Quantum Information Causality

Damián Pitalúa-García
Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, United Kingdom
(Received 7 October 2012; revised manuscript received 11 March 2013; published 22 May 2013)

How much information can a transmitted physical system fundamentally communicate? We introduce the principle of quantum information causality, which states the maximum amount of quantum information that a quantum system can communicate as a function of its dimension, independently of any previously shared quantum physical resources. We present a new quantum information task, whose success probability is upper bounded by the new principle, and show that an optimal strategy to perform it combines the quantum teleportation and superdense coding protocols with a task that has classical inputs.

DOI: 10.1103/PhysRevLett.110.210402 PACS numbers: 03.65.Ta, 03.67.Ac, 03.67.Bg, 03.67.Hk

Quantum information science studies how information can fundamentally be encoded, processed, and communicated via systems described by quantum physics [1]. Interesting features of information arise with this approach. The no-cloning theorem states that unknown quantum states cannot be copied perfectly [2,3]. Unknown quantum states can be teleported [4]. Two classical bits can be encoded in one qubit via the superdense coding protocol [5]. Fundamentally secure cryptography can be achieved with quantum information protocols [6–8]. Many of the quantum information protocols are possible due to quantum entanglement: two systems are entangled if their global quantum state cannot be expressed as a convex combination of individual states in a tensor product form. Another interesting property is quantum nonlocality, that is, measurement outcomes of separate systems can exhibit correlations that cannot be described by local classical models [9,10].

Since the value of quantum correlations does not vary with the time difference of the measurements and the distance between the systems, one could think that they can be used to communicate arbitrarily fast messages. However, quantum physics obeys the no-signaling principle. No-signaling says that a measurement outcome obtained by a party (Bob) does not provide him with any information about what measurement is performed by another party (Alice) at a distant location, despite any nonlocal correlations previously shared by them [11].

If any information that Alice has is to be learned by Bob, no-signaling requires that a physical system sharing correlations with Alice's system must be transmitted to him. Thus, an interesting question to ask is, how much information can a physical system fundamentally communicate? In the scenario in which Alice has a classical random variable X, she encodes its value in a quantum state that she sends Bob and Bob applies a quantum measurement on the received state in order to obtain a classical random variable Y as the output, the Holevo theorem [12] provides an upper bound on the classical mutual information between X and Y. In the scenario in which Alice sends Bob m classical bits, information causality states that the increase of the mutual information between Bob's and Alice's systems is upper bounded by m, independently of any no-signaling physical resources that Alice and Bob previously shared [13]. Information causality has important implications for the set of quantum correlations [13–17]. For example, it implies the Cirel'son bound [18], while the no-signaling principle does not [19].

Here we consider the scenario in which Bob receives a quantum system from Alice, who possibly shares quantum correlations with another party, Charlie, and ask the question, how much quantum information can Bob obtain about Alice's or Charlie's data [20]? We introduce a new principle that we call quantum information causality, which states that the maximum amount of quantum information that a quantum system can communicate is limited by its dimension, independently of any quantum physical resources previously shared by the communicating parties. Namely, the principle says that the increase of the quantum mutual information between Bob's and Charlie's systems, after a quantum system of m qubits is transmitted from Alice to Bob, is upper bounded by $2m$.

In order to illustrate quantum information causality, we introduce a new quantum task that we call the quantum information causality (QIC) game (see Fig. 1).

The QIC game (version I).—Initially, Alice and Bob may share an arbitrary entangled state. However, they do not share any correlations with Charlie. Let A' and B denote the quantum systems at Alice's and Bob's locations,

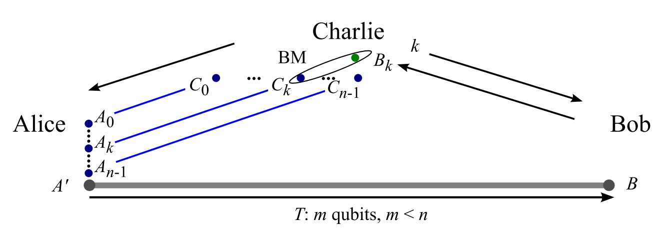

FIG. 1 (color online). The QIC game (version I).

respectively. Charlie prepares the qubits A_j and C_j in the singlet state $|\Psi^-\rangle$, for $j = 0, 1, \ldots, n-1$. Charlie keeps the system $C \equiv C_0 C_1 \ldots C_{n-1}$ and sends Alice the system $A \equiv A_0 A_1 \ldots A_{n-1}$. Charlie generates a random integer $k \in \{0, 1, \ldots, n-1\}$ and gives it to Bob. Bob gives Charlie a qubit B_k, whose joint state with the qubit C_k, denoted as ω_k, must be as close as possible to the singlet. Alice and Bob may play any strategy allowed by quantum physics as long as the following constraint is satisfied: their communication is limited to a single message from Alice to Bob only, encoded in a quantum system T of $m < n$ qubits, with no extra classical communication allowed. Let B' denote the joint system BT after Bob's quantum operations. In general, the qubit B_k is obtained by Bob from B'. Charlie applies a Bell measurement (BM) on the joint system $C_k B_k$. Alice and Bob win the game if Charlie obtains the outcome corresponding to the singlet. The success probability is

$$P \equiv \frac{1}{n} \sum_{k=0}^{n-1} \langle \Psi^- | \omega_k | \Psi^- \rangle. \tag{1}$$

In version II of the QIC game, Charlie does not prepare singlets. Instead, Charlie prepares n qubits in the pure states $\{|\psi_j\rangle\}_{j=0}^{n-1}$ that he gives Alice. Bob outputs a qubit B_k in the state ρ_k. Charlie measures B_k in the orthonormal basis $\{|\psi_k\rangle, |\psi_k^{\perp}\rangle\}$. Alice and Bob win the game if Charlie's outcome corresponds to the state $|\psi_k\rangle$. This version is equivalent to version I and its success probability p satisfies $p = (1 + 2P)/3$ (see details in the Supplemental Material [23]). For convenience, in what follows we only refer to version I of the QIC game, unless otherwise stated.

Consider the following *naive* strategy to play the QIC game. Alice simply sends Bob m of the n received qubits from Charlie without applying any operations on these. Alice and Bob previously agree on which qubits Alice would send Bob, for example, those with index $0 \leq j < m$. If Bob receives from Charlie a number $k < m$, he outputs the correct state; in this case, $\langle \Psi^- | \omega_k | \Psi^- \rangle = 1$. However, if $m \leq k$, Bob does not have the correct state; hence, he can only give Charlie a fixed state, say $|0\rangle$; in this case, $\langle \Psi^- | \omega_k | \Psi^- \rangle = 1/4$. Thus, this strategy succeeds with probability $P_{\mathrm{N}} = (1 + 3m/n)/4$, where the label N stands for naive. There are other strategies that achieve success probabilities higher than P_{N}. However, it turns out that in general, $P < 1$, if $m < n$. We show that this follows from quantum information causality.

The principle of quantum information causality states an upper bound on the amount of quantum information that m qubits can communicate:

$$\Delta I(C{:}B) \leq 2m, \tag{2}$$

where $\Delta I(C{:}B) \equiv I(C{:}B') - I(C{:}B)$ is Bob's gain of quantum information about C, $I(C{:}B) \equiv S(C) + S(B) - S(CB)$ is the quantum mutual information [1] between C and B, $S(C)$ is the von Neumann entropy [1] of C, etc., B' denotes the joint system BT after Bob's quantum operations. Since the quantum mutual information quantifies the total correlations between two quantum systems [24–26], we consider $\Delta I(C{:}B)$ to be a good measure for the communicated quantum information [27].

The proof is very simple. By definition, $I(C{:}BT) = S(C) + S(BT) - S(CBT)$. Subadditivity [29] states that $S(BT) \leq S(B) + S(T)$. The triangle inequality [30], $|S(CB) - S(T)| \leq S(CBT)$, implies that $-S(CBT) \leq S(T) - S(CB)$. Hence, we have that $I(C{:}BT) \leq 2S(T) + I(C{:}B)$. The data-processing inequality states that local operations cannot increase the quantum mutual information [1]. Thus, $I(C{:}B') \leq I(C{:}BT)$, which implies that $I(C{:}B') \leq 2S(T) + I(C{:}B)$. Therefore, we obtain that $\Delta I(C{:}B) \leq 2S(T)$. Finally, since $S(T) \leq \log_2(\dim T)$, the quantum information that T can communicate is limited by its dimension. Therefore, if T is a system of m qubits, Eq. (2) follows because in this case $S(T) \leq m$. Achievability of equality in Eq. (2) requires that T is maximally entangled with C (see details in the Supplemental Material [23]). It is easy to see that the naive strategy in the QIC game saturates this bound.

We notice that in the previous proof we did not require to mention Alice's system. This means that Eq. (2) is valid independently of how much entanglement Alice and Bob share. This also means that Eq. (2) is valid too if we consider that Alice and Charlie are actually the same party. Thus, quantum information causality shows that the maximum possible increase of the quantum mutual information between Charlie's and Bob's systems is only a function of the dimension of the system T received by Bob, independently of whether it is Alice or Charlie who sends Bob the system T and of how much entanglement Bob shares with them.

If the transmitted system T is classical, equality in Eq. (2) cannot be achieved. Information causality states that in this case, $\Delta I(C{:}B) \leq m$, where C is a classical system, B is a quantum system, and $I(C{:}B)$ denotes their quantum mutual information [13]. In fact, this bound is valid even if both systems C and B are quantum (see details in the Supplemental Material [23]).

As stated above, quantum information causality follows from three properties of the von Neumann entropy: subadditivity, the data-processing, and the triangle inequalities. The concept of entropy in mathematical frameworks for general probabilistic theories [31–33] and its implication for information causality have been recently investigated [34–37]. Particularly, it has been shown that a physical condition on the measure of entropy implies subadditivity and the data-processing inequality, and hence that information causality follows from this condition [36]. It would be interesting to investigate whether physically sensible definitions of entropy for more general probabilistic theories satisfy the three mentioned properties, and hence a generalized version of quantum information causality. A different version of information causality in more general probabilistic theories has been considered in Ref. [38].

Quantum information causality implies an upper bound on the success probability in the QIC game:

$$P \leq P', \tag{3}$$

where we define P' to be the maximum solution of the equation $h(P') + (1 - P')\log_2 3 = 2(1 - m/n)$ and $h(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$ denotes the binary entropy. The value of P' is a strictly increasing function of the ratio m/n, achieving $P' = 1/4$ if $m = 0$ and $P' = 1$ if $m = n$. Therefore, we have that $P < 1$ if $m < n$. A plot with some values of P' and the complete proof of Eq. (3) are given in the Supplemental Material [23]. Below we present a sketch of the proof.

First, we notice that for any strategy that Alice and Bob may play that achieves success probability P, there exists a covariant strategy achieving the same value of P that Alice and Bob can perform. By covariance, we mean the following: in version II of the QIC game, if, when Alice's input qubit A_k is in the state $|\psi_k\rangle$, Bob's output qubit state is ρ_k, then, when A_k is in the state $U|\psi_k\rangle$, Bob's output state is $U\rho_k U^\dagger$, for any qubit state $|\psi_k\rangle \in \mathbb{C}^2$ and unitary operation $U \in SU(2)$. Recall that k is the number that Charlie gives Bob. Therefore, without loss of generality, we consider that a covariant strategy is implemented. This means that the Bloch sphere of the qubit A_k is contracted uniformly and output in the qubit B_k. In version I, this means that the joint system $C_k B_k$ is transformed into the state

$$\omega_k = \lambda_k \Psi^- + \frac{1 - \lambda_k}{3}(\Psi^+ + \Phi^+ + \Phi^-), \tag{4}$$

where $1/4 \leq \lambda_k \leq 1$ and Ψ^- denotes $|\Psi^-\rangle\langle\Psi^-|$, etc. That is, the depolarizing map [1] is applied to the qubit A_k, and output by Bob in the qubit B_k.

Then, we use the data-processing inequality and the fact that the qubits C_j and $C_{j'}$ are in a product state for every $j \neq j'$ in order to show that $\sum_{k=0}^{n-1} I(C_k{:}B_k) \leq I(C{:}B')$. We notice that since Charlie's and Bob's systems are initially uncorrelated, Eq. (2) reduces to $I(C{:}B') \leq 2m$. Thus, we have that $\sum_{k=0}^{n-1} I(C_k{:}B_k) \leq 2m$. From this inequality and the concavity property of the von Neumann entropy, we obtain an upper bound on $\sum_{k=0}^{n-1} \lambda_k/n$, which from Eqs. (1) and (4) equals P.

Below we show that an optimal strategy to play the QIC game reduces to an optimal strategy to perform the following task.

The IC-2 game.—Alice is given random numbers $x_j \equiv (x_j^0, x_j^1)$, where $x_j^0, x_j^1 \in \{0, 1\}$, for $j = 0, 1, \ldots, n - 1$. Bob is given a random value of $k = 0, 1, \ldots, n - 1$. The game's goal is that Bob outputs x_k. Alice and Bob can perform any strategy allowed by quantum physics with the only condition that communication is limited to a single message of $2m < 2n$ bits from Alice to Bob. In particular, Alice and Bob may share an arbitrary entangled state. Let $y_k \equiv (y_k^0, y_k^1)$ be Bob's output, where $y_k^0, y_k^1 \in \{0, 1\}$. We define the success probability as

$$Q \equiv \frac{1}{n}\sum_{k=0}^{n-1} P(y_k = x_k). \tag{5}$$

We call this task the IC-2 game. The version we call the IC-1 game, in which the inputs and output are one bit values and Alice's message is of $m < n$ bits, was considered in the Letter that introduced information causality [13]. The strategies to play the IC-1 game in which no entanglement is used were first considered by Wiesner in 1983 with the name of conjugate coding [39]. They were investigated further in 2002 with the name of random access codes [40]. The most general quantum strategy, in which Alice and Bob share an arbitrary entangled state, is called an entanglement-assisted random access code [41].

Let $Q_{\max}$ be the maximum value of Q over all possible strategies to play the IC-2 game. Below we show that $P \leq Q_{\max}$.

Consider the following strategy to play the IC-2 game. Alice and Bob initially share a singlet state in the qubits A_j and C_j, for $j = 0, 1, \ldots, n - 1$. Alice has the system $A \equiv A_0 A_1 \ldots A_{n-1}$, while Bob has the system $C \equiv C_0 C_1 \ldots C_{n-1}$. Alice applies the unitary operation σ_{x_j} on the qubit A_j, for every j, where $\sigma_{0,0} \equiv I$ is the identity operator acting on $\mathbb{C}^2$ and $\sigma_{0,1} \equiv \sigma_1$, $\sigma_{1,0} \equiv \sigma_2$, $\sigma_{1,1} \equiv \sigma_3$ are the Pauli matrices. Then, Alice and Bob play the QIC game, applying some operation on the input system A, which includes a message of m qubits from Alice to Bob. However, instead of sending these m qubits directly, Alice teleports [4] them to Bob. Thus, communication consists of $2m$ bits only, as required. At this stage, Bob does not apply any operations on the system C, which is consistent with the QIC game. As previously indicated, we can consider that in a general strategy in the QIC game the depolarizing map is applied to the qubit A_k. Therefore, Bob outputs the qubit B_k in the joint state $\Omega_k = (I \otimes \sigma_{x_k})\omega_k(I \otimes \sigma_{x_k})$ with the qubit C_k, where ω_k is given by Eq. (4). Then, Bob measures Ω_k in the Bell basis. Bob learns the encoded value x_k with probability λ_k. Thus, from Eq. (5) we have that $Q = \sum_{k=0}^{n-1} \lambda_k/n$, which equals P, as we can see from Eqs. (1) and (4). Since by definition $Q \leq Q_{\max}$, we have that $P \leq Q_{\max}$, as claimed.

Consider the following class of strategies to play the QIC game that combine quantum teleportation [4], superdense coding [5], and the IC-2 game.

Teleportation strategies in the QIC game.—Alice and Bob share a singlet state in the qubits A'_j, at Alice's site, and B_j, at Bob's site, for $j = 0, 1, \ldots, n - 1$. Alice applies a Bell measurement on her qubits $A_j A'_j$ and obtains the two bit outcome $x_j \equiv (x_j^0, x_j^1)$. Thus, the state of the qubit A_j is teleported to Bob's qubit B_j, up to the Pauli error σ_{x_j}. This means that the joint state of the system C_jB_j transforms into one of the four Bell states, according to the value of x_j. Alice and Bob play the IC-2 game with Alice's and Bob's inputs being $x \equiv (x_0, x_1, \ldots, x_{n-1})$ and k, respectively. However, instead of sending Bob the $2m$-bits message directly, Alice encodes it in m qubits via superdense coding. Bob receives the m qubits and decodes the correct $2m$-bits message, which he inputs to his part of the IC-2 game. Bob outputs the two bit number $y_k \equiv (y_k^0, y_k^1)$ and applies the Pauli correction operation σ_{y_k} on the qubit B_k, which then he outputs and gives to Charlie. If $y_k = x_k$, the output state ω_k of the system C_kB_k is the singlet; otherwise, we have that $\langle\Psi^-|\omega_k|\Psi^-\rangle = 0$. Thus, from the definition of P, Eq. (1), we see that $P = Q$, where Q is given by Eq. (5).

Therefore, since $P \leq Q_{\max}$, we see that an optimal strategy in the QIC game is a teleportation strategy in which the IC-2 game is played achieving the maximum success probability $Q = Q_{\max}$. We have obtained an upper bound on Q for a particular class of strategies in the case $m = 1$ (see Supplemental Material [23]).

The best strategy that we have found to play the QIC game in the case $m = 1$ is a teleportation strategy in which the IC-2 game is played with two equivalent and independent protocols in the IC-1 game. In both protocols Bob inputs the number k, while Alice inputs the bits $\{x_j^0\}_{j=0}^{n-1}$ in the first protocol and the bits $\{x_j^1\}_{j=0}^{n-1}$ in the second one. If Bob outputs the correct value of x_k^0 with probability q in the first protocol, and similarly, he outputs the correct value of x_k^1 with probability q in the second protocol, for any k, then the success probability in the IC-2 game is $Q = q^2$. The maximum value of q that has been shown [36,41] is $q = (1 + n^{-1/2})/2$. Explicit strategies to achieve this value are given by entanglement-assisted random access codes in the case in which $n = 2^r3^l$ and r, l are non-negative integers [41]. With this value of Q we achieve a success probability in the QIC game of $P_{\mathrm{T}} = (1 + n^{-1/2})^2/4$, where the label T stands for teleportation.

Here we have introduced the quantum information causality principle as satisfaction of an upper bound on the quantum information that Bob can gain about Charlie's data as a function of the number of qubits m that Alice (who shares correlations with Charlie) sends Bob, Eq. (2). We have presented a new quantum information task, the QIC game, whose success probability is limited by quantum information causality, Eq. (3). We have shown that an optimal strategy to play the QIC game combines the quantum teleportation and the quantum superdense coding protocols, with an optimal strategy to perform another task that has classical inputs, the IC-2 game. An optimal strategy in the IC-2 game remains as an interesting open problem.

I would like to thank Adrian Kent for much assistance with this work, and Nilanjana Datta, Sabri Al-Safi, Tony Short, and Min-Hsiu Hsieh for helpful discussions. I acknowledge financial support from CONACYT México and partial support from Gobierno de Veracruz.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[3] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[6] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984) p. 175.
[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[8] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[9] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[10] J. S. Bell, Physics **1**, 195 (1964).
[11] G. C. Ghirardi, A. Rimini, and T. Weber, Lett. Nuovo Cimento Soc. Ital. Fis. **27**, 293 (1980).
[12] A. S. Kholevo, Probl. Peredachi Inf. **9**, 3 (1973) [Probl. Inf. Transm. **9**, 177 (1973)].
[13] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature (London) **461**, 1101 (2009).
[14] J. Allcock, N. Brunner, M. Pawłowski, and V. Scarani, Phys. Rev. A **80**, 040103 (2009).
[15] D. Cavalcanti, A. Salles, and V. Scarani, Nat. Commun. **1**, 136 (2010).
[16] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, Phys. Rev. Lett. **107**, 210403 (2011).
[17] T. H. Yang, D. Cavalcanti, M. L. Almeida, C. Teo, and V. Scarani, New J. Phys. **14**, 013061 (2012).
[18] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[19] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[20] A different question, investigated in Refs. [21,22], is how much entanglement can increase under local operations and quantum communication.
[21] T. K. Chuan, J. Maillard, K. Modi, T. Paterek, M. Paternostro, and M. Piani, Phys. Rev. Lett. **109**, 070501 (2012).
[22] A. Streltsov, H. Kampermann, and D. Bruß, Phys. Rev. Lett. **108**, 250501 (2012).
[23] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.110.210402 for the proofs of some of the technical results mentioned in the main text.

[24] L. Henderson and V. Vedral, J. Phys. A: Math. Gen. **34**, 6899 (2001).
[25] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[26] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).
[27] Note that Refs. [24–26] propose measures for the purely classical and purely quantum parts of the correlations between two quantum systems, whose sum is equal to the quantum mutual information (see Ref. [28] for a review). We do not consider such a classification in our discussion.
[28] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655 (2012).
[29] O. E. Lanford and D. W. Robinson, J. Math. Phys. (N.Y.) **9**, 1120 (1968).
[30] H. Araki and E. H. Lieb, Commun. Math. Phys. **18**, 160 (1970).
[31] L. Hardy, arXiv:quant-ph/0101012.
[32] J. Barrett, Phys. Rev. A **75**, 032304 (2007).
[33] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, Phys. Rev. Lett. **99**, 240501 (2007).
[34] A. J. Short and S. Wehner, New J. Phys. **12**, 033023 (2010).
[35] H. Barnum, J. Barrett, L. O. Clark, M. Leifer, R. Spekkens, N. Stepanik, A. Wilce, and R. Wilke, New J. Phys. **12**, 033024 (2010).
[36] S. W. Al-Safi and A. J. Short, Phys. Rev. A **84**, 042323 (2011).
[37] O. C. O. Dahlsten, D. Lercher, and R. Renner, New J. Phys. **14**, 063024 (2012).
[38] L. Masanes, M. P. Mueller, R. Augusiak, and D. Perez-Garcia, arXiv:1208.0493.
[39] S. Wiesner, SIGACT News **15**, 78 (1983).
[40] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 496 (2002).
[41] M. Pawłowski and M. Żukowski, Phys. Rev. A **81**, 042326 (2010).