PAPER • OPEN ACCESS

Computing quantum discord is NP-complete

To cite this article: Yichen Huang 2014 *New J. Phys.* **16** 033027

New Journal of Physics
The open access journal at the forefront of physics
Deutsche Physikalische Gesellschaft DPG | IOP Institute of Physics

Computing quantum discord is NP-complete

Yichen Huang
Department of Physics, University of California, Berkeley, CA 94720, USA
E-mail: yichenhuang@berkeley.edu

Received 4 September 2013, revised 3 February 2014
Accepted for publication 11 February 2014
Published 21 March 2014
New Journal of Physics **16** (2014) 033027
doi:10.1088/1367-2630/16/3/033027

Abstract
We study the computational complexity of quantum discord (a measure of quantum correlation beyond entanglement), and prove that computing quantum discord is NP-complete. Therefore, quantum discord is computationally intractable: the running time of any algorithm for computing quantum discord is believed to grow exponentially with the dimension of the Hilbert space so that computing quantum discord in a quantum system of moderate size is not possible in practice. As by-products, some entanglement measures (namely entanglement cost, entanglement of formation, relative entropy of entanglement, squashed entanglement, classical squashed entanglement, conditional entanglement of mutual information, and broadcast regularization of mutual information) and constrained Holevo capacity are NP-hard/NP-complete to compute. These complexity-theoretic results are directly applicable in common randomness distillation, quantum state merging, entanglement distillation, superdense coding, and quantum teleportation; they may offer significant insights into quantum information processing. Moreover, we prove the NP-completeness of two typical problems: linear optimization over classical states and detecting classical states in a convex set, providing evidence that working with classical states is generically computationally intractable.

Keywords: entanglement measures, quantum discord, quantum mechanics, channel capacity, computational complexity

1. Introduction

Quite a few fundamental concepts in quantum mechanics do not have classical analogs: uncertainty relations [6, 11, 45, 46, 72], quantum nonlocality [19, 29, 42, 70], etc. Quantum entanglement [42, 70], defined based on the notion of local operations and classical communication (LOCC), is the most prominent manifestation of quantum correlation. It is a resource in quantum information processing, enabling tasks such as superdense coding [10], quantum teleportation [8] and quantum state merging [39, 40]. Various entanglement measures [42, 70] are reported to quantify entanglement. However, nontrivial quantum correlation also exists in certain separable (not entangled) states. For instance, deterministic quantum computation with one qubit (DQC1) [53] is a model of mixed-state quantum computation with little entanglement. It is argued [23] that quantum discord [37, 66] (a measure of quantum correlation beyond entanglement; see section 3 for its definition) is responsible for the quantum speed-up over classical algorithms. Quantum discord is also a useful concept in common randomness distillation [24], quantum state merging [15, 59, 60], entanglement distillation [60, 77], superdense coding [60], quantum teleportation [60], etc, and has established quantum discord (and related measures of quantum correlation) as an active research topic over the past few years [63]. Nevertheless, computing quantum discord is difficult. Despite considerable effort, few analytical results are known even for 'simple' and useful states (e.g. two-qubit X states [5, 17, 27, 48, 49, 57, 73]). Generally, quantum discord can only be computed numerically.

The notion of NP-completeness [20] is fundamental and remarkable in computational complexity theory. NP-complete problems are the hardest in NP in the sense that an efficient algorithm for any NP-complete problem implies efficient algorithms for all problems in NP, and NP-hard problems are at least as hard as NP-complete problems. An NP-hard/NP-complete problem is computationally intractable: the running time of any algorithm for the problem is believed to grow exponentially with the input size. The NP-completeness of the separability problem (detecting whether a given state is separable) was first proved in [33, 34]; see [30, 52] for technical improvements. This may be the reason why a lot of effort is devoted to entanglement criteria [28, 32, 41, 42, 44, 47, 67, 76], which are simple sufficient conditions for entanglement. The classicality problem (detecting whether a given state has zero quantum discord) can be solved in polynomial time [16, 21, 43], but the computational complexity of quantum discord is not known.

Here we prove that computing quantum discord is NP-complete (theorem 2). Therefore, the running time of any algorithm for computing quantum discord is believed to grow exponentially with the dimension of the Hilbert space, so that computing quantum discord in a quantum system of moderate size is not possible in practice. As by-products, some entanglement measures (namely entanglement cost [9], entanglement of formation [9], relative entropy of entanglement [81], squashed entanglement [18], classical squashed entanglement, conditional entanglement of mutual information [86], and broadcast regularization of mutual information [69]; theorem 1) and constrained Holevo capacity [75] (corollary 1) are NP-hard/NP-complete to compute. As direct applications (one-way), distillable common randomness, regularized one-way classical deficit, entanglement consumption in extended quantum state merging, and minimum loss due to decoherence of the yield of a family of protocols are also NP-hard/NP-complete to compute; such complexity-theoretic results may offer significant insights into quantum information processing. Moreover, we prove the NP-completeness of the

following two typical problems: linear optimization over classical states (proposition 1) and detecting whether there are classical states in a given convex set (proposition 2). The former is the simplest optimization problem over classical states, and the latter is just one step further than the classicality problem. Conceptually, the NP-completeness of these two problems provides evidence that working with classical states is generically computationally intractable. We conclude with some interesting open problems and research directions.

2. NP-hardness/NP-completeness of computing entanglement measures

Let us briefly recall the definitions of some entanglement measures (see the review papers [42, 70] for details). Entanglement cost $E_C(\rho)$ [9] is the minimum rate j/k to convert j copies of the two-qubit maximally entangled state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ to k copies of the bipartite state ρ by LOCC with vanishing error in the asymptotic limit $j, k \to +\infty$. Conversely, distillable entanglement $E_D(\rho)$ [9] is the maximum rate j/k to convert $\rho^{\otimes k}$ to $|\psi\rangle^{\otimes j}$ by LOCC with vanishing error in the asymptotic limit. Entanglement of formation [9] is defined as

$$E_F(\rho_{AB}) = \inf_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\rho_A^i), \tag{1}$$

where the infimum is taken over all ensembles of pure states $\{p_i, \left|\psi_i\right\rangle\}$ satisfying $\rho_{AB} = \sum_i p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|$, and

$$S(\rho_A^i) = -\mathrm{tr}\,(\rho_A^i \log \rho_A^i) \tag{2}$$

is the von Neumann entropy of the reduced density matrix $\rho_A^i = \mathrm{tr}_B \left|\psi_i\right\rangle\left\langle\psi_i\right|$ or the entanglement entropy of $\left|\psi_i\right\rangle$. The relative entropy of entanglement [81]

$$E_R(\rho) = \inf_{\sigma\in\mathcal{S}} S(\rho\,\|\,\sigma) = \inf_{\sigma\in\mathcal{S}} \mathrm{tr}\,(\rho\log\rho - \rho\log\sigma) \tag{3}$$

quantifies the distance from the state ρ to the set $\mathcal{S}$ of all separable states, where $S(\rho\|\sigma)$ is the quantum relative entropy. The regularized relative entropy of entanglement is given by

$$E_R^\infty(\rho) = \lim_{k\to+\infty} E_R(\rho^{\otimes k})/k. \tag{4}$$

Squashed entanglement [18] is defined as

$$E_{sq}(\rho_{AB}) = \frac{1}{2}\inf_{\rho_{ABC}} \{S(\rho_{AC}) + S(\rho_{BC}) - S(\rho_C) - S(\rho_{ABC})\}, \tag{5}$$

where the infimum is taken over all states ρ_{ABC} in an extended Hilbert space satisfying $\rho_{AB} = \mathrm{tr}_C\rho_{ABC}$, and $\rho_{AC} = \mathrm{tr}_B\rho_{ABC}$, etc. Classical squashed entanglement $E_{sq}^C(\rho_{AB})$ is given by (5) where the infimum is taken with the additional restriction that $\rho_{AB|C}$ is quantum-classical (23) across the cut $AB|C$. Conditional entanglement of mutual information [86] is defined as

$$E_I(\rho_{AB}) = \frac{1}{2}\inf_{\rho_{AA'BB'}} \{I(\rho_{AA'|BB'}) - I(\rho_{A'B'})\}, \tag{6}$$

where the infimum is taken over all states $\rho_{AA'BB'}$ satisfying $\rho_{AB} = \mathrm{tr}_{A'B'}\rho_{AA'BB'}$, and

$$I(\rho_{A'B'}) = S(\rho_{A'}) + S(\rho_{B'}) - S(\rho_{A'B'}) \tag{7}$$

is the quantum mutual information. A state $\rho_{X^{\otimes k}}$ with $X^{\otimes k} = \bigotimes_{i=1}^{k} X_i$ is a k-copy broadcast state of ρ_X if $\rho_X = \mathrm{tr}_{X_1X_2\cdots X_{i-1}X_{i+1}\cdots X_k}\rho_{X^{\otimes k}}$ for any $i = 1, 2, \ldots, k$. Broadcast regularization of mutual information [69] is given by

$$I_b^{\infty}(\rho_{AB}) = \frac{1}{2}\lim_{k\to+\infty}\inf_{\rho_{A^{\otimes k}|B^{\otimes k}}} I(\rho_{A^{\otimes k}|B^{\otimes k}})/k, \tag{8}$$

where the infimum is taken over all k-copy broadcast states of ρ_{AB}.

Lemma 1. *(a) The definition (1) of E_F remains the same if the number of states in the ensemble is restricted to be less than or equal to m^2n^2 [64, 78], where $m \times n$ is the dimension of the bipartite state ρ_{AB}.*

(b) $E_C(\rho) = E_F^{\infty}(\rho) = \lim_{k\to+\infty} E_F(\rho^{\otimes k})/k$ [36].

(c) $E_F(\rho) \geqslant E_R(\rho)$ [80], $E_C(\rho) \geqslant E_{sq}(\rho)$ [18], $E_{sq}^{C}(\rho) \geqslant I_b^{\infty}(\rho) \geqslant E_I(\rho) \geqslant E_{sq}(\rho)$ [69].

(d) $E_R^{\infty}(\rho) \geqslant \inf_{\sigma\in\mathcal{S}} \| \rho - \sigma \|_1^2/(2mn \log 2)$ [68], $E_{sq}(\rho) \geqslant \inf_{\sigma\in\mathcal{S}} \| \rho - \sigma \|_2^2/(2448 \log 2)$ [13, 62], where $\|X\|_1 = \mathrm{tr}\sqrt{X^{\dagger}X}$ and $\|X\|_2 = \sqrt{\mathrm{tr}\, X^{\dagger}X}$ are the trace norm and the Frobenius norm, respectively.

Accounting for the finite precision of numerical computing, hereafter, every real number is assumed to be represented by a polynomial number of bits, and the formulation of each computational problem is approximate. Indeed, we will prove that the problems are computationally intractable even if small errors are allowed. We begin by recalling the following lemma.

Lemma 2 (NP-completeness of the separability problem). *Given a bipartite quantum state ρ of dimension $m \times n$ with the promise that either (Y) $\rho \in \mathcal{S}$ or (N) $\inf_{\sigma\in\mathcal{S}} \| \rho - \sigma \|_2 \geqslant \delta$, it is NP-complete to decide which is the case, where $\delta = 1/\mathrm{poly}(m, n)$ is some inverse polynomial in m, n.*

Remark 1. The NP-completeness of the separability problem with $\delta = \exp(-O(m, n))$ is proven in [52], and the NP-hardness of the separability problem with $\delta = 1/\mathrm{poly(m, n)}$ is proven in [30]. The separability problem can be solved in $\exp(O((\log m)(\log n)/\delta^2))$ time (a quasi-polynomial-time algorithm for $\delta = 1/\mathrm{poly}(\log m, \log n)$) [14].

Theorem 1 (NP-hardness/NP-completeness of computing entanglement measures). *Given a bipartite quantum state ρ of dimension $m \times n$ and a real number a with the promise that either (Y) $E_F(\rho) \leqslant a$ or (N) $E_F(\rho) \geqslant a + \varepsilon$, it is NP-complete to decide which is the case, where $\varepsilon = 1/\mathrm{poly}(m, n)$. In the same sense, computing E_R is NP-complete and computing E_C, E_R^{∞}, E_{sq}, E_{sq}^{C}, E_I, I_b^{∞} is NP-hard.*

Proof. Computing E_F, E_R is in NP: the certificates of the yes instances (Y) are the optimal ensemble of pure states $\{p_i, \left|\psi_i\right\rangle\}$ and the closest separable state σ, respectively. The NP-hardness of computing entanglement measures is totally expected, as computing entanglement measures is more difficult than just detecting entanglement. Indeed, the hardness proof is a reduction from lemma 2. Set $a = 0$ and $\varepsilon = \delta^2/(2448mn \log 2) = 1/\text{poly}(m, n)$. (Y) If ρ is separable, then

$$E_C(\rho) = E_F(\rho) = E_R(\rho) = E_R^\infty(\rho) = E_{sq}(\rho) = E_{sq}^C(\rho) = E_I(\rho) = I_b^\infty(\rho) = 0. \quad (9)$$

(N) If $\inf_{\sigma\in\mathcal{S}} \| \rho - \sigma \|_2 \geqslant \delta$, then

$$E_F(\rho) \geqslant E_R(\rho) \geqslant E_R^\infty(\rho),\ E_F(\rho) \geqslant E_C(\rho) \geqslant E_{sq}(\rho),\ E_{sq}^C(\rho) \geqslant I_b^\infty(\rho) \geqslant E_I(\rho) \geqslant E_{sq}(\rho), \quad (10)$$

$$\begin{aligned} E_R^\infty(\rho) &\geqslant \inf_{\sigma\in\mathcal{S}} \| \rho - \sigma \|_1^2/(2mn \log 2) \\ &\geqslant \inf_{\sigma\in\mathcal{S}} \| \rho - \sigma \|_2^2/(2mn \log 2) \geqslant \delta^2/(2mn \log 2) \geqslant \varepsilon, \end{aligned} \quad (11)$$

$$E_{sq}(\rho) \geqslant \inf_{\sigma\in\mathcal{S}} \| \rho - \sigma \|_2^2/(2448 \log 2) \geqslant \delta^2/(2448 \log 2) \geqslant \varepsilon. \quad (12)$$

□

Remark 2. The computational problem in theorem 1 requires a guess of $E_F(\rho)$ as an input. This formulation is reasonable: if there is an efficient subroutine for the problem, a binary search for $E_F(\rho)$ can be done by calling the subroutine $O(\log(\log(mn)/\varepsilon)) = O(\log m, \log n)$ times to achieve the precision $\varepsilon = 1/\text{poly}(m, n)$. The hardness proof does not apply to E_D, as $E_D(\rho)$ can be zero for an entangled state ρ. It is an open problem whether computing E_C, E_R^∞, E_{sq}, E_{sq}^C, E_I, I_b^∞ is in NP. For instance, it is not clear how large the dimension of ρ_{ABC} should be so that the right-hand side of (5) is optimal (or sufficiently close to optimal).

3. NP-completeness of computing quantum discord

As a measure of quantum correlation (beyond entanglement), quantum discord [66]

$$D(\rho_{AB}|B) = I(\rho_{AB}) - J(\rho_{AB}|B) \quad (13)$$

is the difference between total correlation (quantified by quantum mutual information) and classical correlation [37]

$$J(\rho_{AB}|B) = S(\rho_A) - \inf_{\{\Pi_i\}} \sum_i p_i S(\rho_A^i), \quad (14)$$

where $\{\Pi_i\}$ is a measurement on the subsystem B; $p_i = \text{tr}(\rho_{AB}\Pi_i)$ is the probability of the ith measurement outcome; and $\rho_A^i = \text{tr}_B(\rho_{AB}\Pi_i)/p_i$ is the post-measurement state. The infimum is taken over either all von Neumann measurements or all generalized measurements described by positive-operator valued measures (POVM); the corresponding notations are J_N, D_N and J_P, D_P, respectively. See [65] for an introduction to von Neumann measurements and POVM measurements. The definitions of J_P, D_P remain the same if the number of operators in the POVM is restricted to be less than or equal to n^2, where n is the dimension of the subsystem B. This is because the optimal POVM must be extremal [35], and an extremal POVM contains at

most n^2 operators [22]. Regularized classical correlation and quantum discord are given by

$$J^{\infty}(\rho_{AB}|B) = \lim_{k\to+\infty} J(\rho_{AB}^{\otimes k}|B^{\otimes k})/k,\ D^{\infty}(\rho_{AB}|B) = I(\rho_{AB}) - J^{\infty}(\rho_{AB}|B) = \lim_{k\to+\infty} D\left(\rho_{AB}^{\otimes k}|B^{\otimes k}\right)/k. \quad (15)$$

Theorem 2 (NP-completeness of computing quantum discord). *Given a bipartite quantum state ρ_{AB} of dimension $m \times n$ and a real number b with the promise that either (Y) $D_P(\rho_{AB}|B) \leqslant b$ or (N) $D_P(\rho_{AB}|B) \geqslant b + \varepsilon$, it is NP-complete to decide which is the case, where $\varepsilon = 1/\mathrm{poly}(m, n)$. In the same sense, computing D_N, $J_{N,P}$ is NP-complete and computing $D_{N,P}^{\infty}$, $J_{N,P}^{\infty}$ is NP-hard.*

Proof. Computing $D_{N,P}$ is in NP: the certificates of (Y) are the optimal measurements $\{\Pi_i\}$ on the subsystem B. The hardness proof is basically a reduction from theorem 1 via the Koashi–Winter relation [54] between E_F and D_P, and technically we derive a similar relation between E_F and D_N (note that the Koashi–Winter relation is between E_F and D_P rather than between E_F and D_N). Given a bipartite state ρ_{AB} of dimension $m \times n$, by diagonalizing ρ_{AB} we construct a tripartite pure state $|\Psi_{ABC}\rangle$ of dimension $m \times n \times m^2n^2$ satisfying $\rho_{AB} = \mathrm{tr}_C |\Psi_{ABC}\rangle\langle\Psi_{ABC}|$ (note that such a tripartite pure state of dimension $m \times n \times mn$ exists, but a larger dimension of the subsystem C will be useful later). (i) A POVM measurement $\{\Pi_i\}$ on C produces an ensemble $\{p_i, \rho_i\}$ satisfying $\rho_{AB} = \sum_i p_i\rho_i$, where $p_i = \mathrm{tr}(|\Psi_{ABC}\rangle\langle\Psi_{ABC}| \Pi_i)$ and $\rho_i = \mathrm{tr}_C(|\Psi_{ABC}\rangle\langle\Psi_{ABC}| \Pi_i)/p_i$. (ii) For any ensemble $\{p_i, \rho_i\}$ satisfying $\rho_{AB} = \sum_i p_i\rho_i$, a POVM measurement $\{\Pi_i\}$ exists on C such that $p_i = \mathrm{tr}(|\Psi_{ABC}\rangle\langle\Psi_{ABC}| \Pi_i)$ and $\rho_i = \mathrm{tr}_C(|\Psi_{ABC}\rangle\langle\Psi_{ABC}| \Pi_i)/p_i$; moreover, such a von Neumann measurement on C exists if the dimension of C is greater than or equal to the number of states in the ensemble [50] (this condition is satisfied due to lemma 1(a)). As the definition (1) of E_F remains the same if the infimum is taken over all ensembles of possibly mixed states $\{p_i, \rho_i\}$ satisfying $\rho_{AB} = \sum_i p_i\rho_i$, the relation

$$E_F(\rho_{AB}) = D_{N,P}(\rho_{BC}|C) + S(\rho_A) - S(\rho_{AB}) \quad (16)$$

follows immediately from the definitions of E_F and $D_{N,P}$ (note that in the present case $D_N = D_P$, though generically $D_N \neq D_P$). Set $b = a - S(\rho_A) + S(\rho_{AB})$. We complete the reduction from E_F to $D_{N,P}$ by taking ρ_{BC} as the input to the computational problem in theorem 2. The regularized relation

$$E_C(\rho_{AB}) = D_{N,P}^{\infty}(\rho_{BC}|C) + S(\rho_A) - S(\rho_{AB}). \quad (17)$$

implies a reduction from E_C to $D_{N,P}^{\infty}$. These reductions are polynomial-time reductions. □

4. NP-completeness of computing constrained Holevo capacity

A quantum channel Φ is a completely positive trace-preserving linear map [65] from states of dimension n_i to states of dimension n_o. The constrained Holevo capacity [75] is defined as

$$\chi_\Phi(\rho) = S(\Phi(\rho)) - \inf_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\Phi(|\psi_i\rangle\langle\psi_i|)), \tag{18}$$

where the infimum is taken over all ensembles of pure states $\{p_i, |\psi_i\rangle\}$ satisfying $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. The definition (18) of $\chi_\Phi(\rho)$ remains the same if the number of states in the ensemble is restricted to be less than or equal to n_i^2 [65]. The regularized constrained Holevo capacity is given by

$$\chi_\Phi^\infty(\rho) = \lim_{k\to+\infty} \chi_{\Phi^{\otimes k}}(\rho^{\otimes k})/k. \tag{19}$$

The Holevo capacity $\chi_\Phi = \sup_\rho \chi_\Phi(\rho)$ is the maximum rate at which classical information can be transmitted through the quantum channel Φ using product states as codewords [38, 74]. The regularized Holevo capacity is given by

$$\chi_\Phi^\infty = \lim_{k\to+\infty} \chi_{\Phi^{\otimes k}}/k \neq \sup_\rho \chi_\Phi^\infty(\rho). \tag{20}$$

Corollary 1 (NP-completeness of computing constrained Holevo capacity). *Given a quantum channel Φ, a quantum state ρ of dimension n_i, and a real number c with the promise that either (Y) $\chi_\Phi(\rho) \geqslant c$ or (N) $\chi_\Phi(\rho) \leqslant c - \varepsilon$, it is NP-complete to decide which is the case, where $\varepsilon = 1/\mathrm{poly}(n_i, n_o)$. In the same sense, computing $\chi_\Phi^\infty(\rho)$ is NP-hard.*

Proof. Computing $\chi_\Phi(\rho)$ is in NP: the certificate of (Y) is the optimal ensemble of pure states $\{p_i, |\psi_i\rangle\}$. The hardness proof is a reduction from theorem 1 via the relation [61, 75] between E_F and $\chi_\Phi(\rho)$. Given a bipartite state σ_{AB} of dimension $m \times n$, let U be a unitary embedding such that $\sigma_{AB} = U(\rho)$ for a state ρ of dimension $\mathrm{rank}(\sigma_{AB})$. The quantum channel Φ is defined as $\Phi(\rho') = \mathrm{tr}_B U(\rho')$, where $n_i = \mathrm{rank}(\sigma_{AB}) = O(mn)$ and $n_o = m$. Then

$$E_F(\sigma_{AB}) = S(\Phi(\rho)) - \chi_\Phi(\rho). \tag{21}$$

Set $c = S(\Phi(\rho)) - a$. We complete the reduction from $E_F(\sigma_{AB})$ to $\chi_\Phi(\rho)$. The regularized relation

$$E_C(\sigma_{AB}) = S(\Phi(\rho)) - \chi_\Phi^\infty(\rho) \tag{22}$$

implies a reduction from $E_C(\sigma_{AB})$ to $\chi_\Phi^\infty(\rho)$. These reductions are polynomial-time reductions. □

Lemma 3 (NP-completeness of computing Holevo capacity). *Given a quantum channel Φ and a real number c with the promise that either (Y) $\chi_\Phi \geqslant c$ or (N) $\chi_\Phi \leqslant c - \varepsilon$, it is NP-complete to decide which is the case, where $\varepsilon = 1/\mathrm{poly}(n_i, n_o)$.*

Remark 3. This is one of the main results of [7], in which, however, the scaling of ε is not discussed. Indeed, additional work is needed to establish the NP-completeness of computing χ_Φ with $\varepsilon = 1/\mathrm{poly}(n_i, n_o)$. We are not going to present the complete proof here. The computational complexity of χ_Φ^∞ remains an open problem. The set of all states of dimension n_i is convex, and $-\chi_\Phi(\rho)$ is a convex function as $S(\Phi(\rho))$ is concave and the infimum in (18) is convex. Thus an alternative proof of the NP-hardness of computing $\chi_\Phi(\rho)$ is a polynomial-time

reduction from lemma 3 via convex optimization [12]; moreover, the NP-hardness of computing E_F can be proved[1] based on lemma 3.

5. Applications

Common randomness is a resource in information theory and cryptography [3, 4]. One-way distillable common randomness $D_{cr}(\rho_{AB}|B)$ is the maximum rate at which common randomness can be extracted from the bipartite state ρ_{AB} by local operations and one-way classical communication in the asymptotic limit. It is equal to regularized classical correlation $J_P^{\infty}(\rho_{AB}|B)$ [24], and also equal to regularized one-way classical deficit [25]. Thus D_{cr} and regularized one-way classical deficit are NP-hard to compute.

In quantum state merging, Alice and Bob share a bipartite state, and the goal is to transfer Alice's part of the state to Bob by entanglement-assisted LOCC [39, 40]. The minimum amount of entanglement that must be consumed in extended quantum state merging (a variant of quantum state merging) is an operational interpretation of quantum discord [15], and thus NP-complete to compute.

Quantum discord quantifies the effect of decoherence in a family of protocols. It is the minimum difference between the yield of the fully quantum Slepian-Wolf (FQSW) protocol [1] in the presence and absence of decoherence [60]. The same holds for all descendant protocols of FQSW, where 'yield' refers to the amount of entanglement consumed in quantum state merging [59], the amount of distilled entanglement in entanglement distillation [77], the amount of classical information encoded in superdense coding, and the number of teleported qubits in quantum teleportation (see [60] for details). Thus computing the minimum loss due to decoherence of the yield of all aforementioned protocols is NP-complete.

6. Computational complexity of classical states

A bipartite state ρ_{AB} is separable if it can be expressed as

$$\rho_{AB} = \sum_i p_i \left|\psi_i^A\right\rangle\left\langle\psi_i^A\right| \otimes \left|\psi_i^B\right\rangle\left\langle\psi_i^B\right|, \tag{23}$$

where $\left|\psi_i^A\right\rangle$, $\left|\psi_i^B\right\rangle$ are pure states in the subsystems A, B, respectively, and $p_i \geqslant 0$ satisfies $\sum_i p_i = 1$. ρ_{AB} is quantum-classical if

$$\rho_{AB} = \sum_i p_i \rho_i^A \otimes \Pi_i^B, \tag{24}$$

where ρ_i^A's are normalized, possibly mixed states in A, and $\{\Pi_i^B\}$ is a von Neumann measurement on B. ρ_{AB} is quantum-classical if and only if $D(\rho_{AB}|B) = 0$ [66] (note that $D_N(\rho_{AB}) = 0$ if and only if $D_P(\rho_{AB}) = 0$). ρ_{AB} is classical–classical if

[1] Mark M Wilde, private communication.

$$\rho_{AB} = \sum_{i,j} p_{ij} \Pi_i^A \otimes \Pi_j^B, \tag{25}$$

where $p_{ij} \geqslant 0$ satisfies $\sum_{i,j} p_{ij} = 1$.

Lemma 4 (NP-completeness of linear optimization over separable states [52]). *Given an operator O on a bipartite Hilbert space of dimension $m \times n$ and a real number d with the promise that either (Y) $\max_{\rho_{AB} \in \mathcal{S}} \mathrm{tr}\,(\rho_{AB} O) \geqslant d$ or (N) $\max_{\rho_{AB} \in \mathcal{S}} \mathrm{tr}\,(\rho_{AB} O) \leqslant d - \epsilon$, it is NP-complete to decide which is the case, where $\epsilon = 1/\mathrm{poly}(m, n)$.*

Let $\mathcal{QC}$ (CC) be the set of all quantum-classical (classical–classical) states.

Proposition 1 (NP-completeness of linear optimization over classical states). *Given an operator O on a bipartite Hilbert space of dimension $m \times n$ and a real number d with the promise that either (Y) $\max_{\rho_{AB} \in CC} \mathrm{tr}\,(\rho_{AB} O) \geqslant d$ or (N) $\max_{\rho_{AB} \in CC} \mathrm{tr}\,(\rho_{AB} O) \leqslant d - \epsilon$, it is NP-complete to decide which is the case, where $\epsilon = 1/\mathrm{poly}(m, n)$. The same holds for linear optimization over $\mathcal{QC}$.*

Proof. Linear optimization over CC is in NP: the certificate of (Y) is the optimal state ρ_{AB}. $CC \subseteq \mathcal{QC} \subseteq \mathcal{S}$ implies

$$\max_{\rho_{AB} \in CC} \mathrm{tr}\,(\rho_{AB} O) \leqslant \max_{\rho_{AB} \in \mathcal{QC}} \mathrm{tr}\,(\rho_{AB} O) \leqslant \max_{\rho_{AB} \in \mathcal{S}} \mathrm{tr}\,(\rho_{AB} O). \tag{26}$$

For any separable state $\sigma_{AB} = \sum_i p_i \left|\psi_i^A\right\rangle\left\langle\psi_i^A\right| \otimes \left|\psi_i^B\right\rangle\left\langle\psi_i^B\right|$,

$$\mathrm{tr}\,(\sigma_{AB} O) = \sum_i p_i \,\mathrm{tr}\,(\left|\psi_i^A\right\rangle\left\langle\psi_i^A\right| \otimes \left|\psi_i^B\right\rangle\left\langle\psi_i^B\right| O) \leqslant \sum_i p_i \max_{\rho_{AB} \in CC} \mathrm{tr}\,(\rho_{AB} O) = \max_{\rho_{AB} \in CC} \mathrm{tr}\,(\rho_{AB} O), \tag{27}$$

as $\left|\psi_i^A\right\rangle\left\langle\psi_i^A\right| \otimes \left|\psi_i^B\right\rangle\left\langle\psi_i^B\right| \in CC$ and $\sum_i p_i = 1$ [71]. Thus,

$$\max_{\rho_{AB} \in CC} \mathrm{tr}\,(\rho_{AB} O) = \max_{\rho_{AB} \in \mathcal{QC}} \mathrm{tr}\,(\rho_{AB} O) = \max_{\rho_{AB} \in \mathcal{S}} \mathrm{tr}\,(\rho_{AB} O). \tag{28}$$

□

Lemma 5 [26, 55]. *A bipartite quantum state ρ_{AB} is separable if and only if there exists a state $\rho_{AA'|BB'} \in CC$ in an extended Hilbert space such that $\rho_{AB} = \mathrm{tr}_{A'B} \rho_{AA'BB'}$, or if and only if a state $\rho_{A|BB'} \in \mathcal{QC}$ exists such that $\rho_{AB} = \mathrm{tr}_{B'} \rho_{ABB'}$.*

Remark 4. The definition (23) of separability remains the same if the number of terms in the summation is restricted to be less than or equal to $m^2 n^2$ [41], where $m \times n$ is the dimension of the bipartite state ρ_{AB}. By slightly modifying the original proofs in [26, 55], the dimensions of $\rho_{AA'|BB'}$ and $\rho_{A|BB'}$ can be required to be $m^3 n^2 \times m^2 n^3$ and $m \times m^2 n^3$, respectively.

Proposition 2 (NP-completeness of detecting classical states in a convex set). *Given a convex set K of bipartite quantum states (K is given by a polynomial-time algorithm outputting whether a state is in K) with the promise that either (Y) $K \cap CC \neq \varnothing$ or (N) $\inf_{\rho \in K, \sigma \in CC} \| \rho - \sigma \|_1 \geqslant \delta$, it is NP-complete to decide which is the case, where $\delta = 1/\mathrm{poly}(m, n)$. The same holds for detecting quantum-classical states in K.*

Proof. Detecting classical–classical states in K is in NP: the certificate of (Y) is an element in $K \cap CC \neq \varnothing$. The hardness proof is a polynomial-time reduction from lemma 2. Given a bipartite state ρ_{AB}, define the convex set

$$K = \{\rho_{AA'|BB'} \Big| \rho_{AB} = \mathrm{tr}_{A'B'}\rho_{AA'BB'}\}. \tag{29}$$

(Y) If ρ_{AB} is separable, then $K \cap CC \neq \varnothing$. (N) If $\inf_{\sigma_{AB}\in\mathcal{S}} \| \rho_{AB} - \sigma_{AB} \|_2 \geqslant \delta$, then for any $\rho_{AA'BB'} \in K$ and $\sigma_{AA'BB'} \in CC$,

$$\| \rho_{AA'BB'} - \sigma_{AA'BB'} \|_1 \geqslant \| \mathrm{tr}_{A'B'}(\rho_{AA'BB'} - \sigma_{AA'BB'}) \|_1 = \| \rho_{AB} - \sigma_{AB} \|_1 \geqslant \| \rho_{AB} - \sigma_{AB} \|_2 \geqslant \delta, \tag{30}$$

as $\| \cdot \|_1$ is non-increasing under partial trace [56] and $\sigma_{AB} = \mathrm{tr}_{A'B'}\sigma_{AA'BB'}$ is separable. The NP-completeness of detecting quantum-classical states in K can be proved analogously. □

7. Conclusion and outlook

We have proved that computing quantum discord is NP-complete. Therefore, the running time of any algorithm for computing quantum discord is believed to grow exponentially with the dimension of the Hilbert space so that computing quantum discord in a quantum system of moderate size is not possible in practice. As by-products, some entanglement measures and constrained Holevo capacity are NP-hard/NP-complete to compute. These complexity-theoretic results are directly applicable in quantum information processing, and may offer significant insights. Moreover, we have proved the NP-completeness of two typical problems related to classical states, providing evidence that working with classical states is generically computationally intractable.

The NP-completeness of computing quantum discord raises some interesting open problems. Is there an efficient approximation algorithm for computing quantum discord up to a moderate (e.g. constant additive) error? Can quantum discord be efficiently computed for certain important classes of states? What is the computational complexity of other measures of quantum correlation beyond entanglement (e.g. geometric quantum discord [21, 58], quantum deficit)? The computational complexity of quantum correlation in continuous-variable systems is a new research direction. In particular, Gaussian states are of great theoretical and experimental interest [82, 83]. The separability problem for multimode bipartite Gaussian states [84] can be formulated as a semidefinite program [51] and solved efficiently in theory and practice [79] (the analog of lemma 2 for Gaussian states is false). What is the computational complexity of Gaussian entanglement of formation [85] and Gaussian quantum discord [2, 31]?

Acknowledgements

The author would like to thank Sevag Gharibian, Joel E Moore and Mark M Wilde for useful comments. This work was supported by the ARO via the DARPA OLE program.

References

[1] Abeyesinghe A, Devetak I, Hayden P and Winter A 2009 The mother of all protocols: restructuring quantum information's family tree *Proc. R. Soc.* A **465** 2537–63

[2] Adesso G and Datta A 2010 Quantum versus classical correlations in Gaussian states *Phys. Rev. Lett.* **105** 030501
[3] Ahlswede R and Csiszar I 1993 Common randomness in information theory and cryptography. I. Secret sharing *IEEE Trans. Inf. Theory* **39** 1121–32
[4] Ahlswede R and Csiszar I 1998 Common randomness in information theory and cryptography. II. CR capacity *IEEE Trans. Inf. Theory* **44** 225–40
[5] Ali M, Rau A R P and Alber G 2010 Quantum discord for two-qubit X states *Phys. Rev.* A **81** 042105
Ali M, Rau A R P and Alber G 2010 Quantum discord for two-qubit X states *Phys. Rev.* A **82** 069902 (erratum)
[6] Beckner W 1975 Inequalities in Fourier analysis *Ann. Math.* **102** 159–82
[7] Beigi S and Shor P W 2007 On the complexity of computing zero-error and Holevo capacity of quantum channels arXiv:0709.2090
[8] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9
[9] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction *Phys. Rev.* A **54** 3824–51
[10] Bennett C H and Wiesner S J 1992 Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states *Phys. Rev. Lett.* **69** 2881–4
[11] Bialynicki-Birula I and Mycielski J 1975 Uncertainty relations for information entropy in wave mechanics *Commun. Math. Phys.* **44** 129–32
[12] Boyd S and Vandenberghe L 2004 *Convex Optimization* (Cambridge: Cambridge University Press)
[13] Brandao F G, Christandl M and Yard J 2011 Faithful squashed entanglement *Commun. Math. Phys.* **306** 805–30
Brandao F G, Christandl M and Yard J 2012 Faithful squashed entanglement *Commun. Math. Phys.* **316** 287–8 (erratum)
[14] Brandao F G, Christandl M and Yard J 2011 A quasipolynomial-time algorithm for the quantum separability problem *Proc. 43rd Ann. ACM Symp. Theory Comput.* 343–352
[15] Cavalcanti D, Aolita L, Boixo S, Modi K, Piani M and Winter A 2011 Operational interpretations of quantum discord *Phys. Rev.* A **83** 032324
[16] Chen L, Chitambar E, Modi K and Vacanti G 2011 Detecting multipartite classical states and their resemblances *Phys. Rev.* A **83** 020101(R)
[17] Chen Q, Zhang C, Yu S, Yi X X and Oh C H 2011 Quantum discord of two-qubit X states *Phys. Rev.* A **84** 042313
[18] Christandl M and Winter A 2004 'Squashed entanglement': an additive entanglement measure *J. Math. Phys.* **45** 829–40
[19] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880–4
[20] Cook S A 1971 The complexity of theorem-proving procedures *Proc. 3rd Ann. ACM Symp. Theory Comput.* 151–8
[21] Dakic B, Vedral V and Brukner C 2010 Necessary and sufficient condition for nonzero quantum discord *Phys. Rev. Lett.* **105** 190502
[22] D'Ariano G M, Presti P L and Perinotti P 2005 Classical randomness in quantum measurements *J. Phys. A: Math. Gen.* **38** 5979–91
[23] Datta A, Shaji A and Caves C M 2008 Quantum discord and the power of one qubit *Phys. Rev. Lett.* **100** 050502
[24] Devetak I and Winter A 2004 Distilling common randomness from bipartite quantum states *IEEE Trans. Inf. Theory* **50** 3183–96
[25] Devetak I and Winter A 2005 Distillation of secret key and entanglement from quantum states *Proc. R. Soc.* A **461** 207–35

[26] Devi A R U and Rajagopal A K 2008 Generalized information theoretic measure to discern the quantumness of correlations *Phys. Rev. Lett.* **100** 140502
[27] Dillenschneider R 2008 Quantum discord and quantum phase transition in spin chains *Phys. Rev.* B **78** 224413
[28] Duan L-M, Giedke G, Cirac J I and Zoller P 2000 Inseparability criterion for continuous variable systems *Phys. Rev. Lett.* **84** 2722–5
[29] Einstein A, Podolsky B and Rosen N 1935 Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47** 777–80
[30] Gharibian S 2010 Strong NP-hardness of the quantum separability problem *Quantum Inf. Comput.* **10** 343–60
[31] Giorda P and Paris M G A 2010 Gaussian quantum discord *Phys. Rev. Lett.* **105** 020503
[32] Guhne O and Toth G 2009 Entanglement detection *Phys. Rep.* **474** 1–75
[33] Gurvits L 2003 Classical deterministic complexity of Edmonds' problem and quantum entanglement *Proc. 35th Ann. ACM Symp. Theory Comput.* pp 10–19
[34] Gurvits L 2004 Classical complexity and quantum entanglement *J. Comput. Syst. Sci.* **69** 448–84
[35] Hamieh S, Kobes R and Zaraket H 2004 Positive-operator-valued measure optimization of classical correlations *Phys. Rev.* A **70** 052325
[36] Hayden P M, Horodecki M and Terhal B M 2001 The asymptotic entanglement cost of preparing a quantum state *J. Phys. A: Math. Gen.* **34** 6891–8
[37] Henderson L and Vedral V 2001 Classical quantum and total correlations *J. Phys. A: Math. Gen.* **34** 6899–905
[38] Holevo A 1998 The capacity of the quantum channel with general signal states *IEEE Trans. Inf. Theory* **44** 269–73
[39] Horodecki M, Oppenheim J and Winter A 2005 Partial quantum information *Nature* **436** 673–6
[40] Horodecki M, Oppenheim J and Winter A 2007 Quantum state merging and negative information *Commun. Math. Phys.* **269** 107–36
[41] Horodecki P 1997 Separability criterion and inseparable mixed states with positive partial transposition *Phys. Lett.* A **232** 333–9
[42] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865–942
[43] Huang J-H, Wang L and Zhu S-Y 2011 A new criterion for zero quantum discord *New J. Phys.* **13** 063045
[44] Huang Y 2010 Entanglement criteria via concave-function uncertainty relations *Phys. Rev.* A **82** 012335
Huang Y 2010 Entanglement criteria via concave-function uncertainty relations *Phys. Rev.* A **82** 069903 (erratum)
[45] Huang Y 2011 Entropic uncertainty relations in multidimensional position and momentum spaces *Phys. Rev.* A **83** 052124
[46] Huang Y 2012 Variance-based uncertainty relations *Phys. Rev.* A **86** 024101
[47] Huang Y 2013 Entanglement detection: complexity and Shannon entropic criteria *IEEE Trans. Inf. Theory* **59** 6774–8
[48] Huang Y 2013 Quantum discord for two-qubit X states: analytical formula with very small worst-case error *Phys. Rev.* A **88** 014302
[49] Huang Y 2014 Scaling of quantum discord in spin models *Phys. Rev.* B **89** 054410
[50] Hughston L P, Jozsa R and Wootters W K 1993 A complete classification of quantum ensembles having a given density matrix *Phys. Lett.* A **183** 14–18
[51] Hyllus P and Eisert J 2006 Optimal entanglement witnesses for continuous-variable systems *New J. Phys.* **8** 51
[52] Ioannou L M 2007 Computational complexity of the quantum separability problem *Quantum Inf. Comput.* **7** 335–70
[53] Knill E and Laflamme R 1998 Power of one bit of quantum information *Phys. Rev. Lett.* **81** 5672–5

[54] Koashi M and Winter A 2004 Monogamy of quantum entanglement and other correlations *Phys. Rev.* A **69** 022309
[55] Li N and Luo S 2008 Classical states versus separable states *Phys. Rev.* A **78** 024303
[56] Lidar D A, Zanardi P and Khodjasteh K 2008 Distance bounds on quantum dynamics *Phys. Rev.* A **78** 012308
[57] Lu X-M, Ma J, Xi Z and Wang X 2011 Optimal measurements to access classical correlations of two-qubit states *Phys. Rev.* A **83** 012327
[58] Luo S and Fu S 2010 Geometric measure of quantum discord *Phys. Rev.* A **82** 034302
[59] Madhok V and Datta A 2011 Interpreting quantum discord through quantum state merging *Phys. Rev.* A **83** 032323
[60] Madhok V and Datta A 2013 Quantum discord as a resource in quantum communication *Int. J. Mod. Phys.* B **27** 1345041
[61] Matsumoto K, Shimono T and Winter A 2004 Remarks on additivity of the Holevo channel capacity and of the entanglement of formation *Commun. Math. Phys.* **246** 427–42
[62] Matthews W, Wehner S and Winter A 2009 Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding *Commun. Math. Phys.* **291** 813–43
[63] Modi K, Brodutch A, Cable H, Paterek T and Vedral V 2012 The classical-quantum boundary for correlations: discord and related measures *Rev. Mod. Phys.* **84** 1655–707
[64] Nielsen M A 2000 Continuity bounds for entanglement *Phys. Rev.* A **61** 064301
[65] Nielsen M A and Chuang I L 2011 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[66] Ollivier H and Zurek W H 2001 Quantum discord: a measure of the quantumness of correlations *Phys. Rev. Lett.* **88** 017901
[67] Peres A 1996 Separability criterion for density matrices *Phys. Rev. Lett.* **77** 1413–5
[68] Piani M 2009 Relative entropy of entanglement and restricted measurements *Phys. Rev. Lett.* **103** 160504
[69] Piani M, Christandl M, Mora C E and Horodecki P 2009 Broadcast copies reveal the quantumness of correlations *Phys. Rev. Lett.* **102** 250503
[70] Plenio M B and Virmani S 2007 An introduction to entanglement measures *Quantum Inf. Comput.* **7** 1–51
[71] Rahimi R and SaiToh A 2010 Single-experiment-detectable nonclassical correlation witness *Phys. Rev.* A **82** 022314
[72] Robertson H P 1929 The uncertainty principle *Phys. Rev.* **34** 163–4
[73] Sarandy M S 2009 Classical correlation and quantum discord in critical systems *Phys. Rev.* A **80** 022108
[74] Schumacher B and Westmoreland M D 1997 Sending classical information via noisy quantum channels *Phys. Rev.* A **56** 131–8
[75] Shor P W 2004 Equivalence of additivity questions in quantum information theory *Commun. Math. Phys.* **246** 453–72
[76] Simon R 2000 Peres–Horodecki separability criterion for continuous variable systems *Phys. Rev. Lett.* **84** 2726–9
[77] Streltsov A, Kampermann H and Bruss D 2011 Linking quantum discord to entanglement in a measurement *Phys. Rev. Lett.* **106** 160401
[78] Uhlmann A 1998 Entropy and optimal decompositions of states relative to a maximal commutative subalgebra *Open Syst. Inf. Dyn.* **5** 209–28
[79] Vandenberghe L and Boyd S 1996 Semidefinite programming *SIAM Rev.* **38** 49–95
[80] Vedral V and Plenio M B 1998 Entanglement measures and purification procedures *Phys. Rev.* A **57** 1619–33
[81] Vedral V, Plenio M B, Rippin M A and Knight P L 1997 Quantifying entanglement *Phys. Rev. Lett.* **78** 2275–9
[82] Wang X-B, Hiroshima T, Tomita A and Hayashi M 2007 Quantum information with Gaussian states *Phys. Rep.* **448** 1–111

[83] Weedbrook C, Pirandola S, Garcia-Patron R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 Gaussian quantum information *Rev. Mod. Phys.* **84** 621–69
[84] Werner R F and Wolf M M 2001 Bound entangled Gaussian states *Phys. Rev. Lett.* **86** 3658–61
[85] Wolf M M, Giedke G, Kruger O, Werner R F and Cirac J I 2004 Gaussian entanglement of formation *Phys. Rev.* A **69** 052320
[86] Yang D, Horodecki M and Wang Z D 2008 An additive and operational entanglement measure: conditional entanglement of mutual information *Phys. Rev. Lett.* **101** 140501