Entanglement, discord and the power of quantum computing

Aharon Brodutch* and Daniel R. Terno†
Department of Physics & Astronomy, Faculty of Science, Macquarie University, NSW 2109, Australia

It is impossible to implement an entangling bipartite quantum operation with local operations and classical communication (LOCC) without a shared entanglement. When the operation is restricted to act on unentangled input states that are transformed into unentangled outputs, it may seem that the implementation by LOCC alone is possible. We present an example where this assertion fails. Non-zero quantum discord, which is a measure of quantumness of correlations even in the absence of entanglement, may indicate the failure of the LOCC implementation without entanglement.

arXiv:1009.2571v1 [quant-ph] 14 Sep 2010

The question "what makes the quantum computer tick" goes back to the early discussions of quantum algorithms [1]. The issue at stake is weather entanglement is essential for having a speed-up over the classical algorithms, or is it just a byproduct of the quantum superposition [2, 3].

On the one hand, the universal quantum computation is possible if a certain set of one-qubit operations and a two-qubit controlled-NOT (CNOT) gate can be performed [2]. This gate is entangling, i.e it turns a generic non-entangled input into an entangled output. Moreover, any pure-state quantum computation with only a restricted amount of entanglement can be efficiently simulated classically. This also applies to the simulations of low-entanglement states of various many-body systems [4].

On the other hand, the algorithm DQC1 [5] presented us with an example of a quantum speed-up without entanglement, and also drew additional attention to the hierarchy of correlations in quantum mechanics. Particularly, presence of quantum correlations without entanglement is captured by quantum discord [6], which we will use in the following. More precisely, there is no bipartite entanglement in the system at any stage of the DQC1 execution, but the final state has a non-zero discord between the control qubit and the rest.

Our goal is to show that there is some "implicit entanglement" hidden in the operation of two-qubit gates, even if they operate on a restricted set $\mathcal{L}$ of unentangled input states that are transformed into unentangled outputs. To this end we consider a distributed implementation of the gate, where two parties A(lise) and B(ob) execute it by local operations and some shared resources. We show that under quite general assumptions a two-qubit gate may be implemented by-locally even on such $\mathcal{L}$ only if Alice and Bob share some entanglement. We first introduce the relevant properties of the discord, then present a simple example and follow with some general results.

Discord [6] aims to quantify quantum correlations in a given bipartite state through the difference in quantum generalizations of two expressions for the classical mutual information,

$$I(A:B) = H(A) + H(B) - H(AB), \tag{1}$$

and

$$J(A:B) = H(A) - H(A|B) = H(B) - H(B|A), \tag{2}$$

where $H(X)$ is the Shannon entropy of the probability distribution X, $H(B|A)$ the conditional entropy of B given A, and $H(AB)$ is a joint probability distribution [7]. The two classical expressions are equivalent. Quantum measurement procedure M on a state ρ leads to a probability distribution X_ρ^M. The von Neumann entropy $S(\rho_X) = -\mathrm{tr}\,\rho_X \log \rho_X$ replaces the Shannon entropy [8], but the conditional entropy now explicitly depends on the measurement procedure [6, 9] and the optimization goal it tries to achieve. For our purposes it is enough to assume that the measurement Π_A performed by Alice is represented by a complete set of orthogonal projections, and the optimization is chosen to lead to the discord measure D_2 [10, 11]. Then

$$J_2^{\Pi^A}(\rho)_2 := S(\rho_B) - S(\rho_B|\Pi_A) + S(\rho_A) - S(\rho_A^\Pi), \tag{3}$$

where the averaged post-measurement state of A is

$$\rho_A^\Pi = \sum_a p_a \Pi_A^a, \qquad p_a = \mathrm{tr}\,\rho_A \Pi_A^a, \tag{4}$$

the conditional entropy of the post-measurement state

$$S(\rho_B|\Pi_A) := \sum_a p_a S(\rho_{B|\Pi_A^a}). \tag{5}$$

is the weighted average of the entropies of the states

$$\rho_{B|\Pi_A^a} = (\Pi_A^a \otimes \mathbb{1}_B \rho \Pi_A^a \otimes \mathbb{1}_B)/p_a, \tag{6}$$

that correspond to the individual outcomes, so the discord is

$$D_2^A(\rho) := \min_\Pi [H(A_\rho^\Pi) + S(\rho_B|\Pi^A)] - S(\rho_{AB}). \tag{7}$$

Discord has a number of interesting properties and applications [10–13]. We will use the following property [11]:

$$D_2^{\Pi_A}(\rho) = S(\rho^{\Pi^A}) - S(\rho_{AB}), \tag{8}$$

for any set Π_A regardless of its optimality. Often we will speak just of the discord, without specifying its type.

This is justified since all types of discord vanish simultaneously [11].

Example. First we consider a CNOT gate. It can be performed bilocally by Alice and Bob if they share one ebit of entanglement per gate use [14]. Now we investigate a possibility of a bilocal implementation of this gate on a restricted set of states without a shared entanglement. Alice and Bob are restricted to arbitrary local operations and measurements on their respective qubits, and allowed to exchange unlimited classical messages. While it is just the standard LOCC paradigm, we point out one feature of the reduced dynamics of the system that is important in the following.

The measurements are given by arbitrary local positive operator-valued measures (POVM), so Alice's measurement is given by a family of positive operators of the form $E_\mu^A = \Lambda_\mu^A \otimes \mathbb{1}_B$, $\Lambda_\mu^A > 0$, $\sum \Lambda_\mu^A = \mathbb{1}_A$. At each stage the operations and measurements are integrated together with the help of ancilla, which can be further divided into two part $A'A''$, as in [15]. The measurement is accomplished in two stages: first some unitary operation $U_{AA'A''}$ is applied the entire system, and then a standard projective measurement Π_a, $a = 1, \ldots \dim A''$, $\Pi_a\Pi_b = \Pi_a\delta_{ab}$ is applied to the system A''. Depending on the outcome, a unitary $U_{AA'}(a)$ is applied to the remaining part AA'. While the entire evolution is completely positive, i.e. $\rho_A^{\rm in} \mapsto \rho_A^{\rm out} = \sum_\mu K_\mu \rho_A^{\rm in} K_\mu^\dagger$ for some set of Kraus matrices K_μ [2], the evolution of a post-measurement state $\rho_{A|\Pi^a} \mapsto \rho_A^{\rm out} = {\rm tr}_{A'} U_{AA'}(a)\rho'_{AA'}U^\dagger_{AA'}(a)$ generally depends on the correlations between A and A' and may be not completely positive [16].

Alice and Bob share an unknown state from the known list $\mathcal{L}$ and try to implement the CNOT gate by LOCC. It is obvious that if the set of states in question is locally distinguishable, then the the gate can be LOCC implemented. It is also obvious that if its action creates entanglement, the implementation fails. However, absence of entanglement is not sufficient.

Consider the set $\mathcal{L}$ in Table I.

TABLE I: Four inputs/outputs for the CNOT gate

#	State	#	State
a	$\|1\rangle\|Y_+\rangle \to i\|1\rangle\|Y_-\rangle$	c	$\|Y_+\rangle\|X_-\rangle \to \|Y_-\rangle\|X_-\rangle$
b	$\|0\rangle\|Y_+\rangle \to \|0\rangle\|Y_+\rangle$	d	$\|Y_+\rangle\|X_+\rangle \to \|Y_+\rangle\|X_+\rangle$

Here $\sigma_y|Y_\pm\rangle = \pm|Y_\pm\rangle$, $\sigma_x|X_\pm\rangle = \pm|X_\pm\rangle$, where $\sigma_{x,y,z}$ are Pauli matrices.

We now demonstrate that the ability to implement the CNOT gate on $\mathcal{L}$ without shared entanglement allows unambiguously discriminate between these non-orthogonal states using just one input copy, which is impossible [8]. Without specifying the local operations of Alice and Bob we classify them according to their action on the sate $|Y_+\rangle$. An operation Φ is *flipping* (F) if up to a phase $\Phi(|Y_+\rangle) = |Y_-\rangle$, *non-flipping* (N) if $\Phi(|Y_+\rangle) = |Y_+\rangle$, and undetermined otherwise.

Knowing type of the operation allows Alice and Bob to narrow down the list of possible inputs: e.g., Bob's F is incompatible with having input b, while for Alice's operation not to have a definite type excludes both c and d. The resulting list of possible inputs if both operations are of a definite type is presented in Table II. If one of the operations is neither F or N, then the type of another operations allows to determine the input uniquely.

TABLE II: Possible inputs

Alice	Bob F	Bob N
F	$\{a\ c\}$	$\{c\ b\}$
N	$\{a\ d\}$	$\{b\ d\}$

Any pair of outputs can be reset to the original inputs by local unitaries and re-sent through the gate. For example, if the overall operation was of FF type (identifying the inputs as either a or c), the operation $\sigma_z^A \otimes \sigma_x^B$ transforms the outputs $\psi'_a = |1\rangle|Y_-\rangle$ and $\psi'_c = |Y_-\rangle|X_-\rangle$ into the inputs ψ_a and ψ_c.

The operations that implement the gate this time may be of the same type as before, or different. If the gate is such that there is a finite probability of having a different operation type, it will be realized after a finite number of trials. This other type (FN or NF in the above example) will uniquely specifies the input. If a particular pair of inputs is processed always by operations of the same type, then the gate can be used to unambiguously distinguish between one state from this pair and at least one of the two remaining states in a single trial. ■

From this point of view, the role of entanglement in the bilocal implementation of the gate is to make impossible for Alice and Bob identify the effects of their operations.

It is obvious that if only the inputs a and b should be processed, the gate can be implemented by LOCC. What about three inputs? A criterion that we prove below states that (under some assumptions about the gate action) a bilocal implementation without entanglement is impossible if the input states or any of their random mixtures have a non-zero discord

$$D_2(\rho) := \min[D_2^A(\rho), D_2^B(\rho)] \neq 0. \tag{9}$$

Unlike the exact value of discord that can be calculated analytically only in special cases, it is straightforward to check weather the discord is zero or not [11]. Moreover, sates of zero discord (say, $D_2^A = 0$) are of the form

$$\rho = \sum_a p_a \Pi_A^a \otimes \rho_B^a, \qquad p_a \geq 0, \quad \sum_a p_a = 1. \tag{10}$$

Now we specify precisely the implementations of a gate U we consider.

Definition. A bilocal implementation G of a gate U on some (finite) set of unentangled states $\mathcal{L} = \{\rho_i^{\rm in}\}_{i=1}^N$ (and their convex combinations) is a completely positive map that is implemented by local operations on the subsystems A and B, performed separately, and assisted by unlimited classical communication such that for any state $\rho_i \in \mathcal{L}$

$$G(\rho_i^{\rm in}) = \sum_k K_k \rho_i^{\rm in} K_k^\dagger \equiv U\rho_i U^\dagger =: \rho_i^{\rm out}. \qquad (11)$$

Successful implementation of the gate on pure inputs guaranties that it is "reversible", with dual maps [17] playing the role of the inverse.

Lemma 1. The dual map $G^+(\rho) := \sum_k K_k^\dagger \rho K_k$ satisfies

$$\rho_i^{\rm in} = G^+(\rho_i^{\rm out}) \qquad (12)$$

for all pure input states $\rho_\psi \in \mathcal{L}$.

Proof: Since $\rho_\psi^{\rm out} = G(\rho_\psi^{\rm in}) = U\rho_\psi U^\dagger$ is pure, using the Hilbert-Schmidt inner product we see that

$$1 = \langle \rho_\psi^{\rm out}, \rho_\psi^{\rm out}\rangle = \langle \rho_\psi^{\rm in}, G^+(U\rho_\psi^{\rm in}U^\dagger)\rangle, \qquad (13)$$

hence G^+ acts as an inverse for all allowed pure inputs and their convex combinations. ■

It is straightforward to see that if we restrict local operations to projective measurements and unitaries, then the zero discord becomes a necessary criterion for such implementation's success. Namely, since entropies of initial and final states are the same, but a local measurement on a state of non-zero discord increases it according to Eq. (8), we reach a contradiction.

Now we consider a bilocal implementation of a two-qubit gate. We assume that the maximally mixed state is an allowed input (i.e. the gate is unital, $G(\mathbb{1}) = \mathbb{1}$), and also there is one pure input that we can write as $|00\rangle$. We also restrict the allowed local operations to a completely positive maps (this is realized, in particular, if at each stage the ancilla is entirely consumed in the measurement, i.e., $\dim A' = 0$).

Lemma 2. If a set $\mathcal{L}$ contains one pure product state $(00\rangle)$ and the maximally mixed sate $(\mathbb{1}/4)$, and the gate U is implemented by local operations(restricted to arbitrary POVM and CP maps) and classical communication, then all other allowed inputs and their arbitrary convex combinations satisfy $D_2^A(\rho^{\rm in}) = D_2^B(\rho^{\rm in}) = 0$.

Proof: Introduce a CP map $\Phi(\rho) = G^+\big(G(\rho)\big)$. It is a unital map, because G^+ is unital [17]. According to Lemma 1 its application to $\rho_{00} := |00\rangle\langle 00|$ gives $\Phi(\rho_{00}) = \rho_{00}$. Assume that Alice is the first party to perform a measurement on the inputs, so consider a state $\rho_{10} := |10\rangle\langle 10|$ (not necessarily an allowed input). Since Φ is unital,

$$\Phi(\mathbb{1} - \rho_{00}) = \Phi(\rho_{01} + \rho_{10} + \rho_{11}) = \mathbb{1} - \rho_{00}, \qquad (14)$$

so $\langle 0|\Phi(\rho_{10}|0\rangle = 0$, and similarly for two other states in the above equation. As a result, the positivity of $\Phi(\rho_{10})$ ensures that it has a disjoint support from ρ_{00}. Separate the map Φ into Alice's first measurement $\{\Lambda_\mu^A\}$ and everything else. Evolution of any state $\rho^{\rm in}$ can be schematically written as $\rho^{\rm in} \mapsto \rho^\mu \mapsto \rho^{\rm out} \mapsto \rho'$, with $\rho^{\rm out} = U\rho^{\rm in}U^\dagger$ for $\rho^{\rm in} \in \mathcal{L}$, and $\rho' = \rho^{\rm in}$ for pure states in $\mathcal{L}$. Since $\rho' = \Phi_\mu(\rho^\mu)$ for some CP map Φ_μ by the lemma's assumption, and CP maps cannot improve state distinguishability [2, 18], the post-measurement states ρ_{00}^μ and ρ_{10}^μ should have disjoint supports for any outcome μ. Recall that in dealing with these two states Alice measures pure qubits while Bob's sides are identical. Hence Alice's measurement reduces to the projective measurement in the 0,1 basis,

$$\Lambda_a^A = \Pi_a^A = |a\rangle\langle a|_A, \qquad a = 0, 1. \qquad (15)$$

Assume that the states with pure reduced reduced density matrices $\rho_A^{\rm in}$ which are not ρ_{00} or ρ_{10}, or mixed states of non-zero discord are allowed inputs. For pure states $\rho_A^{\rm in}$ the average post-measurement entropy becomes non-zero [2, 8]. For mixed states with $D_2^A \neq 0$ Eq. (8) ensures that $S(\rho^{\Pi^A}) > S(\rho^{\rm in})$. However, projective measurements are repeatable, and the second measurement by Alice will certainly give the same result and induce no change in the state. Hence, if the state $\rho^{\rm in} \in \mathcal{L}$, then $G(\rho_{\rm in}^a) = G(\rho^{\rm in}) = U\rho^{\rm in}U^\dagger$. Since both unitary and unital CP maps preserve entropy [2, 17], we reach a contradiction.

In case the first measurement is performed by Bob we consider the state $|01\rangle$ and use the discord D_2^B. ■

Even if the scheme we considered is not the most general one, it is possible to draw several conclusions. First, absence of entanglement in both input and output does not automatically enable a remote implementation by LOCC. Second, a discrepancy between local and global information content of non-entangled states (which is captured by the discord D_2 in our setting and may have to be generalized in more sophisticated scenarios) requires entanglement for their processing. It would be an interesting to quantify the minimal amount of entanglement required for the gate implementations in different scenarios and relate it to the discord or other suitable measures.

We thank G. Brennen, A. Datta, J. Twamley, and K. Życzkowski for discussions and helpful comments.

---

* Electronic address: aharon.brodutch@mq.edu.au
† Electronic address: daniel.terno@mq.edu.au

[1] A. Ekert and R Jozsa, Phil. Trans. R. Soc. London A **356**, 1769 (1998).
[2] D. Bruß and G. Leuchs, *Lectures on Quantum Information* (Wiley-VCH, Weinheim, 2007); M. A. Nielsen and

I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University, Cambridge, 2000).
[3] V. M. Kendon and W. J. Munro, Quant. Info. Comp. **6**, 630 (2006).
[4] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003); A. J. Daley, C. Kollath, U. Schollwöck and G. Vidal, J. Stat. Mech. P0405, 1742 (2004).
[5] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
[6] H. Ollivier and W. H. Zurek, Phys. Rev. Let. **88**, 017901 (2001); L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (John Wiley & Sons, New York, 1991).
[8] A. Peres, *Quantum Theory: Concepts and Methods*, (Kluwer, Dordrecht, 1995).
[9] A. Datta, *Studies on the Role of Entanglement in Mixed-state Quantum Computation*, Ph. D. thesis (The University of New Mexico, Albuqerque, 2008), e-print arXiv:0807.4490.
[10] W. H. Zurek, Phys. Rev. A **67**, 012320 (2003).
[11] A. Brodutch and D. R. Terno, Phys. Rev. A **81**, 062103 (2010).
[12] A.-m. Kuah, K. Modi, C. A. Rodriguez-Rosario, and E. C. G. Sudarshan, Phys. Rev. A **76** 042113 (2007); A. Shabani and D. A. Lidar, Phys. Rev. Lett. **102**, 100402 (2009).
[13] K. Modi, T. Paterek, W Son, V. Vedral, and M. Williamson, Phys. Rev. Lett. **104**, 080501 (2010).
[14] J. Eisert, K. Jacobs, P. Papadopoulos and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).
[15] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[16] H. A. Carteret, D. R. Terno, and K. Życzkowski, Phys. Rev. A **77**, 042113 (2008).
[17] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States*, Cambridge University Press, Cambridge, 2006.
[18] C. A. Fuchs and J. van de Graaf, IEEE Trans. Info. Theor. **45**, 1216 (1999).