More nonlocality with less purity

Somshubhro Bandyopadhyay
Bose Institute, Kolkata

Reference: S. Bandyopadhyay, Phys. Rev. Lett. 106, 210402 (2011);
also at **arXiv:1106.0104**

PHYSICAL REVIEW A VOLUME 59, NUMBER 2 FEBRUARY 1999

Quantum nonlocality without entanglement

Charles H. Bennett,[1] David P. DiVincenzo,[1] Christopher A. Fuchs,[2] Tal Mor,[3] Eric Rains,[4] Peter W. Shor,[4] John A. Smolin,[1] and William K. Wootters[5]

[1]*IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598*

[2]*Norman Bridge Laboratory of Physics 12-33, California Institute of Technology, Pasadena, California 91125*

[3]*Département d'Informatique et de Recherche Opérationelle, Succursale Centre-Ville, Montréal, Canada H3C 3J7*

[4]*AT&T Shannon Laboratory, 180 Park Avenue, Building 103, Florham Park, New Jersey 07932*

[5]*Physics Department, Williams College, Williamstown, Massachusetts 01267*

(Received 17 June 1998)

VOLUME 90, NUMBER 4 PHYSICAL REVIEW LETTERS week ending 31 JANUARY 2003

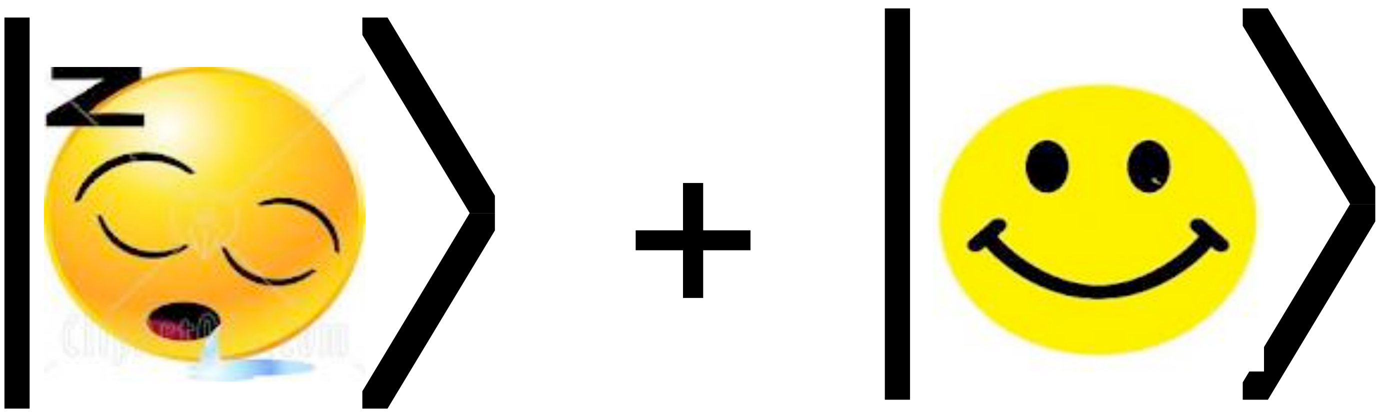
Local Indistinguishability: More Nonlocality with Less Entanglement

Michał Horodecki, Aditi Sen(De), Ujjwal Sen, and Karol Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

(Received 25 July 2002; published 27 January 2003)

Possible quantum states of the audience



Summary

- It is known that orthogonal quantum states of a composite system may not be reliably distinguished by LOCC.

- In a typical setting of LOCC discrimination of quantum states, only a **single copy** of the unknown state is made available.

By relaxing this constraint on the number of copies we will show that,

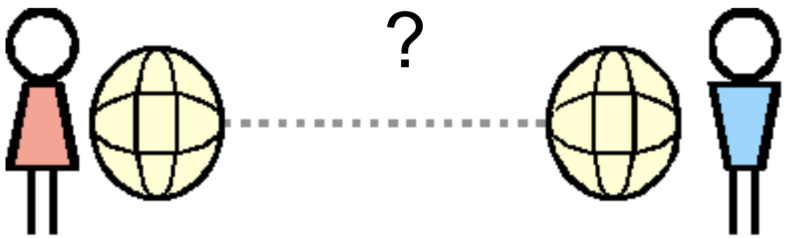
- Any given set of N orthogonal pure states can be reliably distinguished by LOCC while requiring no more than N-1 copies.

- Orthogonal mixed states, on the other hand, may not be perfectly distinguished by LOCC even with many copies.

Thus in the many-copy domain local distinguishability appears to be fundamentally different for pure and mixed states.

Perfect local discrimination of orthogonal quantum states

- Suppose a composite quantum system, consisting of two parts, A and B, held by separated observers (Alice and Bob) were prepared in one of several mutually orthogonal states: $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$



- Alice and Bob wish to determine which state the system is in with certainty only using local operations and classical communication (LOCC).

LOCC

Observers can perform arbitrary quantum operations on their respective systems and communicate classically but are not allowed to exchange quantum information (that is, qubits)

Mathematically quantum operations under LOCC are described by **separable superoperators.**

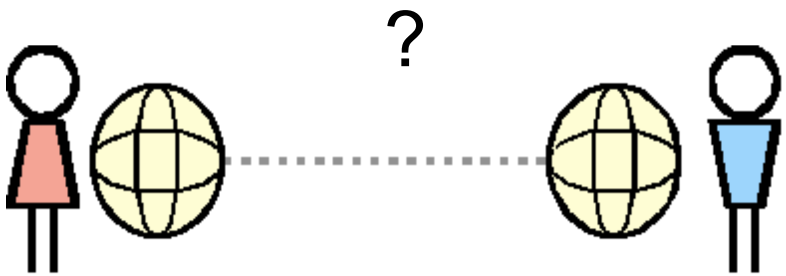
$$\rho \to \rho' = S(\rho) = \sum_i A_i \otimes B_i \rho A_i^\dagger \otimes B_i^\dagger$$

Quantum communication and cryptography primitives and entanglement manipulation (entanglement distillation, entanglement transformations) are described within the framework of LOCC.

Perfect local discrimination of orthogonal quantum states

If a set of orthogonal quantum states $\{\rho_1, \rho_2, \ldots, \rho_n\}$ can be perfectly distinguished by LOCC then it is necessary that there exists a separable POVM $\Pi = \{\Pi_1, \Pi_2, \ldots, \Pi_n\}$ such that

$$\mathrm{Tr}\left(\Pi_i \rho_j\right) = \delta_{ij}$$



Caution: not all separable measurements can be implemented by LOCC

Perfect local discrimination of orthogonal quantum states

In some cases Alice and Bob can indeed figure out correctly the state of the system. For example, any two orthogonal states can be perfectly distinguished.

In some cases they cannot. Examples include the Bell basis, product states exhibiting “nonlocality without entanglement” .

Example: when they can

Walgate, Hardy, Short and Vedral, PRL, 2000

- If the system were prepared in one of two orthogonal quantum states, $|\psi_1\rangle, |\psi_2\rangle$ then Alice and Bob can always determine correctly in which state the system is in.
- By local change of bases Alice and Bob can always bring the states in the following canonical form:

$$|\psi_1\rangle_{AB} = |1\rangle_A |\theta_1\rangle_B + |2\rangle_A |\theta_2\rangle_B + \ldots + |n\rangle_A |\theta_n\rangle_B$$

$$|\psi_2\rangle_{AB} = |1\rangle_A |\theta_1^\perp\rangle_B + |2\rangle_A |\theta_2^\perp\rangle_B + \ldots + |n\rangle_A |\theta_n^\perp\rangle_B$$

$$\langle \theta_i | \theta_j \rangle \neq 0$$

$$\langle \theta_i^\perp | \theta_j^\perp \rangle \neq 0$$

- The result holds regardless of the dimension, entanglement and multipartite structure.

Orthogonal pure states may not be perfectly distinguished by LOCC

Example 1:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)$$

$$|\Psi\rangle = |01\rangle$$

Alice and Bob cannot determine the state in question with certainty

Orthogonal pure states may not be perfectly distinguished by LOCC

Example 2: Bell basis

- Suppose Alice and Bob were given a state from the Bell basis

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle \pm \left|11\right\rangle\right)$$

$$\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle \pm \left|10\right\rangle\right)$$

Alice and Bob cannot determine the state in question with certainty

Ghosh et al, PRL, 2001

Bell states are locally indistinguishable

Ghosh et al, PRL, 2001

$$\rho = \frac{1}{4}\left(|\Phi^+\rangle^{AB}\langle\Phi^+| \otimes |\Phi^+\rangle^{CD}\langle\Phi^+| \; + \; |\Phi^-\rangle^{AB}\langle\Phi^-| \otimes |\Phi^-\rangle^{CD}\langle\Phi^-| \; + \right.$$
$$\left. |\Psi^+\rangle^{AB}\langle\Psi^+| \otimes |\Psi^+\rangle^{CD}\langle\Psi^+| \; + \; |\Psi^-\rangle^{AB}\langle\Psi^-| \otimes |\Psi^-\rangle^{CD}\langle\Psi^-|\right)$$

Smolin, PRA 2000

If A and B can distinguish the four Bell states exactly by LOCC, then they can simply distill a Bell state between C and D. This results in the creation of 1 e-bit of entanglement across the bipartition (or bipartite cut) AC : BD.

However, the Smolin state assumes the same separable form across the bipartite cut AC : BD, and therefore has zero entanglement across AC : BD.

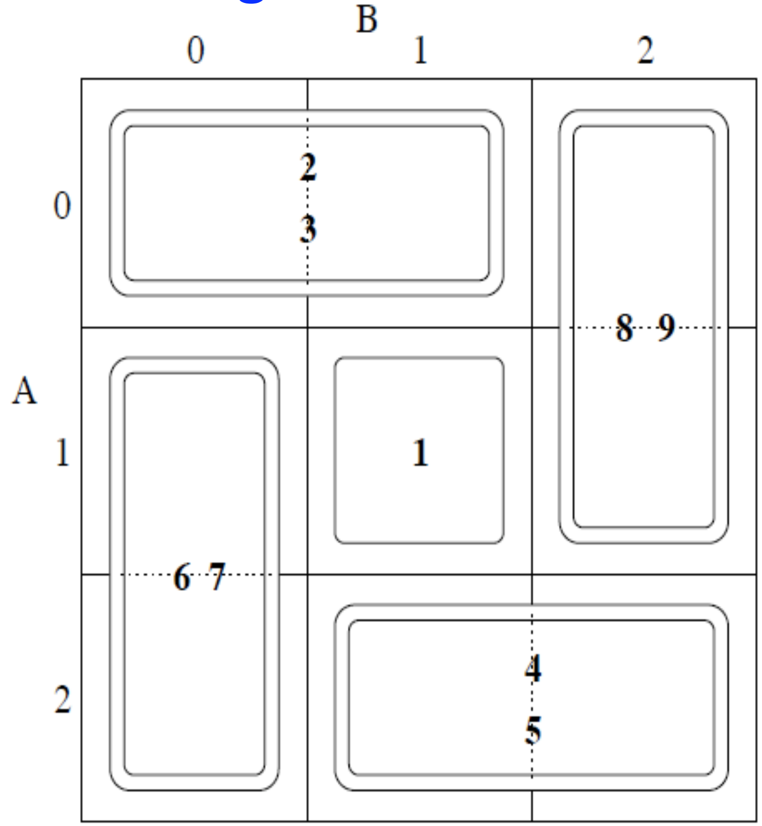
Since one cannot create entanglement from any separable state only by LOCC, it follows that the Bell states are not perfectly LOCC distinguishable.

Orthogonal pure states may not be perfectly distinguished by LOCC

<u>Example 3: Locally indistinguishable product basis</u>

"Nonlocality without entanglement"

$$
\begin{array}{rcll}
 & & |\alpha\rangle(Alice) & |\beta\rangle(Bob) \\
\psi_1 & = & |1\rangle & |1\rangle \\
\psi_2 & = & |0\rangle & |0+1\rangle \\
\psi_3 & = & |0\rangle & |0-1\rangle \\
\psi_4 & = & |2\rangle & |1+2\rangle \\
\psi_5 & = & |2\rangle & |1-2\rangle \\
\psi_6 & = & |1+2\rangle & |0\rangle \\
\psi_7 & = & |1-2\rangle & |0\rangle \\
\psi_8 & = & |0+1\rangle & |2\rangle \\
\psi_9 & = & |0-1\rangle & |2\rangle .
\end{array}
$$



Bennett at al, PRA 1998

Orthogonal pure states may not be perfectly distinguished by LOCC

Example 4: More nonlocality with less entanglement

$$\psi_1 = |00\rangle + \omega|11\rangle + \omega^2|22\rangle,$$
$$\psi_2 = |00\rangle + \omega^2|11\rangle + \omega|22\rangle,$$
$$\psi_3 = |01\rangle + |12\rangle + |20\rangle.$$

Perfectly LOCC distinguishable

Nathanson, JMP (2005)

$$\psi_1 = |00\rangle + \omega|11\rangle + \omega^2|22\rangle,$$
$$\psi_2 = |00\rangle + \omega^2|11\rangle + \omega|22\rangle, \qquad \psi_3' = |01\rangle$$

LOCC indistinguishable

Horodecki et al PRL, 2003

Nonlocality

- Locally indistinguishable (immeasurable) sets of quantum states are said to be nonlocal in the sense that a measurement of the whole can reveal more information about the state than by coordinated local measurements on its parts (LOCC).

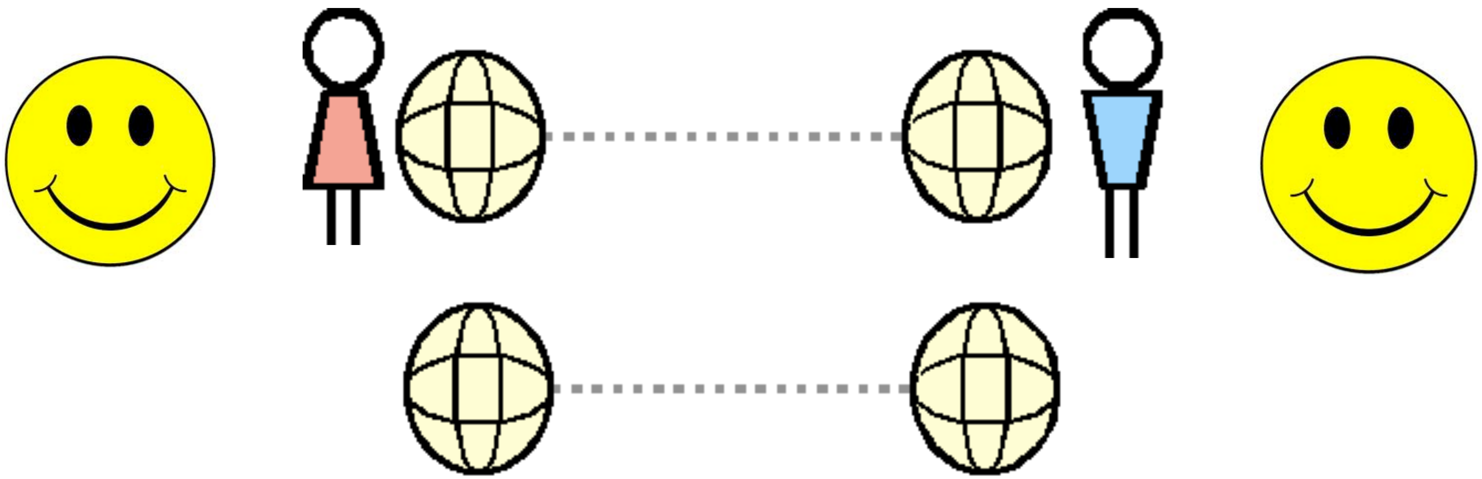
Quantum Physicist

A central assumption

- In the problem of local distinguishability of quantum states, Alice and Bob must work with a single copy of the unknown state.

More than one copy helps

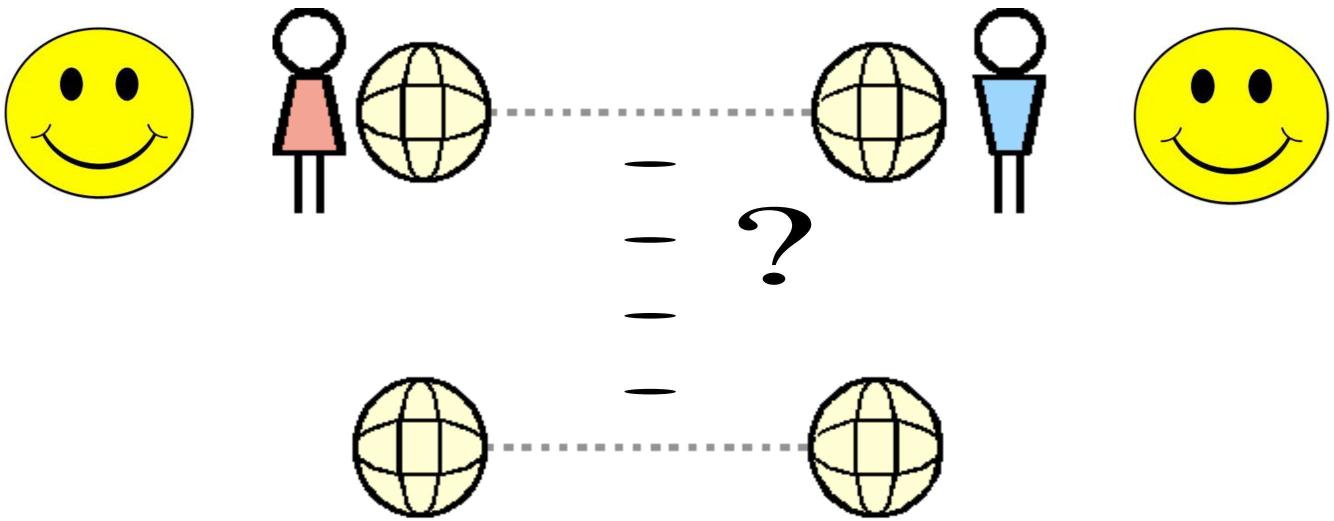
- For example, the Bell basis can be perfectly distinguished with two copies, and so are the product states exhibiting “nonlocality without entanglement”.



Local distinguishability with many copies

- Suppose we relax the single copy constraint, then the question is:

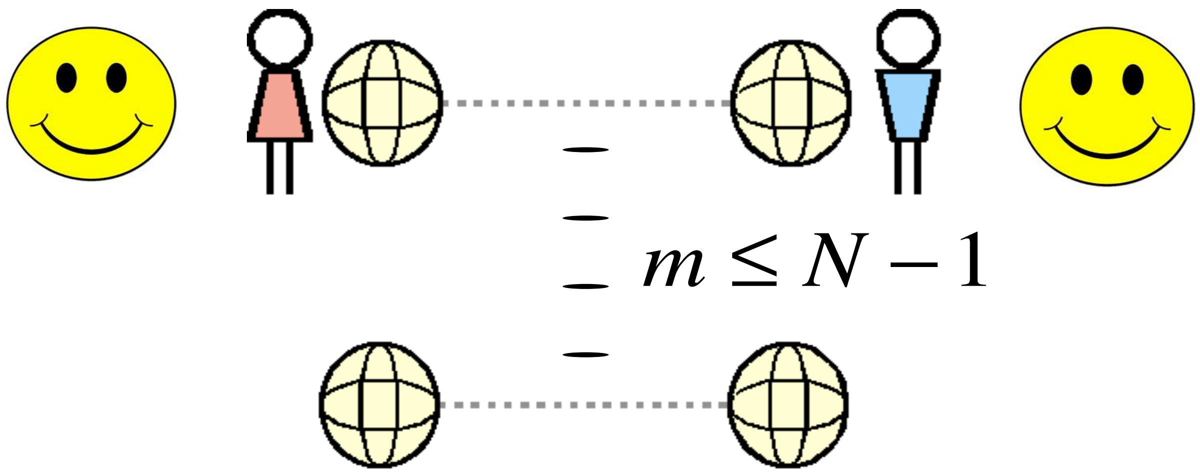
  How many copies of the unknown state are needed to distinguish any set of orthogonal quantum states (pure or mixed) by LOCC?



Perfect local discrimination of orthogonal pure states with many copies

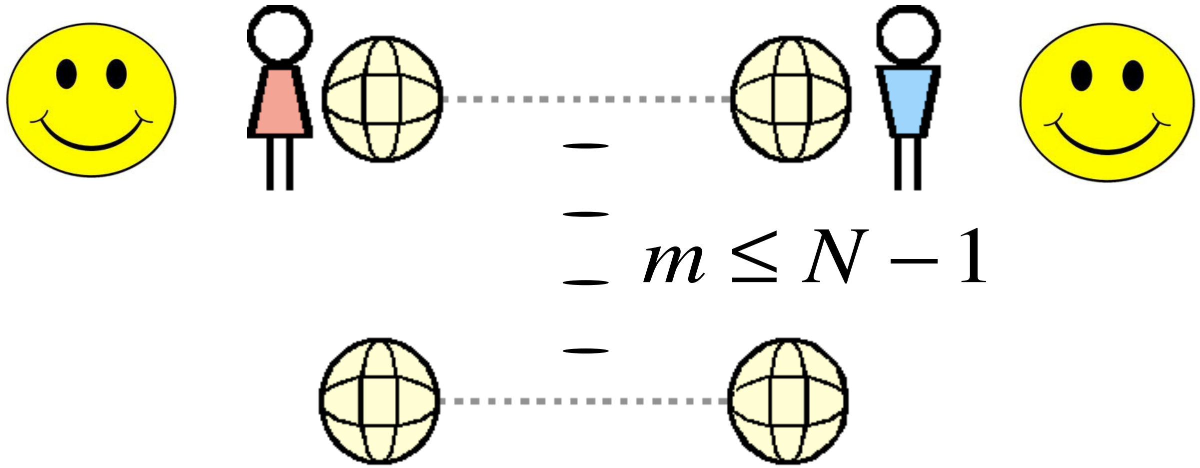
<u>Theorem:</u>

Any *N* orthogonal pure quantum states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle$ are perfectly distinguishable by LOCC with at most (*N*-1) copies regardless of their dimensionality, entanglement and multipartite structure.



Perfect local discrimination of orthogonal pure states with many copies

For any given set of orthogonal pure states $\{|\psi_i\rangle : i = 1,...,N\}$, there exists an integer $1 \le m \le N-1$, such that the set $\{|\psi_i\rangle^{\otimes m} : i = 1,...,N\}$ can be perfectly distinguished by LOCC.



Proof for any three orthogonal states

Walgate et al PRL, 2000

In general

$$\langle \theta_i | \theta_j \rangle \neq 0$$

$$\langle \theta_i^{\perp} | \theta_j^{\perp} \rangle \neq 0$$

$$|\psi_1\rangle_{AB} = |1\rangle_A |\theta_1\rangle_B + |2\rangle_A |\theta_2\rangle_B + \ldots + |n\rangle_A |\theta_n\rangle_B$$

$$|\psi_2\rangle_{AB} = |1\rangle_A |\theta_1^{\perp}\rangle_B + |2\rangle_A |\theta_2^{\perp}\rangle_B + \ldots + |n\rangle_A |\theta_n^{\perp}\rangle_B$$

$$|\psi_3\rangle_{AB} = |1\rangle_A |\phi_1\rangle_B + |2\rangle_A |\phi_2\rangle_B + \ldots + |n\rangle_A |\phi_n\rangle_B$$

$$\langle \phi_i | \theta_i \rangle \neq 0; \langle \phi_i | \theta_i^{\perp} \rangle \neq 0 \text{ for all } i$$

Proof for three orthogonal states

Alice goes first. Suppose the outcome of Alice's measurement is *i.*

$$\left|\psi_1\right\rangle_{AB} \rightarrow \left|i\right\rangle_A \left|\theta_i\right\rangle_B$$

$$\left|\psi_2\right\rangle_{AB} \rightarrow \left|i\right\rangle_A \left|\theta_i^{\perp}\right\rangle_B$$

$$\left|\psi_3\right\rangle_{AB} \rightarrow \left|i\right\rangle_A \left|\phi_i\right\rangle_B$$

$$\left\langle \phi_i \middle| \theta_i \right\rangle \neq 0; \left\langle \phi_i \middle| \theta_i^{\perp} \right\rangle \neq 0$$

Alice Measurement

$$|\psi_1\rangle_{AB} \rightarrow |i\rangle_A |\theta_i\rangle_B$$
$$|\psi_2\rangle_{AB} \rightarrow |i\rangle_A |\theta_i^{\perp}\rangle_B$$
$$|\psi_3\rangle_{AB} \rightarrow |i\rangle_A |\phi_i\rangle_B$$

$$\langle\phi_i|\theta_i\rangle \neq 0; \langle\phi_i|\theta_i^{\perp}\rangle \neq 0$$

Bob measures his system in an orthogonal basis like the one below -

$$|\theta_i\rangle, |\theta_i^{\perp}\rangle, |\eta_1\rangle, \ldots, |\eta_k\rangle$$

Bob's outcome	**State eliminated**	**State of the second copy**
$\lvert\theta_i\rangle$	$\lvert\psi_2\rangle$	$\lvert\psi_1\rangle or \lvert\psi_3\rangle$
$\lvert\theta_i^{\perp}\rangle$	$\lvert\psi_1\rangle$	$\lvert\psi_2\rangle or \lvert\psi_3\rangle$
$\lvert\eta\rangle$	$\lvert\psi_1\rangle, \lvert\psi_2\rangle$	$\lvert\psi_3\rangle$

Proof idea in the general case

- The strategy is to measure each copy separately, one after the other.

- Every round of measurement performed on a single copy succeeds in eliminating at least one state. That is, after K rounds of measurements on K copies, at least K states get eliminated.

Proof for any N orthogonal pure states

$$|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle$$

Walgate et al
PRL, 2000

$$|\psi_1\rangle_{AB} = |1\rangle_A |\theta_1\rangle_B + |2\rangle_A |\theta_2\rangle_B + \ldots + |n\rangle_A |\theta_n\rangle_B$$

$$|\psi_2\rangle_{AB} = |1\rangle_A |\theta_1^\perp\rangle_B + |2\rangle_A |\theta_2^\perp\rangle_B + \ldots + |n\rangle_A |\theta_n^\perp\rangle_B$$

$$\boxed{\begin{array}{l} \langle\theta_i|\theta_j\rangle \neq 0 \\ \langle\theta_i^\perp|\theta_j^\perp\rangle \neq 0 \end{array}}$$

$$|\psi_3\rangle_{AB} = |1\rangle_A |\phi_1^3\rangle_B + |2\rangle_A |\phi_2^3\rangle_B + \ldots + |n\rangle_A |\phi_n^3\rangle_B$$

•

•

•

$$|\psi_N\rangle_{AB} = |1\rangle_A |\phi_1^N\rangle_B + |2\rangle_A |\phi_2^N\rangle_B + \ldots + |n\rangle_A |\phi_n^N\rangle_B$$

$$\langle\phi_i^k|\theta_i\rangle \neq 0; \langle\phi_i^k|\theta_i^\perp\rangle \neq 0 \text{ for all } i \text{ and } k = 3, \ldots, N$$

Proof for N orthogonal states

First round of measurements on the first copy

Alice goes first. Suppose the outcome of Alice's measurement is *i.*

$$|\psi_1\rangle_{AB} \rightarrow |i\rangle_A |\theta_i\rangle_B$$

$$|\psi_2\rangle_{AB} \rightarrow |i\rangle_A |\theta_i^{\perp}\rangle_B$$

$$|\psi_3\rangle_{AB} \rightarrow |i\rangle_A |\phi_i^3\rangle_B$$

$$\vdots$$

$$|\psi_N\rangle_{AB} \rightarrow |i\rangle_A |\phi_i^N\rangle_B$$

$$\langle \phi_i^k | \theta_i \rangle \neq 0$$

$$\langle \phi_i^k | \theta_i^{\perp} \rangle \neq 0$$

$$\langle \phi_i^k | \phi_i^j \rangle \neq 0$$

$$k = 3, \ldots, N$$

Proof for N orthogonal states

Alice Measurement

$$|\psi_1\rangle_{AB} \rightarrow |i\rangle_A |\theta_i\rangle_B$$

$$|\psi_2\rangle_{AB} \rightarrow |i\rangle_A |\theta_i^{\perp}\rangle_B$$

$$|\psi_3\rangle_{AB} \rightarrow |i\rangle_A |\phi_i^{3}\rangle_B$$

•

•

•

$$|\psi_N\rangle_{AB} \rightarrow |i\rangle_A |\phi_i^{N}\rangle_B$$

Bob measures his system in an orthogonal basis like the one below -

$$|\theta_i\rangle, |\theta_i^{\perp}\rangle, |\eta_1\rangle, \ldots, |\eta_k\rangle$$

Bob's outcome	**State eliminated**	**No. of states still left in contention**
$\vert\theta_i\rangle$	$\vert\psi_2\rangle$	$N-1$
$\vert\theta_i^{\perp}\rangle$	$\vert\psi_1\rangle$	$N-1$
$\vert\eta\rangle$	$\vert\psi_1\rangle, \vert\psi_2\rangle$	$N-2$

Proof for N orthogonal states

Same protocol is repeated in the second round on the second copy

After each round we eliminate at least one state from contention.

Thus in the worst case no more than N-1 copies are required.

HOW GOOD IS THE BOUND N-1 ?

Local discrimination of orthogonal mixed states with many copies

Given any set of orthogonal mixed states $\left\{\rho_i : i = 1,\ldots,N\right\}$, we would like to know whether the set $\left\{\rho_i^{\otimes m} : i = 1,\ldots,N\right\}$ can be perfectly distinguished by LOCC for some positive integer m.

Conclusive (unambiguous) state discrimination by LOCC

- Conclusive state discrimination seeks definite knowledge of the system balanced against a probability of failure.

- <u>Definition:</u> A set of orthogonal quantum states (pure or mixed) is conclusively (unambiguously) locally distinguishable if and only if there is a LOCC protocol whereby with some nonzero probability $p > 0$ every state can be correctly identified.

A necessary condition for conclusive/unambiguous state discrimination by LOCC

If a set of orthogonal quantum states $\{\rho_1, \rho_2, ..., \rho_n\}$ is conclusively locally distinguishable by LOCC then it is necessary that for every i there exists a product state $|\phi_i\rangle$ such that $\forall j \neq i \ \langle \phi_j | \rho_i | \phi_j \rangle = 0$ and $\langle \phi_i | \rho_i | \phi_i \rangle \neq 0$.

Chefles, PRA (2004), Bandyopadhyay and Walgate, J Phys A (2007)

Conclusive (unambiguous) vs Perfect local discrimination

- If a set of orthogonal states is not perfectly distinguishable by LOCC then it may still be conclusively locally distinguishable.

  Examples: any three Bell states, “nonlocality w/o entanglement” states

- However, if a set is not conclusively distinguishable, then obviously it cannot be perfectly distinguished by LOCC.

Unextendible product basis (UPB)

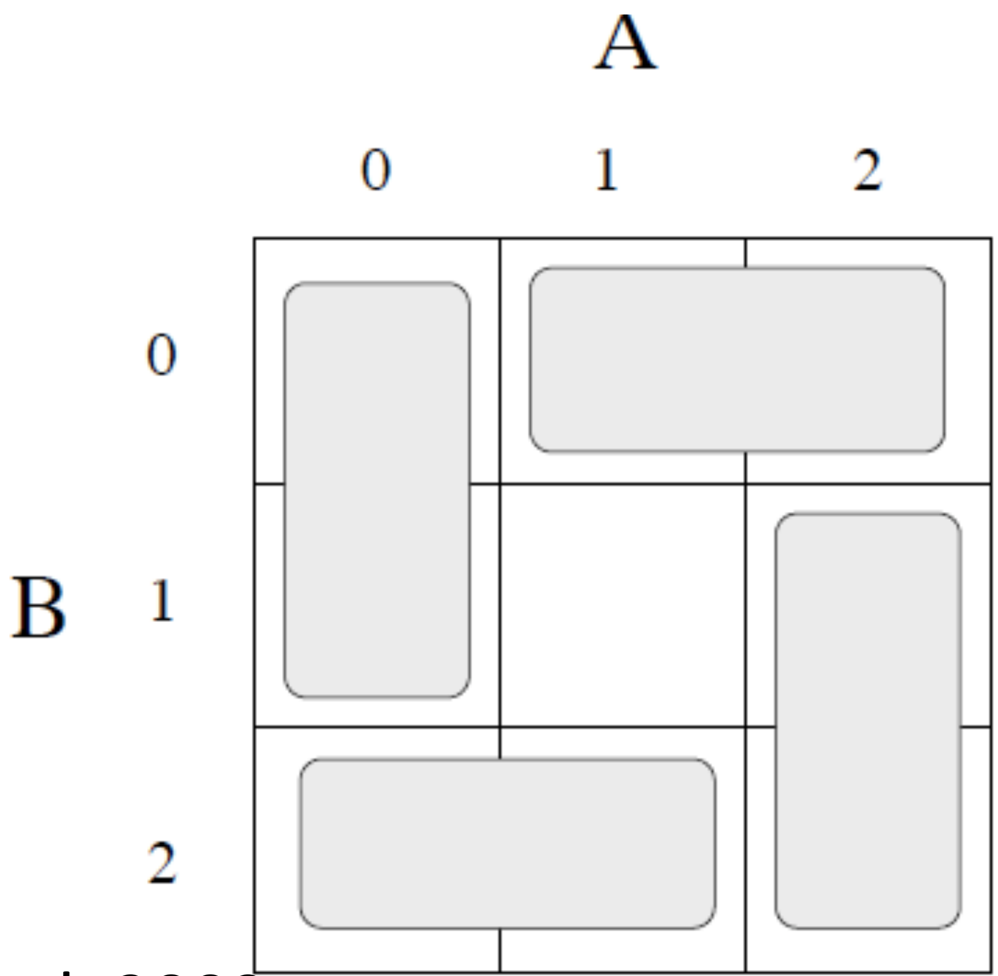
A UPB is an orthogonal product basis on $H = H_A \otimes H_B$ spanning a subspace S of H such that its complementary subspace $S^{\perp}$ contains no product state.

UPB in $3 \otimes 3$

$$
\begin{aligned}
|\psi_0\rangle &= \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle), \\
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle, \quad |\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle, \\
|\psi_4\rangle &= (1/3)(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle).
\end{aligned}
$$

Bennett et al, PRL, 1998

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle),$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle, \quad |\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle,$$
$$|\psi_4\rangle = (1/3)(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle).$$



DiVincenzo et al, 2002

Two orthogonal mixed states may not be perfectly distinguishable by LOCC with single copy

Let S be the subspace spanned by a UPB on $H = H_A \otimes H_B$ and $S^{\perp}$ be its complementary subspce.

Let σ and ρ be the normalized projectors onto the subspace S and $S^{\perp}$ respectively.

$$UPB : \left\{ \left| \psi_1 \right\rangle, \left| \psi_2 \right\rangle, \ldots, \left| \psi_k \right\rangle \right\}$$

$$\sigma = \frac{1}{k} \left(\sum_{i=1}^{k} \left| \psi_i \right\rangle \left\langle \psi_i \right| \right); \rho = \frac{1}{D-k} \left(I - \sum_{i=1}^{k} \left| \psi_i \right\rangle \left\langle \psi_i \right| \right)$$

$$where,\ k = \dim S,\ \text{and}\ D = \dim H$$

Lemma:

The orthogonal density matrices σ and ρ are not conclusively locally distinguishable (and therefore, not perfectly distinguishable by LOCC)

Proof:

Suppose the states can be conclusively locally distinguished. For ρ it implies that there is a product state $|\phi\rangle$ such that the following equations are satisfied:

$$UPB: \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle\}$$

$$\sigma = \frac{1}{k}\left(\sum_{i=1}^{k} |\psi_i\rangle\langle\psi_i|\right)$$

$$\rho = \frac{1}{D-k}\left(I - \sum_{i=1}^{k} |\psi_i\rangle\langle\psi_i|\right)$$

$$\langle\phi|\rho|\phi\rangle \neq 0$$

$$\langle\phi|\sigma|\phi\rangle = 0$$

The second equation implies that the product state $|\phi\rangle \in S^{\perp}$. This is in contradiction with the fact that $S^{\perp}$ contains no product state.

Can we distinguish the density matrices σ, ρ with many copies?

That is, we would like to know whether the orthogonal density matrices $\sigma^{\otimes n}$ and $\rho^{\otimes n}$ can be perfectly distinguished by LOCC for some positive integer n.

Tensor product of UPB subspaces

Lemma:

Let S_1 and S_2 be the UPB subspaces on $H = H_A \otimes H_B$. Then $S_1 \otimes S_2$ is also a UPB subspace on $H_A^{\otimes 2} \otimes H_B^{\otimes 2}$.

Divincenzo et al, 2002

Corollary:

If S is a UPB subspace on $H_A \otimes H_B$, then $S^{\otimes n}$ is also a UPB subspace on $H_A^{\otimes n} \otimes H_B^{\otimes n}$.

The orthogonal density matrices $\sigma^{\otimes n}$ and $\rho^{\otimes n}$ cannot be perfectly distinguished by LOCC.

Proof:

We first make the following observations:

1. $\sigma^{\otimes n}$ is the normalized projector onto $S^{\otimes n}$

2. $\rho^{\otimes n} \in \left(S^{\otimes n} \right)^{\perp}$

3. $\left(S^{\otimes n} \right)^{\perp}$ contains no product state.

Now suppose that the states $\sigma^{\otimes n}$ and $\rho^{\otimes n}$ are conclusively locally distinguishable. Then, for $\rho^{\otimes n}$ it means that there is a product state $|\phi\rangle \in H_A^{\otimes n} \otimes H_B^{\otimes n}$ such that the following two relations hold:

(a) $\langle\phi|\rho^{\otimes n}|\phi\rangle \neq 0$ and (b) $\langle\phi|\sigma^{\otimes n}|\phi\rangle = 0.$

Eq. (b) implies that $|\phi\rangle \in \left(S^{\otimes n} \right)^{\perp}$ – a contradiction.

Main results

- Orthogonal pure states can always be perfectly distinguished with finitely many copies by LOCC.

- Orthogonal mixed states cannot always be perfectly distinguished by LOCC even if multiple copies of the unknown state are available.

Points to ponder

- How good is the N-1 bound for pure states?

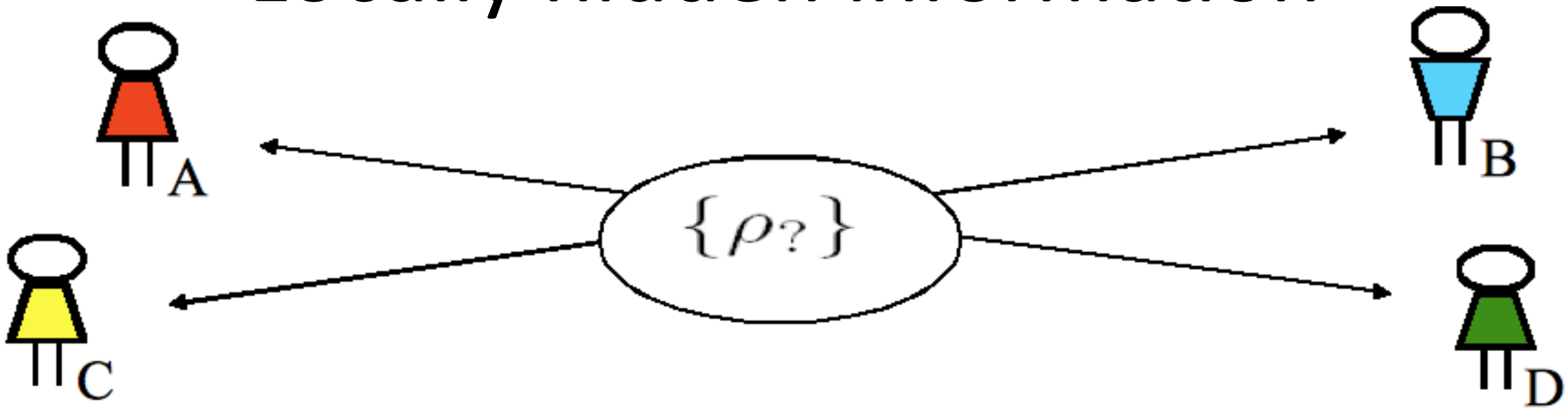
$$N \geq 4 \qquad ???????$$

- For mixed states, study the limit $n \to \infty$

- More precisely behavior of P_E in the limit $n \to \infty$

Thank you for your kind attention

Locally hidden information



Global operations on a quantum system can process information in ways that local operations on system's parts cannot.

Physical information can be stored in quantum systems such that it is inaccessible to local observers, even when they classically communicate freely.

Global measurements upon the whole system reveal information that is harder, or even impossible, to obtain by local means.