SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUANTUM MECHANICS
QUANTUM INFORMATION

Received
9 May 2014

Accepted
20 August 2014

Published
11 September 2014

Correspondence and requests for materials should be addressed to S.-M.F. (feishm@cnu.edu.cn)

Non-commutativity and Local Indistinguishability of Quantum States

Teng Ma[1], Ming-Jing Zhao[2], Yao-Kun Wang[3,4] & Shao-Ming Fei[1,5]

[1]School of Mathematical Sciences, Capital Normal University, Beijing 100048, P. R. China, [2]Department of Mathematics, School of Science, Beijing Information Science and Technology University, Beijing 100192, P. R. China, [3]Institute of Physics, Chinese Academy of Sciences, Beijing 100190, P. R. China, [4]College of Mathematics, Tonghua Normal University, Tonghua 134001, P. R. China, [5]Max-Planck-Institute for Mathematics in the Sciences, Leipzig 04103, Germany.

We study the local indistinguishability problem of quantum states. By introducing an easily calculated quantity, non-commutativity, we present an criterion which is both necessary and sufficient for the local indistinguishability of a complete set of pure orthogonal product states. A constructive distinguishing procedure to obtain the concrete local measurements and classical communications is given. The non-commutativity of ensembles can be also used to characterize the quantumness for classical-quantum or quantum-classical correlated states.

Nonlocality is one of the most important features in quantum mechanics. Quantum entanglement was firstly introduced to characterize and quantify the nonlocality, as it acts as a crucial resource in many quantum information processing tasks[1]. On the other hand, there are also quantum information and computation processing tasks without quantum entanglement, like the quantum computation with one qubit (DQC1)[2]. Other types of quantum correlations such as quantum discord[3] are introduced to capture this kind of quantum advantage. The quantum discord is considered more general than entanglement and captures the quantum correlations that entanglement fails to capture[4].

A well known quantum phenomenon that exhibits quantum nonlocality is the local indistinguishability for some quantum states. State discrimination or distinguishing is essentially primitive for many quantum information tasks, such as quantum cryptography[5] and quantum algorithms[6]. Moreover, with the remarkable experimental advances in preparation and measurement of quantum states[7,8], it becomes essential to have a theory to assess the performance of quantum state discrimination protocols. One basic problem of state discrimination is judging the local distinguishability for a set of pure orthogonal product states (POPS). Consider a set of bipartite POPS, each with a prior probability, which constitutes an ensemble of a density operator ρ_{AB}. Although a set of POPS can always be distinguished globally, it may not be distinguished locally by local operations and classical communications (LOCC). This is called *quantum nonlocality without entanglement*[9]. In[10] the relation between quantum discord and local indistinguishability has been investigated. However, contrary to one's intuitive appeal, the quantum discord of ρ_{AB} is not an indicator of local indistinguishability for a set of states that constitute the pure-state decomposition of ρ_{AB}[4,10]. It shows no relation between zero quantum correlation and the local distinguishability for a set of POPS. The local indistinguishability problem of a set of POPS remains open, although many research have been done so far[9–14,18].

It is natural to ask what kind of quantity or quantumness accounts for the quantum nonlocality. In this article, instead of quantum correlation measures, such as quantum discord, quantum deficit, etc., we investigate local indistinguishability for a set of POPS from the point of quantumness of ensemble. We first introduce an easily calculated quantity, non-commutativity, to quantify the quantumness of a quantum ensemble. Based on the non-commutativity, we present a necessary and sufficient criterion for the local indistinguishability. We also give a constructive distinguishing procedure to judge the local indistinguishability for any given set of POPS by using the criterion. Moreover, by proving the uniqueness of the expression of for semi-classical quantum correlated states, we show that our definition for quantumness of ensembles can be used to characterize the quantumness for semi-classical states.

Results

Non-commutativity for a set quantum states. A quantum ensemble containing only two pure states $|\psi\rangle$ and $|\phi\rangle$ with equal probability can be viewed as a set of binary signals in some communication scheme. If $|\psi\rangle$ and $|\phi\rangle$ are

orthogonal, the ensemble becomes classical since different states of classical information can be thought of merely as orthogonal quantum states[1]. Non complete overlap of the two states, $x = |\langle\psi|\phi\rangle|$, $0 < x < 1$, induces quantumness for the ensemble. In fact the ensemble is most 'quantum' when $x = 1/\sqrt{2}$, i.e. when the two states have an angle 45° between them[15].

Taking the above observation into account, we introduce non-commutativity to characterize the quantumness for a quantum ensemble. Let $A_1, A_2, \ldots, A_n$ be a set of operators. We define the total non-commutativity for this set,

$$N(A_1, A_2, \ldots, A_n) = \sum_{i,j=1, i>j}^{n} \left\| [A_i, A_j] \right\|, \qquad (1)$$

where $[A, B] = AB - BA$, $||A||$ is the trace norm of the operator A, $\|A\| = Tr\sqrt{AA^\dagger}$. The non-commutativity is a natural measure of 'quantumness' for a quantum ensemble $\varepsilon = \{p_i, \rho_i\}$, where ρ_i are density operators with probability p_i. Denote $A_i = p_i\rho_i$, then $N(A_1, A_2, \ldots, A_n)$ is the measure of quantumness for the ensemble ε. Here for the problem of local distinguishability of states $\rho_1, \rho_2, \ldots, \rho_n$, the prior probabilities p_i are irrelevant. One only needs to concern the quantity $N(\varepsilon) = N(\rho_1, \rho_2, \ldots, \rho_n)$ to judge the local distinguishability of the set of states $\rho_1, \rho_2, \ldots, \rho_n$. The prior probabilities p_i do make sense when one concerns the quantumness of a state given by the ensemble $\varepsilon = \{p_i, \rho_i\}$ (see section "The quantumness of semi-classical states").

The non-commutativity N has the following properties, which make it a well defined measure for quantumness of an ensemble:

(1) N is non negative;
(2) N is unitary invariant, $N(\varepsilon) = N(U\varepsilon U^\dagger)$, where $U\varepsilon U^\dagger = \{p_i, U\rho_i U^\dagger\}$ with U being any unitary matrix;
(3) For an ensemble only containing two pure states $A_1 = |\psi\rangle\langle\psi|$ and $A_2 = |\phi\rangle\langle\phi|$, without considering their prior probabilities, $N(A_1, A_2)$ is zero only when the overlap $x = |\langle\phi|\psi\rangle| = 0$ or 1. $N(A_1, A_2)$ gets to a maximum of 1 when $x = 1/\sqrt{2}$ (see Methods for the proof), which coincides with the above analysis of quantumness for two pure states;
(4) The sum of two sets' non-commutativity is equal to or less than the non-commutativity of the sum of the two sets: $N(\{|a_i\rangle\}) + N(\{|b_i\rangle\}) \leq N(\{\{|a_i\rangle\}, \{|b_i\rangle\}\})$. One can easily verify the inequality from the definition of N. The equality holds if $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$ are either mutually orthogonal or identical.

A set of quantum states corresponds to a quantum ensemble. Nevertheless, one density operator may have many quantum ensemble decompositions. For instance, consider the density operator in a 3 ⊗ 3 system, $\rho = \frac{1}{9}\mathrm{I} = \frac{1}{9}\sum_{i=1}^{9} |\psi_i\rangle\langle\psi_i| = \frac{1}{9}\sum_{s,t=1}^{3} |st\rangle\langle st|$, where $|\psi_1\rangle = |1\rangle|1\rangle$, $|\psi_{2,3}\rangle = \frac{1}{\sqrt{2}}|0\rangle|0 \pm 1\rangle$, $|\psi_{4,5}\rangle = \frac{1}{\sqrt{2}}|2\rangle|1 \pm 2\rangle$, $|\psi_{6,7}\rangle = \frac{1}{\sqrt{2}}|1 \pm 2\rangle|0\rangle$, $|\psi_{8,9}\rangle = \frac{1}{\sqrt{2}}|0 \pm 1\rangle|2\rangle$, $|st\rangle = |s\rangle \otimes |t\rangle$, $|s\rangle$ and $|t\rangle$ are the computational basis. Both $\{|\psi_i\rangle\}$ and $\{|st\rangle\}$ are pure-state decompositions of ρ. However, the set $\{|st\rangle\}$ can be locally distinguished while $\{|\psi_i\rangle\}$ cannot[9]. Hence that ρ having zero quantum correlation is not an indicator for the local distinguishability of the states in ρ's pure-state decomposition. On the other hand, if we change the probability of $|\psi_i\rangle$, ρ is no longer an identity and can have nonzero quantum correlation, but the nine states $|\psi_i\rangle$ still remain locally indistinguishable. Usually, the local indistinguishability of a set of pure states has no simple relations with the properties of the related density operator[4].

To study the local indistinguishability, and its relations with the quantumness of a quantum ensemble in terms of non-commutativity, in the following we call an ensemble $\varepsilon = \{p_i, |\psi_i\rangle\}$ classical if $N(\varepsilon) = 0$, and quantum if $N(\varepsilon) > 0$. If $N(\varepsilon) = 0$, from the properties of non-commutativity, $\{|\psi_i\rangle\}$ must be either mutually orthogonal or identical and the states form a set of classical signals from informatics point of view. If $N(\varepsilon) > 0$, among $\{|\psi_i\rangle\}$ there must be at least one pair of states that are neither orthogonal nor identical. Consider a set of bipartite POPS $\{|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle\}$, where $|\psi_i\rangle$ are all mutually orthogonal, $|a_i\rangle$ and $|b_i\rangle$ are associated to partite A and B respectively. Obviously, this set forms a classical ensemble $\varepsilon = \{p_i, |\psi_i\rangle\}$ since $N(\varepsilon) = 0$, where p_i is the probability with respect to $|\psi_i\rangle$. Correspondingly one has ensembles $\varepsilon^A = \{p_i, |a_i\rangle\}$ and $\varepsilon^B = \{p_i, |b_i\rangle\}$ respectively. If $N(\varepsilon^A) = N(\varepsilon^B) = 0$, we call ε a classical-classical ensemble. If $N(\varepsilon^A) = 0$, $N(\varepsilon^B) > 0$, we call ε a classical-quantum ensemble. Analogously we can define quantum-classical and quantum-quantum ensembles.

Local distinguishability for a set quantum states. A set of states is said to be reliably distinguished locally or distinguished locally if all the states in the set can be distinguished by *finite* rounds of LOCC protocols. If there are at least two states in a set which can not be distinguished by finite rounds of LOCC protocols, we say that the set can not be distinguished locally. The arguably more operational "asymptotic local operations and classical communications discrimination problem[16,17]" is not under our consideration.

Theorem 1 If a set of bipartite pure orthogonal product states cannot be locally distinguished, the ensemble composed of these states must be a quantum-quantum ensemble.

Proof. Consider a set of bipartite POPS, not necessarily complete, $\{|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle\}$ with $\langle\psi_i|\psi_j\rangle = 0$, $\forall i \neq j$. Suppose these states form a classical-quantum or classical-classical ensemble $\varepsilon = \{p_i, |a_i\rangle \otimes |b_i\rangle\}$ with non zero p_i. Since $N(\{|a_i\rangle\}) = 0$, $\{|a_i\rangle\}$ must be either mutually orthogonal or identical. To distinguish $\{|\psi_i\rangle\}$ locally, we can first take projective measurement on A side to distinguish those orthogonal states in $\{|a_i\rangle\}$. For those identical states $|a_i\rangle$, for example, $|a_1\rangle = |a_2\rangle$, we can take a projective measurement on B to distinguish state $|a_1\rangle$ from state $|a_2\rangle$, since $|b_1\rangle$ and $|b_2\rangle$ must be mutually orthogonal to ensure that $\langle\psi_1|\psi_2\rangle = 0$. In this way we can distinguish the states in the set ε reliably. The analysis is similar if ε is a quantum-classical ensemble. Therefore if a set of bipartite POPS forms a classical-classical, quantum-classical or classical-quantum ensemble, the set can be locally distinguished. And if the set of POPS states cannot be locally distinguished, the ensemble composed of these states must be a quantum-quantum one. □

Since it is impossible to form a quantum-quantum ensemble for a set of POPS in a 2 ⊗ 2 system, Theorem 1 is both necessary and sufficient for 2 ⊗ 2 systems. For higher dimensional cases, there are quantum-quantum ensembles whose states can be locally distinguished. In fact, for 2 ⊗ n systems, any set of POPS is locally distinguishable[11]. Theorem 1 reveals a relation between local distinguishability and quantumness of a set of states. In the following, we give a necessary and sufficient criterion for local distinguishability for all POPS from the view of quantumness of ensembles.

We say that two sets $\{|a_i\rangle\}$ and $\{|a'_j\rangle\}$ are orthogonal if and only if $\langle a_i|a'_j\rangle = 0$, $\forall i, j$. If a set of states cannot be divided into subsets such that those subsets are mutually orthogonal, then we call the set a single set. Consider a set of states $\varepsilon = \{|a_1\rangle = |0\rangle, |a_2\rangle = |0 + 1\rangle, |a_3\rangle = |2\rangle\}$. This set can be divided into two single subsets $\varepsilon_1 = \{|a_1\rangle, |a_2\rangle\}$ and $\varepsilon_2 = \{|a_3\rangle\}$ which are orthogonal and each subset cannot be split further. We call this partition the direct sum decomposition and denote it as $\varepsilon = \varepsilon_1 \oplus \varepsilon_2$. A single set means that the set cannot be decomposed into such direct sums. If all the subsets are single sets in a direct sum decomposition, we say that the decomposition is a single set decomposition. It can verified that the single set decomposition of a non-single set is unique. For a single set, adding some states in the vector space spanned by itself will keep the set a single one. Nevertheless, taking away some states from a single set, the set could

become a non-single one. In the following, by a set of states' decomposition we mean the single set decomposition.

Lemma For a set of states $\varepsilon = \{|a_i\rangle\}$, $m = \dim(\mathrm{span}\{|a_i\rangle\})$, the following statements are equivalent: (a) ε is a single set. (b) There are m linear independent states $\{|a_{i_k}\rangle\}_{k=1}^{m}$ in ε satisfying the following relations:

$$\begin{aligned} 0 &< N(|a_{i_1}\rangle,|a_{i_2}\rangle) < N(|a_{i_1}\rangle,|a_{i_2}\rangle,|a_{i_3}\rangle) \\ &< \ldots < N(|a_{i_1}\rangle,|a_{i_2}\rangle,\ldots,|a_{i_m}\rangle). \end{aligned} \tag{2}$$

(c) A nondestructive projective measurement, a measurement which keeps the quantum state unchanged[18], can do nothing to distinguish the states in ε.

See Methods for the proof of the Lemma. From the Lemma we have

Theorem 2 For a complete set of $m \otimes n$ POPS, $\varepsilon = \{|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle\}$ with $\langle\psi_i|\psi_j\rangle = 0$, $\forall i \neq j$, the set ε cannot be completely locally distinguished if and only if there exist subsets $\{|\psi'_i\rangle = |a'_i\rangle \otimes |b'_i\rangle\} \subseteq \varepsilon$, such that $\{|a'_i\rangle\}$ and $\{|b'_i\rangle\}$ are all single sets, i.e., there exist $m' = \dim(\mathrm{span}\{|a'_i\rangle\})$ linear independent $\{|a_{i_k}\rangle\}_{k=1}^{m'}$ in $\{|a'_i\rangle\}$ and $n' = \dim(\mathrm{span}\{|b'_i\rangle\})$ linear independent $\{|b_{j_l}\rangle\}_{l=1}^{n'}$ in $\{|b'_i\rangle\}$ satisfying

$$\begin{aligned} 0 &< N(|a_{i_1}\rangle,|a_{i_2}\rangle) < N(|a_{i_1}\rangle,|a_{i_2}\rangle,|a_{i_3}\rangle) \\ &< \ldots < N(|a_{i_1}\rangle,|a_{i_2}\rangle,\ldots,|a_{i_{m'}}\rangle), \\ 0 &< N(|b_{j_1}\rangle,|b_{j_2}\rangle) < N(|b_{j_1}\rangle,|b_{j_2}\rangle,|b_{j_3}\rangle) \\ &< \ldots < N(|b_{j_1}\rangle,|b_{j_2}\rangle,\ldots,|b_{j_{n'}}\rangle). \end{aligned} \tag{3}$$

Proof. Recall that a complete set of POPS can be locally distinguished if and only if the states can be distinguished by local nondestructive projective measurement and classical communication[18]. If a set of states in ε cannot be completely locally distinguished by local nondestructive projective measurement and classical communication, there must exist a subset $\{|\psi'_i\rangle = |a'_i\rangle \otimes |b'_i\rangle\}$ of ε such that $\{|a'_i\rangle\}$ and $\{|b'_i\rangle\}$ are all single sets (Lemma 1). Obviously, the converse is also right. From Lemma 1 we have that the formula (3) holds if and only if $\{|a'_i\rangle\}$ and $\{|b'_i\rangle\}$ are single sets. □

From the view of accessible information, the more quantum an ensemble is, the less information one can get from the ensemble[1,15]. Hence the quantumness of the two parts of a complete set of POPS must be "large" enough, at least larger than $N(\{|a_{i_k}\rangle\})$ and $N(\{|b_{j_l}\rangle\})$, so that one can only get limited information and the states in the set cannot be locally distinguished. Therefore the local quantumness of an ensemble determines the local indistinguishability.

Theorem 2 gives a constructive distinguishing procedure to judge the local distinguishability for a complete set of POPS. Let $\{|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle\}$ be a complete set of POPS, corresponding to two sets $\varepsilon^A = \{|a_i\rangle\}$ and $\varepsilon^B = \{|b_i\rangle\}$. To verify the inequality (3), one needs to find all the subsets involved. This can be done in the following way.

(i) Decompose the sets ε^A and ε^B into subsets, $\varepsilon^A = \varepsilon_1^A \oplus \varepsilon_2^A \oplus \ldots$, $\varepsilon^B = \varepsilon_1^B \oplus \varepsilon_2^B \oplus \cdots$ with the states in each subset constituting a single set. This process employs the corresponding local measurement $M^A = 1P_1^A \oplus 2P_2^A \oplus \ldots$ and $M^B = 1P_1^B \oplus 2P_2^B \oplus \ldots$, where $P_1^A, P_2^A, P_1^B, P_2^B, \ldots$ is the projections to the spaces spanned by $\varepsilon_1^A, \varepsilon_2^A, \varepsilon_1^B, \varepsilon_2^B, \ldots$ respectively.

(ii) Find the overlapped states between these subsets, $\{|\psi_s\rangle\}_{ij} = \varepsilon_i^A \widetilde{\cap} \varepsilon_j^B$, where $\widetilde{\cap}$ means to find the states with the same subscripts by classical communication. For example, if $\varepsilon_1^A = \{|a_1\rangle, |a_2\rangle, |a_3\rangle\}$, $\varepsilon_1^B = \{|b_2\rangle, |b_3\rangle, |b_4\rangle\}$, then $\varepsilon_1^A \widetilde{\cap} \varepsilon_1^B = \{|\psi_2\rangle, |\psi_3\rangle\}_{11}$. Each $\{|\psi_s\rangle = |a_s\rangle \otimes |b_s\rangle\}_{ij}$ corresponds to two new subsets $\varepsilon^{A_{ij}} = \{|a_s\rangle\}$ and $\varepsilon^{B_{ij}} = \{|b_s\rangle\}$.

We repeat the above process n rounds for the new subsets until each of those new subsets has only one element or both A and B parts cannot be decomposed further. At last we have subset $\{|\psi_k\rangle = |a_k\rangle \otimes |b_k\rangle\}_{st,\ldots,ij}$ (here $st, \ldots, ij$ are the measurement outcomes) corresponding to two new sets $\varepsilon^{A_{st,\ldots,ij}} = \{|a_k\rangle\}$ and $\varepsilon^{B_{st,\ldots,ij}} = \{|b_k\rangle\}$, where both $\varepsilon^{A_{st,\ldots,ij}}$ and $\varepsilon^{B_{st,\ldots,ij}}$ are single sets. If all the final single subsets have one element, the set $\{|\psi_i\rangle\}$ can be locally distinguished.

As an example, there is a complete set of POPS for $3 \otimes 4$ system,

$$\begin{aligned} |\psi_1\rangle &= |1\rangle|1\rangle, & |\psi_{8,9}\rangle &= |0 \pm 1\rangle|2\rangle/\sqrt{2}, \\ |\psi_{2,3}\rangle &= |0\rangle|0 \pm 1\rangle/\sqrt{2}, & |\psi_{10}\rangle &= |0\rangle|3\rangle, \\ |\psi_{4,5}\rangle &= |2\rangle|1 \pm 2\rangle/\sqrt{2}, & |\psi_{11}\rangle &= |1\rangle|3\rangle, \\ |\psi_{6,7}\rangle &= |1 \pm 2\rangle|0\rangle/\sqrt{2}, & |\psi_{12}\rangle &= |2\rangle|3\rangle, \end{aligned} \tag{4}$$

which corresponds to two sets, $\varepsilon^A = \{|a_1\rangle = |1\rangle, |a_{2,3}\rangle = |0\rangle, |a_{4,5}\rangle = |2\rangle, |a_6\rangle = \frac{1}{\sqrt{2}}|1+2\rangle, |a_7\rangle = \frac{1}{\sqrt{2}}|1-2\rangle, |a_8\rangle = \frac{1}{\sqrt{2}}|0+1\rangle, |a_9\rangle = \frac{1}{\sqrt{2}}|0-1\rangle, |a_{10}\rangle = |0\rangle, |a_{11}\rangle = |1\rangle, |a_{12}\rangle = |2\rangle\}$ and $\varepsilon^B = \{|b_1\rangle = |1\rangle, |b_2\rangle = \frac{1}{\sqrt{2}}|0+1\rangle, |b_3\rangle = \frac{1}{\sqrt{2}}|0-1\rangle, |b_4\rangle = \frac{1}{\sqrt{2}}|1+2\rangle, |b_5\rangle = \frac{1}{\sqrt{2}}|1-2\rangle, |b_{6,7}\rangle = |0\rangle, |b_{8,9}\rangle = |2\rangle, |b_{10,11,12}\rangle = |3\rangle\}$. The distinguishing process is as follows.

Round 1: (i) There are $3 = \dim(\mathrm{span}\,\varepsilon^A)$ linear independent states in ε^A satisfying $0 < N(|a_1\rangle,|a_6\rangle) = 1 < N(|a_1\rangle,|a_6\rangle,|a_8\rangle) \doteq 2.87$. So ε^A is a single set. Hence the first measurement should not be applied to A side. We denote $\varepsilon^A = \varepsilon_0^A$ (here 0 means to do no measurement). For B side, we have decomposition $\varepsilon^B = \varepsilon_1^B \oplus \varepsilon_2^B$, where $\varepsilon_1^B = \{|b_1\rangle, \ldots, |b_9\rangle\}$ and $\varepsilon_2^B = \{|b_{10}\rangle, |b_{11}\rangle, |b_{12}\rangle\}$ are all single sets. Hence ε_1^B is a single set as there are $3 = \dim(\mathrm{span}\,\varepsilon_1^B)$ linear independent states satisfying $0 < N(|b_1\rangle,|b_2\rangle) = 1 < N(|b_1\rangle,|b_2\rangle,|b_4\rangle) \doteq 2.87$. This decomposition employs measurement $M^B = 1(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|) + 2|3\rangle\langle 3|$ to distinguish ε_1^B from ε_2^B.

(ii) Find the overlapped states by classical communication, $\varepsilon_0^A \widetilde{\cap} \varepsilon_1^B = \{|\psi_1\rangle, \ldots, |\psi_9\rangle\}_{01}$, $\varepsilon_0^A \widetilde{\cap} \varepsilon_2^B = \{|\psi_{10}\rangle, |\psi_{11}\rangle, |\psi_{12}\rangle\}_{02}$. They correspond to four new sets $\varepsilon^{A_{01}} = \{|a_1\rangle, \ldots, |a_9\rangle\}$, $\varepsilon^{B_{01}} = \{|b_1\rangle, \ldots |b_9\rangle\}$, $\varepsilon^{A_{02}} = \{|a_{10}\rangle, |a_{11}\rangle, |a_{12}\rangle\}$, $\varepsilon^{B_{02}} = \{|b_{10}\rangle, |b_{11}\rangle, |b_{12}\rangle\}$.

Round 2: (i) Do decomposition for the above four new sets. Note $\varepsilon^{A_{01}}$, $\varepsilon^{B_{01}}$ are all single sets (the states $|a_4\rangle$, $|a_6\rangle$, $|a_8\rangle$ in $\varepsilon^{A_{2,01}}$ are linear independent and satisfy $0 < N(|a_4\rangle,|a_6\rangle) = 1 < N(|a_4\rangle,|a_6\rangle,|a_8\rangle) \doteq 1.87$, and $\varepsilon^{B_{01}} = \varepsilon_1^B$). Therefore the set $\{|\psi_1\rangle, \ldots, |\psi_9\rangle\}_{01}$ is the subset described in Theorem 2. In fact they are the nine locally indistinguishable states in[9]. But we can distinguish the set $\{|\psi_{10}\rangle, |\psi_{11}\rangle, |\psi_{12}\rangle\}_{02}$ further since we have decomposition $\varepsilon^{A_{02}} = \varepsilon_1^{A_{02}} \oplus \varepsilon_2^{A_{02}} \oplus \varepsilon_3^{A_{02}}$, where $\varepsilon_1^{A_{02}} = \{|a_{10}\rangle\}$, $\varepsilon_2^{A_{02}} = \{|a_{11}\rangle\}$, $\varepsilon_3^{A_{02}} = \{|a_{12}\rangle\}$. This employs measurement $M^A = 1|0\rangle\langle 0| + 2|1\rangle\langle 1| + 3|2\rangle\langle 2|$. However, $\varepsilon^{B_{02}}$ is single, denote $\varepsilon^{B_{02}} = \varepsilon_0^{B_{02}}$.

(ii) Find overlapped states by classical communication, $\varepsilon_1^{A_{02}} \widetilde{\cap} \varepsilon_0^{B_{02}} = \{|\psi_{10}\rangle\}_{10,02}$, $\varepsilon_2^{A_{02}} \widetilde{\cap} \varepsilon_0^{B_{02}} = \{|\psi_{11}\rangle\}_{20,02}$, $\varepsilon_3^{A_{02}} \widetilde{\cap} \varepsilon_0^{B_{02}} = \{|\psi_{12}\rangle\}_{30,02}$. All the above new subsets either have one element each or both sides are single ones.

Finally we can divide the set (4) into four parts, $\{|\psi_1\rangle, \ldots, |\psi_9\rangle\}_{01}$, $\{|\psi_{10}\rangle\}_{10,02}$, $\{|\psi_{11}\rangle\}_{20,02}$, $\{|\psi_{12}\rangle\}_{30,02}$, and the set cannot be completely distinguished due to the subset $\{|\psi_1\rangle, \ldots, |\psi_9\rangle\}_{01}$.

The quantumness of semi-classical states. The non-commutativity defined by (1) can be also used to describe the quantumness for bipartite semi-classical states. For a given semi-classical state, $\rho_{qc} = \sum_i p_i \rho_i \otimes |i\rangle\langle i|$, the corresponding ensemble $\varepsilon = \{p_i, \rho_i\}$ is fixed (see Methods). Denote $X_i = p_i \rho_i$. We have the non-commutativity describing the quantumness for the state ρ_{qc},

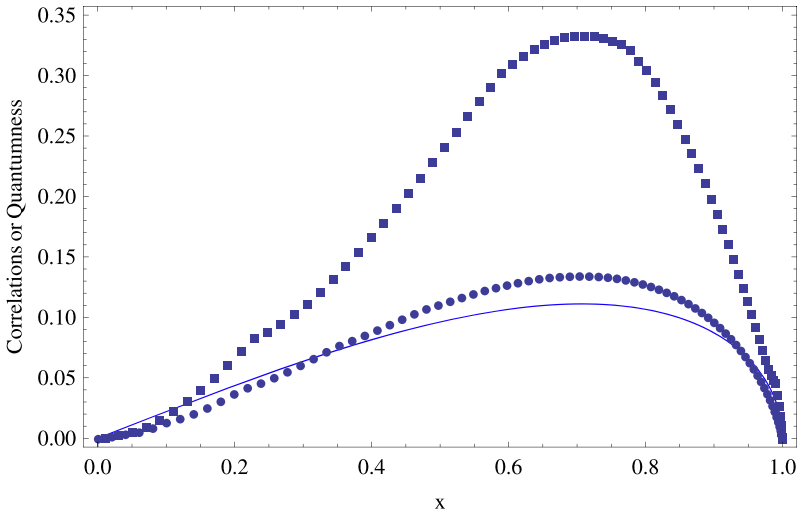

Figure 1 | The comparison between the quantum correlations and the ensemble quantumness for a 3 ⊗ 3 quantum-classical state $\rho_x = 1/3(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| + |\phi_2\rangle\langle\phi_2| \otimes |2\rangle\langle 2|)$, where $|\phi_2\rangle = \cos\theta|0\rangle + \sin\theta|2\rangle$ and horizontal ordinate is the overlap $x = |\langle 0|\phi_2\rangle| = |\cos\theta|$. Quantum correlations, quantum discord (circle doted line) and quantum deficit (square dotted line), and the ensemble quantumness, non-commutativity (solid line), for ρ_x all get minimal at $x = 0$, 1 while get maximal at $x = 1/\sqrt{2}$.

$$N\left(\rho_{qc}\right) = \sum_{i>j} \left\| \left[X_i, X_j\right] \right\|. \tag{5}$$

It is easy to check that $N(\rho_{qc})$ satisfies the following properties, which actually makes it a candidate for quantum-correlation measures for semi-classical states[4]: (a) it is positive, (b) it is zero for classical-classical correlated states, (c) it is invariance under local-unitary transformations, and (d) it is non-increasing when an ancillary system is introduced. This quantity $N(\rho_{qc})$ describes the quantumness of semi-classical states. It is different from those quantum correlation measures, such as quantum discord, quantum deficit, etc., which are based on the measurements and their estimations involve extremely complicated optimization process. Interestingly, while the quantity $N(\rho_{qc})$ can be easily computed, it shows similar behavior to other quantum correlation measures for semi-classical states. Hence, instead of those quantum correlation measures, one can use the non-commutativity to characterize the quantum correlations of semi-classical states ρ_{qc}. Moreover, non-commutativity provides a tool to explore the relation between the ensemble quantumness and those quantum correlation measures. Fig. 1 shows the comparison between quantum correlations and ensemble quantumness (non-commutativity) for a 3 ⊗ 3 system for which it is extremely difficult to calculate quantum correlations analytically.

Discussion

We have proposed non-commutativity as a quantumness measure for an ensemble. It has been shown that the local ensemble quantumness, instead of quantum correlation measure, like quantum discord, quantum deficit, etc., which is a function of a density operator, accounts for the local indistinguishability for a complete set of POPS. It implies that the quantumness of local ensembles must satisfy certain conditions so that the states in the ensemble cannot be locally distinguished.

A constructive distinguishing procedure to obtain the concrete local measurements and classical communications has been presented to judge the local indistinguishability for a complete set of POPS. Our approach to judge the local indistinguishability can also be directly extended to distinguish a complete set of multipartite POPS or a non-complete set of POPS, when the local operations are restricted within nondestructive projective measurements.

Due to that one semi-classical state corresponds to one quantum ensemble, the non-commutativity has been shown to be able to characterize the ensemble quantumness for classical-quantum or quantum-classical systems.

Methods

Proof of the property (2) of the non-commutativity *N*. Consider two pure n dimensional states $A = |\phi\rangle\langle\phi|$ and $B = |\psi\rangle\langle\psi|$. Denote $\langle\phi|\psi\rangle = xe^{i\theta}$ with $x \in [0, 1]$, $\theta \in [0, 2\pi)$. Then $[A, B] = xe^{i\theta}|\phi\rangle\langle\psi| - xe^{-i\theta}|\psi\rangle\langle\phi|$. Under the base $\{|\phi\rangle = |\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{n-1}\rangle\}$, one gets $|\phi\rangle\langle\psi| = \sum_{s=0}^{n-1} \langle\psi|\ \phi_s\rangle|\phi_0\rangle\langle\phi_s|$. $[A, B]$ can then be expressed as

$$\begin{pmatrix} 0 & \psi_{0,1} & \cdots & \psi_{0,n-1} \\ -\psi_{0,1}^* & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ -\psi_{0,n-1}^* & 0 & \cdots & 0 \end{pmatrix} \tag{6}$$

where $\psi_{i,j} = \langle\phi_i|\psi\rangle\langle\psi|\phi_j\rangle$ and $\psi_{i,j}^*$ is the conjugate of $\psi_{i,j}$. The eigenvalues of the above matrix are $\left\{\sqrt{-Z}, -\sqrt{-Z}, 0, \ldots, 0\right\}$, where $Z = \left|\psi_{0,1}\right|^2 + \ldots + \left|\psi_{0,n-1}\right|^2 = \sum_{j=0}^{n-1} \left|\psi_{0,j}\right|^2 - \left|\psi_{0,0}\right|^2 = x^2 - x^4$. One gets $\|[A,B]\| = 2\left|\sqrt{-Z}\right| = 2x\sqrt{1-x^2}$. Therefore for two pure states $|\psi\rangle$ and $|\phi\rangle$, $\|[|\phi\rangle, |\psi\rangle]\|$ is 0 when $|\langle\phi|\psi\rangle| = 0$ or 1, and 1 when $|\langle\phi \mid \psi\rangle| = 1/\sqrt{2}$.

Proof of Lemma 1. (a) ⇒ (b) First choose any vector in ε, say, $|a_{i_1}\rangle$. Then choose the second vector $|a_{i_2}\rangle$ in ε such that it is not equal to or orthogonal to $|a_{i_1}\rangle$, i.e., $N(|a_{i_1}\rangle, |a_{i_2}\rangle) > 0$. The existence of $|a_{i_2}\rangle$ is guaranteed by the fact that ε is a single set. Next choose the third vector $|a_{i_3}\rangle$ in ε such that it is independent of $\{|a_{i_1}\rangle, |a_{i_2}\rangle\}$, and also not orthogonal to $\{|a_{i_1}\rangle, |a_{i_2}\rangle\}$, i.e., $N(|a_{i_1}\rangle, |a_{i_2}\rangle) < N(|a_{i_1}\rangle, |a_{i_2}\rangle, |a_{i_3}\rangle)$. Or else, if $|a_{i_3}\rangle$ does not exist, then ε can be direct sum decomposed into two parts. Continuing with the above process, we can finally get m linear independent states $\{|a_k\rangle\}_{k=1}^m$ in ε satisfying inequality (2).

(b) ⇒ (c) A nondestructive projective measurement is described by an observable, M, an Hermitian operator such that all $|a_i\rangle$ in ε are the eigenvectors of M. If $N(|a_{i_1}\rangle, |a_{i_2}\rangle) > 0$, $|a_{i_1}\rangle$ and $|a_{i_2}\rangle$ are neither identical nor orthogonal. Hence the corresponding eigenvalues of $|a_{i_1}\rangle$ and $|a_{i_2}\rangle$ must be equal, since the eigenvectors corresponding to different eigenvalues are orthogonal. If $N(|a_{i_1}\rangle, |a_{i_2}\rangle) < N(|a_{i_1}\rangle, |a_{i_2}\rangle, |a_{i_3}\rangle)$, $|a_{i_3}\rangle$ is at least not orthogonal to one of $|a_{i_1}\rangle$ and $|a_{i_2}\rangle$. For instance, suppose $N(|a_{i_1}\rangle, |a_{i_3}\rangle) > 0$, then the eigenvalues corresponding to $|a_{i_1}\rangle$ and $|a_{i_3}\rangle$ are equal. Therefore we have that if (2) is satisfied, those m linear independent $|a_{i_k}\rangle$s have the same eigenvalues of M. Therefore M becomes an identity (apart of real factor) and it cannot be used to distinguish the states in ε.

(c) ⇒ (a) Suppose the set is not a single one and has a decomposition $\varepsilon = \varepsilon_1 \oplus \varepsilon_2$. Then one can use a corresponding nondestructive projective measurement $M = aI_1 \oplus bI_2$, where $a \neq b$, I_1, I_2 are identity operators, to distinguish the states in ε_1 from ε_2.

Hence if M cannot do any in distinguishing the states in ε, ε must be a single set, that is, statement (a) holds.

The unique expression of semi-classical states. Let $\rho=\sum_i p_i\rho_i\otimes|\alpha_i\rangle\langle\alpha_i|$ be an arbitrary given semi-classical state, where $\{|\alpha_i\rangle\}$ is an orthogonal base. Suppose there exists another orthogonal base $\{|\beta_i\rangle\}$ such that $\rho=\sigma$, where $\sigma=\sum_i q_i\sigma_i|\beta_i\rangle\langle\beta_i|$. Let $U=\sum_i|\beta_i\rangle\langle\alpha_i|$ be the unitary operator such that $U|\alpha_i\rangle=|\beta_i\rangle$, $(U)_{ij}=u_{ij}=\langle\alpha_i|\beta_j\rangle$, $|\beta_i\rangle=\sum_s^i u_{si}|\alpha_s\rangle$. So σ can be reexpressed as $\sum_{st}\left(\sum_i q_i\sigma_i u_{si}u_{ti}^*\right)\otimes|\alpha_s\rangle\langle\alpha_t|$. Let $\tilde{q}_{kl}^i$ be the entries of $q_i\sigma_i$. Set $Q_{kl}=\sum_i\tilde{q}_{kl}^i|\beta_i\rangle\langle\beta_i|$. Then $\rho=\sigma$ implies that

$$\begin{aligned}0&=\sum_i\tilde{q}_{kl}^i u_{si}u_{ti}^*=\sum_i\tilde{q}_{kl}^i\langle\alpha_s|\beta_i\rangle\langle\alpha_t|\beta_i\rangle^*\\&=\langle\alpha_s|\left(\sum_i\tilde{q}_{kl}^i|\beta_i\rangle\langle\beta_i|\right)|\alpha_t\rangle=\langle\alpha_s|Q_{kl}|\alpha_t\rangle,\end{aligned}\tag{7}$$

for $s\neq t$, which means that both $\{|\alpha_i\rangle\}$ and $\{|\beta_i\rangle\}$ are the eigenvectors of Q_{kl}, and $\tilde{q}_{kl}^i$ are the corresponding eigenvalues. Note that the set $\{q_i\sigma_i\}$ of state σ can be divided into degenerate part (in which all the states are identical) and non-degenerate part (in which all the states are mutually different). For non-degenerate part, taking over all k, l, one will find that the intersection of the eigenspaces belonging to the eigenvalues $\tilde{q}_{kl}^i$ must be one dimensional, namely, $|\alpha_i\rangle=|\beta_i\rangle$ and then $p_i\rho_i=q_i\sigma_i$. For degenerate part, without loss of generality, assume $q_1\sigma_1=q_2\sigma_2$, then $\rho=\sigma$ means $p_1\rho_1\otimes|\alpha_1\rangle\langle\alpha_1|+p_2\rho_2\otimes|\alpha_2\rangle\langle\alpha_2|=q_1\sigma_1\otimes(|\beta_1\rangle\langle\beta_1|+|\beta_2\rangle\langle\beta_2|)$. Therefore $p_1\rho_1=p_2\rho_2=q_1\sigma_1=q_2\sigma_2$. Finally we get $p_i\rho_i=q_i\sigma_i$, $\forall i$.

1. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
2. Knill, E. & Laflamme, R. Power of One Bit of Quantum Information. *Phys. Rev. Lett.* **81**, 5672 (1998).
3. Ollivier, H. & Zurek, W. H. Quantum Discord: A Measure of the Quantumness of Correlations. *Phys. Rev. Lett.* **88**, 017901 (2001).
4. Modi, K., Brodutch, A., Cable, H., Paterek, T. & Verdral, V. The classical-quantum boundary for correlations: Discord and related measures. *Rev. Mod. Phys.* **84**, 1655 (2012).
5. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).
6. Bergou, J. A., Herzog, U. & Hillery, M. Quantum Filtering and Discrimination between Sets of Boolean Functions. *Phys. Rev. Lett.* **90**, 257901 (2003).
7. Raimond, J. M., Brune, M. & Haroche, S. Manipulating quantum entanglement with atoms and photons in a cavity. *Rev. Mod. Phys.* **73**, 565 (2001).
8. Haroche, S. Nobel Lecture: Controlling photons in a box and exploring the quantum to classical boundary. *Rev. Mod. Phys.* **85**, 1083 (2013).
9. Bennett, C. H. *et al.* Quantum nonlocality without entanglement. *Phys. Rev. A* **59**, 1070 (1999).
10. Brodutch, A. & Terno, D. R. Quantum discord, local operations, and Maxwells demons. *Phys. Rev. A* **81**, 062103 (2010).
11. Bennett, C. H. *et al.* Unextendible Product Bases and Bound Entanglement. *Phys. Rev. Lett.* **82**, 5385 (1999).
12. Walgate, J., Short, A. J., Hardy, L. & Vedral, V. Vacuum-Stimulated Raman Scattering Based on Adiabatic Passage in a High-Finesse Optical Cavity. *Phys. Rev. Lett.* **85**, 4872 (2000).
13. Walgate, J. & Hardy, L. Nonlocality, Asymmetry, and Distinguishing Bipartite States. *Phys. Rev. Lett.* **89**, 147901 (2002).
14. Ghosh, S., Kar, G., Roy, A., Sen(De), A. & Sen, U. Distinguishability of Bell States. *Phys. Rev. Lett.* **87**, 277902 (2001).
15. Fuchs, C. A. Just two nonothogonal quantum states. *Quantum Communication, Computing, and Measurement* **2**, 11–16 (Springer Press, 2002).
16. Kleinmann, M. Asymptotically perfect discrimination in the LOCC paradigm. *Phys. Rev. A* **84**, 042326 (2011).
17. Childs, A., Leung, D., Mancinska, L. & Ozols, M. A framework for bounding nonlocality of state discrimination. *Commun. Math. Phys.* **323**, 1121–1153 (2013).
18. Chen, P. X. & Li, C. Z. Distinguishing the elements of a full product basis set needs only projective measurements and classical communication. *Phys. Rev. A* **70**, 022306 (2004).

Acknowledgments

The work is supported by NSFC under number 11275131 and 11401032. The authors thank X.N. Zhu, Z.X. Wang, and W.P. Yang for useful discussions.

Author contributions

T.M., M.Z., Y.W. and S.M. wrote the main manuscript text. All authors reviewed the manuscript.

Additional information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Ma, T., Zhao, M.-J., Wang, Y.-K. & Fei, S.-M. Non-commutativity and Local Indistinguishability of Quantum States. *Sci. Rep.* **4**, 6336; DOI:10.1038/srep06336 (2014).