10-8-2012

Quantum discord and classical correlation can tighten the uncertainty principle in the presence of quantum memory

Arun Kumar Pati
Harish Chandra Research Institute

Mark M. Wilde
Université McGill

A. R.Usha Devi
Bangalore University

A. K. Rajagopal
Harish Chandra Research Institute

Sudha
Inspire Institute Inc.

Recommended Citation

Pati, A., Wilde, M., Devi, A., Rajagopal, A., & Sudha. (2012). Quantum discord and classical correlation can tighten the uncertainty principle in the presence of quantum memory. *Physical Review A - Atomic, Molecular, and Optical Physics, 86* (4) https://doi.org/10.1103/PhysRevA.86.042105

Quantum discord and classical correlation can tighten the uncertainty principle in the presence of quantum memory

Arun Kumar Pati,[1] Mark M. Wilde,[2] A. R. Usha Devi,[3,4] A. K. Rajagopal,[1,4] and Sudha[4,5]

[1]*Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India,*
[2]*School of Computer Science, McGill University, Montreal, Quebec H3A 2A7, Canada,*
[3]*Department of Physics, Bangalore University, Bangalore-560 056, India,*
[4]*Inspire Institute Inc., Alexandria, Virginia, 22303, USA,*
[5]*Department of Physics, Kuvempu University, Shankaraghatta, Shimoga-577 451, India.*

(Dated: November 4, 2018)

Uncertainty relations capture the essence of the inevitable randomness associated with the outcomes of two incompatible quantum measurements. Recently, Berta *et al.* have shown that the lower bound on the uncertainties of the measurement outcomes depends on the correlations between the observed system and an observer who possesses a quantum memory. If the system is maximally entangled with its memory, the outcomes of two incompatible measurements made on the system can be predicted precisely. Here, we obtain a new uncertainty relation that tightens the lower bound of Berta *et al.*, by incorporating an additional term that depends on the quantum discord and the classical correlations of the joint state of the observed system and the quantum memory. We discuss several examples of states for which our new lower bound is tighter than the bound of Berta *et al.* On the application side, we discuss the relevance of our new inequality for the security of quantum key distribution and show that it can be used to provide bounds on the distillable common randomness and the entanglement of formation of bipartite quantum states.

PACS numbers: 03.65.Ta, 03.65.Db, 03.65.Ud

The Heisenberg uncertainty relation is one of the fundamental concepts in quantum theory [1]. In recent years, entropic uncertainty relations (EURs) [2] have gained importance because of their operational applications for privacy issues in cryptographic tasks [3], in the detection of entangled states [3], and in constructing error-correcting codes for communicating quantum or private classical information [4–6]. A revision of the Maasen-Uffink EUR [2], which includes the possibility of a quantum memory correlated with the observed system, has been identified recently by Berta *et al.* [3]. Interestingly, if the system is maximally entangled with its memory, the outcomes of two incompatible measurements made on distinct and identical copies of such a state can be predicted precisely by an observer with access to the quantum memory. It may be noted that the possibility of violating the uncertainty relation using an entangled pair was conceived as early as 1934 by Karl Popper [7], who had proposed an experiment to do so.

The uncertainty principle sets limits on our ability to predict the outcomes of two incompatible measurements, and it was originally formulated by Heisenberg [1] for position and momentum observables. Robertson [8] and Schrödinger [9] generalized it to arbitrary pairs of non-commuting observables P and Q and it is well known in the following form:

$$(\Delta P)(\Delta Q) \geq \frac{1}{2}\,|\langle [P,Q]\rangle|, \tag{1}$$

where the uncertainties in the measurements are quantified in terms of the standard deviations $(\Delta P) \equiv \sqrt{\langle P^2\rangle - \langle P\rangle^2}$, $(\Delta Q) \equiv \sqrt{\langle Q^2\rangle - \langle Q\rangle^2}$, and the commutator $[P,Q] \equiv PQ - QP$.

Deutsch subsequently advocated for characterizing the "spread" in the outcomes of two incompatible measurements via Shannon entropies

$$H(P) \equiv -\sum_i p_i \log_2 p_i, \quad H(Q) \equiv -\sum_j q_j \log_2 q_j, \tag{2}$$

where p_i and q_j are the probability distributions of the measurement outcomes, rather than with standard deviations [10] because EURs provide an information-theoretic basis for quantifying uncertainties [11]. The entropic uncertainty bound for position and momentum observables was first proposed by Hirschmann [12] more than five decades ago, and it was improved further during later years [13, 14]. The entropic constraints for the outcomes of an arbitrary pair of observables P and Q were formulated by Deutsch [10] and were subsequently improved by various authors [15–17]. A conjecture put forth by Kraus [17] was proved by Maassen and Uffink [2], leading to the following EUR:

$$H(P) + H(Q) \geq -2\log_2 c(P,Q), \tag{3}$$

where $c(P,Q) \equiv \max_{i,j}|\langle p_i|q_j\rangle|$, $\{|p_i\rangle\}$, $\{|q_j\rangle\}$ are the eigenvectors of P and Q, respectively. Later, this bound was improved and tightened by several authors [3, 18–20] to hold for arbitrary POVMs and to include a state-dependent term in the lower bound depending on the entropy of the state of the system:

$$H(P) + H(Q) \geq -2\log_2 c(P,Q) + S(\rho), \tag{4}$$

where P is now more generally a positive operator-valued measure (POVM) with elements $\{\Lambda_p\}$, Q is a POVM with elements $\{\Gamma_q\}$, the entropies $H(P)$ and $H(Q)$ are

the Shannon entropies of the distributions $\mathrm{Tr}\{\Lambda_p \rho\}$ and $\mathrm{Tr}\{\Gamma_q \rho\}$, respectively, with ρ the state of the quantum system, $c(P,Q)$ is now an incompatibility measure for the POVMs: $c(P,Q) \equiv \max_{p,q} \left\| \sqrt{\Lambda_p}\sqrt{\Gamma_q} \right\|_\infty^2$, and the entropy $S(\rho)$ is the von Neumann entropy of ρ: $S(\rho) \equiv -\mathrm{Tr}\{\rho \log \rho\}$.

The inequality in (4) bounds the entropies of the outcomes of P and Q in the system when it is not correlated with a quantum memory. Accessibility of a quantum memory (so that the system A and the memory B are in some state ρ_{AB}) leads to a refinement of (4) [3]:

$$S(P|B) + S(Q|B) \geq -2\log_2 c(P,Q) + S(A|B), \quad (5)$$

where the lower bound is expressed similarly to that in (4): as a sum of the measurement incompatibility $-2\log_2 c(P,Q)$ and the state-dependent term $S(A|B)$. The quantities $S(P|B) \equiv S(\rho_{PB}) - S(\rho_B)$ and $S(Q|B) \equiv S(\rho_{QB}) - S(\rho_B)$ are the conditional von Neumann entropies of the post measurement states on the measurement register and the memory:

$$\rho_{PB} = \sum_p |p\rangle\langle p|_P \otimes \mathrm{Tr}_A\{(\Lambda_p \otimes I)\rho_{AB}\}, \quad (6)$$

$$\rho_{QB} = \sum_q |q\rangle\langle q|_Q \otimes \mathrm{Tr}_A\{(\Gamma_q \otimes I)\rho_{AB}\}, \quad (7)$$

respectively resulting after the POVMs P and Q are performed on the system A, with additional information stored in the memory B. The entropies $S(P|B)$ and $S(Q|B)$ quantify the uncertainty about the outcome of a measurement on the system from the perspective of a party holding the quantum memory B. Here, $S(A|B) \equiv S(\rho_{AB}) - S(\rho_B)$ is the conditional von Neumann entropy between A and B. The additional term $S(A|B)$ on the right hand side can become negative when the system A is entangled with its quantum memory B, suggesting that it should be possible to reduce the sum of the conditional uncertainties down to zero. Indeed, suppose that the measurements P and Q are two canonical-conjugate observables and that the system and memory are in a maximally entangled state. In this case, the sum $S(P|B) + S(Q|B)$ is equal to zero, meaning that the possessor of the quantum memory can predict the outcome of either measurement on the system simply by measuring his quantum memory. The RHS of the above inequality is consistent with this—when the system and memory are in a maximally entangled state, the conditional entropy $S(A|B)$ assumes its most negative value so that $S(A|B) = -\log_2 d$ (where d denotes the dimension of the system) and as $-2\log_2 c(P,Q)$ cannot exceed the value $\log_2 d$ [11], the RHS of (5) reduces to zero. This EUR has been recently experimentally tested [21, 22].

One of the major goals in quantum information theory is to understand and exploit various resources like entanglement, quantum correlations [23], and classical correlations [24] in a composite quantum state. Entanglement has been used extensively in many quantum information processing tasks. However, the role of quantum and classical correlations is beginning to be understood and is a subject of extensive research in recent years [25]. Our objective here is to understand how other correlation measures such as quantum discord [23] and classical correlation [24] can play a role in tightening the EUR in (5). This leads to two new EURs, and we will show that the first inequality provides a new lower bound on the regularized entanglement of formation for any density operator shared between Alice and Bob. Also, we show that it can be used to give an upper bound on the distillable common randomness [26, 27] $C_D^{\rightarrow}(\rho_{CB})$ with a third-party system. The second inequality can be used to provide an improved bound for the secure key rate in a quantum key distribution protocol, in the case that Alice and Bob have some description of the state that they share.

In this paper, we prove the following new entropic uncertainty relation:

Theorem 1 *The uncertainties $S(P|B)$ and $S(Q|B)$ are lower bounded by the measurement incompatibility $-2\log_2 c(P,Q)$, the conditional entropy $S(A|B)$ of the state ρ_{AB}, and the larger of zero and the difference between the state's quantum discord $D_A(\rho_{AB})$ and its classical correlation $J_A(\rho_{AB})$:*

$$S(P|B) + S(Q|B) \geq -2\log_2 c(P,Q) + S(A|B) + \max\{0, D_A(\rho_{AB}) - J_A(\rho_{AB})\}. \quad (8)$$

The classical correlation $J_A(\rho_{AB})$ is defined as [24]

$$J_A(\rho_{AB}) \equiv \max_{\{\Upsilon_x\}} I(X;B),$$

where the mutual information $I(X;B) \equiv S(X) + S(B) - S(XB)$ is with respect to the post-measurement state

$$\rho_{XB} = \sum_x |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\{(\Upsilon_x \otimes I)\rho_{AB}\},$$

and the optimization is over all POVMs $\{\Upsilon_x\}$ acting on the system A—note that it suffices to consider rank-one POVMs in this optimization [25], because for every POVM that is not rank-one, one can construct from it a rank-one POVM that gives a higher classical correlation. If a state has no quantum correlations, the classical correlation $J_A(\rho_{AB})$ is equal to the mutual information $I(A;B) \equiv S(\rho_A) + S(\rho_B) - S(\rho_{AB})$ itself [24]. The notion of quantum discord and classical correlation between two systems plays an important role in the study of quantum correlations. If one defines the total correlation using mutual information, then the difference between the total and classical correlations gives the so-called quantum discord [23]:

$$D_A(\rho_{AB}) \equiv I(A;B) - J_A(\rho_{AB}), \quad (9)$$

and it is a measure of quantum correlations in the state ρ_{AB}.

We now prove the uncertainty relation as stated in (8).

Proof [Theorem 1] First consider that it suffices to prove the following inequality:

$$S(P|B) + S(Q|B) \geq -2\log_2 c(P,Q) + S(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB}), \quad (10)$$

because combining it with the bound in (5) leads to the bound in (8). So, consider a bipartite density operator ρ_{AB}. If Alice performs the POVM P, then the post-measurement state is as in (6), and similarly it is as in (7) if she chooses to perform the POVM Q. We then have

$$\begin{aligned} &S(P|B) + S(Q|B) \\ &= H(P) - I(P;B) + H(Q) - I(Q;B) \\ &\geq H(P) + H(Q) - 2J_A(\rho_{AB}) \\ &\geq -2\log_2 c(P,Q) + S(A) - 2J_A(\rho_{AB}) \\ &= -2\log_2 c(P,Q) + S(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB}). \end{aligned} \quad (11)$$

The first equality is an identity for the quantum mutual information. The first inequality follows from the definition of the classical correlation $J_A(\rho_{AB})$ and the fact that the POVMs P or Q may not necessarily be the maximizing POVM for $J_A(\rho_{AB})$, so that $I(P;B) \leq J_A(\rho_{AB})$ and $I(Q;B) \leq J_A(\rho_{AB})$. In the second inequality, we apply the uncertainty relation in (4). The second equality exploits the identity $S(A) = S(A|B) + I(A;B)$ and the definition of the quantum discord in (9). □

Our new lower bound in (8) tightens the state-dependent term of the bound in (5) if the discord $D_A(\rho_{AB})$ is larger than the classical correlation $J_A(\rho_{AB})$. This occurs for several natural examples of bipartite states, including Werner states and isotropic states (see the appendices).

We discuss some examples to illustrate (8). Our first two examples recover the result of Berta *et al.* When the system is uncorrelated with the memory, $\rho_{AB} = \rho_A \otimes \rho_B$, we have $S(P|B) = H(P)$, $S(Q|B) = H(Q)$, $S(A|B) = S(A)$, and $D_A(\rho_{AB}) = J_A(\rho_{AB}) = 0$, resulting in the relation in (4). As a second example, we consider when the system and memory are in a pure maximally entangled state. In this case, $J_A(\rho_{AB}) = S(\rho_B) = \log_2 d$, $I(A;B) = 2\log_2 d$, $D_A(\rho_{AB}) = \log_2 d$, $-2\log_2 c(P,Q) \leq \log_2 d$ and hence the right hand side of (8) reduces to zero—as in the Berta *et al.* inequality—which is consistent with the fact that a quantum memory which is maximally entangled with the system assists in predicting the measurement outcomes of non-commuting observables precisely. In fact, our bound reduces to the bound of Berta *et al.* for all pure bipartite states, since the discord is equal to the classical correlation for these states. This reduction also occurs whenever the state is "classical-quantum" with A classical and B quantum. The discord is equal to zero for these states [25], so that it is always less than the classical correlation.

Our next example illustrates an important difference between our new inequality in (8) and the Berta *et al.* inequality in (5). We consider a two-qubit Werner state:

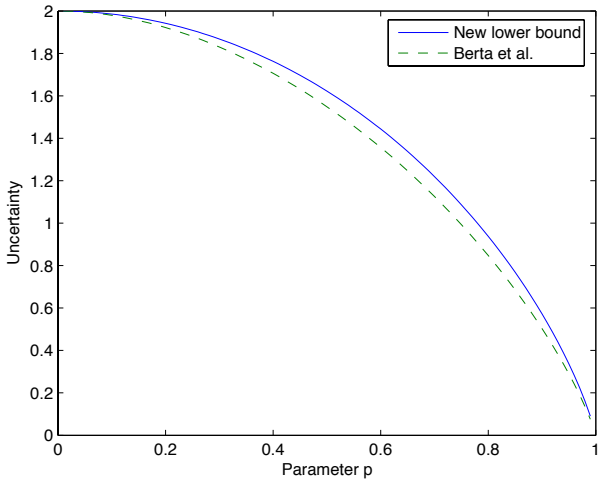

FIG. 1: The right hand side of our new inequality (8) $-2\log_2 c(\sigma_x,\sigma_z) + S(A|B) + \max\{0, D_A(\rho_{AB}) - J_A(\rho_{AB})\}$ (solid blue), and the right hand side of the Berta *et al.* inequality (5) $-2\log_2 c(\sigma_x,\sigma_z) + S(A|B)$ (dashed green), as a function of the noise parameter p, when the system and memory are prepared in the two qubit Werner state (12).

$$\rho_{AB} = \frac{1-p}{4} I_A \otimes I_B + p\,|\Phi^-\rangle_{AB}\langle\Phi^-|, \quad (12)$$

where $|\Phi^-\rangle_{AB} = (|0_A, 1_B\rangle - |1_A, 0_B\rangle)/\sqrt{2}$ is the Bell state and $0 \leq p \leq 1$. Measurements of σ_x and σ_z lead to the conditioned entropies $S(\sigma_x|B) = S(\sigma_z|B) = h((1-p)/2)$, where $h(x)$ is the binary entropy, so that

$$S(\sigma_x|B) + S(\sigma_z|B) = 2h((1-p)/2).$$

The incompatibility $c(\sigma_x,\sigma_z) = 1/\sqrt{2}$, the classical correlation in the state $J_A(\rho_{AB}) = 1 - h((1-p)/2)$, the entropy $S(A) = 1$, and the conditional entropy $S(A|B) = -\frac{3(1-p)}{4}\log_2\frac{(1-p)}{4} - \frac{1+3p}{4}\log_2\frac{1+3p}{4}$. Recall from (11) that our lower bound is equivalent to $-2\log_2 c(P,Q) + S(A) - 2J_A(\rho_{AB})$, which for this example becomes $1 + 1 - 2[1 - h((1-p)/2)] = 2h((1-p)/2)$. Thus the entropy sum $S(\sigma_x|B) + S(\sigma_z|B)$ *coincides with our lower bound* for all values of p, a significant tightening of the Berta *et al.* inequality. In Fig. 1 we have plotted the right hand sides of the inequalities in (5) and (8) to compare the bounds.

Interestingly, what occurs in the above Werner state example extends to higher-dimensional Werner and isotropic states. When the measurement is of Fourier-conjugate observables, the uncertainty sum $S(P|B) + S(Q|B)$ coincides with our lower bound in (8) for all dimensions and parameters of these states, demonstrating that our lower bound is perfectly tight for these states and measurements. Hence, these states may be called *minimum entropic uncertain states* of the EUR in (8). We refer the reader to the appendices for details of this

result, where we exploit recent findings of Chitambar [28]. Note that minimum uncertainty states of the Berta *et al.* bound were studied in Refs. [20, 29].

Berta *et al.* proved the following EUR for a tripartite state ρ_{ABE} [3]: $S(P|B) + S(Q|E) \geq -2\log_2 c(P,Q)$, which has implications for the security of quantum key distribution (QKD). We can further improve the lower bound to be as follows:

$$S(P|B) + S(Q|E) \geq -2\log_2 c(P,Q) + \max\{0, D_A(\rho_{A|(BE')}) - J_A(\rho_{AB})\}, \quad (13)$$

where the discord $D_A(\rho_{A|(BE')})$ is between the A and BE' systems of a purification $|\psi\rangle_{ABEE'}$ of the state ρ_{ABE} (note that $D_A(\rho_{A|(BE')}) = D_A(\rho_{AB})$ if the state ρ_{ABE} is already pure). The above EUR implies tighter security bounds on the ability of an eavesdropper E to predict the outcome of the Q measurement on the system A, again whenever the discord $D_A(\rho_{A|(BE')})$ is larger than the classical correlation $J_A(\rho_{AB})$ and in the case where Alice and Bob have some description of the state that they share. It might not always be possible to have such a description of the state, but in the case that they do, the above inequality may lead to improved bounds on the secure key rate.

The inequality in (13) follows by considering a purification $|\phi\rangle_{ABEE'}$ of the state ρ_{ABE} and the following chain of inequalities that follow from reasoning similar to that in (11):

$$\begin{aligned} &S(P|B) + S(Q|E) \quad (14)\\ &= H(P) - I(P;B) + H(Q) - I(Q;E)\\ &\geq H(P) + H(Q) - J_A(\rho_{AB}) - J_A(\rho_{AE})\\ &\geq -2\log_2(c) + S(A) - J_A(\rho_{AB}) - J_A(\rho_{AE}) \end{aligned}$$

We now focus on rewriting the term $S(A) - J_A(\rho_{AE})$:

$$\begin{aligned} S(A) - J_A(\rho_{AE}) &= S(A) - S(E) + \min_{\{\Lambda_a\}} S(E|\{\Lambda_a\})\\ &= S(A) - S(ABE') + \min_{\{\Lambda_a\}} S(BE'|\{\Lambda_a\})\\ &= S(A) + S(BE') - S(ABE')\\ &\quad - \left[S(BE') - \min_{\{\Lambda_a\}} S(BE'|\{\Lambda_a\})\right]\\ &= I(A;BE') - J_A(\rho_{A|(BE')})\\ &= D_A(\rho_{A|(BE')}) \end{aligned}$$

The first equality follows by definition. The second equality follows by noting that the state on systems $ABEE'$ is pure, so that $S(E) = S(ABE')$. Also, the optimal POVM performed on A is a rank-one POVM, so that the conditional state on EBE' is pure, implying that $\min_{\{\Lambda_a\}} S(E|\{\Lambda_a\}) = \min_{\{\Lambda_a\}} S(BE'|\{\Lambda_a\})$. The other equalities follow from definitions. Substituting back in (14), we obtain

$$S(P|B)+S(Q|E) \geq -2\log_2(c)+D_A(\rho_{A|(BE')})-J_A(\rho_{AB})$$

(Again, it suffices to prove the inequality above because combining it with the bound $S(P|B) + S(Q|E) \geq -2\log_2 c(P,Q)$ of Berta *et al.* leads to the new inequality in (13).)

As a second application of our inequality, we show that it helps to give a lower bound on the entanglement of formation. Suppose that Alice and Bob share the state ρ_{AB}. Recall that the entanglement of formation $E_f(\rho_{AB})$ and its regularization $E_f^\infty(\rho_{AB})$ are as follows [25]:

$$E_f(\rho_{AB}) \equiv \inf \sum_x p(x) S(\phi_A^x),$$

$$E_f^\infty(\rho_{AB}) \equiv \lim_{k\to\infty} \frac{1}{k} E_f((\rho_{AB})^{\otimes k}),$$

where the infimum is over all ensembles $\{p(x), |\phi_x\rangle_{AB}\}$ such that $\rho_{AB} = \sum_x p(x)|\phi_x\rangle\langle\phi_x|_{AB}$ and $\phi_A^x = \mathrm{Tr}_B\{|\phi_x\rangle\langle\phi_x|_{AB}\}$. A recent result of Carlen and Lieb states that $E_f(\rho_{AB}) \geq -S(A|B)$ [30], from which it easily follows that $E_f^\infty(\rho_{AB}) \geq -S(A|B)$, by exploiting the fact that entropies are additive for tensor-power states. Alice and Bob could each measure the observable P on their shares of ρ_{AB}, or they could each measure the observable Q. Let p_e^P be the probability that the outcomes of P on Alice and Bob are different, and let p_e^Q be the probability that the outcomes of Q on Alice and Bob are different. Using the Fano inequality, we have $S(P|B) + S(Q|B) \leq b_F$, where $b_F \equiv h(p_e^P) + p_e^P \log(d-1) + h(p_e^Q) + p_e^Q \log(d-1)$. From the Carlen-Lieb inequality and our inequality in Theorem 1, we obtain a non-trivial lower bound on the regularized entanglement of formation:

$$E_f^\infty(\rho_{AB}) \geq -2\log_2 c(P,Q) + \max\{0, D_A(\rho_{AB}) - J_A(\rho_{AB})\} - b_F. \quad (15)$$

The above inequality shows that from the measurement incompatibility, the two error probabilities, and the discord and classical correlations, one can estimate a lower bound on the regularized entanglement of formation $E_f^\infty(\rho_{AB})$. As a simple example, it is clear that the bound is tight for a Schmidt rank d maximally entangled state for which $E_f^\infty = \log d$, $\max\{0, D_A(\rho_{AB}) - J_A(\rho_{AB})\} = 0$, and by choosing the measurements to be Fourier conjugate so that $-2\log_2 c(P,Q) = \log d$ and $b_F = 0$.

As a further application, we show that our EUR gives an upper bound on the regularized common randomness distillable by means of one-way classical communication from Charlie to Bob. In the study of general resource conversion problems, the notion of distilling common randomness from a given quantum state plays an important role. As shown in [26], the distillable common randomness is the regularized version of the classical correlation. For example, if Charlie and Bob share an arbitrarily large number of copies of ρ_{CB}, then the net amount of correlated classical bits that they can share is given by $C_D^{\rightarrow}(\rho_{CB}) = \lim_{k\to\infty} \frac{1}{k} J((\rho_{CB})^{\otimes k})$. Using the Koashi-Winter [27] equality $C_D^{\rightarrow}(\rho_{CB}) + E_f^\infty(\rho_{AB}) = S(\rho_B)$ for

some state ρ_{AB} such that ρ_{ABC} purifies both ρ_{AB} and ρ_{CB}, we can substitute into (15) in order to obtain the following upper bound on the distillable common randomness of ρ_{CB}:

$$C_D^{\rightarrow}(\rho_{CB}) \leq S(\rho_B) + 2\log_2 c(P,Q) - \max\{0, D_A(\rho_{AB}) - J_A(\rho_{AB})\} + b_F. \quad (16)$$

This is an interesting application of our inequality and the Koashi-Winter relation, giving us an upper bound on the distillable common randomness across another partition from the local entropy on B, the measurement incompatibility, the discord and classical correlation on AB, and the error probabilities on A and B.

In conclusion, we have proved a new uncertainty relation for conditional entropic measures which depends on the incompatibility of two quantum measurements, the conditional entropy, the quantum discord, and the classical correlations of a state shared between the observed system and a quantum memory. This new uncertainty relation tightens that of Berta *et al.* whenever the quantum discord of the bipartite state is larger than its classical correlation. This occurs for several natural examples of bipartite states including all Werner and isotropic states, and it would be interesting to characterize the full class of states for which this tightening occurs. Furthermore, using our new inequality we have given a non-trivial lower bound on the regularized entanglement of formation for a state shared between Alice and Bob. We have also shown that our inequality can give an upper bound on the distillable common randomness of quantum state that Bob shares with a third party. Our results should have several applications in quantum information theory, quantum communication, quantum cryptography and precision measurements.

We thank the anonymous referee for helpful comments on our paper and Kavan Modi for useful discussions.

Appendix A: Werner States

In this appendix, we prove that our lower bound in (8) of the main text is perfectly tight for the class of higher-dimensional Werner states and Fourier-conjugate measurements. A higher-dimensional Werner state has the form:

$$\sigma_{AB} = \frac{2(1-\lambda)}{d(d+1)}\Pi^+ + \frac{2\lambda}{d(d-1)}\Pi^-,$$

where Π^+ is the projector onto the symmetric subspace and Π^- is the projector onto the antisymmetric subspace.

Theorem 2 *For Werner states, the uncertainty sum $S(P|B) + S(Q|B)$ and our lower bound $-2\log c(P,Q) + S(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB})$ in (8) of the main text coincide, and they are equal to*

$$-\frac{4(1-\lambda)}{d+1}\log\left(\frac{2(1-\lambda)}{d+1}\right) - \frac{2(d-1+2\lambda)}{d+1}\log\left(\frac{d-1+2\lambda}{d^2-1}\right).$$

For these states, the lower bound $-2\log c(P,Q) + S(A|B)$ of Berta et al. is equal to

$$-\lambda\log\frac{2\lambda}{d(d-1)} - (1-\lambda)\log\left(\frac{2(1-\lambda)}{d(d+1)}\right).$$

Proof For these states, the entropies $S(A)$, $S(B)$, and $S(A|B)$ are as follows:

$$\begin{aligned} S(A) = S(B) &= \log d, \\ S(A|B) &= -\lambda\log\frac{2\lambda}{d(d-1)} \\ &\quad - (1-\lambda)\log\left(\frac{2(1-\lambda)}{d(d+1)}\right) - \log d. \end{aligned}$$

Chitambar proved that the classical correlation $J_A(\sigma_{AB})$ is equal to [28]

$$\begin{aligned} &J_A(\sigma_{AB}) \\ &= I(A;B) - D_A(\sigma_{AB}) \\ &= \log 2d + \lambda\log\frac{\lambda}{d-1} + (1-\lambda)\log\left(\frac{1-\lambda}{d+1}\right) \\ &\quad - \left[\log(d+1) + \lambda\log\frac{\lambda}{d-1} + (1-\lambda)\log\left(\frac{1-\lambda}{d+1}\right)\right] \\ &\quad + \frac{2(1-\lambda)}{d+1}\log(1-\lambda) + \frac{d-1+2\lambda}{d+1}\log\left(\frac{d-1+2\lambda}{2(d-1)}\right) \\ &= \log\left(\frac{2d}{d+1}\right) + \frac{2(1-\lambda)}{d+1}\log(1-\lambda) \\ &\quad + \frac{d-1+2\lambda}{d+1}\log\left(\frac{d-1+2\lambda}{2(d-1)}\right) \end{aligned}$$

Suppose that the POVMs P and Q correspond to Fourier-conjugate observables so that $P = \{|z\rangle\langle z|\}$ and $Q = \{|\tilde{x}\rangle\langle\tilde{x}|\}$. (In what follows, we just call them $Z = P$ and $X = Q$.) For computing $S(Z|B)$ we need to consider the following state:

$$\sigma_{ZB} \equiv \sum_z (|z\rangle\langle z| \otimes I)\sigma_{AB}(|z\rangle\langle z| \otimes I). \quad (A1)$$

Using the facts that $\Pi^+ = (I+F)/2$ and $\Pi^- = (I-F)/2$ and that

$$\sum_z (|z\rangle\langle z| \otimes I)\ F\ (|z\rangle\langle z| \otimes I) = \sum_z |z\rangle\langle z| \otimes |z\rangle\langle z|,$$

it follows that (A1) is equal to

$$\begin{aligned}
&\frac{(1-\lambda)}{d(d+1)}\left(I+\sum_z |z\rangle\langle z|\otimes|z\rangle\langle z|\right)\\
&\quad+\frac{\lambda}{d(d-1)}\left(I-\sum_z |z\rangle\langle z|\otimes|z\rangle\langle z|\right)\\
&=\left(\frac{(1-\lambda)}{d(d+1)}+\frac{\lambda}{d(d-1)}\right)I\\
&\quad+\left(\frac{(1-\lambda)}{d(d+1)}-\frac{\lambda}{d(d-1)}\right)\sum_z |z\rangle\langle z|\otimes|z\rangle\langle z|\\
&=\frac{d(d-1+2\lambda)}{d^2-1}\frac{I}{d^2}\\
&\quad+\frac{d-1-2\lambda d}{d^2-1}\sum_z \frac{1}{d}|z\rangle\langle z|\otimes|z\rangle\langle z|\\
&=\sum_z \frac{1}{d}|z\rangle\langle z|\otimes\left(\frac{d(d-1+2\lambda)}{d^2-1}\frac{I}{d}+\frac{d-1-2\lambda d}{d^2-1}|z\rangle\langle z|\right)
\end{aligned} \tag{A2}$$

From the above form, we deduce that $H(Z)=\log d$, implying that

$$\begin{aligned}
S(Z|B)&=S(B|Z)+H(Z)-S(B)\\
&=S(B|Z).
\end{aligned}$$

Consider that each conditional state in (A2) can be expressed as

$$\begin{aligned}
&\frac{d(d-1+2\lambda)}{d^2-1}\frac{I}{d}+\frac{d-1-2\lambda d}{d^2-1}|z\rangle\langle z|\\
&=\frac{d-1+2\lambda}{d^2-1}[(I-|z\rangle\langle z|)+|z\rangle\langle z|]+\frac{d-1-2\lambda d}{d^2-1}|z\rangle\langle z|\\
&=\frac{d-1+2\lambda}{d^2-1}(I-|z\rangle\langle z|)+\frac{2(1-\lambda)(d-1)}{d^2-1}|z\rangle\langle z|.
\end{aligned}$$

For the above state, each probability is independent of the particular value of Z, implying that the entropy $S(B|Z)$ is just the von Neumann entropy of the following state:

$$\frac{d-1+2\lambda}{d^2-1}(I-|z\rangle\langle z|)+\frac{2(1-\lambda)(d-1)}{d^2-1}|z\rangle\langle z|.$$

Thus, we have that

$$\begin{aligned}
S(Z|B)&=S(B|Z)\\
&=-(d-1)\frac{d-1+2\lambda}{d^2-1}\log\frac{d-1+2\lambda}{d^2-1}\\
&\quad-\frac{2(1-\lambda)(d-1)}{d^2-1}\log\frac{2(1-\lambda)(d-1)}{d^2-1}\\
&=-\frac{d-1+2\lambda}{d+1}\log\frac{d-1+2\lambda}{d^2-1}\\
&\quad-\frac{2(1-\lambda)}{d+1}\log\frac{2(1-\lambda)}{d+1}.
\end{aligned}$$

By a similar line of reasoning, it follows from the high symmetry of the Werner state that

$$\begin{aligned}
S(X|B)=&-\frac{d-1+2\lambda}{d+1}\log\frac{d-1+2\lambda}{d^2-1}\\
&-\frac{2(1-\lambda)}{d+1}\log\frac{2(1-\lambda)}{d+1}
\end{aligned}$$

Putting everything together, the sum of the uncertainties is equal to

$$\begin{aligned}
S(Z|B)+S(X|B)=&-\frac{2(d-1+2\lambda)}{d+1}\log\frac{d-1+2\lambda}{d^2-1}\\
&-\frac{4(1-\lambda)}{d+1}\log\frac{2(1-\lambda)}{d+1}
\end{aligned} \tag{A3}$$

The lower bound of Berta *et al.* is as follows:

$$\begin{aligned}
-2\log c+S(A|B)=&-\lambda\log\frac{2\lambda}{d(d-1)}\\
&-(1-\lambda)\log\left(\frac{2(1-\lambda)}{d(d+1)}\right),
\end{aligned}$$

while our new lower bound is equal to

$$\begin{aligned}
&-2\log c+S(A)-2J_A(\rho_{AB})\\
&=2\log d-2\log\left(\frac{2d}{d+1}\right)-\frac{4(1-\lambda)}{d+1}\log(1-\lambda)\\
&\quad-\frac{2(d-1+2\lambda)}{d+1}\log\left(\frac{d-1+2\lambda}{2(d-1)}\right)\\
&=2\log\left(\frac{d+1}{2}\right)-\frac{4(1-\lambda)}{d+1}\log(1-\lambda)\\
&\quad-\frac{2(d-1+2\lambda)}{d+1}\log\left(\frac{d-1+2\lambda}{2(d-1)}\right)
\end{aligned}$$

Since $2=\frac{4(1-\lambda)}{d+1}+\frac{2(d-1+2\lambda)}{d+1}$, we then have that the above is equal to

$$\begin{aligned}
&=\frac{4(1-\lambda)}{d+1}\log\left(\frac{d+1}{2}\right)+\frac{2(d-1+2\lambda)}{d+1}\log\left(\frac{d+1}{2}\right)\\
&\quad-\frac{4(1-\lambda)}{d+1}\log(1-\lambda)\\
&\quad-\frac{2(d-1+2\lambda)}{d+1}\log\left(\frac{d-1+2\lambda}{2(d-1)}\right)\\
&=-\frac{4(1-\lambda)}{d+1}\log\left(\frac{2(1-\lambda)}{d+1}\right)\\
&\quad-\frac{2(d-1+2\lambda)}{d+1}\log\left(\frac{d-1+2\lambda}{d^2-1}\right).
\end{aligned}$$

This last equality demonstrates that our new lower bound coincides exactly with the uncertainty sum in (A3) for all dimensions d and for all values of λ. □

Figure 2 plots the difference between our new bound and that of Berta *et al.* for Werner states as a function of the dimension d and the parameter λ.

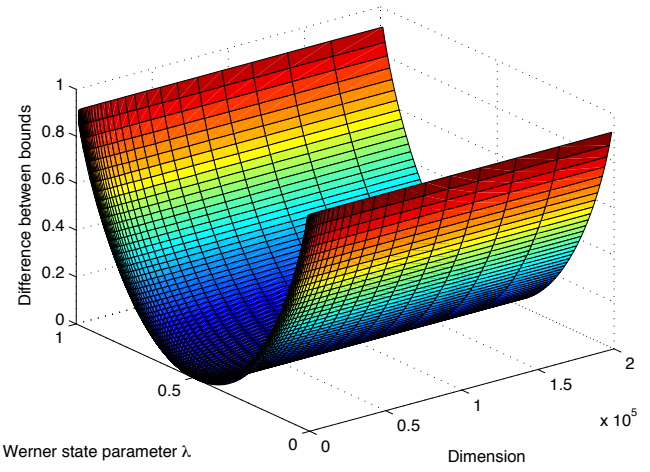

FIG. 2: The difference between our new bound in (8) of the main text and that of Berta *et al.* for Werner states as a function of the dimension d and the parameter λ.

Appendix B: Isotropic States

In this appendix, we prove that our lower bound in (8) of the main text is perfectly tight for the class of higher-dimensional isotropic states and Fourier-conjugate measurements. Isotropic states are defined as

$$\omega_{AB} = \lambda \Phi_d + \frac{1-\lambda}{d^2-1}(I - \Phi_d).$$

Theorem 3 *For isotropic states, the uncertainty sum $S(P|B) + S(Q|B)$ and our lower bound $-2\log c(P,Q) + S(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB})$ in (8) of the main text coincide, and they are equal to*

$$-\frac{2(d\lambda+1)}{d+1}\log\frac{d\lambda+1}{d+1} - \frac{2d(1-\lambda)}{d+1}\log\frac{d(1-\lambda)}{d^2-1}$$

For these states, the lower bound $-2\log c(P,Q) + S(A|B)$ of Berta et al. is equal to

$$-\lambda\log\lambda - (1-\lambda)\log_2\left(\frac{1-\lambda}{d^2-1}\right).$$

Proof For these states,

$$S(A) = S(B) = \log d,$$
$$S(A|B) = -\lambda\log\lambda - (1-\lambda)\log_2\left(\frac{1-\lambda}{d^2-1}\right) - \log d$$

and Chitambar proved that [28]

$$\begin{aligned}
&J_A(\omega_{AB}) \\
&= I(A;B) - D_A(\omega_{AB}) \\
&= 2\log d + \lambda\log\lambda + (1-\lambda)\log_2\left(\frac{1-\lambda}{d^2-1}\right) \\
&\quad - \lambda\log\lambda - \left(\frac{1-\lambda}{d+1}\right)\log\left(\frac{1-\lambda}{d^2-1}\right) \\
&\quad + \frac{d\lambda+1}{d+1}\log\left(\frac{d\lambda+1}{d(d+1)}\right) \\
&= 2\log d + \frac{d(1-\lambda)}{d+1}\log\left(\frac{1-\lambda}{d^2-1}\right) \\
&\quad + \frac{d\lambda+1}{d+1}\log\left(\frac{d\lambda+1}{d(d+1)}\right)
\end{aligned}$$

For computing $S(Z|B)$ we need to consider the following state:

$$\omega_{ZB} \equiv \sum_z (|z\rangle\langle z| \otimes I)\omega_{AB}(|z\rangle\langle z| \otimes I). \tag{B1}$$

Observing that

$$\sum_z (|z\rangle\langle z| \otimes I)\ \Phi_d\ (|z\rangle\langle z| \otimes I) = \sum_z \frac{1}{d}|z\rangle\langle z| \otimes |z\rangle\langle z|,$$

we have that

$$\begin{aligned}
\omega_{ZB} &= \lambda\sum_z \frac{1}{d}|z\rangle\langle z| \otimes |z\rangle\langle z| \\
&\quad + \frac{1-\lambda}{d^2-1}\left(I - \sum_z \frac{1}{d}|z\rangle\langle z| \otimes |z\rangle\langle z|\right) \\
&= \sum_z \frac{1}{d}|z\rangle\langle z| \otimes \left(\lambda - \frac{1-\lambda}{d^2-1}\right)|z\rangle\langle z| \\
&\quad + \frac{d^2(1-\lambda)}{d^2-1}\frac{I}{d^2} \\
&= \sum_z \frac{1}{d}|z\rangle\langle z| \otimes \left[\frac{d^2\lambda-1}{d^2-1}|z\rangle\langle z| + \frac{d(1-\lambda)}{d^2-1}I\right]
\end{aligned}$$

We now focus on rewriting the conditional state above as

$$\begin{aligned}
&\frac{d^2\lambda-1}{d^2-1}|z\rangle\langle z| + \frac{d(1-\lambda)}{d^2-1}I \\
&= \frac{d^2\lambda-1}{d^2-1}|z\rangle\langle z| + \frac{d(1-\lambda)}{d^2-1}[(I - |z\rangle\langle z|) + |z\rangle\langle z|] \\
&= \frac{d\lambda+1}{d+1}|z\rangle\langle z| + \frac{d(1-\lambda)}{d^2-1}(I - |z\rangle\langle z|).
\end{aligned}$$

It follows for the state ω_{ZB} that $H(Z) = \log d$, implying that

$$\begin{aligned}
S(Z|B) &= S(B|Z) + H(Z) - S(B) \\
&= S(B|Z)
\end{aligned}$$

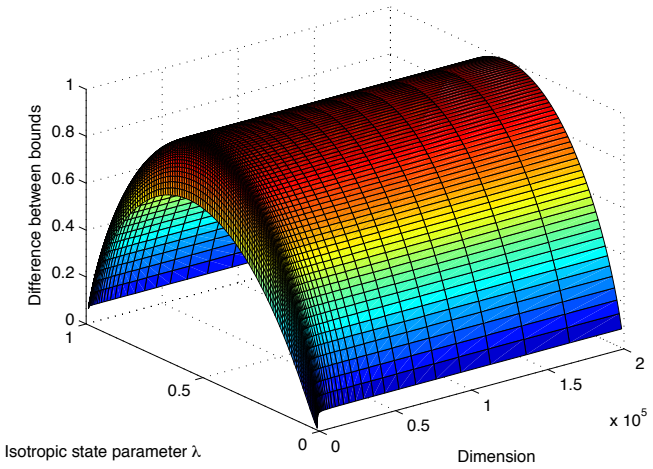

FIG. 3: The difference between our new bound in (8) of the main text and that of Berta *et al.* for isotropic states as a function of the dimension d and the parameter λ.

Observing that the eigenvalues of the above conditional states do not depend on z in any way, the entropy $S(B|Z)$ is the von Neumann entropy of the following state:

$$\frac{d\lambda+1}{d+1}|z\rangle\langle z| + \frac{d(1-\lambda)}{d^2-1}(I - |z\rangle\langle z|).$$

Calculating directly, we obtain

$$\begin{aligned} S(Z|B) &= S(B|Z) \\ &= -\frac{d\lambda+1}{d+1}\log\frac{d\lambda+1}{d+1} \\ &\quad -(d-1)\frac{d(1-\lambda)}{d^2-1}\log\frac{d(1-\lambda)}{d^2-1} \\ &= -\frac{d\lambda+1}{d+1}\log\frac{d\lambda+1}{d+1} \\ &\quad -\frac{d(1-\lambda)}{d+1}\log\frac{d(1-\lambda)}{d^2-1}. \end{aligned}$$

By following the same procedure, we can calculate that $S(X|B)$ is as follows:

$$\begin{aligned} S(X|B) = &-\frac{d\lambda+1}{d+1}\log\frac{d\lambda+1}{d+1} \\ &-\frac{d(1-\lambda)}{d+1}\log\frac{d(1-\lambda)}{d^2-1}, \end{aligned}$$

so that the uncertainty sum is

$$\begin{aligned} S(Z|B) + S(X|B) = &-\frac{2(d\lambda+1)}{d+1}\log\frac{d\lambda+1}{d+1} \\ &-\frac{2d(1-\lambda)}{d+1}\log\frac{d(1-\lambda)}{d^2-1} \end{aligned} \quad \text{(B2)}$$

The Berta *et al.* lower bound is then

$$\begin{aligned} -2\log c + S(A|B) = &-\lambda\log\lambda \\ &-(1-\lambda)\log_2\left(\frac{1-\lambda}{d^2-1}\right), \end{aligned}$$

while our new lower bound is

$$\begin{aligned} &-2\log c + S(A) - 2J_A(\rho_{AB}) = -2\log d \\ &-\frac{2d(1-\lambda)}{d+1}\log\left(\frac{1-\lambda}{d^2-1}\right) - \frac{2(d\lambda+1)}{d+1}\log\left(\frac{d\lambda+1}{d(d+1)}\right) \end{aligned}$$

Since $2 = \frac{2d(1-\lambda)}{d+1} + \frac{2(d\lambda+1)}{d+1}$, we can rewrite the above as

$$\begin{aligned} &-\frac{2d(1-\lambda)}{d+1}\log d - \frac{2(d\lambda+1)}{d+1}\log d \\ &\quad -\frac{2d(1-\lambda)}{d+1}\log\left(\frac{1-\lambda}{d^2-1}\right) \\ &\quad -\frac{2(d\lambda+1)}{d+1}\log\left(\frac{d\lambda+1}{d(d+1)}\right) \\ &= -\frac{2(d\lambda+1)}{d+1}\log\frac{d\lambda+1}{d+1} - \frac{2d(1-\lambda)}{d+1}\log\frac{d(1-\lambda)}{d^2-1} \end{aligned}$$

This last equality demonstrates that our new lower bound coincides exactly with the uncertainty sum in (B2) for all dimensions d and for all values of λ. □

Figure 3 plots the difference between our new bound and that of Berta *et al.* for isotropic states as a function of the dimension d and the parameter λ.

[1] W. Heisenberg, Zeitschrift für Physik **43**, 172 (1927).
[2] H. Maassen and J. B. M. Uffink, Physical Review Letters **60**, 1103 (1988).
[3] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010).
[4] J. M. Renes and J.-C. Boileau, Physical Review A **78**, 032335 (2008).
[5] M. M. Wilde and J. M. Renes (2012), arXiv:1201.2906.
[6] M. M. Wilde and J. M. Renes (2012), arXiv:1203.5794.
[7] K. Popper and v. Weizsäcker, Naturwissenschaften **22**, 807 (1934).
[8] H. P. Robertson, Physical Review **34**, 163 (1929).

[9] E. Schrödinger, Proceedings of The Prussian Academy of Sciences—Physics-Mathematical Section **XIX**, 296 (1930).

[10] D. Deutsch, Physical Review Letters **50**, 631 (1983).

[11] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010).

[12] I. I. Hirschman, American Journal of Mathematics **79**, 152 (1957).

[13] W. Beckner, Annals of Mathematics **102**, 159 (1975).

[14] I. Bialynicki-Birula and J. Mycielski, Communications in Mathematical Physics **44**, 129 (1975).

[15] M. H. Partovi, Physical Review Letters **50**, 1883 (1983).

[16] I. Bialynicki-Birula, Physics Letters A **103A**, 253 (1984).

[17] K. Kraus, Physical Review D **35**, 3070 (1987).

[18] M. Krishna and K. R. Parthasarathy, Sankhya: The Indian Journal of Statistics, Series A **64**, 842 (2002).

[19] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Physical Review A **83**, 062338 (2011).

[20] P. J. Coles, L. Yu, and M. Zwolak (2011), arXiv:1105.4865.

[21] L. Chuan-Feng, J.-S. Xu, X.-Y. Xu, K. Li, and G.-C. Guo, Nature Physics **7**, 752 (2011).

[22] R. Prevedel, D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch, Nature Physics **7**, 757 (2011).

[23] H. Ollivier and W. H. Zurek, Physical Review Letters **88**, 017901 (2001).

[24] L. Henderson and V. Vedral, Journal of Physics A: Mathematical and General **34**, 6899 (2001).

[25] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral (2011), arXiv:1112.6238.

[26] I. Devetak and A. Winter, IEEE Transactions on Information Theory **50**, 3183 (2004).

[27] M. Koashi and A. Winter, Physical Review A **69**, 022309 (2004).

[28] E. Chitambar (2011), arXiv:1110.3057.

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

[30] E. A. Carlen and E. H. Lieb (2012), arXiv:1203.4719.