Entanglement-free certification of entangling gates

Entanglement-free certification of entangling gates

M. P. Almeida,[1,2,*] Mile Gu,[3,4] Alessandro Fedrizzi,[1,2] Matthew A. Broome,[1,2] Timothy C. Ralph,[2] and Andrew G. White[1,2]

[1]*Centre for Engineered Quantum Systems, School of Mathematics and Physics, University of Queensland, Brisbane, QLD 4072, Australia*

[2]*Centre for Quantum Computer and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, QLD 4072, Australia*

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*

[4]*Centre for Quantum Technologies, National University of Singapore, Singapore*

(Received 14 January 2013; revised manuscript received 1 July 2013; published 23 April 2014)

Not all quantum protocols require entanglement to outperform their classical alternatives. The nonclassical correlations that lead to a quantum advantage are conjectured to be captured by quantum discord. Here we demonstrate that discord has an immediate practical application: it allows a client who lacks the ability to generate entanglement or conduct quantum measurements to certify whether an untrusted party has entangling gates. We implement our protocol in the discrete-variable regime with photonic qubits and show its success in the presence of high levels of noise and imperfect gate operations. Our technique offers a practical method to test claims of quantum processing and to benchmark entangling operations for physical architectures in which only highly mixed states are available.

DOI: 10.1103/PhysRevA.89.042323 PACS number(s): 03.67.Lx, 03.67.Ac, 42.50.Dv

I. INTRODUCTION

Models of intermediate quantum computing [1–4] offer an intriguing approach for developing quantum devices that outperform their classical counterparts. These models derive their attraction from the reduced resources compared to scalable quantum computing and, hence, should be realizable sooner. One example of intermediate quantum computation is the mixed-state algorithm DQC1 [1]. Its computational advantage is often [5,6] associated with *quantum discord* [7,8], a nonclassical correlation which is identical to entanglement for pure states but persists for mixed states, even when the entanglement is 0.

The presence of such nonclassical correlations in virtually all mixed states prompted the question whether discord was ultimately a useful quantum resource [9]. While it is now known that quantum circuits consisting of one- and two-qubit gates cannot provide superpolynomial computational speedups without generating discord [10], a formal link to computational advantage for specific protocols such as DQC1 is still missing. This has motivated extensive efforts in identifying the operational significance of discord, both in theory [11–20] and in experiments [21,22].

Here, we show that discord has an immediate practical application, the certification of entangling gates. In this scenario, Alice wishes to test whether an untrusted party, Bob, can perform entangling operations. Conventional methods requires either quantum tomography, tests of Bell inequalities, or generation of quantum entanglement. Such actions require Alice either to conduct quantum measurements herself, to possess entanglement, or to put blind trust in the gate operator Bob. In many situations, this is unrealistic. Bob may represent a commercial entity that markets the services of quantum processing. Alice, a potential client, would thus want to test Bob's claims with minimal technical requirements. We demonstrate this is possible when Alice can only prepare separable, but discordant, states and perform single-qubit operations. We implement our technique using a two-qubit photonic entangling gate and show that we can verify an entangling operation even in the presence of entanglement-breaking noise and imperfect gates. Note that such an asymmetry in resources is a natural assumption in adversarial quantum communication scenarios, such as *blind* quantum computation [23].

We draw inspiration from the *discord consumption* protocol introduced in [22]. In this protocol, Alice randomly encodes information in some discordant bipartite state ρ_{AB}, and Bob is challenged to retrieve as much of this information as possible. If Bob is limited to performing a single local measurement on each bipartition, then his performance is constrained to some incoherent limit. However, coherent bipartite interactions allow Bob to surpass this bound. The protocol suggests that discord could be used to test for Bob's capacity to coherently interact and, thus, entangle the two physical systems.

Direct application of this protocol, however, leads to a loophole. The incoherent limit constrains Bob to measuring each bipartition only once. Bob can potentially cheat using multiple rounds of adaptive measurements on the two bipartitions. In this paper, we close this loophole when Alice's bipartite state consists of two discordant *qubits*. In this scenario, the incoherent limit strictly bounds the amount of information Bob can access with only single-qubit quantum gates. Should Bob surpass this limit, Alice can be certain that Bob has some entangling two-qubit gate.

In brief, the report is organized as follows. In Sec. II we set out our protocol for verifying entangling operations without the use of entangled states. In Sec. III we prove our main result, in particular, we focus on closing the previously discussed loophole which can be achieved in the discrete-variable regime. In Sec. IV we present our experimental results for both the near-ideal case and the case with artificially introduced sources of decoherence. A summary of our work is given in Sec. V.

*marcelo@physics.uq.edu.au

II. THEORY

We first recall that discord quantifies the quantum component of the correlations between two physical systems [7,8]. The total correlations between two systems, A and B, are quantified by the mutual information $I(A,B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$, where $S(\rho)$ is the Shannon entropy of the state ρ. Meanwhile the classical component of these correlations, $J(A|B) = S(\rho_A) - \max_{\{\Pi_b\}\in\mathcal{M}} \sum p_b S(\rho_{A|b})$, is defined by the reduction in the entropy of A after a measurement on B, when maximized over positive operator value measurements (POVMs) performed on B. (Here, p_b is the probability of getting measurement outcome b, leaving A in the conditional state $\rho_{A|b}$; $\mathcal{M}$ represents the class of all possible POVMs; and Π_b represents a generic operator.) Thus, the difference between these quantities quantifies the amount of quantum correlations between A and B. We define this discrepancy, $\delta(A|B) = I(A,B) - J(A|B)$, as the discord. Note that discord is generally asymmetric, $\delta(A|B) \neq \delta(B|A)$.

To execute the protocol, Alice first initializes two qubits in some state ρ_{AB}. She then labels qubits such that $\delta(A|B) \leqslant \delta(B|A)$. If $\delta(A|B) \neq 0$, we say the state contains discord. Alice then generates a random variable $\mathbf{K}$ that is uniformly distributed among the four possible values (b_1,b_2), where $b_1,b_2 \in \{0,1\}$ are random bits [see Fig. 1(a)], and encodes each possible $k = (b_1,b_2)$ in her system by application of the corresponding local unitary $U_k = \sigma_x^{b_1}\sigma_z^{b_2}$ on qubit A.

The qubit pair is given to Bob, who is challenged to guess k by returning an estimate k_m governed by a random variable $\mathbf{K}_m$. Alice quantifies Bob's performance by the amount of information k_m contains about k; i.e., $I_{\text{exp}} = I(\mathbf{K},\mathbf{K}_m)$, the mutual information between $\mathbf{K}$ and $\mathbf{K}_m$.

Let I_c be Bob's best possible performance when he is restricted to single-qubit gates and arbitrary local measurements. Let I_q be his performance when he can also implement arbitrary two-qubit gates on A and B or between either qubit and additional ancilla qubits: $\Delta I = I_q - I_c$ is then the "quantum advantage" of having two-qubit entangling gates. Provided ΔI is nonzero, Alice can be certain that Bob possesses some entangling two-qubit gate. Furthermore, provided A and B represent qubits,

$$I_q - I_c = \delta(A|B). \tag{1}$$

That is, the amount of information Alice can encode within ρ_{AB} that can be accessed by two-qubit operations is given exactly by $\delta(A|B)$.

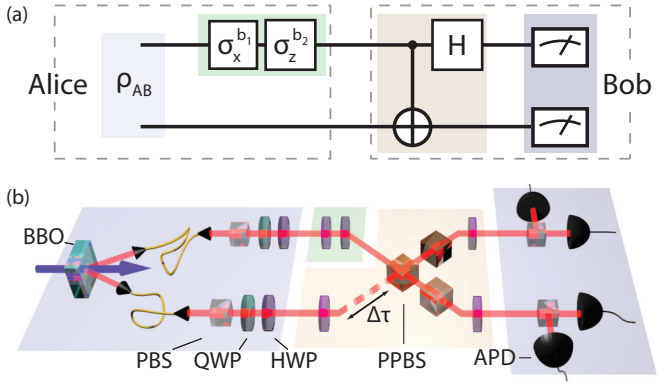

FIG. 1. (Color online) (a) Quantum circuit representation of the protocol. Alice prepares discordant state ρ_{AB} and encodes onto it the classical quaternary variable k via the unitaries $\sigma_x^{b_1}$, $\sigma_z^{b_2}$. Bob conducts an allegedly entangling operation—optimally a Bell-state measurement—to estimate Alice's encoding. (b) Experiment. Alice's qubits are realized using orthogonal polarization states of two 820-nm single photons generated via type I spontaneous parametric down-conversion in a 2-mm β-barium-borate (BBO) crystal pumped by a frequency-doubled (820 → 410 nm) Ti:sapphire laser (100-fs pulse length, 76-MHz repetition rate). Qubits are initialized with polarizing beam splitters (PBSs) and rotated [left (lilac) area] and encoded [small upper-left central (green) area] via quarter-wave plates (QWPs) and half-wave plates (HWPs). Bob's entangling measurement is realized with a nondeterministic CZ gate based on nonclassical interference of photons at a partially polarizing beam splitter (PPBS) of reflectivity $\eta_V = 2/3$ ($\eta_H = 0$) for vertical (horizontal) polarization. The photon arrival time is controlled by a relative temporal delay $\Delta\tau = 0$, which is used to tune the gate quality. The three HWPs enact Hadamard operations to turn the CZ into a CNOT gate and to complete the Bell-state measurement [large central (yellow) area]. Photons are analyed in the Z basis by PBSs and detected by avalanche photodiodes [APDS; right (gray) area].

III. PROOF OF THE MAIN RESULT

We now prove that for an arbitrary two-qubit state ρ_{AB} with discord $\delta(A|B)$, and the aforementioned encoding, Bob's advantage using entangling gates is given by Eq. (1). This is done by closing the multiple measurement loophole in [22]. Let I_c' be Bob's optimal performance when he has no entangling gates and, furthermore, is restricted to a single measurement on each qubit. Clearly this addition restriction implies that $I_c' \leqslant I_c$. We prove, additionally, that, $I_c \leqslant I_c'$, and thus $I_c = I_c'$.

This is done by contradiction. Assume that $I_c > I_c'$, i.e., Bob can exceed a performance of I_c' without use of entangling gates by making multiple measurements on either qubit A or qubit B. Let this be qubit B without loss of generality.

Since A resides in a two-dimensional Hilbert space, subsequent measurements on B are advantageous only if the first was weak, i.e., involving the interaction of B with an ancilla C, followed by a measurement of C. This interaction, however, must have the potential to entangle A and C and thus constitutes an entangling gate. This contradicts out assumption that Bob did not use entangling gates. Therefore $I_c = I_c'$.

In [22], I_c' is referred to as the *incoherent limit*, and it was established that

$$I_q - I_c' = \delta(A|B), \tag{2}$$

provided Alice's choice of encoding is maximal ($\sum_k p_k U_k \rho U^k = \mathbf{I}/2$ is totally mixed for any single-qubit state ρ). This condition is satisfied for the encoding in our protocol, thus, the relation also applies to I_c and $I_q - I_c = \delta(A|B)$.

Finally, we should note that if either system A or system B is not a qubit, then the above argument does not apply, and there is a potential cheating strategy for Bob. In particular, a second measurement on B can still be advantageous if the first measurement on B contains degeneracy. For example, if system B were to consist of a composite system of two qubits, B_1 and B_2, Bob has the extra option of measuring either in the

sequence B_1, A, then B_2 or in the sequence B_1, B_2, then A, conditioned on the outcome of measuring B_1. Such strategies are not accounted for in the protocol described in Ref. [22] and, in general, will allow Bob to achieve a higher I_c.

IV. EXPERIMENT AND RESULTS

Since virtually all mixed states contain nonzero discord, Alice has considerable freedom in her choice of ρ_{AB}. In practice, she will pick a state which is easy to prepare in her given physical architecture, as well as one that contains a significant amount of discord.

Here we consider that Alice can prepare an equal mixture of the three symmetric Bell states,

$$\rho_{AB} = \tfrac{1}{3}(|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+|), \qquad (3)$$

where $|\phi^\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$. The state ρ_{AB} can be rewritten as $\rho_{AB} = \sum_i (|0_i 0_i\rangle\langle 0_i 0_i| + |1_i 1_i\rangle\langle 1_i 1_i|)$, where $i = \{x,y,z\}$, so that $|0\rangle_i$ and $|1\rangle_i$ represent the computational basis states with respect to the Pauli operators σ_i. ρ_{AB} is therefore clearly separable and relatively simple to prepare: Alice can simply initialize two qubits oriented in one of the six orthogonal directions on the Bloch sphere at random. In addition, $\delta(A|B)$ has a simple form for our state of choice because $J(A|B)$ is maximized by any projective measurement. We find $\delta(A|B) = 1/3$, which ranks at the very high end of separable states [24].

Bob's optimal strategy in this scenario is to conduct measurements in the Bell basis. For each k, the resulting state after application of U_k will be an equal mixture of three of the four Bell states

$$\rho_{AB} = \frac{1}{6}\begin{bmatrix} 2-b_1 & 0 & 0 & b_1 r \\ 0 & 1+b_1 & (1-b_1)r & 0 \\ 0 & (1-b_1)r & 1+b_1 & 0 \\ b_1 r & 0 & 0 & 2-b_1 \end{bmatrix}, \qquad (4)$$

where $r = (-1)^{b_2}$. For every instance of the protocol, Bob's Bell-state measurement allows him to eliminate one of the four possible values of k. His probability of correctly guessing k based on each outcome will be $1/3$, which results in an information rate of $I_q = 2 - \log_2(3) \approx 0.415$, assuming zero noise and perfect gate operation.

In contrast, Bob's maximal information rate *without* an entangling two-qubit gate is bounded above by $I_c = I_q - \delta(A|B) = 5/3 - \log_2(3) \approx 0.082$ (see the Appendix). Upon receipt of k_m, Alice can compute Bob's achieved information rate $I_q^{\exp}$. Should this exceed I_c, she is sure that Bob is capable of implementing an entangling two-qubit operation.

In our experiment, Alice encodes ρ_{AB} in the polarization of two single-photon qubits, where horizontal $|H\rangle$ and vertical $|V\rangle$ polarizations correspond to the logical states $|0\rangle$ and $|1\rangle$ [Fig. 1(b)]. Bob conducts his Bell-state measurements using a nondeterministic, controlled-phase (CZ) gate [25,26] and single-qubit Hadamard gates. The CZ gate relies on two-photon interference at a beam splitter, imparting a π phase shift on the input state $U_{\rm CZ}|VV\rangle \to -|VV\rangle$, while leaving other input combinations of basis states unchanged.

Alice constructs her discordant state ρ_{AB} employing the procedure described in Ref. [27]: she sequentially prepares photons in one of the states $\{|HH\rangle,|VV\rangle,|DD\rangle,|AA\rangle,|RR\rangle,|LL\rangle\}$, where $|D\rangle,|A\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$ and $|R\rangle,|L\rangle = (|H\rangle \pm i|V\rangle)/\sqrt{2}$, and applies one of the four encodings k. Bob's Bell-state measurement sums up over all components of Alice's state to extract the final measurement outcomes. The experimental mutual information rate is given by

$$I_q^{\exp} = \sum_k p(k)\log_2(p(k)) - \sum_k \sum_{k_m} p(k,k_m)\log_2\left(\frac{p(k)}{p(k,k_m)}\right). \qquad (5)$$

In Eq. (5), $p(k)$ is the probability of encoding one of the variables $k = (b_1,b_2)$, while $p(k,k_m)$ is the joint probability of encoding k and measuring the estimate k_m. These probabilities are related to the measured coincidence counts $C_{k,l}$ through the expressions

$$p(k) = \frac{\sum_l C_{k,l}}{\sum_k \sum_l C_{k,l}}, \qquad p(k,k_m) = \frac{C_{k,l}}{\sum_k \sum_l C_{k,l}}, \qquad (6)$$

where l represented one of Bob's four detectors. The experimental information rate achieved was $I_q^{\exp} = 0.363 \pm 0.008$, which is more than 35 standard deviations above the classical limit for I_c.

We investigated the robustness of the protocol by studying two key sources of imperfection: (i) the addition of white noise to the ideal state, $\rho(p)_{AB} = p\ \rho_{AB} + (1-p)\ \frac{\mathbb{1}}{4}$; and (ii) imperfect gate operation, caused by increasing the temporal distinguishability between the two interfering photons, $\Delta\tau$. We modeled the latter by mixing one of the CZ gate input modes with a vacuum mode using a virtual beam splitter with transmittivity ξ [25]: the relation of this parameter to the temporal mismatch $\Delta\tau$ is found by mapping to the well-known Gaussian two-photon interference pattern, $\xi = 1 - e^{-(\Delta\omega\Delta\tau)^2}$, where $\Delta\omega$ is the spectral bandwidth of our single photons. Starting from Bob's optimal information rate $I_q \simeq 0.415$, Fig. 2(a) predicts a large operating range with quantum advantage.

We tested these predictions experimentally. In Fig. 2(b) Bob runs the entangling gate optimally, $\Delta\tau = 0$, and Alice increases the noise on her state, i.e., decreases p, until $\tilde{\rho}_{AB}$ is fully mixed. The ideal performance limit for Bob is, in this case, dictated by the Holevo limit $I_q = 2 - S[\rho(p)_{AB}]$. As predicted, we find that Bob *always* retains a quantum advantage over the classical estimate for any given level of noise. In fact, this remains true for general noise. Any additional noise on ρ_{AB} can be interpreted as initiating the protocol with some effective resource state ρ'_{AB}. Provided ρ'_{AB} contains discord—which it generally will, due to the robustness of discord to noise—Alice can use ρ'_{AB} in place of ρ_{AB}.

In Fig. 2(c) Alice prepares the optimal state ρ_{AB} and Bob decreases the gate performance by temporal mode mismatch, where his optimal performance I_q is now limited by the

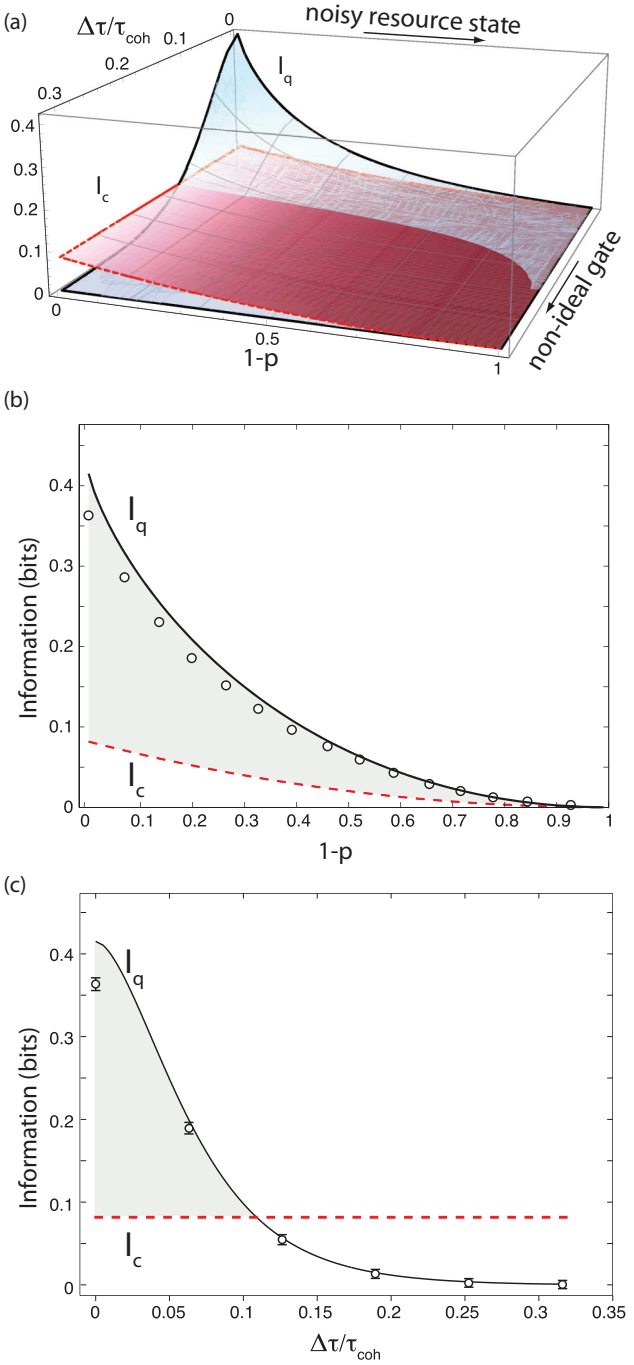

FIG. 2. (Color online) Certification of a quantum operation with discordant states. (a) Theoretical quantum performance I_q achievable by Bob vs classical limit I_c as a function of white noise in Alice's resource states, $1-p$, and the quality of Bob's gate operation, $\Delta\tau/\tau_{\rm coh}$. (b) Alice encodes information within noisy discordant input states $\rho(p)_{AB} = p\rho_{AB} + (1-p)\frac{\mathbb{1}}{4}$. Provided Bob has access to an ideal (CZ) gate, Bob's theoretical performance (solid black line) is guaranteed to exceed the performance limit of someone with single qubit gates [dotted horizontal (red) line]. This quantum advantage is retained in an experiment (open circles) for almost all p. Error bars are smaller than the symbol size. (c) Indeed, even under artificial degradation of the (CZ) gate through temporal mode mismatch $\Delta\tau/\tau_{\rm coh}$ between the interacting photonic qubits, the advantage continues to persist till $\Delta\tau/\tau_{\rm coh}$ exceeds 0.1. Errors are based on Poissonian counting statistics.

vacuum admixture, with ξ taking the role of the noise parameter p. The amount of information I_c extractable without two-qubit gates is independent of the gate operation in this scenario and therefore constant. Again, as predicted, Bob can demonstrate a quantum advantage up to $\sim$0.1 coherence length: Bob can still convince Alice he is capable of performing an entangling operation even when his gate does not perform very well. Conversely, if Alice knows the quality of the states she sent, she will be able to quantify the performance of Bob's entangling gate based on his guess.

V. CONCLUSION

In conclusion, our experiment complements the recent interpretation of discord as a resource for entangling interactions. It also sheds light on the previously considered phenomenon of nonlocality without entanglement [28,29]: Unentangled, but discordant states can be distinguished better than zero-discord states with nonlocal measurements. The consequences of our protocol extend beyond the pragmatic vendor-client application we have presented here. For instance, in computer science, there is significant interest in the resource asymmetry between performing a task and verifying whether an untrusted party can perform specific computational tasks. This is reflected, for example, in the study of NP problems and zero-knowledge proofs (proving to a party that you can do something without revealing how you do it). Here we show that something analogous exists for entanglement: It is possible to prove one has entangling operations without generating entanglement, provided there is some discord.

It is an open question whether this result can be generalized to n-qubit states and gates. There is no straightforward extension of our discord definition for n qubits, but since two-qubit entangling gates are universal when combined with single-qubit operations, one may bootstrap the two-qubit certification. Meanwhile, candidate architectures for quantum computing are intrinsically entangling—such as spins in a solid interacting via J coupling—but are often too noisy to preserve entanglement. Our technique offers an immediate method to certify whether such systems could, in principle, permit genuine quantum processing.

ACKNOWLEDGMENTS

We thank G. G. Gillett for help with data acquisition and Cyril Branciard, K. Modi, and V. Vedral for helpful discussions. This work was supported in part by the Centre for Engineered Quantum Systems (Grant No. CE110001013) and the Centre for Quantum Computation and Communication Technology (Grant No. CE110001027). M.P.A. and A.F. acknowledge support by Australian Research Council Discovery Early Career Awards (No. DE120101899 and No. DE130100240, respectively). M.G. was supported by the National Basic Research Program of China (Grants No. 2011CBA00300 and No. 2011CBA00302) and the National Natural Science Foundation of China (Grants No. 61033001 and No. 61061130540). T.C.R. and A.G.W. were supported by University of Queensland Vice-Chancellor's Senior Research Fellowships.

APPENDIX: EXPLICIT EVALUATION OF I_c

Here we explicitly show that for the specific protocol where ρ_{AB} is a mixture of three Bell states, Bob's optimal performance without two-qubit gates is $I_c = \frac{5}{3} - \log_2(3)$. First, note that Bob can saturate I_c by making a single σ_z measurement on each of two qubits he receives from Alice. If the measurement results are identical, he guesses $k = (0,?)$; otherwise he guesses $k = (1,?)$, where "?" denotes a random guess. This strategy gives no information about the second bit but can reveal the first bit correctly two-thirds of the time. The resulting information rate is $1 - H(\frac{1}{3}) = I_c$, where $H(.)$ denotes the binary entropy.

This strategy is in fact optimal. In Sec. III we show that Bob's optimal strategy need involve only a single measurement on each qubit. Consider first a measurement on system B described by operators $\{\Pi_b\}$. Since the encoding U_k is localized to A, it commutes with the measurement operation. Therefore, if Bob were to get measurement outcome b, Alice would have effectively encoded onto the conditional state $\rho_{A|b}$. Bob's resulting information rate is thus constrained by the Holevo bound, $1 - \sum_b p_b S(\rho_{A|b})$, which is maximized when Bob chooses a measurement that minimizes the expected entropy of the resulting state. Due to the symmetry of ρ_{AB}, any projective measurement does this. Without loss of generality, measurement in the σ_z basis gives

$$S(\rho_{A|b}) = \sigma_x^b \left(\tfrac{2}{3}|0\rangle\langle 0| + \tfrac{1}{3}|1\rangle\langle 1|\right)\sigma_x^b. \tag{A1}$$

This results in a Holevo bound of $1 - H(\frac{1}{3}) = \frac{5}{3} - \log_2(3)$.

To bound the case where Bob decides to measure qubit A, we note that Bell states satisfy the property $(\sigma_x^{b_1}\sigma_z^{b_2} \otimes I)\rho_{AB}(\sigma_x^{b_1}\sigma_z^{b_2} \otimes I) = (I \otimes \sigma_x^{b_1}\sigma_z^{b_2})\rho_{AB}(I \otimes \sigma_x^{b_1}\sigma_z^{b_2})$. That is, although Alice encoded onto qubit A, the resulting state is functionally equivalent to encoding on qubit B. Thus, by inverting A and B, the previous argument applies.

The optimal performance Bob can achieve without entangling two-qubit gates is therefore $I_c = \frac{5}{3} - \log_2(3)$. Since $\delta(A|B) = 1/3$, this agrees with our general result that $I_q - I_c = \delta(A|B)$.

[1] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[2] S. Jordan, Quantum Info. Comput. **10**, 470 (2010).
[3] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. Roy. Soc. A: Math. Phys. Eng. Sci. **467**, 459 (2011).
[4] S. Aaronson and A. Arkhipov, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing STOC'11, San Jose, CA* (ACM, New York, 2011), pp. 333–342.
[5] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
[6] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White, Phys. Rev. Lett. **101**, 200501 (2008).
[7] L. Henderson and V. Vedral, J. Phys. A: Math. Gen. **34**, 6899 (2001).
[8] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[9] A. Ferraro, L. Aolita, D. Cavalcanti, F. M. Cucchietti, and A. Acin, Phys. Rev. A **81**, 052318 (2010).
[10] B. Eastin, arXiv:1006.4402.
[11] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **89**, 180402 (2002).
[12] A. Brodutch and D. R. Terno, Phys. Rev. A **81**, 062103 (2010).
[13] M. Piani, P. Horodecki, and R. Horodecki, Phys. Rev. Lett **100**, 090502 (2008).
[14] S. Luo and W. Sun, Phys. Rev. A **82**, 012338 (2010).
[15] S. Boixo, L. Aolita, D. Cavalcanti, K. Modi, and A. Winter, Int. J. Quantam Inform. **09**, 1643 (2011).
[16] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter, Phys. Rev. A **83**, 032324 (2011).
[17] V. Madhok and A. Datta, Phys. Rev. A **83**, 032323 (2011).
[18] A. Streltsov, H. Kampermann, and D. Bruß, Phys. Rev. Lett. **106**, 160401 (2011).
[19] M. Piani, S. Gharibian, G. Adesso, J. Calsamiglia, P. Horodecki, and A. Winter, Phys. Rev. Lett. **106**, 220403 (2011).
[20] T. K. Chuan, J. Maillard, K. Modi, T. Paterek, M. Paternostro, and M. Piani, Phys. Rev. Lett **109**, 070501 (2012).
[21] B. Dakic, Y. O. Lipp, X. Ma, M. Ringbauer, S. Kropatschek, S. Barz, T. Paterek, V. Vedral, A. Zeilinger, C. Brukner, and P. Walther, Nat. Phys. **8**, 666 (2012).
[22] M. Gu, H. Chrzanowski, S. Assad, T. Symul, K. Modi, T. C. Ralph, V. Vedral, and P. Lam, Nat. Phys. **8**, 671 (2012).
[23] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, 2009, FOCS'09, Los Alamitos, CA* (IEEE, Piscataway, NJ, 2009), pp. 517–526.
[24] A. Al-Qasimi and D. F. V. James, Phys. Rev. A **83**, 032101 (2011).
[25] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, Phys. Rev. A **65**, 062324 (2002).
[26] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White, Phys. Rev. Lett. **95**, 210504 (2005).
[27] A. Fedrizzi, M. Zuppardo, G. G. Gillett, M. A. Broome, M. P. Almeida, M. Paternostro, A. G. White, and T. Paterek, Phys. Rev. Lett. **111**, 230504 (2013).
[28] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[29] G. J. Pryde, J. L. O'Brien, A. G. White, and S. D. Bartlett, Phys. Rev. Lett. **94**, 220406 (2005).