Analytical bounds for non-asymptotic asymmetric state discrimination

Jason L. Pereira,1,2 Leonardo Banchi,2,3 and Stefano Pirandola1

1 Department of Computer Science, University of York, York YO10 5GH, UK
2 Department of Physics and Astronomy, University of Florence, via G. Sansone 1, I-50019 Sesto Fiorentino (FI), Italy
3 INFN Sezione di Firenze, via G. Sansone 1, I-50019, Sesto Fiorentino (FI), Italy

(Dated: July 25, 2022)

Two types of errors can occur when discriminating pairs of quantum states. Asymmetric state discrimination involves minimising the probability of one type of error, subject to a constraint on the other. We give explicit expressions bounding the set of achievable errors, using the trace norm, the fidelity, and the quantum Chernoff bound. These results, however, tell us nothing about the actual values of the two types of errors, only the rates at which they decay.

In this paper, we give explicit expressions for \( \alpha \) and \( \beta \) in terms of the trace norm of a weighted difference between the states. We find Fuchs-van der Graaf style upper and lower bounds on this trace norm in terms of the fidelity, and therefore find bounds on the boundary of the set of achievable errors. We also find similar bounds based on the QCB. One such bound is asymptotically tight. All proofs can be found in the appendices.

Unlike previous results that deal with the asymptotic regime, these bounds allow the receiver operating characteristic for one-shot discrimination between any particular pair of states to be drawn.

In order to use the quantum Neyman-Pearson relation to calculate \( \alpha \) and \( \beta \), one needs to calculate the trace norm of a weighted difference between the states, and for high-dimensional or continuous variable systems (e.g. Gaussian states), this can be difficult to calculate. The bounds we present use the fidelity and the QCB, both of which can be easily calculated for Gaussian states [9,10]. In addition, for multi-copy states, both of these quantities can be expressed in terms of their single-copy values.

I. INTRODUCTION

Suppose we want to carry out one-shot discrimination between a pair of quantum states, \( \rho_1 \) and \( \rho_2 \). There are two types of errors that we are interested in. The type 1 error, which we call \( \alpha \), is the probability of identifying the state as \( \rho_2 \) when it is actually \( \rho_1 \), whilst the type 2 error, which we call \( \beta \), is the probability of identifying the state as \( \rho_1 \) when it is actually \( \rho_2 \).

There are two basic paradigms of quantum state discrimination: symmetric discrimination, where the aim is to minimise the average measurement error probability, and asymmetric discrimination, where the aim is to minimise the probability of one type of error subject to a constraint on the other.

In the symmetric setting, the optimal error probability is given, in terms of the trace distance between states, by the Helstrom bound. For asymmetric discrimination, we have the quantum Neyman-Pearson relation [1], which gives us the minimum weighted average of the two types of errors, and thus implicitly lets us find the boundary of the set of achievable errors. We can bound the trace distance between a pair of states using the fidelity, via the Fuchs-van der Graaf inequalities [2], or by using the quantum Chernoff bound (QCB) [3].

Asymmetric discrimination is needed in situations where one type of error is more undesirable than the other. Quantum target detection involves discriminating between different output states, and for applications such as quantum radar [4], it is often more important to avoid false-negatives (fail to spot a target that is present) than false-positives (detect a target when none is present).

Asymmetric state discrimination has largely been studied in the asymptotic regime, where the aim is to find the maximum exponent for the decay rate of one type of error, subject to a constraint on the other. This problem has been solved, via the quantum Stein’s lemma [5,6] and the quantum Hoeffding bound [7,8]. These results, however, tell us nothing about the actual values of the two types of errors, only the rates at which they decay.

In this paper, we give explicit expressions for \( \alpha \) and \( \beta \) in terms of the trace norm of a weighted difference between the states. We find Fuchs-van der Graaf style upper and lower bounds on this trace norm in terms of the fidelity, and therefore find bounds on the boundary of the set of achievable errors. We also find similar bounds based on the QCB. One such bound is asymptotically tight. All proofs can be found in the appendices.

Unlike previous results that deal with the asymptotic regime, these bounds allow the receiver operating characteristic for one-shot discrimination between any particular pair of states to be drawn.

In order to use the quantum Neyman-Pearson relation to calculate \( \alpha \) and \( \beta \), one needs to calculate the trace norm of a weighted difference between the states, and for high-dimensional or continuous variable systems (e.g. Gaussian states), this can be difficult to calculate. The bounds we present use the fidelity and the QCB, both of which can be easily calculated for Gaussian states [9,10]. In addition, for multi-copy states, both of these quantities can be expressed in terms of their single-copy values.

II. BOUNDS ON OPTIMAL ASYMMETRIC DISCRIMINATION

For measurement operators \( \Pi_1 \) and \( \Pi_2 \), where \( \Pi_2 = I - \Pi_1 \), we can write \( \alpha = \text{Tr}[\Pi_2 \rho_1] \) and \( \beta = \text{Tr}[\Pi_1 \rho_2] \).

The errors are connected via the quantum Neyman-Pearson relation, which states that [1]

\[
\alpha + T \beta \geq \alpha^* + T \beta^* = T - \text{Tr}[(T \rho_2 - \rho_1)_+],
\]

where \( T \) is any positive number, \( \{\alpha^*, \beta^*\} \) are a pair of achievable error probabilities that are optimal for a particular value of \( T \) in that they minimise \( \alpha + T \beta \), and \( (X)_+ \) denotes the positive part of \( X \). Similarly, \( (X)_- \) is defined as \( X - (X)_+ \), and is the negative part of \( X \). \( \{\alpha^*, \beta^*\} \) are achieved by the POVM

\[
\Pi^*_1,T = \{T \rho_2 - \rho_1\}_-, \quad \Pi^*_2,T = \{T \rho_2 - \rho_1\}_+.
\]
where \( \{X\}_\pm \) is the projector onto the positive/negative eigenspace of \( X \) and where we have assumed that \((T\rho_2 - \rho_1)\) is full rank. This assumption is just for the simplicity of ignoring the projector onto the kernel of \((T\rho_2 - \rho_1)\), which, if it exists, can be added to either POVM element.

We want explicit expressions for \( \alpha^* \) and \( \beta^* \) that let us draw the boundary of the set of achievable error probabilities, rather than the implicit expression given in Eq. (4). Such a curve is called the receiver operating characteristic (ROC), and tells us the optimal type 1 error for a given type 2 error and vice versa.

Suppose we have an expression for

\[
 t_p = \|(1-p)\rho_2 - p\rho_1\|_1, 
\]

in terms of the auxiliary parameter \( p \), which lies in the range \( 0 \leq p \leq 1 \). We can express \( \alpha^* \) and \( \beta^* \) as

\[
 \alpha^* = \frac{1 - t_p}{2} - \frac{1 - p}{2} \frac{dt_p}{dp}, \quad \beta^* = \frac{1 - t_p}{2} + p \frac{dt_p}{dp}. 
\]

Suppose, instead of having an expression for \( t_p \), we have an expression that bounds \( t_p \) from either above or below. Can we use this expression to bound \( \{\alpha^*, \beta^*\} \)?

Whilst this is not immediately obvious from Eq. (4), due to the differential term, it is the case that a lower bound on \( t_p \) gives an upper bound on the curve defining the boundary of achievable errors and an upper bound on \( t_p \) gives a lower bound. We are also guaranteed that if functions \( f_1 \) and \( f_2 \) both bound \( t_p \) from the same side, and \( f_2 \) is never tighter than \( f_1 \), then \( f_1 \) will give a tighter bound on the set of achievable errors than \( f_2 \).

### III. BOUNDS BASED ON THE FIDELITY

Let us bound \( t_p \) using Fuchs-van der Graaf style inequalities. Quantum fidelity is defined by \( F(\rho_1, \rho_2) = \|\sqrt{\rho_1} \sqrt{\rho_2}\|_1 \). Defining

\[
 t_p^{(\text{UB,F})} = \sqrt{1 - 4p(1-p)F(\rho_1, \rho_2)^2}, 
\]

\[
 t_p^{(\text{LB,F})} = 1 - 2\sqrt{p(1-p)}F(\rho_1, \rho_2), 
\]

we get the bounds \( t_p^{(\text{LB,F})} \leq t_p \leq t_p^{(\text{UB,F})} \). If both states are pure, the upper bound is an equality.

Using these bounds, we get the expressions

\[
 \alpha^{(\text{LB,F})} = \frac{2(1-p)F^2 - 1 + \sqrt{1 - 4p(1-p)F^2}}{2 \sqrt{1 - 4p(1-p)F^2}}, \quad \beta^{(\text{LB,F})} = \frac{2pF^2 - 1 + \sqrt{1 - 4p(1-p)F^2}}{2 \sqrt{1 - 4p(1-p)F^2}}, 
\]

which provide a lower bound on the boundary of the set of achievable errors, and

\[
 \alpha^{(\text{UB,F})} = \frac{F}{2} \sqrt{\frac{1-p}{p}}, \quad \beta^{(\text{UB,F})} = \frac{F}{2} \sqrt{\frac{p}{1-p}}, 
\]

which provide an upper bound on the boundary of the set of achievable errors.

To eliminate \( p \), we can substitute the expressions for the bounds on \( \beta \) into the expressions for the bounds on \( \alpha \). The lower bound becomes

\[
 \alpha^{(\text{LB,F})} = \beta - 2\beta F^2 + F \left( F - 2\sqrt{(1-\beta)\beta (1-F^2)} \right), \quad \beta^{(\text{LB,F})} = \frac{1}{F^2}\beta^{-1}, 
\]

whilst the upper bound becomes \( \alpha^{(\text{UB,F})} = \frac{1}{F^2}\beta^{-1} \). The lower bound meets the axes (of the ROC) at the points \((0, F^2)\) and \((F^2, 0)\), and is tight for pure states.

Eq. (4) diverges to infinity as \( p \to 0 \) and Eq. (10) diverges as \( p \to 1 \). This is non-physical, because the maximum possible error probability is 1. Therefore, we know the points \((0,1)\) and \((1,0)\) are achievable.

We can improve the upper bound by joining it up with its two tangents that pass through points \((0,1)\) and \((1,0)\) respectively, to get the tighter piecewise function

\[
 \alpha^{(\text{UB,F})} = \begin{cases} 
 1 - \frac{\beta}{F^2} & 0 \leq \beta \leq \frac{F^2}{2} \\
 \frac{F^2}{2\beta} & \frac{F^2}{2} \leq \beta \leq 1
\end{cases}. 
\]

These bounds are illustrated in Fig. 1, for a particular pair of states that have a fidelity of \( \sim 0.714 \).

### IV. BOUNDS BASED ON THE QUANTUM CHERNOFF BOUND

Since the (non-logarithmic) QCB gives a tighter lower bound on the trace distance than the Fuchs-van der Graaf bound, we might suspect that it could provide a tighter upper bound on the ROC. Defining

\[
 Q_s(\rho_1, \rho_2) = \text{Tr}[\rho_2^s \rho_1^{1-s}], 
\]

the QCB, \( Q_s \), is given by

\[
 Q_s = Q_s, \quad s_s = \arg\min_{0 \leq s \leq 1} Q_s. 
\]

We can show that

\[
 t_p \geq 1 - 2p^{1-s}(1-p)^s Q_s. 
\]

This defines a whole family of bounds.

We are interested in two scenarios in particular: fixing \( s \) to some set value, \( s = s_0 \), and setting \( s = s_{\text{opt}} \), the value of \( s \) that minimises the right-hand side of Eq. (15). \( s_{\text{opt}} \) is not a constant, like \( s_s \), but rather a function of \( p \).

For constant \( s = s_0 \)

\[
 \alpha^{(\text{UB,s}_0)} = \left( \frac{1-p}{p} \right)^{s_0} (1-s_0) Q_{s_0}, \quad \beta^{(\text{UB,s}_0)} = \left( \frac{p}{1-p} \right)^{1-s_0} s_0 Q_{s_0},
\]

where \( \{X\}_\pm \) is the projector onto the positive/negative eigenspace of \( X \) and where we have assumed that \((T\rho_2 - \rho_1)\) is full rank. This assumption is just for the simplicity of ignoring the projector onto the kernel of \((T\rho_2 - \rho_1)\), which, if it exists, can be added to either POVM element.
We can eliminate $p$ to get
\[
\alpha^{(UB,s_0)} = (1 - s_0)^{\frac{1}{s_0}} \left( \frac{s_0}{p} \right)^{\frac{1}{s_0}}.
\] (18)

In particular, we might consider setting $s_0 = s_*$, so that $Q_{s*} = Q_*$ (the QCB).

This entire family of bounds (fixed $s = s_0$) diverges when one of the errors is small (similarly to the fidelity-based upper bound). We can again formulate piecewise bounds, using the tangents to these curves that pass through the points $(0,1)$ and $(1,0)$:
\[
\alpha^{(UB,s_0)} = \begin{cases} 
1 - \beta Q_{s_0}^{-\frac{1}{s_0}} & 0 \leq \beta \leq s_0 Q_{s_0}^{-\frac{1}{s_0}} \\
(1 - s_0) Q_{s_0}^{-\frac{1}{s_0}} \left( \frac{s_0}{p} \right)^{\frac{1}{s_0}} & \text{else} \\
(1 - \beta) Q_{s_0}^{-\frac{1}{s_0}} & s_0 \leq \beta \leq 1
\end{cases}.
\] (19)

We will refer to this family of bounds as constant asymmetric QCBs (CAQCBs).

The bounds obtained by setting $s = s_{\text{opt}}$ are
\[
\alpha^{(UB,QCB)} = \exp \left[ -p Q_p^{-1} \frac{dQ_p}{dp} \right] (1 - p) Q_p, \quad \beta^{(UB,QCB)} = \exp \left[ (1 - p) Q_p^{-1} \frac{dQ_p}{dp} \right] p Q_p.
\] (20)

These expressions give the optimal upper bounds based on the QCB, so we will refer to this bound as the optimal asymmetric QCB (OAQCB).

Unlike the upper bound based on the fidelity or the CAQCBs, the OAQCB meets the axes at points $(0, Q_1)$ and $(Q_0, 0)$ (and $Q_*$, 1), so does not require piecewise modification. As demonstrated in Fig. 1, the OAQCB meets the CAQCB with $s_0$ set to $s_*$ at the point $p = s_*$ (in fact, any CAQCB meets the OAQCB at $p = s_0$).

\section{V. Multicopy Scaling}

Let us consider how the bounds scale if we have multi-copy states. This means that the two states we are discriminating between now take the form $\rho_{1}^{\otimes N}$ and $\rho_{2}^{\otimes N}$. We are interested in the scaling of the bounds with $N$.

The trace distance between multi-copy states cannot be expressed in terms of the single-copy trace distance. On the other hand, both the fidelity and $Q_s$ (as defined in Eq. (13)) are simply given by their single-copy values ($F_{(1)}$ and $Q_{s,(1)}$) to the power of $N$. We can write
\[
F_{(N)} = F_{(1)}^N, \quad Q_{s,(N)} = Q_{s,(1)}^N.
\] (22)

This is one major benefit of using bounds based on the fidelity or the QCB rather than the trace norm.

For the bounds based on the fidelity (Eqs. (1) to (2), we replace $F$ with $F_{(1)}^N$, we find the $N$-copy versions of the CAQCBs (Eqs. (18) and (19)) in a similar way (replacing $Q_s$ with $Q_{s,(1)}^N$).

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{ROC for discriminating between a pair of states. Each is the result of transmitting one mode of a two-mode squeezed vacuum, with an average photon number (per mode) of 4, through a thermal loss channel. $\rho_1$ is obtained using a channel with a transmissivity of 0.3 and a thermal number of 1.5 whilst $\rho_2$ is obtained using a channel with a transmissivity of 0.7 and a thermal number of 0.5 [11]. “fid UB” and “fid LB” are the upper and lower bounds based on the fidelity. “CAQCB” is the upper bound obtained by setting $s_0 = s_*$ in Eq. (19). For the fidelity upper bound and the CAQCB, the dashed lines are the piecewise modifications of the bounds, whilst the solid lines are the original bounds. The fidelity lower bound and the OAQCB are the tightest lower and upper bounds and neither diverge for small errors.}
\end{figure}

For the OAQCB, we find:
\[
\alpha_{(N)}^{(UB,QCB)} = \left( \frac{\alpha_{(1)}^{(UB,QCB)}}{(1 - p)^{N-1}} \right)^N, \quad \beta_{(N)}^{(UB,QCB)} = \left( \frac{\beta_{(1)}^{(UB,QCB)}}{p^{N-1}} \right)^N.
\] (23)

\subsection{A. Quantum Hoeding Bound}

The quantum Hoeding bound [7, 8] is an asymptotic bound on the distinguishability of multi-copy states. It constrains the maximum asymptotic decay rate of one type of error, subject to a constraint on the asymptotic decay rate of the other. For a family of discrimination tests on multi-copy states, $T_N$, with corresponding type 1 and 2 errors, $\{\alpha_{N}, \beta_{N}\}$, we define the type 1 and 2 asymptotic decay rates as
\[
\gamma_{\alpha} = \lim_{N \to \infty} -\frac{1}{N} \ln \left( \frac{\alpha_{N}}{N} \right), \quad \gamma_{\beta} = \lim_{N \to \infty} -\frac{1}{N} \ln \left( \frac{\beta_{N}}{N} \right).
\] (25)
The quantum Hoeffding bound then gives the minimum possible value of $\gamma_T^{\alpha}$, subject to a constraint on $\gamma_T^{\beta}$. It states that if we define

$$b_{\text{max}}(r) = \sup_{0 \leq s < 1} b(r, s), \quad b(r, s) = \frac{-s r - \ln[Q_{s,(1)}]}{1 - s},$$

then

$$\sup\{\gamma_T^{\alpha} | \gamma_T^{\beta} \geq r\} = b_{\text{max}}(r).$$

This bound is asymptotic and defines the best achievable scaling with the number of copies, but does not give actual values of $\{\alpha, \beta\}$. It holds for $0 < r < S(p_1 \| p_2)$ (outside this range, the quantum Stein’s lemma applies).

Suppose we have a set of tests that achieve the OAQCB, with $p$ fixed for all $N$. We calculate:

$$\gamma^{\text{UB},\text{QCB}}_{\alpha} = pQ_{p,(1)} - \ln[Q_{p,(1)}],$$

$$\gamma^{\text{UB},\text{QCB}}_{\beta} = -(1 - p)Q_{p,(1)} - \ln[Q_{p,(1)}].$$

Setting $r = \gamma^{\text{UB},\text{QCB}}_{\beta}$ in Eq. (26), we find

$$b_{\text{max}}(\gamma^{\text{UB},\text{QCB}}_{\beta}) = b(\gamma^{\text{UB},\text{QCB}}_{\beta}, p) = \gamma^{\text{UB},\text{QCB}}_{\alpha},$$

showing that the OAQCB achieves the best possible scaling, according to the quantum Hoeffding bound. This means the OAQCB is asymptotically tight, and hence that any tighter upper bound can achieve at most a sub-exponential advantage.

### B. Quantum Stein’s Lemma

The quantum Stein’s lemma [5, 6] states that

$$\sup\{\gamma_T^{\alpha} | \gamma_T^{\beta} \geq 0\} = S(p_2 \| p_1),$$

$$\sup\{\gamma_T^{\alpha} | \gamma_T^{\beta} = S(p_1 \| p_2)\} = 0.$$  

In other words, the maximum exponential rate at which the type 1 error can decrease with $N$ such that the type 2 error does not exponentially increase with $N$ is given by the (single-copy) relative entropy between the states. We have shown that the OAQCB saturates the quantum Hoeffding bound, however this is only applicable in the range $0 < r < S(p_1 \| p_2)$. We can show that it also saturates the quantum Stein’s lemma.

Taking the limit of Eqs. (28) and (29) as $p \to 0$, we get

$$\gamma^{\text{UB},\text{QCB}}_{\alpha,p \to 0} = 0, \quad \gamma^{\text{UB},\text{QCB}}_{\beta,p \to 0} = S(p_1 \| p_2).$$

Taking the limit of Eqs. (28) and (29) as $p \to 1$, we get

$$\gamma^{\text{UB},\text{QCB}}_{\alpha,p \to 1} = S(p_2 \| p_1), \quad \gamma^{\text{UB},\text{QCB}}_{\beta,p \to 1} = 0.$$
where $\rho_{1,j}$ and $\rho_{2,j}$ have the same dimension for all $j$. In other words, both states can be partitioned into $N$ subsystems in the same way (but $\rho_{i,j}$ and $\rho_{i,k}$ can be different from each other, rather than identical copies). The optimal measurement can be achieved by carrying out an adaptive sequence of $N$ measurements on each subsystem individually. The measurement on the next subsystem only depends on the result of the previous measurement (not the entire sequence of results).

Eqs. (7) and (8) give a simple, alternative way to show this result. Consider the two-subsystem states $\rho_1 = \rho_{1,1} \otimes \rho_{1,2}$, where $F_1$ is the fidelity between $\rho_{1,1}$ and $\rho_{2,1}$. Now consider a measurement sequence in which we carry out an optimal measurement (from the curve defined by Eqs. (7) and (8)), with parameter $p_0$, on the first subsystem and then carry out another optimal measurement on the second subsystem, with the parameter depending on the previous measurement result. $p_1$ is the parameter if the first measurement tells us that the state is $\rho_{1,1}$ and $p_2$ is the parameter if the first measurement tells us that the state is $\rho_{2,1}$. Then, we use only the second measurement result to decide which state we have.

Using Eqs. (7) and (8) to calculate the error probabilities for the measurement sequence and setting

$$p_1 = \frac{1}{2} \left( 1 - \sqrt{1 - 4p_0(1 - p_0)F_1^2} \right),$$

$$p_2 = \frac{1}{2} \left( 1 + \sqrt{1 - 4p_0(1 - p_0)F_1^2} \right),$$

we find that this sequence achieves the optimal errors for discriminating between states with a fidelity of $F_1F_2$.

Finally, if the first subsystem can be partitioned into further subsystems, we can decompose the first measurement into a sequence of individual measurements on subsystems. In general, we choose a parameter, $p_0$, for the measurement on the first subsystem and then measurements on the $i$-th subsystem have a parameter value of

$$p_i = \frac{1}{2} \left( 1 \mp \sqrt{1 - 4p_0(1 - p_0) \prod_{j=1}^{i-1} F_j^2} \right),$$

where the minus case is used when the $(i - 1)$-th measurement indicates that the state is $\rho_1$ and the plus case is used when it indicates that the state is $\rho_2$.

\section*{VII. Discussion}

We have presented explicit expressions for the type 1 and 2 errors for discriminating between pairs of quantum states. Unlike asymptotic bounds, these expressions give actual values for the errors, rather than just error exponents. This could be useful for finite-copy scenarios, where the sub-exponential factors could be important. They give ultimate bounds on the performance of receivers, which can be applied to topics such as quantum target detection.

We have given upper and lower bounds on the ROC based on the fidelity, and a family of upper bounds on it based on the QCB (the CAQCBs and the OAQCB). These bounds can be easily calculated analytically for a wide variety of states, including Gaussian states. It is also simple to go from the single-copy expressions to multi-copy expressions.

The fidelity lower bound and the OAQCB are of particular interest. They are the tightest lower and upper bounds respectively, and neither are trivial for any parameter value. The fidelity lower bound is exact for pure states, whilst the OAQCB saturates the quantum Hoeffding bound, and so is asymptotically tight.

\section*{Acknowledgments}

J. L. P. and S. P acknowledge funding from the European Union’s Horizon 2020 Research and Innovation Action under grant agreement No. 862644 (FET-OPEN project: Quantum readout techniques and technologies, QUARTET). L. B. acknowledges funding from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Superconducting Quantum Materials and Systems Center (SQMS) under the contract No. DE-AC02-07CH11359.

\begin{thebibliography}{9}


Combining Eqs. (A5) and (A6), we get

\[ \mu_p = \frac{1}{2} (1 - t_p). \]  

Thus, we can express \( \mu_p \) in terms of \( t_p \), the trace norm of \((1-p)\rho_2 - pp_1\).

We therefore know that there exists some achievable pair of errors, \( \{\alpha_p, \beta_p\} \), such that

\[ po_p + (1-p)\beta_p = \frac{1}{2} (1 - t_p). \]  

Further, we know that there exists no pair of errors with a smaller value of \( \mu_p \). Therefore, the straight line (in a plot of \( \alpha \) versus \( \beta \))

\[ \alpha = - \frac{1-p}{p} \beta + \frac{1 - t_p}{2p} \]  

defines a tangent to the boundary of the set of achievable errors, for any value of \( p \) between 0 and 1. Any two such tangents will intersect at exactly one point (or will be identical, if the boundary is a straight line). Two straight lines defined by \( y = m_1(2) x + c_1(2) \) intersect at

\[ x = \frac{c_2 - c_1}{m_1 - m_2}, \quad y = m_1 \frac{c_2 - c_1}{m_1 - m_2} + c_1. \]  

Let us choose two values of \( p \): \( p_0 \) and \( p_0 + \delta \). The tangents for these two values of \( p \) will intersect at

\[ \alpha_{\text{intersect}} = \frac{1 - t_{p_0}}{2}, \quad \beta_{\text{intersect}} = \frac{1 - t_{p_0} + \delta}{2}. \]  

By taking the limit as \( \delta \to 0 \), we get equations for \( \alpha^* \) and \( \beta^* \) (Eq. (4) in the main text), the boundary values of the set of achievable errors, in terms of the auxiliary parameter \( p \):

\[ \alpha^* = \frac{1 - t_p}{2} - \frac{1 - p}{2} \frac{dt_p}{dp}, \quad \beta^* = \frac{1 - t_p}{2} + \frac{p}{2} \frac{dt_p}{dp}. \]  

Alternatively, we have integrated the expression for the tangents, with regard to \( p \).

Suppose that, instead of having an expression for \( t_p \), we have an expression that bounds \( t_p \) from either above or below. Swapping a lower bound on \( t_p \) for \( t_p \) in Eq. (A10) gives the tangent to the boundary of a set of pairs of errors that is contained by the set of achievable errors, and similarly swapping an upper bound on \( t_p \) for \( t_p \) gives the tangent to the boundary of a set of pairs of errors that contains the set of achievable errors (since it gives a line that is either a tangent to the set of achievable errors or is strictly below it). For the same reason, if functions \( f_1 \) and \( f_2 \) both bound \( t_p \) from the same side, and \( f_2 \) is never tighter than \( f_1 \), then \( f_1 \) gives a tighter bound on the set of achievable errors than \( f_2 \).

Appendix A: Derivation of bounds on the receiver operating characteristic

We can re-formulate the quantum Neyman-Pearson relation in terms of a parameter \( p \), constrained by \( 0 \leq p \leq 1 \). We write

\[ \mu_p = po + (1-p)\beta \]

\[ = p \text{Tr}[\Pi_2 \rho_1] + (1-p) \text{Tr}[(1-\Pi_2)\rho_2] \]

\[ = \text{Tr}[p\Pi_2 \rho_1 - (1-p)\Pi_2 \rho_2 + (1-p) \text{Tr}[\rho_2]] \]

\[ = 1 - p - \text{Tr}[\Pi_2(1-p)\rho_2 - pp_1)]. \]

\( \mu_p \) can be viewed as the average error probability for a measurement if the source emits state \( \rho_1 \) with probability \( p \) and state \( \rho_2 \) with probability \( 1-p \). Minimising \( \mu_p \) over all operators \( \Pi_2 \leq I \), we find that the optimal value, \( \mu_p^* \), is achieved by the POVMs

\[ \Pi_{i,p}^* = \{(1-p)\rho_2 - pp_1\}_-, \quad \Pi_{i,p}^* = \{(1-p)\rho_2 - pp_1\}_+. \]

\( \Pi_{i,p} \) (assuming \( (1-p)\rho_2 - pp_1 \) is full rank), and is equal to

\[ \mu_p^* = 1 - p - \text{Tr}[(1-p)\rho_2 - pp_1] \].

By definition, \( \text{Tr}[X] = \text{Tr}[(X)_+] - \text{Tr}[(X)_-] \), so

\[ \text{Tr}[(1-p)\rho_2 - pp_1] = \text{Tr}[(1-p)\rho_2 - pp_1]_+] - \text{Tr}[(1-p)\rho_2 - pp_1]_- \]

\[ = 1 - 2p. \]

Similarly, \( \|X\|_1 = \text{Tr}[(X)_+] + \text{Tr}[(X)_-] \), so

\[ t_p = \|\{(1-p)\rho_2 - pp_1\}|1 = \text{Tr}[(1-p)\rho_2 - pp_1]_+] + \text{Tr}[(1-p)\rho_2 - pp_1]_- \].

Combining Eqs. (A5) and (A6), we get

\[ \text{Tr}[(1-p)\rho_2 - pp_1]_+] = \frac{1}{2}(1-2p + t_p). \]
Appendix B: Derivation of bounds based on the fidelity

We can bound $t_p$ from above and below in terms of the fidelity, by proceeding similarly to the derivations for the $p = \frac{1}{2}$ case in Ref. [2].

Let $\rho_1$ and $\rho_2$ be a pair of states with fidelity $F$ and let $|\rho_1'\rangle$ and $|\rho_2'\rangle$ be purifications of $\rho_1$ and $\rho_2$ that have the same fidelity (these are guaranteed to exist by the definition of fidelity). For any pair of positive semidefinite numbers, $p$ and $q$, and any pair of quantum states, $|u\rangle$ and $|v\rangle$, we have the following identity

\[
\|p|u\rangle - q|v\rangle\langle v|\|_1 = \sqrt{(p + q)^2 - 4pq|\langle u|v\rangle|^2}.
\] (B1)

Therefore, we can write

\[
\|(1 - p)|\rho_2'\rangle\langle \rho_2'|-p|\rho_1'\rangle\langle \rho_1'\|_1 = \sqrt{1 - 4p(1 - p)}\|\langle \rho_2'\|\rho_1'\rangle\|_2^2.
\] (B2)

Then, since the trace norm is monotonic under partial tracing, we have the upper bound

\[
t_p \leq \sqrt{1 - 4p(1 - p)}F(\rho_1, \rho_2)^2.
\] (B3)

If $\rho_1$ and $\rho_2$ are pure, this bound becomes an equality.

For any pair of positive semidefinite operators, $X$ and $Y$, we can write

\[
\|X - Y\|_1 \geq \|\sqrt{X} - \sqrt{Y}\|_2^2.
\] (B4)

Consequently,

\[
t_p \geq \left\|\sqrt{1 - p}\sqrt{\rho_2} - \sqrt{p}\sqrt{\rho_1}\right\|_2^2
\geq \text{Tr}\left[(\sqrt{1 - p}\sqrt{\rho_2} - \sqrt{p}\sqrt{\rho_1})^2\right]
\geq (1 - p) + p - 2\sqrt{p(1 - p)}\text{Tr}\sqrt{\rho_1\rho_2}
\geq 1 - 2\sqrt{p(1 - p)}F(\rho_1, \rho_2).
\] (B5)

We define (Eqs. [5] and [6] in the main text)

\[
\mu_{p,FB}(\rho_1, \rho_2) = \sqrt{1 - 4p(1 - p)}F(\rho_1, \rho_2)^2, \quad \mu_{p,FB}(\rho_1, \rho_2) = 1 - 2\sqrt{p(1 - p)}F(\rho_1, \rho_2).
\] (B6)

We can now differentiate both with regard to $p$. We get

\[
\frac{d\mu_{p,FB}(\rho_1, \rho_2)}{dp} = \frac{2(2p - 1)F(\rho_1, \rho_2)^2}{\sqrt{1 - 4p(1 - p)}F(\rho_1, \rho_2)^2},
\] (B8)

\[
\frac{d\mu_{p,FB}(\rho_1, \rho_2)}{dp} = \frac{(2p - 1)F(\rho_1, \rho_2)}{\sqrt{p(1 - p)}}.
\] (B9)


\[
\alpha_{LB,F}(p) = \frac{2(1 - p)F^2 - 1 + \sqrt{1 - 4p(1 - p)}F^2}{2\sqrt{1 - 4p(1 - p)}F^2}, \quad (B10)
\]

\[
\beta_{LB,F}(p) = \frac{2pF^2 - 1 + \sqrt{1 - 4p(1 - p)}F^2}{2\sqrt{1 - 4p(1 - p)}F^2}, \quad (B11)
\]

\[
\alpha_{UB,F}(p) = \frac{F}{2} \sqrt{1 - p}, \quad (B12)
\]

\[
\beta_{UB,F}(p) = \frac{F}{2} \sqrt{\frac{1}{1 - p}}, \quad (B13)
\]

Appendix C: Derivation of bounds based on the Quantum Chernoff Bound

From Ref. [3], we have that, for any pair of positive semidefinite operators, $A$ and $B$, and any $0 \leq s \leq 1$,

\[
\text{Tr}[A^s B^{1-s}] \geq \frac{1}{2} \text{Tr}[A + B - |A - B|]. \quad (C1)
\]

Substituting $(1 - p)\rho_2$ for $A$ and $p\rho_1$ for $B$ and rearranging, we get

\[
p^{1-s}(1 - p)^s \text{Tr}[\rho_2^s \rho_1^{1-s}] + \frac{1}{2}\|p(1 - p)\rho_2 - p\rho_1\|_1 \geq \frac{1}{2}. \quad (C2)
\]

Using the definition of $Q_s$, we can therefore write (Eq. (15) in the main text)

\[
t_p \geq 1 - 2p^{1-s}(1 - p)^s Q_s. \quad (C3)
\]

If we set $s = s_{opt}$, Eq. (15) becomes

\[
t_p \geq 1 - 2p^{1-s}(1 - p)^s Q_{s_{opt}}. \quad (C4)
\]

which we expect to be tighter than the inequality in Eq. (B5) for some values of $p$ (in particular, close to $\frac{1}{2}$). Note that this is not the tightest lower bound on $t_p$, since $s_{opt}$ minimises $Q_s$ rather than $p^{1-s}(1 - p)^s Q_s$. The optimal value of $s$ (achieving the tightest bound) is therefore not a constant, but is rather a function of $p$. We call this value $s_{opt}$, and define

\[
Q_{opt} = Q_{s_{opt}}, \quad s_{opt} = \arg \min_{0 \leq s \leq 1} p^{1-s}(1 - p)^s Q_s. \quad (C5)
\]

By differentiation, $s_{opt}$ satisfies

\[
\ln \left[\frac{1 - p}{p}\right] Q_{opt} + \frac{dQ_s}{ds}_{s=s_{opt}} = 0. \quad (C6)
\]

If we have an analytical expression for $Q_s$ in terms of $s$, we can analytically calculate $s_{opt}(p)$ (although we will later show that finding $s_{opt}(p)$ is not necessary).

Defining the family of lower bounds on $t_p$ as

\[
t_p^{LB,s}(p) = 1 - 2p^{1-s}(1 - p)^s Q_s. \quad (C7)
\]
and treating $s$ as a function of $p$, we differentiate to get

$$\frac{dp^{(LB,s)}}{dp} = \frac{\partial p^{(LB,s)}}{\partial p} + \frac{\partial p^{(LB,s)}}{\partial s} \frac{ds}{dp}$$

$$= -2(1-p)^{s-1} \left( (1-p-s)Q_s + p(1-p) \frac{ds}{dp} \ln \left[ \frac{1-p}{p} \right] Q_s + \frac{dQ_s}{ds} \right),$$

(C8)

where $s'$ stands in for either $s_0$ or $s_{\text{opt}}$.

Substituting Eqs. (C4) and (C8) into Eq. (4), we get

$$\alpha^{(UB,s)} = \left( \frac{1-p}{p} \right)^s \left( 1-s \right) Q_s + p(1-p) \frac{ds}{dp} \ln \left[ \frac{1-p}{p} \right] Q_s + \frac{dQ_s}{ds},$$

(C10)

$$\beta^{(UB,s)} = \left( \frac{p}{1-p} \right)^{1-s} sQ_s + p(1-p) \frac{ds}{dp} \ln \left[ \frac{1-p}{p} \right] Q_s - \frac{dQ_s}{ds},$$

(C11)

If we again set $s = s_0$ or $s = s_{\text{opt}}$, we get

$$\alpha^{(UB,s')} = \left( \frac{1-p}{p} \right)^{s'} (1-s')Q_s',$n

(C12)

$$\beta^{(UB,s')} = \left( \frac{p}{1-p} \right)^{1-s'} s'Q_s',$$

(C13)

where $s'$ stands in for either $s_0$ or $s_{\text{opt}}$. The $s = s_0$ case gives Eqs. (16) and (17) from the main text.

For any value of $s$, there exists some value of $p$ for which $s_{\text{opt}}$ is given by that $s$ value. In other words, we can validly write $p(s_{\text{opt}})$ instead of $s_{\text{opt}}(p)$. This follows from the fact that $\frac{p}{1-p}$ can take any positive value, so we can always choose $p$ such that Eq. (C6) is satisfied, and the convexity of $p^{1-s}(1-p)^sQ_s$ (this can be seen from the decompositions in Eqs. (D4) and (D5)), which means that the point at which Eq. (C6) is satisfied is a minimum.

Using Eq. (C6), we can write

$$\frac{p}{1-p} = \exp \left[ Q^{-1}_{\text{opt}} \frac{dQ_s}{ds} \bigg|_{s=s_{\text{opt}}} \right],$$

(C14)

and thus can rewrite Eqs. (C12) and (C13), replacing $p$ as our auxiliary parameter with $s_{\text{opt}}$.

$$\alpha^{(UB,QCB)} = \left( \exp \left[ -sQ_s^{-1} \frac{dQ_s}{ds} \right] (1-s)Q_s \right) \bigg|_{s=s_{\text{opt}}} ,$$

(C15)

$$\beta^{(UB,QCB)} = \left( \exp \left[ (1-s)Q_s^{-1} \frac{dQ_s}{ds} \right] sQ_s \right) \bigg|_{s=s_{\text{opt}}},$$

(C16)

For consistency with the other equations, we redefine $p$ as $s_{\text{opt}}$ and write (Eqs. (20) and (21) in the main text)

$$\alpha^{(UB,QCB)} = \left( \exp \left[ -pQ_p^{-1} \frac{dQ_p}{dp} \right] (1-p)Q_p \right),$$

(C17)

$$\beta^{(UB,QCB)} = \exp \left[ (1-p)Q_p^{-1} \frac{dQ_p}{dp} \right] pQ_p.$$

(C18)

**Appendix D: Connection between the OAQCB and quantum relative entropy**

Ref. [3] points out a connection between the QCB and the quantum relative entropy, namely that for $s_*(\text{the value that minimises } Q_s(\rho_1, \rho_2))$, the following holds:

$$S(\tau_s || \rho_1) = S(\tau_s || \rho_2),$$

(D1)

$$\tau_s = \frac{\rho_2^* \rho_1^{1-s}}{\text{Tr}[\rho_2^* \rho_1^{1-s}]} = \frac{\rho_2^{1-s}}{Q_s},$$

(D2)

where $S(A || B)$, the relative entropy between $A$ and $B$, is defined by

$$S(A || B) = \text{Tr}[A \ln A - A \ln B].$$

(D3)

Note that $\tau_s$ is not, in general, a valid quantum state.

In the discrete variable case, we can decompose $Q_s$ as

$$Q_s = \sum_i c_i \lambda_i^s \mu_i^{1-s},$$

(D4)

where $c_i$, $\lambda_i$, and $\mu_i$ are all positive semidefinite numbers [3]. Note that we could have written this expression with two separate indices for the $\lambda$ values and the $\mu$ values (and a nested sum over both), but we have chosen to combine them into the single index $i$. Similarly, in the continuous variable case, we can decompose $Q_s$ as

$$Q_s = \int c_x \lambda_x^s \mu_x^{1-s} dx,$$

(D5)

where $c_x$, $\lambda_x$, and $\mu_x$ are all positive semidefinite functions of $x$, and where the bounds of the integral may be finite or may be infinite.

By differentiating Eq. (D4) (Eq. (D5) in the continuous variable case) with regard to $s$, we get

$$\frac{dQ_s}{ds} = \sum_i c_i \lambda_i^s \mu_i^{1-s}(\ln[\lambda_i] - \ln[\mu_i])$$

(D6)
(with a similar result in the continuous variable case). We can therefore write
\[ S(\tau_p\|\rho_1) - S(\tau_p\|\rho_2) = Q_p^{-1} \frac{dQ_p}{dp}. \] \hfill (D7)

For instance, if we want the ratio between \( Q_{\text{UB, QCB}} \) and \( Q_{\text{UB, QCB}} \), for some parameter value \( p \), we can express it in terms of the quantum relative entropy as
\[ \frac{\alpha(\text{UB, QCB})}{\beta(\text{UB, QCB})} = \exp \left[ S(\tau_p\|\rho_1) - S(\tau_p\|\rho_2) \right] \frac{1 - p}{p}. \] \hfill (D8)

Taking the limit of Eq. (D6) as \( s \to 0 \), we get
\[ \frac{dQ_s}{ds} \bigg|_{s=0} = \sum_i c_i \mu_i (\ln[\lambda_i] - \ln[\mu_i]) = -S(\rho_1\|\rho_2), \] \hfill (D9)
and taking the limit as \( s \to 1 \), we get
\[ \frac{dQ_s}{ds} \bigg|_{s=1} = \sum_i c_i \lambda_i (\ln[\lambda_i] - \ln[\mu_i]) = S(\rho_2\|\rho_1). \] \hfill (D10)

For some states, the relative entropy \( S(\rho_1\|\rho_2) (S(\rho_2\|\rho_1)) \) can diverge. This corresponds to some of the \( \lambda_i \) (\( \mu_i \)) equalling 0. Note that this only occurs for extremal values of \( s \), since we set \( 0 \ln[0] = 0 \). These are also the states for which \( Q_0, Q_1 \), or both are not equal to 1.

**Appendix E: Multicopy scaling of the OAQCB**

Since
\[ \frac{dQ_N^{(1)}}{dp} = N Q_{p,(1)}^{-1} \frac{dQ_p^{(1)}}{dp}, \] \hfill (E1)
we can write (Eqs. (23) and (24) in the main text)
\[ \alpha_{(N)}^{(\text{UB, QCB})} = \exp \left[ -Np Q_{p,(1)}^{-1} \frac{dQ_p^{(1)}}{dp} \right] (1 - p) Q_p^{N(1)} = \left( \frac{\alpha_{(1)}^{(\text{UB, QCB})}}{1 - p} \right)^N, \] \hfill (E2)
\[ \beta_{(N)}^{(\text{UB, QCB})} = \exp \left[ N (1 - p) Q_{p,(1)}^{-1} \frac{dQ_p^{(1)}}{dp} \right] p Q_p^{N(1)} = \left( \frac{\beta_{(1)}^{(\text{UB, QCB})}}{p} \right)^N. \] \hfill (E3)

We can then use Eqs. (23) and (24) to recover Eqs. (28) and (29) from the main text:
\[ \gamma_{\alpha}^{(\text{UB, QCB})} = p Q_{p,(1)}^{-1} \frac{dQ_p^{(1)}}{dp} - \ln \left[ Q_p^{(1)} \right], \] \hfill (E4)
\[ \gamma_{\beta}^{(\text{UB, QCB})} = -(1 - p) Q_{p,(1)}^{-1} \frac{dQ_p^{(1)}}{dp} - \ln \left[ Q_p^{(1)} \right]. \] \hfill (E5)

**Appendix F: Proof that the OAQCB saturates the quantum Hoeffding bound**

Substituting our expression for \( \gamma_{\beta}^{(\text{UB, QCB})} \) into the expression for \( b(r, s) \), we get
\[ b \left( \gamma_{\beta}^{(\text{UB, QCB})}, s \right) = (1 - s)^{-1} \left( s (1 - p) Q_{p,(1)}^{-1} \frac{dQ_p^{(1)}}{dp} + \right. \] 
\[ \left. s \ln[Q_p^{(1)}] - \ln[Q_s^{(1)}] \right). \] \hfill (F1)

To find the maximum achievable decay rate for \( \alpha \), subject to the constraint that \( \gamma_{\beta}^{(\text{UB, QCB})} \geq r \), we must maximise Eq. (F1) over \( s \) (in the range \( 0 \leq s < 1 \)). Differentiating with regard to \( s \), and noting that \( Q_{p,(1)}^{-1} \frac{dQ_p^{(1)}}{dp} = \frac{d}{dp} (\ln[Q_p^{(1)}]) \), we get
\[ \frac{db \left( \gamma_{\beta}^{(\text{UB, QCB})}, s \right)}{ds} = (1 - s)^{-2} \left( (1 - p) \frac{d}{dp} (\ln[Q_p^{(1)}]) \right) \] 
\[ = (1 - s)^{-2} \left( (1 - p) \frac{d}{dp} (\ln[Q_p^{(1)}]) \right) - \] 
\[ (1 - s) \frac{d}{ds} (\ln[Q_s^{(1)}]) + \ln[Q_p^{(1)}] - \ln[Q_s^{(1)}]). \] \hfill (F2)

Note that the terms in the numerator are either functions only of \( s \) or functions only of \( p \). Defining
\[ a_x = (1 - x) \frac{d}{dx} (\ln[Q_x^{(1)}]) + \ln[Q_x^{(1)}], \] \hfill (F3)
we can write
\[ \frac{db \left( \gamma_{\beta}^{(\text{UB, QCB})}, s \right)}{ds} = \frac{a_p - a_s}{(1 - s)^2}. \] \hfill (F4)

We have a turning point in \( b(\gamma_{\beta}^{(\text{UB, QCB})}, s) \) iff \( a_s = a_p \) (since the denominator is always positive in the range). \( s = p \) is therefore a turning point. To determine whether this turning point is a global maximum, we differentiate \( a_s \) with regard to \( s \). If \( \frac{da_s}{ds} > 0 \) for \( 0 \leq s < 1 \), then \( s = p \) is a global maximum. If \( \frac{da_s}{ds} \geq 0 \) for \( 0 \leq s < 1 \) (a slightly weaker condition), then the value of \( b \) obtained by setting \( s = p \) is still \( b_{\text{max}} \), even if there is an interval of \( s \)-values in the neighbourhood of \( s = p \) that also maximise \( b \).
\[ \frac{da_s}{ds} = (1 - s) \frac{d^2}{ds^2} (\ln[Q_s^{(1)}]). \] \hfill (F5)

Since \( (1 - s) > 0 \) in our range, the condition for \( s = p \) to maximise \( b \) reduces to the requirement that the second differential of \( \ln[Q_s^{(1)}] \) is positive semidefinite. We therefore need to show that the function \( Q_s \) is logarithmically convex (log-convex) in \( s \) [13]. This is a stricter condition than convexity, and means that \( \ln[Q_s] \) is also convex (as well as \( Q_s \)). The second derivative of any convex
function is non-negative, so it suffices to show that $Q_s$ is log-convex.

The condition for a function, $f$, to be log-convex is

$$ f(tx_1 + (1-t)x_2) \leq f(x_1)^t f(x_2)^{1-t}, \quad (F6) $$

for $0 \leq t \leq 1$. From Ref. [14], we have that the set of log-convex functions (referred to in Ref. [14] as super-convex functions) is closed under addition. This means that a linear combination of log-convex functions is also log-convex. Ref. [14] also shows that if every member of a sequence of functions is log-convex, the limit of the supremum of the sequence (limsup) is also log-convex.

First, let us consider the discrete variable case. Recall Eq. (D4) (repeated here for convenience), which tells us that for discrete variables, we can decompose $Q_s$ as

$$ Q_s = \sum_i c_i \lambda_i^s \mu_i^{1-s}. \quad (F2) $$

Let $f(s)$ be the function $s \mapsto c \lambda^s \mu^{1-s}$, for some positive numbers $\lambda$ and $\mu$. $f(s)$ is log-convex:

$$ f(tx_1 + (1-t)x_2) = c \lambda^{tx_1 + (1-t)x_2} \mu^{1-(tx_1 + (1-t)x_2)} = \left( c \lambda^{t x_1} \mu^{t(1-x_1)} \right) \times \left( c \lambda^{1-t x_1} \mu^{(1-t)(1-x_1)} \right) = f(x_1)^t f(x_2)^{1-t}. \quad (F7) $$

Since $Q_s$ is a sum of such functions, it is also log-convex. This is true even if the sum is unbounded and $i$ takes values up to $\infty$.

Let us extend this result to continuous variable states. We can use the fact that the set of log-convex functions is closed under limsup. Suppose that, for any pair of continuous variable states, we can define a sequence of log-convex approximations to $Q_s$, $Q_s^{(i)}$, so that the supremum of the bounds tends to $Q_s$ in the limit of $i \to \infty$. Then, $Q_s$ must also be log-convex. One subtlety is that the $Q_s^{(i)}$ must all be lower bounds, so that $Q_s$ is the limsup, rather than just the limit.

Recall Eq. (D5) (repeated here for convenience), which decomposes $Q_s$ as

$$ Q_s = \int c_x \lambda_x^s \mu_x^{1-s} dx. \quad (F8) $$

Let us initially assume that $0 \leq x < R$, for finite $R$ (i.e. the integral has finite bounds). We can then define our approximations, $Q_s^{(i)}$, as

$$ Q_s^{(i)} = \Delta_i \sum_{j=1}^i \left( \inf_{(j-1)\Delta_i \leq x < j \Delta_i} c_x \right) \left( \inf_{(j-1)\Delta_i \leq x < j \Delta_i} \rho_x \right)^s \times \left( \inf_{(j-1)\Delta_i \leq x < j \Delta_i} \sigma_x \right)^{1-s}, \quad (F8) $$

where $\Delta_i = \frac{R}{i}$. This is a kind of lower Riemann sum, and it is clear that, for any finite number of samples, $i$, $Q_s^{(i)}$ both lower bounds $Q_s$ and is log-convex. Taking the limit as $i \to \infty$, and therefore as $\Delta_i \to 0$, we get $Q_s$. To extend to an infinite domain for $x$, we truncate the function outside the finite domain $0 \leq x < R$, take the limit as $i \to \infty$ and then take the limit again as $R \to \infty$.

We can therefore write

$$ b_{\text{max}}(\gamma^{(UB,\text{QCB})}_\beta, p) = b(\gamma^{(UB,\text{QCB})}_\alpha, p) = \gamma^{(UB,\text{QCB})}_\alpha, \quad (F9) $$

showing that the OAQCB achieves the best possible scaling, according to the quantum Hoeffding bound.

Note that we have assumed that $\gamma^{(UB,\text{QCB})}_\beta$ lies in the range $0 < \gamma^{(UB,\text{QCB})}_\beta < S(p_1 \| p_2)$. We will now show that this always holds, except at the extremal points ($p = 0$ and $p = 1$), at which the quantum Stein’s lemma holds.

**Appendix G: Derivation of results showing the OAQCB saturates the quantum Stein’s lemma**

Eqs. (33) and (34) in the main text come from applying Eqs. (D9) and (D10) when taking the limits.

We show that $\gamma^{(UB,\text{QCB})}_\beta$ is a non-increasing function of $p$ by rewriting Eq. (29) as

$$ \gamma^{(UB,\text{QCB})}_\beta = -(1-p) \frac{d}{dp} \ln [Q_p(1)] - \ln [Q_p(1)]. \quad (G1) $$

and differentiating it, to get

$$ \frac{d\gamma^{(UB,\text{QCB})}_\beta}{dp} = -(1-p) \frac{d^2}{dp^2} \ln [Q_p(1)]. \quad (G2) $$

Since $Q_s$ is log-convex, the right-hand side of Eq. (G2) is negative semi-definite, and so $\gamma^{(UB,\text{QCB})}_\beta$ is a non-increasing function of $p$.

**Appendix H: Error rates for non-adaptive measurement sequences**

Consider the measurement sequences described in Section VTA of the main text. The errors for each case can be calculated using Eqs. (7) and (8), and are given by

$$ \alpha^{(a)} = 1 - \left( 1 - \alpha^{(LB, F(1))} \right)^3, \quad (H1) $$

$$ \beta^{(a)} = \left( \beta^{(LB, F(1))} \right)^3, \quad (H2) $$

for case a,

$$ \alpha^{(b)} = 3 \left( \alpha^{(LB, F(1))} \right)^2 - 2 \left( \alpha^{(LB, F(1))} \right)^3, \quad (H3) $$

$$ \beta^{(b)} = 3 \left( \beta^{(LB, F(1))} \right)^2 - 2 \left( \beta^{(LB, F(1))} \right)^3, \quad (H4) $$
exception at the points given by parameter values $m_{\text{um}}$, given by for case c.

The measurement sequence described in Section VI B of the main text (for states with two subsystems).

Recall that we carry out an optimal measurement, with parameter value $p_0$, on the first subsystem. If this measurement tells us that the state is $p_{1,1}$, we carry out another optimal measurement with parameter value $p_1$, otherwise we carry out a measurement on the second subsystem with parameter value $p_2$. We use only the result of the second measurement to decide which state we have.

The type 1 error for the sequence, $\alpha_{\text{seq}}$, is given by

\begin{equation}
\alpha_{\text{seq}} = (1 - \alpha^{(\text{LB},F_1)}[p_0])\alpha^{(\text{LB},F_2)}[p_1]
\end{equation}

and the type 2 error, $\beta_{\text{seq}}$, is given by

\begin{equation}
\beta_{\text{seq}} = \beta^{(\text{LB},F_1)}[p_0]\beta^{(\text{LB},F_2)}[p_1]
\end{equation}

We set (Eqs. (37) and (38) in the main text)

\begin{align}
p_1 &= \frac{1}{2} \left( 1 - \sqrt{1 - 4p_0(1 - p_0)F_1^2} \right), \\
p_2 &= \frac{1}{2} \left( 1 + \sqrt{1 - 4p_0(1 - p_0)F_1^2} \right).
\end{align}

Substituting these values into Eqs. (11) and (12) (and using Eqs. (7) and (8)), we get

\begin{align}
\alpha_{\text{seq}} &= \frac{2(1 - p_0)F_2^2F_2^2 - 1 + \sqrt{1 - 4p_0(1 - p_0)F_1^2F_2^2}}{2 \sqrt{1 - 4p_0(1 - p_0)F_1^2F_2^2}}, \\
\beta_{\text{seq}} &= \frac{2p_0F_1^2F_2^2 - 1 + \sqrt{1 - 4p_0(1 - p_0)F_1^2F_2^2}}{2 \sqrt{1 - 4p_0(1 - p_0)F_1^2F_2^2}}.
\end{align}

Now note that

\begin{align}
\alpha_{\text{seq}} &= \alpha^{(\text{LB},F_1,F_2)}[p_0], \\
\beta_{\text{seq}} &= \beta^{(\text{LB},F_1,F_2)}[p_0],
\end{align}

so this measurement sequence achieves the optimal errors for discriminating between states with a fidelity of $F_1 F_2$.

---

**Appendix I: Error rates for adaptive measurement sequences**

Let us consider the error rates for the adaptive measurement sequence described in Section VII B of the main text (for states with two subsystems).

FIG. 2. Type 1 and 2 errors for discriminating between a pair of pure, three-copy states, for which the single-copy fidelity is 0.9. In cases a, b and c, the same (optimal) single-copy measurement is carried out on each subsystem of the state. The cases differ in how we determine the identity of the state from the measurement results. All three methods are worse than the optimal joint measurement, denoted “optimum” (except at the two points where the optimal curve meets the axes). Case b - where the state is determined using the majority vote - is never better than both cases a and c.

for case b, and

\begin{align}
\alpha^{(c)} &= \left( \alpha^{(\text{LB},F_{(1)})} \right)^3, \\
\beta^{(c)} &= 1 - \left( 1 - \beta^{(\text{LB},F_{(1)})} \right)^3.
\end{align}

for case c.

All three sets of equations are different from the optimum, given by

\begin{align}
\alpha^{(\text{opt})} &= \alpha^{(\text{LB},F_{(3)}=F^2_{(1)})}, \\
\beta^{(\text{opt})} &= \beta^{(\text{LB},F_{(3)}=F^2_{(1)})},
\end{align}

except at the points given by parameter values $p = 0$ and $p = 1$. This is illustrated in Fig. 2.