Necessary and sufficient condition for non-zero quantum discord

Borivoje Dakić,1 Vlatko Vedral,2,3,4 and Časlav Brukner1,5

1Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria
2Centre for Quantum Technologies, National University of Singapore, Singapore
3Department of Physics, National University of Singapore, Singapore
4Clarendon Laboratory, University of Oxford, Oxford UK
5Institute of Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria

(Dated: November 4, 2010)

Quantum discord characterizes “non-classicality” of correlations in quantum mechanics. It has been proposed as the key resource present in certain quantum communication tasks and quantum computational models without containing much entanglement. We obtain a necessary and sufficient condition for the existence of non-zero quantum discord for any dimensional bipartite states. This condition is easily experimentally implementable.

Based on this, we propose a geometrical way of quantifying quantum discord. For two qubits this results in a closed form of expression for discord. We apply our results to the model of deterministic quantum computation with one qubit (DQC1), showing that quantum discord is unlikely to be the reason behind its speedup.

PACS numbers: 03.67.Mn, 03.65.Ta, 03.67.Ac, 03.67.Lx

Introduction.— Quantum states of a composite system can be divided into entangled and separable ones. Entangled states display “nonlocal features” violating Bell’s inequalities[6–11] and are considered a necessary resource for quantum communication and pure quantum computation allowing computationally speedup over the best classical algorithm[2]. On the contrary, separable states are generally considered as purely classical, since they do not violate Bell’s inequalities and can be prepared by local operations and classical communication. However, it is valid to ask if highly mixed states, and in particular separable states, are completely useless from quantum information perspective. Recent investigations give compelling evidences that this is not the case. A highly mixed state in the DQC1 model[3] is believed to perform a task exponentially faster than any classical algorithm (“without containing much entanglement”). Furthermore, it has been shown that even some separable states contain nonclassical correlations[3,5] and can create an advantage for computing and information processing tasks over their classical counterparts[3,11].

The “non-classicality” of bipartite correlations is measured via quantum discord[4]—the discrepancy between quantum versions of two classically equivalent expressions for mutual information. Recently, it has been shown that almost all quantum states have non-vanishing discord[12]. Quantum discord was proposed as a figure of merit for characterizing the nonclassical resources present in the DQC1[10]. It has been shown that initial zero-discord system-environment state is necessary and sufficient condition for completely-positive map evolution of the system when the environment is traced out[13,14]. Furthermore, in Ref. [15] is demonstrated that if the state can be locally broadcasted than it has vanishing discord.

Despite increasing evidences for relevance of quantum discord in describing non-classical resources in information processing, there is no straightforward criterion to verify the presence of discord in a given quantum state. Its evaluation involves optimization procedure and analytical results are known only in a few cases[16]. In this Letter we derive the necessary and sufficient condition for non-vanishing quantum discord. The criterion is simple and also experimentally friendly, since it can be evaluated directly from a (sub)set of measurements standardly used for quantum state tomography. Based on this, we introduce the geometrical measure of discord and derive an explicit expression for the case of two qubits. Finally, we give arguments putting in question appropriateness of quantum discord to describe the non-classical resource in DQC1 computational model.

Quantum discord.— Correlations between two random variables of classical systems A and B are in information theory quantified by the mutual information $I(A:B) = H(A) + H(B) - H(A,B)$. If A and B are classical systems, than $H(\cdot)$ stands for the Shannon entropy $H(p) = - \sum p_i \log p_i$, where $p = (p_1, p_2, \ldots)$ is the probability distribution vector, while $H(\cdot)$ is the Shannon entropy of the joint probability distribution $p_{ij}$. For quantum systems A and B, function $H(\cdot)$ denotes the von Neumann entropy $H(\rho) = - \text{Tr} \rho \log \rho$ where $\rho$ is the density matrix. In the classical case, we can use the Bayes rule and find an equivalent expression for the mutual information $I(A:B) = H(A) - H(A|B)$ where $H(A|B)$ is the Shannon entropy of A conditioned on the measurement outcome on B. For quantum systems, this quantity is different from the first expression for the mutual information and the difference defines the quantum discord.

Consider a quantum composite system defined by the Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Let dimensions of the local Hilbert spaces be $\dim \mathcal{H}_A = d_A$ and $\dim \mathcal{H}_B = d_B$, while $d = \dim \mathcal{H}_{AB} = d_A d_B$. Given a state $\rho$ (density matrix) of a composite system, the total amount of correlations is quantified by quantum mutual information[17]:

$$I(\rho) = H(\rho_A) + H(\rho_B) - H(\rho),$$

where $H(\rho)$ is the von Neumann entropy and $\rho_{AB} = \text{Tr}_B(\rho)$.
are reduced density matrices. A generalization of the classical conditional entropy is \( H(\rho_{BA}) \), where \( \rho_{BA} \) is the state of \( B \) given a measurement on \( A \). By optimizing over all possible measurements in \( A \), we define an alternative version of the mutual information

\[
Q_A(\rho) = H(\rho_B) - \min_{E_1} \sum_k p_k H(\rho_{B|k}),
\]

where \( \rho_{B|k} = \text{Tr}_A(E_k \otimes \mathbb{1}_B)\rho / \text{Tr}(E_k \otimes \mathbb{1}_B) \) is the state of \( B \) conditioned on outcome \( k \) in \( A \) and \( \{E_k\} \) represents the set of possible operator valued measure elements. The discrepancy between the two measures of information defines the quantum discord:

\[
D_A(\rho) = I(\rho) - Q_A(\rho).
\]

The discord is always non-negative and reaches zero for the classically correlated states. Note that discord is not a symmetric quantity as \( D_A(\rho) \neq D_B(\rho) \). Let us choose basis sets in local Hilbert-Schmidt spaces \( \{A_0\} \text{ and } \{B_0\} \text{ where } n = 1, \ldots, d_A^2 \text{ and } m = 1, \ldots, d_B^2 \). We decompose the state \( \rho \) of composite system into \( \rho = \sum_{i=1}^{d_A} r_{nm} A_i \otimes B_m \). The coefficients \( r_{nm} \) define \( d_A \times d_B \) real matrix \( R \) which we call the correlation matrix. We can find its singular value decomposition (SVD), \( U R W^T = \text{diag}[c_1, c_2, \ldots] \) where \( U \) and \( W \) are \( d_A \times d_A \) and \( d_B \times d_B \) orthogonal matrices, respectively, while \( \text{diag}[c_1, c_2, \ldots] \) is \( d_A \times d_B \) diagonal matrix. SVD defines new basis in local Hilbert-Schmidt spaces \( S_{nm} = \sum_{i=1}^{d_A} U_{ni} A_i \otimes B_m \text{ and } F_m = \sum_{nm} W_{nm} B_m \). The state \( \rho \) in the new basis is of the form \( \rho = \sum_{i=1}^{d_A} r_{nm} S_{nm} \otimes F_m \) where \( L = \text{rank} \rho \) is the rank of correlation matrix \( R \) (the number of non-zero eigenvalues \( c_i \)).

The necessary and sufficient condition becomes

\[
\sum_{k=1}^{d_A} c_k (\sum_k \Pi_k S_{nm} \Pi_k) \otimes F_m = \sum_{i=1}^{L} c_i S_{nm} \otimes F_i
\]

and it is equivalent to the set of conditions:

\[
\sum_k \Pi_k S_{nm} \Pi_k = S_{nm}, \quad n = 1, \ldots, L,
\]

or equivalently \( [S_{nm}, \Pi_k] = 0 \) for all \( k, n \). This means that the set of operators \( \{S_{nm}\} \) have common eigenbasis defined by the set of projectors \( \{\Pi_k\} \). Therefore, the set \( \{\Pi_k\} \) exists if and only if:

\[
[S_{nm}, S_{nl}] = 0, \quad n, m = 1, \ldots, L.
\]

In order to show zero discord we have to check at most \( L(L - 1)/2 \) commutators, where \( L = \text{rank} \rho \leq \min[d_A^2, d_B^2] \). Now, recall that the state of zero discord is of the form \( \rho = \sum_{k=1}^{d_A} p_k \Pi_k \otimes \rho_k \), therefore is a sum of at most \( d_A \) product operators. This bounds the rank of the correlation tensor to \( L \leq d_A \). Thus, the rank of the correlation tensor is the simple discord witness: If \( L > d_A \), the state has a non-zero discord.

Correlation matrix can be obtained directly by simple measurements usually involved in quantum state tomography. However, the detection of non-zero discord does not necessarily require measurement of all \( \{d_A d_B\} \) elements of the correlation matrix (full state tomography). It is sufficient that the experimentalist measures that many elements of the correlation matrix until he finds \( d_A + 1 \) linearly independent rows (or columns) of the correlation matrix.

Geometric measure of discord.— Evaluation of quantum discord given by equation is in general requires considerable numerical minimization. Different measures of quantum discord and their extensions to multipartite systems have been proposed. However, analytical expression are known only for certain classes of states. Here we propose a following geometric measure

\[
D_A^{(2)}(\rho) = \min_{\chi \in \Omega} \|\rho - \chi\|^2,
\]

where \( \Omega \) denotes the set of zero-discord states and \( \|X - Y\|^2 = \text{Tr}(X - Y)^2 \) is the square norm in the Hilbert-Schmidt space. We will show how to evaluate this quantity for an arbitrary two-qubit state.

Two-qubit case.— Consider the case \( \mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2 \). We write a state \( \rho \) in Bloch representation:

\[
\rho = \frac{1}{4} (\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{3} x_i \sigma_i \otimes \mathbb{1} + \sum_{i=1}^{3} y_i \mathbb{1} \otimes \sigma_i + \sum_{i,j=1}^{3} T_{ij} \sigma_i \otimes \sigma_j),
\]

where \( x_i = \text{Tr} \rho (\sigma_i \otimes \mathbb{1}) \), \( y_i = \text{Tr} \rho (\mathbb{1} \otimes \sigma_i) \) are components of the local Bloch vectors, \( T_{ij} = \text{Tr} \rho (\sigma_i \otimes \sigma_j) \) are components of the correlation tensor, and \( \sigma_i, i \in \{1, 2, 3\} \) are the Pauli matrices. To each state \( \rho \) we associate the triple \( \{x, y, T\} \). Now, we characterize the set \( \Omega_0 \). A zero-discord state is of the form \( \chi = p_1 |v_1\rangle \langle v_1| \otimes \rho_1 + p_2 |v_2\rangle \langle v_2| \otimes \rho_2 \), where \( |v_1\rangle, |v_2\rangle \) is a single-qubit orthonormal basis, \( \rho_{1,2} \) are 2 x 2 density matrices,
and $p_{1,2}$ are non-negative numbers such that $p_1 + p_2 = 1$. We define $t = p_1 - p_2$ and three vectors

$$
\vec{c}' = \langle \psi_1 | \hat{c} | \psi_1 \rangle, \quad (10)
$$

$$
\vec{s}'_k = \text{Tr}(p_1 \hat{H} + p_2 \hat{H}) \hat{c}'.
$$

(11)

It can easily be shown that $\vec{c}'$ and $\vec{s}'_k$ represent the local Bloch vectors of the first and second qubit, respectively, while the vector $\vec{s}'$ is directly related to the correlation tensor which is of the product form $T = \vec{c}' \vec{s}'. Therefore, a state of zero-discord $\chi$ has Bloch representation $\vec{\chi}' = \{ t \vec{c}', \vec{s}', \vec{c}' \vec{s}' \}$, where $|t| = 1, \| \vec{s}'_k \| \leq 1$ and $t \in [-1, 1]$. The distance between states $\rho$ and $\chi$ is given by

$$
\| \rho - \chi \|^2 = |\rho| - 2 T \rho \chi + |\chi|^2
$$

$$
= \frac{1}{4}(1 + \|\vec{x}'\|^2 + |\vec{y}'|^2 + |\vec{T}|^2)
$$

$$
- \frac{1}{2} \left(1 + t \vec{c}' \vec{y}' + \vec{x}' \vec{s}' \right)
$$

$$
+ \frac{1}{4} (1 + t^2 + \| \vec{s}'_k \|^2 + \| \vec{s}' \|^2),
$$

where $|\vec{T}|^2 = \text{Tr} T \vec{T}$. First, we optimize the distance over parameters $\vec{s}'_k$ and $t$. The function of equation (12) is convex and quadratic in its variables $t, \vec{s}'_k$. It is straightforward to see that its Hessian is a positive and non-singular matrix. Therefore the function has a unique global minimum. The minimum occurs when the derivative is zero:

$$
\frac{\| \rho - \chi \|^2}{dt} = \frac{1}{2} (- \vec{x}' + t) = 0,
$$

(13)

$$
\frac{\| \rho - \chi \|^2}{d\vec{s}'_k} = \frac{1}{2} (- \vec{y}' + \vec{s}'_k) = 0,
$$

(14)

$$
\frac{\| \rho - \chi \|^2}{d\vec{s}'_k} = \frac{1}{2} (- T \vec{c}' + \vec{s}'_k) = 0,
$$

(15)

which gives the solution $t = \vec{x}' \vec{y}'$, $\vec{s}'_k = \vec{y}'$ and $\vec{s}'_k = T \vec{c}'$. Since the solution lies within the range of parameters, $|\vec{x}'|, |\vec{y}'|, |\vec{T}| \leq 1$ it represents the global minimum. After substituting the solution we obtain $|\rho - \chi|^2 = \frac{1}{4} \left( |\vec{x}'|^2 + |\vec{T}|^2 - \vec{c}' \vec{c}' + T \vec{T} \vec{T} \right)$ which attains the minimum when $\vec{c}'$ is an eigenvector of matrix $K = \vec{x}' \vec{y}' + T \vec{T} \vec{T}$ for the largest eigenvalue. Therefore, we have:

$$
D_A^{(2)}(\rho) = \frac{1}{4} (|\vec{x}'|^2 + |\vec{T}|^2 - k_{\text{max}}),
$$

(16)

where $k_{\text{max}}$ is the largest eigenvalue of matrix $K = \vec{x}' \vec{y}' + T \vec{T} \vec{T}$. Next, we apply our criterion to a class of states.

States with maximally mixed marginals.— We consider an example of two qubit states with maximally mixed marginals. Such a state is locally equivalent (under some local unitary transformation $U_1 \otimes U_2$) to a state $\rho(t) = (\mathbb{I} \otimes I + \sum_{i=1}^3 \tau_i \sigma_i \otimes \sigma_i) / 4$, where $t = (t_1, t_2, t_3)$. The state $\rho(t)$ is physical if $t$ belongs to the tetrahedron (Figure 1) defined by the set of vertices $(-1, -1, -1), (1, 1, 1), (1, -1, 1)$, and $(1, 1, -1)$, while is separable if $t$ belongs to the octahedron defined by the set of vertices $(\pm 1, 0, 0), (0, \pm 1, 0)$ and $(0, 0, \pm 1)$ [22]. Simple calculation shows that $D_A^{(2)}(t) = \frac{1}{4} (t_1^2 + t_2^2 + t_3^2 - \max(t_1^2, t_2^2, t_3^2)).$

FIG. 1. The set of two-qubit states with maximally mixed marginals (i.e. the reduced states of individual qubits are completely mixed). Physical states belong to the tetrahedron, among which separable ones are confined to the octahedron. The zero-discord states are labeled by the red lines (it is therefore clear that almost all states have non-zero discord [13]). The states with maximal value of discord correspond to the vertices of the tetrahedron (the four Bell states). Among the set of separable states, those which maximize discord are the centers of octahedron facets $|z_1, z_1, \pm 1|/3$ (black dots).

The zero-discord states have at most one non-zero component of vector $t$ (Figure 1 red lines). The function $D_A^{(2)}(t)$ reaches its maximal value of $D_A^{(2)} = 1/2$ at the vertices of tetrahedron which represent the four Bell states. Within the set of separable states (octahedron) its maximal value of $D_A^{(2)} = 1/6$ is attained at the centers of octahedron facets $|z_1, z_1, \pm 1|/3$. They represent the states

$$
\rho_{(i1i2)} = \frac{1}{4} (\mathbb{I} \otimes \mathbb{I} + \sum_{k=1}^3 (-1)^k \sigma_k \otimes \sigma_k),
$$

(17)

where $i_k = \pm 1$, and can intuitively be understood as equal mixture of “maximally non-orthogonal” states. The states are symmetric under exchange of subsystems, thus they have the same value of “left” and “right” discord $D_A = D_B$.

DQC1 model.— In [3], Knill and Laflamme introduced the model of mixed-state quantum computing which preforms the task of evaluating the normalized trace of a unitary matrix efficiently. The corresponding quantum circuit is shown in Figure 2. The input state is a highly mixed separable state and consists of a control qubit in the state $\frac{1}{2} (\mathbb{I} + \alpha \sigma_z)$, where $\alpha$ describes the purity, and a collection of $n$ qubits in the maximally mixed state $\frac{1}{2^n} \mathbb{I}_n$, where $\mathbb{I}_n$ is the $n$-qubit identity. The DQC1 circuit consists of the Hadamard gate applied to the control qubit and a control $n$-qubit unitary gate $U_n$. The output state is:

$$
\rho = \frac{1}{2^{n+1}} (\mathbb{I} \otimes \mathbb{I}_n + \alpha |1\rangle \langle 0 | \otimes U_n + \alpha |0\rangle \langle 1 | \otimes U_n^\dagger).
$$

(18)
We consider only the cases $\alpha \neq 0$, otherwise the state at the output is completely mixed and therefore cannot accomplish the task. After measuring the control qubit at the output in the eigenbasis of $\sigma_1$ and $\sigma_2$, we retrieve the normalized trace of the unitary matrix $\tau = Tr U_n / n^2$ with the polynomial overhead scaling $1/n^2$ [10].

The control qubit is completely separable from the rest of the qubits. The output state has vanishingly small entanglement across any bipartite split that groups the control qubit with some of the mixed qubits [3]. However, there is strong evidence that DQC1 task cannot be preformed efficiently using classical computation [9]. The question is what brings a “speed-up” in the considered task? The quantum discord was proposed as a figure of merit for characterizing the resources present in DQC1 model [10]. It has been shown that for almost every unitary matrix $U_n$ (random unitary) the discord in the output state is non-vanishing. Here we derive an explicit condition for characterizing the correlations in the output state and show that the discord is unlikely to be the source of speedup. We re-write it into a form:

$$\rho = \frac{1}{2^{n+1}} \left( |1\rangle \otimes \mathbb{1}_n + \alpha \sigma_1 \otimes \frac{U_n + U_n^\dagger}{2} + \alpha \sigma_2 \otimes \frac{U_n - U_n^\dagger}{2i} \right).$$

Now, we apply the condition (7). The operators $\sigma_1$ and $\sigma_2$ do not commute, therefore, the state $\rho$ is of the zero-discord if and only if the operators $U_n + U_n^\dagger$ and $U_n - U_n^\dagger$ are linearly dependent, or equivalently $U_n^\alpha = k U_n$. This is possible if and only if $U_n = e^{i\theta} A$, where $A^2 = \mathbb{1}$ is a binary operator. For such a unitary all the correlations at the output of DQC1 circuit are classical. However, it is very unlikely that the normalized trace of $e^{i\theta} A$ can be evaluated efficiently on a classical computer, since all it’s eigenvectors can be arbitrarily complex (random states).

We emphasize that our measure of discord is not monotonic under local operations. This, however, is not a shortcoming, as discord, unlike entanglement and mutual information, can in fact increase as well as decrease under local operations (even without the presence of classical correlations). A simple example of the local increase is to start from a zero-discord state $|00\rangle + |11\rangle$ and transform, say the first qubit, so that $|0\rangle \rightarrow |\psi_0\rangle$ and $|1\rangle \rightarrow |\psi_1\rangle$, such that $|\psi_0\rangle$ and $|\psi_1\rangle$ are not orthogonal. The resulting state, $|0\psi_0\rangle (\langle 0 | \psi_0 \rangle + |1\psi_1\rangle \langle 1 | \psi_1 |)$ clearly has a non-vanishing discord. Finally, we point out that our method can be extended to any number of subsystems, though evaluating the measure of discord becomes progressively more difficult with increasing number of subsystems and their dimensionality.

We acknowledge support from the Austrian Science Foundation FWF within Project No. P19570-N16, SFB and CoQuS No. W1210-N16, and the European Commission Project QAP (No. 015848). V.V. acknowledges financial support from the National Research Foundation and Ministry of Education in Singapore and the support of Wolfson College Oxford.

*Note added in proof.—* A related work was done by Datta [23].

---

[1] J. S. Bell, Physics 1, 195 (1964).
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000); M. Hayashi, *Quantum Information: An Introduction* (Springer-Verlag, Berlin, 2006).
[3] E. Knill and R. Laflamme, Phys. Rev. Lett. 81, 5672 (1998).
[4] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. 88, 017901 (2001).
[5] L. Henderson, and V. Vedral, J. Phys. A 34, 6899 (2001).
[6] S. L. Braunstein et al., Phys. Rev. Lett. 83, 1054 (1999).
[7] D. A. Meyer, Phys. Rev. Lett. 85, 2014 (2000).
[8] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A 72, 042316 (2005).
[9] A. Datta, and G. Vidal, Phys. Rev. A 75, 042310 (2007).
[10] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. 100, 050502 (2008).
[11] B. F. Lanyon et al., Phys. Rev. Lett. 101, 200501 (2008).
[12] A. Ferraro et al., Phys. Rev. A 81, 052318 (2010).
[13] A. Shabani, and D.A. Lidar, Phys. Rev. Lett. 102, 100402 (2009).
[14] C. A. Rodriguez-Rosario et al., J. Phys. A: Math. Theor. 41, 205301 (2008).
[15] M. Piani, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. 100, 090502 (2008).
[16] S. Luo, Phys. Rev. A 77, 042303 (2008); R. Dillenschneider, Phys. Rev. B 78, 224413 (2008); M. S. Sarandy, Phys. Rev. A 80, 022108 (2009); M. Ali, A. R. P. Rau, and G. Alber, Phys. Rev. A 81, 042105 (2010); G. Adesso, and A. Datta, Phys. Rev. Lett. 105, 030501 (2010); P. Giorda, and M. G. A. Paris, Phys. Rev. Lett. 105, 020503 (2010).
[17] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A 72, 032317 (2005).
[18] J. Oppenheim et al., Phys. Rev. Lett. 89, 180402 (2002).
[19] K. Modi et al., Phys. Rev. Lett. 104, 080501 (2010).
[20] A. Datta, arXiv:0807.4490 (2008).
[21] A. Brodutch, and D. R. Terno, Phys. Rev. A 81, 062103 (2010).
[22] R. Horodecki, and M. Horodecki, Phys. Rev. A 54, 1838 (1996).
[23] A. Datta, arXiv:1003.5256.