Attainment of the multiple quantum Chernoff bound for certain ensembles of mixed states

Michael Nussbaum
Department of Mathematics, Cornell University, Ithaca NY 14853, USA

We consider the problem of detecting the true quantum state among r possible ones, based on measurements performed on n of copies of a finite dimensional quantum system. It is known that the exponent for the rate of decrease of the averaged error probability cannot exceed the multiple quantum Chernoff bound (MQCB) defined as the worst case (smallest) quantum Chernoff distance between any possible pair of the r states. This error exponent is attainable for r pure states, but for the general case of mixed states only attainability up to a factor 1/3 is known. Here we show that the MQCB is attainable for mixed states if there is a pair which is closer in quantum Chernoff distance than 1/6 times the distance between all other pairs.

I. INTRODUCTION AND MAIN RESULT

Consider the problem of discrimination between several quantum hypotheses $H_i : \rho = \rho_i$, $i = 1, \dots, r$, $r \geq 2$, where $\Sigma = \{\rho_1, \dots, \rho_r\}$ is a set of $d \times d$ density matrices identified with a quantum state on $\mathbb{C}^d$. A quantum decision rule with r possible outcomes is given by a POVM (positive operator valued measure), that is a set of complex self-adjoint positive matrices $d \times d$ matrices $E = \{E_1, \dots, E_r\}$ satisfying $\sum_{i=1}^r E_i = \mathbf{1}$. We will refer to the r-tuple E as a *quantum multiple test* or a *quantum detector*. In the special case where all E_i are projections, the r-tuple E is called a PVM (projection valued measure) or von Neumann measurement. The individual success probability, i.e. the probability to accept hypothesis H_i when ρ_i is the true state, is given by $\mathrm{tr}\,[\rho_i E_i]$, with corresponding error probability $\mathrm{tr}\,[\rho_i(\mathbf{1} - E_i)]$. The total (averaged) sucess and error probabilities are then

$$\mathrm{Succ}(E) := \frac{1}{r}\sum_{i=1}^r \mathrm{tr}\,[\rho_i E_i],$$

$$\mathrm{Err}(E) := 1 - \mathrm{Succ}(E) = \frac{1}{r}\sum_{i=1}^r \mathrm{tr}\,[\rho_i(\mathbf{1} - E_i)].$$

For the case of two hypotheses $r = 2$, the optimal (Bayes) test for each $n \in \mathbb{N}$ is known to be the *Holevo-Helstrom hypothesis test*. It is given by the PVM $E^\dagger = \left\{E_1^\dagger, E_2^\dagger\right\}$ where

$$E_1^\dagger = \mathrm{supp}\,(\rho_1^{\otimes n} - \rho_2^{\otimes n})_+,\ E_2^\dagger = \mathbf{1} - E_1^\dagger, \qquad (1)$$

supp a being the projection onto the space spanned by the columns of a, and a_+ denotes the positive part of a self-adjoint operator a. The Bayes detector $E^\dagger$ for the general case $r \geq 2$ has been described in [4], [12]; explicit expressions for its r components are not known in general if $r > 2$.

The above describes the basic setup where the finite dimension d is arbitrary and the hypotheses are equiprobable. We consider the quantum analog of having n independent identically distributed observations. For this, the r hypotheses are assumed to be given by the set $\Sigma^{\otimes n} := \left\{\rho_1^{\otimes n}, \dots, \rho_r^{\otimes n}\right\}$ $i = 1, \dots, r$, where $\rho^{\otimes n}$ is the n-fold tensor product of ρ with itself. The detectors $E = \{E_1, \dots, E_r\}$ now operate on the states $\rho_i^{\otimes n}$, but E_i need not have tensor product structure. The corresponding total error probability of a detector E is now

$$\mathrm{Err}_n(E) = 1 - \sum_{i=1}^r \frac{1}{r}\mathrm{tr}\,\left[\rho_i^{\otimes n} E_i\right].$$

If for a sequence of detectors $E_{(n)}$ the limit $\lim_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}_n\left(E_{(n)}\right)$ exists, we refer to it as the *(asymptotic) error exponent*. For two density matrices ρ_1 and ρ_2 the *quantum Chernoff bound* is defined by

$$\xi_{QCB}(\rho_1, \rho_2) := -\log \inf_{0\leq s\leq 1} \mathrm{tr}\,\left[\rho_1^{1-s}\rho_2^s\right]. \qquad (2)$$

The basic properties of $\xi_{QCB}(\rho_1, \rho_2)$ have been discussed in [2]. For the binary discrimination problem, it is known that the Holevo-Helstrom (Bayes) detector $E_{(n)}^\dagger$ satisfies

$$\lim_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}_n\left(E_{(n)}^\dagger\right) = \xi_{QCB}(\rho_1, \rho_2), \qquad (3)$$

thus specifying $\xi_{QCB}(\rho_1, \rho_2)$ as the optimal error exponent (cf. [1], [2], [6]), and providing the quantum analog of the classical Chernoff bound.

For a set $\Sigma = \{\rho_1, \dots, \rho_r\}$ of density operators on $\mathbb{C}^d$, where $r \geq 2$, the *multiple quantum Chernoff bound* (MQCB) $\xi_{QCB}(\Sigma)$ was introduced in [7]:

$$\xi_{QCB}(\Sigma) := \min\{\xi_{QCB}(\rho_i, \rho_j) :\ 1 \leq i < j \leq r\}. \qquad (4)$$

If all the states are jointly diagonizable (commuting), then (4) reduces to the classical multiple Chernoff bound, as it was defined in [10], [11] for hypotheses represented by probability distributions. The following statement summarizes the known facts about $\xi_{QCB}(\Sigma)$ as an upper bound on the rate exponent, and its attainability in the general case of mixed states [7], [9].

Proposition 1 *Let $\Sigma = \{\rho_1, \dots, \rho_r\}$ be a finite set of hypothetic states on $\mathbb{C}^d$.*
a) For any sequence $\{E_{(n)}\}$ of quantum detectors relative to $\Sigma^{\otimes n}$ one has

$$\limsup_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}_n\left(E_{(n)}\right) \le \xi_{QCB}(\Sigma). \tag{5}$$

b) There exists a sequence $\{E^{\ddagger}_{(n)}\}$ of quantum detectors such that

$$\lim_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}_n\left(E^{\ddagger}_{(n)}\right) \ge \frac{1}{3}\xi_{QCB}(\Sigma). \tag{6}$$

Note that (6) implies the same relation for the Bayes detector $E^{\dagger}_{(n)}$. In special cases the factor 1/3 in (6) can be removed, e.g. if Σ is a set of (distinct) pure states [7] or more generally if ρ_i are pairwise linearly independent states [9]. For pure states in the context of quantum optics, in a local operations and classical communication (LOCC) framework cf. [5].
The condition of pairwise linear independence [3], [9] does not allow for full rank density matrices ρ_i (faithful states). The purpose of this note is to show attainability of $\xi_{QCB}(\Sigma)$ under another special condition, which allows for faithful states. To state it, for any pair $i<j$, define $\xi_{ij} := \xi_{QCB}(\rho_i,\rho_j)$ and the expression

$$\bar{\xi}_{ij}(\Sigma) := \min\{\xi_{kl} :\ 1 \le k < l \le r, (k,l) \ne (i,j)\}. \tag{7}$$

Theorem. *Assume there is a pair of states $\{\rho_i,\rho_j\} \subset \Sigma$, $i<j$, such that*

$$\xi_{ij} \le \frac{1}{6}\bar{\xi}_{ij}(\Sigma). \tag{8}$$

Then there exists a sequence $\{E_{(n)}\}$ of quantum detectors relative to $\Sigma^{\otimes n}$ such that

$$\lim_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}_n\left(E_{(n)}\right) \ge \xi_{QCB}(\Sigma). \tag{9}$$

Note that under the condition of the Theorem, one has $\xi_{QCB}(\Sigma) = \xi_{ij}$, thus $\{\rho_i,\rho_j\}$ is a unique "least favorable pair", that is, the closest pair in Chernoff distance. The condition says that that there is a pair with distance smaller than 1/6 the distance between all other pairs.

II. PROOF OF THE THEOREM

In what follows we assume a general set Σ of $r \ge 3$ density operators, not necessarily fulfilling (8). We assume w.l.g. that the pair ρ_1,ρ_2 is a least favorable, so that $\xi_{QCB}(\Sigma) = \xi_{12} = \min_{i<j}\xi_{ij}$. Note that in general the least favorable pair need not be unique. To ease notation, we will work with sums (rather than averages) of success and error probabilities $\mathrm{Err}_{\mathrm{sm}}(E) := r\mathrm{Err}(E)$ and $\mathrm{Succ}_{\mathrm{sm}}(E) := r\mathrm{Succ}(E)$.

Proposition 2 *There exists a sequence $\{E_{(n)}\}$ of quantum detectors relative to $\Sigma^{\otimes n}$ such that*

$$-\frac{1}{n}\log \mathrm{Err}_{\mathrm{sm}}(E^{(n)}) \ge \min\left(\xi_{12}, \frac{1}{6}\bar{\xi}_{12}(\Sigma)\right). \tag{10}$$

Consequently (9) holds if (8) is fulfilled.

For the proof, we initially assume formally $n=1$ and construct a POVM relative to Σ which uses the Holevo-Helstrom PVM for the pair ρ_1,ρ_2 as an ingredient. To this end, let E_i, $i=3,\dots,r$ be an arbitrary collection of positive operators on $\mathbb{C}^d$ satisfying $\sum_{i=3}^r E_i \le \mathbf{1}$, $\sum_{i=3}^r E_i \ne \mathbf{1}$. In the POVM to be constructed, the E_i, $i \ge 3$ will be understood as the elements corresponding to a decision in favor of ρ_i. We will complement this to a full POVM for discriminating between all ρ_i, $1 \le i \le r$ in the following way.
Let $E^{\dagger} = \left\{E_1^{\dagger}, E_2^{\dagger}\right\}$ be the Holevo-Helstrom PVM given by (1) for discriminating between ρ_1 and ρ_2. Note the easily verifiable relations

$$\rho_1 E_2^{\dagger} + \rho_2 E_1^{\dagger} = E_2^{\dagger}\rho_1 + E_1^{\dagger}\rho_2 =: \rho_1 \wedge \rho_2 \tag{11}$$

defining a self adjoint, but not necessarily positive matrix $\rho_1\wedge\rho_2$ with the property $\mathrm{tr}\left[\rho_1\wedge\rho_2\right] = \mathrm{Err}_{\mathrm{sm}}\left(E^{\dagger}\right) \ge 0$. Let $\tilde{E}_3 = \sum_{i=3}^r E_i$, let $Q = \mathbf{1} - \tilde{E}_3$ and define the full POVM $E = \{E_1, E_2, E_i, i=3,\dots,r\}$ now by setting

$$E_i := Q^{1/2} E_i^{\dagger} Q^{1/2},\ i=1,2.$$

Indeed this is a POVM: E_i, $i=1,2$ are positive and

$$\begin{aligned} E_1 + E_2 &= Q^{1/2}\left(E_1^{\dagger} + E_2^{\dagger}\right)Q^{1/2} \\ &= Q = \mathbf{1} - \tilde{E}_3 = \mathbf{1} - \sum_{i=3}^r E_i. \end{aligned}$$

Lemma. *With the above determination of a POVM E, we have*

$$\begin{aligned} \mathrm{Err}_{\mathrm{sm}}(E) \le\ & 2\mathrm{tr}\left[\rho_1\wedge\rho_2\right] \\ & + 3\mathrm{tr}\left[(\rho_1+\rho_2)\left(\sum_{i=3}^r E_i\right)\right] \\ & + \sum_{i=3}^r \mathrm{tr}\left[\rho_i\left(\mathbf{1}-E_i\right)\right]. \end{aligned}$$

Proof. Define $F_i := \mathbf{1} - E_i^{\dagger}$, $i=1,2$ (thus $F_1 = E_2^{\dagger}$) ; then for $i=1,2$

$$\begin{aligned} \mathrm{tr}\left[\rho_i E_i\right] &= \mathrm{tr}\left[\rho_i Q^{1/2} E_i^{\dagger} Q^{1/2}\right] \\ &= \mathrm{tr}\left[\rho_i Q^{1/2}\left(\mathbf{1}-F_i\right)Q^{1/2}\right] \\ &= \mathrm{tr}\left[\rho_i Q\right] - \mathrm{tr}\left[\rho_i Q^{1/2} F_i Q^{1/2}\right] \\ &= \mathrm{tr}\left[\rho_i\right] - \mathrm{tr}\left[\rho_i\tilde{E}_3\right] - \mathrm{tr}\left[\rho_i Q^{1/2} F_i Q^{1/2}\right] \\ &= 1 - \mathrm{tr}\left[\rho_i\tilde{E}_3\right] - \mathrm{tr}\left[\rho_i Q^{1/2} F_i Q^{1/2}\right]. \end{aligned}$$

Hence

$$\begin{aligned}
&\mathrm{Succ}_{\mathrm{sm}}(E)\\
&= \sum_{i=1,2} \mathrm{tr}\left[\rho_i E_i\right] + \sum_{i=3}^{r} \mathrm{tr}\left[\rho_i E_i\right]\\
&= 2 - \mathrm{tr}\left[\left(\rho_1+\rho_2\right)\tilde{E}_3\right]\\
&\quad - \sum_{i=1,2} \mathrm{tr}\left[\rho_i Q^{1/2} F_i Q^{1/2}\right] + \sum_{i=3}^{r} \mathrm{tr}\left[\rho_i E_i\right]\\
&= r - \mathrm{tr}\left[\left(\rho_1+\rho_2\right)\tilde{E}_3\right]\\
&\quad - \sum_{i=1,2} \mathrm{tr}\left[\rho_i Q^{1/2} F_i Q^{1/2}\right] - \sum_{i=3}^{r} \mathrm{tr}\left[\rho_i \left(\mathbf{1}-E_i\right)\right].
\end{aligned}$$

This implies

$$\begin{aligned}
\mathrm{Err}_{\mathrm{sm}}(E) &= r - \mathrm{Succ}_{\mathrm{sm}}(E)\\
&= \mathrm{tr}\left[\left(\rho_1+\rho_2\right)\tilde{E}_3\right] + \sum_{i=1,2} \mathrm{tr}\left[\rho_i Q^{1/2} F_i Q^{1/2}\right]\\
&\quad + \sum_{i=3}^{r} \mathrm{tr}\left[\rho_i \left(\mathbf{1}-E_i\right)\right].
\end{aligned}$$

Let $R := \mathbf{1} - Q^{1/2}$; since $0 \le Q \le \mathbf{1}$, we also have $0 \le R \le \mathbf{1}$. Hence

$$\begin{aligned}
&\sum_{i=1,2} \mathrm{tr}\left[\rho_i Q^{1/2} F_i Q^{1/2}\right]\\
&= \mathrm{tr}\left[\rho_1 F_1\right] + \mathrm{tr}\left[\rho_2 F_2\right] \qquad (12)\\
&- 2\mathrm{tr}\left[\rho_1 R F_1\right] - 2\mathrm{tr}\left[\rho_2 R F_2\right] \qquad (13)\\
&+ \mathrm{tr}\left[\rho_1 R F_1 R\right] + \mathrm{tr}\left[\rho_2 R F_2 R\right]. \qquad (14)
\end{aligned}$$

In view of (11), expression (12) equals $\mathrm{tr}\left[\rho_1 \wedge \rho_2\right]$. Regarding (13), we have

$$\begin{aligned}
&\mathrm{tr}\left[\rho_1 R F_1\right] + \mathrm{tr}\left[\rho_2 R F_2\right]\\
&= \mathrm{tr}\left[R F_1 \rho_1\right] + \mathrm{tr}\left[R F_2 \rho_2\right]\\
&= \mathrm{tr}\left[\left(\rho_1 \wedge \rho_2\right) R\right]
\end{aligned}$$

and thus for the modulus of (13),

$$\begin{aligned}
&2\left|\mathrm{tr}\left[\left(\rho_1 \wedge \rho_2\right) R\right]\right|\\
&\le 2 \sum_{i=1,2} \left|\mathrm{tr}\left[F_i \rho_i^{1/2} \rho_i^{1/2} R\right]\right|\\
&\le 2 \sum_{i=1,2} \left(\mathrm{tr}\left[F_i \rho_i F_i\right] \mathrm{tr}\left[R \rho_i R\right]\right)^{1/2}
\end{aligned}$$

by the Cauchy-Schwarz inequality. Using the inequality $2ab \le a^2 + b^2$ we deduce

$$\begin{aligned}
&2\left|\mathrm{tr}\left[\left(\rho_1 \wedge \rho_2\right) R\right]\right|\\
&\le \sum_{i=1,2} \left(\mathrm{tr}\left[F_i \rho_i F_i\right] + \mathrm{tr}\left[R \rho_i R\right]\right)\\
&= \sum_{i=1,2} \left(\mathrm{tr}\left[F_i \rho_i\right] + \mathrm{tr}\left[\rho_i R^2\right]\right)\\
&= \mathrm{tr}\left[\rho_1 \wedge \rho_2\right] + \mathrm{tr}\left[\left(\rho_1+\rho_2\right) R^2\right]
\end{aligned}$$

using the fact that F_i are projections. Note that for any $x \in [0,1]$ we have $\left(1-(1-x)^{1/2}\right)^2 \le x$; hence

$$R^2 = \left(\mathbf{1} - \left(\mathbf{1} - \tilde{E}_3\right)^{1/2}\right)^2 \le \tilde{E}_3. \qquad (15)$$

Hence the term (13) is bounded in absolute value by

$$2\left|\mathrm{tr}\left[\left(\rho_1 \wedge \rho_2\right) R\right]\right| \le \mathrm{tr}\left[\rho_1 \wedge \rho_2\right] + \mathrm{tr}\left[\left(\rho_1+\rho_2\right)\tilde{E}_3\right].$$

For the term (14) we obtain

$$\begin{aligned}
&\sum_{i=1,2} \mathrm{tr}\left[\rho_i R F_i R\right]\\
&= \sum_{i=1,2} \mathrm{tr}\left[\rho_i^{1/2} R F_i R \rho_i^{1/2}\right]\\
&\le \sum_{i=1,2} \mathrm{tr}\left[\rho_i^{1/2} R^2 \rho_i^{1/2}\right]\\
&\le \mathrm{tr}\left[\left(\rho_1+\rho_2\right)\tilde{E}_3\right]
\end{aligned}$$

where in the last inequality (15) has been used again. Summarizing the upper bounds for (12)-(14) we obtain the lemma. ■

In view of the decomposition of the error probability given by the Lemma, the strategy is now to choose a good POVM $\{Q, E_i, i=3,\ldots,r\}$ for decision between $\left(\rho_1+\rho_2\right)/2$ and ρ_i, $i=3,\ldots,r$. We will proceed to the tensor product case where ρ_i is replaced by $\rho_i^{\otimes n}$. Furthermore, set $n = n_1 + n_2$ where n_i will be determined later. Then $\rho_i^{\otimes n} = \rho_i^{\otimes n_1} \otimes \rho_i^{\otimes n_2}$.

For $i=1,2$, let $E^{(n,i)} := \left\{E_i^{(n,i)}, E_j^{(n,i)},\ j=3,\ldots,r\right\}$ be an arbitrary POVM for decision between the $r-1$ density operators $\left\{\rho_i^{\otimes n}, \rho_j^{\otimes n}, j=3,\ldots,r\right\}$. The corresponding sum of error probabilities is, for $i=1,2$

$$\begin{aligned}
\mathrm{Err}_{\mathrm{sm}}(E^{(n,i)}) &= \mathrm{tr}\left[\rho_i^{\otimes n}\left(\mathbf{1} - E_i^{(n,i)}\right)\right]\\
&\quad + \sum_{j=3}^{r} \mathrm{tr}\left[\rho_j^{\otimes n}\left(\mathbf{1} - E_j^{(n,i)}\right)\right].
\end{aligned}$$

We now set

$$E_j^{(n)} := E_j^{(n_1,1)} \otimes E_j^{(n_2,2)},\ j=3,\ldots,r; \qquad (16)$$

this choice determines $\tilde{E}_3 = \sum_{i=3}^{r} E_j^{(n)}$ and hence the full POVM. To estimate the error probability $\mathrm{tr}\left[\frac{1}{2}\left(\rho_1^{\otimes n} + \rho_2^{\otimes n}\right)\tilde{E}_3\right]$, consider the two terms sepa-

rately:

$$\begin{aligned}
&\mathrm{tr}\left[\rho_1^{\otimes n}\tilde{E}_3\right]\\
&=\sum_{j=3}^{r}\mathrm{tr}\left[\rho_1^{\otimes n}\left(E_j^{(n_1,1)}\otimes E_j^{(n_2,2)}\right)\right]\\
&=\sum_{j=3}^{r}\mathrm{tr}\left[\rho_1^{\otimes n_1}E_j^{(n_1,1)}\otimes\rho_1^{\otimes n_2}E_j^{(n_2,2)}\right]\\
&=\sum_{j=3}^{r}\mathrm{tr}\left[\rho_1^{\otimes n_1}E_j^{(n_1,1)}\right]\mathrm{tr}\left[\rho_1^{\otimes n_2}E_j^{(n_2,2)}\right]\\
&\le\sum_{j=3}^{r}\mathrm{tr}\left[\rho_1^{\otimes n_1}E_j^{(n_1,1)}\right]=\mathrm{tr}\left[\rho_1^{\otimes n_1}\left(\mathbf{1}-E_1^{(n_1,1)}\right)\right]\\
&\le\mathrm{Err}_{\mathrm{sm}}(E^{(n_1,1)})
\end{aligned}$$

and analogously

$$\mathrm{tr}\left[\rho_2^{\otimes n}\tilde{E}_3\right]\le\mathrm{Err}_{\mathrm{sm}}(E^{(n_2,2)})$$

Now for $3\le j\le r$ consider the term $\mathrm{tr}\left[\rho_j^{\otimes n}\left(\mathbf{1}-E_j^{(n)}\right)\right]$ in the overall error probability given by the lemma. With our current definition of $E_j^{(n)}$ (16), we have

$$\begin{aligned}
\mathbf{1}-E_j^{(n)}&=\left(\mathbf{1}-E_j^{(n_1,1)}+E_j^{(n_1,1)}\right)\\
&\quad\otimes\left(\mathbf{1}-E_j^{(n_2,2)}+E_j^{(n_2,2)}\right)\\
&\quad-E_j^{(n)}\\
&=\left(\mathbf{1}-E_j^{(n_1,1)}\right)\otimes\left(\mathbf{1}-E_j^{(n_2,2)}\right)\\
&\quad+\left(\mathbf{1}-E_j^{(n_1,1)}\right)\otimes E_j^{(n_2,2)}\\
&\quad+E_j^{(n_1,1)}\otimes\left(\mathbf{1}-E_j^{(n_2,2)}\right).
\end{aligned}$$

Consequently

$$\begin{aligned}
&\mathrm{tr}\left[\rho_j^{\otimes n}\left(\mathbf{1}-E_j^{(n)}\right)\right]\\
&=\mathrm{tr}\left[\rho_j^{\otimes n_1}\left(\mathbf{1}-E_j^{(n_1,1)}\right)\right]\mathrm{tr}\left[\rho_j^{\otimes n_2}\left(\mathbf{1}-E_j^{(n_2,2)}\right)\right]\\
&\quad+\mathrm{tr}\left[\rho_j^{\otimes n_1}\left(\mathbf{1}-E_j^{(n_1,1)}\right)\right]\mathrm{tr}\left[\rho_j^{\otimes n_2}E_j^{(n_2,2)}\right]\\
&\quad+\mathrm{tr}\left[\rho_j^{\otimes n_1}E_j^{(n_1,1)}\right]\mathrm{tr}\left[\rho_j^{\otimes n_2}\left(\mathbf{1}-E_j^{(n_2,2)}\right)\right]\\
&\le\mathrm{tr}\left[\rho_j^{\otimes n_1}\left(\mathbf{1}-E_j^{(n_1,1)}\right)\right]\\
&\quad+\mathrm{tr}\left[\rho_j^{\otimes n_1}\left(\mathbf{1}-E_j^{(n_1,1)}\right)\right]\\
&\quad+\mathrm{tr}\left[\rho_j^{\otimes n_2}\left(\mathbf{1}-E_j^{(n_2,2)}\right)\right].
\end{aligned}$$

Hence the sum of error terms is

$$\begin{aligned}
&\sum_{j=3}^{r}\mathrm{tr}\left[\rho_j^{\otimes n}\left(\mathbf{1}-E_j^{(n)}\right)\right]\\
&\le 2\sum_{i=1,2}\sum_{j=3}^{r}\mathrm{tr}\left[\rho_j^{\otimes n_i}\left(\mathbf{1}-E_j^{(n_i,i)}\right)\right]\\
&\le 2\mathrm{Err}_{\mathrm{sm}}(E^{(n_1,1)})+2\mathrm{Err}_{\mathrm{sm}}(E^{(n_2,2)}).
\end{aligned}$$

Finally we obtain for our overall POVM $E^{(n)}$, according to the Lemma,

$$\begin{aligned}
\mathrm{Err}_{\mathrm{sm}}(E^{(n)})&\le 2\mathrm{tr}\left[\rho_1^{\otimes n}\wedge\rho_2^{\otimes n}\right]\\
&\quad+4\sum_{i=1,2}\mathrm{Err}_{\mathrm{sm}}(E^{(n_i,i)}).
\end{aligned}\tag{17}$$

To evaluate this bound, we now have the choice of n_1, n_2 and the two POVM $E^{(n_1,1)}$, $E^{(n_2,2)}$. We set

$$n_1=[nw_1]\,,\ n_2=n-n_1\ \text{where}\ w_1+w_2=1.$$

Let us make a crude choice $w_1=w_2=1/2$. For the POVM $E^{(n_i,i)}$, which decides between $\rho_i^{\otimes n}$, $\rho_3^{\otimes n},\ldots,\rho_r^{\otimes n}$, we choose the method that attains $1/3$ of the Chernoff bound for this set of states, that is we choose the detector $E^{\ddagger}_{(n_i)}$ from (6), for $i=1,2$. Defining sets of index pairs

$$J_i=\left\{(k,l)\in\{i,3,\ldots,r\}^{\times 2}\,,k<l\right\},i=1,2$$

we obtain for $i=1,2$

$$\begin{aligned}
&-\frac{1}{n_i}\log\mathrm{Err}_{\mathrm{sm}}(E^{(n_i,i)})\\
&\ge\frac{1}{3}\min\left\{\xi_{kl}:(k,l)\in J_i\right\}.
\end{aligned}$$

Now note that with $\bar{\xi}_{12}(\Sigma)$ from (7) we have

$$\min\left\{\xi_{kl}:(k,l)\in J_1\cup J_2\right\}=\bar{\xi}_{12}(\Sigma).$$

Thus, taking into account $n_i=n/2\,(1+o(1))$, $i=1,2$, we obtain

$$\begin{aligned}
&-\frac{1}{n}\log\left(\mathrm{Err}_{\mathrm{sm}}(E^{(n_1,1)})+\mathrm{Err}_{\mathrm{sm}}(E^{(n_2,2)})\right)\\
&\ge\frac{1}{6}\bar{\xi}_{12}(\Sigma).
\end{aligned}$$

Thus from (17) and the binary quantum Chernoff bound (3)

$$-\frac{1}{n}\log\mathrm{tr}\left[\rho_1^{\otimes n}\wedge\rho_2^{\otimes n}\right]\ge\xi_{12}$$

we obtain the claim (10).

III. CONCLUSIONS

Refined results of this type can be obtained if we optimize the sample size weights w_1, w_2 and /or choose the detectors $E^{(n_i,i)}$, $i = 1, 2$ from the blocking algorithm ("test between pairs" method) applied in [8]. Indeed it has been shown in [8] that for every $\varepsilon > 0$, there are ensembles Σ of mixed states and detectors $E_{(n)}$ such that

$$\lim_{n\to\infty} -\frac{1}{n}\log \mathrm{Err}_n\left(E_{(n)}\right) \geq (1-\varepsilon)\xi_{QCB}(\Sigma),$$

improving the general bound (6). Furthermore, the method applied here, based on the risk decomposition given in the Lemma, may be applied recursively. This shows that there is a multitude of special configurations of the set Σ of general (possibly mixed) states where the MQCB is attained, lending further support to the conjecture that it is attainable in general.

[1] Audenaert, K.M.R., Casamiglia, J., Munoz-Tapia, R., Bagan, E., Masanes, Ll., Acin, A., and Verstraete, F., *Phys. Rev. Lett.* **98**, 160501 (2007)

[2] Audenaert, K.M.R., Nussbaum, M., Szkoła, A., and Verstraete, F., *Comm. Math. Phys.* **279** (1), 251-283 (2008)

[3] Eldar, Y. , *Phys. Review A* **68**, 052303 (2003)

[4] Holevo, A.S., *J. Multivar. Anal.* **3** (4), 337-394 (1973)

[5] Nair, R., Guha, S. and Tan, S., arXiv:1212.2048 (2013)

[6] Nussbaum, M. and Szkoła, A., *Ann. Statist.* **37** (2), 1040-1057 (2009)

[7] Nussbaum, M. and Szkoła, A., in *Theory of Quantum Computation, Communication and Cryptography.* 5th Conference, TQC 2010, Leeds, UK. Revised Selected Papers. Lecture Notes in Computer Science, Vol 6519, van Dam, W., Kendon, V. M., and Severini, S. (Eds.), 1-8, Springer (2011)

[8] Nussbaum, M. and Szkoła, A., *J. Math. Phys.* **51**, 072203 (2010)

[9] Nussbaum, M. and Szkoła, A. , *Ann. Statist.* **39** (6), 3211-3233 (2011)

[10] Salikhov, N. P. *Dokl. Akad. Nauk SSSR* **209**, 54-57 (Russian, 1973)

[11] Salikhov, N. P., *Theory Probab. Appl.* **47** (2), 286-298 (2003)

[12] Yuen, H.P., Kennedy, R.S., and Lax, M., *IEEE Trans. Inform. Theory* **IT-21** (2), 125-134 (1975)