes n}, (\lambda \Phi_m)^{\otimes n}; p). \]

Following a similar arguments to Proposition 6 obtains the desired result. \(\square\)

In the following Propositions 24 and 25, we apply similar techniques as before to calculate the binary hypothesis of a symmetric state embedded in a high-dimensional system and its orthogonal complement.

**Proposition 24.** Consider the binary hypothesis

\[
\begin{align*}
H_0: \rho_0^{\otimes n} &= \left(\sigma_m \oplus \bigotimes_{d^2-m^2} J\right)^{\otimes n}, \\
H_1: \rho_1^{\otimes n} &= \left(\lambda \sigma_m \oplus (1 - \lambda) \tau_{d^2-m^2}\right)^{\otimes n}, \quad \forall n,
\end{align*}
\]

where \(\lambda \in [0, 1]\) is arbitrary. Then, it holds that

\[ P^{\text{LOCC}}_{\text{LOCC}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = \min\left\{ p \left(\frac{m-1}{m+1}\right)^n, (1-p)\lambda^n \right\}. \]

**Proof.** The proof follows similar reasoning as in Theorem 22. We choose the POVM as

\[
\left\{ \left(1_m^{\otimes 2n} - \tilde{\Phi}_m^{\otimes n}\right) \oplus \bigotimes_{d^2-m^2} J, \tilde{\Phi}_m^{\otimes n} \oplus 1_{d^2-m^2} \right\},
\]

where \(\tilde{\Phi}_m := \frac{m-1}{m+1} \Pi_s + \Pi_a\) as in Eq. (13) of [53], and \(\Pi_s\) and \(\Pi_a\) are the projections onto the support of the symmetric and anti-symmetric subspaces, respectively.

Then, the average error probability for the chosen LOCC protocol is

\[
P^{\text{LOCC}}_{\text{LOCC}} = p \text{Tr} \left[ \tilde{\Phi}_m^{\otimes n} \oplus \bigotimes_{d^2-m^2} J \cdot \sigma_m^{\otimes n} \oplus 1_{d^2-m^2} \right] \\
\quad + (1-p) \text{Tr} \left[ \left(1_m^{\otimes 2n} - \tilde{\Phi}_m^{\otimes n}\right) \oplus \bigotimes_{d^2-m^2} J \cdot \left(\lambda \sigma_m \oplus (1 - \lambda) \tau_{d^2-m^2}\right)^{\otimes n} \right] \\
= p \text{Tr} \left[ \tilde{\Phi}_m^{\otimes n} \cdot \sigma_m^{\otimes n} \right] \\
= p \left(\frac{m-1}{m+1}\right)^n
\]

where we invoke Eq. (17) of [53] in the last line. On the other hand, we can also choose the POVM as shown in Eq. (35) to obtain \( P^{\text{LOCC}}_{\text{LOCC}} = (1-p)\lambda^n \). We then choose the minimum of the two to complete the achievability.

The converse follows from Lemma 21 and [53, Proposition 3]. \(\square\)

**Proposition 25.** Consider the binary hypothesis

\[
\begin{align*}
H_0: \rho_0^{\otimes n} &= \left(\sigma_m \oplus \bigotimes_{d^2-m^2} J\right)^{\otimes n}, \\
H_1: \rho_1^{\otimes n} &= \left(\lambda \sigma_m \oplus (1 - \lambda) \tau_{d^2-m^2}\right)^{\otimes n}, \quad \forall n,
\end{align*}
\]

for some \(\lambda \in [0, 1]\). Then, it holds that

\[ P^{\text{LOCC}}_{\text{LOCC}}(\rho_0^{\otimes n}, \rho_1^{\otimes n}; p) = \min\left\{ (1-p) \left(\frac{m-1}{m+1}\right)^n, p \right\}. \]
Proof. We choose the POVM as
\[
\{ \bar{M}_m^{\otimes n} \oplus \mathbb{I}_{d^{2n} - m^2} \cdot (\mathbb{I}_{m^2} - \bar{M}_m^{\otimes n}) \oplus \mathbb{I}_{d^{2n} - m^2} \},
\]
where \( \bar{M}_m := m - \frac{1}{m+1} \Pi_s + \Pi_d \) as in equation (13) of [53] and the proof of Theorem 24.

Then, the average error probability for the chosen LOCC protocol is
\[
P_e^{\text{LOCC}} = p \text{Tr} \left[ \left( \mathbb{I}_{m^2} - \bar{M}_m^{\otimes n} \right) \oplus \mathbb{I}_{d^{2n} - m^2} \cdot \sigma_m^{\otimes n} \oplus \mathbb{I}_{d^{2n} - m^2} \right]
\]
\[+ (1 - p) \text{Tr} \left[ \bar{M}_m^{\otimes n} \oplus \mathbb{I}_{d^{2n} - m^2} \cdot \left( \lambda \sigma_m \oplus (1 - \lambda) \tau d^2 - m^2 \right)^{\otimes n} \right].\]

Finally, we choose \( \rho_1^{\otimes n} \) whenever \( p_{e^{\text{LOCC}}} > p \).

The converse follows Lemma 21 and [53, Proposition 3].

\( \square \)

Remark A.2. The Stein, Hoeffding, and strong converse exponents can be obtained by following the same arguments in Section A. Table 1 provides a summary of the results.

References

1. Lehmann, E.L.: Testing Statistical Hypotheses. Springer, New York (1986)
2. Blahut, R.E.: Hypothesis testing and information theory. IEEE Trans. Inf. Theory 20(4), 405–417 (1974)
3. Haroutunian, E.A., Haroutunian, M.E., Harutyunyan, A.N.: Reliability criteria in information theory and in statistical hypothesis testing. Found. Trends Commun. Inf. Theory 4(2–3), 97–263 (2007)
4. Csiszár, I., Körner, J.: Information Theory: Coding Theorems for Discrete Memoryless Systems, 2nd edn. Cambridge University Press (CUP), Cambridge (2011)
5. Polyanskiy, Y., Poor, H.V., Verdu, S.: Channel coding rate in the finite blocklength regime. IEEE Trans. Inform. Theory 56(5), 2307–2359 (2010)
6. Cheng, H.-C., Hsieh, M.-H.: Moderate deviation analysis for classical-quantum channels and quantum hypothesis testing. IEEE Trans. Inf. Theory 64(2), 1385–1403 (2018)
7. Cheng, H.-C., Hsieh, M.-H., Tomamichel, M.: Quantum sphere-packing bounds with polynomial prefactors. IEEE Trans. Inf. Theory 65(5), 2872–2898 (2019)
8. Cheng, H.-C.: Error exponent analysis in quantum information theory. Ph.D. Thesis (University of Technology Sydney) (2018)
9. Goldreich, O., Goldwasser, S., Ron, D.: Property testing and its connection to learning and approximation. J. ACM 45(4), 653–750 (1998)
10. Kearns, M., Ron, D.: Testing problems with sub-learning sample complexity. In: Proceedings of the Eleventh Annual Conference on Computational Learning Theory—COLT’ 98. ACM Press (1998)
11. Ron, D.: Property testing: a learning theory perspective. Found. Trends Mach. Learn. 1(3), 307–402 (2007)
12. Ron, D.: Algorithmic and analysis techniques in property testing. Found. Trends Theor. Comput. Sci. 5(2), 73–205 (2009)
13. Fischer, E.: The art of uninformed decisions: A primer to property testing. In: Current Trends in Theoretical Computer Science, pp. 229–263. World Scientific (2004)
14. Acharya, J., Daskalakis, C., Kamath, G.: Optimal testing for properties of distributions. Adv. Neural Inf. Process. Syst. 28, 3591–3599 (2015)
15. Canonne, C.L.: A survey on distribution testing: Your data is big. But is it blue? Electron. Colloq. Comput. Complex. 22(63), 1–1 (2015)
16. Yu, N.: Efficient independence testing for quantum states. arXiv:1904.03218 [quant-ph]
17. Wasserman, L., Zhou, S.: A statistical framework for differential privacy. J. Am. Stat. Assoc. 105(489), 375–389 (2010)
18. Duchi, J.C., Jordan, M.I., Wainwright, M.J.: Local privacy and statistical minimax rates. In: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. IEEE (2013)
19. Kairouz, P., Oh, S., Viswanath, P.: The composition theorem for differential privacy. IEEE Trans. Inf. Theory 63(6), 4037–4049 (2017)
20. Balle, B., Barthe, G., Gaboardi, M., Hsu, J., Sato, T.: Hypothesis testing interpretations and Rényi differential privacy. arXiv:1905.09982 [cs.LG]
21. Dong, J., Roth, A., Su, W.J.: Gaussian differential privacy. arXiv:1905.02383 [cs.LG]
22. Helstrom, C.W.: Quantum Detection and Estimation Theory. Elsevier, Amsterdam (1976)
23. Neyman, J., Pearson, E.S.: On the problem of the most efficient tests of statistical hypotheses. Philos. Trans. R. Soc. A Math. Phys. Eng. Sci. 231(694–706), 289–337 (1933)
24. Chernoff, H.: A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. Ann. Math. Stat. 23(4), 493–507 (1952)
25. Chernoff, H.: Large-sample theory: parametric case. Ann. Math. Stat. 27(1), 1–22 (1956)
26. Hoeffding, W.: Asymptotically optimal tests for multinomial distributions. Ann. Math. Stat. 36(2), 369–401 (1965)
27. Audenaert, K.M.R., Calsamiglia, J., Muñoz-Tapia, R., Bagan, E., Masanes, L., Acín, A., Verstraete, F.: Discriminating states: the quantum Chernoff bound. Phys. Rev. Lett. 98, 160501 (2007)
28. Audenaert, K.M.R., Nussbaum, M., Szkola, A., Verstraete, F.: Asymptotic error rates in quantum hypothesis testing. Commun. Math. Phys. 279(1), 251–283 (2008)
29. Nussbaum, M., Szkola, A.: The Chernoff lower bound for symmetric quantum hypothesis testing. Ann. Stat. 37(2), 1040–1057 (2009)
30. Hiai, F., Petz, D.: The proper formula for relative entropy and its asymptotics in quantum probability. Commun. Math. Phys. 143(1), 99–114 (1991)
31. Ogawa, T., Nagaoka, H.: Strong converse and Stein’s lemma in quantum hypothesis testing. IEEE Trans. Inf. Theory 46(7), 2428–2433 (2000)
32. Umegaki, H.: Conditional expectation in an operator algebra. IV. Entropy and information. Kodai Math. Semin. Rep. 14(2), 59–85 (1962)
33. Petz, D.: Quasi-entropies for finite quantum systems. Rep. Math. Phys. 23(1), 57–65 (1986)
34. Nagaoka, H.: The converse part of the theorem for quantum Hoeffding bound (2006). arXiv:quant-ph/0611289 [quant-ph]
35. Nagaoka, H: Strong converse theorems in quantum information theory. In: Asymptotic Theory of Quantum Statistical Inference. World Scientific, pp. 64–65 (2005)
36. Mosonyi, M., Ogawa, T.: Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. Commun. Math. Phys. 334(3), 1617–1648 (2014)
37. Müller-Lennert, M., Dupuis, F., Szehr, O., Fehr, S., Tomamichel, M.: On quantum Rényi entropies: a new generalization and some properties. J. Math. Phys. 54(12), 12203 (2013)
38. Wilde, M.M., Winter, A., Yang, D.: Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy. Commun. Math. Phys. 331(2), 593–622 (2014)
39. Hayashi, M.: Optimal sequence of quantum measurements in the sense of Stein’s lemma in quantum hypothesis testing. J. Phys. A Math. Gen. 35(50), 10759–10773 (2002)
40. Bjelaković, I., Siegmund-Schultze, R.: Quantum Stein’s lemma revisited, inequalities for quantum entropies, and a concavity theorem of Lieb (2003). arXiv:quant-ph/0307170
41. Bjelaković, I., Deuschel, J.-D., Krüger, T., Seiler, R., Siegmund-Schultze, R., Szkola, A.: A quantum version of Sanov’s theorem. Commun. Math. Phys. 260(3), 659–671 (2005)
42. Nagaoka, H., Hayashi, M.: An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses. IEEE Trans. Inf. Theory 53(2), 534–549 (2007)
43. Tomamichel, M., Hayashi, M.: A hierarchy of information quantities for finite block length analysis of quantum tasks. IEEE Trans. Inf. Theory 59(11), 7693–7710 (2013)
44. Li, K.: Second-order asymptotics for quantum hypothesis testing. Ann. Stat. 42(1), 171–189 (2014)
45. Chubb, C.T., Tan, V.Y.F., Tomamichel, M.: Moderate deviation analysis for classical communication over quantum channels. Commun. Math. Phys. 355(3), 1283–1315 (2017)
46. Boixo, S., Isakov, S.V., Smelyanskiy, V.N., Babbush, R., Ding, N., Jiang, Z., Brenner, M.J., Martinis, J.M., Neven, H.: Characterizing quantum supremacy in near-term devices. Nat. Phys. 14(6), 595–600 (2018)
47. Preskill, J.: Quantum computing in the NISQ era and beyond. Quantum 2, 79 (2018)
48. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. 70(13), 1895–1899 (1993)
49. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2009)
50. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. Rev. Mod. Phys. 81(2), 865–942 (2009)
Discrimination of Quantum States Under Locality Constraints

51. Chitambar, E., Leung, D., Mančinska, L., Ozols, M., Winter, A.: Everything you always wanted to know about LOCC (but were afraid to ask). Commun. Math. Phys. 328(1), 303–326 (2014)

52. Bennett, C.H., DiVincenzo, D.P., Fuchs, C.A., Mor, T., Rains, E., Shor, P.W., Smolin, J.A., Wootters, W.K.: Quantum nonlocality without entanglement. Phys. Rev. A 59(2), 1070 (1999)

53. Matthews, W., Winter, A.: On the Chernoff distance for asymptotic LOCC discrimination of bipartite quantum states. Commun. Math. Phys. 285(1), 161–174 (2008)

54. Brandão, F.G., Harrow, A.W., Lee, J.R., Peres, Y.: Adversarial hypothesis testing and a quantum Stein’s lemma for restricted measurements. In Proceedings of the 5th Conference on Innovations in Theoretical Computer Science, pp. 183–194. ACM (2014)

55. Owari, M., Hayashi, M.: Asymptotic local hypothesis testing between a pure bipartite state and the completely mixed state. Phys. Rev. A 90(3), 032327 (2014)

56. Matthews, W., Winter, A.: Local hypothesis testing between a pure bipartite state and the white noise state. IEEE Trans. Inf. Theory 61(12), 6995–7011 (2015)

57. Hayashi, M., Owari, M.: Tight asymptotic bounds on local hypothesis testing between a pure bipartite state and the white noise state. IEEE Trans. Inf. Theory 63(6), 4008–4036 (2017)

58. Calsamiglia, J., Muñoz-Tapia, R., Masanes, L., Acín, A., Bagan, E.: Quantum Chernoff bound as a measure of distinguishability between density matrices: application to qubit and gaussian states. Phys. Rev. A 77(3), 032311 (2008)

59. Calsamiglia, J., de Vicente, J.I., Muñoz-Tapia, R., Bagan, E.: Local discrimination of mixed states. Phys. Rev. Lett. 105(8), 080504 (2010)

60. Nathanson, M.: Testing for a pure state with local operations and classical communication. J. Math. Phys. 51(4), 042102 (2010)

61. Nengkun, Yu, Duan, Runyao, Ying, Mingsheng: Four locally indistinguishable ququd–ququd orthogonal maximally entangled states. Phys. Rev. Lett. 109(2), 020502 (2016)

62. Nengkun, Yu, Duan, Runyao, Ying, Mingsheng: Distinguishability of quantum states by positive operator-valued measures with positive partial transpose. IEEE Trans. Inf. Theory 60(4), 2069–2079 (2014)

63. Li, Y., Wang, X., Duan, R.: Indistinguishability of bipartite states by positive-partial-transpose operations in the many-copy scenario. Phys. Rev. A 95(5), 052346 (2017)

64. Yu, N., Zhou, L.: When is the Chernoff exponent for quantum operations finite? IEEE Trans. Inf. Theory 67(7), 4517–4523 (2021)

65. Akibue, S., Kato, G.: Bipartite discrimination of independently prepared quantum states as a counterexample to a parallel repetition conjecture. Phys. Rev. A 97(4), 042309 (2018)

66. Cheng, H.-C., Datta, N., Rouzé, C.: Strong converse bounds in quantum network information theory: distributed hypothesis testing and source coding (2019). arXiv:1905.00873 [quant-ph]

67. Cheng, H.-C., Datta, N., Rouzé, C.: Strong converse for classical-quantum degraded broadcast channels (2019) arXiv:1905.00874 [quant-ph]

68. Rains, E.: A semidefinite program for distillable entanglement. IEEE Trans. Inf. Theory 47(7), 2921–2933 (2001)

69. Terhal, B.M., DiVincenzo, D.P., Leung, D.W.: Hiding bits in Bell states. Phys. Rev. Lett. 86(25), 5807–5810 (2001)

70. DiVincenzo, D., Leung, D., Terhal, B.: Quantum data hiding. IEEE Trans. Inf. Theory 48(3), 580–598 (2002)

71. Matthews, W., Wehner, S., Winter, A.: Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. Commun. Math. Phys. 291(3), 813–843 (2009)

72. Lancien, C., Winter, A.: Distinguishing multi-partite states by local measurements. Commun. Math. Phys. 323(2), 555–573 (2013)

73. Lami, L., Palazuelos, C., Winter, A.: Ultimate data hiding in quantum mechanics and beyond. Commun. Math. Phys. 361(2), 661–708 (2018)

74. Werner, R.F.: Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model. Phys. Rev. A 40(8), 4277–4281 (1989)

75. Polyanskiy, Y.: Saddle point in the minimax converse for channel coding. IEEE Trans. Inf. Theory 59(5), 2576–2595 (2013)

76. Bennett, C.H., DiVincenzo, D.P., Mor, T., Shor, P.W., Smolin, J.A., Terhal, B.M.: Unextendible product bases and bound entanglement. Phys. Rev. Lett. 82(26), 5385–5388 (1999)

77. DiVincenzo, D.P., Mor, T., Shor, P.W., Smolin, J.A., Terhal, B.M.: Unextendible product bases, uncompletable product bases and bound entanglement. Commun. Math. Phys. 238(3), 379–410 (2003)

78. Bandyopadhyay, S., Cosentino, A., Johnston, N., Russo, V., Watrous, J., Yu, N.: Limitations on separable measurements by convex optimization. IEEE Trans. Inf. Theory 61(6), 3593–3604 (2015)

79. Dembo, A., Zeitouni, O.: Large Deviations Techniques and Applications. Springer, Berlin (1998)

Communicated by M. Christandl