No-Signalling Bound on Quantum State Discrimination

Sarah Croke,1,2 Erika Andersson,1 and Stephen M. Barnett1

1Department of Physics, SUPA, University of Strathclyde, Glasgow G4 0NG, UK
2Department of Mathematics, University of Glasgow, Glasgow G12 8QW, UK

(Dated: August 29, 2007)

Quantum correlations do not allow signalling, and any operation which may be performed on one system of an entangled pair cannot be detected by measurement of the other system alone. This no-signalling condition limits allowed operations and, in the context of quantum communication, may be used to put bounds on quantum state discrimination. We find that the natural figure of merit to consider is the confidence in identifying a state, which is optimised by the maximum confidence strategy. We show that this strategy may be derived from the no-signalling condition, and demonstrate the relationship between maximum confidence measurements and entanglement concentration.

PACS numbers: 03.65.Ud, 03.67.Hk, 03.65.Ta

Although entanglement appears to allow particles which are separated in space to influence one another instantaneously 1, it has been shown that this cannot be used to transmit information superluminally 2, thus reconciling quantum mechanics and special relativity. Any operation which can be performed on a quantum system must therefore be compatible with no-signalling, and imposing this condition allows us to put limits on certain tasks, for example those obtained on the fidelity of quantum cloning machines 3, and on error-free discrimination between non-orthogonal quantum states 4. As a consequence, it has been suggested that no-signalling should be given the status of a physical principle, used to restrict quantum mechanics and possible extensions of it 4. However, and interestingly, a quantum key distribution protocol has been devised which is provably secure against attacks from an eavesdropper limited only by no-signalling 5.

In state discrimination, in addition to the limits derived on error-free discrimination 4, the no-signalling condition has been used to bound the minimum probability of error in discriminating between two non-orthogonal states 6. In this paper we show that, in the problem of discriminating between a set of non-orthogonal states \{\psi_i\}, the no-signalling condition leads us to consider the conditional probability \(P(\psi_j | \omega_j)\), where \(\omega_j\) denotes the measurement outcome which leads us to choose state \(\psi_j\). This is the figure of merit optimised by the recently introduced maximum confidence strategy 6. We will show that no-signalling gives a direct way to obtain a tight bound on this figure of merit, without reference to Probability Operator Measures (POMs) 10. Further, by considering when the bound is reached, we will show that it is then possible to derive the POM describing the optimal measurement using only no-signalling. We illustrate this by means of an example, and discuss the relationship to entanglement concentration.

Suppose that two systems, referred to as left and right, are entangled in the state

\[ |\Psi\rangle = \sum_{i=0}^{N-1} p_i^{1/2} |\psi_i\rangle_L |i\rangle_R \]

where the states \{\psi_i\}_L\) of the left system lie in a \(D \leq N\) dimensional space, and the set \{\(i\)_R\} forms an orthonormal basis for the right system. In a quantum communication protocol, the states \{\psi_i\}_L\) may be prepared with a priori probabilities \(\{p_i\}\) by performing a projective measurement onto the orthogonal states \{|i\>_R\} of the right system. Further, suppose that a measurement is subsequently performed on the left system to discriminate between these states. After measurement, the probability that the initial state was \(\psi_j\)_L may be interpreted as the probability that the measurement on the right system gave the outcome corresponding to state \(|j\>_R\). As operations on different systems commute, this interpretation is valid regardless of the order in which the measurements are performed. Thus, if a measurement performed on the left system of the entangled state \(|\Psi\rangle\) yields outcome \(\omega_j\), the reduced density operator of the right system is transformed to \(\hat{\rho}_{R|i\rangle}\) and the probability \(P(\psi_j | \omega_j)\), the confidence in identifying state \(|\psi_j\>_L\), may be expressed:

\[ P(\psi_j | \omega_j) = ||\langle j | \hat{\rho}_{R|i\rangle} | j \rangle || R. \]

It is therefore natural to consider conditional probabilities of this form. The no-signalling condition restricts \(\hat{\rho}_{R|i\rangle}\), and therefore may be used to put a bound on the above probability. The Schmidt decomposition 11 of the entangled state \(|\Psi\rangle\) may be written

\[ |\Psi\rangle = \sum_{i=0}^{D-1} \lambda_i^{1/2} |\lambda_i\>_L |\lambda_i\>_R \]

where \(\sum_i \lambda_i = 1\) and \(L\langle \lambda_i | \lambda_j\>_L = R (\lambda_i | \lambda_j\>_R = \delta_{ij}\). Thus the set \{\(|\lambda_i\>_L\)\} is an orthonormal basis of the left system, and we can construct \(N - D\) states \(|\Psi^+_i\>_R\) of the right system alone, such that \{\(|\lambda_i\>_R; i = 0, ..., D-1\), \(|\Psi^+_i\>_R; i =
0\ldots N - D - 1 \} forms an orthonormal basis of the right system, and \( R(\Psi_j^+ | \Psi) = 0 \). The no signalling condition implies that no operation performed on the left system may be detected by observation of the right system alone. In particular, after the measurement described above is made on the left system, the state of the right system is described by the density operator \( \hat{\rho}_{R|i} \). Clearly if \( R(\Psi_j^+ | \hat{\rho}_{R|i} | \Psi)^+_{|R} \neq 0 \) for any \( |\Psi_j^+\rangle_{R} \), there is a finite probability that the operation could be detected by a measurement on the right system alone. Such a transformation would allow the possibility of superluminal communication, and is therefore forbidden.

The N-dimensional right system is thus confined to a \( D \)-dimensional subspace, \( \mathcal{H}_{RD} \), due to its entanglement with the left system. The projector onto this subspace is

\[
\hat{P}_D = \hat{I}_R - \sum_{i=0}^{N - D - 1} |\Psi_i^+\rangle_{RR} \langle \Psi_i^+ | = \sum_{i=0}^{D - 1} |\lambda_i\rangle_{RR} \langle \lambda_i |.
\]

It is useful to write this in the form

\[
\hat{P}_D = \text{Tr}_L(\hat{\rho}_L^{-1/2} |\Psi\rangle \langle \Psi | \hat{\rho}_L^{-1/2}),
\]

where \( \hat{\rho}_L \) is the reduced density operator of the left system,

\[
\hat{\rho}_L = \text{Tr}_R(|\Psi\rangle \langle \Psi |) = \sum_{i=0}^{N - D - 1} \lambda_i |\lambda_i\rangle_{LL} \langle \lambda_i |,
\]

\[
= \sum_{i=0}^{D - 1} \lambda_i |\lambda_i\rangle_{LL} \langle \lambda_i |.
\]

We wish to maximise \( R(|j\rangle |\hat{\rho}_{R|i} |j\rangle_R \) subject to the constraint that \( \hat{\rho}_{R|i} \) lies in the subspace \( \mathcal{H}_{RD} \). Clearly then \( \hat{\rho}_{R|i} \) is simply the projection of \(|j\rangle_R \) onto this subspace

\[
\hat{\rho}_{R|i} = \frac{\hat{P}_D |j\rangle \langle j|R}{\text{Tr}_R(\hat{P}_D |j\rangle \langle j|R)},
\]

giving

\[
[P(|\psi_j\rangle |\omega_j)]_{max} = R(|j\rangle |\hat{P}_D |j\rangle_R).
\]

Thus an upper limit on the confidence with which it is possible to identify state \(|\psi_j\rangle_L \) is given by the overlap of the corresponding state \(|j\rangle_R \) of the right system with \( \mathcal{H}_{RD} \). Using Eq. [5] we now obtain

\[
[P(|\psi_j\rangle |\omega_j)]_{max} = R(|j\rangle |\text{Tr}_L(\hat{\rho}_L^{-1/2} |\Psi\rangle \langle \Psi | \hat{\rho}_L^{-1/2} |j\rangle_R) = 
\text{Tr}_L(\hat{\rho}_L^{-1/2} |\Psi\rangle \langle \Psi | \hat{\rho}_L^{-1/2} |j\rangle_R) = 
p_j \text{Tr}_L(\hat{\rho}_L |j\rangle \langle j|R \hat{\rho}_L^{-1/2}) \]
\]

where \( \hat{\rho}_{L|i} = |\psi_j\rangle_{LL} \langle \psi_j |. \) This bound agrees with that given in [9], and has been reached experimentally for a set of three elliptical polarisation states [12].

To derive the optimal POM we note from Eq. [7] that the limit is achieved if \( \hat{\rho}_{R|i} \propto \hat{P}_D |j\rangle_R |j\rangle_R |\hat{P}_D \). Using Eq. [5] we see that

\[
P_D |j\rangle_R = \text{Tr}_L \left( \hat{\rho}_L^{-1/2} |\Psi\rangle \langle \Psi | \hat{\rho}_L^{-1/2} |j\rangle_R \right) = \text{Tr}_L \left( \hat{\rho}_L^{-1/2} |\Psi\rangle \langle \psi_j | \hat{\rho}_L^{-1/2} \right) = p_j^{1/2} \langle \psi_j | \hat{\rho}_L^{-1/2} |\Psi\rangle
\]

and thus

\[
\hat{\rho}_{R|i} \propto p_j |\psi_j\rangle \langle \psi_j | \hat{\rho}_L^{-1/2} |\Psi\rangle \langle \psi_j | \hat{\rho}_L^{-1/2} |\psi_j\rangle_L = \text{Tr}_L \left( |\Psi\rangle \langle \Psi | \hat{\rho}_L^{-1/2} p_j \hat{\rho}_L \hat{\rho}_L^{-1} \right).
\]

Suppose now that the measurement outcome \( \omega_j \) is associated with the POM element \( \hat{\Pi}_j \) acting on the left system.

\[
\hat{\rho}_{R|i} \propto \text{Tr}_L(|\Psi\rangle \langle \Psi | \hat{\Pi}_j),
\]

and thus

\[
\hat{\Pi}_j \propto \hat{\rho}_L^{-1} p_j \hat{\rho}_L \hat{\rho}_L^{-1}.
\]

This reproduces the result in [9], but has arisen here as a direct consequence of the no-signalling condition. It is a feature of the maximum confidence strategy that the optimal POM elements are only defined up to an arbitrary constant, as may be seen from Eq. [13]. Note that these POM elements may not form a complete measurement, and in general an inconclusive result is also needed [9].

For mixed states \{\hat{\rho}_{L|i}\} similar results can be obtained. In this case we can consider the entangled state

\[
|\Psi\rangle = \sum_{i\in\{\beta\}} \beta_i^{1/2} |\beta_i\rangle_L |i\rangle_R,
\]

where \( \sigma(j) \) is an index set associated with \( \hat{\rho}_{L|i} \), \( |\beta_i\rangle_L = 1 \), and \( \sum_{i\in\{\beta\}} \beta_i = p_j \), such that \( p_j \hat{\rho}_L = \sum_{i\in\{\beta\}} \beta_i |\beta_i\rangle_L \langle \beta_i | \). The maximum confidence and optimal POM element may be derived using any valid decomposition of \( p_j \hat{\rho}_L \), and \{\{\beta_i\}_L\} need not be the eigenkets of \( \hat{\rho}_L \). We will not discuss the full derivation for the general case, as it follows the same arguments outlined above, but proceed instead to illustrate both the pure state case, and the extension of the arguments to include mixed states, by means of an example.

Consider therefore the example of one mixed state and one pure state in a two-dimensional space, given by:

\[
\hat{\rho}_0 = q |0\rangle \langle 0| + (1 - q) |1\rangle \langle 1|,
\]

\[
\hat{\rho}_1 = |\psi\rangle \langle \psi| = \frac{1}{2} (|0\rangle \langle 0| + |1\rangle \langle 1|),
\]

with a priori probabilities \( p \) and \( 1 - p \) respectively. Following Eq. [13] we construct the entangled state:

\[
|\Psi\rangle = (pq)^{1/2} |0\rangle_L |0\rangle_R + (p(1 - q))^{1/2} |1\rangle_L |1\rangle_R + (1 - p)^{1/2} |\psi\rangle_L |2\rangle_R,
\]

We first consider the projector \( \hat{P}_D \). It is clear that \( \langle \Psi | \Psi^+ \rangle = 0 \) where

\[
|\Psi^+ \rangle = k((1 - p)^{1/2} (1 - q)^{1/2} |0\rangle_R + q^{1/2} |1\rangle_R - (2pq(1 - q))^{1/2} |2\rangle_R),
\]

and \( k = (1 - p + 2pq(1 - q))^{-1/2} \) is a normalisation factor chosen to ensure \( \langle \Psi^+ | \Psi^+ \rangle = 1 \). Thus

\[
\hat{P}_D = \hat{I}_R - |\Psi^+ \rangle \langle \Psi^+ |.
\]
The probability that the state of the left system was \( \hat{\rho}_0 \) is equivalent to the probability that the right system lies in the subspace with the projector \( |0\rangle_R R |0\rangle + |1\rangle_R R |1\rangle \) after measurement. Thus for state \( \hat{\rho}_0 \), we obtain

\[
P(\hat{\rho}_0|\omega_0) = \text{Tr}_L \left( \hat{P}_D \hat{\rho}_0 \hat{P}_D \right) = \text{Tr}_L \left( \hat{P}_D \hat{\rho}_0 \hat{P}_D \right),
\]

where we have used \( \hat{\rho}_{R0} = \hat{P}_D \hat{\rho}_{R0} \hat{P}_D \), as \( \hat{\rho}_{R0} \) lies in the subspace with the projector \( \hat{P}_D \), and \( \gamma_{\max} (X) \) denotes the largest eigenvalue of \( X \). Note that \( |\phi_0\rangle = q^{1/2} |0\rangle_R - (1 - q)^{1/2} |1\rangle_R \) is an eigenvector with eigenvalue 1 of both \( \hat{P}_D \) and \( |0\rangle_R R |0\rangle + |1\rangle_R R |1\rangle \). Thus this limit is 1, corresponding to unambiguous discrimination, as expected, and the limit is reached if \( \hat{\rho}_{R0} = |\phi_0\rangle \langle \phi_0| \).

We can readily deduce the optimal POM element \( \hat{\Pi}_0 \) by noting that \( R \langle 2 | \hat{\rho}_{R0} | 2 \rangle_R = 0 \), and therefore, according to Eq. (12) we require

\[
R \langle 2 | \text{Tr}_L (\hat{\rho} | \hat{\Pi}_0 \rangle | 2 \rangle_R = (1 - p)_L \langle \psi | \hat{\Pi}_0 | \psi \rangle_L = 0.
\]

Thus \( \hat{\Pi}_0 \) is a projector onto the state orthogonal to \( |\psi\rangle \), also as expected.

For result \( \omega_1 \), using Eq. (8) we obtain

\[
P(\hat{\rho}_1 | \omega_1) \leq 1 - |\langle \Psi^- | R | 2 \rangle_R|^2 = \frac{1 - p}{1 - p + 2pq(1 - q)}
\]

This limit is achieved if \( \hat{\rho}_{R1} \propto \hat{P}_D | 2 \rangle_R R | 2 \rangle_R \hat{P}_D \). Thus, from Eq. (12) we require

\[
\text{Tr}_L (\hat{\rho} | \hat{\Pi}_1 \rangle | 0 \rangle_L = c_1 R \langle 0 | \hat{P}_D | 2 \rangle_R R | 2 \rangle_R \hat{P}_D
\]

where we have introduced the constant of proportionality \( c_1 \). We now note that we can easily write down the matrix elements of \( \hat{\Pi}_1 \) in the basis \( \{ |0\rangle_L, |1\rangle_L \} \) as follows. Clearly

\[
L \langle 0 | \hat{\Pi}_1 | 0 \rangle_L = \frac{R \langle 0 | \text{Tr}_L (\hat{\rho} | \hat{\Pi}_1 \rangle | 0 \rangle_R}{pq} = c_1 R \langle 0 | \hat{P}_D | 2 \rangle_R R | 2 \rangle_R \hat{P}_D
\]

\[
= \frac{| \langle 0 | \Psi^- | R | 2 \rangle_R |^2}{pq} = c_1 k^2 (1 - p)(1 - q)^2.
\]

Similarly we can show

\[
L \langle 0 | \hat{\Pi}_1 | 1 \rangle_L = L \langle 1 | \hat{\Pi}_1 | 0 \rangle_L = c_1 k^2 2(1 - p)q(1 - q)
\]

\[
L \langle 1 | \hat{\Pi}_1 | 1 \rangle_L = c_1 k^2 (1 - p)q^2,
\]

As \( \{ |0\rangle_L, |1\rangle_L \} \) forms an orthonormal basis for the left system, the above completely specifies the probability operator \( \hat{\Pi}_1 \), which is given by

\[
\hat{\Pi}_1 = c_1 k^2 (1 - p) ((1 - q) |0\rangle_L + q |1\rangle_L)
\]

\[
((1 - q)L |0\rangle_R + q_L |1\rangle_R).
\]

Note that we have derived the bounds and optimal POM elements without needing to diagonalise \( \hat{\rho}_L \), which in this case would be tedious (but straight-forward). For higher dimensional systems, as it becomes more difficult to diagonalise \( \hat{\rho}_L \), this approach may therefore be useful.

The above arguments allow us to interpret the bound solely in terms of the geometry of the right system, from which some results follow naturally. The restriction imposed by no signalling ensures that the right system is confined to a \( D \)-dimensional subspace \( \mathcal{H}_D \), and clearly the bounds in Eqs. (8) and (12) depend only on the overlap between this subspace and the basis states \( |i\rangle_R \) of the right system. We first note that for linearly independent pure states, \( D = N \), and the right system occupies the entire space available. The limit is therefore unity, corresponding to unambiguous or error-free discrimination [12].

Consider now the effect on these bounds of a transformation of the left system \( \{ \hat{\rho}_L, \rho_i \} \rightarrow \{ \hat{\rho}_L, \rho'_i \} \). Suppose that we have a transformation conditioned on the outcome of some measurement, and that for a given measurement result the associated Kraus operator [14] is \( \hat{A}_L \).

It then follows that

\[
\hat{\rho}_L = \hat{A}_L \hat{\rho}_L \hat{A}_L^\dagger, \quad \rho'_i = p_i \text{Tr}(\hat{\rho}_L \hat{A}_L \hat{A}_L^\dagger),\]

where \( \hat{A}_L \) is chosen such that \( \text{Tr}(\hat{A}_L \hat{A}_L^\dagger) = 1 \). If \( \hat{A}_L \)

has rank \( M \leq D \), the transformed set occupies an \( M \)-dimensional subspace. By considering again the Schmidt decomposition of the transformed entangled state \( \hat{A}_L | \Psi \rangle \), we can see that the right system must also now occupy an \( M \)-dimensional subspace \( \mathcal{H}_M \). No signalling requires that \( \mathcal{H}_M \subseteq \mathcal{H}_D \), with equality if and only if \( M = D \).

But the maximum confidence depends only on the overlap of the projector \( \sum_{i \in \sigma} |i\rangle_R |i\rangle_R \) with the subspace \( \mathcal{H}_M \) (respectively \( \mathcal{H}_D \) for the transformed system). Thus it is clear that \( P(\hat{\rho}_L | \omega_j) \leq P(\hat{\rho}_L | \omega_j) \) i.e. no physically allowed transformation, deterministic or probabilistic, of a given set of states \( \{ \hat{\rho}_i \} \) with associated probabilities \( \{ p_i \} \) can result in a set which is more distinguishable by this measurement strategy. In particular, for a rank \( D \) operator (i.e. one describing an invertible transformation), this figure of merit is identical for the transformed and untransformed sets, as pointed out in [12].

Finally, we note that there is an relationship between entanglement concentration and maximum confidence discrimination, analogous to that which exists for unambiguous discrimination [15]. Unambiguous discrimination may be thought of as occuring in two steps - transformation of the states into mutually orthogonal ones with some probability of success, followed by a von Neumann measurement to discriminate perfectly between the transformed states. If the transformation fails, the out-
come is interpreted as inconclusive. It turns out that the optimal transformation (that minimising the probability of an inconclusive result), is also the one which transforms an appropriately chosen non-maximally entangled state to a maximally entangled one, with the optimal probability of success \[13\]. The maximum confidence measurement may also be thought of as a two-step process, in a way completely analogous to that for unambiguous discrimination \[9\]. In the first step, the states are transformed according to \(\hat{\Pi} = I - \frac{p_{\text{succ}}}{\lambda_i D} \hat{\rho}^{-1}\) with some probability of success \(p_{\text{succ}}\). If this fails, the outcome may be interpreted as inconclusive, and is associated with a probability operator \(\hat{\Pi}_{\text{fail}} = I - \frac{p_{\text{fail}}}{\lambda_i D} \hat{\rho}^{-1}\). If it succeeds, the second step consists of a measurement corresponding to projectors onto the new states (for pure states). The probability of success is limited by the condition \(\hat{\Pi}_{\text{fail}} \geq 0\). Thus

\[
\hat{I} - \frac{p_{\text{succ}}}{\lambda_i D} \hat{\rho}^{-1} = \sum_{i=0}^{D-1} \left( 1 - \frac{p_{\text{succ}}}{\lambda_i D} \right) |\lambda_i\rangle \langle \lambda_i| \geq 0, \tag{29}
\]

and we require \(p_{\text{succ}} \leq \lambda_i D, \forall \lambda_i\). The optimal probability of success for the transformation \(\hat{\rho} \rightarrow \frac{1}{\lambda_i D} \hat{\rho}^{1/2} \hat{\rho}^{-1/2} \hat{\rho}^{1/2}\) is therefore \(\lambda_{\text{min}} D\). Consider now the effect of this transformation on the entangled state \(|\Psi\rangle\) from Eq. \[4\]

\[
|\Psi\rangle \rightarrow \frac{1}{\sqrt{D}} \hat{\rho}^{1/2} |\Psi\rangle = \frac{1}{\sqrt{D}} \sum_{i=0}^{D-1} |\lambda_i\rangle_L |\lambda_i\rangle_R. \tag{30}
\]

This operation transforms the non-maximally entangled state \(|\Psi\rangle\) into a maximally entangled one. Note that the optimal probability of success, \(p_{\text{succ}} = \lambda_{\text{min}} D\), reaches the bound given in \[10\] for transforming a non-maximally entangled state to a maximally entangled one by local operations and classical communication.

No signalling condition is fundamental in reconciling quantum mechanics and special relativity, and there are now several examples of this condition being employed as a physical law to limit quantum mechanical operations. In this paper we have used no-signalling as a principle to limit quantum state discrimination, and have shown that these considerations lead naturally to the maximum confidence strategy. We have shown explicitly that for pure states the bound and optimal measurement may be derived from no-signalling. We have also discussed how this may be extended to mixed states, and illustrated the argument by means of an example. The no-signalling argument provides a direct way to find the bound and optimal measurement, without the need to diagonalise the density operator, as would otherwise be required. No-signalling thus provides an alternative approach, both enhancing our understanding of this strategy, and serving as a calculational tool. Some results arise naturally from this approach, notably that the bound cannot increase under any transformation, deterministic or probabilistic, of the states. We also demonstrated the link between maximum confidence measurements and entanglement concentration. The manipulation of entanglement is of considerable interest at the present time due to its importance in quantum information processing \[11\].

We thank J. Jeffers and C. Gilson for helpful discussions. S. C. acknowledges support by the Synergy fund of the Universities of Glasgow and Strathclyde. E. A. acknowledges financial support from the Royal Society. S. M. B. thanks the Royal Society and the Wolfson Foundation for support.