Information conservation and entropy change in quantum measurements

Shunlong Luo[*]
Fakultät für Mathematik, Universität Bielefeld, D-33615 Bielefeld, Germany and
Academy of Mathematics and Systems Science, Chinese Academy of Sciences, 100190 Beijing, People's Republic of China

(Received 18 August 2010; published 2 November 2010)

The information transfer in the system-apparatus-environment trio is of fundamental importance for both the theory and practice of quantum information. Based on a canonical joint purification which encodes the system, apparatus, and environment as well as their interplay, we establish several basic relations involving various entropies arising from the most general quantum measurements. Some celebrated results concerning entropy change and information-disturbance tradeoff are recaptured as particular cases in a unified framework of information conservation.

DOI: 10.1103/PhysRevA.82.052103 PACS number(s): 03.65.Ta, 03.67.−a

I. INTRODUCTION

The characteristics and nature of information transfer and entropy change in a quantum measurement are of basic significance for quantum theory. This issue was investigated by many authors [1–10]. In particular, various entropic inequalities including the Holevo-type bounds [11–18] and information-disturbance tradeoff [19–29] were established. However, most investigations in this line ignored the information carried away by the measuring apparatus and the environment. In order to gain a deeper understanding of the information change in a measurement, it is necessary to keep track of the interplay among the quantum system, the measuring apparatus, and the environment. For this purpose, we introduce a canonical joint purification of state and measurement and establish some relations concerning entropy change in a unified framework.

Consider a general measurement $\mathcal{M} = \{\mathcal{M}_\mu\}$ described by a family of quantum operations. Each $\mathcal{M}_\mu$ can be expressed in the Kraus form as $\mathcal{M}_\mu\rho := \sum_s M_{\mu s}\rho M_{\mu s}^\dagger$ with $\sum_s M_{\mu s}^\dagger M_{\mu s} \leqslant \mathbf{1}$ [30]. The completeness of the measurement then imposes that $\sum_{\mu s} M_{\mu s}^\dagger M_{\mu s} = \mathbf{1}$, which is equivalent to that $\{E_\mu := \sum_s M_{\mu s}^\dagger M_{\mu s}\}$ constitutes a positive operator-valued measure (POVM) used in describing the outcome probabilities. $\mathcal{M}$ is also called a quantum instrument, which is a more general notion than that of a POVM since it captures not only the outcome probabilities but also the postmeasurement states [28,30,31]. The measurement $\mathcal{M}$ is efficient (or ideal) if the index set of s degenerates to a single point [20,32]; that is, each $\mathcal{M}_\mu$ has a single Kraus operator in the sense that $\mathcal{M}_\mu\rho = M_\mu\rho M_\mu^\dagger$.

After performing the measurement $\mathcal{M}$ on a quantum state ρ, there are two scenarios for the postmeasurement states: In the selective case, the outcomes constitute a quantum ensemble $\{p_\mu,\rho_\mu\}$ with

$$p_\mu := \mathrm{tr}\mathcal{M}_\mu\rho, \quad \rho_\mu := \frac{1}{p_\mu}\mathcal{M}_\mu\rho.$$

The outcome labeled by μ occurs with probability p_μ and the corresponding postmeasurement state conditioned on μ is ρ_μ. In the nonselective case, the distinction among the various outcomes is discarded, and the overall postmeasurement state representing the state-of-knowledge is

$$\mathcal{M}\rho := \sum_\mu p_\mu\rho_\mu.$$

The natural questions arise as for the relations among the various entropies:

$$S(\rho), \quad S(\mathcal{M}\rho), \quad \sum_\mu p_\mu S(\rho_\mu), \quad H(p).$$

Here $S(\rho) := -\mathrm{tr}\rho\ln\rho$ is the von Neumann entropy, and $H(p) := -\sum_\mu p_\mu \ln p_\mu$ denotes the Shannon entropy of $p := \{p_\mu\}$. The difference

$$S(\mathcal{M}\rho) - \sum_\mu p_\mu S(\rho_\mu)$$

is the Holevo quantity of the ensemble $\{p_\mu,\rho_\mu\}$, which is a key concept in transmitting classical information by quantum means [11–18]. The difference

$$S(\rho) - \sum_\mu p_\mu S(\rho_\mu)$$

is the entropy reduction. In particular, it is of fundamental importance to estimate the entropy changes

$$S(\mathcal{M}\rho) - S(\rho), \quad S(\rho) - \sum_\mu p_\mu S(\rho_\mu).$$

Some celebrated results in this respect are as follows.

The first is that $\mathcal{M}$ may increase or decrease the entropy; that is, $S(\mathcal{M}\rho) - S(\rho)$ may sometimes be positive and sometimes be negative (of course, sometimes zero). However, when $\mathcal{M}$ is a (Lüders) projective measurement $\Pi = \{\Pi_\mu\}$, then $S(\Pi\rho) - S(\rho) \geqslant 0$: Any projective measurement increases entropy [5,33]. More generally, if $\mathcal{M}$ preserves the identity operator $\mathbf{1}$, then

$$S(\mathcal{M}\rho) - S(\rho) \geqslant 0. \tag{1}$$

This can be readily seen from the monotonicity of quantum relative entropy [4,9,33],

$$D(\mathcal{M}\rho|\mathcal{M}\sigma) \leqslant D(\rho|\sigma),$$

by simply taking σ to be the maximally mixed state (proportional to $\mathbf{1}$). Here $D(\rho|\sigma) := \mathrm{tr}\rho(\ln\rho - \ln\sigma)$. Conversely, in order for inequality (1) to be true for any ρ, it is also necessary

[*] luosl@amt.ac.cn

that $\mathcal{M}$ preserves the identity operator since the maximally mixed state has the maximal entropy.

The second result concerns the positivity of the entropy reduction first conjectured by Groenewold [2]: For any projective measurement, it holds that

$$S(\rho) - \sum_{\mu} p_{\mu} S(\rho_{\mu}) \geqslant 0. \tag{2}$$

This inequality was first proved by Lindblad [5] and further generalized by Ozawa [8], who identified the conditions for $\mathcal{M}$ such that the foregoing inequality holds.

The main purpose of the present article is to establish some information conservation relations and to derive significantly more stringent bounds than inequalities (1) and (2). We derive various entropic inequalities, information-disturbance tradeoff, and leakage-disturbance tradeoff relations in a unified fashion. Apart from their own intrinsic significance for quantifying Heisenberg's intuition on the uncertainty principle from the information perspective, these relations are useful in practice for quantum communication and quantum estimation. For example, in quantum cryptography, the eavesdropping strategies are limited by the information-disturbance tradeoff, which actually lies at the heart of Biham *et al.*'s proof of the unconditional security of the BB84 quantum key distribution protocol [19].

The article is structured as follows. In Sec. II, we introduce a purification framework which keeps track of all the information transfer in a quantum measurement. With the help of this purification scheme, we establish several information conservation and entropic relations in Sec. III. We discuss the information-disturbance tradeoff and the leakage-disturbance tradeoff in Sec. IV. Finally, we summarize the results in Sec. V.

II. PURIFICATION: APPARATUS AND ENVIRONMENT

In order to get deeper relations concerning the entropy change induced by a measurement, it is necessary to go beyond $\mathcal{M}$ and ρ and to take full account of the information carried away by the measuring apparatus and the environment. Thus, in addition to the system space H^b, we introduce an apparatus space H^c recording the measurement outcomes and an environment space H^d recording the internal degree of measurement operations, with orthonormal bases $\{|\mu\rangle\}$ and $\{|s\rangle\}$, respectively. With respect to these spaces, we introduce two auxiliary quantum operations $\bar{\mathcal{M}} = \{\bar{\mathcal{M}}_s\}$ and $\tilde{\mathcal{M}} = \{\tilde{\mathcal{M}}_\mu\}$ as

$$\bar{\mathcal{M}}_s \rho := \sum_{\mu\nu} \mathrm{tr}(M_{\mu s} \rho M_{\nu s}^{\dagger}) |\mu\rangle\langle\nu|, \tag{3}$$

$$\tilde{\mathcal{M}}_\mu \rho := \sum_{st} \mathrm{tr}(M_{\mu s} \rho M_{\mu t}^{\dagger}) |s\rangle\langle t|, \tag{4}$$

which are maps from the system state space to the apparatus state space and the environment state space, respectively. The intuition and motivation for introducing these maps come from the desire to make manifest some intrinsic characteristics of $\mathcal{M}$ in the apparatus and the environment. We may describe $\bar{\mathcal{M}}_s$ and $\tilde{\mathcal{M}}_\mu$ in the Stinespring representation [27] as $\bar{\mathcal{M}}_s = \mathrm{tr}_b A_s \rho A_s^{\dagger}$ and $\tilde{\mathcal{M}}_\mu = \mathrm{tr}_b B_\mu \rho B_\mu^{\dagger}$, respectively. Here $A_s : H^b \to H^b \otimes H^c$ and $B_\mu : H^b \to H^b \otimes H^d$ are defined as

$$A_s |\phi^b\rangle := \sum_{\mu} M_{\mu s} |\phi^b\rangle \otimes |\mu\rangle,$$

$$B_\mu |\phi^b\rangle := \sum_{s} M_{\mu s} |\phi^b\rangle \otimes |s\rangle,$$

respectively. Clearly, $A_s^{\dagger} A_s \leqslant \mathbf{1}$ and $B_\mu^{\dagger} B_\mu \leqslant \mathbf{1}$.

While $\mathcal{M}$ records the physical effects on the measured system, $\bar{\mathcal{M}}$ and $\tilde{\mathcal{M}}$ keep track of the physical effects on the apparatus and the environment, respectively. Now in addition to the entropies related to the original measurement $\mathcal{M}$, we also have the corresponding entropies $S(\bar{\mathcal{M}}\rho)$ and $(\tilde{\mathcal{M}}\rho)$ induced by the quantum operations $\bar{\mathcal{M}}$ and $\tilde{\mathcal{M}}$, which will be exploited to establish various inequalities concerning the entropy change induced by the original measurement $\mathcal{M}$. $S(\mathcal{M}\rho)$, as the entropy of the postmeasurement state, may be called the measurement entropy [3,6], and following Refs. [7,34], $S(\bar{\mathcal{M}}\rho)$ may be called the exchange entropy. It is also tempting to call $S(\tilde{\mathcal{M}}\rho)$ the leaking entropy since it represents the entropy leaking into the environment. When $\mathcal{M}$ is an efficient measurement, $S(\tilde{\mathcal{M}}\rho)$ vanishes because $\tilde{\mathcal{M}}\rho$ is a pure state.

Let ρ be a state on the system space $H = H^b$ with the spectral decomposition $\rho = \sum_j \lambda_j |j\rangle\langle j|$, and let $\mathcal{M} = \{\mathcal{M}_\mu\}$ be a measurement on H. Let H^a be an auxiliary space which is a copy of H^b and let $H^c \otimes H^d$ be the apparatus-environment space spanned by the orthonormal bases $\{|\mu\rangle \otimes |s\rangle\}$ which are used in Eqs. (3) and (4). We introduce the four-partite state

$$|\Omega^{abcd}\rangle := \sum_{j\mu s} \sqrt{\lambda_j} |j\rangle \otimes M_{\mu s} |j\rangle \otimes |\mu\rangle \otimes |s\rangle$$

in $H^a \otimes H^b \otimes H^c \otimes H^d$, which captures and encodes the state ρ, the measurement $\mathcal{M}$, the apparatus, and the environment as well as their interplay in a single pure state. This state may be viewed as a joint purification of ρ and $\mathcal{M}$ with very natural and informative characteristics as will be seen, and it will play a central role in our information-theoretical analysis of information transfer in quantum measurements.

Put $\rho^{abcd} := |\Omega^{abcd}\rangle\langle\Omega^{abcd}|$, then the various reduced one-partite states are just

$$\rho^a = \rho, \quad \rho^b = \mathcal{M}\rho, \quad \rho^c = \bar{\mathcal{M}}\rho, \quad \rho^d = \tilde{\mathcal{M}}\rho.$$

Thus the measurements $\bar{\mathcal{M}}$ and $\tilde{\mathcal{M}}$ are put on an equal footing with the original measurement $\mathcal{M}$ in the sense that they all constitute one-partite marginal states of the joint purification and have the physical significance for recording the impact of the original measurement $\mathcal{M}$ on the apparatus and the environment, respectively.

The various reduced tripartite states of ρ^{abcd} are

$$\rho^{abc} := \sum_{s} q_s \big|\Upsilon_s^{abc}\big\rangle\big\langle\Upsilon_s^{abc}\big|,$$

$$\rho^{abd} = \sum_{\mu} p_\mu \big|\Phi_\mu^{abd}\big\rangle\big\langle\Phi_\mu^{abd}\big|,$$

$$\rho^{acd} = \sum_{jk\mu\nu st} q_{jk\mu\nu st} |j\rangle\langle k| \otimes |\mu\rangle\langle\nu| \otimes |s\rangle\langle t|,$$

$$\rho^{bcd} = \sum_{j} \lambda_j \big|\Psi_j^{bcd}\big\rangle\big\langle\Psi_j^{bcd}\big|,$$

where $q_s := \mathrm{tr} \sum_\mu M_{\mu s}\rho M_{\mu s}^\dagger$ and

$$q_{jk\mu\nu st} := \sqrt{\lambda_j\lambda_k}\mathrm{tr}(M_{\mu s}|j\rangle\langle k|M_{\nu t}^\dagger),$$

$$\left|\Upsilon_s^{abc}\right\rangle := \sum_{j\mu}\sqrt{\lambda_j}|j\rangle \otimes \frac{1}{\sqrt{q}_s}M_{\mu s}|j\rangle \otimes |\mu\rangle,$$

$$\left|\Phi_\mu^{abd}\right\rangle := \sum_{js}\sqrt{\lambda_j}|j\rangle \otimes \frac{1}{\sqrt{p}_u}M_{\mu s}|j\rangle \otimes |s\rangle,$$

$$\left|\Psi_j^{bcd}\right\rangle := \sum_{\mu s} M_{\mu s}|j\rangle \otimes |\mu\rangle \otimes |s\rangle.$$

These states are basic ingredients in characterizing information conservation in quantum measurements.

III. ENTROPIC RELATIONS

Now we investigate entropic relations arising from the interplay between the state, the measurement, the apparatus, and the environment. Since ρ^{abcd} is a pure state, we have $S(\rho^a) = S(\rho^{bcd})$, $S(\rho^b) = S(\rho^{acd})$, $S(\rho^c) = S(\rho^{abd})$, and $S(\rho^d) = S(\rho^{abc})$. Noting that $\rho^a = \rho$, $\rho^b = \mathcal{M}\rho$, $\rho^c = \bar{\mathcal{M}}\rho$, and $\rho^d = \tilde{\mathcal{M}}\rho$, we immediately obtain the following identities, which may be interpreted as concrete realizations for information conservation.

Proposition 1. It holds that

$$S(\rho) = S\left(\sum_j \lambda_j \left|\Psi_j^{bcd}\right\rangle\left\langle\Psi_j^{bcd}\right|\right),$$

$$S(\mathcal{M}\rho) = S\left(\sum_{jk\mu\nu st} q_{jk\mu\nu st}|j\rangle\langle k| \otimes |\mu\rangle\langle\nu| \otimes |s\rangle\langle t|\right),$$

$$S(\bar{M}\rho) = S\left(\sum_\mu p_\mu \left|\Phi_\mu^{abd}\right\rangle\left\langle\Phi_\mu^{abd}\right|\right),$$

$$S(\tilde{\mathcal{M}}\rho) = S\left(\sum_s q_s \left|\Upsilon_s^{abc}\right\rangle\left\langle\Upsilon_s^{abc}\right|\right).$$

These information conservation formulas, apart from their own interests, allow us to systematically derive entropic inequalities when combined with the monotonicity of quantum relative entropy. For example, from the last two equations, it immediately follows that

$$S(\bar{\mathcal{M}}\rho) \leqslant H(p), \quad S(\tilde{\mathcal{M}}\rho) \leqslant H(q).$$

Concerning the entropy change under any nonselective measurement, we have the following results.

Proposition 2. It holds that

$$S(\rho) \leqslant S(\mathcal{M}\rho) + S(\bar{\mathcal{M}}\rho) + S(\tilde{\mathcal{M}}\rho), \tag{5}$$

$$S(\rho) \geqslant S(\mathcal{M}\rho) - S(\bar{\mathcal{M}}\rho) - S(\tilde{\mathcal{M}}\rho). \tag{6}$$

In particular, if $\mathcal{M}$ is efficient, then $S(\tilde{\mathcal{M}}\rho) = 0$ and consequently [7,18]

$$S(\mathcal{M}\rho) - S(\bar{\mathcal{M}}\rho) \leqslant S(\rho) \leqslant S(\mathcal{M}\rho) + S(\bar{\mathcal{M}}\rho). \tag{7}$$

To prove inequality (5), noting that ρ^{bcd} has three marginal states $\rho^b = \mathcal{M}\rho$, $\rho^c = \bar{\mathcal{M}}\rho$, and $\rho^d = \bar{\mathcal{M}}\rho$, by the subadditivity of the von Neumann entropy, we immediately have

$$\begin{aligned} S(\rho) = S(\rho^a) = S(\rho^{bcd}) &\leqslant S(\rho^b) + S(\rho^c) + S(\rho^d) \\ &= S(\mathcal{M}\rho) + S(\bar{\mathcal{M}}\rho) + S(\tilde{\mathcal{M}}\rho). \end{aligned}$$

Similarly, inequality (6) follows from

$$\begin{aligned} S(\mathcal{M}\rho) = S(\rho^b) = S(\rho^{acd}) &\leqslant S(\rho^a) + S(\rho^c) + S(\rho^d) \\ &= S(\rho) + S(\tilde{\mathcal{M}}\rho) + S(\bar{\mathcal{M}}\rho). \end{aligned}$$

It should be emphasized that inequalities (5), (6), and (7) still hold when the four entropies $S(\rho), S(\mathcal{M}\rho)$, $S(\bar{\mathcal{M}}\rho)$, and $S(\tilde{\mathcal{M}}\rho)$ are arbitrarily permutated. The proofs are completely similar.

Concerning the entropy change under any selective quantum measurement, we have the following inequalities which refine the Groenewold-Lindblad-Ozawa result [2,5,8] and inequality (9) in Ref. [18].

Proposition 3. It holds that

$$-S(\tilde{\mathcal{M}}\rho) \leqslant S(\rho) - \sum_\mu p_\mu S(\rho_\mu) \leqslant S(\tilde{\mathcal{M}}\rho) + S(\bar{\mathcal{M}}\rho). \tag{8}$$

In particular, if $\mathcal{M}$ is efficient, then

$$0 \leqslant S(\rho) - \sum_\mu p_\mu S(\rho_\mu) \leqslant S(\bar{\mathcal{M}}\rho). \tag{9}$$

To establish the first inequality in (8), consider $\rho^{bc} = \sum_{\mu\nu s} M_{\mu s}\rho M_{\nu s}^\dagger \otimes |\mu\rangle\langle\nu|$ and the projective measurement $\Pi = \{\mathbf{1}^b \otimes |\mu\rangle\langle\mu|\}$ (which is of course efficient), we have $\bar{\Pi}\rho^{bc} = \sum_{\mu\nu}\pi_{\mu\nu}|\mu\rangle\langle\nu|$ with

$$\pi_{\mu\nu} = \mathrm{tr}(\mathbf{1}^b \otimes |\mu\rangle\langle\mu|)\rho^{bc}(\mathbf{1}^b \otimes |\nu\rangle\langle\nu|) = \delta_{\mu\nu}p_\mu,$$

and thus $S(\bar{\Pi}\rho^{bc}) = H(p)$ and $S(\tilde{\Pi}\rho^{bc}) = 0$. Now applying inequality (6) to the state ρ^{bc} and the measurement Π, we have

$$\begin{aligned} S(\rho^{bc}) &\geqslant S(\Pi\rho^{bc}) - S(\bar{\Pi}\rho^{bc}) \\ &= S\left(\sum_\mu p_\mu\rho_\mu \otimes |\mu\rangle\langle\mu|\right) - S(\bar{\Pi}\rho^{bc}) \\ &= \sum_\mu p_\mu S(\rho_\mu) + H(p) - H(p) \\ &= \sum_\mu p_\mu S(\rho_\mu). \end{aligned}$$

The desired result follows by noting that

$$S(\rho^{bc}) = S(\rho^{ad}) \leqslant S(\rho^a) + S(\rho^d) = S(\rho) + S(\tilde{\mathcal{M}}\rho).$$

To prove the second inequality in (8), put $\rho_\mu^{abd} := |\Phi_\mu^{abd}\rangle \langle\Phi_\mu^{abd}|$, then $\sum_\mu p_\mu\rho_\mu^{abd} := \rho^{abd}$ and the various reduced states satisfy $\rho_\mu^b = \rho_\mu$ and

$$\sum_\mu p_\mu\rho_\mu^a = \rho^a = \rho, \quad \sum_\mu p_\mu\rho_\mu^b = \mathcal{M}\rho, \quad \sum_\mu p_\mu\rho_\mu^d = \tilde{\mathcal{M}}\rho.$$

Now the desired inequality follows from

$$\begin{aligned}
S(\bar{M}\rho) &= S\left(\sum_\mu p_\mu \rho_\mu^{abd}\right)\\
&= \sum_\mu p_\mu D\big(\rho_\mu^{abd}\big|\rho^{abd}\big) \ \big(\text{since } \rho_\mu^{abd} \text{ is pure}\big)\\
&\geqslant \sum_\mu p_\mu D\big(\rho_\mu^{a}\big|\rho^{a}\big)\\
&= S(\rho) - \sum_\mu p_\mu S\big(\rho_\mu^{a}\big)\\
&= S(\rho) - \sum_\mu p_\mu S\big(\rho_\mu^{bd}\big) \ \big(\text{since } \rho_\mu^{abd} \text{ is pure}\big)\\
&\geqslant S(\rho) - \sum_\mu p_\mu \big[S\big(\rho_\mu^{b}\big) + S\big(\rho_\mu^{d}\big)\big]\\
&\geqslant S(\rho) - \sum_\mu p_\mu S(\rho_\mu) - S(\tilde{\mathcal{M}}\rho).
\end{aligned}$$

Concerning the entropy change relating selective and nonselective measurements, we have the following result, which extends inequality (8) in Ref. [18] to the general measurement case.

Proposition 4. It holds that

$$S(\mathcal{M}\rho) - \sum_\mu p_\mu S(\rho_\mu) \leqslant S(\bar{\mathcal{M}}\rho).$$

This follows readily from

$$\begin{aligned}
S(\bar{M}\rho) &= \sum_\mu p_\mu D\big(\rho_\mu^{abd}\big|\rho^{abd}\big) \geqslant \sum_\mu p_\mu D\big(\rho_\mu^{b}\big|\rho^{b}\big)\\
&= S(\mathcal{M}\rho) - \sum_\mu p_\mu S\big(\rho_\mu^{b}\big) = S(\mathcal{M}\rho) - \sum_\mu p_\mu S(\rho_\mu).
\end{aligned}$$

IV. INFORMATION, DISTURBANCE, LEAKAGE

With the purpose of quantifying the information-disturbance-leakage relations, we investigate the distribution of correlations, as quantified by the quantum mutual information, among various bipartite states reduced from the overall state ρ^{abcd}. Recall that the total correlations in the bipartite state ρ^{ab} is well quantified by the quantum mutual information [9,35]

$$I(\rho^{ab}) := S(\rho^a) + S(\rho^b) - S(\rho^{ab}).$$

We also need the conditional quantum mutual information

$$I(\rho^{abc}|\rho^c) := S(\rho^{ac}|\rho^c) + S(\rho^{bc}|\rho^c) - S(\rho^{abc}|\rho^c),$$

which is non-negative by the strong subadditivity of the von Neumann entropy. Here $S(\rho^{ac}|\rho^c) := S(\rho^{ac}) - S(\rho^c)$ and $S(\rho^{abc}|\rho^c) := S(\rho^{abc}) - S(\rho^c)$ are the conditional quantum entropies.

Let $|\Theta^{ab}\rangle := \sum_j \sqrt{\lambda_j}|j\rangle \otimes |j\rangle$ be the canonical purification of ρ. Define the map $\mathbf{M}{:}H^b \to H^b \otimes H^c \otimes H^d$ as

$$\mathbf{M}|\phi^b\rangle := \sum_{\mu s} M_{\mu s}|\phi^b\rangle \otimes |\mu\rangle \otimes |s\rangle,$$

then $|\Omega^{abcd}\rangle = (\mathbf{1} \otimes \mathbf{M})(|\Theta^{ab}\rangle)$. We gauge the information gain of the measurement $\mathcal{M}$ by

$$G(\rho,\mathcal{M}) := I(\rho^{ac}).$$

The physical intuition behind this is that the reference system H^a, as an image ghost of H^b, records the initial quantum state $\rho = \rho^b$ faithfully through $|\Theta^{ab}\rangle$, and the correlation quantity $I(\rho^{ac})$ records the information generated by the measurement $\mathcal{M}$ in the apparatus H^c about the original state $\rho = \rho^a$ and thus represents the information flow from ρ to the apparatus. This is in the original spirit of von Neumann when he considered a quantum measurement as the creation of correlations between the system and the apparatus [36].

Similarly, the disturbance to the quantum state ρ may be quantified by the decreasing of quantum mutual information between the auxiliary system H^a and the measured system H^b as

$$D(\rho,\mathcal{M}) := I(|\Theta^{ab}\rangle\langle\Theta^{ab}|) - I(\rho^{ab}),$$

which is equivalent to that introduced by Maccone in terms of $S(\rho) - I_c(\rho,\mathcal{M})$ from an axiomatic approach combined with heuristic quantum communication considerations [25]. Here $I_c(\rho,\mathcal{M}) := S(\mathcal{M}\rho) - S(\rho^{ab})$ is the coherent information [37,38]. Our definition seems more straightforward and intuitive. Interestingly, $D(\rho,\mathcal{M})$ can also be rewritten as

$$D(\rho,\mathcal{M}) = I(\rho^{a:cd}) = S(\rho^a) + S(\rho^{cd}) - S(\rho^{acd}),$$

which turns out also to be equivalent to the measure of disturbance defined by Buscemi *et al.* via a generalization of the notion of coherent information loss for quantum communication [28]. This can be seen from

$$\begin{aligned}
I(|\Theta^{ab}\rangle\langle\Theta^{ab}|) - I(\rho^{ab}) &= S(\rho^a) + S(\rho^{ab}) - S(\rho^b)\\
&= S(\rho^a) + S(\rho^{cd}) - S(\rho^{acd}).
\end{aligned}$$

Consequently, $D(\rho,\mathcal{M})$ unifies the seemingly different approaches of Maccone [25] and Buscemi *et al.* [28] in our setting. We further define the information leakage

$$L(\rho,\mathcal{M}) := I(\rho^{ad}),$$

which is the information that leaks out to the environment. The inefficiency of the measurement $\mathcal{M}$ may be characterized by this quantity: When $\mathcal{M}$ is efficient, $L(\rho,\mathcal{M})$ vanishes.

To summarize more transparently the physical significance of the information gain G, the disturbance D, and the leakage L in a unified fashion, recall that the detailed measurement characteristics of $\mathcal{M}$ are encoded in the four-partite state $|\Omega^{abcd}\rangle = (\mathbf{1} \otimes \mathbf{M})|\Theta^{ab}\rangle$. This resulting state stems from the action of the measurement process on the initial purification of the state ρ which bears no relation to the apparatus space H^c and the environment space H^d; that is, the initial correlations between the purified system and both the apparatus and the environment vanish. Consequently, the emerging correlation $G(\rho,\mathcal{M}) = I(\rho^{ac})$ between $\rho^a = \rho$ and the apparatus is just the information gained by the measurement, and the emerging correlation $L(\rho,\mathcal{M}) = I(\rho^{ad})$ between the state $\rho^a = \rho$ and the environment is just the information carried away by the environment (thus may be interpreted as the information leakage to the environment). Finally, since the initial correlation between ρ^a and ρ^b is $I(|\Theta^{ab}\rangle\langle\Theta^{ab}|)$, and after the measurement, the correlation between ρ^a and ρ^b is $I(\rho^{ab})$, the loss $D(\rho,\mathcal{M}) = I(|\Theta^{ab}\rangle\langle\Theta^{ab}|) - I(\rho^{ab})$ due to the measurement may be naturally interpreted as a figure of merit quantifying the disturbance caused by $\mathcal{M}$.

In this context, we recover the information-disturbance balance relation

$$G(\rho,\mathcal{M}) + I(\rho^{acd}|\rho^c) = D(\rho,\mathcal{M})$$

due to Buscemi *et al.* [28]. In particular, since $I(\rho^{acd}|\rho^c) \geqslant 0$, we see that the information gain is always dominated by the disturbance. Similarly, we have the leakage-disturbance relation

$$L(\rho,\mathcal{M}) + I(\rho^{acd}|\rho^d) = D(\rho,\mathcal{M}).$$

These relations may be useful in quantum cryptographic analysis.

V. SUMMARY

By exploiting a powerful joint purification of state and measurement, we have obtained some information conservation relations for quantum states under general measurements. Based on these relations, we have derived various inequalities for entropy change under both selective and nonselective measurements in a unified framework. Some fundamental entropic inequalities are recaptured as particular instances. The joint purification scheme may also be useful in other contexts such as the study of quantum cryptography. It will be desirable to further explore the consequence and implications of these entropic relations for practical issues.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant No. 10771208), the Science Fund for Creative Research Groups (Grant No. 10721101), and the Key Lab of Random Complex Structures and Data Science, Chinese Academy of Sciences (Grant No. 2008DP173182).

[1] H. Umegaki, Kōdai Math. Sem. Rep. **14**, 59 (1962).

[2] H. J. Groenewold, Int. J. Theor. Phys. **4**, 327 (1971).

[3] R. S. Ingarden, Rep. Math. Phys. **10**, 43 (1976).

[4] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).

[5] G. Lindblad, Commun. Math. Phys. **28**, 245 (1972); **33**, 305 (1973); **39**, 111 (1974); **40**, 147 (1975).

[6] R. Balian, M. Vénéroni, and N. Balazs, Europhys. Lett. **1**, 1 (1986).

[7] G. Lindblad, in *Quantum Aspects of Optical Communication*, edited by C. Benjaballah *et al.* (Springer, Berlin, 1991), pp. 71–80.

[8] M. Ozawa, J. Math. Phys. **27**, 759 (1986).

[9] V. Vedral, Rev. Mod. Phys. **74**, 197 (2002).

[10] A. Barchielli and G. Lupieri, Quantum Inf. Comput. **6**, 016 (2006).

[11] A. S. Holevo, Prob. Inf. Transm. **9**, 177 (1973).

[12] H. P. Yuen and M. Ozawa, Phys. Rev. Lett. **70**, 363 (1993).

[13] R. Jozsa, D. Robb, and W. K. Wootters, Phys. Rev. A **49**, 668 (1994).

[14] H. Scutaru, Phys. Rev. Lett. **75**, 773 (1995).

[15] B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. Lett. **76**, 3452 (1996).

[16] M. J. W. Hall, Phys. Rev. A **55**, 100 (1997).

[17] K. Jacobs, Phys. Rev. A **68**, 054302 (2003).

[18] W. Roga, M. Fannes, and K. Zyczkowski, Phys. Rev. Lett. **105**, 040505 (2010).

[19] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 715–724.

[20] C. A. Fuchs and K. Jacobs, Phys. Rev. A **63**, 062305 (2001).

[21] K. Banaszek, Phys. Rev. Lett. **86**, 1366 (2001).

[22] H. Barnum, e-print arXiv:quant-ph/0205155v1.

[23] G. M. D'Ariano, Fortschr. Phys. **51**, 318 (2003).

[24] M. F. Sacchi, Phys. Rev. Lett. **96**, 220502 (2006).

[25] L. Maccone, Europhys. Lett. **77**, 40002 (2007).

[26] F. Buscemi, Phys. Rev. Lett. **99**, 180501 (2007).

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

[28] F. Buscemi, M. Hayashi, and M. Horodecki, Phys. Rev. Lett. **100**, 210504 (2008).

[29] S. L. Zhang, X. B. Zou, C. F. Li, C.-H. Jin, and G.-C. Guo, J. Phys. A **43**, 235301 (2010).

[30] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin, 1983).

[31] E. B. Davis and J. T. Lewis, Commun. Math. Phys. **17**, 239 (1970).

[32] M. A. Nielsen and C. M. Caves, Phys. Rev. A **55**, 2547 (1997).

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

[34] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

[35] N. Li and S. Luo, Phys. Rev. A **76**, 032327 (2007).

[36] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, 1955).

[37] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).

[38] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).