Minimax estimation of qubit states with Bures risk

Anirudh Acharya and Mădălin Guţă

School of Mathematical Sciences, University of Nottingham,
University Park, NG7 2RD Nottingham, UK

Abstract

The central problem of quantum statistics is to devise measurement schemes for the estimation of an unknown state, given an ensemble of n independent identically prepared systems. For locally quadratic loss functions, the risk of standard procedures has the usual scaling of $1/n$. However, it has been noticed that for fidelity based metrics such as the Bures distance, the risk of conventional (non-adaptive) qubit tomography schemes scales as $1/\sqrt{n}$ for states close to the boundary of the Bloch sphere. Several proposed estimators appear to improve this scaling, and our goal is to analyse the problem from the perspective of the maximum risk over all states.

We propose qubit estimation strategies based on separate adaptive measurements, and collective measurements, that achieve $1/n$ scalings for the maximum Bures risk. The estimator involving local measurements uses a fixed fraction of the available resource n to estimate the Bloch vector direction; the length of the Bloch vector is then estimated from the remaining copies by measuring in the estimator eigenbasis. The estimator based on collective measurements uses local asymptotic normality techniques which allows us to derive upper and lower bounds to its maximum Bures risk. We also discuss how to construct a minimax optimal estimator in this setup. Finally, we consider quantum relative entropy and show that the risk of the estimator based on collective measurements achieves a rate $O(n^{-1} \log n)$ under this loss function. Furthermore, we show that no estimator can achieve faster rates, in particular the 'standard' rate n^{-1}.

1 Introduction

Quantum state tomography plays in an important role in quantum information processing tasks, as a method of estimating and validating experimentally prepared quantum states [1]. The aim of state tomography is the estimation of an unknown density matrix ρ from the outcomes of measurements performed on n identical copies of the state available as a resource. The quality of the resulting estimate $\hat{\rho}$ is quantified in terms of its average error, or risk. Given a measurement design M, and the corresponding set of outcomes X, the risk of the measurement-estimator pair is

$$R(\rho, \hat{\rho}) := \mathbb{E}\left[D(\hat{\rho}(X), \rho)\right], \tag{1}$$

1

where the expectation is taken with respect to the measurement outcomes X, given the unknown state ρ. The risk depends on the choice of the error, or loss function $D(\hat{\rho}, \rho)$, which is a measure of the deviation of the estimated state from the true state ρ. Examples of commonly used loss functions are squared Frobenius (norm-two) distance, infidelity, the trace-norm distance, and the Bures distance. The risk is a function of the resource size n, and one is interested in its behaviour in the limit of large n. Typically, for a 'good' estimator and particular choices of loss functions, (e.g. locally quadratic functions) the optimal risk exhibits a rate of $O(1/n)$ *uniformly* over all states ρ.

However, for certain loss functions (e.g. squared Bures distance, or infidelity) , the risk is known to behave differently for states of unknown purity [2,3]. This is readily illustrated in the qubit case, where the fidelity between the state ρ and its estimate $\hat{\rho}$ is defined as $F(\rho, \hat{\rho}) := [\text{Tr}(\sqrt{\sqrt{\rho}\hat{\rho}\sqrt{\rho}})]^2$ and can be expressed as

$$F(\rho, \hat{\rho}) := \frac{1}{2}(1 + \sqrt{1 - |r|}\sqrt{1 - |\hat{r}|} + \boldsymbol{r} \cdot \hat{\boldsymbol{r}}), \tag{2}$$

where $\boldsymbol{r}, \hat{\boldsymbol{r}} \in \mathbb{R}^3$ are the Bloch vectors of the two states. For ρ within the Bloch sphere, the fidelity is locally quadratic in the components $\delta_i := r_i - \hat{r}_i$, with $i = x, y, z$. However, for states close to the boundary of the Bloch sphere, the fidelity becomes linear in $|\delta_i|$. Standard tomographic estimation of the Bloch vector components by measuring the spin operators $\sigma_x, \sigma_y, \sigma_z$ gives an accuracy of the order of $n^{-1/2}$ in estimating δ_i. This implies that for a loss function such as the infidelity $1 - F(\hat{\rho}, \rho)$, or the square Bures distance $D_B(\rho, \hat{\rho}_n)^2 := 2(1 - \sqrt{F(\rho, \hat{\rho}_n)})$, the risk scales as $O(1/n)$ for states within the Bloch sphere, but only as $O(1/\sqrt{n})$ for nearly pure states.

This poor scaling is a feature of not just the standard tomographic procedure, but any estimation method involving fixed basis measurements. This fact is significant as the preparation and estimation of pure states is ubiquitous in quantum information processing tasks. Several papers propose estimation methods that improve this risk and aim to recover the $O(1/n)$ scaling. A key idea is the performing of adaptive measurements that take into account outcomes from previous measurement stages to inform subsequent measurements. Estimation strategies involving such adaptive protocols have been proposed for both global and local measurements.

Two-step adaptive quantum tomography has been considered in [2,6–9], and involves using a fraction n_1 of the available resource n to obtain a preliminary estimate of the eigenbasis of ρ, and then performing measurements along the estimated eigenbasis on the remaining $n - n_1$ copies of the state. In [8] it is shown that using a vanishing fraction $n_1 = n^\alpha$, with $1/2 < \alpha < 1$ for the preliminary estimate gives a rate of $O(1/n)$ for the average infidelity with respect to certain distributions over states. However, it has been pointed out in [2], that for certain states a vanishing fraction is insufficient, and that for almost pure states the worst case infidelity scales as $O(n^{-5/6})$. Numerical results in [2] suggest that using a fixed fraction $n_0 = \beta n$ instead gives the $O(1/n)$ scaling for nearly pure states. The two step adaptive protocols have been experimentally implemented [2,9], showing a quadratic improvement in scaling for nearly pure states. The extension of the two-step adaptive protocol to a fully adaptive one has been considered in [7,10–12], where the measurement basis is aligned according to a current estimate after every measurement step. In the Bayesian

framework, 'self-learning' measurement protocols have been considered in [13–16]. A detailed review of various adaptive protocols and experimental results is found in [17].

Protocols considering collective (or joint rather than separate) measurements have also been considered [18–21]. It is known that joint measurements perform better than separate measurements in the case of mixed states [19]. In a Bayesian framework, [18] showed that with certain optimal joint measurements, the asymptotic infidelity averaged over a prior distribution achieved a value of $\frac{3+2\langle r\rangle}{4n}$ for mixed qubit states, where $\langle r \rangle$ is the mean purity over the prior distribution. Work in [20] proposes a two-step adaptive estimation strategy that is shown to be *locally* optimal, achieving an infidelity risk of $\frac{1+4\lambda_{\max}(\rho)}{4n}$ for mixed qubit states, where $\lambda_{\max}(\rho)$ is the maximum eigenvalue of ρ. Although many papers discuss the issues surrounding quantum tomography for Bures (and infidelity) risk and study such adaptive estimation protocols, in this work we consider the problem in the context of minimax estimation (see also [4, 5]), i.e. where the figure of merit is the *maximum risk* over all states

$$R_{max}(\hat{\rho}_n) := \sup_\rho R(\rho, \hat{\rho}_n) = \sup_\rho \mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2\right]. \tag{3}$$

To the best of our knowledge a scaling of n^{-1} of this maximum risk has not been demonstrated for any of the estimation strategies proposed in the literature. Furthermore, existing theoretical results cannot be directly used to derive the n^{-1} scaling of the minimax risk. In this paper we propose two different estimators, one based on adaptive local measurements similar to [2, 8], and a second based on global collective measurements and Local Asymptotic normality (LAN) as in [20, 21]. We demonstrate that both estimation strategies achieve the n^{-1} scaling of the maximum risk. We also investigate the asymptotically minimax optimal estimation strategy for the estimator based on collective measurements.

In terms of local measurements, we consider a two step adaptive strategy much in line with already proposed estimators [2, 6–9]. A *fixed fraction* of the total sample size n is used to obtain a preliminary estimate $\tilde{\mathbf{r}}$ of the Bloch vector $\mathbf{r}$ of the state, by performing standard tomographic measurements of the spin observables. The remaining copies of the state are used to estimate the eigenvalues of the state by performing measurements along the estimated direction $\tilde{\mathbf{r}}/|\tilde{\mathbf{r}}|$. The final estimate $\hat{\rho}_n$ of the state is then constructed from the estimated eigenvalues in the adaptive step and the preliminary estimate. For this estimator, we upper-bound the maximum Bures risk and demonstrate a scaling of n^{-1}.

The estimator based on global collective measurements uses established LAN results for qubit states [20, 21]. The measurement strategy involves two stages. The first stage involves the standard tomographic measurements of the spin components on a *vanishing number* of copies of the state $\tilde{n} \ll n$. A preliminary estimate $\tilde{\rho}$ is constructed from the outcomes. The second measurement stage depends on this preliminary estimate, and for technical purposes related to the asymptotic analysis we consider the following two cases: $|\tilde{\mathbf{r}}| < \delta$ and $|\tilde{\mathbf{r}}| \geq \delta$ for some small constant $\delta > 0$. When $\tilde{\rho}$ is close to the fully mixed state, the standard tomographic measurements are performed

3

on the remaining copies of the state. When the preliminary estimate $\tilde{\rho}$ is away from the fully mixed state, a joint measurement is performed on the remaining copies of the state. The joint state $\rho_n^{\boldsymbol{\theta}} := \rho_{\boldsymbol{\theta}}^{\otimes n}$ has a block-diagonal form following the Weyl decomposition of the underlying space $(\mathbb{C}^2)^{\otimes n}$. Information about the eigenvalue parameter λ is encoded in a probability distribution over the different blocks of the decomposition, while information about the local parameters (u, v) is encoded in the block states. We consider a parameterisation of states $\rho_{\boldsymbol{\theta}}$, with $\boldsymbol{\theta} = (\lambda, u, v) \in \mathbb{R}^3$, where λ parametrises the smallest eigenvalue of the states and $\boldsymbol{w} = (u, v)$ are certain local rotation parameters around a fixed state ρ_0. The parameter λ is then estimated from the outcomes of a "which-block" measurement, while the local parameters u, v are optimally estimated by exploiting the local asymptotic normality of the block states. The LAN results in [20] establish that in the limit $n \to \infty$, the block states converge to Gaussian states $\phi^{\boldsymbol{w}}$, with displacement proportional to parameters (u, v) (Theorem 1). The optimal estimator of u, v is then the optimal estimator of the displacement of a Gaussian state $\phi^{\boldsymbol{w}}$, which is known to be the heterodyne measurement (see Appendix A.3 for a description of the measurement). We derive minimax upper and lower bounds for the risk (3), and demonstrate that the maximum Bures risk for the estimator $\hat{\rho}_n$ scales as C/n, with C being a constant. We obtain lower bound of $5/4$ for this constant, and an upper bound of $3/2$.

An important element in the derivation of the upper-bounds for the maximum risk of both estimators is the fact that Bures distance can locally approximated as a sum of contributions from the eigenvalue parameter and the 'rotation' parameters. More explicitly, we have that

$$D_B(\rho, \hat{\rho}_n)^2 \approx D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})^2 + \frac{1}{4} \frac{(1 - 2\lambda)(1 - 2\hat{\lambda})}{\sqrt{(1 - \lambda)(1 - \hat{\lambda})} + \sqrt{\lambda\hat{\lambda}}} \Phi^2, \tag{4}$$

where $D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})^2 := \|\sqrt{\boldsymbol{\lambda}} - \sqrt{\hat{\boldsymbol{\lambda}}}\|^2$ with $\boldsymbol{\lambda} = (\lambda, 1 - \lambda)$ is the classical Hellinger distance, and Φ is the angle between the Bloch vectors of the two states. The optimal rate of estimation of the 'rotation' parameters is shown to be $1/n$ for all states. The problem of establishing minimax results for the Bures distance therefore converts a problem of establishing minimax results for the Hellinger risk of estimating the eigenvalue parameter. To the best of our knowledge such minimax results for the Hellinger risk are not known. Instead, we upper-bound this risk by the Kullback-Leibler risk, and use known results about the minimax estimator in this case. However, in section 5 we propose a minimax optimal estimator of the classical parameter λ under the Hellinger risk gives a minimax optimal estimator $\hat{\rho}_n$ for qubit states.

In section 6, we consider the quantum relative entropy (QRE) $S(\rho\|\rho') = \mathrm{Tr}[\rho(\log \rho - \log \rho')]$, and bound the maximum risk under this loss function. As in the case with the Bures distance, an important element is a local decomposition of the QRE risk into contributions from the Kullback-Leibler risk and a term involving the 'rotation parameters'. Namely, we have that for qubit states

$$S(\rho\|\hat{\rho}) = D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}) + \frac{1 - 2\lambda}{4}(\Phi^2 + O(\Phi^4)) \log\left(\frac{1 - \hat{\lambda}}{\hat{\lambda}}\right),$$

where $D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})$ is the Kullback-Leibler distance between the two distributions $\boldsymbol{\lambda} = (\lambda, 1 - \lambda)$ and $\hat{\boldsymbol{\lambda}} = (\hat{\lambda}, 1 - \hat{\lambda})$. Using this local decomposition we show that the global estimator we propose achieves a rate of $O(n^{-1} \log n)$. Furthermore we make the case that no estimator can achieve faster rates, and show that the minimax QRE risk scales as $O(n^{-1} \log n)$.

The paper is organised as follows. In section 2 we consider an estimator based on local measurements and detail a two step adaptive measurement strategy. We demonstrate that the proposed estimator achieves a minimax rate of $1/n$. In section 3 we propose a second estimator based on global collective measurements. We begin in section 3.1 by describing the preliminary measurement stage and introduce our parametrisation of states. In section 3.2, we describe the second measurement stage, and overview the block decomposition of the joint state and results of LAN. The minimax bounds for this estimator are derived in section 4, and in section 5 we discuss and state the proposition that a minimax estimator for the Hellinger loss function implies a minimax optimal estimator for qubit states. Finally in section 6 we consider the quantum relative entropy and establish that the minimax rate under this loss function scales as $O(n^{-1} \log n)$.

2 Estimator based on local adaptive measurements

We let ρ be an arbitrary density matrix associated with a single qubit state. Given n identical copies of the state as a resource, we wish to construct an estimator of the state. As briefly discussed in the introduction, in this section we propose a two-step adaptive measurement strategy based on local measurements. While the idea of an adaptive local measurement strategy is not new and has been treated in various instances in the literature [2, 6–9], we are interested in analysing the performance of the proposed estimator $\hat{\rho}_n$ in terms of the *maximum risk* with respect to the *Bures distance* defined in equation (3) and its asymptotic rescaled version

$$r_{\max}(\hat{\rho}) = \lim \sup_{n \to \infty} \sup_{\rho} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2\right] = \limsup_{n \to \infty} nR_{\max}(\hat{\rho}_n). \tag{5}$$

We will derive an upper bound for the latter risk, thereby demonstrating a n^{-1} scaling for maximum risk over all states ρ. Since the maximum risk of any estimation procedure cannot scale faster than n^{-1}, this implies that the existence of a non-trivial scaling constant for the *minimax risk* given by

$$r_{\mathrm{minimax}} := \limsup_{n \to \infty} \inf_{\hat{\rho}_n} nR_{\max}(\hat{\rho}_n). \tag{6}$$

Finding the value of the minimax constant remains an open problem. We will come back to this problem in section 5 where it is shown that the minimax qubit estimation problem reduces to that of minimax estimation of a coin probability with respect to the square Hellinger distance risk.

The estimator we propose is constructed as follows. The first stage is a preliminary localisation step involving standard projective measurements of Pauli observables $\sigma_x, \sigma_y, \sigma_z$ on a fixed fraction n_1 of the total number of qubits n. An estimate $\tilde{\mathbf{r}}$ of the state's Bloch vector $\mathbf{r}$ is constructed from the outcomes of these measurements. In the second (adaptive) stage, the spin component $\Xi := \vec{\sigma} \cdot \tilde{\mathbf{r}} / |\tilde{\mathbf{r}}|$

5

is measured on the remaining $n_2 := n - n_1$ copies of the state. This provides an estimate $\hat{\lambda}$ of the eigenvalue of the state, which together with the direction vector determine the final state estimator in equation (9) below.

With respect to the first stage, the following lemma shows that with high probability the estimated directional vector is within an angle of $O(n_1^{-1/2+\epsilon_1})$ of the true vector, where ϵ_1 is a fixed (small) positive constant.

Lemma 1. *Let X_i, Y_i, Z_i be the outcomes of measurements of $\sigma_x, \sigma_y, \sigma_z$ performed on independent qubits in state ρ with Bloch vector $\mathbf{r}$, where $i = 1, \ldots, n_1/3$. Let $\tilde{\mathbf{r}}$ be the estimate of the Bloch vector, where each Bloch vector component is obtained by averaging the outcome results, e.g $\tilde{r}_x := \frac{3}{n_1} \sum_i X_i$. Then we have that for $\epsilon_1 > 0$,*

$$\mathbb{P}\left(\|\mathbf{r} - \tilde{\mathbf{r}}\|^2 > 6n_1^{-1+2\epsilon_1} \right) \leq 6\exp\left(-\frac{2n_1^{2\epsilon_1}}{3} \right). \tag{7}$$

The proof of this lemma follows directly from the Hoeffding's inequality applied to the binomial distribution corresponding to each of the Bloch vector components. The concentration inequality implies that when $|\mathbf{r}|$ is bounded away from zero, the magnitude of the angle Φ between the directional vectors $\mathbf{r}/|\mathbf{r}|$ and $\tilde{\mathbf{r}}/|\tilde{\mathbf{r}}|$ is of the order $O(n_1^{-1/2+\epsilon_1})$ with high probability.

The second adaptive stage involves preforming measurements along this estimated direction. That is, projective measurements of the observable $\Xi := \vec{\sigma} \cdot \tilde{\mathbf{r}}/|\tilde{\mathbf{r}}|$ are performed on the remaining $n_2 := n - n_1$ copies of the state. Let k be the total number of -1 outcomes from these measurements. It is easy to see that k is distributed binomially $B_{n_2,\tilde{p}}(k)$ with (random) binomial parameter $\tilde{p} := (1 - |\mathbf{r}|\cos\Phi)/2$. We estimate this parameter as $\hat{p}$ from the measurement outcomes using the 'add-beta' estimator [22, 23] defined as follows,

$$\hat{p}_{n_2} = \begin{cases} \frac{1/2}{n_2+5/4}, & k = 0, \\ \frac{2}{n_2+7/4}, & k = 1, \\ \frac{k+3/4}{n_2+3/2}, & k = 2, \ldots, n_2 - 2, \\ \frac{n_2-1/4}{n_2+7/4}, & k = n_2 - 1, \\ \frac{n_2+3/4}{n_2+5/4}, & k = n_2. \end{cases} \tag{8}$$

While this estimator is not in any sense optimal, it is known to be the minimax estimator for the Kulback-Leibler risk achieving a rate of $\frac{1}{2n_2} + O(n_2^{-2})$. We shall shortly use this fact below in deriving the upper bound for qubit tomography. It is worth noting that unlike the maximum likelihood estimator which would assign $\hat{p}_{n_2} = 0$ for $k = 0$, the 'add-beta' estimator 'hedges' against unobserved events [4].

The final estimate of the state puts together the estimate $\hat{p}_{n_2}$ and the estimated Bloch vector $\tilde{\mathbf{r}}$ as follows

$$\hat{\rho}_n = \frac{1}{2}\left(I + \frac{1 - 2\hat{p}_{n_2}}{|\tilde{\mathbf{r}}|}\tilde{\mathbf{r}} \cdot \vec{\sigma} \right). \tag{9}$$

It is easy to see that $\hat{p}_{n_2} = \hat{\lambda}_n$ by construction, where $\hat{\lambda}_n$ is the smallest eigenvalue of $\hat{\rho}_n$.

2.1 An upper bound scaling as n^{-1}

We now look at deriving an upper bound for the Bures risk of this estimator, and demonstrate that the maximum over all states scales as n^{-1}. Recall that the Bures distance between the final estimate $\hat{\rho}_n$ and the true state ρ is defined as $D_B(\rho, \hat{\rho}_n)^2 := 2\left[1 - \sqrt{F(\rho, \hat{\rho}_n)}\right]$, where the fidelity can be expressed in terms of the Bloch vectors $\hat{\mathbf{r}}$ and $\mathbf{r}$ as

$$
\begin{aligned}
F(\rho, \hat{\rho}) &= \frac{1}{2}\left(1 + \sqrt{1 - |\mathbf{r}|^2}\sqrt{1 - |\hat{\mathbf{r}}|^2} + \mathbf{r} \cdot \hat{\mathbf{r}}\right) \\
&= \frac{1}{2}\left(1 + \sqrt{1 - |\mathbf{r}|^2}\sqrt{1 - |\hat{\mathbf{r}}|^2} + |\mathbf{r}||\hat{\mathbf{r}}|\cos\Phi\right),
\end{aligned}
\tag{10}
$$

where Φ is the angle between the Bloch vectors.

In the following arguments we will assume that $\rho \in B_\delta^c$ where $B_\delta = \{\rho : |\mathbf{r}| < \delta\}$ is a small ball or fixed radius $\delta > 0$ around the completely depolarised state. From Lemma 1, the angle Φ is known to be of the order $O(n^{-1/2+\epsilon_1})$ with high probability, uniformly over states $\rho \in B_\delta^c$. This implies that the cosine term in (10) can be expanded to leading order in Φ. In this case, the Bures distance is expressed as

$$
D_B(\rho, \hat{\rho}_n)^2 = D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)^2 + \frac{1}{4}\frac{(1-2\lambda)(1-2\hat{\lambda}_n)}{\sqrt{(1-\lambda)(1-\hat{\lambda}_n)} + \sqrt{\lambda\hat{\lambda}_n}}\Phi^2 + O(\Phi^4)
\tag{11}
$$

where $\lambda = (1 - |\mathbf{r}|)/2$, $\hat{\lambda}_n = (1 - |\hat{\mathbf{r}}_n|)/2$ are the smallest eigenvalues of ρ and respectively $\hat{\rho}_n$, and

$$
D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})^2 := \left(\sqrt{\lambda} - \sqrt{\hat{\lambda}}\right)^2 + \left(\sqrt{1-\lambda} - \sqrt{1-\hat{\lambda}}\right)^2
\tag{12}
$$

is the square Hellinger distance between the probability distributions $\boldsymbol{\lambda} = (\lambda, 1 - \lambda)$ and $\hat{\boldsymbol{\lambda}} = (\hat{\lambda}, 1 - \hat{\lambda})$. The proof of this approximation can be found in Appendix A.2.

Identifying $\hat{\boldsymbol{\lambda}} = (\hat{p}_{n_2}, 1 - \hat{p}_{n_2})$, we upper bound the Bures distance as

$$
\begin{aligned}
D_B(\rho, \hat{\rho}_n)^2 &\leq D_H(\boldsymbol{\lambda}, \hat{\mathbf{p}}_{n_2})^2 + \frac{1}{4}\Phi^2 + O(\Phi^4) \\
&\leq 2D_H(\boldsymbol{\lambda}, \tilde{\mathbf{p}})^2 + 2D_H(\tilde{\mathbf{p}}, \hat{\mathbf{p}}_{n_2})^2 + \frac{1}{4}\Phi^2 + O(\Phi^4)
\end{aligned}
\tag{13}
$$

where the second inequality is established using the fact that the Hellinger distance satisfies the triangle inequality. Using the inequality $D_H^2(\boldsymbol{\lambda}, \tilde{\mathbf{p}}) \leq 2|\lambda - p|$ and $p = (1 - |\mathbf{r}|\cos\Phi)/2$ we further upper bound the risk as

$$
D_B(\rho, \hat{\rho}_n)^2 \leq D_H(\tilde{\mathbf{p}}, \hat{\mathbf{p}}_{n_2})^2 + \left(\frac{1}{4} + |\mathbf{r}|\right)\Phi^2 + O(\Phi^4).
\tag{14}
$$

7

Taking expectation with respect to the measurement outcomes given the true state ρ, we have

$$\mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2\right] \leq 2\mathbb{E}\left[2D_H(\tilde{\mathbf{p}}, \hat{\mathbf{p}}_{n_2})^2\right] + \frac{5}{4}\mathbb{E}\left[\Phi^2\right] + O(n_1^{-2+4\epsilon_1}) \tag{15}$$

The maximum risk over B_δ^c is therefore bounded from above as

$$\begin{aligned}
\sup_{\rho \in B_\delta^c} \mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2\right] &\leq \sup_{\tilde{\mathbf{p}}} 2\mathbb{E}\left[D_H(\tilde{\mathbf{p}}, \hat{\mathbf{p}}_{n_2})^2\right] + O(n_1^{-1}) + O(n_1^{-2+4\epsilon_1}) \\
&\leq \sup_{\tilde{\mathbf{p}}} 2\mathbb{E}\left[D_{KL}(\tilde{\mathbf{p}}, \hat{\mathbf{p}}_{n_2})\right] + O(n_1^{-1}) + O(n_1^{-2+4\epsilon_1}) \tag{16}
\end{aligned}$$

In the first inequality we upped bounded $\mathbb{E}[\Phi^2]$ as $O(n_1^{-1})$; this follows from the concentration inequality of Lemma 1. The second step employs the inequality between the squared Hellinger distance and the Kullback-Leibler (KL) distance

$$D_H(\hat{\mathbf{p}}, \tilde{\mathbf{p}}) \leq D_{KL}(\hat{\mathbf{p}}, \tilde{\mathbf{p}}) := \hat{p}\log\frac{\hat{p}}{\tilde{p}} + (1-\hat{p})\log\frac{1-\hat{p}}{1-\tilde{p}}. \tag{17}$$

The reason for employing this inequality is that to the best of the authors' knowledge the asymptotic minimax optimal Hellinger risk of estimating the binomial parameter $\tilde{p}$ is not known in the literature. A discussion related to the difficulty in obtaining the asymptotic minimax Hellinger risk is left to section 5. However, the minimax optimal rate for the KL loss function under the binomial distribution is known. The minimax optimal estimator is precisely the 'add beta' estimator defined in (8) , and is known to achieve the asymptotic rate $\frac{1}{2n_2}(1+o(1))$ [22,23]. Therefore, by choosing n_1 to be constant fraction of the total number of samples n (e.g. $n_1 = n_2 = n/2$) we find that the right side in (16) has an overall rate of $O(1/n)$.

It remains to consider the case $\rho \in B_\delta$. Using concentration arguments similar to Lemma 1 we find that for large n the estimator $\hat{\rho}_n$ belongs to a ball $B_{2\delta}$, with high probability. In this region the Bures distance upper bounded by the Euclidian distance

$$d_B(\rho, \hat{\rho}) < C_\delta \|\mathbf{r} - \hat{\mathbf{r}}\|^2 \tag{18}$$

so that the maximum risk in B_δ scales as

$$\sup_{\rho \in B_\delta} \mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2\right] = O(n^{-1}). \tag{19}$$

Putting together the two upper bounds we conclude that $R_{max}(\hat{\rho}_n) = O(n^{-1})$. and therefore

$$r_{\max}(\hat{\rho}) = \limsup_{n\to\infty} nR_{\max}(\hat{\rho}_n) < \infty. \tag{20}$$

A numerical estimate of the constant $r_{\max}(\hat{\rho})$ could in principle be obtained by a detailed analysis of the above inequalities; however, we will not pursue this issue here, and instead do that for the collective measurement estimator discussed in section 4.

3 Irreducible representations, collective measurements and local asymptotic normality

In this section we describe the key ingredients of a two stage estimator of the qubit state, which uses collective rather than separate measurements. In section 4 we will come back to the details of the estimation procedure and establish upper and lower bounds for the asymptotic maximum risk. The first stage is a localisation one which uses a vanishing fraction $\tilde{n}$ of the overall ensemble of n qubits, to produce a preliminary estimator $\tilde{\rho}$, by performing separate Pauli measurements. The second stage of the protocol involves collective measurements on the remaining $n - \tilde{n}$ copies of the state. Since this will not affect the asymptotic rates, we will continue to denote the number of copies in the second stage by n. Since ρ belongs to a shrinking neighbourhood of $\tilde{\rho}$, we can work in the eigenbasis of the latter and parametrise ρ as follows

$$\rho_{\boldsymbol{\theta}} := U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right)\begin{pmatrix} 1-\lambda & 0 \\ 0 & \lambda \end{pmatrix} U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right)^* \tag{21}$$

where $\boldsymbol{\theta} = (\lambda, \boldsymbol{w}) = (\lambda, u, v)$ is an unknown parameter, with λ being the eigenvalue and $\boldsymbol{w}$ are 'local' rotation parameters, i.e. $U(\boldsymbol{w}) := \exp(i(u\sigma_x + v\sigma_y))$. We now provide a brief overview of the joint measurements stage based on the techniques of local asymptotic normality (LAN) [20,21], cf. section 3.3.

A key ingredient in the description of the LAN based protocol is the fact that the joint state of the ensemble admits a block-diagonal decomposition along the irreducible representations of two symmetry groups $SU(2)$ and $S(n)$

$$\rho_{\boldsymbol{\theta}}^{\otimes n} = \bigoplus_{j=0,1/2}^{n/2} p_{n,\lambda}(j)\rho_{j,n}^{\boldsymbol{w}} \otimes \frac{\mathbf{1}}{n_j}. \tag{22}$$

The various blocks of the decomposition carry probability weights $p_{n,\lambda}(j)$ which concentrates around the representation with total spin $j_n := n(1/2 - \lambda)$. The distribution carries information about the eigenvalue parameter λ and can be sampled by performing a 'which block' projective measurement producing an outcome j with probability $p_{n,\lambda}(j)$, cf. section 3.2. This outcome will be used to construct the estimator $\hat{\lambda}_n$ as discussed in detail in section 4.

Information about the 'rotation' parameters $\boldsymbol{w}$ is encoded in the conditional quantum state $\rho_{j,n}^{\boldsymbol{w}}$ of block selected by the 'which block' measurement. LAN theory shows that in the limit of large n, each block $\rho_{j,n}^{\boldsymbol{w}}$ can be mapped isometrically onto an approximate Gaussian state $\phi^{\boldsymbol{w}}$ of a quantum harmonic oscillator with displacement proportional to $\boldsymbol{w} = (u, v)$. The optimal measurement for estimating the displacement parameters (and therefore $\boldsymbol{w}$) is the heterodyne measurement of the continuous variables system [20,21] (see Appendix A.3 for a description of the measurement) . By putting together the eigenvalue and rotation parameters estimators $\hat{\lambda}_n, \hat{\boldsymbol{w}}_n$ we obtain the (final and more refined) second stage estimator expressed in the eigenbasis of the preliminary estimator $\tilde{\rho}$.

The performance of this estimator will be analysed in section 4.

3.1 Preliminary localisation and parametrisation

The first stage is a preliminary localisation step that involves performing standard projective measurements of the Pauli observables $\sigma_x, \sigma_y, \sigma_z$ on a vanishing fraction $\tilde{n}$ of the overall ensemble of n identically prepared qubits. An estimate $\tilde{\rho}$ of the state is constructed from the outcomes of these measurements. The following lemma shows that *with high probability* the true state ρ lies within a ball of radius $O(n^{-1/2+\epsilon_2})$ of this estimate $\tilde{\rho}$. This allows us to restrict our attention to a local neighbourhood of the preliminary estimator in the second stage of the estimation.

Lemma 2. *Let X_i, Y_i, Z_i be independent outcomes of measurements of $\sigma_x, \sigma_y, \sigma_z$ performed on independent qubits in state ρ with Bloch vector $\mathbf{r}$, where $i = 1, \ldots, \tilde{n}/3$. Let $\tilde{\rho}$ be the estimator with Bloch vector $\tilde{\mathbf{r}}$ obtained by averaging the outcome results, e.g. $\tilde{r}_x := \frac{3}{\tilde{n}} \sum_i X_i$.*

In order to obtain a physical state, the final estimate of the state is constructed as

$$\tilde{\rho} := \arg\min_{\tau \in \mathcal{S}_2} \|\tau - (\mathbb{1} + \tilde{\boldsymbol{r}} \cdot \boldsymbol{\sigma})/2\|_1^2 \tag{23}$$

where the minimisation is over all the space of all 2×2 density matrices $\mathcal{S}_2$. For this estimator $\tilde{\rho}$, we have that for all $\epsilon_2 > 0$,

$$\mathbb{P}\left(\|\tilde{\rho} - \rho\|_1^2 > 3n^{2\epsilon_2 - 1}\right) \leq 6\exp\left(-\frac{2\tilde{n}n^{2\epsilon_2 - 1}}{3}\right), \qquad \text{for all } \rho \in \mathcal{S}_2. \tag{24}$$

The proof of this lemma follows from an application of Hoeffding's inequality, and can be found in Appendix A.1. Setting $\tilde{n} = n^{1-\kappa}$, with $0 < \kappa < 2\epsilon_2$, the probability of failure is exponentially small. The preliminary measurement stage therefore places the estimate $\tilde{\rho}$ in a local neighbourhood around the true state. Since $\|\tilde{\rho} - \rho\|_1^2 = \|\tilde{\boldsymbol{r}} - \boldsymbol{r}\|^2$, the angle between the two normalised Bloch vectors $\boldsymbol{r}/|\boldsymbol{r}|$ and $\tilde{\boldsymbol{r}}/|\tilde{\boldsymbol{r}}|$ is of the order $O(n^{-1/2+\epsilon_2})$ with high probability.

For technical reasons related to local asymptotic normality theory and the derivation of certain error bounds, the subsequent measurement depends on $\tilde{\rho}$, and we distinguish the following two cases.

i) If $\tilde{\rho}$ is within a fixed but small ball B_δ of radius $\delta > 0$ around the fully mixed state (i.e, $|\tilde{r}| \leq \delta$), the secondary measurement stage consists of the standard tomographic measurements in the σ_i, $i = x, y, z$ bases. For each i, measurements of σ_i are performed on $(n - \tilde{n})/3$ identical copies of the state. The final estimate of the state $\hat{\rho}_n$ is constructed from the outcomes of these measurements, and is detailed in section 4.

ii) If $\tilde{\rho}$ is outside B_δ, we can apply the tools of LAN. The remaining $n - \tilde{n}$ copies of the state available for the second stage are rotated such that the estimated Bloch vector $\tilde{r}$ is pointing along the z-axis. From Lemma 2, the angle between the directional vectors $\boldsymbol{r}/|\boldsymbol{r}|$ and $\tilde{\boldsymbol{r}}/|\tilde{\boldsymbol{r}}|$ is known to be of the order $O(n^{-1/2+\epsilon_2})$ with high probability. This allows us to consider a restricted parametrisation of states which we describe now for an arbitrary but fixed state ρ_0 with its Bloch vector along the z-axis (which is $\tilde{\rho}$ written in its own eigenbasis)

$$\rho_0 = \begin{pmatrix} 1 - \lambda_0 & 0 \\ 0 & \lambda_0 \end{pmatrix} \tag{25}$$

10

with $0 < \lambda_0 < 1/2$. We consider a parametrisation $\boldsymbol{\theta} \to \rho_{\boldsymbol{\theta}}$ of states obtained by small unitary rotations of ρ_0, and different choices of the eigenvalue. We choose the parameter vector $\boldsymbol{\theta} := (\lambda, \boldsymbol{w})$, where $\boldsymbol{w} = (u, v) \in \mathbb{R}^2$ corresponds to the small unitary rotations of the eigenvectors, and λ is the smallest eigenvalue. That is, any state ρ described by $\boldsymbol{\theta} = (\lambda, u, v)$ is of the form

$$\rho_{\boldsymbol{\theta}} := U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right) \begin{pmatrix} 1 - \lambda & 0 \\ 0 & \lambda \end{pmatrix} U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right)^* \tag{26}$$

where the unitary $U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right)$ is given by

$$U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right) := \exp\left(\frac{i}{\sqrt{n}}(u\sigma_x + v\sigma_y)\right) = \begin{pmatrix} \cos|\boldsymbol{w}|/\sqrt{n} & -\exp(-i\varphi)\sin|\boldsymbol{w}|/\sqrt{n} \\ \exp(i\varphi)\sin|\boldsymbol{w}|/\sqrt{n} & \cos|\boldsymbol{w}|/\sqrt{n} \end{pmatrix}$$

with $\varphi = \mathrm{Arg}(-v + iu)$. Note that in this parametrisation we have $\rho_0 = \rho_{\boldsymbol{\theta}_0}$ with $\boldsymbol{\theta}_0 = (\lambda_0, 0, 0)$. The aim of the second measurement stage is then to estimate the unknown parameter vector $\boldsymbol{\theta} = (\lambda, u, v) = (\lambda, \boldsymbol{w})$ corresponding to the true state ρ.

3.2 The 'which block' measurement stage

The second measurement stage involves a joint measurement on the $n - \tilde{n}$ remaining copies of the state. We therefore consider the joint states $\rho_n^{\boldsymbol{\theta}} := \rho_{\boldsymbol{\theta}}^{\otimes n}$ on n identical qubits, with the parametrisation around the preliminary estimator $\rho_0 = \tilde{\rho}$ described above. It is known that the states $\rho_n^{\boldsymbol{\theta}}$ have a block-diagonal form with respect to the decomposition of the underlying space $(\mathbb{C}^2)^{\otimes n}$ in irreducible representations of the groups $SU(2)$ and $S(n)$ [18, 20, 24]. The representation π_n of $SU(2)$ is given by $\pi^{(n)}(u) = u^{\otimes n}$ for any $u \in SU(2)$, and the representation $\tilde{\pi}_n$ of the symmetric group $S(n)$ is given by the permutation of factors

$$\tilde{\pi}^{(n)}(\tau) : v_1 \otimes \ldots \otimes v_n \to v_{\tau^{-1}(1)} \otimes \ldots \otimes v_{\tau^{-1}(n)}, \qquad \tau \in S(n) \tag{27}$$

According to Weyl's Theorem, the following decomposition holds

$$(\mathbb{C}^2)^{\otimes n} = \bigoplus_{j=0,1/2}^{n/2} \mathcal{H}_j \otimes \mathcal{H}_n^j \tag{28}$$

where the lower limit in the direct sum is 0 for even n and $1/2$ for odd n. The two group representations decompose into direct sums of irreducible representations as $\pi^{(n)}(u) = \oplus_j \pi_j(u) \otimes \mathbb{1}$ and $\tilde{\pi}^{(n)}(\tau) = \oplus_j \mathbb{1} \otimes \tilde{\pi}_j(\tau)$ where π_j is the irreducible representation of $SU(2)$ with total angular momentum $J^2 = j(j+1)$ which acts on $\mathcal{H}_j \cong \mathbb{C}^{2j+1}$, and $\tilde{\pi}_j$ is the irreducible representation of the symmetric group $S(n)$ acting on $\mathcal{H}^j \cong \mathbb{C}^{n_j}$ with

$$n_j = \binom{n}{n/2 - j} - \binom{n}{n/2 - j - 1}, \qquad j \neq n/2 \tag{29}$$

and $n_{j=n/2} = 1$. The density matrix ρ_n^{θ} is invariant under permutations and can be decomposed as

$$\rho_n^{\boldsymbol{\theta}} = \bigoplus_{j=0,1/2}^{n/2} p_{n,\lambda}(j)\rho_{j,n}^{\boldsymbol{w}} \otimes \frac{\mathbf{1}}{n_j} \tag{30}$$

where the probability distribution $p_{n,\lambda}(j)$ is given by [18, 20, 21]

$$p_{n,\lambda}(j) := \frac{n_j}{1-2\lambda}\lambda^{n/2-j}(1-\lambda)^{n/2+j+1}(1-p^{2j+1}) \tag{31}$$

with $p = \frac{\lambda}{1-\lambda}$. The above distribution can be written in the form

$$p_{n,\lambda}(j) := B_{n,\lambda}(n/2-j) \times K(j,n,\lambda), \tag{32}$$

where $B_{n,\lambda}(k) = \binom{n}{k}\lambda^k(1-\lambda)^{n-k}$ is the binomial distribution and the term $K(j,n,\lambda)$ is given by

$$K(j,n,\lambda) := (1-p^{2j+1})\frac{n+(2(j-j_n)+1)/(1-2\lambda)}{n+(j-j_n+1)/(1-\lambda)}, \quad j_n := n(1/2-\lambda).$$

The binomially distributed variable $n/2-j$ concentrates around its mean value of $n\lambda$ with high probability

$$\mathbb{P}\left[n\lambda - n^{1/2+\epsilon_3} \le n/2 - j \le n\lambda + n^{1/2+\epsilon_3}\right] \ge 1 - 2\exp(-2n^{2\epsilon_3}),$$

where $\epsilon_3 > 0$ is an arbitrary constant. This follows from a straightforward application of Hoeffding's inequality (66) to the binomial distribution. Therefore, the mass of the distribution $B_{n,\lambda}(n/2-j)$ concentrates over values of j in the interval

$$\mathcal{J}_n := \{j|\, j_n - n^{1/2+\epsilon_3} \le j \le j_n + n^{1/2+\epsilon_3}\}. \tag{33}$$

For all $j \in \mathcal{J}_n$, the factor $K(j,n,\lambda) = 1 + O(n^{-1/2+\epsilon_3})$ provided that λ is bounded away from $1/2$, which is one of the reasons we chose to treat the two cases above separately. Additionally we note that the factor $K(j,n,\lambda)$ remains bounded over all values of j as long as $\lambda < 1/2$. From the concentration of the binomial distribution over values of $j \in \mathcal{J}_n$, and the value of $K(j,n,\lambda)$ in this interval it follows that

$$p_{n,\lambda}(\mathcal{J}_n) = 1 - O(n^{-1/2+\epsilon_3}). \tag{34}$$

A "which block" measurement corresponds to an output of a particular value of j from the distribution (32), and an associated posterior state $\rho_{j,n}^{\boldsymbol{w}}$. This value of j lies in the set $\mathcal{J}_n$ with high probability, and serves to estimate the eigenvalue parameter λ. As in the case of the local adaptive estimator in section 2, we shall define $\hat{\lambda}_n$ as the 'add-beta' estimator introduced in equation (8), with $k = n/2 - j$. A detailed discussion regarding this choice for the estimator $\hat{\lambda}_n$ is postponed to section 5. However we note that a possible physical implementation of such a measurement is detailed in [20], and involves coupling the joint states to different bosonic field and performing a homodyne measurement.

12

3.3   Local asymptotic normality

The block state $\rho_{j,n}^{\boldsymbol{w}}$ encodes information about the rotation parameters $\boldsymbol{w} = (u, v)$. The optimal estimation strategy for these parameters has been established using results about the LAN of qubit states [20]. This shows that for large n, the block states $\rho_{j,n}^{\boldsymbol{w}}$ approach a Gaussian state $\phi^{\boldsymbol{w}}$ of a one-mode continuous variables system *uniformly* over all $j \in \mathcal{J}_n$ and $\|\boldsymbol{w}\| \leq n^{\eta}$. The rotation parameters (u, v) are encoded linearly into the mean of the Gaussian state $\phi^{\boldsymbol{w}}$. So the problem of the optimal estimation of these parameters for the block state can be translated into one of estimating the displacement of $\phi^{\boldsymbol{w}}$. These ideas have been treated in detail in [20], and we only include a brief overview here. The block states $\rho_{j,n}^{\boldsymbol{w}}$ depend on the parameters (u, v) in the following way

$$\rho_{j,n}^{\boldsymbol{w}} = U_j\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right) \rho_{j,n}^{\boldsymbol{0}} U_j\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right)^* \tag{35}$$

where the unitaries are defined as $U_j(\boldsymbol{w}) := \exp(i(uJ_{j,x} + vJ_{j,y}))$, with $J_{j,l}$ being the generators of rotations in the irreducible representation π_j of SU(2). The state $\rho_{j,n}^{\boldsymbol{0}}$ is expressed as

$$\rho_{j,n}^{\boldsymbol{0}} = \frac{1-p}{1-p^{2j+1}} \sum_{m=-j}^{j} p^{j-m} |j, m\rangle\langle j, m| \tag{36}$$

with $p = \lambda/(1 - \lambda)$ as before. The set $\{|j, m\rangle : m = -j, \ldots, j\}$ is an orthonormal basis on $\mathcal{H}_j$ such that $J_{j,z}|j, m\rangle = m|j, m\rangle$. It has been demonstrated [20] that the family of states $\mathcal{F}_n := \{\rho_{j,n}^{\boldsymbol{w}}, \|\boldsymbol{w}\| \leq n^{\eta}, j \in \mathcal{J}_n\}$ is asymptotically Gaussian. This mean that as $n \to \infty$ the family of states $\rho_{j,n}^{\boldsymbol{w}}$ "converges" to a family of Gaussian states $\phi^{\boldsymbol{w}}$ of a one-mode continuous variables system, for all $j \in \mathcal{J}_n$ and $\|\boldsymbol{w}\| \leq n^{\eta}$. In order to make this convergence more precise, we let

$$\phi^{\boldsymbol{0}} := (1-p) \sum_{k=0} p^k |k\rangle\langle k| \tag{37}$$

be a centred Gaussian state of a one mode continuous variables system, with $\{|k\rangle : k \geq 0\}$ denoting the Fock basis. The states $\phi^{\boldsymbol{w}}$ are defined as

$$\phi^{\boldsymbol{w}} := D(\sqrt{1 - 2\lambda}\alpha_{\boldsymbol{w}})\phi^{\boldsymbol{0}} D(-\sqrt{1 - 2\lambda}\alpha_{\boldsymbol{w}}) \tag{38}$$

where $\alpha_{\boldsymbol{w}} = -v + iu \in \mathbb{C}$. The operator $D(\alpha) := \exp(\alpha a^* - \overline{\alpha}a)$ is the displacement operator that for every $\alpha \in \mathbb{C}$ maps the vacuum vector $|0\rangle$ to the coherent state $|\alpha\rangle$, with a^*, a being the creation and annihilation operators satisfying $[a, a^*] = 1$. The convergence of the block state $\rho_{n,j}^{\boldsymbol{w}}$ to the Gaussian state $\phi^{\boldsymbol{w}}$ is formalised in the following Theorem.

Theorem 1. *Let $V_j : \mathcal{H}_j \to L^2(\mathbb{R})$ be the isometry*

$$V_j : |j, m\rangle \to |j - m\rangle \tag{39}$$

that maps the orthonormal basis of $\mathcal{H}_j$ into the Fock basis of $L^2(\mathbb{R})$. Then for the family of block states $\rho_{n,j}^{\boldsymbol{w}}$ defined by (35), and the family of Gaussian states $\phi^{\boldsymbol{w}}$ defined by (38), the following convergence holds for any $0 \leq \eta \leq 1/6$ and $0 < \epsilon_3 < 1/2$

$$\sup_{\|\boldsymbol{w}\| \leq n^\eta} \max_{j \in \mathcal{J}_n} \|V_j \rho_{j,n}^{\boldsymbol{w}} V_j^* - \phi^{\boldsymbol{w}}\|_1 = O(n^{-1/4+\eta+\epsilon_3}) \tag{40}$$

over the set $\mathcal{J}_n = \{j \mid j_n - n^{1/2+\epsilon_3} \leq j \leq j_n + n^{1/2+\epsilon_3}\}$. The convergence is uniform over $\lambda \geq 1/2(1+\delta)$ for an arbitrary fixed $\delta > 0$.

The interpretation is that the block state $\rho_{j,n}^{\boldsymbol{w}}$ can be mapped by means of physical transformations (in this case an isometric embedding $T_j(\cdot) = V_j \cdot V_j^*$) into the Gaussian state $\phi^{\boldsymbol{w}}$ with vanishing norm-one error, uniformly over the unknown parameter $\boldsymbol{w}$ and over the block index j. A possible physical implementation is detailed in [20]; the ensemble of qubits is coupled with a Bosonic field such that the state is transferred to the field after some time.

In order to estimate the rotation parameters $\boldsymbol{w} = (u, v)$, one first maps the qubit state via the isometry V_j, and then performs a heterodyne measurement, which is optimal for estimating displacement (see Appendix A.3 for a description of the measurement). In the next section we discuss the Bures risk of the estimation procedure described above.

4 Upper and lower bounds for collective measurements

The overall two stages adaptive measurement procedure we propose can be briefly summarised as follows. The first stage is preliminary localisation step, where a vanishing number $\tilde{n}$ of copies of the state is used to localise the state ρ. The resulting estimate $\tilde{\rho}$ informs the choice of measurements in the second stage, and is used in defining the local parametrisation $\boldsymbol{\theta} = (\lambda, u, v)$ as described in the previous section. When $\tilde{\rho}$ is within a fixed ball of radius $\delta > 0$ around the fully mixed state, standard tomographic measurements are performed on the remaining copies of the state. However, if $\tilde{\rho}$ lies outside this ball, the measurements performed in second stage use techniques based on the principle of LAN to estimate the parameter vector $\boldsymbol{\theta} = (\lambda, u, v)$. In this section we look at the Bures risk of the measurement estimator pair $R(\rho, \hat{\rho}_n) := \mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2\right]$. As we will show below, the risk of a good estimators scales as $1/n$, and we would like to find asymptotic upper and lower bounds for the rescaled maximum risk

$$r_{max}(\hat{\rho}) = \limsup_{n \to \infty} \sup_{\rho \in \mathcal{S}_2} nR(\rho, \hat{\rho}_n).$$

4.1 The upper bound

We now make concrete our final estimator for the state ρ. The first stage involves using a vanishing number of copies $\tilde{n} := n^{1-\kappa}$ (with $\kappa > 0$) to get a rough estimate $\tilde{\rho}$. This estimate informs the

second measurement stage. The subsequent measurement stage differs depending on whether the state is estimated to be close to the fully mixed state.

Case 1. If the estimate $\tilde{\rho}$ lies in a small ball of radius $\delta > 0$ around the fully mixed state, then measurements in the standard σ_i, $i = x, y, z$ basis are performed on $(n - \tilde{n})/3$ copies of the state. The outcomes of each measurement are ± 1, and the associated probabilities are $p(\pm 1 | \sigma_i) = p_i(\pm 1) := \mathrm{Tr}(\rho P_i^{\pm 1})$, where the projectors $P_i^{\pm 1}$ are defined via $\sigma_i = P_i^{+1} - P_i^{-1}$. The total number n_i of $+1$ outcomes obtained by $n/3$ measurements of σ_i is binomially distributed $B_{n/3, p_i(+1)}(n_i)$. The final estimate of the state is constructed as the maximum likelihood (ML) estimate from these measurement outcomes

$$\hat{\rho}_n = \arg\max_{\tau \in \mathcal{S}_2} \sum_{i=x,y,z} n_i \log \mathrm{Tr}(\tau P_i^{+1}) + (n/3 - n_i) \log \mathrm{Tr}(\tau P_i^{-1}) \tag{41}$$

where the maximisation is over the space of all 2×2 density matrices $\mathcal{S}_2$.

Case 2. On the other hand, if the preliminary estimate $\tilde{\rho}$ lies away from the fully mixed state, we perform the following measurements to estimate the parameter vector $\boldsymbol{\theta} = (\lambda, u, v)$. A 'which block' measurement outputs a value of j from which the eigenvalue λ is estimated, cf. section 3.2. Similarly to the separate measurements strategy, we consider the following 'add-beta' estimator for the eigenvalue λ [22, 23]

$$\hat{\lambda}_n = \begin{cases} \frac{1/2}{n+5/4}, & \frac{n}{2} - j = 0, \\ \frac{2}{n+7/4}, & \frac{n}{2} - j = 1, \\ \frac{n/2-j+3/4}{n+3/2}, & \frac{n}{2} - j = 2, \ldots, n-2, \\ \frac{n-1/4}{n+7/4}, & \frac{n}{2} - j = n-1, \\ \frac{n+3/4}{n+5/4}, & \frac{n}{2} - j = n \end{cases} \tag{42}$$

The range of possible values of j is $[0, n/2]$, and therefore only some of the rules of the estimator described above are used. However, we describe the estimator over the range $[0, n]$ as this will be used shortly to upper bound the minimax risk.

Conditional on j, we are left with the block state $\rho_{j,n}^{\boldsymbol{w}}$. Using Theorem 1 we can isometrically map this state onto the Fock space, close to the Gaussian state $\phi^{\boldsymbol{w}}$. In order to estimate the displacement parameter $\boldsymbol{w}$ we perform a heterodyne measurement with outcome $\hat{\boldsymbol{w}}_n$ (see Appendix A.3 for a description of the measurement). The final estimate of our the state $\hat{\rho}_n$ is constructed from the estimated parameter vector $\hat{\boldsymbol{\theta}}_n = (\hat{\lambda}_n, \hat{\boldsymbol{w}}_n)$ as

$$\hat{\rho}_n = U\left(\frac{\hat{\boldsymbol{w}}_n}{\sqrt{n}}\right) \begin{pmatrix} 1 - \hat{\lambda}_n & 0 \\ 0 & \hat{\lambda}_n \end{pmatrix} U\left(\frac{\hat{\boldsymbol{w}}_n}{\sqrt{n}}\right)^*. \tag{43}$$

We now state precisely the upper bound for the minimax risk of the Bures distance for the measurement strategy described above.

15

Theorem 2. *Let $\hat{\rho}_n$ be the estimator described above. The asymptotic rescaled maximum risk is bounded from above as*

$$\limsup_{n\to\infty} \sup_{\rho} nR(\rho, \hat{\rho}_n) \leq \frac{3}{2}. \tag{44}$$

The proof of this theorem is detailed in the appendix (A.3), and here we only provide an outline of the arguments. The choice of measurements in the second stage depend on whether the preliminary estimate $\tilde{\rho}$ lies inside or outside a small ball of radius $\delta > 0$ around the fully mixed state. In keeping with this, let us therefore denote $\hat{\rho}_n^1$ as the estimator (41) chosen when $|\tilde{r}| \leq \delta$, and let $\hat{\rho}_n^2$ be the LAN based estimator (43), when $|\tilde{r}| > \delta$. The minimax risk can then be bounded from above as follows

$$\limsup_{n\to\infty} \sup_{\rho} nR(\rho, \hat{\rho}_n) \leq \max \left\{ \limsup_{n\to\infty} \sup_{\rho\in B_1} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2 \big| |\tilde{r}| \leq \delta \right], \right.$$

$$\left. \limsup_{n\to\infty} \sup_{\rho\notin B_2} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^2)^2 \big| |\tilde{r}| > \delta \right] \right\} \tag{45}$$

where B_1 and B_2 are balls of radius $\delta + n^{-1/2+\epsilon_2}$ and $\delta - n^{-1/2+\epsilon_2}$ respectively. The two terms are evaluated explicitly in section (A.3) of the appendix. The term corresponding to the estimator $\hat{\rho}_n^1$ is straightforward to evaluate as the Bures distance is locally quadratic for states in B_1. From this quadratic expansion and the efficiency of the maximum likelihood estimator in the asymptotic regime, the risk can be expressed as

$$\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2 \right] \approx \frac{1}{n}\text{Tr}\left(I(\rho)^{-1}G \right) \tag{46}$$

where G is the weight matrix reconstructing the quadratic approximation of the Bures distance, and I is the Fisher information matrix. From the explicit form of G and I, the asymptotic risk can be bounded as

$$\limsup_{n\to\infty} \sup_{\rho\in B_1} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2 \right] \leq \frac{3}{4}\left(1 + \frac{\delta}{1-\delta} \right). \tag{47}$$

The other term in (45) corresponding to the estimator $\hat{\rho}_n^2$ uses the local parameterisation of states $\boldsymbol{\theta} = (\lambda, \boldsymbol{w})$, and the approximation of the Bures distance used in section 2, and detailed in the appendix (A.2). We therefore get that the risk can be bounded as

$$\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^2)^2 \right] \leq \mathbb{E}\left[D_H(\lambda, \hat{\lambda}_n)^2 + \frac{1}{4}\Phi^2 \right] + O(\Phi^4) \tag{48}$$

$$\leq \mathbb{E}\left[D_H(\lambda, \hat{\lambda}_n)^2 \right] + \frac{1}{n}\mathbb{E}\left[(u - \hat{u}_n)^2 + (v - \hat{v}_n)^2 \right] + O(n^{-2}) \tag{49}$$

The term corresponding to the rotation parameters has been evaluated in [20] using LAN based techniques. Since LAN holds in the limit of large n, the problem of estimating the rotation parameters is translated to one of determining the displacement of a Gaussian state $\phi^{\boldsymbol{w}}$. The heterodyne

measurement is known to be the optimal measurement in this case [20, 21]. The first term corresponding to the Hellinger risk is bounded from above by the Kullback-Leibler (KL) risk of estimating a binomial parameter λ from outcomes k distributed as $B_{n,\lambda}(k)$. The 'add-beta' estimator is known to be minimax optimal in this case, and its rate is known in the literature. Together with the LAN results for the rotation parameters, we bound risk as

$$\limsup_{n\to\infty} \sup_{\rho\notin B_2} nR(\rho, \hat{\rho}_n^2) \leq \limsup_{n\to\infty} \sup_{\lambda} n\mathbb{E}_{\text{Binom}}\left[D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)\right] + 1 \leq \frac{3}{2}. \tag{50}$$

Comparing this bound with (47), we arrive at the stated upper bound of $3/2$ in Theorem 2 provided $\delta < 1/2$.

4.2 The lower bound

In this section we derive a lower bound on the asymptotic rescaled risk with respect to the Bures distance. The key idea is to restrict the attention to a smaller state space region where the state is "hardest" to estimate, and evaluate the minimax risk over this region, thus obtaining a lower bound for the overall minimax risk.

Let us consider that the true state ρ lies in a local neighbourhood of size $n^{-1/2+\epsilon}$ around an arbitrary but fixed state ρ_0 as defined in equation (25), whose smallest eigenvalue satisfies $0 < \lambda_0 < 1/2$. For any estimation procedure $\hat{\rho}_n$ we have the lower bound for the maximum risk

$$
\begin{aligned}
\limsup_{n\to\infty} \sup_{\rho\in\mathcal{S}_2} nR(\rho, \hat{\rho}_n) &\geq \limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1\leq n^{-1/2+\epsilon}} nR(\rho, \hat{\rho}_n) \\
&\geq \limsup_{n\to\infty} \inf_{\hat{\rho}_n} \sup_{\|\rho-\rho_0\|_1\leq n^{-1/2+\epsilon}} nR(\rho, \hat{\rho}_n) \\
&:= r_{minmax}(\rho_0)
\end{aligned}
\tag{51}
$$

where the right side is the *local minimax* risk at ρ_0.

Since the state ρ_0 is taken to be away from the boundary of the Bloch sphere, we can parametrise its local neighbourhood using the local parameter $\boldsymbol{\theta} = (h, \mathbf{u})$

$$\rho = \rho_{\boldsymbol{\theta}} := U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right)\left(\begin{array}{cc} 1-\lambda_0-h/\sqrt{n} & 0 \\ 0 & \lambda_0+h/\sqrt{n} \end{array}\right)U\left(\frac{\boldsymbol{w}}{\sqrt{n}}\right)^*. \tag{52}$$

The Bures distance is locally quadratic

$$D_B(\rho_{\boldsymbol{\theta}}, \rho_{\boldsymbol{\theta}'})^2 = \frac{1}{n}(\boldsymbol{\theta}-\boldsymbol{\theta}')^T\Gamma_0(\boldsymbol{\theta}-\boldsymbol{\theta}') + O(n^{-3/2}) \tag{53}$$

where Γ_0 is the weight matrix

$$\Gamma_0 = \begin{pmatrix} \frac{1}{4\lambda_0(1-\lambda_0)} & 0 & 0 \\ 0 & (1-2\lambda_0)^2 & 0 \\ 0 & 0 & (1-2\lambda_0)^2 \end{pmatrix}. \tag{54}$$

17

In this case we can apply the LAN theory [20] to obtain the local minimax risk for Bures distance. The upshot of the theory is that the classical statistical model given by the distribution over blocks (cf. equation (31)) can be approximated by a one-dimensional Gaussian model $N(h, v_0)$ with fixed variance $v_0 = \lambda_0(1 - \lambda_0)$ and mean equal to the unknown local parameter h. Additionally, the quantum statistical model described by the quantum state of the irreducible block can be approximated by a quantum Gaussian shift model (independent of the classical one), as described in Theorem 1. The optimal measurement here is the heterodyne, and after rescaling by a constant factor we obtain the unbiased estimator $\hat{\mathbf{u}}$ which has a two-dimensional Gaussian distribution $\hat{\mathbf{u}} \sim N(\mathbf{u}, w_0 \cdot I_2)$ with $w_0 = (1 - \lambda_0)/(2(1 - 2\lambda_0)^2)$. The local minimax risk is the sum of the contribution from the classical and respectively the quantum part of the Gaussian model, weighted with the matrix Γ_0

$$
\begin{aligned}
R_{minmax}(\rho_0) &= \Gamma_{00}\mathbb{E}[(\hat{h} - h)^2] + \Gamma_{11}\mathbb{E}[(\hat{u} - u)^2] + \Gamma_{22}\mathbb{E}[(\hat{v} - v)^2] \\
&= \frac{1}{4\lambda_0(1 - \lambda_0)}v_0 + 2(1 - 2\lambda_0)^2 w_0 = \frac{1}{4} + (1 - \lambda_0) = \frac{5}{4} - \lambda_0. \quad (55)
\end{aligned}
$$

As the state ρ_0 defining the local neighbourhood is chosen arbitrarily, we see that the right side of the above equation achieves its maximum as $\lambda_0 \to 0$, and we therefore get the asymptotic lower bound for the rescaled maximum risk of any estimator.

$$
\limsup_{n \to \infty} \sup_{\rho \in \mathcal{S}_2} nR(\rho, \hat{\rho}_n) \geq \frac{5}{4}.
$$

As expected, the above lower bound is smaller than the $3/2$ upper bound derived in section 4.1.

5   The minimax optimal estimator

In deriving the minimax bounds for both the proposed estimators, the key observation was that the Bures risk decomposes locally into contributions from the Hellinger risk of estimating the eigenvalue parameter λ and a quadratic risk corresponding to the estimation of the rotation parameters (see (11) and appendix A.2). The Hellinger risk was then bounded from above by the Kullback-Leibler (KL) risk of estimating the binomial parameter. The estimator of the binomial parameter achieving the minimax rate for the KL risk is known to be 'add-beta' estimator, and both the local and global estimators for the state ρ proposed use this estimator for the eigenvalue parameter, cf. equations (8) and (42) .

The reason why we were not able to prescribe an asymptotically minimax estimator is that we could not devise a minimax estimator for the binomial parameter λ, with respect to the Hellinger distance. The following proposition follows immediately from the asymptotic analysis of section 4 and shows that the original optimal state estimation problem reduces to the 'classical' one of estimating the binomial parameter λ, which for the moment remains an open problem.

Proposition 1. *Let $\hat{\lambda}_{opt}$ be an asymptotically minimax estimator of the binomial parameter λ under the Hellinger loss function. Then a state estimator defined by replacing the 'add-beta' estimators for λ in equation (42) with $\hat{\lambda}_{opt}$ is asymptotically minimax optimal for qubit states.*

Although we were not able to devise a minimax estimator under the Hellinger distance, we would like to make some comments on this problem, emphasising that it is crucial to study what happens at the boundary when $\lambda \approx 0$. Indeed, for values of λ away from this boundary, the local asymptotic minimax rate is easily derived as the squared Hellinger distance square is locally quadratic and the classical asymptotic efficiency theory [25] applies. The standard estimator $\hat{\lambda} = k/n$ is a natural first choice as it is unbiased and achieves the Cramer Rao lower bound with variance $\mathrm{Var}(\hat{\lambda}) = (nI)^{-1}$, where $I = \frac{1}{\lambda(1-\lambda)}$ is the Fisher information. In the region where $\lambda > 0$, using a locally quadratic approximation for the Hellinger risk, we have

$$\mathbb{E}_{\mathrm{Binom}}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})^2\right] = \frac{1}{4\lambda(1-\lambda)}\mathrm{Var}(\hat{\lambda}) + o(n^{-1}) = \frac{1}{4n} + o(n^{-1}).$$

This holds for every *fixed* $\lambda \in (0, 1/2]$, and gives the same rate as the one in the lower bound (55). However the convergence is not uniform over λ close to the zero, which affects the constant in the asymptotic maximum risk. To see this, consider the case when λ is n-dependent such that $n\lambda \to \mu$, with $\mu > 0$ being a fixed constant. The Hellinger risk is given by

$$\mathbb{E}_{\mathrm{Binom}}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})^2\right] = \mathbb{E}_{\mathrm{Binom}}\left[\left(\hat{\lambda}^{1/2} - \lambda^{1/2}\right)^2\right] + \mathbb{E}_{\mathrm{Binom}}\left[\left((1-\hat{\lambda})^{1/2} - (1-\lambda)^{1/2}\right)^2\right]. \quad (56)$$

The second term on the right in the above equation is bounded as

$$\mathbb{E}_{\mathrm{Binom}}\left[\left((1-\hat{\lambda})^{1/2} - (1-\lambda)^{1/2}\right)^2\right] \leq \mathbb{E}_{\mathrm{Binom}}\left[(\lambda - \hat{\lambda})^2\right]/(1-\lambda) = \mu/n^2. \quad (57)$$

Substituting (57) in (56), we have

$$\mathbb{E}_{\mathrm{Binom}}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})^2\right] = \mathbb{E}_{\mathrm{Binom}}\left[(\hat{\lambda}^{1/2} - \lambda^{1/2})^2\right] + O(n^{-2}) \qquad (58)$$

$$= \frac{1}{n}\mathbb{E}_{\mathrm{Po}(\mu)}\left[\left(K^{1/2} - \mu^{1/2}\right)^2\right] + O(n^{-2}) \qquad (59)$$

In the last equality we used the fact that under the scaling $n\lambda \to \mu$, the Binomial random variable converges to a Poisson random variable $K \sim \mathrm{Po}(\mu)$. Therefore the risk in this case is given by the function $R(\mu) = \mathbb{E}_{\mathrm{Po}(\mu)}\left[\left(K^{1/2} - \mu^{1/2}\right)^2\right]$, where the expectation is taken with respect to the Poisson distribution with parameter μ. If this function was bounded such that $R(\mu) \leq 1/4$, then it would suggest that the standard estimator $\hat{\lambda}$ might be globally asymptotically minimax. However, plotting the function $R(\mu)$ numerically, we see from Figure 1 that it attains a maximum value of $\max R(\mu) \approx 0.455$ around $\mu = 1.11$, and converges to $1/4$ for large values of μ which corresponds
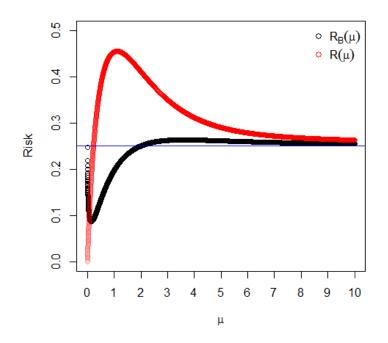
19

Figure 1: Plots of the Hellinger risk functions $R(\mu)$ and $R_B(\mu)$ for various values of the Poisson parameter μ. The horizontal blue line marks a value of 1/4. See main text for details.

to λ away from zero. This shows that the standard estimator doesn't achieve a minimax constant of $1/4$ for all λ, and illustrates that the difficulty in deriving a minimax rate for the Hellinger distance lies in the Poisson range.

As an alternative to the standard estimator, we consider the Bayes estimator $\hat{\mu}_B^{1/2}$ for $\mu^{1/2}$, and plot numerically the 'frequentist' risk of this estimator $R_B(\mu) := \mathbb{E}_\mu \left[(\hat{\mu}_B^{1/2} - \mu^{1/2})^2 \right]$. We now describe the Bayes estimator $\hat{\mu}_B^{1/2}$ of the Poisson parameter. It is known that a conjugate family for the Poisson model is the Gamma family of priors, i.e

$$\mu \sim f_{\alpha,\beta}(t) = \frac{t^{\alpha-1} \exp\left(-t/\beta\right)}{\beta^\alpha \Gamma(\alpha)}, \quad t > 0 \tag{60}$$

where α, β are the shape and scale parameters respectively. Given an outcome $K = k$ from the Poisson distribution $\text{Po}(\mu)$, the posterior distribution for μ is easily calculated to be $\Gamma(\alpha + k, \frac{\beta}{\beta+1})$. The Bayes estimator is then the expectation of $\sqrt{\mu}$ taken with respect to the posterior distribution.

20

This is easily calculated to be

$$\hat{\mu}_B^{1/2} := \frac{\Gamma(k + \alpha + 1/2)}{\Gamma(k + \alpha)} \left(\frac{\beta}{\beta + 1}\right)^{1/2} \tag{61}$$

In Figure 1, we plot the 'frequentist' risk $R_B(\mu)$ for the Bayes estimate (61) under a particular prior with $\alpha = 0.41$ and $\beta = 200$ (chosen for its favourable maximum risk), and a range of values for μ. We see that the risk remains upper-bounded by a value only slightly greater than 1/4, and for large values of μ the risk tends to a limiting value of $1/4$. This supports the conjecture that the minimax constant for the Hellinger distance is $1/4$.

6   Quantum Relative Entropy

In our derivation of the minimax upper bounds, we bounded the Hellinger risk of estimating the eigenvalues by the Kullback-Leibler (KL) risk for which the asymptotic minimax rate is known. As the KL distance is the classical analogue of the quantum relative entropy $S(\rho\|\rho') = \mathrm{Tr}[\rho(\log\rho - \log\rho')]$, a question naturally arises - can the techniques used in this paper be applied to derive the minimax rate for the quantum relative entropy (QRE)? A key element would be to decompose the QRE locally. Similar to decomposition of the Bures distance in (11), the QRE risk can be shown to locally decompose into a sum of contributions from the KL risk and a term involving the 'rotation parameters' . For qubit states, the QRE between the state ρ and the estimate $\hat{\rho}_n$ is represented in terms of the Bloch vectors as [26]

$$S(\rho\|\hat{\rho}_n) = \frac{1}{2}\left[\log\left(1 - |\boldsymbol{r}|^2\right) - \log\left(1 - |\hat{\boldsymbol{r}}_n|^2\right) + |\boldsymbol{r}|\log\left(\frac{1 + |\boldsymbol{r}|}{1 - |\boldsymbol{r}|}\right)\right.$$
$$\left. - |\boldsymbol{r}|\cos\Phi\log\left(\frac{1 + |\hat{\boldsymbol{r}}_n|}{1 - |\hat{\boldsymbol{r}}_n|}\right)\right] \tag{62}$$

where Φ is the angle between the Bloch vectors of the two states. This can be rewritten as

$$\begin{aligned} S(\rho\|\hat{\rho}_n) &= D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n) + \frac{1 - 2\lambda}{2}(1 - \cos\Phi)\log\left(\frac{1 - \hat{\lambda}_n}{\hat{\lambda}_n}\right) \\ &= D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n) + \frac{1 - 2\lambda}{4}(\Phi^2 + O(\Phi^4))\log\left(\frac{1 - \hat{\lambda}_n}{\hat{\lambda}_n}\right) \end{aligned} \tag{63}$$

where $D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})$ is the Kullback-Leibler distance between the two distributions $\boldsymbol{\lambda} = (\lambda, 1 - \lambda)$ and $\hat{\boldsymbol{\lambda}} = (\hat{\lambda}, 1 - \hat{\lambda})$, and in the second equality we expanded the cosine term to leading order in Φ. The proof of this decomposition can be found in appendix A.4.

We will show that the global estimator discussed in section 4 achieves the rate $O(n^{-1}\log n)$ and no estimator can achieve faster rates, in particular the 'standard' rate n^{-1}.

21

Consider the estimator defined by equations (42) and (43), and note that the classical component estimator $\hat{\lambda}_n$ is the minimax optimal estimator for the binomial model and is always larger than c/n for some fixed constant $c > 0$. Using the same arguments as in Theorem 2 we find

$$\sup_\rho \mathbb{E}[D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)] = O(n^{-1}).$$

On the other hand, since $\hat{\lambda}_n \geq c/n$, the second term in equation (63) is bounded by $c' \log n(\Phi^2 + O(\Phi^4))$; since Φ is estimated at standard rate, the second term is therefore upper bounded as

$$\sup_\rho \mathbb{E}\left[\frac{1-2\lambda}{4}(\Phi^2 + O(\Phi^4)) \log\left(\frac{1-\hat{\lambda}_n}{\hat{\lambda}_n}\right)\right] = O(n^{-1}\log n)$$

which determines the rate.

We will now show that no estimator can have maximum risk converging faster that $n^{-1}\log n$. Since we are interested in the maximum risk, we will set $\lambda = 0$ (pure states), and show that the risk cannot decrease faster that $n^{-1}\log n$ even if we know that the state is pure! As a consequence of local asymptotic normality, any estimator will have the property that $\mathbb{P}[1 - \cos\Phi \geq c/n] \geq \epsilon$ for some constants c, ϵ. Therefore we will consider the contribution to the risk conditional on $1 - \cos\Phi \geq c/n$. By expanding the $D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}})$ term we have

$$S(\rho\|\hat{\rho}_n) \geq \log\frac{1}{1-\hat{\lambda}_n} + \frac{c}{4n}\log\left(\frac{1-\hat{\lambda}_n}{\hat{\lambda}_n}\right). \tag{64}$$

However, the righthand side achieves its minimum at $\hat{\lambda}_n = c/4n$, so the risk is larger than $c'\log n/n$. This shows that the minimax risk for the quantum relative entropy scales as $\log n/n$.

7 Conclusion

In this paper we proposed two adaptive estimators for the qubit mixed state, one based on local measurements and the other on collective global measurements. In section 2 we upper-bounded the minimax Bures distance risk for the estimator based on local measurements and showed that it scales as $1/n$. In section 3, we proposed an estimator based on collective measurements and used LAN theory to obtain upper and lower bounds for the risk of $3/2n$ and $5/4n$ respectively. A key element in obtaining the upper bounds was the local decomposition of the Bures risk into contributions from the Hellinger risk of estimating the eigenvalue, and a quadratic contribution from the risk of estimating the 'rotation parameters'. While the contribution to the Bures risk from the 'rotation terms' is easily shown to scale as $O(1/n)$, we noticed that the difficulty in establishing minimax results for the Bures distance is encapsulated in the challenges of establishing minimax results for the Hellinger risk. Finally in section 5, we considered these challenges and proposed that

a minimax optimal estimator for the mixed qubit state ρ is immediately obtained given a minimax optimal estimator for the binomial parameter under the Hellinger loss function.

We also briefly considered the derivation of minimax bounds for the quantum relative entropy (QRE) risk. We derived a local decomposition of the QRE similar to the one obtained for the Bures distance, and demonstrated that the global estimator proposed achieves a rate of $O(n^{-1} \log n)$. We also showed that no estimator can achieve faster rates and established that the minimax QRE risk scales as $O(n^{-1} \log n)$.

Directions for future work include generalise the results presented in this paper to the multi-qubit case, and to investigate the minimax rate for the Hellinger distance under the binomial/multinomial distributions. Another topic of interest would be to study the behaviour of the maximum Bures risk in the case when the measurement outcomes are noisy. In particular, it has been pointed out in [4] that in the case of the noisy coin, a maximum risk of $O(n^{-1/2})$ is intrinsic to the setup and in fact unavoidable. This is of relevance to the study of the maximum Bures risk in the noisy measurement scenario as locally the 'classical' component of the Bures risk is given by the Hellinger risk of estimating the bias of a coin.

Acknowledgements

References

[1] Haffner H, Hansel W, Roos C F, Benhelm J, Chek-al kar D, Chwalla M, Korber T, Rapol U D, Riebe M, Schmidt P O, Becher C, Guhne O, Dur W and Blatt R 2005 *Nature* 643–646

[2] Mahler D H, Rozema L A, Darabi A, Ferrie C, Blume-Kohout R and Steinberg A M 2013 *Phys. Rev. Lett.* **111**(18) 183601

[3] Acharya A and Guţă M 2017 *Journal of Physics A: Mathematical and Theoretical* **50** 195301

[4] Ferrie C and Blume-Kohout R 2012 *AIP Conf. Proc.* **1443** 14–21

[5] Ferrie C and Blume-Kohout R 2016 *Phys. Rev. Lett.* **116** 090407

[6] Gill R D and Massar S 2000 *Phys. Rev. A* **61**(4) 042312

[7] Řeháček J, Englert B G and Kaszlikowski D 2004 *Phys. Rev. A* **70**(5) 052321

[8] Bagan E, Ballester M A, Gill R D, Muñoz Tapia R and Romero-Isart O 2006 *Phys. Rev. Lett.* **97**(13) 130501

[9] Hou Z, Zhu H, Xiang G Y, Li C F and Guo G C 2016 *Npj Quantum Information* **2** 16001 EP

[10] Okamoto R, Iefuji M, Oyama S, Yamagata K, Imai H, Fujiwara A and Takeuchi S 2012 *Phys. Rev. Lett.* **109**(13) 130404

[11] Fujiwara A 2006 *Journal of Physics A: Mathematical and General* **39** 12489

[12] Ferrie C 2014 *Phys. Rev. Lett.* **113**(19) 190404

[13] Fischer D G, Kienle S H and Freyberger M 2000 *Phys. Rev. A* **61**(3) 032306

[14] Granade C, Ferrie C and Flammia S T 2016 *arXiv:1605.05039*

[15] Hannemann T, Reiss D, Balzer C, Neuhauser W, Toschek P E and Wunderlich C 2002 *Phys. Rev. A* **65**(5) 050303

[16] Kravtsov K S, Straupe S S, Radchenko I V, Houlsby N M T, Huszár F and Kulik S P 2013 *Phys. Rev. A* **87**(6) 062122

[17] Straupe S S 2016 *JETP Letters* **104** 510–522 ISSN 1090-6487

[18] Bagan E, Ballester M A, Gill R D, Monras A and Muñoz Tapia R 2006 *Phys. Rev. A* **73**(3) 032301

[19] Bagan E, Baig M, Muñoz Tapia R and Rodriguez A 2004 *Phys. Rev. A* **69**(1) 010304

[20] Guţă M, Janssens B and Kahn J 2008 *Communications in Mathematical Physics* **277** 127–160

[21] Guţă M and Kahn J 2006 *Phys. Rev. A* **73**(5) 052108

[22] Braess D and Dette H 2004 *Sankhyā: The Indian Journal of Statistics (2003-2007)* **66** 707–732 ISSN 09727671

[23] Braess D and Sauer T 2004 *Journal of Approximation Theory* **128** 187 – 206 ISSN 0021-9045

[24] Cirac J I, Ekert A K and Macchiavello C 1999 *Phys. Rev. Lett.* **82**(21) 4344–4347

[25] Young G A and Smith R L 2005 *Essentials of statistical inference* (Cambridge University Press)

[26] Cortese J A 2003 *Quantum Information Theory: Classical Communication over Quantum Channels* Ph.D. thesis California Institute of Technology Pasadena, California

A   Appendix

A.1   Proof of Lemma 2

The proof is a straightforward application of Hoeffding's inequality.

Theorem 3 (Hoeffding's inequality). *Let $R_1, \ldots, R_m$ be independent random variables with $a_i \leq R_i \leq b_i$. Let $S = \sum_{i=1}^{m} R_i$, and $\mu = \mathbb{E}[S]$. Then for all $t > 0$*

$$\mathbb{P}\left(|S - \mu| \geq nt\right) \leq 2 \exp^{-2n^2 t^2 / \sum_i (b_i - a_i)}. \tag{65}$$

We have $X_i \in [-1, 1]$, and $\mathbb{E} \sum_i X_i = \frac{\tilde{n}}{3} r_x$. Applying Hoeffding's inequality we get

$$\mathbb{P}\left(\left|\frac{3}{\tilde{n}} \sum_i X_i - r_x\right|^2 \geq t^2\right) \leq 2 \exp^{-2t^2 \tilde{n}/3} \tag{66}$$

and similarly for the other spin components. Applying the three inequalities together, with $t^2 = n^{2\epsilon_2} - 1$ and $\epsilon_2 > 0$, we have

$$\mathbb{P}\left(\sum_{j=x,y,z} |r'_j - r_j|^2 \geq 3n^{2\epsilon_2 - 1}\right) \leq 6 \exp^{-2\tilde{n} n^{2\epsilon_2 - 1}/3}. \tag{67}$$

The estimate $\tilde{\rho}$ is then the closest state in trace distance to the matrix $\frac{1}{2}(\mathbb{1} + \boldsymbol{r}' \cdot \boldsymbol{\sigma})$. As $\|\rho - \tilde{\rho}\|_1^2 = \sum_{i=x,y,z} |\tilde{r}_i - r_i|^2$, (67) implies the stated bound.

$\square$

A.2 Expansion of the Bures distance

Here we derive the expansion (11) of the Bures distance $D_B(\rho, \rho')^2 := 2\left[1 - \sqrt{F(\rho, \rho')}\right]$. We know that for qubits the fidelity between two states can be expressed in terms of the Bloch vectors as

$$F(\rho, \rho') := \frac{1}{2}\left(1 + \sqrt{1 - |\mathbf{r}|^2}\sqrt{1 - |\mathbf{r}'|^2} + \mathbf{r} \cdot \mathbf{r}'\right)$$
$$= \frac{1}{2}\left(1 + \sqrt{1 - |\mathbf{r}|^2}\sqrt{1 - |\mathbf{r}'|^2} + |\mathbf{r}||\mathbf{r}'|\cos\Phi\right)$$

where Φ is the angle between the Bloch vectors. For two sufficiently close states, the angle Φ is small and the cosine term can be expanded as

$$F(\rho, \rho') = \frac{1}{2}\left(1 + \sqrt{1 - |\mathbf{r}|^2}\sqrt{1 - |\mathbf{r}'|^2} + |\mathbf{r}||\mathbf{r}'| - \frac{|\mathbf{r}||\mathbf{r}'|}{2}\Phi^2 + \frac{|\mathbf{r}||\mathbf{r}'|}{24}\Phi^4\right)$$
$$= \left(\sqrt{(1-\lambda)(1-\lambda')} + \sqrt{\lambda\lambda'}\right)^2 - \frac{|\mathbf{r}||\mathbf{r}'|}{4}\Phi^2 + \frac{|\mathbf{r}||\mathbf{r}'|}{24}\Phi^4$$

where we have use the fact that $|\mathbf{r}| = 1 - 2\lambda$. Therefore the Bures distance is given by

$$D_B(\rho, \rho')^2 = 2\left[1 - \sqrt{\left(\sqrt{(1-\lambda)(1-\lambda')} + \sqrt{\lambda\lambda'}\right)^2 - \frac{|\mathbf{r}||\mathbf{r}'|}{4}\Phi^2 + \frac{|\mathbf{r}||\mathbf{r}'|}{24}\Phi^4}\right]$$

$$= 2\left[1 - \left(\sqrt{(1-\lambda)(1-\lambda')} + \sqrt{\lambda\lambda'}\right) + \frac{1}{8}\frac{|\mathbf{r}||\mathbf{r}'|}{\sqrt{(1-\lambda)(1-\lambda')} + \sqrt{\lambda\lambda'}}\Phi^2 + O(\Phi^4)\right]$$

$$= D_H(\boldsymbol{\lambda}, \boldsymbol{\lambda}')^2 + \frac{1}{4}\frac{(1-2\lambda)(1-2\lambda')}{\sqrt{(1-\lambda)(1-\lambda')} + \sqrt{\lambda\lambda'}}\Phi^2 + O(\Phi^4)$$

where $D_H(\boldsymbol{\lambda}, \boldsymbol{\lambda}')^2$ is the Hellinger distance between the binary distributions $\boldsymbol{\lambda} = (\lambda, 1 - \lambda)$ and $\boldsymbol{\lambda}' = (\lambda', 1 - \lambda')$.

$\square$

A.3   Proof of Theorem 2

Since the first measurement stage is the localisation of the true state by the estimate $\tilde{\rho}$, we write the risk as a sum of two terms

$$R(\rho, \hat{\rho}_n) = \mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2\right]$$
$$= \mathbb{P}\left(|\tilde{r}| \leq \delta\right) \cdot \mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2 \mid |\tilde{r}| \leq \delta\right] + \mathbb{P}\left(|\tilde{r}| > \delta\right) \cdot \mathbb{E}\left[D_B(\rho, \hat{\rho}_n)^2 \mid |\tilde{r}| > \delta\right] \quad (68)$$

The expectation is taken over the measurement outcomes given the true state ρ. The final estimate $\hat{\rho}_n$ is defined by either (41) or (43) depending on the preliminary estimate $\tilde{\rho}$. Specifically, if the estimate $\tilde{\rho}$ is within a ball of radius $\delta > 0$ of the fully mixed state, we perform standard tomographic measurements on the remaining copies of the state. The final estimate is then the maximum likelihood (ML) estimate given by (41). While in the other instance the technology of LAN is utilised and the final estimate is (43). In order to make the difference between the two estimators explicit, we let $\hat{\rho}_n^1$ denote the final estimator in the case when $|\tilde{r}| \leq \delta$ and $\hat{\rho}_n^2$ be the final estimate when $|\tilde{r}| > \delta$. Therefore, we have

$$R(\rho, \hat{\rho}_n) = \mathbb{P}\left(|\tilde{r}| \leq \delta\right) \cdot \mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2 \mid |\tilde{r}| \leq \delta\right] + \mathbb{P}\left(|\tilde{r}| > \delta\right) \cdot \mathbb{E}\left[D_B(\rho, \hat{\rho}_n^2)^2 \mid |\tilde{r}| > \delta\right]$$
$$= R_1 + R_2. \quad (69)$$

We consider the contribution to the risk from the term R_1 first. Let B_1 be a ball of radius $\delta + n^{-1/2+\epsilon_2}$ around the centre of the Bloch sphere. When the true state $\rho \notin B_1$, we note that the probability $\mathbb{P}\left(|\tilde{r}| \leq \delta\right)$ goes to zero exponentially fast in n. This is because the estimate $\tilde{\rho}$ lies within a ball of radius $O(n^{-1/2+\epsilon_2})$ around the true state with high probability (Lemma 2). This along with the fact that the Bures distance is bounded as $D_B(\sigma, \pi) \leq 2$ for any pair of density matrices σ, π implies that when $\rho \notin B_1$, the term R_1 can be neglected. However, when $\rho \in B_1$,

the term R_1 has a non zero contribution and is written as

$$R_1 = \begin{cases} \mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2 \middle| |\tilde{r}| \leq \delta\right] \cdot \mathbb{P}\left(|\tilde{r}| \leq \delta\right), & \rho \in B_1 \\ o(1) & \rho \notin B_1 \end{cases} \tag{70}$$

The term R_2 can be treated similarly. Let B_2 be a ball of radius $\delta - n^{-1/2+\epsilon_2}$ around the centre of the Bloch sphere. As the probability $\mathbb{P}(|\tilde{r}| > \delta)$ decays exponentially if $\rho \in B_2$, the term R_2 is relevant only when $\rho \notin B_2$

$$\begin{cases} R_2 = \mathbb{E}\left[D_B(\rho, \hat{\rho}_n^2)^2 \middle| |\tilde{r}| > \delta\right] \cdot \mathbb{P}\left(|\tilde{r}| > \delta\right), & \rho \notin B_2 \\ o(1) & \rho \in B_2 \end{cases} \tag{71}$$

Substituting (70), (71) in (69) we see that the minimax risk is bounded from above as

$$\limsup_{n\to\infty} \sup_{\rho} nR(\rho, \hat{\rho}_n) \leq \limsup_{n\to\infty} \max\left\{ \sup_{\rho \in B_1} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2 \middle| |\tilde{r}| \leq \delta\right], \right.$$
$$\left. \sup_{\rho \notin B_2} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^2)^2 \middle| |\tilde{r}| > \delta\right] \right\} \tag{72}$$

Case 1 : $\rho \in B_1$ and $|\tilde{r}| \leq \delta$

We now evaluate the risk when the state ρ is in B_1 while the estimate $\tilde{\rho}$ is within a ball of radius $\delta > 0$ around the fully mixed state. The final estimate $\hat{\rho}_n^1$ is the ML estimate and given by (41). The outcomes from the $n/3$ repeated measurements in a setting σ_i are i.i.d, this implies that the ML estimate of the Bloch vector parameters r_x, r_y, r_z from the outcomes of the standard tomographic measurements are asymptotically Gaussian in distribution

$$\lim_{n\to\infty} \sqrt{n}(\hat{r}_i - r_i) = \mathcal{N}(0, I(\rho)^{-1}), \qquad i = x, y, z \tag{73}$$

where the covariance matrix is the inverse of the Fisher information matrix $I(\rho)$. The elements of the matrix $I(\rho)$ are defined for each $i, j \in \{x, y, z\}$ as

$$I(\rho)_{i,j} = \frac{1}{(1 + r_i)(1 - r_i)} \delta_{i,j} \tag{74}$$

The local expansion of the Bures distance for states away from the boundary of the Bloch sphere is quadratic in the Bloch vector components

$$D_B(\rho, \hat{\rho}_n^1)^2 = (\boldsymbol{r} - \hat{\boldsymbol{r}})^T G(\boldsymbol{r} - \hat{\boldsymbol{r}}) + O(\|\boldsymbol{r} - \hat{\boldsymbol{r}}\|^3) \tag{75}$$

where G is the weight matrix of the Bures distance

$$G_{j,k} := \frac{1}{4}\left(1 + \frac{r_i^2}{(1 - |r|^2)}\right)\delta_{j,k}.$$

27

The asymptotic behaviour of the ML estimator (41) together with this local expansion of the Bures distance, implies that the risk of the ML estimate scales as follows for large n

$$\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2\right] = \frac{1}{n}\text{Tr}\left(I(\rho)^{-1}G\right) + o(n^{-1}) \tag{76}$$

It is easy to see that $I(\rho) \geq \mathbb{1}$, and therefore we have that asymptotically the minimax Bures risk is upper bounded by

$$\limsup_{n\to\infty} \sup_{\rho\in B_1} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^1)^2\right] \leq \frac{3}{4}\left(1 + \frac{\delta}{1-\delta}\right) \tag{77}$$

where we used the fact that $|r| \leq \delta + O(n^{-1/2+\epsilon_2})$.

Case 2: $|\tilde{r}| > \delta$, $\rho \notin B_2$

We now consider the case when $\tilde{\rho}$ is away from the fully mixed state. Since the state $\tilde{\rho}$ is within the ball of radius $O(n^{-1/2+\epsilon_2})$ of the true state $\rho \notin B_2$, we consider the local parametrisation of the states $\boldsymbol{\theta} = (\lambda, \boldsymbol{w})$, and perform the secondary measurements on the joint state $\rho_n^{\boldsymbol{\theta}} = \rho_{\boldsymbol{\theta}}^{\otimes n}$ of n qubits. Using the approximation of the Bures distance in (11), the risk is expressed as

$$\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^2)^2\right] = \mathbb{E}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)^2 + \frac{1}{4}\frac{(1-2\lambda)(1-2\hat{\lambda}_n)}{\left(\sqrt{(1-\lambda)(1-\hat{\lambda}_n)} + \sqrt{\lambda\hat{\lambda}_n}\right)^2}\Phi^2\right] + O(n^{-2})$$

$$\leq \mathbb{E}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)^2\right] + \frac{1}{n}\mathbb{E}\left[(u-\hat{u}_n)^2 + (v-\hat{v}_n)^2\right] + O(n^{-2}).$$

The second term on the right corresponding to the rotation parameters has been evaluated in [20]. Since LAN holds in the limit of large n, the problem of estimating the rotation parameters is translated to one of determining the displacement of a Gaussian state $\phi^{\boldsymbol{w}}$. The heterodyne measurement is known to be the optimal measurement in this case [20,21]. This measurement along with a possible physical implementation is detailed in [20]. Here we only note that a heterodyne measurement involves the joint measurement of the quadratures $\boldsymbol{Q}_1 := (\boldsymbol{Q}+\boldsymbol{Q}_v)/\sqrt{2}$ and $\boldsymbol{P}_2 := (\boldsymbol{P}-\boldsymbol{P}_v)/\sqrt{2}$, such that $[\boldsymbol{Q}_1, \boldsymbol{P}_2] = 0$. Where $\boldsymbol{Q}_v$ and $\boldsymbol{P}_v$ are vacuum quadratures and $\boldsymbol{Q} := (\hat{a} + \hat{a}^*)/\sqrt{2}$, $\boldsymbol{P} := -i(\hat{a}-\hat{a}^*)/\sqrt{2}$. Since the quadrature $\boldsymbol{Q}$ is distributed as $\mathcal{N}\left(\sqrt{2(1-2\lambda)}u, 1/(2(1-2\lambda))\right)$, and $\boldsymbol{P}$ as $\mathcal{N}\left(\sqrt{2(1-2\lambda)}v, 1/(2(1-2\lambda))\right)$, we have that the rescaled distribution of the output

$$\left((\boldsymbol{Q}+\boldsymbol{Q}_v)/\sqrt{2(1-2\lambda)}, (\boldsymbol{P}-\boldsymbol{P}_v)/\sqrt{2(1-2\lambda)}\right), \tag{78}$$

is given by

$$\mathcal{N}(u, (1-\lambda)/(2(1-2\lambda)^2)) \times \mathcal{N}(v, (1-\lambda)/(2(1-2\lambda)^2)). \tag{79}$$

Therefore the rescaled result of the heterodyne measurement is seen to be an unbiased estimator of the parameters (u, v). From the above distribution it is clear that that both $\mathbb{E}\left[(u - \hat{u}_n)^2\right]$ and $\mathbb{E}\left[(v - \hat{v}_n)^2\right]$ are bounded from above by $(1 - \lambda)/(2(1 - 2\lambda)^2) \leq 1/2$. Substituting these values, the minimax risk becomes

$$
\begin{aligned}
\limsup_{n\to\infty} \sup_{\rho \notin B_2} nR(\rho, \hat{\rho}_n^2) &= \limsup_{n\to\infty} \sup_{\boldsymbol{\theta}} n\mathbb{E}\left[D_B(\rho, \hat{\rho}_n^2)\right] \\
&\leq \limsup_{n\to\infty} \sup_{\lambda} n\mathbb{E}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)^2\right] + 1.
\end{aligned}
\tag{80}
$$

The minimax risk is upper bounded by 1 plus the minimax risk of the Hellinger distance. We now deal with this term. The expectation is taken over the probability distribution $p_{n,\lambda}(j)$ defined in equation (32),

$$
\begin{aligned}
\mathbb{E}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)^2\right] &= \sum_{j=0,1/2}^{n/2} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \times K(j, n, \lambda) \\
&\leq \sum_{j=0,1/2}^{n/2} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \times |1 - K(j, n, \lambda)| \\
&\quad + \sum_{j=0,1/2}^{n/2} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) = E_1 + E_2.
\end{aligned}
\tag{81}
$$

We now consider the term E_1 separately. We split the sum in E_1 over the values of $j \in \mathscr{J}_n$, and $j \notin \mathscr{J}_n$, where $\mathscr{J}_n$ is interval defined in (33). Thus, we have

$$
\begin{aligned}
E_1 &= \sum_{j \in \mathscr{J}_n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \times |1 - K(j, n, \lambda)| \\
&\quad + \sum_{j \notin \mathscr{J}_n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \times |1 - K(j, n, \lambda)| \\
&\leq \max_{j \in \mathscr{J}_n} |1 - K(j, n, \lambda)| \sum_{j \in \mathscr{J}_n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \\
&\quad + \max_{j \notin \mathscr{J}_n} |1 - K(j, n, \lambda)| \sum_{j \notin \mathscr{J}_n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \\
&\leq O(n^{-1/2+\epsilon_3}) \sum_{j \in \mathscr{J}_n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \\
&\quad + \max_{j \notin \mathscr{J}_n} |1 - K(j, n, \lambda)| \sum_{j \notin \mathscr{J}_n} 2 B_{n,\lambda}(n/2 - j).
\end{aligned}
\tag{82}
$$

29

In the last inequality, we used the fact that $K(j, n, \lambda) = 1 + O(n^{-1/2+\epsilon_3})$ on the values of $j \in \mathcal{J}_n$, and that $D_H(\boldsymbol{p}, \boldsymbol{q})^2 \leq 2$ for any pair of probability distributions $\boldsymbol{p}, \boldsymbol{q}$. The value $\max_{j \notin \mathcal{J}_n} |1 - K(j, n, \lambda)|$ is uniformly bounded for λ away from 1/2. This along with the fact that the mass of the binomial distribution $B_{n,\lambda}(n/2 - j)$ is concentrated on values of $j \in \mathcal{J}_n$ implies that the second term in (82) goes to zero exponentially fast in n. Therefore,

$$E_1 \leq O(n^{-1/2+\epsilon_3}) \sum_{j \in \mathcal{J}_n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(k))^2 B_{n,\lambda}(k). \tag{83}$$

Substituting this back in (81), we have that the Hellinger risk is upper bounded by

$$
\begin{aligned}
\mathbb{E}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)^2\right] &\leq O(n^{-1/2+\epsilon_3}) \sum_{j \in \mathcal{J}_n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \\
&\quad + \sum_{j=0,1/2}^{n/2} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(j))^2 B_{n,\lambda}(n/2 - j) \\
&\leq O(n^{-1/2+\epsilon_3}) \sum_{k=0}^{n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(k))^2 B_{n,\lambda}(k) + \sum_{k=0}^{n} D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(k))^2 B_{n,\lambda}(k) \\
&= \left(1 + O(n^{-1/2+\epsilon_3})\right) \mathbb{E}_{\text{Binom}}\left[D_H(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(k))^2\right] \tag{84} \\
&\leq \left(1 + O(n^{-1/2+\epsilon_3})\right) \mathbb{E}_{\text{Binom}}\left[D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n(k))\right]. \tag{85}
\end{aligned}
$$

In the second line we expand the sums over the entire support of the binomial distribution $k \in \{0, \ldots, n\}$, and let $\mathbb{E}_{\text{Binom}}$ mark expectation with respect to the binomial distribution. The last inequality employs the inequality between the squared Hellinger distance and the Kullback-Leibler (KL) distance, defined as $D_{KL}(\boldsymbol{p}, \boldsymbol{q}) := p \log \frac{p}{q} + (1 - p) \log \frac{1-p}{1-q}$. Substituting (85) in (80), and noting that the 'add-beta' estimator $\hat{\lambda}_n$ was defined in (42) over the full support, we have

$$\limsup_{n \to \infty} \sup_{\rho \notin B_2} nR(\rho, \hat{\rho}_n^2) \leq \limsup_{n \to \infty} \sup_{\lambda} n\mathbb{E}_{\text{Binom}}\left[D_{KL}(\boldsymbol{\lambda}, \hat{\boldsymbol{\lambda}}_n)\right] \left(1 + O(n^{-1/2+\epsilon_3})\right) + 1 \leq \frac{1}{2} + 1.$$

The rate follows from the fact that the 'add beta' estimator of the binomial parameter, defined in equation (42), is known to be asymptotically minimax for the KL risk, achieving the rate $\frac{1}{2n}(1 + o(1))$ [22, 23].

Comparing this rate with the one in (77), we see that $3/2$ is the larger value provided $\delta < 1/2$. This gives the upper bound stated in Theorem 2.

$\square$

A.4 Expansion of Quantum Relative Entropy

We derive the expansion of the quantum relative entropy $S(\rho\|\rho') = \text{Tr}[\rho(\log \rho - \log \rho')]$. For qubits the relative entropy between two states can be expressed in terms of the Bloch vector com-

ponents as

$$S(\rho\|\rho') = \frac{1}{2}\left[\log\left(1 - |\boldsymbol{r}|^2\right) - \log\left(1 - |\boldsymbol{r}'|^2\right) + |\boldsymbol{r}|\log\left(\frac{1+|\boldsymbol{r}|}{1-|\boldsymbol{r}|}\right)\right. \tag{86}$$
$$\left. - |\boldsymbol{r}|\cos\Phi\log\left(\frac{1+|\boldsymbol{r}'|}{1-|\boldsymbol{r}'|}\right)\right]$$

where Φ is the angle between the Bloch vectors of the two states. For sufficiently close states, the angle Φ is small and the cosine term in the above equation can be expanded as

$$S(\rho\|\rho') = \frac{1}{2}\left[\log\left(1 - |\boldsymbol{r}|^2\right) - \log\left(1 - |\boldsymbol{r}'|^2\right) + |\boldsymbol{r}|\log\left(\frac{1+|\boldsymbol{r}|}{1-|\boldsymbol{r}|}\right)\right. \tag{87}$$
$$\left. - |\boldsymbol{r}|\log\left(\frac{1+|\boldsymbol{r}'|}{1-|\boldsymbol{r}'|}\right)\right] + \frac{|\boldsymbol{r}|}{4}(\Phi^2 + O(\Phi^4))\log\left(\frac{1+|\boldsymbol{r}'|}{1-|\boldsymbol{r}'|}\right)$$

Using the fact that $|\boldsymbol{r}| = 1 - 2\lambda$ and simplifying, we get

$$S(\rho\|\rho') = \frac{1}{2}\left[\log\left(\frac{\lambda(1-\lambda)}{\lambda'(1-\lambda')}\right) - (1-2\lambda)\log\left(\frac{\lambda(1-\lambda')}{\lambda'(1-\lambda)}\right)\right] + \frac{|\boldsymbol{r}|}{4}(\Phi^2 + O(\Phi^4))\log\left(\frac{1+|\boldsymbol{r}'|}{1-|\boldsymbol{r}'|}\right)$$
$$= \lambda\log\left(\frac{\lambda}{\lambda'}\right) + (1-\lambda)\log\left(\frac{1-\lambda}{1-\lambda'}\right) + \frac{1-2\lambda}{4}(\Phi^2 + O(\Phi^4))\log\left(\frac{1-\lambda'}{\lambda'}\right) \tag{88}$$
$$= D_{KL}(\boldsymbol{\lambda},\boldsymbol{\lambda}') + \frac{1-2\lambda}{4}(\Phi^2 + O(\Phi^4))\log\left(\frac{1-\lambda'}{\lambda'}\right) \tag{89}$$

Where $D_{KL}(\boldsymbol{\lambda},\boldsymbol{\lambda}')$ is the Kullback-Leibler distance between the two distributions $\boldsymbol{\lambda} = (\lambda, 1-\lambda)$ and $\boldsymbol{\lambda}' = (\lambda', 1-\lambda')$.

$\square$