Quantum locking of classical correlations and quantum discord of classical-quantum states

S. Boixo
Department of Chemistry and Chemical Biology, Harvard University,
Cambridge MA, USA
boixocastrillo@fas.harvard.edu

L. Aolita
ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park,
08860 Castelldefels (Barcelona), Spain

D. Cavalcanti
Centre for Quantum Technologies, National University of Singapore, Singapore

K. Modi
Centre for Quantum Technologies, National University of Singapore, Singapore

A. Winter
Department of Mathematics, University of Bristol, Bristol, UK
Centre for Quantum Technologies, National University of Singapore, Singapore

A locking protocol between two parties is as follows: Alice gives an encrypted classical message to Bob which she does not want Bob to be able to read until she gives him the key. If Alice is using classical resources, and she wants to approach unconditional security, then the key and the message must have comparable sizes. But if Alice prepares a quantum state, the size of the key can be comparatively negligible. This effect is called quantum locking. Entanglement does not play a role in this quantum advantage. We show that, in this scenario, the quantum discord quantifies the advantage of the quantum protocol over the corresponding classical one for any classical-quantum state.

Keywords: Quantum discord, entanglement, quantum locking.

1. Introduction

The separation between classical and quantum correlations in a quantum system has puzzled physicists since the early days of quantum information science. The fact that unentangled or separable states can be created by local operations and classical communication lead to the belief that all quantum correlations which are non-classical can be ascribed to entanglement. A bipartite quantum state is
separable or unentangled if it can written in the form

\[ \rho_{AB} = \sum_j p_j \rho_A^{(j)} \otimes \rho_B^{(j)} . \]  

(1)

The subscripts A and B, or Alice and Bob, denote the two parties. In fact, all correlations of separable quantum states are local, i.e. can be explained by classical local-hidden-variable models. Nevertheless, Ollivier and Zurek gave a new measure of non-classical correlations according to which some separable quantum states can contain quantum correlations. For separable states, this comes simply from the possibility of choosing among different non-orthogonal local bases - a typical quantum feature - in the preparation and measurement. The measure proposed by Ollivier and Zurek to quantify these more general quantum correlations is called quantum discord.

Quantum discord has received an astonishingly amount of interest recently, triggered mostly by the possibility of being the reason for the speedup of a quantum computation model (called deterministic quantum computation with one qubit, or DQC1 for short). In the last years, quantum discord has been studied in several contexts like quantum computation, decoherence processes, local broadcasting, open-quantum-system formalism, and quantum phase transitions, just to cite some. Recently, more formal characterizations of quantum discord have been put forward, and it has also been probed in the laboratory. Finally, quantum discord can be related to the difference between the efficiency of quantum and classical Maxwell’s demons, and it has been given information theoretical operational interpretations as the entanglement consumption in an extended quantum state merging protocol and as the markup in the cost of quantum communication in the process of quantum state merging.

\section{Quantum discord and accessible information}

We review now the definition of quantum discord. A good place to start is by reminding ourselves of the information theoretical classical measure of correlations for classical random variables. We associate temporarily to each party Alice and Bob a classical random variable, denoted A and B respectively. Then the amount of correlations in the classical probability distribution \( p(A, B) \) can be measured by the mutual information

\[ I(A; B) = D_{\text{KL}}(p(A, B) \parallel p(A)p(B)), \]  

(2)

where \( p(A) \) and \( p(B) \) are the marginal distributions and \( D_{\text{KL}} \) is the Kullback-Leibler divergence which measures the distance or relative entropy. That is, the mutual information is the distance to the corresponding uncorrelated probability distribution. An equivalent expression for the mutual information is found in terms of the (classical) conditional entropy, which itself has the expression

\[ H(A|B) = \sum_b p(b)H(A|B = b) = H(A, B) - H(B), \]  

(3)
where $H = - \sum_b p(b) \log p(b)$ is the Shannon entropy. The (classical) conditional entropy is the expected value of the entropies of the conditional distribution. The mutual information gets the expression

$$I(A;B) = H(A) - H(A|B) = H(A) + H(B) - H(A, B) ,$$

(4)

The mutual information is then the reduction in the uncertainty of Alice random variable due to the knowledge of Bob’s outcome.\(^{36}\)

Quantum states $\rho_{AB}$ give rise to similar expressions when substituting each Shannon entropy $H(A)$ by the von Neumann entropy $S(\rho_A) = -\text{Tr}\rho_A \log \rho_A$. In what follows we will use the notation $S(A) = S(\rho_A)$ and so forth. The quantum mutual information is

$$I(A;B) = S(A) - S(A|B) = S(A) + S(B) - S(A, B) ,$$

(5)

which is also a measure of the total amount of quantum correlations. Indeed, the quantum mutual information is also the relative entropy between $\rho_{AB}$ and $\rho_A \otimes \rho_B$. Operationally, it can be seen that it corresponds to the minimal rate of randomness that is required to completely erase all the correlations in $\rho_{AB}$.\(^{5}\)

Consider now the following scenario, quite standard in a quantum communication context: Alice produces classical (orthogonal) states $|a\rangle \langle a|$ according to a probability distribution $\{p_a\}$ and communicates with Bob through a quantum channel. Bob wants to know the value or “letter” $a$ that Alice holds. If the transmission channel is perfect, Bob can reliably determine which $|a\rangle \langle a|$ was sent. However, if the channel used to transmit the states introduces errors, Bob will usually get mixed states $\sigma_B(a)$. In this scenario the final quantum state shared between Alice and Bob in the enlarged Hilbert space representation is a classical-quantum state, given by

$$\rho_{cq} = \sum_a p_a |a\rangle \langle a| \otimes \sigma_B(a).$$

(6)

Notice that, because Alice holds a classical system, there is no entanglement involved in this quantum effect. All classical-quantum states are of the form given by Eq. (1).

Assume that Bob now measures his state to obtain information about Alice’s letter. The maximum amount of classical correlations that Bob can obtain about Alice’s letter in the previous scenario is quantified by the accessible information $I_{acc}$.\(^{37}\) This is defined as the maximum mutual information $I(A;B)$ that he can extract from $\rho_{cq}$ by making a measurement $M_B$, i.e.

$$I_{acc}(\rho_{AB}) = \max_{M_B} I(A;B)$$

$$= S(\rho_A) - \min_{M_B} \sum_b p_b S(\rho_{A|b}),$$

(7)

where the state $\rho_{A|b}$ is the state of Alice given that Bob performs a measurement $M_B = \{M_b\}$ in his subsystem and receives outcome $b$, i.e. $\rho_{A|b} = \text{Tr}_B [M_b \rho]/p_b$. The probability of outcome $b$ is given by $p_b = \text{Tr}[\rho M_b]$. Notice that the expected values of the entropies is the conditional information, in accordance with Eq. (3).
At this point, a natural way of defining purely quantum correlations in a quantum state is to subtract the amount of classical correlations accessible to Bob from the total amount of correlations that the state contains. This is precisely how quantum discord is defined: the quantum discord of a bipartite quantum state \( \rho_{AB} \) is
\[
D(\rho_{AB}) = I(A; B) - I_{\text{acc}}(\rho_{AB}).
\]

The corresponding general version of the accessible information (with the same definition, but Alice’s state is not assumed classical) has been proposed as a measure of classical correlations. Quantum discord can also be defined for all quantum states with the same expression \((7)\) (not just classical-quantum states). Interestingly, part of the motivation of the original definition of quantum discord is that the quantum conditional entropy used in Eq. \((5)\) can take negative values, whereas the average conditional entropy of Eq. \((7)\) is always positive. Later the negative values of the quantum conditional information was given an operational interpretation in the quantum state merging protocol, and this plays a key role in the later operational interpretations of quantum discord.

3. Quantum locking of classical correlations

Before stating our main result let us describe the idea of locking classical correlations in quantum systems. We first present the simplest example of this protocol, and calculate the quantum discord in this case. This will help gain intuition and understand better the more general case that we will present later. We should remark that the connection between the quantum discord and quantum locking of classical correlations was suggested in Refs.\(^{10,12}\). Here we will prove that this connection is indeed valid for classical-quantum states.

The protocol is now this: Alice wants to give a message \(a\) to Bob, but wants to keep it secret for the moment. She encrypts the message, and does not want Bob to be able to read it until she gives him the key \(k\). Think of the encrypted mission plans of a war movie. We are interested in unconditional security which, barring a security proof of a more practical encryption protocol, can only mean information theoretical security.

Our aim is to minimize the size of the key. Continuing with the war time analogy, it is very expensive to secure a channel of communication to deliver the key after Bob departs, and every bit counts. How big must the key be if we are limited to using classical resources? Let \(m\) denote the number of bits of Alice’s message. Bob must be able to read the message after receiving the key, and therefore the mutual information between the message and Bob’s quantum state plus key must be \(m\)
\[
I(A; B, K) = m,
\]
where \(K\) is the random variable corresponding to the keys. Using the chain rule for conditional entropies
\[
m = I(A; B, K) = I(A; B) + I(A; K|B).
\]
The conditional mutual information is defined as the mutual information but using conditional entropies, and the chain rule follows directly from this definition. If Alice wants to approach unconditional security then $I(A; B)$ must be negligible. In addition, because at this point we are assuming that Alice and Bob are using classical resources, the conditional mutual information $I(A; K|B)$ is bounded by the size of the key $|K|$. Therefore, the key must be almost as big as the message $m \sim |K|$. For example, in one-time pad a message of $m$ bits is added to a random key of the same length, which hides the message in the (classical) correlations between the key and the message.

The fact that for classical locking of correlations with almost unconditional security we must have $m \sim |K|$ is consistent with the following intuition: one should expect that by the transmission of $l$ bits Alice and Bob cannot increase the correlations by more than $l$ bits. In fact, this is basically the content of the principle of Information Causality, which can be used to explain the Tsirelson bound of the CHSH inequality. This principle basically follows from the chain rule of conditional entropies, as in the derivation above.

The chain rule is indeed obeyed by several measures of correlations, such as the quantum and classical mutual information. Surprisingly, DiVincenzo et al. showed that the accessible information $I_{\text{acc}}$ violates this rule: some states have an arbitrarily large amount of classical correlations unlocked after the exchange of some small amount (even one bit) of communication. This effect became known as quantum locking of classical correlations. In other words, the transmission of $l$ bits results in a much larger increase of the accessible correlations.

We can define the amount of extra correlations as

$$\Delta = I_{\text{acc}}(A, K; B, K) - (I_{\text{acc}}(A, K; B) + |K|).$$

This quantity can be interpreted as follows. The first term, $I_{\text{acc}}(A, K; B, K)$, is the maximum amount of correlations Bob can get if he waits for the communication of the key from Alice to make the measurement in his system. The second term, $I_{\text{acc}}(A, K; B) + |K|$, refers to the maximum amount of correlations that Bob can get if he measures before receiving the key. Thus, $\Delta$ can be thought as the amount of extra correlations that Bob can get if he waits for Alice’s communication due to the quantum unlocking of classical correlations.

*In fact, it is enough that the key is classical. To see this, we can first use the chain rule to write

$$I(A; K|B) = I(AB; K) - I(B; K).$$

The term $I(B; K)$ is positive by subadditivity. The first term, in the general (quantum) case is

$$I(AB; K) = S(K) - S(K|B) \leq |K|.$$
In the simplest case, the state considered by DiVincenzo et al. is:

$$\rho_{AB} = \frac{1}{2^{m+1}} \sum_{a=0}^{2^m-1} \sum_{k=0}^{1} |a, k\rangle \langle a, k|_A \otimes (U_k |a\rangle \langle a| U_k^\dagger)_B,$$

being $U_0 = \mathbb{1}$ and $U_1$ a unitary such that $U_1 |a\rangle$ is a mutually unbiased basis with respect to $|a\rangle$. The accessible information without the key $I_{\text{acc}}(A, K; B)$ is $m/2$ bits, while the accessible information with the key $I_{\text{acc}}(A, K; B, K)$ is $m + 1$. The excess of accessible information $\Delta$ unlocked with the single bit $k$ is $m/2$. The quantum mutual information $I(A, K; B)$ is $m$. The difference between the quantum mutual information and the accessible information without the key, that is, the discord $D(\hat{A}B)$ of the initial state, is also $m/2 = \Delta$. Therefore, the discord of this state, without entanglement, describes the advantage for quantum locking, the difference between the optimal classical increment of shared information, and the one achievable in this protocol. There exist quantum locking protocols that have an arbitrary small amount of prior accessible information, and the rest is unlocked by a small key.

4. Locking and discord of general classical-quantum states

We have just shown that the quantum discord quantifies the amount of extra correlations that Alice and Bob gets if Bob waits until he gets some communication to perform a measurement, if they share the state (12). As we proceed to show now, the same interpretation is valid for more general classical-quantum states. The only difference will be that, in general, Alice and Bob will have to share many copies to attain the quantities $I_q$ and $I_{\text{acc}}$. In other words, we will work in the so-called asymptotic regime.

Let us now show that for any locking protocol that, by design, works with a single copy, the amount of quantum locked correlations is always equal to its quantum discord. Note that, since after receiving the key the message $a$ is completely revealed to Bob we must have

$$I_{\text{acc}}(A, K; B, K) = I_q(A, K; B, K) = m + |K|. \quad (13)$$

On the other hand,

$$I_q(A, K; B, K) \leq I_q(A, K; B) + |K| \leq m + |K|. \quad (14)$$

As explained above, the first inequality comes from the fact that the quantum mutual information can not increase by more than the $|K|$ bits of information being transmitted, while the second is simply a bound on the correlations of the encrypted message $|B| = m$. We thus conclude that

$$I_{\text{acc}}(A, K; B, K) = I_q(A, K; B, K) = I_q(A, K; B) + |K|. \quad (15)$$

Finally, plugging it back in (11), we get

$$\Delta = I_q(A, K; B) - I_{\text{acc}}(A, K; B) = D(\hat{A}B) \quad (16)$$
which is nothing but the quantum discord.

For the general classical-quantum state we point out that asymptotically (in the limit of many copies), the discord of a CQ state is always equal to the advantage of quantum locking. This can be seen from the classical data compression with quantum side information result of Ref. 42, which builds upon the product classical information capacity of a noisy quantum channel (HSW)\textsuperscript{43,44}. We only give the intuition here and refer to Ref. 42 and references therein for the details.

The intuition for the HSW result is the same as for Shannon’s noisy channel coding theorem. Alice builds a quantum code by randomly choosing a subset of size $2^{nR}$ of strings of size $n$ generated according to some distribution $A$. For each input letter $a$, Bob gets output $\sigma_B^{(a)} = E(\rho_a)$, where $\rho_a$ is part of the quantum code construction. The rate of the code is $R$. Denote by $a^n$ a possible input of size $n$, and by $\sigma_B^{(a^n)}$ the corresponding output. The dimension of the subspace of typical sequences for the output of the channel on Bob’s size goes like $2^{nS(B)}$. In average, the dimension of the subspace corresponding to the conditional typical output sequences (taking into account the channel noise) goes like $2^{nS(B|A)}$. That is, in average, the number of outputs for each input is $2^{nS(B|A)}$. The size of the subset of inputs in the quantum code, given by the rate $R$, must be such that we can identify the code word corresponding to the output, so we must assign a subspace of dimension $2^{nS(B|A)}$, out of the total $2^{nS(B)}$, for each code word. That is, the rate must obey

$$2^{nR} \approx 2^{nS(B)} / 2^{nS(B|A)} = 2^{n(S(B) - S(B|A))} = 2^{nI(A;B)}.$$\hspace{1cm} (17)

This is the content of the HSW theorem: the product classical information capacity of a noisy quantum channel is given by the mutual information $I(A;B)$.

With this background, we can approach the content of Ref. 42. The question is, for a CQ state, how many quantum codes are necessary to cover the typical sequences of $n$ copies? There are $2^{nS(A)}$ typical sequences in Alice’s side, and a quantum code, by the HSW theorem, has size $2^{nI(A;B)}$, so the number of necessary quantum codes is $2^n(S(A) - I(A;B)) = 2^{nS(A|B)}$. Then Alice sends only information identifying the quantum code, $S(A|B)$ bits per copy of the CQ state, and Bob measures with that code, obtaining Alice’s complete message.

When Bob is forced to measure each copy of the output state before Alice sends the key, the amount of information unknown to Bob is quantified by Alice’s entropy conditional on Bob’s measurement outcome, that is, $\min_{M_B} \sum_b p_b S(\rho_{A|b})$. Because Bob measurement turns the quantum state into a classical random variable, the optimal choice of measurement for the accessible information also defines a corresponding classical protocol. The number of bits that Alice must send to Bob in this case is $\min_{M_B} \sum_b p_b S(\rho_{A|b})$. We have seen that, using quantum codes, Alice must send only $S(A|B)$ bits. The difference is the quantum advantage for quantum
locking, quantified by the discord $D(\hat{AB})$ for CQ states

$$D(\hat{AB}) = I(A; B) - I_{\text{acc}}(A; B) = \min_{M_B} \sum_b p_b S(\rho_{A|b}) - S(A|B).$$

(18)

5. Conclusions

For a classical-quantum state, the difference between the accessible correlations and the quantum correlations gives a measure of purely quantum correlations, called quantum discord. This is despite the fact that the quantum state is separable and, therefore, admits a local hidden variable description. These purely quantum correlations are the source of the quantum advantage of a quantum locking protocol. In the simplest case, Alice encrypts her message in the choice of basis (as in the BB84 cryptographic protocol\textsuperscript{45}). If Alice then announces the choice of basis to Bob, he can perform a measurement which unambiguously identifies the encrypted message.

For a general classical-quantum state, the state $\rho_{AB}^\otimes n$ also has the property of being decomposable into subensembles with mutually orthogonal elements in the asymptotic limit. In both cases, quantum discord quantifies the quantum advantage. This also points towards a relation of discord to some quantum cryptography protocols.

Acknowledgments

Part of this work was done while SB was at the Institute for Quantum Information at the California Institute of Technology. This work was supported by the National Research Foundation, the Ministry of Education of Singapore, the Spanish “Juan de la Cierva” Programme, the Royal Society, U.K. EPSRC, the European Commission, ERC and the Philip Leverhulme Trust.

References

1. R. F. Werner, *Phys. Rev. A* **40** (October 1989) p. 4277.
2. W. H. Zurek, *Annalen der Physik (Leipzig)* **9** (2000) p. 853.
3. H. Ollivier and W. Zurek, *Phys. Rev. Lett.* **88** (Jan 2001) p. 017901.
4. L. Henderson and V. Vedral, *J. Phys. A: Math. Gen.* **34** (2001) 6899.
5. B. Groisman, S. Popescu and A. Winter, *Phys. Rev. A* **72** (Sep 2005) p. 032317.
6. N. Li and S. Luo, *Phys. Rev. A* **76** (2007) p. 032327.
7. D. Kaszlikowski, A. Sen(De), U. Sen, V. Vedral and A. Winter, *Phys. Rev. Lett.* **101** (2008) p. 070502.
8. C. H. Bennett, A. Grudka, M. Horodecki, P. Horodecki and R. Horodecki, *Phys. Rev. A* **83** (January 2011) p. 012312.
9. S. Luo, *Phys. Rev. A* **77** (February 2008) p. 022301.
10. S. Wu, U. V. Poulsen and K. Mølmer, *Phys. Rev. A* **80** (2009) p. 032319.
11. A. Datta, A. Shaji and C. Caves, *Phys. Rev. Lett.* **100** (2008) p. 050502.
12. A. Datta and S. Gharibian, *Phys. Rev. A* **79** (April 2009) p. 042325.
13. A. Ferraro, L. Aolita, D. Cavalcanti, F. M. Cucchietti and A. Acín, *Phys. Rev. A* **81** (2010) p. 052318.
14. T. Werlang, S. Souza, F. F. Fanchini and C. J. Villas-Boas, *Phys. Rev. A* **80** (2009) p. 024103.
15. J. Maziero, L. C. Celeri, R. M. Serra and V. Vedral, *Phys. Rev. A* **80** (2009) p. 044102.
16. M. Piani, P. Horodecki and R. Horodecki, *Phys. Rev. Lett.* **100** (2008) p. 090502.
17. C. A. Rodriguez-Rosario, K. Modi, A.-M. Kuah, A. Shaji and E. C. G. Sudarshan, *J. Phys. A: Math. Gen.* **41** (2008) p. 205301.
18. A. Shabani and D. A. Lidar, *Phys. Rev. Lett.* **102** (March 2009) p. 100402.
19. M. S. Sarandy, *Phys. Rev. A* **80** (2009) p. 022108.
20. J. Maziero, H. C. Guzman, L. C. Céleri, M. S. Sarandy and R. M. Serra, *Phys. Rev. A* **82** (July 2010) p. 012106.
21. S. Luo, *Phys. Rev. A* **77** (April 2008) p. 042303.
22. K. Modi, T. Paterek, W. Son, V. Vedral and M. Williamson, *Phys. Rev. Lett.* **104** (2010) p. 080501.
23. P. Giorda and M. G. A. Paris, *Phys. Rev. Lett.* **105** (2010) p. 020503.
24. G. Adesso and A. Datta, *Phys. Rev. Lett.* **105** (2010) p. 030501.
25. L. Mazzola, J. Piilo and S. Maniscalco, *Phys. Rev. Lett.* **104** (2010) p. 200401.
26. F. F. Fanchini, T. Werlang, C. A. Brasil, L. G. E. Arruda and A. O. Caldeira, *Phys. Rev. A* **81** (2010) p. 052107.
27. B. Dakić, V. Vedral and v. Brukner, *Phys. Rev. Lett.* **105** (Nov 2010) p. 190502.
28. A. Datta, *arXiv:1003.5256* (2010)
29. E. Knill and R. Laflamme, *Phys. Rev. Lett.* **81** (December 1998) p. 5672.
30. B. P. Lanyon, M. Barbieri, M. P. Almeida and A. G. White, *Phys. Rev. Lett.* **101** (2008) p. 200501.
31. J.-S. Xu et al., *Nat. Comm.* **1** (2010) p. 7.
32. W. H. Zurek, *Phys. Rev. A* **67** (January 2003) p. 012320.
33. A. Brodutch and D. R. Terno, *Phys. Rev. A* **81** (June 2010) p. 062103.
34. D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani and A. Winter, *Phys. Rev. A* **83** (March 2011) p. 032324.
35. V. Madhok and A. Datta, *Phys. Rev. A* **83** (March 2011) p. 032323.
36. T. M. Cover and J. A. Thomas, *Elements of information theory* (John Wiley and Sons, 2006).
37. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
38. M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter and M. Zukowski, *Nature* **461** (October 2009) 1101.
39. D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin and B. M. Terhal, *Phys. Rev. Lett.* **92** (2003) p. 067902.
40. P. Hayden, D. Leung, P. W. Shor and A. Winter, *Comm. Math. Phys.* **250** (2004) p. 371.
41. O. Fawzi, P. Hayden and P. Sen, *arXiv:1010.3007* (October 2010)
REFERENCES

42. I. Devetak and A. Winter, *Phys. Rev. A* **68** (2003) p. 42301.
43. A. S. Holevo, *Probl. Inf. Transm.* **9** (1973) p. 177.
44. B. Schumacher and M. D. Westmoreland, *Phys. Rev. A* **56** (July 1997) p. 131.
45. C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in *Proc. IEEE Int. Conf. Computers, systems and Signal Processing*, 1984, p. 175.