A Return to the Optimal Detection of Quantum Information

Eric Chitambar and Min-Hsiu Hsieh

1 Department of Physics and Astronomy, Southern Illinois University, Carbondale, Illinois 62901, USA
2 Centre for Quantum Computation & Intelligent Systems (QCIS), Faculty of Engineering and Information Technology (FEIT), University of Technology Sydney (UTS), NSW 2007, Australia

(Dated: May 10, 2014)

In 1991, Asher Peres and William Wootters wrote a seminal paper on the nonlocal processing of quantum information [Phys. Rev. Lett. 66 1119 (1991)]. We return to their classic problem and solve it in various contexts. Specifically, for discriminating the “double trine” ensemble with minimum error, we prove that global operations are more powerful than local operations with classical communication (LOCC). Even stronger, there exists a finite gap between the optimal LOCC probability and that obtainable by separable operations (SEP). Additionally we prove that a two-way, adaptive LOCC strategy can always beat a one-way protocol. Our results provide the first known instance of “nonlocality without entanglement” in two qubit pure states.

One physical restriction that naturally emerges in quantum communication scenarios is nonlocality. Here, two or more parties share some multi-part quantum system, but their subsystems remain localized with no “global” quantum interactions occurring between them. Instead, the system is manipulated through local quantum operations and classical communication (LOCC) performed by the parties.

Asher Peres and William Wootters were the first to introduce the LOCC paradigm and study it as a restricted class of operations in their seminal work [1]. To gain insight into how the LOCC restriction affects information processing, they considered a seemingly simple problem. Suppose that Alice and Bob each possess a qubit, and with equal probability, their joint system is prepared in one of the states belonging to the set \( \{ |D_i\rangle = |s_i\rangle \otimes |s_i\rangle \}_{i=0}^2 \), where \( |s_i\rangle = U_i |0\rangle \) and \( U = \exp(-\frac{i\pi}{3} \sigma_y) \). This highly symmetric ensemble is known as the “double trine,” and we note that lying orthogonal to all three states is the singlet \( |\Psi^\pm\rangle = \sqrt{1/2}(|01\rangle - |10\rangle) \).

Alice and Bob’s goal is to identify which double trine element was prepared only by performing LOCC. Like any quantum operation used for state identification, Alice and Bob’s collective action can be described by some positive-operator valued measure (POVM). While the non-orthogonality of the states prohibits the duo from perfectly identifying their state, there are various ways to measure how well they can do. Peres and Wootters chose the notoriously difficult measure of accessible information [2], but their paper raises the following two general conjectures concerning the double trine ensemble, which can apply to any measure of distinguishability:

C1: LOCC is strictly sub-optimal compared to global operations,

C2: The optimal LOCC protocol involves two-way communication and adaptive measurements.

The set of global POVMs will be denoted by GLOBAL, and C1 can be symbolized by \( \text{GLOBAL} > \text{LOCC} \). A two-way LOCC protocol with adaptive measurement refers to at least three rounds of measurement, Alice \( \rightarrow \) Bob \( \rightarrow \) Alice, where the choice of measurement in each round depends on the outcome of the other party’s measurement in the previous round. We symbolize C2 as \( \text{LOCC} > \text{LOCC} \rightarrow \). In Ref. [1] Peres and Wootters obtained numerical data to support both C1 and C2, but these conjectures have never been proven for the double trine.

Before we present our contribution to the problem, we would like to briefly highlight the legacy of the Peres-Wootters paper. Perhaps most notably is that it subsequently led to the discovery of quantum teleportation [3]. Other celebrated phenomena can also directly trace their roots to Ref. [1] such as so-called nonlocality without entanglement [4] and quantum data hiding [5]. More generally, Ref. [1] paved the way for future research into LOCC and its fundamental connection to quantum entanglement [6].

We finally note that in a return to Ref. [1] of his own, Wootters constructed a separable POVM that obtains the same information as the best known global measurement [7]. A POVM \( \{ \Pi_i \} \) belongs to the class of separable
operations (SEP) if each POVM element can be decomposed as a tensor product $\Pi_i = A_i \otimes B_i$ over the two systems. SEP is an important class of operations since every LOCC operation belongs to SEP [4].

In this paper, we prove that conjectures C1 and C2 are indeed true when distinguishability success is measured by the minimum error probability, which is defined as follows. For an ensemble $\mathcal{E} = \{|\psi_i\rangle, p_i\}_{i=1}^k$, the error probability associated with some identification POVM $\{|\Pi_i\rangle\}_{i=1}^k$ is given by $1 - \sum_{i=1}^k p_i \langle\psi_i|\Pi_i|\psi_i\rangle$. Then the minimum error probability of distinguishing $\mathcal{E}$ with respect to a class of operations $\mathcal{S}$ (such as LOCC, SEP, GLOBAL, etc.) is given by the infimum of error probabilities taken over all POVMs that can be generated by $\mathcal{S}$. Note that we can replace “infimum” by “minimum” only if $\mathcal{S}$ is a compact set of operations. While GLOBAL, SEP and LOCC all have this property, LOCC does not [8, 9]. Hence, to properly discuss the LOCC minimum error, we must consider the class of so-called asymptotic LOCC, which is LOCC plus all its limit operations [9]. We will prove C1 with respect to this more general class of operations.

A. Global and Separable Operations: The double trine ensemble has a group-covariant structure which greatly simplifies the analysis. In fact, Ban et al. have proven that the so-called “Pretty Good Measurement” (PGM) [10] is indeed an optimal global POVM for discriminating ensembles with such symmetries [11]. For the double trine, the PGM consists of simply projecting onto the orthonormal basis $\{|\Psi^-\rangle, U^i \otimes U^{i'}|F_i\rangle\}_{i=0}^2$, where

$$|F_i\rangle \propto U^i \otimes U^{i'}[(\sqrt{2} + 1)|00\rangle - (\sqrt{2} - 1)|11\rangle]. \tag{1}$$

The corresponding error probability is

$$1/2 - \sqrt{2}/3 \approx 2.86 \times 10^{-2}. \tag{2}$$

To show that SEP can also obtain this probability, we explicitly construct a separable POVM. The idea is to mix a sufficient amount of the singlet state with each of the PGM POVM elements so to obtain separability (a similar strategy was employed in Ref. [7]). The resulting POVM is $\{||\bar{F}_i\rangle\langle\bar{F}_i||\}_{i=0}^2$ with $||\bar{F}_i\rangle\langle\bar{F}_i|| = |F_i\rangle\langle F_i| + 1/3|\Psi^-\rangle\langle\Psi^-|$. It is fairly straightforward to compute that $\bar{F}_0 = 1/2(|\varphi_+\rangle\langle\varphi_+| + |\varphi_-\rangle\langle\varphi_-|)$, where $|\varphi_{\pm}\rangle = |F_0\rangle \pm \sqrt{1/3}|\Psi^-\rangle$ is a product state. This suffices to prove separability of the POVM.

B. LOCC and Asymptotic LOCC: Let us begin with a clear description of asymptotic LOCC discrimination.

In general, a sequence of POVMs $\mathcal{P}^{(n)} := \{\Pi^{(n)}_i\}_{i=1}^k$ asymptotically attains an error probability $P$ on ensemble $\{|\psi_i\rangle, p_i\}_{i=1}^k$ if for every $\epsilon > 0$ we have $P + \epsilon > 1 - \sum_{i=1}^k p_i \langle\psi_i|\Pi^{(n)}_i|\psi_i\rangle$ for sufficiently large $n$. If each POVM in the sequence $\mathcal{P}^{(n)}$ can be generated by LOCC, then $P$ is achievable by asymptotic LOCC.

It is known that for an ensemble of linearly independent pure states, the global POVM attaining minimum error consists of orthonormal, rank one projectors [11] (see also [12]). We strengthen this result and extend it to the asymptotic setting.

**Theorem 1.** Let $\mathcal{E} = \{|\psi_i\rangle, p_i\}_{i=1}^k$ be an ensemble of linearly independent states spanning some space $S$. Suppose that $P_{opt}$ is the global minimum error probability of $\mathcal{E}$. Then there exists a unique orthonormal basis $\{|\phi_i\rangle\}_{i=1}^k$ of $S$ such that: (a) A POVM attains an error probability $P_{opt}$ on $\mathcal{E}$ if and only if it can also distinguish the $\{|\phi_i\rangle\}_{i=1}^k$ with no error, and (b) A sequence of POVMs asymptotically attains an error probability $P_{opt}$ on $\mathcal{E}$ if and only if it contains a subsequence that can asymptotically distinguish the $\{|\phi_i\rangle\}_{i=1}^k$ with no error.

The proof is given in the Appendix. Theorem 1 essentially reduces optimal distinguishability of non-orthogonal linearly independent ensembles to perfect discrimination of orthogonal ensembles. Applying part (a) to the double trine ensemble, if an LOCC POVM could attain the error probability of Eq. (1), then it can also perfectly distinguish the $|F_i\rangle$ given by (1). However, these are three entangled states which, by a result of Walgate and Hardy, means they cannot be distinguished perfectly by LOCC [13]. Therefore, the global minimum error probability is unattainable by LOCC.

But is the probability attainable by asymptotic LOCC? If it is, then part (b) of Theorem 1 likewise implies that the $|F_i\rangle$ must be perfectly distinguishable by asymptotic LOCC. While Ref. [13] provides simple criteria for deciding perfect LOCC distinguishability of two qubit ensembles, no analogous criteria exists for asymptotic LOCC. The only general result for asymptotic discrimination has been recently obtained by Kleinmann et al. [14]. Here we cite their result in its strongest form, adapted specifically for the problem at hand.

**Proposition 1** ([14]). If the states $\{|F_i\rangle\}_{i=0}^2$ can be perfectly distinguished by asymptotic LOCC, then for all $\chi \in [1/3, 1]$ there is a product operator $E \geq 0$ such...
that (i) \(\sum_{i=0}^{2} |F_i|E|F_i\rangle = 1\), (ii) \(\langle F_0|E|F_0\rangle = \chi\), and (iii) the normalized states \(|F_i\rangle := \frac{1}{\sqrt{\langle F_i|E|F_i\rangle}} E^{1/2}|F_i\rangle\) are perfectly distinguishable by separable operations.

In the appendix we prove that these three conditions cannot be simultaneously satisfied; therefore, GLOCC > LOCC for minimum error discrimination. Here, we provide a little intuition into why Proposition 1 must be true. For every LOCC protocol that correctly identifies the given state with probability 1, that can be identified with probability \(\chi = 1/3\) to its final average value (\(\chi = 1 - \epsilon\)). Then for each \(\chi \in (1/3, 1 - \epsilon)\), the protocol can be halted after some sequence of measurement outcomes (collectively represented by the product operator \(E\)) such that given these outcomes: (1) there is one state that can be identified with probability \(\chi\) (which by symmetry we can assume is \(|F_0\rangle\)), and (2) the transformed ensemble can be discriminated by a separable POVM with success probability no less than \(1 - \epsilon\). By compactness of SEP, we let \(\epsilon \to 0\) and replace (2) by the condition that a separable POVM perfectly distinguishes the post-halted ensemble.

C. LOCC > LOCC-\(\epsilon\): We will now compute the minimum one-way error probability for the double trine, and then describe an explicit two-way protocol with a smaller error probability. In the one-way task, Alice makes a measurement and communicates her result to Bob. Without loss of generality, we fine-grain Alice’s measurement so that each POVM element is rank one \(|\eta\rangle\langle \eta|\), with \(|\eta\rangle = r \cos \theta|0\rangle + r e^{i\phi} \sin \theta |1\rangle\). Given outcome \(\eta\), Bob’s task is to optimally discriminate the ensemble \(\{|s_i\rangle\}_{i=0}^{2}\), but now with an updated distribution \(\{p_i\}_{i=0}^{2}\) given by

\[
p_k = \frac{|\langle \eta|s_k\rangle|^2}{2P(\eta)} = \frac{1}{3} \cos \frac{2\pi k}{3} \cos \theta + e^{i\phi} \sin \frac{2\pi k}{3} \sin \theta^2. \tag{3}
\]

Here, \(P(\eta) = \frac{1}{3} \sum_{i=0}^{2} |\langle \eta|s_i\rangle|^2\), and we’ve used the covariance \(\frac{1}{3} \sum_{i=0}^{2} |\langle \eta|s_i\rangle|^2 = \frac{1}{2}\). Additionally, we can assume that \(p_0 \geq p_1, p_2\), since if \(|\eta\rangle\) fails to generate a distribution with this property, by the symmetry we can always rotate \(|\eta\rangle\) such that \(p_0\) is indeed the maximum post-measurement probability. This means we can only restrict attention to \(-\pi/6 \leq \theta \leq \pi/6\).

Next, we observe that Bob’s task of distinguishing the ensemble \(\{|s_i\rangle, p_i\}_{i=0}^{2}\) is no easier than distinguishing between the two weighted states \(\rho = p_0|s_0\rangle\langle s_0|\) and \(\sigma = p_1|s_1\rangle\langle s_1| + p_2|s_2\rangle\langle s_2|\). Indeed, any protocol distinguishing the three \(|s_i\rangle\) can always be converted into a protocol for distinguishing \(\rho\) and \(\sigma\) by simply coarse-graining over all outcomes corresponding to \(|s_2\rangle\) and \(|s_3\rangle\). The minimum error probability in distinguishing \(\rho\) and \(\sigma\) is readily found to be (see Appendix):

\[
\frac{1}{2} - \frac{1}{2} \sqrt{1 - 3p_1p_2 - p_0p_1 - p_0p_2}, \tag{4}
\]

which simplifies to \(\frac{1}{2} - \frac{1}{2} \sqrt{1 + 75 + 32 \cos(2\theta) - 7 \cos(4\theta) + 18 \cos(2\phi) \sin^2(2\theta)}\). In the interval \(-\pi/6 \leq \theta < \pi/6\), a minimum is obtained at \(\theta = -\pi/6\) and \(\phi = 0\). This corresponds to \(p_0 = p_1 = 1/2\) and \(p_2 = 0\) with an error probability of \(1/2 - \sqrt{3}/4\). Now, this probability lower bounds the error probability along each branch of Alice’s measurement, and therefore it places a lower bound on any one-way LOCC measurement scheme. In fact, this lower bound turns out to be tight. When Alice performs the POVM \(\{|s_i\rangle\}_{i=0}^{2}\) outcome \(i\) will eliminate \(|s_i\rangle\) \(\otimes |s_i\rangle\) but leave the other two states with an equal post-measurement probability. Thus, in each branch we obtain the error probability \(1/2 - \sqrt{3}/4 \approx 6.70 \times 10^{-2}\), and this provides the minimum one-way error probability.

If we allow feedback from Bob, there exists better measurement strategies. The following protocol generalizes the optimal one-way scheme just described. (Round I) Alice performs the measurement with Kraus operators given by \(\{A_i\}_{i=0}^{2}\) with

\[
A_i = \sqrt{1/3(1-p)}|s_i\rangle\langle s_i| + \sqrt{1/3(1+p)}|s_i^+\rangle\langle s_i^+|.
\]

Here \(|s_i^+\rangle\) is the state orthogonal to \(|s_i\rangle\) (explicitly \(|s_i^+\rangle = U^\dag |1\rangle\)). Note that this is the square-root of the POVM given by Peres and Wootters [4]. Without loss of generality, we suppose that Alice obtains outcome “0” and communicates the result to Bob. Her (normalized) post-measurement states are \(|s_0\rangle = |0\rangle\), \(|s_1^\prime\rangle = [2(2+p)]^{-1/2}(\sqrt{1-p}|0\rangle - \sqrt{3(1+p)}|1\rangle)\), and \(|s_2^\prime\rangle = (2p)\sqrt{1/2} |0\rangle + \sqrt{3(1+p)}|1\rangle\). (Round II) From Bob’s perspective, he is still dealing with the original states \(|s_i\rangle\), but now their prior probabilities have changed to \(p_i|A_0 = P_{Ai}|\). He now proceeds as if Alice had completely eliminated the state \(|s_0\rangle\) (i.e. if she had chosen \(p = 1\) as the strength of her measurement). Specifically, he projects onto the eigenbasis of \(|s_1\rangle\langle s_1| - |s_2\rangle\langle s_2|\) which are the states \(|\pm\rangle = \sqrt{1/2}(|0\rangle \pm |1\rangle)\). A “+” outcome is associated with \(|s_1\rangle\) and a “−” outcome is associated with \(|s_2\rangle\); this is the optimal measurement for distinguishing between two pure
states \[15\]. By the symmetry of the states, it is sufficient to only consider the “+” outcome, which he communicates to Alice. The conditional probabilities are \(P_{A_0 B_+|0} = (1-p)/6\), \(P_{A_0 B_+|1} = 1/24(2 + \sqrt{3})(2 + p)\), and \(P_{A_0 B_+|2} = 1/24(2 - \sqrt{3})(2 + p)\). These can be inverted to give \(P_{i|A_0 B_+} = 2P_{A_0 B_+|i}\) (Round III) At this point, Alice still has three distinct states \(|s'_0\rangle\), \(|s'_1\rangle\) and \(|s'_2\rangle\). Here, \(|s'_1\rangle\) will have the greatest probability while \(|s'_0\rangle\) will have the smallest when \(p\) is close to 1. Alice then ignores \(|s'_2\rangle\) and performs optimal discrimination between just \(|s'_0\rangle\) and \(|s'_1\rangle\). Letting \(Q = P_{0|A_0 B_+} + P_{1|A_0 B_+}\), the minimum error probability is given by the well-known Helstrom bound \[15\] with normalized probabilities:

\[
P_{err}^{(A_0 B_+)} = 1 - \frac{Q}{2} \left(1 + \sqrt{1 - 4 \frac{P_{0|A_0 B_+} P_{1|A_0 B_+}}{Q^2} |\langle s'_0|s'_1\rangle|^2}\right).
\]

By symmetry, each sequence of outcomes \((A_i, B_\mu)\) - with \(i \in \{0, 1, 2\}\), \(\mu \in \{+,-\}\) - occurs with the same probability. Hence, the total error probability across all branches is given by \(P_{err} = 6P_{err}^{(A_0 B_+)}\). The plot is given in Fig. 1. It obtains a minimum of approximately \(6.47 \times 10^{-2}\), which is smaller than the one-way optimal of \(1/2 - \sqrt{3}/4 \approx 6.70 \times 10^{-2}\). The one-way optimal probability is obtained at the point \(p = 1\).

![Fig. 1](image)

FIG. 1. The error probability \(P_{err}\) using the above protocol as a function of Alice’s measurement strength \(p\). The point \(p = 1\) is the one-way minimum error probability.

Discussion and Conclusions: Our results for minimum error discrimination of the double trine ensemble can be summarized as:

GLOBAL = SEP > LOCC > LOCC\(\rightarrow\).

We thus put substantial closure to a problem first posed over 20 years ago. A primary motivation for studying this problem is to better understand the limitations of processing quantum information by LOCC. Our results complement a series of recent results in this direction \[9, 13, 16\]. In particular is Ref. \[14\] which provides a necessary condition for perfect discrimination by asymptotic LOCC discrimination (Prop. 1 above). Theorem 1 of our paper largely extends this result as we reduce asymptotic minimum error discrimination of linearly independent states to asymptotic perfect discrimination.

Our proofs of C1 and C2 are the first of its kind for two qubit ensembles, and we contrast it with previous work on the subject. C1 was first shown by Massar and Popescu for two qubits randomly polarized in the same direction \[17\]. However, a different distinguishability measure was used and the asymptotic case was not considered. Later, Koashi et al. showed an asymptotic form of C1 for two qubit mixed states with respect to the different task of “unambiguous discrimination” \[18\] (the same can also be shown for the double trine ensemble \[19\]). Finally, C2 has been observed by Owari and Hayashi on mixed states and only for a special sort of distinguishability measure \[20\]. Our work is distinct from all previous results in that it deals with pure states and minimum error probability, a highly natural measure of distinguishability. The fact that we consider pure ensembles with three states is significant since it is well-known that any two pure states can be distinguished optimally via LOCC (i.e. LOCC = GLOBAL) \[21, 22\]. Thus, with the double trine being a real, symmetric, and pure ensemble of two qubits, we have identified the simplest type of ensemble in which LOCC \(\neq\) GLOBAL for state discrimination.

Even more, since the double trine ensemble consists of product states (i.e. no entanglement), we have shown that “nonlocality without entanglement” can exist in even the simplest types of ensembles with more than two states. This distinction is further sharpened by considering that LOCC \(\neq\) SEP for the optimal discrimination of the double trine. Separable operations are interesting since, like LOCC operations, they lack the ability to create entanglement. Nevertheless, SEP evidently possesses some nonlocal power as it can outperform LOCC in discriminating the double trine. Thus, entanglement and nonlocality can truly be regarded as two distinct resources, even when dealing with two qubit pure states.

We would like to thank Runyao Duan, Debbie Leung,
Appendix

Proof of Theorem 1

(a) We first recall a few general facts about minimum error discrimination. A POVM \{\Pi_j\}_{j=1}^k is optimal on \mathcal{E} if and only if \Lambda \geq p_j|\psi_j\rangle\langle\psi_j| for all \langle\psi_j|, in which the operator \Lambda := \sum_{j=1}^k p_j \Pi_j |\psi_j\rangle\langle\psi_j| is hermitian [2,11,22]. Since \sum_{i=1}^k \Pi_i = I, we have

\[ 0 = tr[\Lambda - \Lambda] = \sum_{j=1}^k tr[\Pi_j (\Lambda - p_j \rho_j)]. \]

Then as \Lambda - p_j \rho_j \geq 0 and \[tr[\Pi_j (\Lambda - p_j \rho_j)] = tr[\Pi_j^{1/2} (\Lambda - p_j \rho_j) \Pi_j^{1/2}] \geq 0, \]
we must have that

\[ \Pi_j (\Lambda - p_j |\psi_j\rangle\langle\psi_j|) = (\Lambda - p_j |\psi_j\rangle\langle\psi_j|) \Pi_j = 0. \quad (5) \]

Our argument now proceeds analogously to the one given in Ref. [22]. Let \( P_S \) be the projector onto \( S \), and for some POVM \{\Pi_j\}_{j=1}^k that obtains \( P_{\text{opt}} \) on \( E \), define \( P_i = P_S \Pi_i P_S \). As the \(|\psi_i\rangle\) are linearly independent, there exists a set of dual states \(|\psi_i^\perp\rangle\) such that \( \langle\psi_i^\perp|\psi_j\rangle = \delta_{ij} \). We first note that \( \Lambda - p_i |\psi_i\rangle\langle\psi_i| \geq 0 \) implies \( \Lambda \geq \hat{\Lambda} = \sum_{j=1}^k p_j \hat{\Pi}_j |\psi_j\rangle\langle\psi_j| \). Thus, the POVM \{\[I - P_S, \hat{\Pi}_j\]_{j=1}^k\} also obtains \( P_{\text{opt}} \) on \( E \). We next note that \( \hat{\Pi}_j (|\psi_j\rangle) \neq 0 \) for all \( j \). For if this were not true for some \(|\psi_i\rangle\), then we could contract with \(|\psi_j^\perp\rangle\) to obtain

\[ 0 \leq \langle\psi_j^\perp| (\Lambda - p_j |\psi_j\rangle\langle\psi_j|) |\psi_j^\perp\rangle = -p_j. \]

Next, since \{\[I - P_S, \hat{\Pi}_j\]_{j=1}^k\} is an optimal POVM, the corresponding equality of Eq. [5] is 0 = \( \hat{\Pi}_j (\Lambda - p_j |\psi_j\rangle\langle\psi_j|) \). Applying \(|\psi_i^\perp\rangle\) to the RHS yields

\[ \hat{\Pi}_j (p_i \hat{\Pi}_j |\psi_j\rangle) = \delta_{ij} p_i \hat{\Pi}_j |\psi_j\rangle. \quad (6) \]

Thus, \(|\phi_i\rangle := \frac{1}{\sqrt{\langle\psi_i^\perp|\psi_i\rangle}} \hat{\Pi}_i |\psi_i\rangle\) (which is nonzero) lies in the kernel of \( \hat{\Pi}_j \) for \( i \neq j \), while \(|\phi_i\rangle\) is an eigenvector of \( \hat{\Pi}_j \) with eigenvalue 1. Hence, \( \hat{\Pi}_i = |\phi_i\rangle\langle\phi_i| \) and \(|\phi_i|\langle\phi_i| = \delta_{ij}, \) with \( \sum_{i=1}^k |\phi_i\rangle\langle\phi_i| = P_S \). We obviously have \langle\phi_i|\Pi_j|\phi_i\rangle = \delta_{ij}, which means the original POVM can perfectly distinguish the \(|\phi_i\rangle\). Conversely, any POVM \{\Pi_j\}_{j=1}^k that perfectly distinguishes the \(|\phi_i\rangle\) will satisfy \( P_S \Pi_j P_S = |\phi_i\rangle\langle\phi_i| \), and will therefore obtain \( P_{\text{opt}} \) on \( E \).

Finally, let \( \Pi_S \) be the compact, convex set of POVMs with \( k = \text{dim}(S) \) elements, each having support on \( S \). We have just shown that the continuous linear function \( f : \Pi_S \to \mathbb{R} \) given by \( f(\Pi)_{i=1}^k = 1 - \sum_{i=1}^k P_i (|\psi_i\rangle\langle\psi_i|) \) can be maximized only by an extreme point of \( \Pi_S \) (rank one projectors). Convexity of \( \Pi_S \) implies that this extreme point \( P_0 := \{|\phi_i\rangle\langle\phi_i|\}_{i=1}^k \) must be unique.

(b) For the asymptotic statement, we will need to endow \( \Pi_S \) with a metric. For two POVMs \( \mathcal{P} = \{\Pi_1, ..., \Pi_k\} \) and \( \mathcal{P}' = \{\Pi'_1, ..., \Pi'_k\} \) in \( \Pi_S \), we can define a distance measure by \( d(\mathcal{P}, \mathcal{P}') = \frac{1}{2} \sum_{i=1}^k \|\Pi_i - \Pi'_i\|_1 \), where \( \|A\|_1 = \text{Tr}[A] \). Note that when \( \Pi'_i = |\phi_i\rangle\langle\phi_i| \) is pure, we have \( \frac{1}{2} \|\Pi_i - |\phi_i\rangle\langle\phi_i|\|_1 \geq 1 - \|\phi_i\rangle\langle\phi_i|\|_1 \). \[2\]

For any \( \mathcal{P} = \{\Pi_i\}_{i=1}^k \), define \( \mathcal{P} = \{P_S \Pi_i P_S\}_{i=1}^k \). Suppose there exists a sequence of POVMs \( \mathcal{P}(n) \) such that for any \( \epsilon > 0 \), \( f(\mathcal{P}(n)) < P_{\text{opt}} + \epsilon \) for sufficiently large \( n \).

As \( \mathcal{P}(n) \) is a sequence in the compact metric space \( \Pi_S \), by the Weierstrass Theorem from analysis, there will exist some convergent subsequence \( \mathcal{P}(n') \to \mathcal{P} \). Continuity of \( f \) implies that \( \lim_{n \to \infty} f(\mathcal{P}(n')) = f(\mathcal{P}_0) = f(\mathcal{P}) \) (recall \( P_{\text{opt}} = f(\mathcal{P}_0) \)). However, by part (a), the POVM in \( \Pi_S \) obtaining \( P_{\text{opt}} \) is unique and so \( \mathcal{P} = \mathcal{P}_0 \). Thus, \( d(\mathcal{P}(n'), \mathcal{P}_0) \to 0 \), and so the error on \( E \) of each subsequence \( \mathcal{P}(n') \) satisfies

\[ 1 - \frac{1}{k} \sum_{i=1}^k \langle\phi_i|\Pi_i(n')|\phi_i\rangle \leq \frac{1}{k} d(\mathcal{P}(n'), \mathcal{P}_0) \to 0. \]

Conversely, if \( 1 - \frac{1}{k} \sum_{i=1}^k \langle\phi_i|\Pi_i(n')|\phi_i\rangle \to 0 \), then \( 1 - \langle\phi_i|\Pi_i(n')|\phi_i\rangle \geq \frac{1}{k} \|\Pi_i(n') - |\phi_i\rangle\langle\phi_i|\|_1 \to 0 \) [2], which means \( d(\mathcal{P}(n'), \mathcal{P}_0) \to 0 \). By continuity of \( f \), we have \( 1 - \sum_{i=1}^k p_i \langle\phi_i|\Pi_i(n')|\phi_i\rangle \to f(\mathcal{P}(n')) \to P_{\text{opt}} \).

All Conditions of Proposition 1 Cannot be Simultaneously Satisfied

Condition (iii) requires orthogonality \( \langle F_i|E_j\rangle = 0 \) for \( i \neq j \), and so in the basis \( \{(|\Psi^-\rangle, |F_i\rangle\}_{i=0}^2 \), \( E \) must take the form

\[ s|\Psi^-\rangle\langle\Psi^-| + \sum_{i=0}^2 (a_i |F_i\rangle\langle F_i| + |b_i\rangle\Psi^-\langle F_i| + C.C.) \]

where \( s, a_i \geq 0, \sum_{i=0}^2 a_i = 1 \), and \( C.C. \) denotes the complex conjugate. If \( E \) is a product operator across Alice and Bob’s system, then \( \gamma_{01} = A(0|E|1)_A \) must commute with \( \gamma_{10} = A(1|E|0)_A \). Here we are taking partial contractions on Alice’s system so that \( \gamma_{01} \) and \( \gamma_{10} \) are operators acting on Bob’s system. By directly computing
the commutator using Eqs. (1) and (7), the condition 
\[ \langle 0 | [\gamma_{01}, \gamma_{10}] | 0 \rangle = 0 \] becomes
\[ 0 = 6 |Im(b_2 - b_3)|^2 + (s + a_0 - \frac{2}{3}) (s - \frac{1}{3}). \] (8)
With \( a_0 = \chi \geq \frac{1}{3} \) (condition (ii)), it is clear that \( s \leq \frac{1}{3} \).
However, if \( s < \frac{1}{3} \), then this equation cannot hold for any \( a_0 \in \left[ \frac{1}{3}, \frac{2}{3} - s \right] \).
Thus, the product form constraint on \( E \) requires \( a_0 = \frac{1}{3} \).

Next, we focus on the range \( a_0 \in \left[ \frac{1}{3}, \frac{1}{2} \right] \), which because of (iii), guarantees that \( E \) is full rank. It is known that the \( |F_i^\prime\rangle \) can be perfectly distinguished by separable operations if and only if \( \sum_{i=0}^{2} C(F_i^\prime) = C(\Psi^\prime) \), where \( C(\cdot) \) is the concurrence of the state and \( |\Psi^\prime\rangle = \sqrt{|\Psi^\prime - E^{-1}|^2} |\Psi^\prime\rangle \) (see Thm. 2 of [21]). We combine this with the fact that for a general two qubit state \( \sqrt{\langle \varphi | M \otimes M N \otimes N | \varphi \rangle} \), its concurrence is given by is \( C(\varphi) \times \frac{|\det(M)| |\det(N^\dagger)|}{|\det(M)\otimes\det(N^\dagger)|} \). Therefore after noting that \( C(F_i) = 1/3 \) and writing \( E = A \otimes B \), condition (iii) of Proposition 1 can be satisfied if and only if
\[ 1 = \frac{1}{3} \sum_i \sqrt{\det(A \otimes B)} \langle \Psi^\prime | A^{-1} \otimes B^{-1} | \Psi^\prime \rangle_{\{F_i|A \otimes B|F_i\}}. \] (9)
To compute \( \langle \Psi^\prime | A^{-1} \otimes B^{-1} | \Psi^\prime \rangle_{\{F_i|A \otimes B|F_i\}} \), we use Cramer’s Rule, which says \( (A \otimes B)^{-1} = \frac{1}{\det(AB)} \text{Adj}(A \otimes B) \), where \( \text{Adj}(\cdot) \) denotes the adjugate matrix. From (7), we have that \( \langle \Psi^\prime | \text{Adj}(A \otimes B) | \Psi^\prime \rangle = \prod_{i=1}^{3} \langle F_i|A \otimes B|F_i\rangle \). Substituting this into the above equation gives
\[ 1 = \frac{1}{3} \sum_i \frac{1}{\sqrt{\det(A \otimes B)}} \prod_{i=1}^{3} \langle F_i|A \otimes B|F_i\rangle \geq \frac{1}{3} \frac{a_0a_1 + a_0a_2 + a_1a_2}{\sqrt{1/3a_0a_1a_2}}, \] (10)
where we have used (7) and Hadamard’s inequality: \( \det(A \otimes B) \leq sa_0a_1a_2 = 1/3a_0a_1a_2 \). It is a straightforward optimization calculation to see that under the constraint \( \sum_{i=0}^{2} a_i = 1 \), the RHS of (10) obtains a minimum of 1 if and only if \( a_0 = a_1 = a_2 = \frac{1}{3} \). This proves that condition (iii) is impossible whenever \( \chi > \frac{1}{3} \).

Eq. (4) and the Minimum Error for one Mixed and one Pure State

We compute an analytic formula for the minimum error probability in distinguishing weighted qubit states \( \rho = p_0 |\psi_0\rangle \langle \psi_0 | \) and \( \sigma = p_1 |\psi_1\rangle \langle \psi_1 | + p_2 |\psi_2\rangle \langle \psi_2 | \). The minimum error probability is given by \( P_{err} = 1/2 - 1/2 \| \rho - \sigma \|_1 \), where \( \| \cdot \|_1 \) is the trace norm. Since \( \rho - \sigma \) is hermitian with eigenvalues \( \lambda_i \), we have \( \| \rho - \sigma \|_1 = \sum_i |\lambda_i| \).
Thus, it is just a matter of computing the eigenvalues of \( \Delta := \rho - \sigma = p_0 |\psi_0\rangle \langle \psi_0 | - p_1 |\psi_1\rangle \langle \psi_1 | - p_2 |\psi_2\rangle \langle \psi_2 | \).
Taking \( |\psi_i\rangle = c_i |0\rangle + c_{i1} |1\rangle \), we write \( \Delta \) in coordinates:
\[ \Delta = p_0 \left( |c_0|_0^2 c_{00}^* c_{01} + |c_0|_1^2 c_{00}^* c_{11} \right) - \frac{2}{3} p_1 \left( |c_0|_0^2 c_{00} c_{11} + |c_0|_1^2 c_{00} c_{11} \right). \]
For a \( 2 \times 2 \) matrix, \( M = \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \), its eigenvalues are given by the expression \( \lambda_\pm = 1/2(a + d \pm \sqrt{(a + d)^2 - 4 \det M}) \). Thus, have that
\[ |\lambda_+| + |\lambda_-| = \begin{cases} |a + d| & \text{if } \det M \geq 0 \\ \sqrt{(a + d)^2 - 4 \det M} & \text{if } \det M \leq 0. \end{cases} \]
Letting \( M = \Delta \), we can compute that \( a + d = p_0 - p_1 - p_2 \) and
\[ \det \Delta = p_1 p_2 (1 - |\langle \psi_1 | \psi_2 \rangle|^2) - p_0 p_1 (1 - |\langle \psi_0 | \psi_1 \rangle|^2) - p_0 p_2 (1 - |\langle \psi_0 | \psi_2 \rangle|^2). \]
Therefore, we arrive at the following

**Lemma 1.** For the weighted states \( \rho \) and \( \sigma \), the minimum error probability is
\[ \frac{1}{2} - \frac{1}{2} \sqrt{1 - 4p_1 p_2 (1 - |\langle \psi_1 | \psi_2 \rangle|^2) - 4p_0 \sum_{i=1}^{2} p_i |\langle \psi_i | \psi_i \rangle|^2} \]
if \( \det(\rho - \sigma) < 0 \), and \( \frac{1}{2} - \frac{1}{2} |p_0 - p_1 - p_2| \) if \( \det(\rho - \sigma) \geq 0 \).

Now, we use this result with Eq. (3) to prove Eq. (4). Specifically, since \( |\langle s_i | s_j \rangle|^2 = \frac{1}{4} \) for the trine states, we have that \( \det \Delta \) is given by
\[ \frac{-1}{192} (3(3 + \cos(2\phi)) + 32 \cos(2\theta) - (13 + 3 \cos(2\phi)) \cos(4\theta)). \]
It is straightforward to verify that this is not positive for \( \phi \in [0, 2\pi) \) and \( \theta \in [-\pi/6, \pi/6] \). Therefore, by Lemma 1, we obtain Eq. (4).

---

*echitamb@siu.edu

minhsiuh@gmail.com

[1] A. Peres and W. K. Wootters, Phys. Rev. Lett. 66, 1119 (1991)

[2] A. Holevo, J. Multivar. Anal. 3, 337 (1973) M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. 70, 1895 (1993).

[4] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 59, 1070 (1999), quant-ph/9804053.

[5] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. 86, 5807 (2001); D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory 48, 580 (2002), quant-ph/0103098.

[6] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. 86, 5807 (2001); D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory 48, 580 (2002), quant-ph/0103098.

[7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009).

[8] E. Chitambar, W. Cui, and H.-K. Lo, Phys. Rev. Lett. 108, 240504 (2012).

[9] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, (2012), arXiv:1210.3583.

[10] Recall that the “Pretty Good Measurement” for an ensemble \(\{|\phi_i\rangle, p_i\}_{i=1}^k\) is the POVM with elements 
\[\rho^{-1/2}|\phi_i\rangle\langle\phi_i|\rho^{-1/2},\]
where \(\rho = \sum_{i=1}^k p_i |\phi_i\rangle\langle\phi_i|\). 

[11] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. 36, 1269 (1997); H. Yuen, R. Kennedy, and M. Lax, IEEE Trans. Inf. Theory 21, 125 (1975).

[12] C. Mochon, Phys. Rev. A 73, 032328 (2006).

[13] J. Walgate and L. Hardy, Phys. Rev. Lett. 89, 147901 (2002).

[14] M. Kleinmann, H. Kampermann, and D. Bruß, Phys. Rev. A 84, 042326 (2011), 1105.5132.

[15] C. W. Helstrom, Quantum detection and estimation theory (Academic Press, New York, 1976).

[16] A. M. Childs, D. Leung, L. Mančinska, and M. Ozols, (2012), arXiv:1206.5822.

[17] S. Massar and S. Popescu, Phys. Rev. Lett. 74, 1259 (1995).

[18] M. Koashi, F. Takenaga, Y. Yamamoto, and N. Imoto, (2005), 0709.3196.

[19] E. Chitambar and M.-H. Hsieh, (2013), manuscript in preparation.

[20] M. Owari and M. Hayashi, New J. Phys. 10, 013006 (2008), 0708.3154.

[21] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. 85, 4972 (2000).

[22] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, Phys. Lett. A 288, 62 (2001); S. M. Barnett and S. Croke, J. Phys. A 42, 062001 (2009).

[23] A perhaps more natural distance measure between two POVMs is the difference in measurement probabilities, maximized over all trace one, non-negative inputs: 
\[\max \sum_{i=1}^k |\text{tr}(\rho(\Pi_i - \Pi'_i))|\]. As we are only concerned with issues of convergence, it suffices to consider the equivalent metric \(d\) introduced above.

[24] R. Duan, Y. Feng, Y. Xin, and M. Ying, IEEE Trans. Inf. Theory 55, 1320 (2009), 0705.0795.

[25] F. Verstraete, J. Dehaene, and B. DeMoor, Phys. Rev. A 64, 010101 (2001).

[26] P. Hausladen and W. K. Wootters, J. Mod. Opt. 41, 2385 (1994).