

## Locking Classical Correlations in Quantum States

David P. DiVincenzo,<sup>1,2</sup> Michał Horodecki,<sup>3</sup> Debbie W. Leung,<sup>1,2,4</sup> John A. Smolin,<sup>1</sup> and Barbara M. Terhal<sup>1,2</sup>

<sup>1</sup>*IBM Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598, USA*

<sup>2</sup>*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125-8100, USA*

<sup>3</sup>*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

<sup>4</sup>*Mathematical Science Research Institute, 1000 Centennial Drive, Berkeley, California 94720, USA*

(Received 13 March 2003; published 12 February 2004)

We show that there exist bipartite quantum states which contain a large locked classical correlation that is unlocked by a disproportionately small amount of classical communication. In particular, there are  $(2n + 1)$ -qubit states for which a one-bit message doubles the optimal classical mutual information between measurement results on the subsystems, from  $n/2$  bits to  $n$  bits. This phenomenon is impossible classically. However, states exhibiting this behavior need not be entangled. We study the range of states exhibiting this phenomenon and bound its magnitude.

DOI: 10.1103/PhysRevLett.92.067902

PACS numbers: 03.67.-a

The study of possible correlations between quantum systems was initiated by Einstein, Podolsky, and Rosen [1] and Schrödinger [2]. These pioneers were concerned with entanglement—quantum correlations that are non-existent in classical physics. Recent development in quantum information theory has motivated extensive study of entanglement (see [3] for a review). Furthermore, an exciting subject of characterizing other interesting types of correlations has emerged. For example, correlation that is purely quantum, purely classical, or mixed quantum and classical, has been studied [4–8].

The classical mutual information of a quantum state  $\rho_{AB}$  can be defined naturally [8] as the maximum classical mutual information that can be obtained by local measurements  $M_A \otimes M_B$  on the state  $\rho_{AB}$ :

$$I_c(\rho) \equiv \max_{M_A \otimes M_B} I(A:B). \quad (1)$$

Here  $I(A:B)$  is the classical mutual information defined as  $I(A:B) \equiv H(p_A) + H(p_B) - H(p_{AB})$ ,  $H$  is the entropy function [9], and  $p_{AB}$ ,  $p_A$ ,  $p_B$  are the probability distributions of the joint and individual outcomes of performing the local measurement  $M_A \otimes M_B$  on  $\rho$ . The physical relevance of  $I_c$  is manifold. First,  $I_c(\rho)$  is the maximum classical correlation obtainable from  $\rho$  by purely local processing. Second,  $I_c(\rho)$  corresponds to the usual classical mutual information when  $\rho$  is “classical,” i.e., diagonal in some local product basis and corresponds to a classical distribution. Third, when  $\rho$  is pure,  $I_c(\rho)$  is the correlation calculated in the Schmidt basis and thus equal to the entanglement of the pure state [10,11]. Finally  $I_c(\rho) = 0$  if and only if  $\rho = \rho_A \otimes \rho_B$  [12].

Any good correlation measure should satisfy certain axiomatic properties. First, correlation is a nonlocal property and should not increase under local processing (*monotonicity*) (I). Second, a protocol starting from an uncorrelated initial state and using  $l$  qubits or  $2l$  classical bits of communication (one-way or two-way) and local

operations should not create more than  $2l$  bits of correlation. We call this property *total proportionality* (II). The intuition is that if  $2l$  bits of correlation can be established with fewer than  $2l$  bits of communication, then it may be possible to establish nonzero correlation with no communication if the receiver guesses the message.

We may expect other properties for any correlation measure. If a protocol has several rounds of communication, one may consider the increase of correlation due to each round of communication. Intuitively, a small amount of communication should not increase correlation abruptly. In particular, one may expect that the transmission of  $l$  qubits or  $2l$  bits should not increase the correlation of *any initial state* by more than  $2l$  bits. We call this property *incremental proportionality* (III). This strengthens total proportionality by allowing all possible initial states, or equivalently by considering the increase in correlation stepwise. Other properties such as *continuity* in  $\rho$  are also expected (IV).

All of these properties (I–IV) hold for some well-known correlation measures. As an important example, they hold for the classical mutual information  $I(A:B)$  when communication is classical [13]. As another example, they also hold for the quantum mutual information  $I_q(\rho)$  [8] for any communication (quantum and interactive) [14]. Here  $I_q(\rho) \equiv S(\rho_A) + S(\rho_B) - S(\rho)$  with  $S(\rho) \equiv -\text{Tr} \rho \log \rho$  being the von Neumann entropy and  $\rho_A = \text{Tr}_B \rho$ ,  $\rho_B = \text{Tr}_A \rho$ . For  $I_c$ , defined in Eq. (1), monotonicity, total proportionality, and continuity hold [8]. Incremental proportionality was proved for pure initial states  $\rho$  for any communication [8]. It also holds for classical states  $\rho$  when the communication is classical (due to the first example). However, little is known beyond these special cases.

In this Letter, we report the surprising fact that incremental proportionality for  $I_c$  can be violated in an extreme manner for a mixed initial state  $\rho$ . We will see that a single classical bit, sent from Alice to Bob, can result in

an *arbitrarily large* increase in  $I_c$ . Recall that  $I_c$  satisfies total proportionality. If one bit of communication increases  $I_c$  by a large amount, the correlation must be “present” initially, though hidden or locked as indicated by a small initial value of  $I_c$ . Only after the one-bit transmission can the large amount of correlation become accessible or unlocked. Thus violation of incremental proportionality indicates a way of locking classical correlation in the quantum state  $\rho$ . Furthermore, since incremental proportionality of  $I_c$  holds in the classical case, the effect of locked correlation is entirely quantum in nature. It is a direct consequence of the indistinguishability of nonorthogonal quantum states. Applications of such indistinguishability are well known, most notably in quantum key distribution [15] and the various partial quantum bit commitment and coin tossing protocols (see [16,17], and references therein). Curiously, the simple effect that we observe and bound in this Letter has not been noted before.

For a given initial state  $\rho$  and the amount and type of communication, we can quantify the increase in correlation by defining the following functions:

$$I_c^{(l)}(\rho) = \max_{\Lambda^{(l)}} I_c(\Lambda^{(l)}(\rho)), \quad I_c^{[l]}(\rho) = \max_{\Lambda^{[l]}} I_c(\Lambda^{[l]}(\rho)). \quad (2)$$

The operator  $\Lambda$  denotes a bipartite quantum operation that consists of local operations and no more than  $l$  bits or qubits of communication, a constraint denoted by the superscript  $(l)$  or  $[l]$ , respectively. Note that  $I_c(\rho) = I_c^{(0)}(\rho) = I_c^{[0]}(\rho)$ . Throughout the Letter, we use  $\rho$  and  $\rho'$  to denote the states before and after the quantum operation with communication,  $\rho' = \Lambda(\rho)$ .

With this notation, we summarize our main results:

(i) We present an example in which one bit of classical communication increases  $I_c$  by  $\frac{1}{2} \log d$  bits, where  $\rho$  consists of  $1 + \log d$  and  $\log d$  qubits in Alice and Bob's systems, respectively. This demonstrates an extreme violation of incremental proportionality and locking of classical correlation.

(ii) We bound the extent of incremental proportionality violation in terms of the amount of initial correlation and the amount of communication. The amount of correlation unlocked by  $l$  bits of one-way classical communication can be bounded as (Theorem 1)

$$I_c^{(l)}(\rho) - I_c(\rho) \leq l + (2^l - 1) I_c(\rho). \quad (3)$$

For small  $I_c(\rho)$ , the amount unlocked by  $l$  qubits (two-

way) can be bounded as (Theorem 2)

$$I_c^{[l]}(\rho) - I_c(\rho) \leq 2l + O(d^2 \sqrt{I_c(\rho)} \log I_c(\rho)). \quad (4)$$

We now describe the example in which an arbitrary amount of correlation is unlocked with a one-bit message. The initial state  $\rho$  is shared between subsystems held by Alice and Bob, with respective dimensions  $2d$  and  $d$ ,

$$\rho = \frac{1}{2d} \sum_{k=0}^{d-1} \sum_{t=0}^1 (|k\rangle\langle k| \otimes |t\rangle\langle t|)_A \otimes (U_t |k\rangle\langle k| U_t^\dagger)_B. \quad (5)$$

Here  $U_0 = I$  and  $U_1$  changes the computational basis to a conjugate basis [ $\forall_{i,k} \langle i|U_1|k\rangle = (1/\sqrt{d})$ ]. In this example, Bob is given a random draw  $|k\rangle$  from  $d$  states in two possible random bases (depending on whether  $t = 0$  or 1), while Alice has complete knowledge of his state. To achieve  $I_c^{(1)}(\rho) = \log d + 1$ , Alice sends  $t$  to Bob, who then undoes  $U_t$  on his state and measures  $k$  in the computational basis. Alice and Bob now share both  $k$  and  $t$ , with  $\log d + 1$  bits of correlation.

For example, the state  $\rho$  can arise from the following scenario. Let  $d = 2^n$ . Alice picks a random  $n$ -bit string  $k$  and sends Bob  $|k\rangle$  or  $H^{\otimes n}|k\rangle$  depending on whether the random bit  $t = 0$  or 1. Here  $H$  is the Hadamard transform. Alice can send  $t$  to Bob to unlock the correlation later. Experimentally, Hadamard transform and measurement on single qubits are sufficient to prepare the state  $\rho$  and later extract the unlocked correlation in  $\rho'$ —they can be realized using photons and linear optical elements such as quarter-wave plates and calcite crystals.

Now we prove that the initial correlation is small,  $I_c(\rho) = \frac{1}{2} \log d$ . First, the complete measurement  $M_A$  in the basis  $\{|k\rangle \otimes |t\rangle\}$  is provably optimal for Alice: Since the outcome tells her precisely which pure state from the ensemble she has, she can apply *classical, local* post-processing to obtain the output distribution for any other measurement she could have performed. For Alice's choice of optimal measurement,  $I_c(\rho)$  is simply Bob's *accessible* information  $I_{\text{acc}}$  [10] about the uniform ensemble of states  $\{|k\rangle, U_1|k\rangle\}_{k=0,\dots,d-1}$ .

In general, the accessible information  $I_{\text{acc}}$  about an ensemble of mixed states  $\mathcal{E} = \{p_i > 0, \eta_i\}$  is the maximum mutual information between  $i$  and the outcome of a measurement.  $I_{\text{acc}}(\mathcal{E})$  can be maximized by a POVM (positive operator valued measure) with rank 1 elements only [10]. Let  $M = \{\alpha_j |\phi_j\rangle\langle\phi_j|\}_j$  stand for a POVM with rank 1 elements where each  $|\phi_j\rangle$  is normalized and  $\alpha_j > 0$ . Then  $I_{\text{acc}}(\mathcal{E})$  can be expressed as

$$I_{\text{acc}}(\mathcal{E}) = \max_M \left[ - \sum_i p_i \log p_i + \sum_i \sum_j p_i \alpha_j \langle\phi_j|\eta_i|\phi_j\rangle \log \frac{p_i \langle\phi_j|\eta_i|\phi_j\rangle}{\langle\phi_j|\mu|\phi_j\rangle} \right], \quad (6)$$

where  $\mu = \sum_i p_i \eta_i$ .

We now apply Eq. (6) to the present problem. Our ensemble is  $\{1/(2d), U_i|k\rangle\}_{k,t}$  with  $i = k, t$ ,  $p_{k,t} = 1/(2d)$ ,  $\mu = I/d$ , and  $\langle\phi_j|\mu|\phi_j\rangle = 1/d$ . Putting all these in Eq. (6),

$$I_c(\rho) = \max_M \left[ \log 2d + \sum_{jkt} \frac{\alpha_j}{2d} |\langle \phi_j | U_t | k \rangle|^2 \log \frac{|\langle \phi_j | U_t | k \rangle|^2}{2} \right] = \max_M \left[ \log d + \sum_j \frac{\alpha_j}{d} \left( \frac{1}{2} \sum_{kt} |\langle \phi_j | U_t | k \rangle|^2 \log |\langle \phi_j | U_t | k \rangle|^2 \right) \right],$$

where we use  $\sum_j \alpha_j = d$  and  $\forall_{jt} \sum_k |\langle \phi_j | U_t | k \rangle|^2 = 1$  to obtain the last line. Since  $\sum_j \frac{\alpha_j}{d} = 1$ , the second term is a convex combination, and can be upper bounded by maximization over just one term:

$$I_c(\rho) \leq \log d + \max_{|\phi\rangle} \frac{1}{2} \sum_{kt} |\langle \phi | U_t | k \rangle|^2 \log |\langle \phi | U_t | k \rangle|^2. \quad (7)$$

Note that  $-\sum_{kt} |\langle \phi | U_t | k \rangle|^2 \log |\langle \phi | U_t | k \rangle|^2$  is the sum of the entropies of measuring  $|\phi\rangle$  in the computational basis and the conjugate basis. Reference [18] proves that such a sum of entropies is at least  $\log d$ . Lower bounds of these type are called entropic uncertainty inequalities, which quantify how much a vector  $|\phi\rangle$  cannot be simultaneously aligned with states from two conjugated bases. It follows that  $I_c(\rho) \leq \frac{1}{2} \log d$ . Equality can in fact be attained when Bob measures in the computational basis, so that  $I_c(\rho) = \frac{1}{2} \log d$  and  $I_c^{(1)}(\rho) - I_c(\rho) = 1 + \frac{1}{2} \log d$ .

We remark that incremental proportionality remains violated for multiple copies of  $\rho$ . Wootters proved that [19] the accessible information from  $m$  independent draws of an ensemble  $\mathcal{E}$  of separable states is additive,  $I_{\text{acc}}(\mathcal{E}^{\otimes m}) = m I_{\text{acc}}(\mathcal{E})$ . It follows  $I_c(\rho^{\otimes m}) = m I_c(\rho)$  in our example.

One would hope for a stronger locking effect when the message (a key) is longer than one bit. There are two figures of merit: First, the ‘‘amplification’’ of correlation,  $r_1 = I_c(\rho')/I_c(\rho)$ , should be large. Second, the amount of unlocked information, compared to the key size,  $r_2 = [I_c(\rho') - I_c(\rho)]/l$ , should be large. Ideally, we want both  $r_1$  and  $r_2$  to be arbitrarily large. We have investigated (see Appendix of [20] for details) this possibility by generalizing our two-bases example to  $L > 2$  conjugate (or mutually unbiased) bases. The key size is then  $l = \log L$ . We have found rigorous results for the two extreme cases, namely, the previous example with  $L = 2$  in which  $(r_1, r_2) \approx (2, \log d)$  and the case of  $L = d + 1$  bases in which  $(r_1, r_2) \approx (2 \log d, 2)$ . We believe some intermediate values of  $L$  will make both  $r_1, r_2$  large. For example, any  $\log L = o(\log d)$  will guarantee that  $r_1$  is large. But an analytic proof that  $r_2$  is also large has proved to be difficult, and numerical studies are inconclusive (see [20]).

An even stronger kind of locking would be what we call *complete locking*, in which  $I_c(\rho)$  would decrease rapidly with the key size  $l$ , yet the key can retrieve a finite fraction of the data. For example,

$$I_c(\rho) \propto 2^{-\alpha l} \quad \text{and} \quad I_c(\rho') - l \approx \delta \log d, \quad (8)$$

where  $\rho$  is supported on two  $d$ -dimensional systems,  $\delta > 0$  is independent of  $d$  and  $l$ , and  $\alpha > 0$ . Note that  $r_1, r_2$  are automatically large for large  $d$  in complete locking. We find that for large  $d$  complete locking cannot

occur with  $\alpha \geq 1$  or for very short keys  $l = o(\log \log d)$ . This follows from the following Theorem:

**Theorem 1:** *If  $\rho'$  is obtained from  $\rho$  with  $l$  bits of one-way classical communication,  $I_c(\rho) \geq 2^{-l} [I_c(\rho') - l]$ . It follows that  $I_c^{(1)}(\rho) - I_c(\rho) \leq l + (2^l - 1)I_c(\rho)$ .*

The intuition behind the proof is that Bob can just guess the classical key. If he guesses correctly (with probability  $1/2^l$ ), he gains  $I_c(\rho')$  bits of information, so that the average information gain is at least  $(1/2^l)I_c(\rho')$ . This intuition can be turned into a rigorous proof, and is described in detail in Ref. [20].

We can bound the violation of incremental proportionality in yet another way. Total proportionality for  $I_c$  [when  $I_c(\rho) = 0$ , transmitting  $l$  qubits can increase  $I_c$  by at most  $l$  bits] can be restated as ‘‘ $I_c(\rho) = 0$ ’’ implies no incremental proportionality violation. We may thus expect a small violation of incremental proportionality when  $I_c(\rho)$  is small. We are able to prove the following:

**Theorem 2:** *Let  $\rho$  be a bipartite state on  $C^d \otimes C^d$  and  $\rho'$  be obtained from  $\rho$  by  $l$  qubits of two-way communication. If  $I_c(\rho) \leq \frac{1}{6 \ln 2} \frac{1}{(d+1)^2}$ ,*

$$I_c(\rho') - I_c(\rho) \leq 2l - (2d)^2 \sqrt{(2 \ln 2) I_c(\rho)} \log \sqrt{(2 \ln 2) I_c(\rho)}.$$

The proof of Theorem 2 relies essentially on the following lemma (see Appendix of [20] for a proof) which says that when  $I_c(\rho)$  is small,  $\rho$  must be close to an uncorrelated state (in trace distance).

**Lemma 1.**—If  $\rho$  is a bipartite state on  $C^d \otimes C^d$ , then

$$\text{Tr} |\rho_{AB} - \rho_A \otimes \rho_B| \leq (2d)^2 \sqrt{(2 \ln 2) I_c(\rho)}, \quad (9)$$

where  $\rho_{A/B} = \text{Tr}_{B/A} \rho$ .

The theorem is proved by first relating  $I_c$  to  $I_q$  which obeys incremental proportionality (with an extra factor of 2). Then Lemma 1 and the continuity of  $I_q$  implies that  $I_q(\rho)$  is close to  $I_q(\rho_A \otimes \rho_B)$ , giving the desired bound (see [20] for details).

The weakness of Lemma 1 and thus that of Theorem 2 stems from the factor  $d^2$  in Lemma 1. This factor comes from an analysis that uses measurements in all mutually unbiased bases to distinguish  $\rho_A \otimes \rho_B$  from  $\rho$ , and the analysis is probably not optimal. Note that the dependence on the dimension  $d$  in the bound in Theorem 2 makes it impossible to rule out complete locking.

We turn to some discussions concerning the main results described above. Our locking scheme has a classical analogue [21]. Suppose Alice has an  $n$ -bit string  $x$  together with an extra bit  $t$ . Bob also has an  $n$ -bit string  $y$ . If  $t = 0$ ,  $y = x$  and if  $t = 1$ ,  $y = f(x)$ , where  $f$  is an invertible function. This is analogous to the quantum example in that, Bob can guess  $x$  correctly with

probability  $1/2$ . However, it is different in that Bob knows  $x = y$  or  $f^{-1}(y)$ . Given each value of  $t$ , he knows the string, and his information about  $x$  is  $n - 1$  bits. This is in sharp contrast with the quantum locking scheme in which there is one basis  $t$  in which Bob has *no information* about  $x$ .

Our locking scheme is closely related to quantum key distribution (QKD), in particular, BB84 [15], in which Alice holds a basis bit (computational or Hadamard) for each of Bob's qubits. Transmitting the locked state limits the classical correlation between Alice and any potential eavesdropper (Eve) and forbids her from tampering without disturbance. Announcing the basis bits at a later stage enables Alice and Bob to unlock the correlation. Furthermore, incomplete unlocked correlation (as indicated by the test bits) reveals Eve's tampering. However, in BB84, one bit is sent for every bit to be unlocked, and there is no extreme unlocking behavior as shown by our examples.

Further research into the phenomenon of locking will be worthwhile. For instance, we have seen differences in the locking effect by quantum and classical keys. Another important factor affecting the strength of locking is the number of rounds of communication allowed. In fact, a striking difference between one-way and two-way communications can be seen if one generalizes the state in Eq. (5) so each of Alice and Bob has a one-bit key register, and the rotation  $U_t$ , now performed on both Bob's and Alice's state, is determined by the *parity* of the two key bits. Full unlocking is possible with two-way communication, but not with one-way communication. Finally, the possibility of complete locking, or its impossibility (by improving Lemma 1 and Theorem 2) are important open questions; it may be interesting to see how complete locking relates to known restrictions on partial bit commitments [16].

We thank I. Devetak and C. Bennett for extremely helpful discussions, W. Wootters for enlightening discussion on mutually unbiased bases, and D. Gottesman for a discussion on complete locking. Part of this work was completed while M.H. was visiting at the MSRI program on Quantum Computation. M.H. is supported by EC, Contract No. IST-2001-37559 (RESQ), IST-2001-38877 (QUPRODIS), and also by EQUIP. D.P.DV., J.A.S., and B.M.T. are supported in part by the NSA and the ARDA through ARO Contract No. DAAD19-01-C-0056. D.W.L. acknowledges support from the Tolman Endowment Fund and the NSF under Grant No. EIA-0086038.

- [1] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [2] E. Schrödinger, *Naturwissenschaften* **23**, 807 (1935).
- [3] Special issue on *Entanglement: Theory and Experiment* [*Quantum Inf. Comput.* **1** (2001)].
- [4] W. Zurek, *Ann. Phys. (Leipzig)* **9**, 855 (2000).
- [5] L. Henderson and V. Vedral, *J. Phys. A* **34**, 6899 (2001).
- [6] H. Ollivier and W. Zurek, *Phys. Rev. Lett.* **88**, 17901 (2002).
- [7] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **89**, 180402 (2002).
- [8] B. Terhal, M. Horodecki, D. Leung, and D. DiVincenzo, *J. Math. Phys. (N.Y.)* **43**, 4286 (2002).
- [9] T. Cover and J. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
- [10] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1993).
- [11] When  $\rho$  is classical, the measurement along the local product basis is optimal, and when  $\rho$  is pure, the measurement along the Schmidt basis is optimal. This is due to the data processing inequality [9] and the fact that the distributions of the outcomes of other measurements are obtainable by local processing of the optimal ones.
- [12] Obviously,  $I_c(\rho_A \otimes \rho_B) = 0$ . The converse follows from Eq. (9) in Lemma 1.
- [13] For example, incremental proportionality of  $I(A:B)$  for the classical case follows from the fact [9] that  $\max(H(p_A), H(p_B)) \leq H(p_{AB}) \leq H(p_A) + H(p_B)$ , so that when Alice sends a classical system  $A'$  to Bob,  $I_c(\rho') = I(A; BA') \leq I(AA'; B) + H(p_{A'})$ . Total proportionality then follows from incremental proportionality.
- [14] Throughout the paper, the most general form of communication can be quantum or classical, and can involve any number of rounds of forward and backward communication between Alice and Bob. We call this type of communication "any communication."
- [15] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
- [16] R. Spekkens and T. Rudolph, *Phys. Rev. A* **65**, 012310 (2001).
- [17] R. Spekkens and T. Rudolph, *Phys. Rev. Lett.* **89**, 227901 (2002).
- [18] H. Maassen and J. Uffink, *Phys. Rev. Lett.* **60**, 1103 (1988).
- [19] D. DiVincenzo, D. Leung, and B. Terhal, *IEEE Trans. Inf. Theory* **48**, 580 (2001).
- [20] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, *quant-ph/0303088*.
- [21] D. DiVincenzo and B. Terhal, *Phys. World* **16** (5), 26 (2003).