

Measuring quantum relative entropy with finite-size effect

Masahito Hayashi^{1,2,3}

¹School of Data Science, The Chinese University of Hong Kong, Shenzhen, Longgang District, Shenzhen, 518172, China

²International Quantum Academy, Futian District, Shenzhen 518048, China

³Graduate School of Mathematics, Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464-8602, Japan

We study the estimation of relative entropy $D(\rho\|\sigma)$ when σ is known. We show that the Cramér-Rao type bound equals the relative varentropy. Our estimator attains the Cramér-Rao type bound when the dimension d is fixed. It also achieves the sample complexity $O(d^2)$ when the dimension d increases. This sample complexity is optimal when σ is the completely mixed state. Also, it has time complexity $O(d^6 \text{ polylog } d)$. Our proposed estimator unifiedly works under both settings.

1 Introduction

Distinguishing a given known state σ from another state ρ is a fundamental task in quantum information. When the state ρ is known as well as σ and n copies of the unknown state are prepared, quantum Stein's lemma [1, 2] guarantees that the quantum relative entropy $D(\rho\|\sigma) := \text{Tr}(\rho(\log \rho - \log \sigma))$ gives the limitation of the optimal discrimination power. The measurement achieving the optimal performance depends only on the state σ [3]. Further, quantum Sanov theorem [4, 5] shows that the construction of the test achieving the optimal performance depends only on the state σ and the value of the quantum relative entropy $D(\rho\|\sigma)$. That is, when we construct the test achieving the optimal performance, the information of the quantum relative entropy $D(\rho\|\sigma)$ is needed in addition to the information of σ . Although the papers [6, 7] studied the estimation of von Neumann entropy and Rényi entropy, they did not study the estimation of the quantum relative entropy $D(\rho\|\sigma)$ with the known state σ . Due to the non-commutativity between ρ and σ , the method in [6, 7] cannot be

applied to the estimation of the quantum relative entropy $D(\rho\|\sigma)$ even when the state σ is known. In particular, the simple use of Schur sampling [8, 9, 10, 11, 12, 13] does not work for the estimation of the quantum relative entropy $D(\rho\|\sigma)$ although the paper [6] employs Schur sampling. Therefore, this paper studies how to estimate the quantum relative entropy $D(\rho\|\sigma)$ with n copies of the unknown state ρ when σ is known.

In fact, when we intend to prepare a specific state σ , it is crucial to identify the difference between the known target state σ and the unknown actual real state ρ . In this situation, we often focus on the fidelity $F(\rho, \sigma) := \text{Tr}[\sqrt{\rho}\sqrt{\sigma}]$ for this aim. Many papers [14, 15, 16, 17, 18] studied this problem when σ is a pure state. However, no paper focuses on this topic when σ is a mixed state. Instead of the fidelity, one can evaluate the difference between σ and ρ by using the quantum relative entropy $D(\rho\|\sigma)$ because of the bounding inequality $-2 \log F(\rho, \sigma) \leq D(\rho\|\sigma)$ [19, Eq.(3.49)]. That is, our problem works for evaluating this difference.

The estimation of $D(\rho\|\sigma)$ with the unknown state ρ is formulated as a special case of the estimation of a function output with nuisance parameters. This general problem setting has been studied in various researches [20, 21, 22, 23, 24, 25]. The reference [25, Section III] addressed the estimation problem of $D(\rho\|\sigma)$ as a special case, and showed that the estimation error is lower bounded by the relative varentropy $V(\rho\|\sigma) := \text{Tr}(\rho((\log \rho - \log \sigma) - D(\rho\|\sigma))^2)$, which appears in the second-order theory of hypothesis testing [26, 27] while it did not show its attainability. Under a general setting, the reference [22, Section 4.3] showed that the optimal precision of the estimation is given by the Cramér-Rao type bound C with nuisance parameters, which equals the inverse of the projected symmetric logarithmic derivative (SLD) Fisher information in the

Masahito Hayashi: hmasahito@cuhk.edu.cn,
masahito@math.nagoya-u.ac.jp

one-parameter case. The meaning of the Cramér-Rao type bound C is the following: when n copies of the unknown state ρ is prepared under a fixed model, the mean square of our best estimator behaves as $\frac{C}{n} + o(\frac{1}{n})$. When we have no nuisance parameter, the recent paper [28] showed the existence of an estimator whose mean square error (MSE) equals $\frac{C}{n}$ without additional term under special models. However, such an estimator does not exist in general.

In this paper, as the first step, using the results for estimation with nuisance parameters in [22, Section 4.3], we show that the Cramér-Rao type bound C of this problem equals the relative varentropy $V(\rho\|\sigma) := \text{Tr}\rho((\log\rho - \log\sigma) - D(\rho\|\sigma))^2$, which was obtained as a lower bound in [25]. In practice, it is necessary to find an estimator to achieve the MSE $\frac{C}{n} + o(\frac{1}{n})$. In addition, it is also desired to clearly evaluate the difference between its mean square error and the Cramér-Rao type bound $\frac{C}{n}$. Since our problem is one-parameter estimation, it is possible to achieve the above bound without the use of collective measurements across several quantum systems. However, this method requires an adaptive choice of measurement. A typical method is the two-step estimator, consisting of a pre-estimation stage and a local optimal estimation stage. When we have n copies of the unknown state ρ , theoretically, in order to achieve the optimal bound, it is sufficient to allocate $\sqrt{n}$ copies to the pre-estimation stage [29, 21]. Although this method achieves the optimal mean square error in the order $\frac{1}{n}$, i.e., the first order, it is not so clear how the mean square error is close to the leading term $\frac{C}{n}$. From the practical viewpoint, it is necessary to upper bound this difference by using the number n of unknown copies. Unfortunately, the above method has difficulty to evaluate the difference between its mean square error and $\frac{C}{n}$. The papers [30, 31] also proposed different adaptive methods for parameter estimation, but their methods have the same problem. In addition, the above adaptive approach does not work when the dimension d of the quantum system increases in addition to the number n of copies.

In summary, to account for finite-size effects in our estimation, we need to find an estimator of the quantum relative entropy $D(\rho\|\sigma)$ to satisfy the following conditions. It asymptotically attains the Cramér-Rao type bound $V(\rho\|\sigma)$ in

the sense of the order $\frac{1}{n}$ when the dimension d is fixed. The difference between its mean square error and the Cramér-Rao type bound is evaluated in terms of the number n of copies. Furthermore, the estimator performs well even when the dimension d of the quantum system increases in addition to the number n of the prepared copies.

As the second step of this paper, to satisfy the above requirements, we propose an alternative estimation method by using Schur transform [32]. Then, we evaluate its mean square error and compare it to the Cramér-Rao type bound with a finite number n . In addition, we evaluate the tail probability.

As the third step, similar to the papers [6, 7], we study the case when the dimension d increases when n increases. Unlike the estimation of von Neumann entropy, the range of the quantum relative entropy or the relative varentropy is not bounded even with fixed dimension d . Therefore, to study the sample complexity, we need to restrict the possible range of ρ and σ . We show that the sample complexity of our method is $O(d^2)$ under a certain natural restriction for this range. Our method extensively improves the sample complexity over the simple application of the full tomography [33]. In particular, the restriction of the possible range of σ is crucial in this analysis. We also show that our time complexity is $O(d^6 \text{polylog } d)$.

When σ is fixed to the completely mixed state, our problem is the same as the estimation of von Neumann entropy, which was studied in the papers [6, 7]. Our result contains the case studied in the papers [6, 7]. In this special case, the paper [6] also showed that the lower bound of the sample complexity is $O(d^2)$ for the Empirical Young Diagram (EYD) algorithm, which is given as the entropy of the diagonal state determined by the Young indices. Although this case improves the sample complexity over the simple application of the full tomography, the improvement is incremental. The paper [7] also showed a lower bound $O(d)$ for the sample complexity, without restricting our algorithm to EYD algorithm. In this special case, we show that our measurement can be restricted to Schur sampling.

The remaining part of this paper is organized as follows. First, Section 2 derives the Cramér-Rao type bound for the estimation of quantum relative entropy. Section 3 presents our estima-

tor for quantum relative entropy, and its performance. Then, this section shows that this estimator asymptotically attains the Cramér-Rao type bound when d is fixed. Section 4 studies the sample complexity of our method when d increases. Section 5 studies the time complexity of our method when d increases. Appendices are devoted to the proofs of the results presented in Section 3.

2 Cramér-Rao type bound

To clarify the minimum mean square error with the first order $\frac{1}{n}$, we discuss the Cramér-Rao type bound C with nuisance parameters, which is mathematically formulated as a lower bound of MSE under the local unbiasedness condition. The reference [25, (3.24), (3.52)] showed that the varentropy $V(\rho_*\|\sigma)$ is a lower bound under the estimation of $D(\rho\|\sigma)$ at $\rho = \rho_*$. That is, they showed that

$$C \geq V(\rho_*\|\sigma), \quad (1)$$

and did not discuss whether the equality holds.

In the following, we show the equality in (1). For this aim, we review the Cramér-Rao type bound C for a general function $f(\rho)$ in the full parameter model under a d -dimensional system as follows. We choose a parameterization ρ_θ with $\theta = (\theta^1, \theta^2, \dots, \theta^{d^2-1}) \in \mathbb{R}^{d^2-1}$ such that the first parameter gives the value of the function to be estimated and the other parameters are orthogonal to the first parameter at $\rho = \rho_*$. That is, our parameter needs to satisfy the following conditions.

$$\rho_{\theta_0} = \rho_*, \quad (2)$$

$$\left. \frac{\partial f(\rho_\theta)}{\partial \theta^1} \right|_{\theta=\theta_0} = 1, \quad (3)$$

$$\left. \frac{\partial f(\rho_\theta)}{\partial \theta^j} \right|_{\theta=\theta_0} = 0 \quad (4)$$

for $j = 2, \dots, d^2 - 1$, where $\theta_0 := (\theta_0^1, 0, \dots, 0)$, and $\theta_0^1 := f(\rho_*)$.

For the latter discussion, we introduce the symmetric logarithmic derivative (SLD) inner product. Given two Hermitian matrices X, Y , we define $X \circ Y := (XY + YX)/2$. Then, we define the SLD inner product $\langle X, Y \rangle_\rho := \text{Tr}(\rho \circ X)Y = \text{Tr}(\rho(X \circ Y))$. We define the SLD norm $\|X\|_\rho :=$

$\sqrt{\langle X, X \rangle_\rho}$. We choose the SLD $L_1, \dots, L_{d^2-1}$ as

$$\left. \frac{\partial \rho_\theta}{\partial \theta^j} \right|_{\theta=\theta_0} = \rho_* \circ L_j \quad (5)$$

for $j = 1, \dots, d^2 - 1$. We also assume the following orthogonal condition;

$$\langle L_1, L_j \rangle_{\rho_*} = \text{Tr} \left. \frac{\partial \rho_\theta}{\partial \theta^j} \right|_{\theta=\theta_0} L_1 = 0 \quad (6)$$

for $j = 2, \dots, d^2 - 1$. Then, we can calculate the Cramér-Rao type bound, i.e., the minimum mean square error under the local unbiasedness condition even under the full parameter model.

Proposition 1 ([22, Theorem 5.3]). *Assume the conditions (2)–(6). The Cramér-Rao type bound for the estimation of $f(\rho_\theta)$ is $\langle L_1, L_1 \rangle_{\rho_*}^{-1}$ at $\theta = \theta_0$.*

To calculate the Cramér-Rao type bound for $D(\rho\|\sigma)$ at $\rho = \rho_*$, we choose the Hermitian matrix

$$L^1 := ((\log \rho_* - \log \sigma) - D(\rho_*\|\sigma)I), \quad (7)$$

and $d^2 - 1$ linearly independent Hermitian traceless matrices $X_1, X_2, \dots, X_{d^2-1}$ such that

$$X_1 = V(\rho_*\|\sigma)^{-1} \rho_* \circ L^1 \quad (8)$$

$$\text{Tr} X_j L^1 = 0 \quad (9)$$

for $j = 2, \dots, d^2 - 1$. Then, we choose our parameterization ρ_θ as

$$\rho_\theta := \rho_* + (\theta^1 - \theta_0^1)X_1 + \sum_{j=2}^{d^2-1} \theta^j X_j. \quad (10)$$

This parameterization satisfies the condition (2).

Since $\left. \frac{\partial \rho_\theta}{\partial \theta^j} \right|_{\theta=\theta_0} = X_j$, we have

$$\begin{aligned} & \left. \frac{\partial D(\rho_\theta\|\sigma)}{\partial \theta^1} \right|_{\theta=\theta_0} \\ &= \text{Tr} \left. \frac{\partial \rho_\theta}{\partial \theta^1} \right|_{\theta=\theta_0} (\log \rho_* - \log \sigma) \\ & \quad + \text{Tr} \rho_* \left. \frac{\partial \log \rho_\theta}{\partial \theta^1} \right|_{\theta=\theta_0} \\ & \stackrel{(a)}{=} \text{Tr} X_1 (\log \rho_* - \log \sigma) + \text{Tr} X_1 \\ & \stackrel{(b)}{=} \text{Tr} X_1 L^1 + \text{Tr} X_1 D(\rho_*\|\sigma)I + \text{Tr} X_1 \stackrel{(c)}{=} 1. \end{aligned} \quad (11)$$

Here, (b) and (c) follow from (7) and the pair of (8) and the relation $\langle L^1, L^1 \rangle_{\rho_*} = V(\rho_*\|\sigma)$,

respectively. In addition, (a) can be shown as follows.

$$\begin{aligned} & \text{Tr}_{\rho_{\theta_0}} \frac{\partial \log \rho_{\theta}}{\partial \theta^1} \Big|_{\theta=\theta_0} \\ & \stackrel{(a)}{=} \text{Tr} \int_0^1 \rho_{\theta_0}^s \frac{\partial \log \rho_{\theta}}{\partial \theta^1} \Big|_{\theta=\theta_0} \rho_{\theta_0}^{1-s} ds \\ & = \text{Tr} \frac{\partial \rho_{\theta}}{\partial \theta^1} \Big|_{\theta=\theta_0} = \text{Tr} X_1, \end{aligned} \quad (12)$$

where (a) follows from [19, Eq. (6.32)].

Using (9) and a similar discussion, we have

$$\begin{aligned} \frac{\partial D(\rho_{\theta} \parallel \sigma)}{\partial \theta^j} \Big|_{\theta=\theta_0} &= \text{Tr} X_j (\log \rho_* - \log \sigma) + \text{Tr} X_j \\ &= 0. \end{aligned} \quad (13)$$

Then, (12) and (13) imply the conditions (3) and (4).

Due to (8) and (9), we have $L_1 = V(\rho_* \parallel \sigma)^{-1} L^1$ and

$$\text{Tr} \frac{\partial \rho_{\theta}}{\partial \theta^j} L_1 = \text{Tr} X_j L_1 = 0 \text{ for } j = 2, \dots, d^2 - 1, \quad (14)$$

which implies the condition (6). Therefore, since all the conditions (2) – (6) hold, due to Proposition 1, the Cramér-Rao type bound for the estimation of $D(\rho \parallel \sigma)$ is $\langle L_1, L_1 \rangle_{\rho_*}^{-1} = V(\rho_* \parallel \sigma)$ at $\theta = \theta_0$. That is, the minimum mean square error under the local unbiasedness condition is $V(\rho_* \parallel \sigma)$. That is, the Cramér-Rao type bound for the estimation of $D(\rho \parallel \sigma)$ is the relative var-entropy $V(\rho_* \parallel \sigma)$. Thus, the quality in (1) holds.

3 Estimator based on Schur transform

Similar to the papers [34, 3, 8, 9, 10, 11, 12, 13, 5, 35, 36], we employ Schur duality of $\mathcal{H}^{\otimes n}$. For this aim, we prepare several notations. A sequence of monotone-increasing non-negative integers $\lambda = (\lambda_1, \dots, \lambda_d)$ is called Young index. Although many references [36, 37, 38] define Young index as monotone-decreasing non-negative integers, we define it in the opposite way for notational convenience. We denote the set of Young indices λ with the condition $\sum_{j=1}^d \lambda_j = n$ by Y_d^n . Then, as explained in [36, Section 6.2], we have

$$\mathcal{H}^{\otimes n} = \bigoplus_{\lambda \in Y_d^n} \mathcal{U}_{\lambda} \otimes \mathcal{V}_{\lambda}. \quad (15)$$

Here, $\mathcal{U}_{\lambda}$ expresses the irreducible space of $\text{SU}(d)$ and $\mathcal{V}_{\lambda}$ expresses the irreducible space of the representation π of the permutation group $\mathfrak{S}_n$. We define $d_{\lambda} := \dim \mathcal{U}_{\lambda}$, $d'_{\lambda} := \dim \mathcal{V}_{\lambda}$. Then, for states σ, ρ , we have

$$\rho^{\otimes n} = \sum_{\lambda \in Y_d^n} \rho_{\lambda} \otimes \rho_{\lambda, \text{mix}}, \quad (16)$$

$$\sigma^{\otimes n} = \sum_{\lambda \in Y_d^n} \sigma_{\lambda} \otimes \rho_{\lambda, \text{mix}}, \quad (17)$$

where $\rho_{\lambda, \text{mix}}$ is the completely mixed state on $\mathcal{V}_{\lambda}$. In the above equations, we consider that matrices on the subspace $\mathcal{U}_{\lambda} \otimes \mathcal{V}_{\lambda}$ are matrices on the whole space $\mathcal{H}^{\otimes n}$. In the first step, we apply the Schur transform U_{Schur} , which realizes a basis change to block-diagonalize $U^{\otimes n}$ for an arbitrary unitary U . It is known that the Schur transform U_{Schur} can be efficiently done [32]. We choose a basis $\{|u_{\lambda, j}\rangle\}_{j=1}^{d_{\lambda}}$ of $\mathcal{U}_{\lambda}$ such that $|u_{\lambda, j}\rangle$ is an eigenvector of σ_{λ} .

To estimate the quantum relative entropy $D(\rho \parallel \sigma)$, we employ the POVM $M = \{M_{\lambda, j}\}_{\lambda, j}$ defined as

$$M_{\lambda, j} := |u_{\lambda, j}\rangle \langle u_{\lambda, j}| \otimes I(\mathcal{V}_{\lambda}), \quad (18)$$

where $I(\mathcal{V}_{\lambda})$ is the identity operator on $\mathcal{V}_{\lambda}$. The measurement outcome is given as (λ, j) so that it obeys the probability distribution

$$P_{\rho, \sigma}^{(n)}(\lambda, j) := \text{Tr} M_{\lambda, j} \rho^{\otimes n}. \quad (19)$$

To estimate the quantum relative entropy $D(\rho \parallel \sigma)$, we employ the estimate $x_{\lambda, j}$ defined as $-\frac{1}{n} \log \text{Tr} M_{\lambda, j} \sigma^{\otimes n}$. Our estimation protocol is summarized as Protocol 1.

Protocol 1 Estimation of relative entropy

Step 1. We apply the Schur transform U_{Schur} .

Step 2. We measure the system by using the measurement $M = \{M_{\lambda, j}\}_{\lambda, j}$.

Step 3. We set our estimate to be $x_{\lambda, j} := -\frac{1}{n} \log \text{Tr} M_{\lambda, j} \sigma^{\otimes n}$.

To evaluate the mean square error of this estimator, we denote the dimension of $\bigoplus_{\lambda \in Y_d^n} \mathcal{U}_{\lambda}$ by $d_{n, d}$. Since as shown in [36, (6.16) and (6.18)],

we have

$$\dim \mathcal{U}_{\lambda} \leq (n+1)^{d(d-1)/2}, \quad |Y_d^n| \leq (n+1)^{d-1}, \quad (20)$$

the relation

$$d_{n,d} \leq (n+1)^{(d+2)(d-1)/2} \quad (21)$$

holds.

The reason of our choices of the POVM $M_{\lambda,j}$ and the estimate $x_{\lambda,j}$ is the following. The reference [34] essentially showed the relation

$$\begin{aligned} D(\rho^{\otimes n} \| \sigma^{\otimes n}) - \frac{d(d-1)}{2} \log(n+1) \\ \leq D_M(\rho^{\otimes n} \| \sigma^{\otimes n}) \leq D(\rho^{\otimes n} \| \sigma^{\otimes n}), \end{aligned} \quad (22)$$

where

$$\begin{aligned} D_M(\rho^{\otimes n} \| \sigma^{\otimes n}) \\ := \sum_{\lambda,j} \text{Tr} M_{\lambda,j} \rho^{\otimes n} (\log \text{Tr} M_{\lambda,j} \rho^{\otimes n} - \log \text{Tr} M_{\lambda,j} \sigma^{\otimes n}). \end{aligned}$$

This relation shows that the POVM $M_{\lambda,j}$ almost preserves the information with respect to the relative entropy $D(\rho^{\otimes n} \| \sigma^{\otimes n})$. Further, since the Shannon entropy $H(P_{\rho,\sigma}^{(n)}(\lambda, j)) := -\sum_{\lambda,j} \text{Tr} M_{\lambda,j} \rho^{\otimes n} \log \text{Tr} M_{\lambda,j} \rho^{\otimes n}$ satisfies

$$0 \leq H(P_{\rho,\sigma}^{(n)}(\lambda, j)) \leq \log d_{n,d}, \quad (23)$$

the the combination of (21) and (22) implies

$$\begin{aligned} D(\rho^{\otimes n} \| \sigma^{\otimes n}) - (d+1)(d-1) \log(n+1) \\ \leq - \sum_{\lambda,j} \text{Tr} M_{\lambda,j} \rho^{\otimes n} \log \text{Tr} M_{\lambda,j} \sigma^{\otimes n} \\ \leq D(\rho^{\otimes n} \| \sigma^{\otimes n}). \end{aligned} \quad (24)$$

That is, the average of $-\frac{1}{n} \log \text{Tr} M_{\lambda,j} \sigma^{\otimes n}$ is close to the value $D(\rho \| \sigma)$ to be estimated. This is the reason why we choose the estimate $x_{\lambda,j}$.

The mean square error of this estimator is evaluated as follows.

Theorem 2. *For any states ρ and σ , we have*

$$\begin{aligned} \text{MSE}_n(\rho \| \sigma) &:= \sum_{(\lambda,j)} P_{\rho,\sigma}^{(n)}(\lambda, j) (x_{\lambda,j} - D(\rho \| \sigma))^2 \\ &\leq \left(\frac{1}{\sqrt{n}} \sqrt{V(\rho \| \sigma)} + \frac{1}{n} \log d_{n,d} \right)^2. \end{aligned} \quad (25)$$

This theorem is proved in Appendix A. The difference between the upper bound (25) and the leading term $\frac{1}{n} V(\rho \| \sigma)$ is $\frac{1}{n^2} (\log d_{n,d})^2 +$

$\frac{2}{n\sqrt{n}} \sqrt{V(\rho \| \sigma)} \log d_{n,d}$. Using (21), this different is upper bounded by $\frac{1}{n^2} \left(\frac{(d+2)(d-1)}{2} \log(n+1) \right)^2 + \frac{2}{n\sqrt{n}} \sqrt{V(\rho \| \sigma)} \frac{(d+2)(d-1)}{2} \log(n+1)$. n times of these terms go to zero.

Next, we focus on the tail probability for our estimator, i.e., we study the estimation error probability as

$$\delta_{\rho,\sigma}^{(n),+, \epsilon} := P_{\rho,\sigma}^{(n)} \{ (\lambda, j) : x_{\lambda,j} - D(\rho \| \sigma) > \epsilon \} \quad (26)$$

$$\delta_{\rho,\sigma}^{(n),-, \epsilon} := P_{\rho,\sigma}^{(n)} \{ (\lambda, j) : x_{\lambda,j} - D(\rho \| \sigma) < -\epsilon \}. \quad (27)$$

When ϵ behaves as $c/\sqrt{n}$, as shown in Appendix B the probabilities $\delta_{\rho,\sigma}^{(n), \pm, c/\sqrt{n}}$ converges to a normal distribution as follows.

Theorem 3. *For any states ρ and σ , we have*

$$\delta_{\rho,\sigma}^{(n),+, c/\sqrt{n}} \rightarrow \int_{c/\sqrt{V(\rho \| \sigma)}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx \quad (28)$$

$$\delta_{\rho,\sigma}^{(n),-, c/\sqrt{n}} \rightarrow \int_{-\infty}^{c/\sqrt{V(\rho \| \sigma)}} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx. \quad (29)$$

This property is called local asymptotic normality.

When the error term ϵ is constant, the tail probability goes to zero exponentially. We use the sandwich relative entropy $D_{\alpha}(\sigma \| \rho) := \frac{1}{\alpha-1} \log \text{Tr}(\rho^{\frac{1-\alpha}{2\alpha}} \sigma \rho^{\frac{1-\alpha}{2\alpha}})^{\alpha}$. As shown in Appendix C, using the method in Section X of [35], we have the following theorem.

Theorem 4. *For any states ρ , σ , and $R, r > 0$, we have*

$$\delta_{\rho,\sigma}^{(n),+, R-D(\rho \| \sigma)} \leq (d_{n,d})^{\alpha} e^{-n\alpha(D_{1-\alpha}(\rho \| \sigma) - R)}, \quad (30)$$

$$\begin{aligned} \delta_{\rho,\sigma}^{(n),-, R-D(\rho \| \sigma)} &\leq e^{-n(R-r-\alpha(D_{1+\alpha}(\rho \| \sigma)))} \\ &\quad + d_{n,d} e^{-nr}. \end{aligned} \quad (31)$$

In (30), $\alpha \in (0, 1)$, and in (31), $\alpha > 0$.

Theorem 4 guarantees that $\delta_{\rho,\sigma}^{(n),+, \epsilon}$ and $\delta_{\rho,\sigma}^{(n),-, \epsilon}$ go to zero exponentially. This property is called the large deviation.

4 Analysis with increasing d

Similar to [6, 7], we consider the case when the dimension d increases. When $n = O(d^{4+\delta})$, $\frac{1}{\sqrt{n}} \log d_{n,d} \leq \frac{1}{\sqrt{n}} \frac{(d+1)(d-1)}{2} \log(n+1) \rightarrow 0$. In

this case, due to Theorem 2, the Cramér-Rao type bound can be attained because the second term of RHS in (25) goes to zero.

We now discuss the behavior of n with respect to d that allows the error to converge to zero as $d \rightarrow \infty$, rather than assuming $n = O(d^{4+\delta})$. We denote the d -dimensional system by $\mathcal{H}_d$. To discuss this case, we consider the sequence of states σ_d depending on the dimension d . We also choose a subset $\mathcal{S}_d$ of the set $\mathcal{S}(\mathcal{H}_d)$ of states on $\mathcal{H}_d$. We assume the following condition for σ_d and $\mathcal{S}_d$:

$$c_0 := \lim_{d \rightarrow \infty} \frac{1}{d^2} \max_{\rho \in \mathcal{S}_d} V(\rho \| \sigma_d) < \infty. \quad (32)$$

For example, when σ_d is fixed to the completely mixed state ρ_{mix} , $V(\rho \| \rho_{\text{mix}})$ equals the varentropy $\text{Tr} \rho (\log \rho)^2 - (\text{Tr} \rho \log \rho)^2$. Since Lemma 8 of [3] showed that $\text{Tr} \rho (\log \rho)^2 \leq (\log d)^2$, the condition (32) holds even with $\mathcal{S}_d = \mathcal{S}(\mathcal{H}_d)$ so that the term $\frac{1}{n} \log d_{n,d}$ is the major term in the RHS of (25). Further, the condition (32) holds with $\mathcal{S}_d = \mathcal{S}(\mathcal{H}_d)$ under certain conditions for σ_d .

Lemma 5. *When the minimum eigenvalue of σ_d is lower bounded by e^{-td} with a fixed real number $t > 0$, the condition (32) holds even when $\mathcal{S}_d$ equals $\mathcal{S}(\mathcal{H}_d)$.*

Proof. Considering the definition of $V(\rho \| \sigma_d)$ and the norm $\| \cdot \|_\rho$, we have

$$\begin{aligned} & \sqrt{V(\rho \| \sigma_d)} \\ &= \| \log \rho - (\text{Tr} \rho \log \rho) - \log \sigma_d + (\text{Tr} \rho \log \sigma_d) \|_\rho \\ &\leq \| \log \rho - (\text{Tr} \rho \log \rho) \|_\rho \\ &\quad + \| \log \sigma_d - (\text{Tr} \rho \log \sigma_d) \|_\rho. \end{aligned} \quad (33)$$

Using the property of the norm $\| \cdot \|_\rho$, we have

$$\begin{aligned} & \| \log \rho - (\text{Tr} \rho \log \rho) \|_\rho^2 \\ &= \text{Tr} \rho (\log \rho - (\text{Tr} \rho \log \rho))^2 \\ &= (\text{Tr} \rho (\log \rho)^2) - (\text{Tr} \rho \log \rho)^2 \\ &\leq (\text{Tr} \rho (\log \rho)^2) \stackrel{(a)}{\leq} (\log d)^2, \end{aligned} \quad (34)$$

where (a) follows from [3, Lemma 8]. Similarly, we have

$$\begin{aligned} & \| \log \sigma_d - (\text{Tr} \rho \log \sigma_d) \|_\rho^2 \\ &= \text{Tr} \rho (\log \sigma_d - (\text{Tr} \rho \log \sigma_d))^2 \\ &= (\text{Tr} \rho (\log \sigma_d)^2) - (\text{Tr} \rho \log \sigma_d)^2 \\ &\leq (\text{Tr} \rho (\log \sigma_d)^2) \leq (td)^2. \end{aligned} \quad (35)$$

Combining (33), (34), and (35), we obtain the condition (32). $\square$

The sample complexity is characterized as the following theorem.

Theorem 6. *When the condition (32) holds and $n = cd^2$, we have*

$$\begin{aligned} & \lim_{d \rightarrow \infty} \max_{\rho \in \mathcal{S}_d} \delta_{\rho, \sigma}^{(n), +, \epsilon} + \delta_{\rho, \sigma}^{(n), -, \epsilon} \\ &\leq \frac{1}{\epsilon^2} \left(\frac{\sqrt{c_0}}{\sqrt{c}} + \min_{0 < s < 1} \frac{c^{s-1}}{s(1-s)} \right)^2 \\ &\leq \frac{(\sqrt{c_0} + 4)^2}{c\epsilon^2}. \end{aligned} \quad (36)$$

When we choose c to be $\frac{(\sqrt{c_0} + 4)^2}{\epsilon' \epsilon^2}$ for any $\epsilon, \epsilon' > 0$, i.e., $n = \frac{(\sqrt{c_0} + 4)^2}{\epsilon' \epsilon^2} d^2$, we have

$$\lim_{d \rightarrow \infty} \max_{\rho \in \mathcal{S}_d} \delta_{\rho, \sigma}^{(n), +, \epsilon} + \delta_{\rho, \sigma}^{(n), -, \epsilon} \leq \epsilon'. \quad (37)$$

Hence, when the condition (37) is imposed for the estimation error, we obtain an upper bound $O(d^2)$ of the sample complexity for the estimation of $D(\rho \| \sigma_d)$ when ρ belongs to $\mathcal{S}_d$.

Now, we compare the sample complexity of our method with the sample complexity of the simple application of full tomography [33, 39]. In particular, we employ the error analysis on the trace norm [33] rather than other error criteria because the trace norm is most useful to evaluate the error of the relative entropy. Their method achieves the estimation error

$$\| \hat{\rho} - \rho \|_1 \leq \epsilon \quad (38)$$

with high probability by sample complexity $O(d^2/\epsilon^2)$, where $\hat{\rho}$ is the estimated density and ρ is the true density. When the known density σ_d is the completely mixed state, our problem is reduced to the estimation of von Neumann entropy $S(\rho)$. Fannes inequality implies the relation

$$|S(\hat{\rho}) - S(\rho)| \leq \| \hat{\rho} - \rho \|_1 \log d. \quad (39)$$

That is, to achieve the condition

$$|S(\hat{\rho}) - S(\rho)| \leq \epsilon', \quad (40)$$

we need the sample complexity $O(d^2(\log d)^2/\epsilon'^2)$. Although our method and the method by [6] improves the sample complexity over the above method, the degree of the improvement is incremental in this case.

When the known state σ_d is a general state to satisfy the condition of Lemma 5, i.e., the minimum eigenvalue of σ_d is lower bounded by e^{-td}

with a fixed real number $t > 0$, the part $\log \sigma_d$ has the operator norm td at most. Hence, we have

$$\begin{aligned} & |D(\hat{\rho} \parallel \sigma_d) - D(\rho \parallel \sigma_d)| \\ & \leq |S(\hat{\rho}) - S(\rho)| + |\text{Tr}(\hat{\rho} - \rho) \log \sigma_d| \\ & \leq \|\hat{\rho} - \rho\|_1 \log d + \|\hat{\rho} - \rho\|_1 \log \sigma_d \\ & \leq \|\hat{\rho} - \rho\|_1 (\log d + td). \end{aligned} \quad (41)$$

That is, to achieve the condition

$$|D(\hat{\rho} \parallel \sigma_d) - D(\rho \parallel \sigma_d)| \leq \epsilon', \quad (42)$$

we need the sample complexity $O(d^2(\log d + td)^2/\epsilon'^2) = O(d^4/\epsilon'^2)$. Our method greatly improves the sample complexity over the simple application of full tomography [33]. That is, our extension to the estimation of the relative entropy realizes significant improvement in the sample complexity over the above method.

In fact, the paper [39] also considers the sample complexity when Bures χ^2 -divergence and Bures distance are adopted. However, the evaluation of the error under these criteria does not fit well with the above method. Moreover, it is challenging to find a good upper bound of the estimation errors of $S(\hat{\rho}) - S(\rho)$ and $D(\hat{\rho} \parallel \sigma) - D(\rho \parallel \sigma)$ by using the estimation error based on these criteria.

Proof of Theorem 6. We choose $s \in (0, 1)$. Using Weyl's dimension formula [38, Theorem 7.1.7], we have

$$\begin{aligned} \log \dim \mathcal{U}_\lambda &= \log \prod_{1 \leq i < j \leq d} \frac{j - i + \lambda_j - \lambda_i}{j - i} \\ &= \sum_{1 \leq i < j \leq d} \log \left(1 + \frac{\lambda_j - \lambda_i}{j - i} \right) \\ &= \sum_{l=1}^d \sum_{i=1}^{d-l} \log \left(1 + \frac{\lambda_{l+i} - \lambda_i}{l} \right) \\ &= \sum_{l=1}^d (d-l) \sum_{i=1}^{d-l} \frac{1}{d-l} \log \left(1 + \frac{\lambda_{l+i} - \lambda_i}{l} \right) \\ &\stackrel{(a)}{\leq} \sum_{l=1}^d (d-l) \log \left(1 + \sum_{i=1}^{d-l} \frac{1}{d-l} \frac{\lambda_{l+i} - \lambda_i}{l} \right) \\ &\leq \sum_{l=1}^d (d-l) \log \left(1 + \frac{n}{(d-l)l} \right) \\ &\stackrel{(b)}{\leq} \sum_{l=1}^d \frac{(d-l)}{s} \left(\frac{n}{(d-l)l} \right)^s = \sum_{l=1}^d \frac{(d-l)^{1-s} n^s}{sl^s}, \end{aligned} \quad (43)$$

where (a) follows from Jensen inequality for the concave function $x \mapsto \log(1+x)$ and the uniform distribution over $\{1, \dots, d-l\}$. (b) can be shown as follows.

$$\begin{aligned} \log \left(1 + \frac{n}{(d-l)l} \right) &= \frac{1}{s} \log \left(1 + \frac{n}{(d-l)l} \right)^s \\ &\stackrel{(c)}{\leq} \frac{1}{s} \log \left(1 + \left(\frac{n}{(d-l)l} \right)^s \right) \stackrel{(d)}{\leq} \frac{1}{s} \left(\frac{n}{(d-l)l} \right)^s, \end{aligned} \quad (44)$$

where (c) follows from the inequality $(x+y)^s \leq x^s + y^s$ for $x, y \geq 0$, and (d) follows from the inequality $\log(1+x) \leq x$. Thus, we have

$$\begin{aligned} \log d_{n,d} &\leq \log |Y_d^n| \max_{\lambda} \dim \mathcal{U}_\lambda \\ &\leq \log |Y_d^n| + \sum_{l=1}^d \frac{(d-l)^{1-s} n^s}{sl^s} \\ &\leq (d-1) \log(n+1) + \sum_{l=1}^d \frac{(d-l)^{1-s} n^s}{sl^s}. \end{aligned} \quad (45)$$

When $n = cd^2$, we have

$$\begin{aligned} \frac{1}{d^2} \log \dim \mathcal{U}_\lambda &\leq \frac{1}{d^2} \sum_{l=1}^d \frac{(d-l)^{1-s} c^s d^{2s}}{sl^s} \\ &\rightarrow \int_0^1 \frac{(1-x)^{1-s} c^s}{sx^s} dx \\ &\leq \int_0^1 \frac{c^s}{sx^s} dx = \left[\frac{c^s}{s(1-s)} x^{1-s} \right]_0^1 = \frac{c^s}{s(1-s)}. \end{aligned} \quad (46)$$

Since the term $\frac{1}{n}(d-1) \log(n+1)$ goes to zero, the term $\frac{1}{n} \log d_{n,d}$ is evaluated as

$$\lim_{d \rightarrow \infty} \frac{1}{n} \log d_{n,d} \leq \min_{0 < s < 1} \frac{c^{s-1}}{s(1-s)}. \quad (47)$$

The definition of c_0 implies

$$\lim_{d \rightarrow \infty} \frac{1}{\sqrt{n}} \max_{\rho \in \mathcal{S}_d} \sqrt{V(\rho \parallel \sigma_d)} = \frac{\sqrt{c_0}}{\sqrt{c}}. \quad (48)$$

Thus, we have

$$\begin{aligned} &\lim_{d \rightarrow \infty} \max_{\rho \in \mathcal{S}_d} \text{MSE}_n(\rho \parallel \sigma_d) \\ &\stackrel{(e)}{\leq} \left(\frac{\sqrt{c_0}}{\sqrt{c}} + \min_{0 < s < 1} \frac{c^{s-1}}{s(1-s)} \right)^2 \stackrel{(f)}{\leq} \frac{(\sqrt{c_0} + 4)^2}{c}, \end{aligned} \quad (49)$$

where (e) follows from the combination of (47), (48), and Theorem 2, (f) follows by choosing $s = 1/2$. Finally, applying Chebyshev's inequality, we obtain the desired inequalities. $\square$

The key point of this proof is the derivation (43). In particular, the derivation (44) is the heart in this part. The idea of this derivation comes from the proof of (12) given in Appendix IV of the paper [40], which gives the security analysis in information-theoretic security.

5 Analysis on time complexity

To implement our estimator, we need to apply suitable unitary gates before the measurement based on the computation basis. For simplicity, we consider the case when σ is a diagonal matrix. For a general density σ , we need to apply a unitary diagonalizing the density σ to each system $\mathcal{H}$ before the following procedure.

The references [32, 41, 42, 43] proposed quantum algorithms for the Schur transform U_{Schur} . We evaluate its precision as follows. Given a required error $\epsilon > 0$ and a target unitary V , we say that a unitary U is an ϵ -approximate of V when any pure state $|\psi\rangle$ satisfies

$$\|(U - V)|\psi\rangle\| \leq \epsilon. \quad (50)$$

When the constructed unitary is an ϵ -approximate of the Schur transform U_{Schur} , the time complexity of the construction [42] is $O(nd^4 \text{polylog}(n, d, 1/\epsilon))$. Since these constructions realize the approximation (50), the estimation error probability increases at most only ϵ^2 . We denote the distribution of (λ, j) when we employ an ϵ -approximate of the Schur transform U_{Schur} by $P_{\rho, \sigma}^{(n), \epsilon}$.

In the classical part of our estimator, we need to calculate $x_{\lambda, j} = -\frac{1}{n} \log \text{Tr} M_{\lambda, j} \sigma^{\otimes n}$. When σ has diagonal elements $s_1, \dots, s_d$, the eigenvalue of $\sigma^{\otimes n}$ on the projection $M_{\lambda, j}$ has the form $\prod_{j=1}^d s_j^{n_j}$, where $\sum_{j=1}^d n_j = n$. Then, we have

$$\text{Tr} M_{\lambda, j} \sigma^{\otimes n} = \dim \mathcal{V}_{\lambda} \prod_{j=1}^d s_j^{n_j}. \quad (51)$$

For a Young index λ , the dimension $\mathcal{V}_{\lambda}$ is evaluated as

$$\dim \mathcal{V}_{\lambda} = \frac{n!}{\lambda!} e(\lambda) \quad (52)$$

$$e(\lambda) := \prod_{j>i} \frac{\lambda_j - \lambda_i - i + j}{\lambda_j + j - i} < 1, \quad (53)$$

where $\lambda! := \lambda_1! \lambda_2! \dots \lambda_d!$. For its detail, see [37, Eq. (2.72)]. Using [19, Theorem 2.5], we have

$$e^{nH(\frac{\lambda}{n})} (n+1)^{-(d-1)} \leq \frac{n!}{\lambda!} \leq e^{nH(\frac{\lambda}{n})}. \quad (54)$$

The value $e(\lambda)$ is evaluated as

$$\begin{aligned} -\log e(\lambda) &= \sum_{j>i} \log \frac{\lambda_j + j - i}{\lambda_j - \lambda_i - i + j} \\ &= \sum_{j>i} \log \left(1 + \frac{\lambda_i}{\lambda_j - \lambda_i + j - i} \right) \\ &\leq \sum_{j>i} \log \left(1 + \frac{\lambda_i}{j - i} \right) \\ &= \sum_{l=1}^d (d-l) \sum_{i=1}^{d-l} \frac{1}{d-l} \log \left(1 + \frac{\lambda_i}{l} \right) \\ &\stackrel{(a)}{\leq} \sum_{l=1}^d (d-l) \log \left(1 + \sum_{i=1}^{d-l} \frac{1}{d-l} \frac{\lambda_i}{l} \right) \\ &\leq \sum_{l=1}^d (d-l) \log \left(1 + \frac{n}{(d-l)l} \right) \\ &\stackrel{(b)}{\leq} \sum_{l=1}^d \frac{(d-l)^{1-s} n^s}{s l^s}, \end{aligned} \quad (55)$$

where (a) follows from Jensen inequality for the concave function $x \mapsto \log(1+x)$, and (b) follows from (44) in the same way as (43).

Instead of $x_{\lambda, j}$, we use its approximation $x_{\lambda, j}^* := H(\frac{\lambda}{n}) - \sum_{j=1}^d \frac{n_j}{n} \log s_j$, whose time complexity is $O(n)$. Then, we have

$$\begin{aligned} 0 &\leq x_{\lambda, j}^* - x_{\lambda, j} \leq \frac{1}{n} (d \log(n+1) - \log e(\lambda)) \\ &\leq \frac{1}{n} \left(d \log(n+1) - \sum_{l=1}^d \frac{(d-l)^{1-s} n^s}{s l^s} \right). \end{aligned} \quad (56)$$

When $n = cd^2$, $\lim_{n \rightarrow \infty} \frac{1}{n} (d \log(n+1) - \sum_{l=1}^d \frac{(d-l)^{1-s} n^s}{s l^s}) \leq \frac{4}{\sqrt{c}}$.

Given an arbitrary number $\epsilon > 0$, we choose $c = \frac{16}{\epsilon^2}$. When $n = cd^2$, the limit of the upper bound in (56) can be bounded by ϵ . Then, we define

$$\delta_{\rho, \sigma}^{(n), +, \epsilon, \epsilon_1} := P_{\rho, \sigma}^{(n), \epsilon_1} \{(\lambda, j) : x_{\lambda, j}^* - D(\rho \| \sigma) > \epsilon\} \quad (57)$$

$$\delta_{\rho, \sigma}^{(n), -, \epsilon, \epsilon_1} := P_{\rho, \sigma}^{(n), \epsilon_1} \{(\lambda, j) : x_{\lambda, j}^* - D(\rho \| \sigma) < -\epsilon\}. \quad (58)$$

Thus, when $n = cd^2$, using (37), we have

$$\begin{aligned} & \lim_{d \rightarrow \infty} \max_{\rho \in \mathcal{S}_d} \delta_{\rho, \sigma}^{(n), +, \epsilon, \epsilon_1} + \delta_{\rho, \sigma}^{(n), -, \epsilon, \epsilon_1} \\ & \leq \frac{(\sqrt{c_0} + 4)^2}{c(\epsilon - \frac{4}{\sqrt{c}})^2} + \epsilon_1^2. \end{aligned} \quad (59)$$

Hence, when we choose $\epsilon_1 = \sqrt{\epsilon'/2}$ and $c = \min(\frac{64}{\epsilon^2}, \frac{8(4+\sqrt{c_0})^2}{\epsilon^2 \epsilon'})$ for any $\epsilon, \epsilon' > 0$, we have

$$\lim_{d \rightarrow \infty} \max_{\rho \in \mathcal{S}_d} \delta_{\rho, \sigma}^{(n), +, \epsilon, \epsilon_1} + \delta_{\rho, \sigma}^{(n), -, \epsilon, \epsilon_1} \leq \epsilon'. \quad (60)$$

Overall, when $n = O(d^2)$, we use the construction of Schur transform U_{Schur} by [42] with the time complexity $O(d^6 \text{polylog}(d, 1/\epsilon))$ and the estimate $x_{\lambda, j}$ with the time complexity $O(n) = O(d^2)$. That is, the total construction has a total time complexity $O(d^6 \text{polylog}(d))$ to realize the condition (60) with a fixed value $\epsilon > 0$.

Remark 7. Initially, the paper [32] gives a polynomial algorithm for Schur transform U_{Schur} . However, it did not give a precise evaluation of its time complexity. Although the paper [42] writes that the protocol by the paper [32] has time complexity $O(nd^3 \text{polylog}(n, d, 1/\epsilon))$ in its Table 1, the paper [42] does not give the derivation of this evaluation because its main focus is the implementation of the mixed Schur transform $U_{\text{MixedSchur}}$, which realizes a basis change to block-diagonalize $U^{\otimes n} \otimes \bar{U}^{\otimes m}$ for an arbitrary unitary U . In fact, the paper [42] proved that its time complexity is $O((n+m)d^4 \text{polylog}(n, m, d, 1/\epsilon))$, and the recent paper [43] also proposed the same algorithm as the algorithm by [42]. In this paper, to make a safer statement, we employ the statement that the time complexity of the unitary $U_{\text{MixedSchur}}$ is $O((n+m)d^4 \text{polylog}(n, m, d, 1/\epsilon))$. Its special case with $m = 0$ corresponds to U_{Schur} and covers our case with the time complexity $O(nd^4 \text{polylog}(n, d, 1/\epsilon))$.

Remark 8. The paper [7] also mentions that there exists an algorithm for Schur transform U_{Schur} whose time complexity is $O(d^6 \text{polylog}(d, 1/\epsilon))$ when $n = O(d^2)$ [44]. First, they employ the algorithm for weak Schur sampling given in [45, Section 4.2.2]. Although this method employs the quantum Fourier transform the permutation group $\mathfrak{S}_n$, they proposed to use the algorithm by [46] for this

part. The obtained algorithm has time complexity $O(n^3 \text{polylog}(n, d, 1/\epsilon))$. When $n = d^2$, it equals $O(d^6 \text{polylog}(d, 1/\epsilon))$. This implementation of weak Schur sampling was mentioned earlier in [47, Section 1.1.2].

Remark 9. Recently, the paper [48] studied the estimation of relative entropy with two unknown densities ρ and σ when an estimator of the state is given and the estimator converges to the true density. The analysis [48] is different from ours in the following points. (i) We assume that σ is known, but the paper [48] assumes that it is unknown. (ii) We discuss the optimality of our estimator in various settings. Under the case with fixed d , we optimize the MSE. When d increases, we discuss the sample complexity. But, when an estimator of the state is given, the paper [48] discusses the behavior of the estimator of relative entropy by using the behavior of the estimator. In addition, the paper [48] mentioned that the limiting distribution of the normalized estimator is the normal distribution. When d is fixed, the discussion explains how this problem is reduced to a special case of the parameter estimation with nuisance parameters. The paper [21] also showed that the limiting distribution of the normalized estimator is the normal distribution in the parameter estimation with nuisance parameters.

6 Discussion

We have studied the estimation of quantum relative entropy $D(\rho \parallel \sigma)$ when the second argument σ is known. Our estimator has a good performance in the following two senses. First, when the dimension d is fixed, our estimator attains Cramér-Rao type bound asymptotically. Second, when the dimension d increases, our estimator has sample complexity $O(d^2)$ under natural assumptions, which greatly improves the sample complexity by the simple application of full tomography [33]. Third, when d is large, although the calculation of our estimator is difficult, we have an alternative estimator whose time complexity is $O(d^6 \text{polylog}(d))$. The difference between this alternative estimator and our original estimator approaches zero asymptotically. In the above way, our estimator works well unifiedly, which is a unique feature and did not appear in existing studies [6, 7, 22].

Since our estimator assumes the knowledge of the form of the second argument σ , it is needed to develop an estimator that works without this knowledge. In this case, we need to prepare n copies of the unknown state σ as well. To attain the Cramér-Rao type bound with fixed d , it is sufficient to estimate the form of the density matrix σ . However, such a method has a large time complexity when d increases. It is an interesting open problem to derive an efficient estimator of the quantum relative entropy in the above setting.

Acknowledgement

The author is supported in part by the National Natural Science Foundation of China (Grant No. 62171212) and the General R&D Projects of 1+1+1 CUHK-CUHK(SZ)-GDST Joint Collaboration Fund (Grant No. GRDP2025-022). The author is grateful for Professor Kun Fang to a helpful discussion. Also, the author would like to thank Mr Dmitry Grinko and Dr. Qisheng Wang for helpful discussions on the time complexity of Schur transform. In addition, the author would like to thank Prof. Jun Suzuki and Dr. Francesco Albarelli for helpful discussions on the Cramér-Rao type bound. Also, the author would like to thank Prof. Macro Tomamichel and Dr. Hu Yanglin for helpful discussions for the relation with full tomography and informing the references [33, 39].

A Evaluation of mean square error: Proof of Theorem 2

We define the state $\rho_n := \sum_{\lambda} \rho_{\lambda}$ on the system $\oplus_{\lambda \in Y_d^n} \mathcal{U}_{\lambda}$. We choose an orthogonal basis $\{|v_{\lambda,j'}\}_{j'}$ of $\mathcal{V}_{\lambda}$.

We use the methods [3, 26, 49]. Then, we have the following calculation.

$$\begin{aligned} x_{\lambda,j} - D(\rho\|\sigma) &= -\frac{1}{n} \log \text{Tr} M_{\lambda,j} \sigma^{\otimes n} - D(\rho\|\sigma) \\ &= -\frac{1}{n} (\log \langle u_{\lambda,j}, v_{\lambda,j'} | \sigma^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle + \log d'_{\lambda}) \\ &\quad - D(\rho\|\sigma) \end{aligned}$$

$$\begin{aligned} &= -\frac{1}{n} (\log \langle u_{\lambda,j}, v_{\lambda,j'} | \sigma^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle \\ &\quad - \log \langle u_{\lambda,j}, v_{\lambda,j'} | \rho^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle) - D(\rho\|\sigma) \\ &\quad - \frac{1}{n} (\log d'_{\lambda} + \log \langle u_{\lambda,j}, v_{\lambda,j'} | \rho^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle) \\ &= \frac{1}{n} (-\log \langle u_{\lambda,j}, v_{\lambda,j'} | \sigma^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle \\ &\quad + \log \langle u_{\lambda,j}, v_{\lambda,j'} | \rho^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle) - D(\rho\|\sigma) \\ &\quad - \frac{1}{n} \log \langle u_{\lambda,j} | \rho_{\lambda} | u_{\lambda,j} \rangle. \end{aligned} \tag{61}$$

Therefore, we have

$$\begin{aligned} &\sum_{(\lambda,j)} P_{\rho,\sigma}^{(n)}(\lambda,j) (x_{\lambda,j} - D(\rho\|\sigma))^2 \\ &= \sum_{(\lambda,j)} P_{\rho,\sigma}^{(n)}(\lambda,j) \left(\frac{1}{n} (-\log \langle u_{\lambda,j} | \sigma_{\lambda} | u_{\lambda,j} \rangle \right. \\ &\quad \left. - D(\rho\|\sigma)) \right)^2 \\ &= \sum_{(\lambda,j,j')} \langle u_{\lambda,j}, v_{\lambda,j'} | \rho^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle \\ &\quad \left(\frac{1}{n} (-\log \langle u_{\lambda,j}, v_{\lambda,j'} | \sigma_{\lambda} \otimes \rho_{\lambda,\text{mix}} | u_{\lambda,j}, v_{\lambda,j'} \rangle \right. \\ &\quad \left. + \log \langle v_{\lambda,j'} | \rho_{\lambda,\text{mix}} | v_{\lambda,j'} \rangle) - D(\rho\|\sigma) \right)^2 \\ &= \sum_{(\lambda,j,j')} \langle u_{\lambda,j}, v_{\lambda,j'} | \rho^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle \\ &\quad \left(\frac{1}{n} (-\log \langle u_{\lambda,j}, v_{\lambda,j'} | \sigma^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle \right. \\ &\quad \left. + \log \langle u_{\lambda,j}, v_{\lambda,j'} | \sum_{\lambda'} I_{\mathcal{U}_{\lambda}} \otimes \rho_{\lambda',\text{mix}} | u_{\lambda,j}, v_{\lambda,j'} \rangle) \right. \\ &\quad \left. - D(\rho\|\sigma) \right)^2 \\ &= \text{Tr} \rho^{\otimes n} \left(\frac{1}{n} (-\log \sigma^{\otimes n} + \sum_{\lambda} \log(I_{\mathcal{U}_{\lambda}} \otimes \rho_{\lambda,\text{mix}})) \right. \\ &\quad \left. - D(\rho\|\sigma) \right)^2 \\ &= \text{Tr} \rho^{\otimes n} \left(\frac{1}{n} (-\log \sigma^{\otimes n} + \sum_{\lambda} \log(\rho_{\lambda} \otimes \rho_{\lambda,\text{mix}})) \right. \\ &\quad \left. - D(\rho\|\sigma) - \sum_{\lambda} \log(\rho_{\lambda} \otimes I_{\mathcal{V}_{\lambda}}) \right)^2 \\ &= \text{Tr} \rho^{\otimes n} \left(\frac{1}{n} (-\log \sigma^{\otimes n} + \log \rho^{\otimes n}) - D(\rho\|\sigma) \right. \\ &\quad \left. - \frac{1}{n} \sum_{\lambda} \log(\rho_{\lambda} \otimes I_{\mathcal{V}_{\lambda}}) \right)^2 \end{aligned}$$

$$\begin{aligned}
&= \left\| \frac{1}{n} (-\log \sigma^{\otimes n} + \log \rho^{\otimes n}) - D(\rho \| \sigma) \right\|_{\rho^{\otimes n}} \\
&\quad - \frac{1}{n} \sum_{\lambda} \log(\rho_{\lambda} \otimes I_{\mathcal{V}_{\lambda}}) \Big\|_{\rho^{\otimes n}}^2 \\
&\leq \left(\left\| \frac{1}{n} (-\log \sigma^{\otimes n} + \log \rho^{\otimes n}) - D(\rho \| \sigma) \right\|_{\rho^{\otimes n}} \right. \\
&\quad \left. + \left\| \frac{1}{n} \sum_{\lambda} \log(\rho_{\lambda} \otimes I_{\mathcal{V}_{\lambda}}) \right\|_{\rho^{\otimes n}} \right)^2. \quad (62)
\end{aligned}$$

Also, we have

$$\begin{aligned}
&\left\| \frac{1}{n} (-\log \sigma^{\otimes n} + \log \rho^{\otimes n}) - D(\rho \| \sigma) \right\|_{\rho^{\otimes n}} \\
&= \text{Tr} \rho^{\otimes n} \left(\frac{1}{n} (-\log \sigma^{\otimes n} + \log \rho^{\otimes n}) - D(\rho \| \sigma) \right)^2 \\
&= \frac{1}{n} V(\rho \| \sigma), \quad (63)
\end{aligned}$$

and

$$\begin{aligned}
&\left\| -\frac{1}{n} \sum_{\lambda} \log(\rho_{\lambda} \otimes I_{\mathcal{V}_{\lambda}}) \right\|_{\rho^{\otimes n}}^2 \\
&= \text{Tr} \rho^{\otimes n} \left(\frac{1}{n} \sum_{\lambda} \log(\rho_{\lambda} \otimes I_{\mathcal{V}_{\lambda}}) \right)^2 \\
&= \frac{1}{n^2} \text{Tr} \rho_n (\log \rho_n)^2 \stackrel{(a)}{\leq} \frac{1}{n^2} (\log d_{n,d})^2, \quad (64)
\end{aligned}$$

where (a) follows from [3, Lemma 8]. The combination of (62), (63), and (64) implies (25).

B Local asymptotic normality: Proof of Theorem 3

The random variable $\sqrt{n}(-\frac{1}{n}(\log \langle u_{\lambda,j}, v_{\lambda,j'} | \sigma^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle + \log \langle u_{\lambda,j}, v_{\lambda,j'} | \rho^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle) - D(\rho \| \sigma))$ has additional variable j' . The joint distribution of (λ, j, j') is given as $\langle u_{\lambda,j}, v_{\lambda,j'} | \rho^{\otimes n} | u_{\lambda,j}, v_{\lambda,j'} \rangle$.

We define the pinching map $\Gamma_{\sigma,n}$ as

$$\begin{aligned}
&\Gamma_{\sigma,n}(\rho') \\
&:= \sum_{\lambda \in Y_d^n, j} (|u_{\lambda,j}\rangle \langle u_{\lambda,j}| \otimes P(\mathcal{V}_{\lambda})) \rho' \\
&\quad \cdot (|u_{\lambda,j}\rangle \langle u_{\lambda,j}| \otimes P(\mathcal{V}_{\lambda})) \quad (65)
\end{aligned}$$

for a general state ρ' on $\mathcal{H}^{\otimes n}$, where $P(\mathcal{V}_{\lambda})$ is the projection to $\mathcal{V}_{\lambda}$. Then, this random variable coincides with $\sqrt{n}(\frac{1}{n}(\log \Gamma_{\sigma,n}(\rho^{\otimes n}) - \log \sigma^{\otimes n}) - D(\rho \| \sigma))$ under the state $\Gamma_{\sigma,n}(\rho^{\otimes n})$ studied in Section V of [26]. The discussion in Section V

of [26] showed that it converges to Gaussian distribution with variance $V(\rho \| \sigma)$ in probability as $n \rightarrow \infty$.

In addition, in the same way as (64), using [3, Lemma 8], we have

$$\begin{aligned}
&\sum_{(\lambda,j)} P_{\rho,\sigma}^{(n)}(\lambda, j) \left(\frac{1}{\sqrt{n}} \log \langle u_{\lambda,j} | \rho_{\lambda} | u_{\lambda,j} \rangle \right)^2 \\
&= \sum_{(\lambda,j)} P_{\rho,\sigma}^{(n)}(\lambda, j) \left(\frac{1}{\sqrt{n}} \log P_{\rho,\sigma}^{(n)}(\lambda, j) \right)^2 \\
&= \frac{1}{n} \text{Tr} \rho_n (\log \rho_n)^2 \leq \frac{1}{n} (\log d_{n,d})^2 \\
&\leq \frac{1}{n} \left(\frac{(d+2)(d-1)}{2} \log(n+1) \right)^2 \rightarrow 0. \quad (66)
\end{aligned}$$

Thus, the random variable $\frac{1}{\sqrt{n}} \log \langle u_{\lambda,j} | \rho_{\lambda} | u_{\lambda,j} \rangle$ under the distribution $P_{\rho,\sigma}^{(n)}$ converges to zero in probability as $n \rightarrow \infty$. Therefore, the probabilities $\delta_{\rho,\sigma}^{(n), \pm, c/\sqrt{n}}$ can be asymptotically characterized by Gaussian distribution with variance $V(\rho \| \sigma)$.

C Large deviation evaluation

C.1 Preparation

Since the system $\mathcal{V}_{\lambda}$ has no information, it is sufficient to handle the two states $\oplus_{\lambda \in Y_d^n} \rho_{\lambda}$ and $\oplus_{\lambda \in Y_d^n} \sigma_{\lambda}$ over $\oplus_{\lambda \in Y_d^n} \mathcal{U}_{\lambda}$. We define the map

$$\begin{aligned}
\kappa_{\sigma,n}(\rho') &:= \sum_{\lambda \in Y_d^n, j} \text{Tr}_{\mathcal{V}_{\lambda}} (|u_{\lambda,j}\rangle \langle u_{\lambda,j}| \otimes P(\mathcal{V}_{\lambda})) \rho' \\
&\quad \cdot (|u_{\lambda,j}\rangle \langle u_{\lambda,j}| \otimes P(\mathcal{V}_{\lambda})) \quad (67)
\end{aligned}$$

for a general state ρ' on $\mathcal{H}^{\otimes n}$. Due to the above-mentioned structure, the states $\Gamma_{\sigma,n}(\rho^{\otimes n})$ and $\sigma^{\otimes n}$ are commutative with each other.

We have the pinching inequality:

$$\rho' \leq d_{n,d} \Gamma_{\sigma,n}(\rho'). \quad (68)$$

In fact, applying the matrix monotone function to (68), for $\alpha \in (0, 1)$, we have

$$\begin{aligned}
&d_{n,d}^{\alpha-1} ((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \Gamma_{\sigma,n}(\rho^{\otimes n}) (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}})^{\alpha-1} \\
&= \left(d_{n,d} \Gamma_{\sigma,n} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right) \right)^{\alpha-1} \\
&\leq \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1}. \quad (69)
\end{aligned}$$

Thus, we have

$$\begin{aligned}
& \text{Tr} \left(\Gamma_{\sigma,n}(\rho^{\otimes n}) \right)^\alpha (\sigma^{\otimes n})^{1-\alpha} \\
&= \text{Tr} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \Gamma_{\sigma,n}(\rho^{\otimes n}) (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \\
&= \text{Tr} \left(\Gamma_{\sigma,n} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right) \right)^\alpha \\
&= \text{Tr} \left(\Gamma_{\sigma,n} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right) \right. \\
&\quad \cdot \left. \left(\Gamma_{\sigma,n} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right) \right)^{\alpha-1} \right) \\
&= \text{Tr} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right) \\
&\quad \cdot \left(\Gamma_{\sigma,n} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right) \right)^{\alpha-1} \\
&\stackrel{(a)}{\leq} d_{n,d}^{1-\alpha} \text{Tr} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right) \\
&\quad \cdot \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \\
&= d_{n,d}^{1-\alpha} \text{Tr} \left((\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \rho^{\otimes n} (\sigma^{\otimes n})^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \\
&= d_{n,d}^{1-\alpha} (\text{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha)^n, \tag{70}
\end{aligned}$$

where Step (a) follows from (69).

C.2 Proof of Theorem 4

Here, we define the projection $\{X > Y\}$ as the projection to the subspace spanned by the eigenvectors of $X - Y$ with positive eigenvalues. For $\alpha \in (0, 1)$, we have

$$\begin{aligned}
& \sum_{(\lambda,j): x_{\lambda,j} < R} \text{Tr} M_{\lambda,j} \rho^{\otimes n} \\
&= \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\sigma^{\otimes n}) > e^{-nR} \} \\
&\stackrel{(b)}{\leq} \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\sigma^{\otimes n}) > e^{-nR} \kappa_{\sigma,n}(\rho^{\otimes n}) \} \\
&\stackrel{(c)}{\leq} \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n})^{1-\alpha} \kappa_{\sigma,n}(\sigma^{\otimes n})^\alpha e^{n\alpha R} \\
&= \text{Tr} \Gamma_{\sigma,n}(\rho^{\otimes n})^{1-\alpha} (\sigma^{\otimes n})^\alpha e^{n\alpha R} \\
&\stackrel{(d)}{\leq} d_{n,d}^\alpha (\text{Tr}(\sigma^{\frac{\alpha}{2(1+\alpha)}} \rho \sigma^{\frac{\alpha}{2(1+\alpha)}})^{1-\alpha} e^{\alpha R})^n \\
&= d_{n,d}^\alpha e^{-n\alpha(D_{1+\alpha}(\rho\|\sigma) - R)}. \tag{71}
\end{aligned}$$

Here, (b) follows from $\kappa_{\sigma,n}(\rho^{\otimes n}) \leq I$, and (d) follows from (70). The relation (c) follows from

$$\begin{aligned}
& \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\sigma^{\otimes n}) > e^{-nR} \kappa_{\sigma,n}(\rho^{\otimes n}) \} \\
&= \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ e^{\alpha n R} (\kappa_{\sigma,n}(\sigma^{\otimes n}))^\alpha > (\kappa_{\sigma,n}(\rho^{\otimes n}))^\alpha \} \\
&\stackrel{(e)}{\leq} \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n})^{1-\alpha} (\kappa_{\sigma,n}(\sigma^{\otimes n}))^\alpha e^{n\alpha R} \\
&\quad \cdot \{ e^{\alpha n R} (\kappa_{\sigma,n}(\sigma^{\otimes n}))^\alpha > (\kappa_{\sigma,n}(\rho^{\otimes n}))^\alpha \} \\
&\leq \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n})^{1-\alpha} (\kappa_{\sigma,n}(\sigma^{\otimes n}))^\alpha e^{n\alpha R}, \tag{72}
\end{aligned}$$

where (e) follows from the following relation.

$$\begin{aligned}
& \text{Tr} \left[(\kappa_{\sigma,n}(\rho^{\otimes n}))^{1-\alpha} \right. \\
&\quad \cdot \left. \left((\kappa_{\sigma,n}(\rho^{\otimes n}))^\alpha - (\kappa_{\sigma,n}(\sigma^{\otimes n}))^\alpha e^{n\alpha R} \right) \right. \\
&\quad \cdot \left. \{ e^{\alpha n R} (\kappa_{\sigma,n}(\sigma^{\otimes n}))^\alpha > (\kappa_{\sigma,n}(\rho^{\otimes n}))^\alpha \} \right] \leq 0. \tag{73}
\end{aligned}$$

For $\alpha > 0$, we have

$$\begin{aligned}
& \sum_{(\lambda,j): x_{\lambda,j} > R} \text{Tr} M_{\lambda,j} \rho^{\otimes n} \\
&= \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\sigma^{\otimes n}) < e^{-nR} \} \\
&\leq \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\sigma^{\otimes n}) < e^{-nR} \} \{ \kappa_{\sigma,n}(\rho^{\otimes n}) > e^{-nr} \} \\
&\quad + \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\rho^{\otimes n}) \leq e^{-nr} \} \\
&\leq \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\sigma^{\otimes n}) < e^{-nR+nR} \kappa_{\sigma,n}(\rho^{\otimes n}) \} \\
&\quad + \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n}) \{ \kappa_{\sigma,n}(\rho^{\otimes n}) \leq e^{-nr} \} \\
&\leq \text{Tr} \kappa_{\sigma,n}(\rho^{\otimes n})^{1+\alpha} \kappa_{\sigma,n}(\sigma^{\otimes n})^{-\alpha} e^{-n\alpha(R-r)} + d_{n,d} e^{-nr} \\
&= \text{Tr} \Gamma_{\sigma,n}(\rho^{\otimes n})^{1+\alpha} (\sigma^{\otimes n})^{-\alpha} e^{-n\alpha(R-r)} + d_{n,d} e^{-nr} \\
&\stackrel{(f)}{\leq} \text{Tr} \left((\sigma^{\otimes n})^{-\frac{\alpha}{2(1+\alpha)}} \rho^{\otimes n} (\sigma^{\otimes n})^{-\frac{\alpha}{2(1+\alpha)}} \right)^{1+\alpha} e^{-\alpha(R-r)n} \\
&\quad + d_{n,d} e^{-nr} \\
&= (\text{Tr}(\sigma^{-\frac{\alpha}{2(1+\alpha)}} \rho \sigma^{-\frac{\alpha}{2(1+\alpha)}})^{1+\alpha} e^{-\alpha(R-r)n}) + d_{n,d} e^{-nr} \\
&= e^{-n(R-r-\alpha(D_{1+\alpha}(\rho\|\sigma) - R))} + d_{n,d} e^{-nr}. \tag{74}
\end{aligned}$$

where (f) follows from the monotonicity of sandwich Rényi relative entropy.

References

- [1] Fumio Hiai and Denez Petz. “The proper formula for relative entropy and its asymptotics in quantum probability”. *Communications in Mathematical Physics* **143**, 99–114 (1991).
- [2] T. Ogawa and H. Nagaoka. “Strong converse and stein’s lemma in quantum hypothesis

- testing”. *IEEE Transactions on Information Theory* **46**, 2428–2433 (2000).
- [3] Masahito Hayashi. “Optimal sequence of quantum measurements in the sense of stein’s lemma in quantum hypothesis testing”. *Journal of Physics A: Mathematical and General* **35**, 10759 (2002).
 - [4] Igor Bjelaković, Jean-Dominique Deuschel, Ruedi Seiler Tyll Krüger, Rainer Siegmund-Schultze, and Arleta Szkoła. “A quantum version of sanov’s theorem”. *Communications in Mathematical Physics* **260**, 659–671 (2005).
 - [5] J Nötzel. “Hypothesis testing on invariant subspaces of the symmetric group: part i. quantum sanov’s theorem and arbitrarily varying sources”. *Journal of Physics A: Mathematical and Theoretical* **47**, 235303 (2014).
 - [6] Jayadev Acharya, Ibrahim Issa, Nirmal V. Shende, and Aaron B. Wagner. “Estimating quantum entropy”. *IEEE Journal on Selected Areas in Information Theory* **1**, 454–468 (2020).
 - [7] Qisheng Wang and Zhicheng Zhang. “Time-efficient quantum entropy estimator via sampler”. In Timothy Chan, Johannes Fischer, John Iacono, and Grzegorz Herman, editors, *Proceedings of the 32nd Annual European Symposium on Algorithms. Volume 308 of Leibniz International Proceedings in Informatics*, pages 1–15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2024).
 - [8] M. Keyl and R. F. Werner. “Estimating the spectrum of a density operator”. *Phys. Rev. A* **64**, 052311 (2001).
 - [9] Matthias Christandl and Graeme Mitchison. “The spectra of quantum states and the kronecker coefficients of the symmetric group”. *Communications in Mathematical Physics* **261**, 789–797 (2006).
 - [10] Matthias Christandl, Aram W Harrow, and Graeme Mitchison. “Nonzero kronecker coefficients and what they tell us about spectra”. *Communications in Mathematical Physics* **270**, 575–585 (2007).
 - [11] Ryan O’Donnell and John Wright. “Quantum spectrum testing”. *Communications in Mathematical Physics* **387**, 1–75 (2021).
 - [12] Masahito Hayashi and Keiji Matsumoto. “Quantum universal variable-length source coding”. *Phys. Rev. A* **66**, 022311 (2002).
 - [13] Masahito Hayashi. “Exponents of quantum fixed-length pure-state source coding”. *Phys. Rev. A* **66**, 032321 (2002).
 - [14] Masahito Hayashi. “Group theoretical study of locc-detection of maximally entangled states using hypothesis testing”. *New Journal of Physics* **11**, 043028 (2009).
 - [15] Masahito Hayashi and Tomoyuki Morimae. “Verifiable measurement-only blind quantum computing with stabilizer testing”. *Phys. Rev. Lett.* **115**, 220502 (2015).
 - [16] Sam Pallister, Noah Linden, and Ashley Montanaro. “Optimal verification of entangled states with local measurements”. *Phys. Rev. Lett.* **120**, 170502 (2018).
 - [17] Huangjun Zhu and Masahito Hayashi. “Efficient verification of pure quantum states in the adversarial scenario”. *Phys. Rev. Lett.* **123**, 260504 (2019).
 - [18] Zihao Li, Huangjun Zhu, and Masahito Hayashi. “Robust and efficient verification of graph states in blind measurement-based quantum computation”. *npj Quantum Information* **9**, 115 (2023).
 - [19] M. Hayashi. “Quantum information theory: Mathematical foundation”. *Graduate Texts in Physics*. Springer Berlin, Heidelberg. New York, NY (2017). 2nd ed. edition.
 - [20] Yu Watanabe, Takahiro Sagawa, and Masahito Ueda. “Uncertainty relation revisited from quantum estimation theory”. *Phys. Rev. A* **84**, 042121 (2011).
 - [21] Yuxiang Yang, Giulio Chiribella, and Masahito Hayashi. “Communication cost of quantum processes”. *IEEE Journal on Selected Areas in Information Theory* **1**, 387–400 (2020).
 - [22] Jun Suzuki, Yuxiang Yang, and Masahito Hayashi. “Quantum state estimation with nuisance parameters”. *Journal of Physics A: Mathematical and Theoretical* **53**, 453001 (2020).
 - [23] Rafał Demkowicz-Dobrzański, Wojciech Górecki, and Mădălin Guță. “Multi-parameter estimation beyond quantum

- fisher information”. *Journal of Physics A: Mathematical and Theoretical* **53**, 363001 (2020).
- [24] Jonathan A Gross and Carlton M Caves. “One from many: estimating a function of many parameters”. *Journal of Physics A: Mathematical and Theoretical* **54**, 014001 (2020).
- [25] Mankei Tsang, Francesco Albarelli, and Animesh Datta. “Quantum semiparametric estimation”. *Phys. Rev. X* **10**, 031023 (2020).
- [26] Marco Tomamichel and Masahito Hayashi. “A hierarchy of information quantities for finite block length analysis of quantum tasks”. *IEEE Transactions on Information Theory* **59**, 7693–7710 (2013).
- [27] Ke Li. “Second-order asymptotics for quantum hypothesis testing”. *The Annals of Statistics* **42**, 171 – 189 (2014).
- [28] Hiroshi Nagaoka and Akio Fujiwara. “Autoparallelity of quantum statistical manifolds in the light of quantum estimation theory” (2023).
- [29] Masahito Hayashi. “Comparison between the cramer-rao and the mini-max approaches in quantum channel estimation”. *Communications in Mathematical Physics* **304**, 689–709 (2011).
- [30] Akio Fujiwara. “Strong consistency and asymptotic efficiency for adaptive quantum estimation problems”. *Journal of Physics A: Mathematical and General* **39**, 12489 (2006).
- [31] Marco A. Rodríguez-García, Isaac Pérez Castillo, and P. Barberis-Blostein. “Efficient qubit phase estimation using adaptive measurements”. *Quantum* **5**, 467 (2021).
- [32] Dave Bacon, Isaac L. Chuang, and Aram W. Harrow. “Efficient quantum circuits for schur and clebsch-gordan transforms”. *Phys. Rev. Lett.* **97**, 170502 (2006).
- [33] Jeongwan Haah, Aram W. Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. “Sample-optimal tomography of quantum states”. *IEEE Transactions on Information Theory* **63**, 5628–5641 (2017).
- [34] Masahito Hayashi. “Asymptotics of quantum relative entropy from a representation theoretical viewpoint”. *Journal of Physics A: Mathematical and General* **34**, 3413 (2001).
- [35] Masahito Hayashi and Yuki Ito. “Entanglement measures for detectability”. *IEEE Transactions on Information Theory* (2025).
- [36] Masahito Hayashi. “A group theoretic approach to quantum information”. *Springer*. (2017).
- [37] Masahito Hayashi. “Group representation for quantum theory”. *Springer*. (2017).
- [38] R. Goodman and N. R. Wallach. “A group theoretic approach to quantum information”. Cambridge University Press. (1999).
- [39] Steven T. Flammia and Ryan O’Donnell. “Quantum chi-squared tomography and mutual information testing”. *Quantum* **8**, 1381 (2024).
- [40] Masahito Hayashi. “Exponential decreasing rate of leaked information in universal random privacy amplification”. *IEEE Transactions on Information Theory* **57**, 3989–4001 (2011).
- [41] Hari Krovi. “An efficient high dimensional quantum Schur transform”. *Quantum* **3**, 122 (2019).
- [42] Q. T. Nguyen. “The mixed schur transform: efficient quantum circuit and applications” (2023).
- [43] Dmitry Grinko, Adam Burchardt, and Maris Ozols. “Gelfand-tsetlin basis for partially transposed permutations, with applications to quantum information” (2023).
- [44] Q. Wang. “private communication to m. hayashi”. Private communication (2024). Received on July 2024.
- [45] Ashley Montanaro and Ronald de Wolf. “A survey of quantum property testing”. *Pages 1–81*. Number 7 in Graduate Surveys. Theory of Computing Library. (2016).
- [46] Yasuhito Kawano and Hiroshi Sekigawa. “Quantum fourier transform over symmetric groups — improved result”. *Journal of Symbolic Computation* **75**, 219–243 (2016).

- [47] Qisheng Wang and Zhicheng Zhang. “Fast quantum algorithms for trace distance estimation”. [IEEE Transactions on Information Theory](#) **70**, 2720–2733 (2024).
- [48] Sreejith Sreekumar and Mario Berta. “Limit distribution theory for quantum divergences”. [IEEE Transactions on Information Theory](#) **71**, 459–484 (2025).
- [49] Masahito Hayashi and Marco Tomamichel. “Correlation detection and an operational interpretation of the Rényi mutual information”. [Journal of Mathematical Physics](#) **57**, 102201 (2016).