Entropic uncertainty and measurement reversibility

This content has been downloaded from IOPscience. Please scroll down to see the full text.
2016 New J. Phys. 18 073004
(http://iopscience.iop.org/1367-2630/18/7/073004)

View the table of contents for this issue, or go to the journal homepage for more

Download details:

IP Address: 131.180.33.71
This content was downloaded on 16/03/2017 at 13:43

Please note that terms and conditions apply.

You may also be interested in:

Discrete Quantum Mechanics: Entanglement
H T Williams

Measures and applications of quantum correlations
Gerardo Adesso, Thomas R Bromley and Marco Cianciaruso

Optimal quantum networks and one-shot entropies
Giulio Chiribella and Daniel Ebler

Quantum preparation uncertainty and lack of information
Filip Rozpdek, Jdrzej Kaniewski, Patrick J Coles et al.

Device-independent two-party cryptography secure against sequential attacks
Jdrzej Kaniewski and Stephanie Wehner

The symmetric extendibility of quantum states
Marcin L Nowakowski

Measurement-device-independent quantification of entanglement for given Hilbert space dimension
Koon Tong Goh, Jean-Daniel Bancal and Valerio Scarani

Self-testing through EPR-steering
Ivan Šupi and Matty J Hoban

Semi device independence of the BB84 protocol
Erik Woodhead
Entropic uncertainty and measurement reversibility

Mario Berta¹, Stephanie Wehner² and Mark M Wilde³,⁴

¹ Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA 91125, USA
² QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands
³ Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Baton Rouge, LA 70803, USA
⁴ Author to whom any correspondence should be addressed.

E-mail: mwilde@lsu.edu

Keywords: uncertainty principle, quantum relative entropy, measurement reversibility

Abstract

The entropic uncertainty relation with quantum side information (EUR-QSI) from (Berta et al 2010 Nat. Phys. 6 659) is a unifying principle relating two distinctive features of quantum mechanics: quantum uncertainty due to measurement incompatibility, and entanglement. In these relations, quantum uncertainty takes the form of preparation uncertainty where one of two incompatible measurements is applied. In particular, the ‘uncertainty witness’ lower bound in the EUR-QSI is not a function of a post-measurement state. An insightful proof of the EUR-QSI from (Coles et al 2012 Phys. Rev. Lett. 108 210405) makes use of a fundamental mathematical consequence of the postulates of quantum mechanics known as the non-increase of quantum relative entropy under quantum channels. Here, we exploit this perspective to establish a tightening of the EUR-QSI which adds a new state-dependent term in the lower bound, related to how well one can reverse the action of a quantum measurement. As such, this new term is a direct function of the post-measurement state and can be thought of as quantifying how much disturbance a given measurement causes. Our result thus quantitatively unifies this feature of quantum mechanics with the others mentioned above. We have experimentally tested our theoretical predictions on the IBM quantum experience and find reasonable agreement between our predictions and experimental outcomes.

1. Introduction

The uncertainty principle is one of the cornerstones of modern physics, providing a striking separation between classical and quantum mechanics [1]. It is routinely used to reason about the behavior of quantum systems, and in recent years, an information-theoretic refinement of it that incorporates quantum side information has been helpful for witnessing entanglement and in establishing the security of quantum key distribution [2]. This latter refinement, known as the entropic uncertainty relation with quantum side information (EUR-QSI), is the culmination of a sequence of works spanning many decades [3–12] and is the one on which we focus here (see [13] for a survey).

Tripartite uncertainty relations. There are two variations of the EUR-QSI [2], one for tripartite and one for bipartite scenarios. Tripartite uncertainty relations capture an additional feature of quantum mechanics, namely the monogamy of entanglement [14]. Consider three systems, which we will refer to as Alice (A), Bob (B) and Eve (E). The monogamy of entanglement states that if A is very entangled with B, then A necessarily has very little entanglement with E. This physical effect is not only key to the security of quantum key distribution, but has far reaching consequences up to the recent firewall debate concerning the physics of black holes [15]. Tripartite uncertainty relations are one way to quantify the monogamy of entanglement by considering correlations amongst Alice, Bob and Eve. Let \( \rho_{ABE} \) denote a tripartite quantum state shared between Alice, Bob, and Eve, and let \( \mathcal{X} \equiv \{ P^x_A \} \) and \( \mathcal{Z} \equiv \{ Q^z_b \} \) be projection-valued measures (PVMs) that can be performed on Alice’s system (note that considering PVMs implies statements for the more general positive operator-valued measures, by invoking the Naimark extension theorem [16]). If Alice chooses to measure \( \mathcal{X} \), then the post-measurement state
is as follows:

\[ \sigma_{\text{XBE}} \equiv \sum_{x} |x⟩⟨x| Y \otimes \sigma_{\text{BE}}, \quad \text{where} \]
\[ \sigma_{\text{BE}} \equiv \text{Tr}_{\text{A}} \{ (P_{\text{A}} \otimes I_{\text{BE}}) \rho_{\text{ABE}} \}. \]

Similarly, if Alice instead chooses to measure \( Z \), then the post-measurement state is

\[ \omega_{\text{ZBE}} \equiv \sum_{z} |z⟩⟨z| Y \otimes \omega_{\text{BE}}, \quad \text{where} \]
\[ \omega_{\text{BE}} \equiv \text{Tr}_{\text{A}} \{ (Q_{\text{A}} \otimes I_{\text{BE}}) \rho_{\text{ABE}} \}. \]

In the above, \(|x⟩⟩_{\text{X}}\) and \(|z⟩⟩_{\text{Z}}\) are orthonormal bases that encode the classical outcome of the respective measurements. The following tripartite EUR-QSI in (3) quantifies the trade-off between Bob’s ability to predict the outcome of the \( X \) measurement with the help of his quantum system \( B \) and Eve’s ability to predict the outcome of the \( Z \) measurement with the help of her system \( E \):

\[ H (X|B)_{\omega} + H (Z|E)_{\omega} \geq - \log \epsilon, \]

where here and throughout we take the logarithm to have base two. In the above

\[ H (F|G)_{\tau} \equiv H (FG)_{\tau} - H (G)_{\tau} = H (t_{FG}) - H (t_{G}), \]

denotes the conditional von Neumann entropy of a state \( t_{FG} \), with \( H (\tau) \equiv - \text{Tr} \{ \tau \log \tau \} \), and the parameter \( \epsilon \) captures the incompatibility of the \( X \) and \( Z \) measurements:

\[ \epsilon \equiv \max_{x,z} \| P_{\text{A}} Q_{\text{A}} \|_{\infty} \in [0, 1]. \]

The conditional entropy \( H (F|G) \) is a measure of the uncertainty about system \( F \) from the perspective of someone who possesses system \( G \), given that the state of both systems is \( t_{FG} \). The uncertainty relation in (3) thus says that if Bob can easily predict \( X \) given \( B \) (i.e., \( H (X|B) \) is small) and the measurements are incompatible, then it is difficult for Eve to predict \( Z \) given \( E \) (i.e., \( H (Z|E) \) is large). As such, (5) at the same time quantifies measurement incompatibility and the monogamy of entanglement [17]. A variant of (3) in terms of the conditional min-entropy [18] can be used to establish the security of quantum key distribution under particular assumptions [19, 20].

The EUR-QSI in (3) can be summarized informally as a game involving a few steps. To begin with, Alice, Bob, and Eve are given a state \( \rho_{\text{ABE}} \). Alice then flips a coin to decide whether to measure \( X \) or \( Z \). If she gets heads, she measures \( X \) and tells Bob that she did so. Bob then has to predict the outcome of her \( X \) measurement and can use his quantum system \( B \) to help so do. If Alice gets tails, she instead measures \( Z \) and tells Eve that she did so. In this case, Eve has to predict the outcome of Alice’s \( Z \) measurement and can use her quantum system \( E \) as an aid. There is a trade-off between their ability to predict correctly, which is captured by (3).

**Bipartite uncertainty relations.** We now recall the second variant of the EUR-QSI from [2]. Such bipartite relations can be used to quantify and witness aspects of entanglement shared between only two parties, Alice and Bob. Here we have a bipartite state \( \rho_{\text{AB}} \) shared between Alice and Bob and again the measurements \( X \) and \( Z \) mentioned above. Alice chooses to measure either \( X \) or \( Z \), leading to the respective post-measurement states \( \sigma_{\text{XB}} \) and \( \omega_{\text{ZB}} \) defined from (1) and (2) after taking a partial trace over the \( E \) system. The following EUR-QSI in (6) quantifies the trade-off between Bob’s ability to predict the outcome of the \( X \) or \( Z \) measurement:

\[ H (Z|B)_{\omega} + H (X|B)_{\omega} \geq - \log \epsilon + H (A|B), \]

where the incompatibility parameter \( \epsilon \) is defined in (5) and the conditional entropy \( H (A|B) \) is a signature of both the mixedness and entanglement of the state \( \rho_{\text{AB}} \). For (6) to hold, we require the technical condition that the \( Z \) measurement be a rank-one measurement [21] (however see also [22, 23] for a lifting of this condition). The EUR-QSI in (6) finds application in witnessing entanglement, as discussed in [2].

The uncertainty relation in (6) can also be summarized informally as a game, similar to the one discussed above. Here, we have Alice choose whether to measure \( X \) or \( Z \). If she measures \( X \), she informs Bob that she did so, and it is his task to predict the outcome of the \( X \) measurement. If she instead measures \( Z \), she tells Bob, and he should predict the outcome of the \( Z \) measurement. In both cases, Bob is allowed to use his quantum system \( B \) to help in predicting the outcome of Alice’s measurement. Again there is generally a trade-off between how well Bob can predict the outcome of the \( X \) or \( Z \) measurement, which is quantified by (6). The better that Bob can predict the outcome of either measurement, the more entangled the state \( \rho_{\text{AB}} \) is.

**2. Main result**

The main contribution of the present paper is to refine and tighten both of the uncertainty relations in (3) and (6) by employing a recent result from [24] (see also [25–27]). This refinement adds a term involving measurement
reversibility, next to the original trade-offs in terms of measurement incompatibility and entanglement. An insightful proof of the EUR-QSIs above makes use of an entropy inequality known as the non-increase of quantum relative entropy [28, 29]. This entropy inequality is fundamental in quantum physics, providing limitations on communication protocols [30] and thermodynamic processes [31]. The main result of [24–27] offers a strengthening of the non-increase of quantum relative entropy, quantifying how well one can recover from the deleterious effects of a noisy quantum channel. Here we apply the particular result from [24] to establish a tightening of both uncertainty relations in (3) and (6) with a term related to how well one can ‘reverse’ an additional $\mathcal{X}$ measurement performed on Alice’s system at the end of the uncertainty game, if the outcome of the $\mathcal{X}$ measurement and the $B$ system are available. The upshot is an entropic uncertainty relation which incorporates measurement reversibility in addition to quantum uncertainty due to measurement incompatibility, and entanglement, thus unifying several genuinely quantum features into a single uncertainty relation.

In particular, we establish the following refinements of (3) and (6):

$$H(Z|E_\omega) + H(X|B_\omega) \geq -\log c - \log f,$$

(7)

$$H(Z|B_\omega) + H(X|B_\omega) \geq -\log c - \log f + H(A|B)_{\omega},$$

(8)

where $c$ is defined in (5),

$$f \equiv F(\rho_{AB}, \mathcal{R}_{XB\to AB}(\sigma_{XB})),,$$

(9)

and in (8) we need the projective $Z$ measurement to be a rank-one measurement (i.e., $Q_\omega^z = |z\rangle \langle z|$). In addition to the measurement incompatibility $c$, the term $f$ quantifies the disturbance caused by one of the measurements, in particular, how reversible such a measurement is. $F(\rho_1, \rho_2) \equiv \|\sqrt{\rho_1} \sqrt{\rho_2}\|$ denotes the quantum fidelity between two density operators $\rho_1$ and $\rho_2$ [32], and $\mathcal{R}_{XB\to AB}$ is a recovery quantum channel with input systems $XB$ and output systems $AB$. Appendix A details a proof for (7) and (8). In section 4, we discuss several simple exemplary states and measurements to which (8) applies, and in section 5, we detail the results of several experimental tests of the theoretical predictions, finding reasonable agreement between the experimental results and our predictions.

In the case that the $Z$ measurement has the form $Q_\omega^z = |z\rangle \langle z|$ for an orthonormal basis $\{|z\rangle_A\}$, the action of the recovery quantum channel $\mathcal{R}_{XB\to AB}$ on an arbitrary state $\xi_{XB}$ is explicitly given as follows (see appendix B for details):

$$\mathcal{R}_{XB\to AB}(\xi_{XB}) = \sum_{z,z'} \langle z| \rho_{A|z}\rangle (|z'|_A \otimes \mathcal{R}_{XB\to A}(\xi_{XB})),$$

(10)

where

$$\mathcal{R}_{XB\to A}(\xi_{XB}) = \int_{[-\infty,\infty]} dt \ p(t) (\omega_B^{+i\pi t}) (\theta_B^{+i\pi t}) \cdot \text{Tr}_X \ {\langle x| \langle x|_X (\xi_{XB}) \rangle} \ (\theta_B^{+i\pi t}) (\omega_B^{+i\pi t}),$$

(11)

with the probability density $p(t) \equiv \frac{1}{\pi} (\cosh(\pi t) + 1)^{-1}$. (Note that $\mathcal{R}_{XB\to AB}$ is not a channel—we are merely using this notation as a shorthand.) In the above, $\theta_X$ is the state resulting from Alice performing the $\mathcal{X}$ measurement, following with the $\mathcal{X}$ measurement, and then discarding the outcome of the $Z$ measurement:

$$\theta_X \equiv \sum_x \langle x| \otimes \theta_B^x,$$

with

$$\theta_B^x \equiv \sum_z \langle z| P_A^x_z |z\rangle \omega_B^x.$$

(12)

For this case, $\omega_B^x$ from (2) reduces to $\omega_B^x = (|z\rangle_A \otimes I_B) \rho_{AB} (|z\rangle_A \otimes I_B)$. As one can readily check by plugging into (10), the recovery channel $\mathcal{R}$ has the property that it perfectly reverses an $\mathcal{X}$ measurement if it is performed after a $Z$ measurement:

$$\mathcal{R}_{XB\to AB}(\theta_X) = \sum_z \langle z| \otimes \omega_B^z,$$

(13)

The fidelity $F(\rho_{AB}, \mathcal{R}_{XB\to AB}(\sigma_{XB}))$ thus quantifies how much disturbance the $\mathcal{X}$ measurement causes to the original state $\rho_{AB}$ in terms of how well the recovery channel $\mathcal{R}$ can reverse the process. We note that there is a trade-off between reversing the $\mathcal{X}$ measurement whenever it is greatly disturbing $\rho_{AB}$ and meeting the constraint in (13). Since the quantum fidelity always takes a value between zero and one, it is clear that (7) and (8) represent a state-dependent tightening of (3) and (6), respectively.

### 3. Interpretation

It is interesting to note that just as the original relation in (6) could be used to witness entanglement, the new relation can be used to witness both entanglement and recovery from measurement, as will be illustrated using...
First suppose that \( r_{AB} = |+\rangle \langle +| \otimes \pi_B \), where \( \pi \) is the maximally mixed state. In this case, Bob’s system \( B \) is of no use to help predict the outcome of a measurement on the \( A \) system because the systems are in a product state. Here we find by direct calculation that \( H(A|B)_B = 0, H(X|B)_B = 0, \) and \( H(Z|B)_B = 1 \). By (8), this then implies that there exists a recovery channel \( \mathcal{R}^{(8)} \) such that (13) is satisfied and, given that \( \sigma_{XB} = |0\rangle \langle 0|_X \otimes \pi_B \), we also have the perfect recovery.
To determine the recovery channel $R^{(1)}$, consider that
\[
\sum_z |z\rangle \langle z| \otimes \omega_B^z = \pi_Z \otimes \pi_B,
\]
\[
\sum_x |x\rangle \langle x| \otimes \theta_B^x = \pi_X \otimes \pi_B,
\]
with the states on the left in each case defined in (2) and (12), respectively. Plugging into (10), we find that the recovery channel in this case is given explicitly by
\[
R^{(1)}_{XB \rightarrow AB}(\pi_X \otimes \pi_B) = |+\rangle \langle +|_A \otimes \text{Tr}_X \{ |0\rangle \langle 0|_X \xi_{XB} \} + |-\rangle \langle -|_A \otimes \text{Tr}_X \{ |1\rangle \langle 1|_X \xi_{XB} \},
\]
so that we also see that
\[
R^{(1)}_{XB \rightarrow AB}(\pi_X \otimes \pi_B) = \pi_A \otimes \pi_B. \tag{21}
\]

4.1.2. Z eigenstate on system A
The situation in which $\rho_{AB} = |0\rangle \langle 0|_A \otimes \pi_B$ is similar in some regards, but the recovery channel is different—i.e., we have by direct calculation that $H(A|B)_a = 0$, $H(X|B)_a = 1$, and $H(Z|B)_a = 0$, which implies the existence of a different recovery channel $R^{(2)}$ such that (13) is satisfied, and given that $\sigma_{XB} = \pi_X \otimes \pi_B$, we also have the perfect recovery
\[
R^{(2)}_{XB \rightarrow AB}(\sigma_{XB}) = |0\rangle \langle 0|_A \otimes \text{Tr}_X \{ \xi_{XB} \}. \tag{22}
\]

4.1.3. Maximally entangled state on systems A and B
Now suppose that $\rho_{AB} = \{\Phi\} \langle \Phi|_{AB}$ is the maximally entangled state, where $\{\Phi\} \equiv (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$. In this case, we have that both $H(X|B)_a = 0$ and $H(Z|B)_a = 0$, but the conditional entropy is negative: $H(A|B)_a = -1$. So here again we find the existence of a recovery channel $R^{(3)}$ such that (13) is satisfied, and given that $\sigma_{XB} = (|0+\rangle \langle 0+|_X \otimes |1-\rangle \langle 1-|_X)/2$, we also have the perfect recovery
\[
R^{(3)}_{XB \rightarrow AB}((|0+\rangle \langle 0+|_X \otimes |1-\rangle \langle 1-|_X)/2) = \{\Phi\} \langle \Phi|_{AB}. \tag{25}
\]
To determine the recovery channel $R^{(3)}$, consider that
\[
\sum_z |z\rangle \langle z| \otimes \omega_B^z = \frac{1}{2} (|0\rangle \langle 0|_X \otimes |0\rangle \langle 0|_B + |1\rangle \langle 1|_X \otimes |1\rangle \langle 1|_B),
\]
\[
\sum_x |x\rangle \langle x| \otimes \theta_B^x = \pi_X \otimes \pi_B
\]
with the states on the left in each case defined in (2) and (12), respectively. Plugging into (10), we find that the recovery channel in this case is given explicitly by
\[
R^{(3)}_{XB \rightarrow AB}(\xi_{XB}) = \sum_{x,z',z} (-1)^{x+z'} |z\rangle \langle z'|_A \otimes |z\rangle \langle z'|_B \text{Tr}_X \{ |x\rangle \langle x|_X \otimes |z\rangle \langle z'|_B \xi_{XB} \}, \tag{28}
\]
i.e., with the following Kraus operators:
\[
\left\{ \sum_x (-1)^{x+z} (|z\rangle \langle z|_A \otimes |z\rangle \langle z|_B) \right\} \otimes \langle x|_X \otimes \langle z|_B \}. \tag{29}
\]

These Kraus operators give the recovery map $R^{(3)}_{XB \rightarrow AB}$ the interpretation of (1) measuring the $X$ register and (2) coherently copying the contents of the $B$ register along with an appropriate relative phase. It can be implemented by performing a controlled-NOT gate from $B$ to $A$, followed by a controlled-phase gate on $X$ and $B$ and a partial trace over system $X$.

**Remark 1.** All of the examples mentioned above involve a perfect recovery or a perfect reversal of the $X$ measurement. This is due to the fact that the bound in (6) is saturated for these examples. However, the refined inequality in (8) allows to generalize these situations to the approximate case, in which $\rho_{AB}$ is nearly indistinguishable from the states given above. It is then the case that the equalities in (18)–(25) become approximate equalities, with a precise characterization given by (8).
4.2. Maximum uncertainty states

We now investigate the extreme opposite situation, when the bound in (6) is far from being saturated but its refinement in (8) is saturated. Let $\rho_{AB} = |+\rangle \langle +|_A \otimes \tau_B$, where $|+\rangle$ is defined from the relation $\sigma_Y |+\rangle = |+\rangle$. In this case, we find that both $H(X|B)_A = 1$ and $H(Z|B)_A = 1$. Thus, we could say that $\rho_{AB}$ is a ‘maximum uncertainty state’ because the sum $H(X|B)_A + H(Z|B)_A$ is equal to two bits and cannot be any larger than this amount. We also find that $H(A|B)_B = 0$, implying that (6) is one bit away from being saturated. Now consider that $\sigma_{XB} = \theta_{XB} = \pi_X \otimes \pi_B$ and $\omega_{ZB} = \pi_Z \otimes \pi_B$, and thus one can explicitly calculate the recovery channel $R^{(4)}$ from (10) to take the form:

$$R^{(4)}_{XB \rightarrow AB}(\xi_{XB}) \equiv |+\rangle \langle +|_A \otimes \text{Tr}_X \{0\} \langle 0|_X \xi_{XB} + |-\rangle \langle -|_A \otimes \text{Tr}_X \{1\} \langle 1|_X \xi_{XB} \}.$$

Note that the recovery channel $R^{(4)}_{XB \rightarrow AB}$ is the same as $R^{(4)}_{AB \rightarrow XB}$ in (20).

This implies that

$$R^{(4)}_{XB \rightarrow AB}(\sigma_{XB}) = \pi_A \otimes \pi_B,$$

and in turn that

$$-\log F(\rho_{AB}, R^{(4)}_{XB \rightarrow AB}(\theta_{XB})) = 1.$$

Thus the inequality in (8) is saturated for this example. The key element is that there is one bit of uncertainty when measuring a $Y$ eigenstate with respect to either the $X$ or $Z$ basis. At the same time, the $Y$ eigenstate is pure, so that its entropy is zero. This leaves a bit of uncertainty available and for which we have now interpreted in terms of how well one can reverse the $X$ measurement, using the refined bound in (8). One could imagine generalizing the idea of this example to higher dimensions in order to find more maximum uncertainty examples of this sort.

5. Experiments

We have experimentally tested three of the examples from the previous section, namely, the $X$ eigenstate, the maximally entangled state, and the $Y$ eigenstate examples. We did so using the recently available IBM quantum experience (QE) [34]. Three experiments have already appeared on the arXiv, conducted remotely by theoretical groups testing out experiments which had never been performed previously [35–37]. The QE architecture consists of five fixed-frequency superconducting transmon qubits, laid out in a ‘star geometry’ (four ‘corner’ qubits and one in the center). It is possible to perform single-qubit gates $X, Y, Z, H, T, S$, and $S^\dagger$, a Pauli measurement $Z$, and Bloch sphere tomography on any single qubit. However, two-qubit operations are limited to controlled-NOT gates with any one of the corner qubits acting as the source and the center qubit as the target. Thus, one must ‘recompile’ quantum circuits in order to meet these constraints. More information about the architecture is available at the user guide at [34].

Our experiments realize and test three of the examples from the previous section and, in particular, are as follows:

1. Prepare system $A$ in the state $|+\rangle$. Measure Pauli $\sigma_X$ on qubit $A$ and place the outcome in register $X$. Perform the recovery channel given in (20), with output system $A'$. Finally, perform Bloch sphere tomography on system $A'$.

2. Prepare system $A$ in the state $|+\rangle$. Measure Pauli $\sigma_Y$ on qubit $A$ and place the outcome in register $Z$. Measure Pauli $\sigma_X$ on qubit $A$ and place the outcome in register $X$. Perform the recovery channel given in (20), with output system $A'$. Finally, perform Bloch sphere tomography on system $A'$.

3. Same as Experiment 1 but begin by preparing system $A$ in the state $|+\rangle_A$.

4. Same as Experiment 2 but begin by preparing system $A$ in the state $|+\rangle_A$.

5. Prepare systems $A$ and $B$ in the maximally entangled Bell state $|\Phi^+\rangle_{AB}$. Measure Pauli $\sigma_X$ on qubit $A$ and place the outcome in register $X$. Perform the recovery channel given in (28), with output systems $A'$ and $B$. Finally, perform measurements of $\sigma_X$ on system $A'$ and $\sigma_Y$ on system $B$, or $\sigma_Y$ on system $A'$ and $\sigma_X$ on system $B$, or $\sigma_Y$ on system $A'$ and $\sigma_Z$ on system $B$.

6. Prepare systems $A$ and $B$ in the maximally entangled Bell state $|\Phi^-\rangle_{AB}$. Measure Pauli $\sigma_Z$ on qubit $A$ and place the outcome in register $Z$. Measure Pauli $\sigma_X$ on qubit $A$ and place the outcome in register $X$. Perform the recovery channel given in (28), with output systems $A'$ and $B$. Finally, perform measurements of $\sigma_X$ on
system $A'$ and $\sigma_X$ on system $B$, or $\sigma_Y$ on system $A'$ and $\sigma_Y^x$ on system $B$, or $\sigma_Z$ on system $A'$ and $\sigma_Z$ on system $B$.

A quantum circuit that can realize Experiments 1–4 is given in figure 2(a), and a quantum circuit that can realize Experiments 5–6 is given in figure 2(b). These circuits make use of standard quantum computing gates, detailed in [38], and one can readily verify that they ideally have the correct behavior, consistent with that discussed for the examples in the previous section. As stated above, it is necessary to recompile these circuits into a form which meets the constraints of the QE architecture.

Figure 3 plots the results of Experiments 1–6. Each experiment consists of three measurements, with Experiments 1–4 having measurements of each of the Pauli operators, and Experiments 5–6 having three different measurements each as outlined above. Each of these is repeated 8192 times, for a total of $6 \times 3 \times 8192 = 147,456$ experiments. The standard error for each kind of experiment is thus $\sqrt{p(1 - p)/8192}$, where $p_i$ is the estimate of the probability of a given measurement outcome in a given experiment. The caption of figure 3 features discussions of and comparisons between the predictions of the previous section and the experimental outcomes. While it is clear that the QE chip is subject to significant noise, there is still reasonable agreement with the theoretical predictions of the previous section. One observation we make regarding figure 3(e) is that the frequencies for the outcomes of the $\sigma_Y$ and $\sigma_Z$ measurements are much closer to the theoretically predicted values than are the other measurement outcomes.

6. Conclusion

The EUR-QSI is a unifying principle relating quantum uncertainty due to measurement incompatibility and entanglement. Here we refine and tighten this inequality with a state-dependent term related to how well one can reverse the action of a measurement. The tightening of the inequality is most pronounced when the measurements and state are all chosen from mutually unbiased bases, i.e., in our ‘maximum uncertainty’ example with the measurements being $\sigma_X$ and $\sigma_Z$ and the initial state being a $\sigma_Y$ eigenstate. We have...
experimentally tested our theoretical predictions on the IBM QE and find reasonable agreement between our predictions and experimental outcomes.

We note that in terms of the conditional min-entropy, other refinements of \((6)\) are known [39] that look at the measurement channel and its own inverse channel, and it would be interesting to understand their relation. Going forward, it would furthermore be interesting to generalize the results established here to infinite-dimensional and multiple measurement scenarios.

Acknowledgments

The authors acknowledge discussions with Siddhartha Das, Michael Walter, and Andreas Winter. We are grateful to the team at IBM and the IBM Quantum Experience project. This work does not reflect the views or opinions of IBM or any of its employees. MB acknowledges funding provided by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028). Additional funding support was provided by the ARO grant for Research on Quantum algorithms at the IQIM (W911NF-12-1-0521). SW acknowledges support from STW, Netherlands and an NWO VIDI Grant. MMW is grateful to SW and her group for hospitality during a research visit to QuTech in May 2015 and acknowledges support from startup funds from the Department of Physics and Astronomy at LSU, the NSF under Award No. CCF-1350397, and the DARPA Quiness Program through US Army Research Office award W31P4Q-12-1-0019.
Appendix A. Proof of (7) and (8)

The main idea of the proof of (7) follows the approach first put forward in [21] (see also [33]), for which the core argument is the non-increase of quantum relative entropy. Here we instead apply a refinement of this entropy inequality from [24] (see also [25–27]). In order to prove (7), we start by noting that it suffices to prove it when $\rho_{\text{ABE}} = |\psi\rangle\langle\psi|_{\text{ABE}}$ (i.e., the shared state is pure). This is because the conditional entropy only increases under the discarding of one part of the conditioning system. We consider the following isometric extensions of the measurement channels [40], which produce the measurement outcomes and post-measurement states:

$$U_{\text{A} \rightarrow \text{XX}'A} \equiv \sum_x |x\rangle \otimes |x\rangle_{X'} \otimes P^x_A,$$

(A1)

$$V_{\text{A} \rightarrow \text{ZZ}'A} \equiv \sum_z |z\rangle \otimes |z\rangle_{Z'} \otimes Q^z_A.$$

(A2)

We also define the following pure states, which represent purifications of the states $\sigma_{\text{XBE}}$ and $\omega_{\text{ZBE}}$ defined in (1) and (2), respectively:

$$|\sigma\rangle_{\text{XX}'\text{ABE}} \equiv U_{\text{A} \rightarrow \text{XX}'A}|\psi\rangle_{\text{ABE}},$$

(A3)

$$|\omega\rangle_{\text{ZZ}'\text{ABE}} \equiv V_{\text{A} \rightarrow \text{ZZ}'A}|\psi\rangle_{\text{ABE}}.$$

(A4)

Consider from duality of conditional entropy for pure states (see, e.g., [33]) that

$$H(Z|E)_\rho = -H(Z|\text{Z'}\text{AB})_\rho = D(\omega_{\text{ZZ}'\text{AB}}||I_Z \otimes \omega_{\text{Z}'\text{AB}}),$$

(A5)

where $D(\rho||\sigma) \equiv \text{Tr} \{\rho \log \rho - \sigma \log \sigma\}$ is the quantum relative entropy [41], defined as such when $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and as $+\infty$ otherwise. Now consider the following quantum channel

$$\mathcal{P}_{\text{ZZ}'\text{A}}(\cdot) \rightarrow \Pi(\cdot)\Pi + (I - \Pi)(\cdot)(I - \Pi),$$

(A6)

where $\Pi \equiv VV^\dagger$. From the monotonicity of quantum relative entropy with respect to quantum channels [28, 29], we find that

$$D(\omega_{\text{ZZ}'\text{AB}}||I_Z \otimes \omega_{\text{Z}'\text{AB}}) \geq D(\mathcal{P}_{\text{ZZ}'\text{A}}(\omega_{\text{ZZ}'\text{AB}})||\mathcal{P}_{\text{ZZ}'\text{A}}(I_Z \otimes \omega_{\text{Z}'\text{AB}})).$$

(A7)

Consider that $\mathcal{P}_{\text{ZZ}'\text{A}}(\omega_{\text{ZZ}'\text{AB}}) = \omega_{\text{ZZ}'\text{AB}}$. Due to the fact that

$$(I - \Pi)\omega_{\text{ZZ}'\text{AB}}(I - \Pi) = 0,$$

(A8)

and from the direct sum property of the quantum relative entropy (see, e.g., [33]), we have that

$$D(\mathcal{P}_{\text{ZZ}'\text{A}}(\omega_{\text{ZZ}'\text{AB}})||\mathcal{P}_{\text{ZZ}'\text{A}}(I_Z \otimes \omega_{\text{Z}'\text{AB}})) = D(\omega_{\text{ZZ}'\text{AB}}||I_Z \otimes \omega_{\text{Z}'\text{AB}})\Pi.$$  

(A9)

Consider that

$$\Pi(I_Z \otimes \omega_{\text{Z}'\text{AB}}) = VV^\dagger VV^\dagger = V\left(\sum_z Q^z_A \rho_{AB} Q^z_A\right)V^\dagger.$$

(A10)

This, combined with $\omega_{\text{ZZ}'\text{AB}} = V\rho_{AB} V^\dagger$, then implies that

$$D(\omega_{\text{ZZ}'\text{AB}}||\Pi(I_Z \otimes \omega_{\text{Z}'\text{AB}})) = D\left(V\rho_{AB} V^\dagger||V\left(\sum_z Q^z_A \rho_{AB} Q^z_A\right)V^\dagger\right)$$

$$= D\left(\rho_{AB}||\sum_z Q^z_A \rho_{AB} Q^z_A\right).$$

(A11)

(A12)

where the last equality follows from the invariance of quantum relative entropy with respect to isometries. Now consider the following quantum channel:

$$\mathcal{M}_{\text{A} \rightarrow \text{X}} \equiv \text{Tr}_{\text{X}'A} \circ U_{\text{A} \rightarrow \text{XX}'A},$$

(A13)

where $U_{\text{A} \rightarrow \text{XX}'A}(\cdot) \equiv U(\cdot)U^\dagger$. Consider that $\mathcal{M}_{\text{A} \rightarrow \text{X}}(\rho_{AB}) = \sigma_{XB}$. Also, we can calculate

$$\mathcal{M}_{\text{A} \rightarrow \text{X}}\left(\sum_z Q^z_A \rho_{AB} Q^z_A\right)$$

as follows:

$$(\text{Tr}_{\text{X}'A} \circ U_{\text{A} \rightarrow \text{XX}'A})\left(\sum_z Q^z_A \rho_{AB} Q^z_A\right) = \theta_{ XB}.$$

(A14)

(A15)

From [24], we have the following inequality holding for a density operator $\rho$, a positive semi-definite operator $\sigma$, and a quantum channel $\mathcal{N}$:
\[
D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \geq -\log F(\rho, \mathcal{R}(\mathcal{N}(\rho))) ,
\]  
where \(\text{supp}(\rho) \subseteq \text{supp}(\sigma)\) and \(\mathcal{R}\) is a recovery channel with the property that \(\mathcal{R}(\mathcal{N}(\sigma)) = \sigma\). Specifically, \(\mathcal{R}\) is what is known as a variant of the Petz recovery channel, having the form
\[
\mathcal{R}(\cdot) = \int dt \ p(t)\sigma^{-i\mathcal{N}}(\mathcal{R}_\sigma\mathcal{N}(\sigma)^{1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2})\sigma^{i\mathcal{N}}
\]
with \(p(t) = \frac{1}{2}(\cosh(\pi t) + 1)^{-1}\),
\[
\text{supp} \mathcal{R}_\sigma = \text{supp} \mathcal{N} ,
\]
where \(\mathcal{R}_\sigma\mathcal{N}\) is the Petz recovery channel [42–44] defined as
\[
\mathcal{R}_\sigma\mathcal{N}(\cdot) \equiv \sigma^{1/2}\mathcal{N}^{-1}(\mathcal{N}(\sigma)^{-1/2}(\cdot)\mathcal{N}(\sigma)^{-1/2})\sigma^{1/2},
\]
with \(\mathcal{N}^+\) the adjoint of \(\mathcal{N}\) (with respect to the Hilbert–Schmidt inner product). Applying this to our case, we find that
\[
D\left(\rho_{AB}\|\sum_z Q^z_A \rho_{AB} Q^z_A \right) \geq D\left(\mathcal{M}_{A\rightarrow X}(\rho_{AB})\|\mathcal{M}_{A\rightarrow X}\left(\sum_z Q^z_A \rho_{AB} Q^z_A \right)\right)
- \log F(\rho_{AB}, \mathcal{R}_{XB\rightarrow AB}(\mathcal{M}_{A\rightarrow X}(\rho_{AB}))) ,
\]
where the recovery channel is such that
\[
\mathcal{R}_{XB\rightarrow AB}\left(\mathcal{M}_{A\rightarrow X}\left(\sum_z Q^z_A \rho_{AB} Q^z_A \right)\right) = \sum_z Q^z_A \rho_{AB} Q^z_A ,
\]
Consider from our development above that
\[
D\left(\mathcal{M}_{A\rightarrow X}(\rho_{AB})\|\mathcal{M}_{A\rightarrow X}\left(\sum_z Q^z_A \rho_{AB} Q^z_A \right)\right) = D(\sigma_{AB}\|\theta_{AB})
\geq D(\sigma_{AB}\|\|I_X \otimes \sigma_B) - \log c ,
\]
where we have used \(\sigma \leq \sigma' \Rightarrow D(\rho\|\sigma) \leq D(\rho\|\sigma')\) (see, e.g., [33]), applied to \(Q^z_A P^z_B Q^z_A = |Q^z_A P^z_B|^2 \leq c \cdot I_A\), with \(c\) defined in (5). Putting everything together, we conclude that
\[
D(\omega_{ZZ'AB}\|\|I_Z \otimes \omega_{Z'BA}) \geq D(\sigma_{AB}\|\|I_X \otimes \sigma_B) - \log c - \log F(\rho_{AB}, \mathcal{R}_{XB\rightarrow AB}(\sigma_{AB})),
\]
which, after a rewriting, is equivalent to (7) coupled with the constraint in (A20).

The inequality in (8) follows from (7) by letting \(|\psi\rangle_{ABE}\) be a purification of \(\rho_{AB}\) and observing that
\[
H(Z|E)_\omega - H(Z|B)_\omega = -H(A|B)_\rho ,
\]
whenever \(\rho_{ABE}\) is a pure state and \(Q^z_A = |z\rangle \langle z|_A\) for some orthonormal basis \(|z\rangle_A\).

### Appendix B. Explicit form of recovery map

Here we establish the explicit form given in (10) for the recovery map, in the case that \(\{Q^z_A\} = \{|z\rangle \langle z|_A\}\) for some orthonormal basis \(|z\rangle_A\). The main idea is to determine what \(\mathcal{R}_{XB\rightarrow AB}\) in (A19) should be by inspecting (A16) and (A17). For our setup, we are considering a bipartite state \(\rho_{AB}\), a set \(\{Q^z_A\}\) of measurement operators, and the measurement channel
\[
\mathcal{M}_{A\rightarrow X}(\zeta_A) \equiv \sum_x \text{Tr}\left[ P^z_{\Lambda} \zeta_A \right] |x\rangle \langle x|_X ,
\]
where \(\{P^z_A\}\) is a set of projective measurement operators. The entropy inequality in (A19) reduces to
\[
D\left(\rho_{AB}\|\sum_x |z\rangle \langle z|_A \otimes \omega^z_B \right) - D\left(\mathcal{M}_{A\rightarrow X}(\rho_{AB})\|\sum_x |x\rangle \langle x|_X \otimes \theta^z_B \right)
\geq -\log F(\rho_{AB}, \mathcal{R}_{XB\rightarrow AB}(\mathcal{M}_{A\rightarrow X}(\rho_{AB}))) ,
\]
where
\[
\omega^z_B \equiv (|z\rangle \langle z|_A \otimes I_B)\rho_{AB}(|z\rangle \langle z|_A \otimes I_B) ,
\quad \theta^z_B \equiv \sum_z \langle z| P^z_A |z\rangle A_\Lambda \omega^z_B .
\]
Observe that
\[
\sum_x |x\rangle \langle x|_X \otimes \theta^z_B = \mathcal{M}_{A\rightarrow X}\left(\sum_z |z\rangle \otimes \omega^z_B \right) .
\]
Writing the measurement channel as
\[ \mathcal{M}_{\alpha \to y} (\xi) = \sum_x \text{Tr} \{ P^\alpha_x \xi P^\alpha_x \} \langle x | x \rangle = \sum_{x,j} \langle j | A P^\alpha_x \xi P^\alpha_j | j \rangle \langle x | x \rangle \]
(B5)
\[ = \sum_{x,j} \langle x | x \rangle \langle j | A P^\alpha_x \xi P^\alpha_j | j \rangle \]
(B6)
we can see that a set of Kraus operators for it is \{ \langle x | x \rangle | x \}. So its adjoint is as follows:
\[ (\mathcal{M}_{\alpha \to y})^\dagger (\xi) = \sum_{x,j} \langle x | x \rangle \xi \langle x | x \rangle \]
(B7)
\[ \text{and} \]
\[ = \sum_{x} \langle x | x \rangle \xi x j . \]
(B8)
So by inspecting (A16) and (A17), we see that the recovery map has the following form:
\[ \mathcal{R}_{XB \to AB}(\xi_{XB}) = \int dt \ P(t) \left( \sum_{x} | x \rangle \langle x | \otimes \omega^x_B \right)^{1+u} \sum_{x} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes I_B) \left( \sum_{x'} | x' \rangle \langle x' | x \rangle \otimes \theta^x_B \right)^{1+u} \]
(B9)
\[ \times \left( \sum_{x} | x'' \rangle \langle x'' | x \rangle \otimes (\theta^x_B)^{-1+u} \right) \left( \sum_{x} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes I_B) \right) \left( \sum_{x} | x'' \rangle \langle x'' | x \rangle \otimes (\theta^x_B)^{-1+u} \right), \]
(B10)
\[ = \int dt \ P(t) \left( \sum_{x} | x \rangle \langle x | \otimes \omega^x_B \right)^{1+u} \sum_{x,x',x''} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes (\theta^x_B)^{1+u}) \]
\[ \times \left( \sum_{x} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes (\theta^x_B)^{-1+u}) \right), \]
(B11)
\[ = \int dt \ P(t) \left( \sum_{x} | x \rangle \langle x | \otimes \omega^x_B \right)^{1+u} \sum_{x} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes (\theta^x_B)^{1+u}) \]
\[ \times \left( \sum_{x} | x' \rangle \langle x' | x \rangle \otimes (\omega^x_B)^{1+u} \right), \]
(B12)
\[ = \int dt \ P(t) \sum_{x,x',x''} | x \rangle \langle x | \otimes (\omega^x_B)^{1+u} \sum_{x,x'} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes (\theta^x_B)^{-1+u}) \sum_{x} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes (\theta^x_B)^{-1+u}) \]
\[ \times \sum_{x} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes (\omega^x_B)^{1+u}). \]
(B13)
We can thus abbreviate its action as
\[ \mathcal{R}_{XB \to AB}(\xi_{XB}) = \sum_{x,x',x''} | x \rangle \langle x | \otimes \mathcal{R}_{XB \to AB}^{x,x',x''}(\xi_{XB}), \]
(B14)
where
\[ \mathcal{R}_{XB \to AB}^{x,x',x''}(\xi_{XB}) \equiv \int dt \ P(t) (\omega^x_B)^{1+u} (\theta^x_B)^{-1+u} \text{Tr}_X \{ \langle x | \langle x | \otimes (\omega^x_B)^{1+u} (\theta^x_B)^{1+u} \}
\]
(B15)
(Note that \( \mathcal{R}_{XB \to AB}^{x,x',x''}(\xi_{XB}) \) is not a channel.) So then the action on the classical-quantum state \( \sigma_{XB} \), defined as
\[ \sigma_{XB} \equiv \sum_{x} | x \rangle \langle x | \otimes \sigma^x_B, \]
(B16)
with \( \sigma^x_B \equiv \text{Tr}_A \{ P^\alpha_x \rho_{AB} \} \), is as follows:
\[ \mathcal{R}_{XB \to AB}(\sigma_{XB}) = \sum_{x,x',x''} | x \rangle \langle x | \otimes \sum_{x,x'} \mathcal{P}^\alpha_x (\langle x | x \rangle \otimes (\omega^x_B)^{1+u} (\theta^x_B)^{1+u} \sigma^x_B (\omega^x_B)^{1+u}). \]
(B17)
References