Max-Planck-Institut
für Mathematik
in den Naturwissenschaften
Leipzig

Exponential error rates in multiple state discrimination on a spin chain

by

Michael Nussbaum, and Arleta Szkola

Preprint no.: 3 2010

Exponential error rates in multiple state discrimination on a quantum spin chain

Michael Nussbaum[1], Arleta Szkoła[2]

[1]Department of Mathematics, Cornell University
Ithaca NY, 14853, USA
e-mail: nussbaum@math.cornell.edu

[2]Max Planck Institute for Mathematics in the Sciences
Inselstrasse 22, 04103 Leipzig, Germany
e-mail: szkola@mis.mpg.de

January 15, 2010

Abstract

We consider decision problems on finite sets of hypotheses represented by pairwise different shift-invariant states on a quantum spin chain. The decision in favor of one of the hypotheses is based on outputs of generalized measurements performed on local states on blocks of finite size. We assume existence of the mean quantum Chernoff distances of any pair of states from the given set and refer to the minimum of them as the mean generalized quantum Chernoff distance.

We establish that this minimum specifies an asymptotic bound on the exponential decay of the averaged probability of rejecting the true state in increasing block size, if the mean quantum Chernoff distance of any pair of the hypothetic states is achievable as an asymptotic error exponent in the corresponding binary problem. This assumption is in particular fulfiled by shift-invariant product states (i.i.d. states).

Further, we provide a constructive proof for the existence of a sequence of quantum tests in increasing block size, which achieves an asymptotic error exponent which is equal to the mean generalized quantum Chernoff distance of the given set of states up to a factor, which depends on the set itself. It can be arbitrary close to 1 and is not less than $1/m$ for m being the number of different pairs of states from the set considered.

1 Introduction

In the series of papers [18], [1], [2] the decision problem between two density operators associated to quantum states of a finite quantum system has been solved in the setting of asymptotic quantum hypothesis testing -for some earlier useful results obtained in this context see also [16] and [20]. There decisions in favor of one of the two hypothetic states appearing with an a priori probability strictly larger than zero are based on outcomes of generalized measurements performed on a finite number of copies of the quantum system, where the corresponding quantum state is associated to a tensor product of one of the two hypothetic density operators. The limit of a large number of copies corresponds to a shift-invariant product state on a quantum spin chain. According to [18], [1], [2] it turns out that there is a quantum version of the Chernoff distance defined for pairs of hypothetic density operators, which specifies the best asymptotic exponential decay of the averaged probability of rejecting the true quantum state. This is in analogy to results from classical asymptotic hypothesis testing.

A canonical extension of the binary decision problem refers to a finite number of hypotheses. In the setting of classical asymptotic multiple hypothesis testing, where the hypotheses are represented by probability distributions, the best asymptotic error exponent is equal to the generalized Chernoff distance, see [22]. In our recent work [19], in analogy to the classical definition given in [22], we have introduced the *generalized quantum Chernoff distance* of a finite set of density operators as the minimum of the binary quantum Chernoff distances over all possible pairs of different hypothetic density operators. We could identify this minimum as a bound on asymptotic error exponents in corresponding multiple quantum hypothesis testing and establish that it is achievable in the special case where the hypotheses are represented by pure quantum states. For completeness we want to mention that there is a wide literature treating the related problem of optimal multiple state discrimination in a finite, i.e. non asymptotic setting, cf. [24], [13], [14], [17], [23], [3], [12]. The optimal discrimination between exactly two density operators has been completely solved by Helstrom and Holevo, see [7], [15].

In the presence of correlations among the single quantum systems of a spin chain the hypothetic states are represented by (in an appropriate sense) compatible sequences, in an increasing block size, of density operators in respective local algebras of observables. Several special cases of hypotheses represented by correlated quantum states on spin chains has been investigated by Hiai et. al in a series of papers [8], [9], [10]. There the quantum Chernoff distance of two density operators has been replaced by the mean quantum Chernoff distance of two shift-invariant states on a spin chain, which, roughly speaking, is defined as the asymptotic rate of quantum Chernoff distances of the pairs of local quantum states, if the corresponding limits exist. This is in line with other well-established extensions of entropic quantities to the case of shift-invariant correlated states on a spin chain; compare the concepts of mean quantum relative entropy [11] and mean quantum entropy/quantum entropy rate [4]. From our point of view the most relevant result among [8], [9], [10] is given in [8]. It identifies a class

of shift-invariant states on a quantum spin chain, which is characterized by a factorization property, as a domain where the mean binary Chernoff distances exist and specify the best asymptotically achievable error exponents in corresponding binary decision problems. Note that similar classes of correlated states with appropriate factorization property have been shown to permit (classical and quantum) Sanov type theorems, which resolve some related asymmetric decision problems, cf. [5].

In this paper we define the *mean generalized quantum Chernoff distance* of finite sets of pairwise different shift-invariant quantum states on a spin chain as the minimum of the mean quantum Chernoff distances of all the possible quantum state pairs. Notice that the minimum is well-defined on the set of shift-invariant quantum states, where all the binary quantum Chernoff distances exist, i.e. in particular on both the set of shift-invariant product states and the strictly larger set of shift-invariant states fulfilling the factorization assumption as specified in [8]. We point out that in the case of shift-invariant product states the mean generalized quantum Chernoff distance coincides with the generalized quantum Chernoff distance of the corresponding density operators associated to the local states on the blocks of size 1.

Extending the result presented in Theorem 1 of our previous paper [19], we show that the mean generalized quantum Chernoff distance, if it exists for a given finite set of shift-invariant states, specifies a bound on the exponential decay of the averaged error probability in corresponding multiple state discrimination. Here, again, we assume that each of the hypothetic states appears with an a priori probability strictly larger than zero. As our main contribution we establish that an exponential decay, i.e. a strictly positive asymptotic error exponent, is indeed achievable in multiple state discrimination. To the best of our knowledge this has not been shown so far apart from the case of *two* hypotheses, cf. [2], [8], and the special case of multiple pure (i.i.d.) state discrimination, cf. [19]. More precisely, we construct a sequence of quantum tests for the set of hypothetic local states, such that the exponential decay of the averaged error probability in increasing block size is equal to the mean generalized quantum Chernoff distance up to a factor, which depends on the configuration of the states. The factor can be arbitrary close to 1. In the worst case, where all the involved binary mean Chernoff distances are equal, it is equal to $1/\binom{r}{2}$, where r is the number of different hypothetic states. Our construction represents an appropriate blockwise combination of the optimal quantum tests of the associated asymptotic binary decision problems.

The outline of our paper is as follows:

- In Section 2 we introduce our notations, explain shortly the mathematical framework of a quantum spin chain and its state space, present the definitions of the here relevant Chernoff type distances and finally we are in the position to state precisely our main results in Theorems 1 and 2.

- The proof of Theorem 1, which adopts the idea of the proof of Theorem 1 from our previous paper [19], is given in Section 3.

- Section 4 contains a construction of quantum tests for multiple states on a quantum spin chain, which -subject to the assumptions of Theorem 2- achieves an asymptotic error exponent equal to the mean generalized quantum Chernoff distance up to a factor depending on the set of states itself. This proves our main Theorem 2.

2 Notations and main results

Let $\mathcal{H}$ be a complex Hilbert space with $\dim \mathcal{H} = d < \infty$ and $\mathcal{A}$ be a unital C^*-subalgebra of linear operators on $\mathcal{H}$. For each finite subset $\Lambda \subset \mathbb{Z}$ denote by $\mathcal{A}_\Lambda$ the tensor product $\bigotimes_{i\in\Lambda} \mathcal{A}$, which is a C^*-subalgebra of linear operators on $\bigotimes_{i\in\Lambda} \mathcal{H}$. The construction of quasi-local C^*-algebras $\mathcal{A}^\infty$ formalizes the limit of $\mathcal{A}_\Lambda$, as Λ tends to be $\mathbb{Z}$, compare [21] or [6].

The state space $\mathcal{S}(\mathcal{A}^\infty)$ of $\mathcal{A}^\infty$ consists of positive linear functionals $\omega : \mathcal{A}^\infty \to \mathbb{C}$ fulfilling the normalization condition $\omega(\mathbf{1}) = 1$, where $\mathbf{1}$ denotes the identity in $\mathcal{A}^\infty$. Each $\omega \in \mathcal{S}(\mathcal{A}^\infty)$ corresponds one-to-one to a family of local states ω_Λ, $\Lambda \subset \mathbb{Z}$ with $|\Lambda| < \infty$, being restrictions of ω onto $\mathcal{A}_\Lambda$, respectively. We are primarily interested in the convex subset $\mathcal{T}(\mathcal{A}^\infty)$ of shift-invariant states on $\mathcal{A}^\infty$. Note that the shift-invariance implies that for any $\Lambda_1, \Lambda_2 \subset \mathbb{Z}$ of equal size, i.e. with $|\Lambda_1| = |\Lambda_2|$, we can identify the corresponding restrictions ω_{Λ_1} and ω_{Λ_2} of $\omega \in \mathcal{T}(\mathcal{A}^\infty)$. It follows that a shift-invariant state ω is determined by a sequence of local states $\omega^{(n)}$, $n \in \mathbb{N}$, on $\mathcal{A}^{(n)} := \mathcal{A}_{[1,n]}$, respectively. For each $n \in \mathbb{N}$ the associated density operator $\rho^{(n)} \in \mathcal{A}^{(n)}$ satisfies $\omega^{(n)}(a) = \mathrm{tr}\ \rho^{(n)} a$ for all $a \in \mathcal{A}^{(n)}$.

Let Σ be a finite set of states $\omega_i \in \mathcal{T}(\mathcal{A}^\infty)$, $i = 1, \ldots, r$, representing the hypotheses H_i, respectively. We can identify Σ with the sequence $\Sigma^{(n)}$, $n \in \mathbb{N}$, of sets of associated density operators $\rho_i^{(n)}$, $i = 1, \ldots, r$, in $\mathcal{A}^{(n)}$, respectively. For each $n \in \mathbb{N}$ let $E^{(n)} = \{E_i^{(n)}\}_{i=1}^r$ be a positive operator valued measure (POVM) in $\mathcal{A}^{(n)}$, i.e. each $E_i^{(n)}$, $i = 1, \ldots, r$, is a self-adjoint element of $\mathcal{A}^{(n)}$ with $E_i^{(n)} \geq 0$ and $\sum_{i=1}^r E_i^{(n)} = \mathbf{1}$. The POVMs $E^{(n)}$ determine generalized measurements. By identifying the measurement outcome corresponding to $E_i^{(n)}$, $i = 1, \ldots, r$, with the hypothesis $H_i \sim \rho_i^{(n)}$, respectively, they describe quantum tests for discrimination between the quantum states associated to density operators from $\Sigma^{(n)}$, or simply *quantum tests for* $\Sigma^{(n)}$. If ω_i happens to be the true state then the corresponding *individual success probability* is given by

$$\mathrm{Succ}_i(E^{(n)}) := \mathrm{tr}\ [\rho_i^{(n)} E_i^{(n)}]. \tag{1}$$

and consequently the *individual error probability* is

$$\mathrm{Err}_i(E^{(n)}) := \mathrm{tr}\ [\rho_i^{(n)} (\mathbf{1} - E_i^{(n)})]. \tag{2}$$

It refers to the situation when H_i is rejected. Assuming $0 < p_i < 1$, $i = 1, \ldots, r$, with $\sum_{i=1}^r p_i = 1$ to be the prior distribution on the given set of r hypotheses the *averaged error*

probability is given by

$$\mathrm{Err}(E^{(n)}) = \sum_{i=1}^{r} p_i \mathrm{tr}\ [\rho_i^{(n)}(\mathbf{1} - E_i^{(n)})]. \tag{3}$$

If the limit $\lim_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}(E^{(n)})$ exists, we refer to it as the *asymptotic error exponent*. Otherwise we have to consider the corresponding lim sup and lim inf expressions.

For two density operators ρ_1 and ρ_2 the *quantum Chernoff distance* is defined by

$$\xi_{QCB}(\rho_1, \rho_2) := -\log \inf_{0\le s\le 1} \mathrm{tr}\ \rho_1^{1-s}\rho_2^s. \tag{4}$$

It specifies the optimal achievable asymptotic error exponent in discriminating between ρ_1 and ρ_2, compare [18], [1], [2]. Quantum tests with minimal averaged error probability for a pair of density operators ρ_1 and ρ_2 on the same Hilbert space $\mathcal{H}$ are well-known to be given by the respective *Holevo-Helstrom projectors*

$$\Pi_1 := \mathrm{supp}\ (\rho_1 - \rho_2)_+, \tag{5}$$
$$\Pi_2 := \mathrm{supp}\ (\rho_2 - \rho_1)_+ = \mathbf{1} - \Pi_1, \tag{6}$$

where supp a denotes the support projector of a self-adjoint operator a, while a_+ means its positive part, i.e. $a_+ = (|a| + a)/2$ for $|a| := (a^*a)^{1/2}$, see [15], [7]. The Holevo-Helstrom projectors generalize the maximum likelihood tests for two probability distribution. This can be verified by letting ρ_1 and ρ_2 be two commuting density matrices.

For a set $\Sigma = \{\rho_i\}_{i=1}^r$ of density operators in $\mathcal{A}$, where $r > 2$, we have introduced in [18] the *generalized quantum Chernoff distance*

$$\xi_{QCB}(\Sigma) := \min\{\xi_{QCB}(\rho_i, \rho_j) :\ 1 \le i < j \le r\}. \tag{7}$$

This is in full analogy to the classical case where the hypotheses are represented by probability distributiosn P_i, $i = 1, \ldots, r$, on a finite sample space Ω, see [22].

In [8] the *mean quantum Chernoff distance* between two states ω_1 and ω_2 in $\mathcal{T}(\mathcal{A}^\infty)$, each of them corresponding one-to-one to the respective sequences $\{\rho_i^{(n)}\}_{n\in\mathbb{N}}$, $i = 1, 2$, of density operators in corresponding local algebras $\mathcal{A}^{(n)}$, has been defined by

$$\bar{\xi}_{QCB}(\omega_1, \omega_2) := \sup_{0\le s\le 1} \bar{\xi}^{(s)}_{QCB}(\omega_1, \omega_2) \tag{8}$$

if the limits

$$\bar{\xi}^{(s)}_{QCB}(\omega_1, \omega_2) := \lim_{n\to\infty} -\frac{1}{n}\log \mathrm{tr}\ [(\rho_1^{(n)})^{1-s}(\rho_2^{(n)})^s], \tag{9}$$

exist for $0 \leq s \leq 1$. Note that in the special case where ω_1 and ω_2 both are shift-invariant product states, i.e. $\rho_i^{(n)} = \rho_i^{\otimes n}$ for all $n \in \mathbb{N}$, we have the relation $\bar{\xi}_{QCB}(\omega_1, \omega_2) = \xi_{QCB}(\rho_1, \rho_2)$, i.e. the mean quantum Chernoff distance coincides with the quantum Chernoff distance of the associated density operators ρ_1 and ρ_2 in $\mathcal{A}^{(1)}$.

Finally, for a set $\Sigma = \{\omega_i\}_{i=1}^r$ of states on $\mathcal{A}^\infty$ where the mean quantum Chernoff distances $\bar{\xi}_{QCB}(\omega_i, \omega_j)$ exist for all pairs (ω_i, ω_j) with $i \neq j$, we introduce the *mean generalized quantum Chernoff distance*

$$\bar{\xi}_{QCB}(\Sigma) := \min\{\bar{\xi}_{QCB}(\omega_i, \omega_j) : \ 1 \leq i < j \leq r\}. \tag{10}$$

In [19], see Theorem 1 therein, we have shown that in the case of multiple shift-invariant product states on $\mathcal{A}^\infty$ the generalized quantum Chernoff distance of the associated set of local states on $\mathcal{A}^{(1)}$ provides a bound on asymptotically achievable error exponent in the corresponding multiple quantum hypothesis testing. Here we extend the statement to the case of hypotheses being represented by elements from a class of shift-invariant correlated quantum states on $\mathcal{A}^\infty$. The bound is then given by the corresponding mean generalized quantum Chernoff distance.

Theorem 1 *Let $r \in \mathbb{N}$ and $\Sigma = \{\omega_i\}_{i=1}^r$ be a set of states on $\mathcal{A}^\infty$ with respective prior probability $0 < p_i < 1$. If for every (i, j), $1 \leq i < j \leq r$, the mean quantum Chernoff distance $\xi_{QCB}(\omega_i, \omega_j)$ exists and specifies the optimal asymptotic error exponent in the corresponding binary quantum hypothesis testing, then it holds for any sequence $E^{(n)}$, $n \in \mathbb{N}$ of POVMs for $\Sigma^{(n)}$, respectively,*

$$\limsup_{n\to\infty} -\frac{1}{n} \log Err(E^{(n)}) \leq \bar{\xi}_{QCB}(\Sigma), \tag{11}$$

where $\bar{\xi}_{QCB}(\Sigma)$ denotes the mean generalized quantum Chernoff distance defined by (10).

As already mentioned, the assumption of Theorem 1 above is in particular satisfied on the set of shift-invariant product states on $\mathcal{A}^\infty$, cf. [2]. Moreover, it has been shown in [8], that it is also fulfilled on a subset of shift-invariant correlated states with certain lower and upper factorization properties. More preciesely, for a corresponding shift-invariant state $\omega \in \mathcal{T}(\mathcal{A}^\infty)$ there exist constants $\alpha, \beta \in \mathbb{R}$, and an $m_0 \in \mathbb{N}$ such that for all $m \geq m_0$ and $k \in \mathbb{N}$ it holds

$$\omega_{[1,km]} \geq \alpha^{k-1} \omega_{[1,m]}^{\otimes k}, \qquad \omega_{[1,km]} \leq \beta^{k-1} \omega_{[1,m]}^{\otimes k},$$

where $\omega_{[1,m]}$ denotes the restriction of ω onto the local subalgebra $\mathcal{A}_{[1,n]} \subset \mathcal{A}^\infty$ associated to the finite block $[1, n]$ of the lattice $\mathbb{Z}$, which underlies the quantum spin chain. For more details on the factorization property and nontrivial examples such as Gibbs states of translation-invariant finite-range interactions and finitely correlated states see [8].

According to Theorem 2 in [19], in the special case of a finite set of pure states on $\mathcal{A}^{(1)}$ the corresponding generalized quantum Chernoff distance indeed is achievable as an exponential decay of minimal averaged error probability in discrimination between the associated shift-invariant product states on $\mathcal{A}^{\infty}$. The following theorem states that in the general case of arbitrary (i.e. possibly mixed) density operators in $\mathcal{A}^{(1)}$ an exponential rate of decay is achievable. We exhibit an exponent which equals to the generalized quantum Chernoff distance up to a factor, where the factor depends on the set of states considered. Moreover, a similar result holds in the case of shift-invariant correlated states on $\mathcal{A}^{\infty}$ fulfilling the assumptions of Theorem 1. Here we find an exponent which equals the *mean* generalized quantum Chernoff distance up to a factor, where again the factor depends on Σ.

Theorem 2 *Let Σ be a finite set consisting of hypotheses $\omega_i \in \mathcal{T}(\mathcal{A}^{\infty})$, $i = 1, \ldots, r$, such that the mean quantum Chernoff distances $\bar{\xi}_{QCB}(\omega_i, \omega_j)$, $1 \leq i < j \leq r$, exist, are greater than zero, and represent achievable asymptotic error exponents in the corresponding binary hypothesis testing problems. Then there exists a sequence of quantum tests $\{E^{(n)}\}_{n\in\mathbb{N}}$ for $\Sigma^{(n)}$, respectively, such that the corresponding averaged error probabilities satisfy*

$$\liminf_{n\to\infty} -\frac{1}{n} \log Err(E^{(n)}) \geq \bar{\xi}_{QCB}(\Sigma)\varphi(\Sigma), \tag{12}$$

where

$$\varphi(\Sigma) := \left(\sum_{1\leq j<i\leq r} \frac{\bar{\xi}_{QCB}(\Sigma)}{\bar{\xi}_{QCB}(\omega_i, \omega_j)} \right)^{-1}. \tag{13}$$

The factor $\varphi(\Sigma)$ satisfies

$$\frac{1}{m} = \frac{1}{\sum_{1\leq j<i, 1\leq i\leq r} 1} \leq \varphi(\Sigma) \leq \frac{1}{\frac{\bar{\xi}_{QCB}}{\bar{\xi}_{QCB}}} = 1.$$

As a result, we can claim that the mean quantum Chernoff bound $\bar{\xi}_{QCB}(\Sigma)$ is attainable up to a factor $\varphi(\Sigma)$. This factor is close to 1 if the pairwise mean quantum Chernoff distance for the least favorable pair (i^*, j^*) (i.e. $\bar{\xi}_{QCB}(\Sigma) = \bar{\xi}_{QCB}(\omega_{i^*}, \omega_{j^*})$) is sufficiently small compared to the pairwise mean quantum Chernoff distance $\bar{\xi}_{QCB}(\omega_i, \omega_j)$ for all other pairs, in other words, if the least favorable pair (i^*, j^*) sufficiently "stands out" with regard to its estimation difficulty. If the other extreme holds, i.e. all $\bar{\xi}_{QCB}(\omega_i, \omega_j)$ are equal, then $\varphi(\Sigma)$ is equal to its lower bound $1/m$.

3 A Chernoff type bound in multiple state discrimination

In this section we show that the generalized mean quantum Chernoff distance provides a bound on the asymptotically achievable error exponent in multiple quantum hypotheses testing,

where the hypotheses are represented by states on $\mathcal{A}^\infty$, such that for any pair of them the (binary) mean Chernoff distance exists, is greater than zero, and specifies the asymptotically optimal error exponent in the corresponding binary hypothesis testing problem.

PROOF. [Theorem 1] Denote by $\mathrm{Err}_i(E^{(n)})$ the individual error probability pertaining to the case that the true hypothesis H_i corresponding to the n-block density operator $\rho_i^{(n)} \in \mathcal{A}^{(n)}$ is rejected on the base of outcomes of the quantum test $E^{(n)}$ for Σ. Fix any two indices $1 \leq i < j \leq r$. For $n \in \mathbb{N}$ let $A^{(n)}, B^{(n)} \in \mathcal{A}^{(n)}$ be two positive operators such that $A^{(n)} + B^{(n)} = \mathbf{1} - E_i^{(n)} - E_j^{(n)}$. Then the positive operators $\tilde{E}_i{}^{(n)} := E_i^{(n)} + A^{(n)}$ and $\tilde{E}_j{}^{(n)} := E_j^{(n)} + B^{(n)}$ represent a POVM $\tilde{E}^{(n)}$ in $\mathcal{A}^{(n)}$, which we regard as a quantum test for the pair $\{\rho_i^{(n)}, \rho_j^{(n)}\}$. We obtain for the modified individual error probabilities

$$\mathrm{Err}_i(\tilde{E}^{(n)}) = \mathrm{tr}\,[\rho_i^{(n)}(\mathbf{1} - \tilde{E}_i{}^{(n)})] \leq \mathrm{tr}\,[\rho_i^{(n)}(\mathbf{1} - E_i^{(n)})] = \mathrm{Err}_i(E^{(n)}),$$

and similarily $\mathrm{Err}_j(\tilde{E}^{(n)}) \leq \mathrm{Err}_j(E^{(n)})$. It follows a lower bound on the average error probability with respect to the original tests $\{E_i^{(n)}\}_{i=1}^r$:

$$\mathrm{Err}(E^{(n)}) = \frac{1}{r}\sum_{k=1}^{r}\mathrm{Err}_k(E^{(n)}) \geq \frac{1}{r}\left(\mathrm{Err}_i(E^{(n)}) + \mathrm{Err}_j(E^{(n)})\right) \geq \frac{1}{r}\left(\mathrm{Err}_i(\tilde{E}^{(n)}) + \mathrm{Err}_j(\tilde{E}^{(n)})\right),$$

which implies

$$\begin{aligned}
\limsup_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}(E^{(n)}) &\leq \limsup_{n\to\infty}\frac{1}{n}\log r + \limsup_{n\to\infty} -\frac{1}{n}\log\left(\mathrm{Err}_i(\tilde{E}^{(n)}) + \mathrm{Err}_j(\tilde{E}^{(n)})\right) \\
&= \limsup_{n\to\infty} -\frac{1}{n}\log\frac{1}{2}\left(\mathrm{Err}_i(\tilde{E}^{(n)}) + \mathrm{Err}_j(\tilde{E}^{(n)})\right) \\
&\leq \xi_{QCB}(\omega_i, \omega_j).
\end{aligned}$$

Here the last inequality holds by assumption of the validity of the quantum Chernoff theorem for binary hypothesis testing. Since the pair of indices (i, j) was choosen arbitrarily, the statement of the theorem follows. □

4 Exponential decay of the averaged error probability

The main idea of the proof of Theorem 2 is a blockwise application of the optimal quantum test for pairs of quantum states from the given set Σ. More in detail, the construction of our quantum test can be described as follows. Consider all pairs of states ω_i, ω_j, $i \neq j$, and divide the n-block density operator into blocks of unequal size. Each block will be used for testing between a particular pair, and the size of the blocks is chosen in such a way that pairs of states

which are more difficult to discriminate are assigned longer blocks (more sample size). Within each block a quantum measurement is performed confirming to the pair of states, creating a decision random variable with values in $\{i, j\}$ (a "vote" for either i or j). When the random variables for all blocks are realized, a final decision is made in favor of hypothesis $H_i \sim \omega_i$ if this hypothesis has the most number of votes. This can be broken in any way, for instance by considering the numerical rank of i.

It is easy to see that in the commuting case, where for each n-block the corresponding hypothetic density operators commute, this method is related to maximum likelihood, though it does not coincide. In the commuting case, there is no need for blocking and a direct maximum likelihood decision is better. In the quantum (noncommuting) case, the Yuen-Kennedy-Lax (YKL) test is the appropriate generalization of maximum likelihood, see [24]. It has minimum error probability for any n, and it is a conjecture that its risk asymptotics is described by the generalized (multiple) quantum Chernoff distance. Our construction by blocking yields a feasible quantum test which can be near-optimal for certain configurations of states, in terms of the (mean) generalized quantum Chernoff distance. In this cases, it provides an upper risk bracket close to the Chernoff bound for the YKL test.

PROOF. [Theorem 2] Let $m := \binom{r}{2}$. This equals the number of different pairs of states in Σ. Since we are interested in the asymptotic behaviour in n there is no loss of generality assuming $n \geq m$.

The main idea is to divide the discrete interval $[1, n] =: \mathcal{I}^{(n)}$ into disjoint subblocks $\mathcal{I}_k^{(n)}$, $k = 1, \ldots, m$, of length n_k each, each of them being associated to one of the m different density operator pairs $\{\rho_i^{(n_k)}, \rho_j^{(n_k)}\}$, $i \neq j$. In order to make the correspondence between $\{\mathcal{I}_k^{(n)}\}_{k=1}^m$ and the set of unordered pairs $\left\{\{\rho_i^{(n_k)}, \rho_j^{(n_k)}\}\right\}$ one-to-one, we define the mapping

$$\{1, \ldots, m\} \ni k \mapsto (k_1, k_2) \in \{1, \ldots, r\}^2, \tag{14}$$

which to each $k \in \{1, \ldots, m\}$ assigns an ordered pair of indices (i, j) in their lexicographic order, for $1 \leq i \leq r-1$ and $i < j \leq r$. Now, that the one-to-one mapping $k \leftrightarrow \{i, j\}, i \neq j$ is specified, we write $n(i, j) := n_k$ for the length of the subblock associated to the pair $\{i, j\}$, and for ease of notation we also set $n(i, j) := n(j, i)$ for $j < i$. The lengths n_k which satisfy $\sum_{s=1}^m n_k = n$ will be left unspecified for now; we will determine them later.

In this construction, each subbblock $\mathcal{I}_k^{(n)}$ is now associated to a pair of density operators

$$\mathcal{I}_k^{(n)} \mapsto \left\{\rho_{k_1}^{(n(i,j))}, \rho_{k_2}^{(n(i,j))}\right\}, \qquad k = 1, \ldots, m.$$

We intend to construct the quantum test $E^{(n)}$ for $\Sigma^{(n)}$ as a composition of quantum tests of minimal averaged error probability for the different pairs $\{\rho_i^{(n_k)}, \rho_j^{(n_k)}\}$, $1 \leq i < j \leq r$.

Optimal binary quantum tests for any block size n are known to be given by the Holevo-Helstrom tests $(P_{i,j}^{(n)}, P_{j,i}^{(n)})$, where

$$P_{i,j}^{(n)} := \text{supp } (\rho_i^{(n)} - \rho_j^{(n)})_+$$

is the orthogonal projector associated to the density operator $\rho_i^{(n)}$, while $P_{j,i}^{(n)} := \mathbf{1} - P_{i,j}^{(n)}$ is associated to $\rho_j^{(n)}$. We will apply these for any pair $\{i,j\}$ in the corresponding block of given size $n(i,j)$. More precisely, our construction of $E^{(n)}$ works as follows. Let π_0 and π_1 be permutations given by

$$\pi_0(i,j) := (i,j) \quad \text{and} \quad \pi_1(i,j) := (j,i)$$

for $(i,j) \in \mathbb{N} \times \mathbb{N}$, and define for any vector $\mathbf{b} \in \{0,1\}^m$ an m-fold tensor product projector in $\mathcal{A}^{(n)}$

$$P_{\mathbf{b}}^{(n)} := \bigotimes_{k=1}^{m} P_{\pi_{b_k}(k_1,k_2)}^{(n_k)}, \tag{15}$$

where $b_k \in \{0,1\}$ denotes the kth coordinate of $\mathbf{b}$. Observe that the orthogonal projectors $P_{\mathbf{b}}^{(n)}$, $\mathbf{b} \in \{0,1\}^m$, define a decomposition of the identity $\mathbf{1}_n$ in $\mathcal{A}^{(n)}$, i.e.

$$\sum_{\mathbf{b}\in\{0,1\}^m} P_{\mathbf{b}}^{(n)} = \mathbf{1}_n, \tag{16}$$

and in this sense they represent a POVM $\tilde{E}^{(n)}$ in $\mathcal{A}^{(n)}$ with 2^m elements.

We want to modify $\tilde{E}^{(n)}$, such that it represents a POVM consisting of fewer, namely m positive elements. Subsequently, by associating each of the newly defined m elements to a different density operator from $\Sigma^{(n)}$ we obtain a *quantum test* for $\Sigma^{(n)}$. For each $i \in \{1,\ldots,r\}$ we introduce the function

$$\begin{aligned} n_i : \{0,1\}^m &\to \{0,\ldots,r-1\}, \\ \mathbf{b} &\mapsto n_i(\mathbf{b}) := |\{k : \ \pi_{b_k}^{(1)}(k_1,k_2) = i\}|, \end{aligned} \tag{17}$$

where $\pi_{b_k}^{(1)}(k_1,k_2)$ denotes the first coordinate of $\pi_{b_k}(k_1,k_2)$. Further, we define for each $1 \le i \le r$ a subset $B_i \subset \{0,1\}^m$ by

$$\begin{aligned} B_i := \{\mathbf{b} : \ n_i(\mathbf{b}) &> n_j(\mathbf{b}) \text{ for } 1 \le j < i, \\ n_i(\mathbf{b}) &\ge n_j(\mathbf{b}) \text{ for } i \le j \le r\}. \end{aligned} \tag{18}$$

Finally, we set

$$E_i^{(n)} := \sum_{\mathbf{b}\in B_i} P_{\mathbf{b}}^{(n)}. \tag{19}$$

Note that $B_i \cap B_j = \emptyset$, for $i \neq j$, and $\bigcup_{i=1}^r B_i = \{0,1\}^m$, i.e. $\{B_i\}_{i=1}^r$ represents a (disjoint) decomposition of the set $\{0,1\}^m$ of binary sequences of length m. Hence $\{E_i^{(n)}\}_{i=1}^r$ defines a POVM in $\mathcal{A}^{(n)}$, and associating the measurement outcome corresponding to $E_i^{(n)}$, $i = 1, \ldots, r$, to the density operator $\rho_i^{(n)}$, respectively, we obtain a proper quantum test for $\Sigma^{(n)}$.

It remains to verify the asymptotic behaviour (12) for $E^{(n)}$. To this end, we fix an $i \in \{1, \ldots, r\}$, define a corresponding index set

$$K_i := \{k \in \{1, \ldots, m\} : \ k_1 = i \text{ or } k_2 = i\},$$

and consider the individual error probability $\mathrm{Err}_i(E^{(n)})$. We have

$$\begin{aligned}
\mathrm{Err}_i(E^{(n)}) &= \mathrm{tr}\,[\rho_i^{(n)}(\mathbf{1}_n - E_i^{(n)})] \\
&= \mathrm{tr}\,[\rho_i^{(n)} \sum_{j\neq i} E_j^{(n)}] \\
&= \mathrm{tr}\,[\rho_i^{(n)} \sum_{\mathbf{b}\notin B_i} P_{\mathbf{b}}^{(n)}] \\
&\leq \sum_{k\in K_i} \mathrm{tr}\,[\rho_i^{(n_k)} P_{i_k^\perp,i}^{(n_k)}] = \sum_{1\leq j\leq r, j\neq i} \mathrm{tr}\,[\rho_i^{(n(i,j))} P_{j,i}^{(n(i,j))}],
\end{aligned} \tag{20}$$

where the first line is by definition of individual error probability and the second line is according to (19). The index $i_k^\perp$ appearing on the right hand side of inequality (20) is such that the subblock $\mathcal{I}_k^{(n)}$ corresponds to the pair of density operators $\rho_i^{(n_k)}$ and $\rho_{i_k^\perp}^{(n_k)}$. Inequality (20) follows from the fact that at least one tensor factor of a projector $P_{\mathbf{b}}^{(n)}$ with $\mathbf{b} \notin B_i$ is equal to a Holevo-Helstrom projector of the form $P_{j,i}^{(n(i,j))}$, where $j \neq i$, i.e. $P_{j,i}^{(n(i,j))}$ corresponds to decision in favor of $\rho_j^{(n(i,j))}$ and against $\rho_i^{(n(i,j))}$. More in detail, we deduce the inequality as follows. For any $\mathbf{b} \notin B_i$ there exists an index $k \in K_i$ with $\pi_{b_k}^{(1)}(k_1, k_2) \neq i$. Let $k_{\mathbf{b}}$ be the smallest of such indices corresponding to $\mathbf{b}$. We denote by $B_i^\perp(k)$ the set consisting of all $\mathbf{b} \notin B_i$ with $k_{\mathbf{b}} = k$:

$$B_i^\perp(k) := \{\mathbf{b} \notin B_i : \ k_{\mathbf{b}} = k\}.$$

Observe that $\{B_i^\perp(k)\}_{k\in K_i}$ represents a decomposition of $B_i^\perp := \{0,1\}^m \setminus B_i$ into $r-1$ disjoint subsets. For each $k \in K_i$ we deduce the following upper bound on the sum of projectors

$P_{\mathbf{b}}^{(n)} \in \mathcal{A}^{(n)}$ over $B_i^{\perp}(k)$ in terms of the projector $P_{i_k^{\perp},i}^{(n_k)}$, which is understood here as an element in the local algebra $\mathcal{A}_{\mathcal{I}_k^{(n)}} \subseteq \mathcal{A}_{\mathcal{I}^{(n)}} = \mathcal{A}^{(n)}$:

$$\sum_{\mathbf{b}\in B_i^{\perp}(k)} P_{\mathbf{b}}^{(n)} \leq P_{i_k^{\perp},i}^{(n_k)} \otimes \mathbf{1}_{\mathcal{I}^{(n)}\setminus\mathcal{I}_k^{(n)}}. \tag{21}$$

The index $i_k^{\perp}$ is again determined by k as explained below (20), and $\mathbf{1}_{\mathcal{I}^{(n)}\setminus\mathcal{I}_k^{(n)}}$ denotes the identity in the local algebra $\mathcal{A}_{\mathcal{I}^{(n)}\setminus\mathcal{I}_k^{(n)}} \subset \mathcal{A}^{(n)}$ associated to the subset $\mathcal{I}^{(n)} \setminus \mathcal{I}_k^{(n)}$ of $\mathcal{I}^{(n)}$. It follows the estimate

$$\sum_{\mathbf{b}\notin B_i} P_{\mathbf{b}}^{(n)} = \sum_{k\in K_i} \sum_{\mathbf{b}\in B_i^{\perp}(k)} P_{\mathbf{b}}^{(n)} \quad \leq \quad \sum_{k\in K_i} P_{i_k^{\perp},i}^{(n_k)} \otimes \mathbf{1}_{\mathcal{I}^{(n)}\setminus\mathcal{I}_k^{(n)}},$$

which, applying the shift-invariance of ω_i, implies the upper bound (20) on $\mathrm{Err}_i(E^{(n)})$.

Assume now that all subblock lengths $n(i,j)$, $i \neq j$, are (asymptotically) proportional to n with factor w_{ij}, i.e.

$$\begin{aligned} n(i,j) &= w_{ij}\, n\, (1+o(1))\,, \\ \sum_{1\leq j<i, 1\leq i\leq r} w_{ij} &= 1. \end{aligned} \tag{22}$$

Recall that for each pair (i,j) of indices the $P_{j,i}^{n(j,i)}$ in (20) denote the Holevo-Helstrom projectors corresponding to the two density operators $\rho_i^{(n(i,j))}$ and $\rho_j^{(n(i,j))}$, and hence they represent a sequence of (asymptotically) optimal quantum tests for $\{\omega_i, \omega_j\}$ achieving the asymptotic error exponent equal to the mean quantum Chernoff distance $\bar{\xi}_{QCB}(\omega_i, \omega_j)$. Hence we obtain from (20) as n tends to infinity

$$-\liminf_{n\to\infty} \frac{1}{n} \log \mathrm{Err}_i(E^{(n)}) \geq \min_{i\neq j} w_{ij} \bar{\xi}_{QCB}(\omega_i, \omega_j). \tag{23}$$

Note that the minimum on the right hand side appears due to the fact that asymptotically the largest term in (20) dominates.

In order to get the best lower bound, i.e. to maximize the right hand side of (23) under the restriction (22), we solve the problem

$$\max_{w_{ij}} \left\{ \min_{i\neq j} w_{ij} \bar{\xi}_{QCB}(\omega_i, \omega_j) : \sum_{1\leq j<i, 1\leq i\leq r} w_{ij} = 1 \right\}.$$

The solution is obtained by making all $w_{ij}\bar{\xi}_{QCB}(\omega_i,\omega_j)$ equal, that is by setting

$$w_{ij} = \frac{1}{\left(\bar{\xi}_{QCB}(\omega_i,\omega_j)\sum_{1\le t<s,1\le s\le r}\frac{1}{\bar{\xi}_{QCB}(\omega_s,\omega_t)}\right)}$$

whence

$$\min_{i\neq j} w_{ij}\bar{\xi}_{QCB}(\omega_i,\omega_j) = \frac{1}{\sum_{1\le j<i,1\le i\le r}\frac{1}{\bar{\xi}_{QCB}(\omega_i,\omega_j)}}.$$

The mean generalized quantum Chernoff bound of the set Σ was defined as $\bar{\xi}_{QCB}(\Sigma) = \min_{i\neq j}\bar{\xi}_{QCB}(\omega_i,\omega_j)$, and we obtain

$$-\liminf_{n\to\infty}\frac{1}{n}\log \mathrm{Err}_i(E^{(n)}) \ge \frac{1}{\sum_{1\le j<i,1\le i\le r}\frac{1}{\bar{\xi}_{QCB}(\omega_i,\omega_j)}} = \bar{\xi}_{QCB}\cdot\varphi(\Sigma), \tag{24}$$

where the factor on the right hand side is given by (13), i.e. $\varphi(\Sigma) = \left(\sum_{1\le j<i,1\le i\le r}\frac{\bar{\xi}_{QCB}}{\bar{\xi}_{QCB}(\omega_i,\omega_j)}\right)^{-1}$. Since the lower bound (24) on the individual error exponent does not depend on the index i, $i = 1,\ldots,r$, the statement of the Theorem 2, which refers to the exponential rate of the averaged error probability, follows. □

Acknowledgements. A. S. likes to thank the members of the groups of Nihat Ay and Jürgen Jost at the MPI MiS, Milán Mosonyi and Markus Müller for their interest in the topic and useful discussions. The work of M. N. was supported in part by NSF Grant DMS-03-06497.

References

[1] K.M.R. Audenaert, J. Casamiglia, R. Munoz-Tapia, E. Bagan, Ll. Masanes, A. Acin and F. Verstraete, *Discriminating States: The Quantum Chernoff Bound*, Phys. Rev. lett. 98, 160501 (2007)

[2] K.M.R. Audenaert, M. Nussbaum, A. Szkoła and F. Verstraete, *Asymptotic Error Rates in Quantum Hypothesis Testing*, Commun. Math. Phys. (2008)

[3] S. Barett and S. Croke, *On the conditions for discrimination between quantum states with minimum error*, J. Phys. A: Math. Theor. 42 (2009)

[4] I. Bjelaković, T. Krüger, R. Seiler, Ra. Siegmund-Schultze and A. Szkoła, *The Shannon-McMillan theorem for ergodic quantum lattice systems*, Invent. Math. 155 Nr. 1 (2004)

[5] I. Bjelaković, T. Krüger, R. Seiler, Ra. Siegmund-Schultze and A. Szkoła, *Typical Support and Sanov Large Deviations of Correlated States*, Commun. Math. Phys. Vol 279, No. 2, 559–584 (2008)

[6] O. Bratteli and D.W. Robinson, *Operator Algebras and Quantum Statistical Mechanics I*, Springer, New York (1979)

[7] C.W. Helstrom, *Quantum Detection and Estimation Theory*, Acadamic Press, New York (1976)

[8] F. Hiai, M. Mosonyi, and T. Ogawa, *Large deviations and Chernoff bound for certain correlated states on the spin chain*, J. Math. Phys. 48, 123301 (2007)

[9] F. Hiai, M. Mosonyi, and T. Ogawa, *Error exponents in hypothesis testing for correlated states on a spin chain*, J. Math. Phys. 49, 032112 (2008)

[10] F. Hiai, M. Mosonyi, T. Ogawa, and M. Fannes, *Asymptotic distinguishability measures for shift-invariant quasi-free states of fermionic lattice systems*, J. Math. Phys. 49, 072104 (2008)

[11] F. Hiai, and D. Petz, *The proper formular for relative entropy and its asymptotics in quantum probability*, Commun. Math. Phys. 143, 99-114 (1991)

[12] G. Kimura, T. Miyadera, and H. Imai, *Optimal State Discrimination in General Probabilistic Theories*, arXiv:0808.3844

[13] A.S. Kholevo, *Probabilistic and Statsitical Aspects of Quantum Theory*, North-Holland Series in Probability and Statistics (1982)

[14] A.S. Kholevo, *On asymptotically optimal hypothesis testing in quantum statistics*, Theor. Probab. Appl. 23, 411–415 (1978)

[15] A.S. Holevo, *Investigations in the general theory of statistical decision*, Trudy Mat. Inst. Stelkov 124 (1978) (in Russian) [Engl. Translation in Proc. Stelkov Inst. of Math. 3 (1978)]

[16] V. Kargin, *On the Chernoff bound for efficiency of quantum hypothesis testing*, Ann. Statist. 33, 959-976 (2005)

[17] R. König, R. Renner, and C. Schaffner, *The operational meaning of mon- and max-entropy*, arXiv:0807.1338

[18] M. Nussbaum and A. Szkoła, *The Chernoff lower bound for symmetric quantum hypothesis testing*, The Annals of Statistics Vol.37, No. 2, 1040–1057 (2009)

[19] M. Nussbaum and A. Szkoła, *Asymptotically optimal discrimination between pure quantum states*, MPI MiS preprint 1/2010, submitted to TQC 2010 Proceedings (2010)

[20] T. Ogawa, and M. Hayashi, *On error exponents in quantum hypothesis testing*, IEEE Trans. Inform. Theory 50, 1368-1372 (2004)

[21] D. Ruelle, *Statistical Mechanics*, W.A. Benjamin, New York (1969)

[22] N.P Salikhov, *On one generalisation of Chernov's distance*, Theory Probab. Appl. Vol. 43, No. 2, 239-255 (1999)

[23] J. Tyson, *Two-sided estimates of minimum-error distinguishability of mixed quantum states via generalized Holevo-Curlander bounds* J. Math. Phys. 50, 032106 (2009)

[24] H.P. Yuen, R.S. Kennedy, and M. Lax, *Optimum testing of Multiple Hypotheses in Quantum Detection Theory*, IEEE Trans. Inform. Thoery Vol. IT-21, No. 2, 125–134 (1975)