Complementary sequential measurements generate entanglement

Patrick J. Coles[1] and Marco Piani[2]

[1]*Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, 117543 Singapore*
[2]*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L3G1*

We present a paradigm for capturing the complementarity of two observables. It is based on the entanglement created by the interaction between the system observed and the two measurement devices used to measure the observables sequentially. Our main result is a lower bound on this entanglement and resembles well-known entropic uncertainty relations. Besides its fundamental interest, this result directly bounds the effectiveness of sequential bipartite operations—corresponding to the measurement interactions—for entanglement generation. We further discuss the intimate connection of our result with two primitives of information processing, namely, decoupling and coherent teleportation.

Heisenberg's uncertainty principle [1] tries to capture one of the fundamental traits of quantum mechanics: the complementarity of observables such as position and momentum. There are several variants of the principle which may be considered conceptually very different [2]. For example, one can consider the uncertainty related to the independent measurement of two observables, with the measurements performed on two *independent but identically prepared* quantum systems. In this scenario, the uncertainty principle for complementary observables can be understood as stating that there is an *unavoidable uncertainty* about the outcomes of the associated measurements. Alternatively, one can consider the *sequential* measurement of such two observables, performed on the *same* physical system. In this case, the uncertainty principle is understood as the *unavoidable disturbance* on the second observable due to the measurement of the first. Although this latter disturbance-based interpretation of the principle is the one originally considered by Heisenberg in his famous γ-ray thought experiment [3], researchers have more often focused on the first scenario.

Unavoidable uncertainty was stated quantitatively by Kennard [4] and Robertson [5] in the famous uncertainty relation involving standard deviations. Since then, uncertainty relations have been cast in information-theoretic terms [6]. For example, a well-known *entropic uncertainty relation* is that of Maassen and Uffink [7]. Working in finite dimensions, they consider two orthonormal bases $\{|X_j\rangle\}$ and $\{|Z_k\rangle\}$ for the Hilbert space $\mathcal{H}_S$ of a quantum system S, to which one can associate observables X and Z, respectively. For any state ρ_S, they find

$$H(X) + H(Z) \geqslant \log_2(1/c), \tag{1}$$

where $H(X) := -\sum_j p(X_j) \log_2 p(X_j)$ is the Shannon entropy associated with the probability distribution $p(X_j) := \langle X_j|\rho_S|X_j\rangle$ [similarly for $H(Z)$], and $c := \max_{j,k} |\langle X_j|Z_k\rangle|^2$ quantifies the complementarity between the X and Z observables. The right-hand side of (1) vanishes when X and Z share an eigenstate. At the other extreme, when X and Z are complementary—so-called mutually unbiased bases (MUBs) with $|\langle X_j|Z_k\rangle|^2 = 1/d$, $\forall j,k$, and $d = \dim(\mathcal{H}_S)$—the right-hand side becomes $\log_2 d$. In the latter case, Eq. (1) implies that when our uncertainty about X approaches zero, our uncertainty about Z must approach its maximum value $\log_2 d$.

In this Rapid Communication, we offer a different view on what complementarity entails by relating it to another fundamental trait of quantum mechanics: *entanglement* [8]. In Ref. [9] it was already proved that an entropic uncertainty relation such as (1) has a correspondent entanglement certainty relation. In more detail, Ref. [9] considers the generation of entanglement between measurement devices and independent, although identically prepared, copies of some physical system, and proves that, when dealing with complementary observables, there is unavoidable creation of entanglement between at least one copy of the system and one measuring device. Here, as Heisenberg did originally, we instead consider sequential measurements performed on the same physical system, rather than independent copies of the system; on the other hand, following Refs. [9–13], we still focus on the entanglement generated between the system and the measurement devices. In general, for any X and Z, we can lower-bound the entanglement $E(X,Z)$ between the system and the measurement devices created from sequentially measuring X and Z with

$$E(X,Z) \geqslant \log_2(1/c), \tag{2}$$

where the c factor appearing here is precisely the same c appearing in Eq. (1), and we provide more details on how we quantify entanglement in the following.

Besides the fact that our approach connects in a fundamental way two basic properties of quantum mechanics, complementarity—in the sequential-measurement scenario—and entanglement, our results have also direct operational interpretations. On one hand, they provide bounds on the usefulness of sequential bipartite operations—corresponding to the measurement interactions—for entanglement generation. On the other hand, we argue below that our analysis is directly linked to the quantum information processing primitives of decoupling [14–18] and coherent teleportation [19,20].

Setup. The basic setup corresponding to our main result is given in Fig. 1. The system is initially described by some arbitrary density operator $\rho_S^{(0)}$. It first interacts with a device M_1 meant to measure the observable X. We depict this interaction with the controlled-NOT (CNOT) symbol, although more generally it represents a controlled-shift unitary, $U_X = \sum_j [X_j] \otimes \mathbb{S}^j \otimes \mathbb{1}_{M_2}$, acting on the tripartite Hilbert space $\mathcal{H}_{SM_1M_2}$, where $\mathbb{S} = \sum_k |k+1\rangle\langle k|$ is the shift operator and $[X_j]$ is a shorthand notation for the dyad $|X_j\rangle\langle X_j|$. This is a unitary model for the measurement process [21]. After this, the system interacts with a second device M_2, which measures
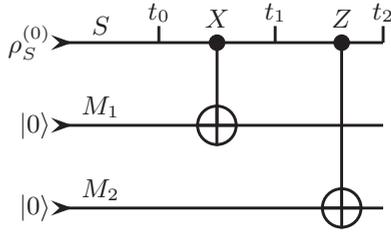
FIG. 1. Circuit diagram for the sequential measurement of the X and Z observables on system S.

the Z observable; the unitary is given by $U_Z = \sum_j [Z_j] \otimes \mathbb{1}_{M_1} \otimes \mathbb{S}^j$. We suppose that both M_1 and M_2 are initially in the $|0\rangle$ state, although later in this Rapid Communication we consider the effect of relaxing this assumption. We denote the states at times t_0, t_1, and t_2 in Fig. 1 as $\rho_{SM_1M_2}^{(0)}$, $\rho_{SM_1M_2}^{(1)}$, and $\rho_{SM_1M_2}^{(2)}$, respectively.

Entanglement generation. We focus on the bipartite entanglement $E(X,Z)$ between S and the joint system M_1M_2 present in the final state:

$$\rho_{SM_1M_2}^{(2)} = \sum_{j,k,l,m} [Z_l][X_j]\rho_S^{(0)}[X_k][Z_m] \otimes |j\rangle\langle k| \otimes |l\rangle\langle m|.$$

For concreteness we consider E to be the distillable entanglement [8], i.e., the optimal rate for distilling Einstein-Podolsky-Rosen (EPR) pairs $(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$ using local operations and classical communication (LOCC) in the asymptotic limit of infinitely many copies of the state. However, our result holds for several other entanglement measures, because distillable entanglement is itself a lower bound for such measures [8].

Consider first the case where X and Z are MUBs. In this case, $\rho_{SM_1M_2}^{(2)}$ is maximally entangled across the $S:M_1M_2$ cut, regardless of the system's initial state $\rho_S^{(0)}$. One can see this by noting that, if we choose the LOCC operation that measures M_1 in the standard basis and communicates the result to the party holding S, the resulting conditional pure state on SM_2 is, up to an irrelevant local change of basis, an EPR pair (generalized to dimension d) of the form $\sum_{i=0}^{d-1} |i\rangle|i\rangle/\sqrt{d}$. Alternatively, and more elegantly, we can factor out a maximally entangled state simply by performing a local unitary on M_1M_2; more precisely, the following holds.

Proposition 1. Let X and Z be MUBs. Define $H_{M_1} = \sum_j |X_j\rangle\langle j|$ and the controlled unitary $U_{M_1M_2} = \sum_j \sigma_X^j \otimes [j]$, where $\sigma_X^j := \sqrt{d} \sum_k \langle X_k | Z_j \rangle [X_k]$. Then

$$U_{M_1M_2} H_{M_1} \rho_{SM_1M_2}^{(2)} H_{M_1}^\dagger U_{M_1M_2}^\dagger = [\Phi]_{SM_2} \otimes \left(\rho_S^{(0)}\right)_{M_1}, \quad (3)$$

with $|\Phi\rangle = (\sum_j |Z_j\rangle|j\rangle)\sqrt{d}$: The local unitary $U_{M_1M_2} H_{M_1}$ applied to $\rho_{SM_1M_2}^{(2)}$ leaves M_1 in the system's initial state $\rho_S^{(0)}$, and SM_2 maximally entangled.

Thus, in the case of MUBs, we can identify several tasks that are accomplished by sequentially measuring X and Z as in Fig. 1. Besides producing maximal entanglement, the state $\rho_S^{(0)}$ is "teleported" from the system to the measurement devices. Indeed, the protocol we have described above is commonly known as *coherent teleportation* [19,20]. Furthermore, since S is maximally entangled to M_1M_2 at the end of the protocol, then, by the monogamy principle [22], S must be completely

uncorrelated with any other system S'. The procedure of performing an operation on S to destroy its potential correlations with S' is known as *decoupling* [14–18]. Our main contribution is to extend the above discussion to the case where X and Z have partial complementarity ($c > 1/d$): *Can we still create entanglement, coherently teleport, and decouple even if X and Z are not MUBs, and if so, to what degree?*

Our main result (2), says that, as soon as there is partial complementarity between X and Z, some distillable entanglement is present in $\rho_{SM_1M_2}^{(2)}$.

Theorem 2. Let $E(X,Z)$ denote the distillable entanglement between S and M_1M_2 at time t_2 in Fig. 1. Then (2) holds.

Proof. We give two alternative proofs. The first is based on the uncertainty principle with quantum memory [23] and the second is based on the monotonicity of entanglement under LOCC [8]. The second proof approach yields a slightly stronger version of (2).

In the first approach we apply the uncertainty principle with quantum memory [23] at time t_1 (just after the X measurement) to get

$$H(X|M_1M_2)_{\rho^{(1)}} + H(Z|S')_{\rho^{(1)}} \geqslant \log_2(1/c), \quad (4)$$

where we let S' purify the initial state $\rho_S^{(0)}$, and where the first and second terms in (4) are the conditional entropies of $\rho_{XM_1M_2}^{(1)} := \sum_j [X_j]\rho_{SM_1M_2}^{(1)}[X_j]$ and $\rho_{ZS'}^{(1)} := \sum_k [Z_k]\rho_{SS'}^{(1)}[Z_k]$, respectively. The von Neumann conditional entropy of σ is defined as $H(A|B)_\sigma := H(\sigma_{AB}) - H(\sigma_B)$, with $H(\sigma) = -\text{Tr}(\sigma \log_2 \sigma)$ the von Neumann entropy. Because X was already measured by M_1, we have $H(X|M_1M_2)_{\rho^{(1)}} = 0$. Also, from a result in Refs. [9,24], we have $H(Z|S')_{\rho^{(1)}} = E(X,Z)$, completing the proof.

In the second approach, we note that the final entanglement is larger than the average entanglement obtained from measuring M_1 in the standard basis followed by communicating the result to the party holding system S. That is, $E(X,Z) \geqslant \sum_j p_j H(\rho_{S,j}^{(2)})$, where we used that the conditional states associated with different measurement outcomes are bipartite pure states, $p_j \rho_{SM_2,j}^{(2)} = \text{Tr}_{M_1}[(\mathbb{1} \otimes |j\rangle\langle j| \otimes \mathbb{1})\rho_{SM_1M_2}^{(2)}]$, hence their entanglement is the entropy of the reduced state $\rho_{S,j}^{(2)} = \text{Tr}_{M_2}(\rho_{SM_2,j}^{(2)})$. We obtain

$$E(X,Z) \geqslant \sum_j p_j H(\{|\langle X_j | Z_k\rangle|^2\}_k), \quad (5)$$

where the entropy on the rhs is the classical entropy of the set of overlaps obtained from varying the index k. Equation (5) is slightly more complicated than (2) because it depends on the initial state through the probabilities $p_j = \langle X_j | \rho_S^{(0)} | X_j \rangle$. On the other hand, it is slightly stronger, implying (2) by noting that Shannon entropy upper-bounds the min-entropy $H_{\min}(\{q_k\}) = -\log_2 \max_k q_k$, and averaging over j in (5) yields a larger value than minimizing over j, completing the proof. ∎

So, even for limited complementarity, the circuit in Fig. 1 still generates entanglement "efficiently." Using our main result, we also prove below that decoupling and coherent teleportation are approximately achieved in the case of approximate complementarity. We further consider two generalizations of our results: to the case of mixed

measurement devices, and to the case of an arbitrary number of sequential measurements.

Decoupling. Decoupling [14–18] consists in transforming an arbitrary bipartite state $\rho_{SS'}$ into some tensor product $\sigma_S \otimes \sigma_{S'}$, and it has specific applications in state merging [25] and quantum cryptography [26]. Decoupling strategies often involve a local operation performed on system S only. Note that the effect on S of the circuit of Fig. 1 is equivalent to a random unitary channel $\rho_S^{(0)} \mapsto (1/d^2) \sum_{k,l} (\sigma_Z^k \sigma_X^l) \rho_S^{(0)} (\sigma_Z^k \sigma_X^l)^\dagger$, consisting of d^2 unitaries, each of which is a product of generalized Pauli operators $\sigma_X = \sum_j \omega^j |X_j\rangle\langle X_j|$ and $\sigma_Z = \sum_j \omega^j |Z_j\rangle\langle Z_j|$ with $\omega = e^{2\pi i/d}$. It is well known that when X and Z are MUBs, this results in $\rho_{SS'}^{(0)} \mapsto \rho_{SS'}^{(2)} = \mathbb{1}/d \otimes \rho_{S'}^{(2)}$.

Can we guarantee approximate decoupling when X and Z exhibit only approximate complementarity? Because of monogamy of correlations, this question is closely related to the question of whether the X and Z measurements create entanglement [18]: If S is highly entangled to $M_1 M_2$, then it is almost completely decoupled from some other system S'. Thus, (2) must imply a corresponding decoupling result. To prove this, we consider the relative entropy distance $D(\sigma \| \tau) := \text{Tr}(\sigma \log_2 \sigma) - \text{Tr}(\sigma \log_2 \tau)$ [27]. We find the following.

Corollary 3. For any initial $\rho_{SS'}^{(0)}$, at time t_2,

$$D\left(\rho_{SS'}^{(2)} \big\| \mathbb{1}/d \otimes \rho_{S'}^{(2)}\right) \leqslant \log_2(dc). \qquad (6)$$

Proof. The state $\rho_{SM_1M_2}^{(2)}$ falls into a class of states [9,28] for which the distillable entanglement satisfies $E(X,Z) = -H(S|M_1M_2)_{\rho^{(2)}}$. Moreover, $H(S|M_1M_2)_{\rho^{(2)}} + H(S|S')_{\rho^{(2)}} \geqslant 0$ because of strong subadditivity of entropy [29]. Finally, note that $\log_2 d - H(S|S')_{\rho^{(2)}}$ is the relative entropy on the left-hand side of (6). ∎

If X and Z are complementary, $c = 1/d$ and Corollary 3 implies $\rho_{SS'}^{(2)} = \mathbb{1}/d \otimes \rho_{S'}^{(2)}$. More generally, (6) shows that S and S' are *almost* decoupled if X and Z are *almost* complementary.

Coherent teleportation. When X and Z are MUBs, Proposition 1 says that there exists a local unitary on $M_1 M_2$ that recovers the input state $\rho_S^{(0)}$. As we decrease the complementarity between X and Z, the channel $\mathcal{E} : S(t_0) \to S(t_2)$ goes from the completely depolarizing channel to the dephasing channel (in the limit $X = Z$), while the complementary channel $\mathcal{E}^c : S(t_0) \to M_1 M_2(t_2)$ goes from a perfect quantum channel to a dephasing channel. One can therefore consider the quantum capacity of $\mathcal{E}^c$, i.e., the optimal rate at which $\mathcal{E}^c$ allows for the reliable transmission of quantum information [30], as a measure of the complementarity of X and Z. We make these ideas quantitative in the following corollary.

Corollary 4. The quantum capacity $Q(\mathcal{E}^c)$ of the channel $\mathcal{E}^c$ satisfies $Q(\mathcal{E}^c) \geqslant \log_2(1/c)$. Furthermore, there exists a recovery map $\mathcal{R}$ such that the entanglement fidelity $F_e(\mathcal{R} \circ \mathcal{E}^c) := \text{Tr}([\Phi]_{SS'}(\mathcal{R} \circ \mathcal{E}^c)_S([\Phi]_{SS'}))$ is lower-bounded by $F_e(\mathcal{R} \circ \mathcal{E}^c) \geqslant 1/(dc)$.

Proof. Suppose $\rho_S^{(0)} = \mathbb{1}/d = \text{Tr}_{S'}[\Phi]_{SS'}$; then from (2),

$$\log_2(1/c) \leqslant E(X,Z) = -H(S|M_1M_2)_{\rho^{(2)}}$$
$$= H\left(\rho_{M_1M_2}^{(2)}\right) - H\left(\rho_S^{(2)}\right), \qquad (7)$$

where the second equality follows from $H(\rho_{SM_1M_2}^{(2)}) = H(\rho_S^{(0)}) = H(\rho_S^{(2)})$. The last line is a lower bound on the quantum capacity of the channel $\mathcal{E}^c$ [30].

The proof of the second claim follows from the operational meaning of the conditional min-entropy [31] $H_{\min}(A|B)_\sigma = -\log_2[\dim(\mathcal{H}_A) \max_{\mathcal{R}} \langle \Phi | (\mathcal{I} \otimes \mathcal{R})(\sigma_{AB}) | \Phi \rangle]$, where the max is over all completely positive trace-preserving maps $\mathcal{R}$, which gives $\max_{\mathcal{R}} F_e(\mathcal{R} \circ \mathcal{E}^c) = (1/d) 2^{-H_{\min}(S'|M_1M_2)_{\rho^{(2)}}}$, where S' purifies $\rho_S^{(0)}$. Finally note that $-H_{\min}(S'|M_1M_2)_{\rho^{(2)}} \geqslant -H(S'|M_1M_2)_{\rho^{(2)}} = E(X,Z)$. ∎

Corollary 4 allows us to say that we can *approximately* teleport the state $\rho_S^{(0)}$ when X and Z are *almost* MUBs. Conceptually, Corollary 4 follows from (2) since the latter says that S becomes highly entangled to $M_1 M_2$, which implies that $\rho_S^{(2)}$ must be close to the maximally mixed state regardless of the input $\rho_S^{(0)}$, which implies that $\mathcal{E}$ is a bad channel and hence the complementary channel $\mathcal{E}^c$ must be good [32].

Initially mixed devices. In Fig. 1, we assumed the initial states of the measurement devices were pure, $\rho_{M_1}^{(0)} = |0\rangle\langle 0|$ and $\rho_{M_2}^{(0)} = |0\rangle\langle 0|$. We now focus on the effects of mixing. While we still assume that the system-device interaction takes place on a time scale on which coherence is preserved, it is natural to restrict our attention to the case where the device's initial state is diagonal in the basis—which we have taken as the standard basis—in which the measurement result is "recorded": Off-diagonal elements in this basis typically correspond to macroscopic superpositions and are rapidly decohered [21]. So we write $\rho_{M_1}^{(0)} = \sum_j \alpha_j |j\rangle\langle j|$ and $\rho_{M_2}^{(0)} = \sum_j \beta_j |j\rangle\langle j|$, with $\{\alpha_j\}$ and $\{\beta_j\}$ normalized probability distributions.

For a single measurement, the effect of mixing is to reduce the ability of the device to "accept" information [33]. Thus, one expects mixing to adversely affect the creation of entanglement in our setup. However, as proven in the Supplemental Material [34], we find that limited mixing only partially hinders entanglement creation. We have the following simple bound that generalizes Eq. (2) to the case of mixed devices:

$$E(X,Z) \geqslant \log_2(1/c) - \left[H\left(\rho_{M_1}^{(0)}\right) + H\left(\rho_{M_2}^{(0)}\right) \right]. \qquad (8)$$

For decoupling, (6) will of course still hold in the case of initially mixed devices, since $\rho_{SS'}^{(2)}$ is the same regardless of whether $\rho_{M_1}^{(0)}$ and $\rho_{M_2}^{(0)}$ are mixed. For coherent teleportation, Corollary 4 generalizes in a simple way [34]; for example, we find

$$Q(\mathcal{E}^c) \geqslant \log_2(1/c) - \left[H\left(\rho_{M_1}^{(0)}\right) + H\left(\rho_{M_2}^{(0)}\right) \right]. \qquad (9)$$

More than two measurements. Our main result can be generalized in a different way. Instead of two measurements, we may consider $n \geqslant 2$ measurements. Suppose then that system S interacts sequentially with n measurement devices, each initialized in $|0\rangle$. Time t_m corresponds to the time immediately after the mth measurement device M_m, which measures observable X^m of S, has interacted with S. We are interested in the entanglement at time t_n between S and the measurement devices $M_1 \ldots M_n$, denoted $E(X^1, \ldots, X^n)$. One could also consider the entanglement at some prior

time $t_m < t_n$; however, this will always be smaller than the entanglement at time t_n, because

$$E(X^1, \ldots, X^n) \geqslant E(X^1, \ldots, X^{n-1}). \qquad (10)$$

The proof of (10) notes that each measurement can be thought of as a random-unitary channel acting on S, where the information about which unitary is applied is stored in the measurement device. Consider the LOCC operation that extracts this information from M_n and then communicates the result to S, allowing the local unitary on S to be undone [35]. Thus, for every outcome this will restore the state on $SM_1 \ldots M_{n-1}$ to the state at time t_{n-1} [13]. Since E is nonincreasing under LOCC [8], the desired result follows.

The following bound generalizes (2) to the case $n \geqslant 2$:

$$E(X^1, \ldots, X^n) \geqslant \max_{m < n} \log_2 \frac{1}{c_{m,m+1}}, \qquad (11)$$

where $c_{m,m+1} := \max_{j,k} |\langle X_j^m | X_k^{m+1} \rangle|^2$. The proof of (11) is essentially the same as that of (2) and is provided in Ref. [34]. Equation (11) implies that if two MUBs are measured one after the other at any point in the sequence of measurements, then the system will become maximally entangled with the measurement devices, and any further measurements will not generate any more entanglement.

By the same argument in Corollary 3, the analogous decoupling result follows:

$$D\big(\rho_{SS'}^{(n)} \big| \big| \mathbb{1}/d \otimes \rho_{S'}^{(n)}\big) \leqslant \min_{m < n} \log_2(dc_{m,m+1}), \qquad (12)$$

where $\rho_{SS'}^{(n)}$ is the state at time t_n. Likewise, by the same argument in Corollary 4, the analogous coherent teleportation result follows:

$$Q(\mathcal{E}^c) \geqslant \max_{m < n} \log_2 \frac{1}{c_{m,m+1}}, \qquad (13)$$

where $\mathcal{E}^c$ is the channel from S at t_0 to $M_1 \ldots M_n$ at t_n, and the analogous generalization for F_e also holds.

Conclusions. We proposed that a signature and a quantification of complementarity of two observables is given by the entanglement generated when the two observables are sequentially measured on the same system by means of a coherent interaction with corresponding measurement devices. We also noted how this approach to complementarity is intimately related to the information-processing primitives of decoupling and coherent teleportation.

The importance of complementarity in quantum information processing has been explored previously, e.g., by Renes and collaborators (see Ref. [36] and references therein). Such works typically focus on the transmission of information in complementary bases, which turns out to be sufficient to ensure transmission of quantum information. However, the physical scenario of sequential coherent complementary measurements is not obviously connected to mathematical theorems [37–40] regarding the knowledge or transmission of complementary information, particularly in the case of partial complementarity.

The fact that, in our scheme, the complementarity of two observables measures their power to process quantum information suggests to search for further "uncertainty" (or "certainty") relations for other information-processing tasks or quantum computing algorithms. Reference [41] has already made some progress along these lines, and we expect that our work will stimulate further results in the same perspective.

Note added in proof. One of us (P.J.C.) has also coauthored Ref. [42]. There, preexisting entanglement is connected to the uncertainty of measurements on distinct but identically prepared systems. Such work is not closely related to the present one, since we consider dynamically created entanglement during sequential measurements.

[1] W. C. Price and S. S. Chissick, *The Uncertainty Principle and Foundations of Quantum Mechanics* (Wiley, New York, 1977).

[2] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).

[3] W. Heisenberg, Z. Phys. **43**, 172 (1927).

[4] E. Kennard, Z. Phys. **44**, 326 (1927).

[5] H. P. Robertson, Phys. Rev. **34**, 163 (1929).

[6] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).

[7] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[8] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[9] P. J. Coles, Phys. Rev. A **86**, 062334 (2012).

[10] A. Streltsov, H. Kampermann, and D. Bruß, Phys. Rev. Lett. **106**, 160401 (2011).

[11] M. Piani, S. Gharibian, G. Adesso, J. Calsamiglia, P. Horodecki, and A. Winter, Phys. Rev. Lett. **106**, 220403 (2011).

[12] S. Gharibian, M. Piani, G. Adesso, J. Calsamiglia, and P. Horodecki, Int. J. Quantum Inf. **9**, 1701 (2011).

[13] M. Piani and G. Adesso, Phys. Rev. A **85**, 040301 (2012).

[14] B. Schumacher and M. D. Westmoreland, Quantum Inf. Process. **1**, 5 (2002).

[15] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, arXiv:1012.6044.

[16] F. Dupuis, Ph.D. thesis, Université de Montréal, 2009.

[17] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).

[18] F. Buscemi, New J. Phys. **11**, 123002 (2009).

[19] G. Brassard, S. L. Braunstein, and R. Cleve, Physica D **120**, 43 (1998).

[20] A. Harrow, Phys. Rev. Lett. **92**, 097902 (2004).

[21] W. H. Zurek, Rev. Mod. Phys. **75**, 715 (2003).

[22] M. Seevinck, Quantum Inf. Process. **9**, 273 (2010).

[23] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).

[24] P. J. Coles, Phys. Rev. A **85**, 042103 (2012).

[25] M. Horodecki, J. Oppenheim, and A. Winter, Nature (London) **436**, 673 (2005).

[26] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[27] While the relative entropy operationally measures distinguishability [43], it is, mathematically speaking, not a distance; for example, it is not symmetric in σ and τ. Nonetheless, Pinsker's inequality relates it to the trace distance: $D(\sigma\|\tau) \geqslant \|\sigma - \tau\|_1^2/(2\ln 2)$, $\|X\|_1 = \text{Tr}\sqrt{X^\dagger X}$.

[28] M. F. Cornelio, M. C. de Oliveira, and F. F. Fanchini, Phys. Rev. Lett. **107**, 020502 (2011).

[29] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 5th ed. (Cambridge University Press, Cambridge, UK, 2000).

[30] M. M. Wilde, *Quantum Information Theory*, 1st ed. (Cambridge University Press, Cambridge, 2013).

[31] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[32] D. Kretschmann, D. Schlingemann, and R. Werner, IEEE Trans. Inf. Theory **54**, 1708 (2008).

[33] V. Vedral, Phys. Rev. Lett. **90**, 050401 (2003).

[34] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.89.010302 for proofs and elaboration of our results.

[35] M. Gregoratti and R. F. Werner, J. Mod. Opt. **50**, 915 (2003).

[36] J. M. Renes, Habilitation Thesis, TU Darmstadt, 2011, arXiv:1212.2379.

[37] M. Christandl and A. Winter, IEEE Trans. Inf. Theory **51**, 3159 (2005).

[38] J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).

[39] J. M. Renes, arXiv:1003.1150.

[40] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **83**, 062338 (2011).

[41] F. G. S. L. Brandao and M. Horodecki, Quantum Inf. Comput. **13**, 0901 (2013).

[42] M. Berta, P. J. Coles, and S. Wehner, arXiv:1302.5902.

[43] M. Ohya and D. Petz, *Quantum Entropy and Its Use* (Springer, Berlin, 2004).