

Tight asymptotic bounds on local hypothesis testing between a pure bipartite state and the white noise state

Masahito Hayashi^{1,2}, Masaki Owari³

¹ Graduate School of Mathematics, Nagoya University, Japan.

² Centre for Quantum Technologies, National University of Singapore, Singapore.

³ NTT Communication Science Laboratories, NTT Corporation
3-1, Morinosato Wakamiya Atsugi-Shi, Kanagawa, 243-0198, Japan

We consider asymptotic hypothesis testing (or state discrimination with asymmetric treatment of errors) between an arbitrary fixed bipartite pure state $|\Psi\rangle$ and the completely mixed state under one-way LOCC, two-way LOCC, and separable POVMs. As a result, we derive the Hoeffding bounds under two-way LOCC POVMs and separable POVMs. Further, we derive a Stein's lemma type of optimal error exponents under one-way LOCC, two-way LOCC, and separable POVMs up to the third order, which clarifies the difference between one-way and two-way LOCC POVM. Our study gives a very rare example in which the optimal performance under the infinite-round two-way LOCC is also equal to the one under separable operations, and can be attained with two-round communication, but cannot be attained with the one-way LOCC.

Background: When a distant bipartite system is given as two parties, Alice and Bob, it is natural to restrict their operations to local operation and classical communication (LOCC) [50] because it is not so easy to realize a quantum operation across both of the distant systems. LOCC operations can be classified by the direction of classical communication. When the direction of classical communication is restricted to only one direction, the LOCC operation is called a one-way LOCC. Otherwise, it is called a two-way LOCC. Although a one-way LOCC operation requires only one-round classical communication, a two-way LOCC operation does plural-round classical communication. In this case, a two-way LOCC protocol with k -round classical communication has $k + 1$ steps. For example, in the case of 2-round classical communication, the total protocol is given as follows when the initial operation is done by Alice: First, Alice performs her operation with her measurement and sends her outcome to Bob. Second, Bob receives Alice's outcome, performs his operation with his measurement, and sends his outcome to Alice. Third, Alice receives Bob's outcome and performs her measurement.

To consider the relation between accessible information and these kinds of restrictions for the operations, many studies state discrimination with LOCC restriction for our measurement [1–30]. In this paper, we focus on hypothesis testing (state discrimination with asymmetric treatment of errors) of a pair of quantum states. When our operations are limited to one-way LOCC operations or two-way LOCC operations, hypothesis testing is called local hypothesis testing. If we do not impose any constraint for our measurement, a general asymptotic theory has been established even for the quantum case when multiple copies of the unknown states are available. For example, Hiai et al. [47] and Ogawa et al. [44] derived the quantum version of Stein's bound [35], i.e., the optimal exponent of the second error under the constant constraint for the first error. Audenaert et al. [31] and Nussbaum et al. [39] did the quantum version of the Chernoff bound [35], i.e., the optimal exponent of the sum of the first and second errors. Other papers [32, 38] did the quantum version of the Hoeffding bound [40, 45, 46], which is the optimal exponent of the second error under the exponential constraint for the first error, and can be considered as a generalization of the Chernoff bound. However, when we impose the one-way or two-way LOCC constraint on our measurement, these problems become very difficult, and they have not been solved completely. In particular, it is quite difficult to solve these problems for an arbitrary fixed pair of quantum states.

To avoid a difficulty caused by generality, this paper discusses the problem of distinguishing an arbitrary fixed pure entangled state $|\Psi\rangle$ from the white noise state, i.e., the completely mixed state. In the non-asymptotic setting, our previous paper [15] addressed the problem under the constraint that $|\Psi\rangle$ is detected with probability 1, and our previous paper [34] did it in a more general setting. In particular, the paper [34] proposed concrete two-round classical communication two-way LOCC protocols that are not reduced to one-way LOCC. Then, our previous paper [36]

extended the problem to the case when the entangled state is given as the n -copy state of a certain entangled state. As asymptotic results, it showed that there is no difference between one-way and two-way LOCC for the Stein's bound, i.e., the optimal exponent of the second error under the constant constraint for the first error. To make an upperbound of the optimal performance of the two-way LOCC case, these papers [15, 34, 36] also considered the performance in the case of separable operations, which can be easily treated because of their mathematically simple forms. The class of separable operations includes LOCC, but there exist a separable operations which are not LOCC [3].

However, our previous paper [36] could not derive the Hoeffding bound for two-way LOCC, i.e., the optimal exponent of the second error under the exponential constraint for the first error, while it derived it for one-way LOCC. Further, even under the constant constraint for the first error, the paper did not consider the higher order of the decreasing rate of the second error. Indeed, in information theory, Strassen [37] derived the decreasing rate of the second error up to the third-order $\log n$ under the same constraint in the classical setting when n is the number of available copies. Tomamichel et al [42] and Li [41] extended this result up to the second order \sqrt{n} .

Our obtained results: In this paper, we derive the Hoeffding bound for two-way LOCC and the optimal decreasing rate of the second error under the constant constraint for the first error up to the third-order $\log n$ for one-way and two-way LOCC. We also derive them for separable measurements. Then, we find the following:

- (1) There is a difference in the Hoeffding bound between the one-way and two-way LOCC constraints unless the entangled state $|\Psi\rangle$ is maximally entangled. However, there is no difference in the Hoeffding bound between two-way LOCC and separable constraints.
- (2) The optimal decreasing rate of the second error under the constant constraint for the first error has no difference between the one-way and two-way LOCC constraints up to the second order \sqrt{n} , but has a difference in the third order $\log n$ unless the entangled state $|\Psi\rangle$ is maximally entangled. On the other hand, this optimal decreasing rate has no difference between the two-way LOCC and separable constraints up to the third order $\log n$.
- (3) Three-step two-way LOCC protocol proposed in [34] can achieve the Hoeffding bound as well as the optimal decreasing rate of the second error under the constant constraint for the first error up to the third order $\log n$ for two-way LOCC.

Mathematical description of obtained results: A single copy of a bipartite Hilbert space is written as $\mathcal{H}_{AB} \stackrel{\text{def}}{=} \mathcal{H}_A \otimes \mathcal{H}_B$, and its local dimensions are written as $d_A \stackrel{\text{def}}{=} \dim \mathcal{H}_A$ and $d_B \stackrel{\text{def}}{=} \dim \mathcal{H}_B$. We consider asymptotic hypothesis testing between n -copies of an arbitrary known pure-bipartite state $|\Psi\rangle$ with the Schmidt decomposition as $|\Psi\rangle \stackrel{\text{def}}{=} \sum_{i=1}^d \sqrt{\lambda_i} |i\rangle \otimes |i\rangle$ and n -copies of the completely mixed state (or the white noise) $\rho_{mix} \stackrel{\text{def}}{=} \frac{I_{AB}}{d_A d_B}$ under the various restrictions on available POVMs: global POVMs, separable POVMs, one-way LOCC POVMs, and two-way LOCC POVMs [49, 50]. We choose the completely mixed state $\rho_{mix}^{\otimes n}$ as a null hypothesis and the state $|\Psi\rangle^{\otimes n}$ as an alternative hypothesis. The optimal type-2 error under the condition that the type-1 error is no more than a constant $\alpha \geq 0$ is written as

$$\beta_{n,C}^L(\alpha | \Psi || \rho_{mix}) \stackrel{\text{def}}{=} \min_{T_n: 0 \leq T_n \leq I} \{ \log \beta_n(T_n) \mid \alpha_n(T_n) \leq \alpha, \{T_n, I - T_n\} \in C \}, \quad (1)$$

where $\beta_n(T_n) := \langle \Psi |^{\otimes n} T_n | \Psi \rangle^{\otimes n}$, $\alpha_n(T_n) := \text{Tr}(I - T_n) \rho_{mix}^{\otimes n}$, and C is either \rightarrow , \leftrightarrow , *Sep*, or *g* corresponding to a classes of one-way LOCC, two-way LOCC, separable and global POVMs, respectively. Further, we denote the class of two-way LOCCs with k -round classical communication by \leftrightarrow, k . In this notation, $\leftrightarrow, 1$ is equivalent with \rightarrow .

We introduce the Rényi entropy $H_{1-s}(\Psi) := \frac{\log \sum_i \lambda_i^{1-s}}{s}$ of the entangled state $|\Psi\rangle$, and $H_1(\Psi)$ is defined as the limit $\lim_{s \rightarrow 0} H_{1-s}(\Psi)$. By using the Rényi entropy $H_{1-s}(\Psi)$, the entropy of the entanglement $E(|\Psi\rangle)$, the Schmidt rank $R_S(|\Psi\rangle)$ [49, 50], and the logarithmic robustness of

entanglement $LR(|\Psi\rangle)$ [51, 52] are characterized as $E(|\Psi\rangle) = H_1(\Psi)$, $\log R_s(|\Psi\rangle) = H_0(\Psi)$, and $LR(|\Psi\rangle) = H_{1/2}(\Psi)$. In the following, for the unified treatment, we only use the notation $H_{1-s}(\Psi)$. We also prepare the quantity $V(\Psi) := \sum_i \lambda_i (\log \lambda_i + H_1(\Psi))^2$.

Our previous paper [36] showed that the Stein bounds are given as follows. For a given $\epsilon > 0$, we have the following expansion.

$$\beta_{n,\rightarrow}^L(\epsilon|\Psi\|\rho_{mix}) = \beta_{n,\leftrightarrow}^L(\epsilon|\Psi\|\rho_{mix}) + o(n) = \beta_{n,sep}^L(\epsilon|\Psi\|\rho_{mix}) + o(n) = -n(\log d_A d_B - H_1(\Psi)) + o(n). \quad (2)$$

In [36], we also characterized the Hoeffding bounds as follows.

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \beta_{n,\rightarrow}^L(e^{-nr}|\Psi\|\rho_{mix}) = \sup_{0 \leq s < 1} \frac{-s}{1-s} r - H_s(\Psi) + \log d_A d_B. \quad (3)$$

Further, for the specific parameter r satisfying $r \geq \log d - \frac{1}{4}H'_{1/2}$, [36] also showed

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \beta_{n,\rightarrow}^L(e^{-nr}|\Psi\|\rho_{mix}) = \log d_A d_B - H_{1/2}. \quad (4)$$

As a refinement of (2), we obtain the following for a given $\epsilon > 0$:

$$\beta_{n,\rightarrow}^L(\epsilon|\Psi\|\rho_{mix}) = -n(\log d_A d_B - H_1(\Psi)) + \sqrt{n} \sqrt{V(\Psi)} \Phi^{-1}(\epsilon) - \frac{1}{2} \log n + O(1) \quad (5)$$

$$\beta_{n,\leftrightarrow}^L(\epsilon|\Psi\|\rho_{mix}) = \beta_{n,sep}^L(\epsilon|\Psi\|\rho_{mix}) + O(1) = -n(\log d_A d_B - H_1(\Psi)) + \sqrt{n} \sqrt{V(\Psi)} \Phi^{-1}(\epsilon) - \log n + O(1), \quad (6)$$

where $\Phi(x) := \int_{-\infty}^x \frac{e^{-y^2/2}}{\sqrt{2\pi}} dy$. The above relations show that the difference between $\beta_{n,\rightarrow}^L(\epsilon|\Psi\|\rho_{mix})$ and $\beta_{n,\leftrightarrow}^L(\epsilon|\Psi\|\rho_{mix})$ exists only in the order $\log n$. We also completely characterized the Hoeffding bounds of two-way LOCC and separable cases without any restriction for the parameter r as follows:

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \beta_{n,\leftrightarrow}^L(e^{-nr}|\Psi\|\rho_{mix}) = \lim_{n \rightarrow \infty} -\frac{1}{n} \beta_{n,sep}^L(e^{-nr}|\Psi\|\rho_{mix}) = \sup_{0 \leq s < 1} \frac{-2s}{1-s} r - H_{\frac{1+s}{2}}(\Psi) + \log d_A d_B. \quad (7)$$

The optimal two-way LOCC protocol: The optimal two-way LOCC protocol is the three-step LOCC protocol having the following feature:

1. Alice's first measurement is diagonal in the Schmidt basis of $|\Psi\rangle$.
2. Bob's measurement is in the mutually unbiased basis of the Schmidt basis of the post-measurement state of Alice's first measurement.
3. Alice's second measurement is chosen such that when the true state is $|\Psi\rangle$, Alice always gives the correct answer.

Conclusion: In this paper, we have treated local asymptotic hypothesis testing between an arbitrary known bipartite pure state $|\Psi\rangle$ and the completely mixed state ρ_{mix} . Under the exponential constraint for the type-1 error probability (the Hoeffding bound), there clearly exists a difference between the optimal exponential decreasing rates of the type-2 error probabilities under one-way and two-way LOCC POVMs. However, when we surpass the constraint for the type-1 error probability, this kind of difference is very subtle. That is, there exists a difference only in the third order for the optimal exponential decreasing rates of the type-2 error probabilities under one-way and two-way LOCC POVMs. From the beginning of the study of LOCC, many studies focused on the effect by increasing the number of the communication round, as well as the difference between two-way LOCC and separable operations. In this viewpoint, our study gives a very rare example in which the optimal performance under the infinite-round two-way LOCC, which is different from

the one under the one-way LOCC, can be attained with two-round communication, and is also equal to the one under separable operations.

Acknowledgement

This research was partially supported by the MEXT Grant-in-Aid for Young Scientists (A) No. 20686026, and Grant-in-Aid for Scientific Research (A) No. 23246071. The Center for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

-
- [1] A. Peres and W.K. Wootters, *Phys. Rev. Lett.* **66**, 1119, (1991).
 - [2] S. Massar and S. Popescu, *Phys. Rev. Lett.* **74**, 1259 (1995)
 - [3] C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, and W.K. Wootters, *Phys. Rev. A*, **59**, 1070, (1999).
 - [4] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, *Phys. Rev. Lett.*, **85**, 4972, (2000).
 - [5] B. Groisman, L. Vaidman, *J. Phys. A: Math. Gen.*, **34** 6881 (2001).
 - [6] S. Virmani, M.F. Sacchi, M.B. Plenio, and D. Markham, *Phys. Lett. A*, **288**, 62, (2001).
 - [7] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, *Phys. Rev. Lett.*, **87**, 277902, (2001).
 - [8] B.M. Terhal, D.P. DiVincenzo, and D.W. Leung, *Phys. Rev. Lett.*, **86**, 5807, (2001).
 - [9] J. Watrous, *Phys. Rev. Lett.*, **95**, 080505, (2005).
 - [10] M. Hayashi, D. Markham, M. Muraio, M. Owari, and S. Virmani, *Phys. Rev. Lett.*, **96**, 040501, (2006).
 - [11] M. Hayashi, K. Matsumoto, Y. Tsuda, *J. Phys. A: Math. Gen.*, **39**,14427, (2006).
 - [12] M. Owari and M. Hayashi, *Phys. Rev. A*, **74**, 032108 (2006).
 - [13] M. Koashi, F. Takenaga, T. Yamamoto, N. Imoto, arXiv:0709.3196 (2007)
 - [14] S.M. Cohen *Phys. Rev. A*, **75** 052313, (2007).
 - [15] M. Owari, and M. Hayashi, *New J. of Phys.*, **10**, 013006, (2008).
 - [16] Y. Ishida, T. Hashimoto, M. Horibe, and A. Hayashi, *Phys. Rev. A* **78**, 012309, (2008).
 - [17] W. Matthews and A. Winter, *Comm. Math. Phys.*, **285**, 161, (2009).
 - [18] R. Duan, Y. Feng, Y. Xin, M. Ying, *IEEE Trans. Inf. Theory*, **55**, 1320, (2009).
 - [19] M. Hayashi, *New J. Phys.*, **11**, 043028, (2009).
 - [20] W. Jiang, X.-J. Ren, X. Zhou, Z.-W. Zhou, and G.-C. Guo *Phys. Rev. A* **79**, 032330, (2009).
 - [21] J. Calsamiglia, J. I. de Vicente, R. Muñoz-Tapia, and E. Bagan *Phys. Rev. Lett.*, **105**, 080504 (2010)
 - [22] W. Jiang, X.-J. Ren, Y.-C. Wu, Z.-W. Zhou, G.-C. Guo and H. Fan *J. Phys. A: Math. Theor.* **43**, 325303, (2010)
 - [23] S. Bandyopadhyay, *Phys. Rev. A*, **81**, 022327 (2010)
 - [24] M. Nathanson, *J. Math. Phys.* **51**, 042102, (2010).
 - [25] M. Kleinmann, H. Kampermann, and D. Bruß, *Phys. Rev. A*, **84**, 042326 (2011).
 - [26] K. Li, A. Winter, *Comm. Math. Phys.*, **326** (1) 63-80 (2014)
 - [27] E. Chitambar and M.-H. Hsieh, *Phys. Rev. A* **88**, 020302(R) (2013)
 - [28] A. M. Childs, D. Leung, L. Mancinska, M. Ozols, *Comm. Math. Phys.*, **323**, 1121 (2013)
 - [29] H. Fu, D. Leung, L. Mancinska, *Phys. Rev. A* **89**, 052310 (2014)
 - [30] F.G.S.L. Brandao, A.W. Harrow, J.R. Lee, Y. Peres, *Proc. of 5th ITCS*, pp. 183-194 (2014)
 - [31] K.M.R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acín, F. Verstraete, *Phys. Rev. Lett.* **98**, 160501 (2007).
 - [32] M. Hayashi *Phys. Rev. A*, **76**, 062301 (2007)
 - [33] K.M.R. Audenaert, M. Nussbaum, A. Szkola, F. Verstraete, *Comm. Math. Phys.* 279, 251-283 (2008)
 - [34] M. Owari, M. Hayashi, arXiv:1006.2744 (2010)
 - [35] H. Chernoff, *Ann. Math. Stat.* **23**, 493 (1952)
 - [36] M. Owari and M. Hayashi, arXiv:1105.3789 (2011); Accepted for *Phys. Rev. A*.
 - [37] V. Strassen, "Asymptotische Abschätzungen in Shannon's Informationstheorie," *Trans. Third Prague Conf. Information Theory*, 1962. English translation by M. Luthy available from <http://www.math.cornell.edu/~pmlut/strassen.pdf>.
 - [38] H. Nagaoka "The Converse Part of The Theorem for Quantum Hoeffding Bound," arXiv:quant-ph/0611289
 - [39] M. Nussbaum, and A. Szkola, "The Chernoff lower bound for symmetric quantum hypothesis testing," *Annals of Statistics*, Vol. 37, No. 2, 1040-1057, 2009.

- [40] W. Hoeffding, "Asymptotically Optimal Tests for Multinomial Distributions", *Ann. Math. Statist.* **36**, 369-401 (1965)
- [41] K. Li, "Second Order Asymptotics for Quantum Hypothesis Testing," *Annals of Statistics* Vol. 42, No. 1, 171-189 (2014).
- [42] M. Tomamichel and M. Hayashi, "A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks," *IEEE Trans. Inf. Theory*, Vol. 59, No. 11, 7693-7710 (2013).
- [43] I. Csiszár and J. Körner, *Information theory: Coding Theorem for Discrete Memoryless systems*, Academic Press, New York, (1981)
- [44] T. Ogawa, and H. Nagaoka, *IEEE Trans. Inf. Theory*, vol.46, no. 7, pp. 2428-2433, (2000).
- [45] R.E. Blahut, *IEEE Trans. Inf. Theory*, **60**, 405 (1974)
- [46] I. Csiszár, G. Longo, *Studia Sci. Math. Hungarica*, **6**, 181 (1971)
- [47] F. Hiai and D. Petz, *Comm. Math. Phys.*, vol.143, 99, (1991).
- [48] E. Chitambar, D. Leung, L. Mancinska, M. Ozols, A. Winter, *Comm. Math. Phys.*, vol. 328, no. 1, pp. 303-326 (2014).
- [49] S. Virmani and M.B. Plenio, *Quant. Inf. Comp.* **7**, 1, (2007).
- [50] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Rev. Mod. Phys.* **81**, 865, (2009).
- [51] F.G.S.L. Brandao, *Phys. Rev. A*, **72**, 022310 (2005).
- [52] N. Datta, *Int. J. Quant. Inf.* **7**, 475 (2009).