PHYSICAL REVIEW A, VOLUME 63, 062305

Information-tradeoff relations for finite-strength quantum measurements

Christopher A. Fuchs* and Kurt Jacobs
T-8, Theoretical Division, Los Alamos National Laboratory, Los Alamos, New Mexico 87545
(Received 27 September 2000; published 16 May 2001)

In this paper we describe a way to quantify the folkloric notion that quantum measurements bring a disturbance to the system being measured. We consider two observers who initially assign identical mixed-state density operators to a two-state quantum system. The question we address is to what extent one observer can, by measurement, increase the purity of his density operator without affecting the purity of the other observer's. If there were no restrictions on the first observer's measurements, then he could carry this out trivially by measuring the initial density operator's eigenbasis. If, however, the allowed measurements are those of finite strength—i.e., those measurements strictly within the interior of the convex set of all measurements—then the issue becomes significantly more complex. We find that for a large class of such measurements the first observer's purity increases the most precisely when there is some loss of purity for the second observer. More generally the tradeoff between the two purities, when it exists, forms a monotonic relation. This tradeoff has potential application to quantum state control and feedback.

DOI: 10.1103/PhysRevA.63.062305 PACS number(s): 03.67.−a, 02.50.−r, 03.65.Ta

I. INTRODUCTION

Since the earliest days of quantum mechanics, a common idea associated with the measurement process has been that it necessarily disturbs or interferes with the system being observed. For instance Bohr, in his reply to the Einstein-Podolsky-Rosen paper [1], wrote that the quantum description ''may be characterized as a rational utilization of all possibilities of unambiguous interpretation . . . compatible with the finite and uncontrollable interaction between the objects and the measuring instruments'' [2,3] (also see Refs. [4,5]). Or Pauli, on a much later occasion, wrote that ''every act of observation is an interference, of undeterminable extent, with the instruments of observation as well as with the system observed, and interrupts the causal connection between the phenomena preceding and succeeding it'' [6]. See Refs. [7,8] for a more complete bibliographic account of this issue.

Without question, it has also been apparent since the earliest days of the theory that these proclamations are somewhat dubious. The question is this: What is it that is being interfered with or disturbed in a measurement? If there were a set of hidden variables underneath the statistical predictions of quantum theory, then the answer would be at hand: The act of measurement disturbs the hidden variables. In the absence of a hidden-variable explanation [9], however, this becomes a moot point. Measuring x cannot disturb p if p does not have an independent existence before a measurement elicits its value [10]. In fact one has to wonder why the word ''measurement'' is used at all in this context: If there are no free-standing values x and p to disturb, then surely there are no values to measure either.

Eschewing metaphysical concerns, one might try to give a precise sense to the idea that measurements cause disturbance by focusing solely on the wave function itself. This is because the wave function appears to be the simplest term in the theory that would even allow a precise formulation of the question. One might say for instance, that ''the word measurement is a misnomer for our experimental interventions into the course of nature [11,12]. The unpredictable wave-function collapse is the quantitative signature of a disturbance in quantum measurement. Since the state change is random, the measurement causes an uncontrollable disturbance.'' But this formulation too is not without problem. The quantum state resulting from a measurement depends in a crucial way on the precise form of the measurement interaction [13]. In particular, if there is only a single quantum state under scrutiny—as was the case in the original Heisenberg uncertainty relation discussion [14]—or even an unknown state drawn from a fixed orthogonal set [15], then a measurement interaction can always be rigged for *any* observable so that, upon completion of the process, the quantum state is returned to its initial value [16]. It does not matter that the measurement outcome is random and unpredictable: If the discussion is limited to a single quantum state or an orthogonal set, then there need be no disturbance in the sense of a *necessary* wave-function change.

What appears to be needed is a situation where more than one quantum state from within a nonorthogonal set arises naturally into the considerations. Indeed, perhaps the first phenomenon to give a precise meaning to the idea that information-gathering measurements necessarily cause an accompanying disturbance is quantum cryptography [17,18]. There it is essential that the systems are known to be prepared in one or another quantum state drawn from some fixed *nonorthogonal* set [19–21]. These nonorthogonal states are used to encode a potentially secret cryptographic key to be shared between the sender and receiver. In this case, the information an eavesdropper seeks is not about some nonexistent hidden variable like x or p, but instead about which quantum state was actually prepared in each individual transmission. What is novel here is that the encoding of the proposed key into nonorthogonal states forces the information-gathering process to induce a disturbance to the overall

*Permanent address: Bell Laboratories, Lucent Technologies, Rm. 2C-420, 600-700 Mountain Ave., Murray Hill, NJ 07974.

set of states. That is, the presence of an active eavesdropper transforms the initial pure states into a set of mixed states or, at the very least, into a set of pure states with larger overlaps than before. This action ultimately results in a loss of predictability for the sender over the outcomes of the receiver's measurements and, so, is directly detectable by the receiver revealing some of those outcomes for the sender's inspection. In fact, there is a direct connection between the statistical information gained by an eavesdropper and the consequent disturbance she must induce to the quantum states in the process. As the information gathered increases, the necessary disturbance also increases in a precisely formalizable way [22–24].

Note the two ingredients that appear in this formulation. First, the information gathering or measurement is grounded with respect to one observer (in this case, the eavesdropper), while the disturbance is grounded with respect to another (here the sender). In particular, the disturbance is a disturbance to the sender's previous information—this is measured by his diminished ability to predict the outcomes of certain measurements the legitimate receiver might perform. No hint of any variable intrinsic to the system is made use of in this formulation. In itself, this is already a break from the common folklore of disturbance in measurement. As far as we can tell, all early literature on the subject refers the discussion of disturbance exclusively to the system and the invasive measuring device, not to the perspective of various observers [7].

The second ingredient is another break with folklore. One must consider at least two possible nonorthogonal preparations in order for the formulation to have any meaning. This is because the information gathering is not about some classically defined observable—i.e., about some unknown hidden variable or reality intrinsic to the system—but is instead about which of the unknown states the sender actually prepared. The lesson is this: Disregard the unknown preparation, and the random outcome of the quantum measurement is information about nothing. It is simply ''quantum noise'' with no connection to any preexisting variable.

How crucial is this second ingredient, i.e., that there be at least two nonorthogonal states within the set under consideration? We can start to readdress its necessity by making a slight shift in the account above. Divorcing the discussion from a cryptographic protocol, one might say that the eavesdropper's goal is not so much to uncover the identity of the unknown quantum state, but to sharpen her predictability over the receiver's measurement outcomes. In fact, she would like to do this at the same time as disturbing the sender's predictions as little as possible. Changing the language still further to the terminology of Ref. [12], the eavesdropper's actions serve to sharpen her information about the potential consequences of the receiver's further interventions upon the system. (Again, she would like to do this while minimally diminishing the sender's previous information about those same consequences.) In the cryptographic context, a by-product of this effort is that the eavesdropper ultimately comes to a more sound prediction of the secret key. From the present point of view, however, the importance of this change of language is that it leads to an almost Bayesian perspective on the information-disturbance problem [25].

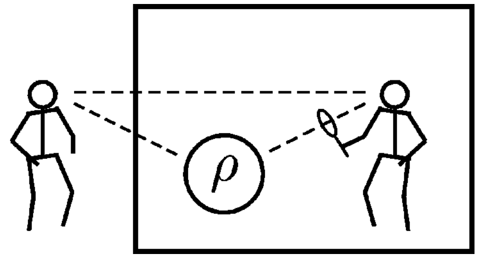

FIG. 1. Here two observers both ascribe a density matrix ρ to a quantum system. The observer inside the box (Alice) makes a measurement on the system without telling the result to the observer outside (Bob). Alice wishes to obtain as much knowledge about the system as she can, while causing as little disturbance to Bob's state of knowledge as possible.

Within Bayesian probability theory, one of the overarching themes is to identify the conditions under which a set of decision-making agents can come to a common belief or probability assignment for some specified random variable even though the agents' initial beliefs may differ [26]. One might similarly view the process of quantum eavesdropping. The sender and the eavesdropper start off initially with differing quantum state assignments for a single physical system. In this case it so happens that the sender can make sharper predictions than the eavesdropper about the outcomes of the receiver's measurements. The eavesdropper, not satisfied with the situation, performs a measurement on the system in an attempt to sharpen those predictions. In particular, there is an attempt to come into something of an agreement with the sender, but without revealing the outcomes of her measurements or, indeed, her very presence.

It is at this point that a distinct *property* of the quantum world makes itself known. The eavesdropper's attempt to surreptitiously come into alignment with the sender's predictability is always shunted away from its goal. This shunting of various observer's predictability (and perhaps only this shunting [27]) is the subtle manner in which the quantum world is sensitive to our experimental interventions.

This motivates finally the following problem, which is the subject of our paper. Suppose two players—let us call them Alice and Bob from this point on—come to agree about the way a quantum system will react to any measurement. In other words, by Gleason's theorem [28], suppose they start with an identical density operator assignment ρ for the system. The case we are interested in most is when ρ is a mixed state. Under what conditions can one player—Alice, say—surreptitiously increase her knowledge of the system without forcing the other player's knowledge to become less relevant (see Fig. 1)?

To move toward making this question precise, imagine that a third player will perform some measurement on the system in the future, but neither Alice nor Bob know which it will be. Depending upon which measurement is ultimately performed, Alice and Bob will have varying degrees of predictability for its outcomes. For instance, consider how their predictability fares with respect to various simple von Neumann measurements. If the measurement happens to be the eigenbasis of ρ, the Shannon entropy of the outcomes—which is a good measure of predictability [29]—will be the minimal value it can be [30]. This turns out to be the von Neumann entropy $S(\rho)=-\mathrm{tr}\,\rho\log\rho$. On the other hand, if the measurement happens to be a ''mutually unbiased'' basis [31] to the eigenbasis, then all measurement outcomes will be equally probable, and the outcome entropy will be $\log d$, where d is the dimension of the system's Hilbert space.

For the purpose at hand, we would like to capture in a single number something about how much Alice and Bob can predict of the unknown measurement. As a simple example, we might average the Shannon entropy of the measurement outcomes over the unique unitarily invariant measure (or ''uniform'' measure) on the space of von Neumann measurements [32,33]. This would represent how well Alice and Bob will fare on average with respect to a completely random von Neumann measurement. Or we might simply consider the entropy of the best case scenario, i.e., the von Neumann entropy of ρ as above. Without getting specific—all will be made precise later—we will generically call these kinds of measures *measures of purity*. The main intuition we want to capture is that when $\rho=|\psi\rangle\langle\psi|$ is a pure state, then Alice and Bob should generally have the most predictability over the third party's measurements. When ρ is the ''completely mixed state''—i.e., proportional to the identity operator, $\rho=(1/d)I$—they should have the least predictability.

The precise question we want to address is, can Alice secretly increase the purity of her quantum state assignment at the same time as leaving the other player's purity unscathed? If she cannot, then such a failure may hint at another interesting way to quantify a quantum-information–disturbance tradeoff. The hallmark of this formulation would be that it works even in a case when there is only a *single* initial quantum state (albeit a mixed state), while still capturing the shift in language we used to reformulate the quantum eavesdropping process.

Unfortunately, the answer is trivial if we leave the question posed in such a simplistic way. We need only suppose that Alice measures an eigenbasis $\Pi_b=|b\rangle\langle b|$ of ρ to negate the whole program. Upon finding some result b, Alice will collapse her description of the system from the mixed state ρ to the pure state [34],

$$\rho_b=\frac{1}{p_b}\Pi_b\rho\Pi_b\,, \tag{1}$$

where $p_b=\mathrm{tr}(\rho\Pi_b)$ is the probability of the particular outcome. The result is to make Alice's final purity for the system maximal, while as far as Bob is concerned the system's density operator will not be affected at all. This is because, with respect to Bob's state of knowledge, the quantum state evolves simply to a mixture of Alice's states, i.e.,

$$\rho\rightarrow\sum_b p_b\rho_b=\rho, \tag{2}$$

and so his purity and indeed his quantum state assignment remain the same.

The key to finding something interesting here is to ask what would happen in the case where there is a well-justified restriction to the class of measurements Alice can perform. For instance, suppose Alice has not yet reached the technologically advanced stage of being able to perform a truly perfect von Neumann measurement. Maybe she is using a Stern-Gerlach device to perform a spin measurement on an electron. Very commonly, the limitations of her laboratory will not allow her to place the particle detectors infinitely far behind the magnets so that the particle beams' overlap will be zero. Then, every now and then a spin will be registered down when it should have registered a spin up. To put this another way, instead of projecting ρ into the states Π_0 and Π_1 as Alice would like, the Stern-Gerlach device projects ρ according to a more general Lüder's rule for positive operator valued measures (POVM's) [35,36],

$$\rho\rightarrow\rho_b=\frac{1}{p_b}E_b^{1/2}\rho E_b^{1/2}, \tag{3}$$

where, in this case,

$$E_0=\kappa\Pi_0+(1-\kappa)\Pi_1, \tag{4}$$

$$E_1=(1-\kappa)\Pi_0+\kappa\Pi_1, \tag{5}$$

and $p_b=\mathrm{tr}(\rho E_b)$. Similarly, the description of the state change from Bob's perspective must be in accord with this, and so

$$\rho\rightarrow\tilde{\rho}=\sum_b p_b\rho_b\,. \tag{6}$$

When κ is a number strictly between 0 and 1, we will call this an instance of a *finite-strength* quantum measurement. (We use this suggestive terminology because we imagine that Alice can never really get to a perfect von Neumann measurement without the expenditure of an infinite amount of effort.) What can be said in a case like this?

Again, Alice will be able to generally increase the purity of her state without causing any decrease to Bob's purity. She does this, as before, simply by choosing Π_0 and Π_1 to be eigenprojectors of ρ. Then E_0 and E_1 commute with the initial density operator, and it is straightforward to check that $\tilde{\rho}=\rho$. However, we can now ask whether this is the strategy that brings the greatest benefit to Alice. Might it be the case that Alice can increase her purity even more on average if she chooses Π_0 and Π_1 to be noncommuting with ρ? Moreover if it does, what kind of effect will this have on Bob's description of the system? What we are imagining here, in the imagery of the Stern-Gerlach device is that though Alice may not be able to extend her laboratory so that her particle detector is infinitely far behind the magnets, she may be able to adjust the magnets' spatial orientation at will. Is this a freedom she should make use of?

Interestingly, it turns out that there is a tradeoff in the two final purities. Whenever ρ is nonpure (so that there is actually something to be ''learned'') and $0<\kappa<1$ (so that the measurement is of finite strength), Alice's final purity will be the greatest on average precisely when Bob's purity has decreased the most in turn. Moreover, varying through the class of measurements that lead from the least average final purity to the most (with respect to Alice), we find that Bob's purity goes down monotonically as Alice's goes up. As we will show, this is an example of a more general phenomenon where the measurement operators are not so restricted as in Eqs. (4) and (5): for a large class of finite-strength quantum measurements, a nontrivial tradeoff relation always exists.

The plan of the remainder of the paper is as follows. In Sec. II, we give a precise formulation of the problem in the widest setting, including definitions of various measures of purity and also a definition of the general notion of a finite strength quantum measurement (without feedback). In Sec. III, we work out an analytic form for the changes of purity for both Alice and Bob under the assumption of a particularly simple measure of purity *and* the restriction that Alice's quantum measurements have only two outcomes. We then explore the various regimes of the convex set of measurements, and exhibit the general information tradeoff relation where it exists. We close in Sec. IV with a few concluding remarks about the significance of this result. In Appendix A, we prove that any efficient measurement (POVM) will increase Alice's purity on average (for any measure of purity that is a convex function of the density operator's eigenvalues)—this result is essentially identical to one proven recently in Ref. [37] and builds upon the significant early work of Lindblad [38]. In Appendix B, for comparison with the main result here, we consider a variation of the problem where we vary over all measurements of a given finite strength instead of only those on the unitary orbits of a given fiducial measurement.

II. FORMULATION

Our problem concerns two agents, Alice and Bob, who initially ascribe a single density operator ρ to a quantum system in which they have some interest. The most important case for us is when ρ is a mixed state, i.e., $\mathrm{tr}\,\rho^2<1$. For generality in the formulation, let us assume that ρ is a density operator over a d-dimensional Hilbert space $\mathcal{H}_d$. Detailed considerations begin when Alice tries to surreptitiously increase her ''knowledge'' of the system—that is, to obtain a new density operator that is closer to being a pure state than her initial ascription. The only way she can do this is by performing a quantum measurement behind Bob's back. To be as generous as we can be without trivializing the problem, let us assume that Bob knows everything of Alice's *plan*, even her precise measurement interaction. The only information barred from Bob is the precise outcome of Alice's measurement.

The formalism for treating the most general kind of quantum measurement is that of the POVM [39]. In this formalism a measurement corresponds to a sequence of operators on $\mathcal{H}_d$—denoted by $\mathcal{E}=(E_b)_{b=1}^{\infty}$—with a *finite* number of nonvanishing E_b, such that each element of the sequence is a positive semidefinite operator, i.e.,

$$\langle\psi|E_b|\psi\rangle\geq 0 \;\; \forall|\psi\rangle, \tag{7}$$

and, together, the elements form a resolution of the identity:

$$\sum_b E_b=I. \tag{8}$$

The outcomes of the measurement are specified by the index b, and occur with probabilities $p_b=\mathrm{tr}\,\rho E_b$.

Upon finding an outcome b, the laws of quantum mechanics specify that Alice's state can evolve into any other density operator of the form [16]

$$\rho\rightarrow\rho_b=\frac{1}{p_b}\sum_i A_{bi}\rho A_{bi}^{\dagger}, \tag{9}$$

where

$$\sum_i A_{bi}^{\dagger}A_{bi}=E_b. \tag{10}$$

Since Bob knows nothing of Alice's outcome, as far as he is concerned the state of the quantum system will evolve according to

$$\rho\rightarrow\tilde{\rho}=\sum_b p_b\rho_b \tag{11}$$

$$=\sum_{b,i} A_{bi}\rho A_{bi}^{\dagger}. \tag{12}$$

Note that the decomposition of each E_b into the operators A_{bi} in Eqs. (9) and (10) depends crucially upon the interaction Alice chooses for carrying out the measurement $\mathcal{E}$. Whenever the range of the index i is restricted to a single value, we say that Alice's measurement is an *efficient* one [40].

Efficient quantum measurements (with respect to a given $\mathcal{E}$) correspond to holding on to as much information as possible in the measurement process. That is to say, such measurements do not break quantum coherence more than is necessary for the given POVM. In the subsequent development we will consider only efficient measurements for just this reason. Hence, in the language of equations, we will only consider conditional state changes of the form

$$\rho\rightarrow\rho_b=\frac{1}{p_b}A_b\rho A_b^{\dagger}, \tag{13}$$

where $A_b^{\dagger}A_b=E_b$.

By the polar decomposition theorem for operators [41], we can always write

$$A_b=U_bE_b^{1/2}, \tag{14}$$

where U_b is a unitary operator. This decomposition can be endowed with a physical meaning if one thinks of the measurement process as allowing for a sort of *feedback* to the quantum system. The raw measurement causes a ''collapse''

$$\rho\rightarrow\sigma_b=\frac{1}{p_b}E_b^{1/2}\rho E_b^{1/2} \tag{15}$$

in one's description of the system. But then, conditioned upon the outcome, one can think of the interaction as causing the system to unitarily evolve further to

$$\sigma_b \rightarrow \rho_b = U_b \sigma_b U_b^\dagger. \tag{16}$$

This split, of course, is a conceptual one: it may or may not correspond to the actual workings of the device carrying out the measurement $\mathcal{E}$. Nevertheless, it can be quite useful for classifying different kinds of measurement interaction.

Efficient measurements *without* feedback hold a special place in our considerations. These are measurement interactions for which $U_b = I$, so that Alice's state change is ultimately of the simple form:

$$\rho \rightarrow \rho_b = \frac{1}{p_b} E_b^{1/2} \rho E_b^{1/2}. \tag{17}$$

These hold a special place for us first and foremost because they correspond to the ''rawest'' kind of measurement interaction allowed for a given POVM. Therefore, they are worthy of study in their own right [36]. Second, however, there are other problems for which they correspond to the least perturbing implementation of a POVM. That is, if one contemplates performing the measurement on a system initially prepared in a completely random pure state, then the mean input-output fidelity will be the greatest if the measurement has no feedback [42,43]. Finally, it stands to reason that if we can delineate the tradeoff between information and disturbance for such a special case, we will be better prepared for understanding the more general one of an arbitrary efficient measurement. We will also be better prepared to understand the precise role of feedback for controlling quantum systems [44].

Our focus hereafter will be on efficient measurements without feedback. What is the *strength* of such a measurement? This issue is explored in Ref. [44], where a more refined notion of the concept is given a quantitative formulation. For the purposes here, we will only need the rawest of distinctions: finite vs infinite measurement strength. An efficient measurement $\mathcal{E}$ is said to be of finite strength as long as each nonvanishing E_b has support on the whole Hilbert space $\mathcal{H}_d$—that is, as long as

$$\text{rank } E_b = d \quad \text{for all } b \text{ such that } E_b \neq 0. \tag{18}$$

A measurement is of infinite strength any time one of the nonvanishing E_b's has a rank strictly less than d.

The utility of this notion comes about from noting that the set of all POVM's is a convex set. This follows from the fact that one can invent a notion of convex addition operation for POVM's: simply take [45]

$$p\mathcal{E} + (1-p)\mathcal{F} \equiv [pE_b + (1-p)F_b]_{b=1}^{\infty}. \tag{19}$$

By a similar consideration, it is also true that the set of all POVM's with a fixed number n of nonvanishing elements E_b is a convex set. Thinking of this set as embedded in a space of length-n sequences of all Hermitian operators, one has that the boundary of such a set is given by precisely what we are calling the infinite strength measurements (with n outcomes). The finite strength measurements lie strictly within the interior of the set. Making this identification in terminology is an attempt to capture the idea that an experimenter would need to expend an infinite amount of effort to work his way out to the boundary. This is because, if he could get all the way to the edge, there would be some preparations of the system for which he could predict with *absolute* certainty that some outcomes of the measurement would not occur. That strikes us as an insurmountable task. As technology advances, we can imagine experimentalists getting ever closer to the boundary, but never quite reaching it.

Let us now start applying these distinctions of measurement to the problem at hand—namely, to that of an Alice trying to surreptitiously increase her ''knowledge'' of a system while affecting Bob's knowledge of it as little as possible. How shall we quantify knowledge in this context? There are at least three canonical ways.

The first has to do with the von Neumann entropy of a density operator ρ,

$$S(\rho) = -\text{tr}\, \rho \log \rho = -\sum_{k=1}^{d} \lambda_k \log \lambda_k, \tag{20}$$

where the λ_k signify the eigenvalues of ρ. [We evaluate all logarithms in base 2, so that information is measured in bits, rather than nats or hartleys [46]. Also, we use the convention that $\lambda \log \lambda = 0$ whenever $\lambda = 0$, so that $S(\rho)$ is always well defined.]

The intuitive meaning of the von Neumann entropy can be found by first thinking about the Shannon entropy. Consider any von Neumann measurement $\mathcal{P}$ consisting of d one-dimensional orthogonal projectors Π_i. The Shannon entropy for the outcomes of this measurement is given by

$$H(\mathcal{P}) = -\sum_{i=1}^{d} (\text{tr}\, \rho \Pi_i) \log(\text{tr}\, \rho \Pi_i). \tag{21}$$

This number is bounded between 0 and $\log d$, and there are several reasons to think of it as a good measure of *unpredictability* over the outcomes of a measurement $\mathcal{P}$. Perhaps the most important of these is that it quantifies the number of *yes-no* questions one can expect to ask per measurement, if one's only means to ascertain the measurement outcome is from a colleague who knows the actual result [29]. Under this quantification, the lower the Shannon entropy the more predictable a measurement's outcomes.

A natural question to ask is the following: With respect to a given density operator ρ, which measurement $\mathcal{P}$ will give the most predictability over its outcomes? As it turns out, the answer is any $\mathcal{P}$ that forms a set of eigenprojectors for ρ [30]. When this is the case, the Shannon entropy of the measurement outcomes reduces simply to the von Neumann entropy of the density operator. The von Neumann entropy, then, signifies the amount of unpredictability one achieves by way of a standard measurement in a best case scenario. Indeed, true to one's intuition, one has the most knowledge by this account when ρ is a pure state—for then $S(\rho) = 0$. Alternatively, one has the least knowledge when ρ is proportional to the identity operator—for then any measurement $\mathcal{P}$ will have outcomes that are all equally likely.

The best case scenario for predictability, however, is a very limited case, and not so very informative about the density operator as a whole. Since the density operator contains, in principle, all that can be said about every possible measurement [28], it seems a shame to throw away the vast part of that information in our considerations.

This issue leads to our next quantification of ''knowledge'' of a quantum system. For this, we again rely on the Shannon information as our basic notion of predictability. The difference is that we evaluate it with respect to a ''typical'' measurement rather than the best possible one. However with this, a new question arises: Typical with respect to what? The notion of typical is only defined with respect to a given *measure* on the set of measurements.

Luckily, there is a fairly canonical answer. There is a unique measure $d\Omega_\Pi$ on the space of one-dimensional projectors that is invariant with respect to all unitary operations. This in turn naturally induces a canonical measure $d\Omega_{\mathcal{P}}$ on the space of von Neumann measurements $\mathcal{P}$ [32,33]. Using this measure gives rise to the quantity

$$\overline{H}(\rho)=\int H(\Pi)d\Omega_{\mathcal{P}} \tag{22}$$

$$=-d\int(\mathrm{tr}\,\rho\Pi)\log(\mathrm{tr}\,\rho\Pi)d\Omega_\Pi, \tag{23}$$

which is intimately connected to the so-called quantum ''subentropy'' of Ref. [47]. Interestingly, this mean entropy can be evaluated explicitly in terms of the eigenvalues of ρ and takes on the expression

$$\overline{H}(\rho)=\frac{1}{\ln 2}\left(\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{d}\right)+Q(\rho), \tag{24}$$

where the subentropy $Q(\rho)$ is defined by

$$Q(\rho)=-\sum_{k=1}^{d}\left(\prod_{i\neq k}\frac{\lambda_k}{\lambda_k-\lambda_i}\right)\lambda_k\log\lambda_k. \tag{25}$$

In the case where ρ has degenerate eigenvalues, $\lambda_l=\lambda_m$ for $l\neq m$, one need only reset them to $\lambda_l+\epsilon$ and $\lambda_m-\epsilon$ and consider the limit as $\epsilon\to 0$. The limit is convergent, and hence $Q(\rho)$ is finite for all ρ. With this, one can also see that for a pure state ρ, $Q(\rho)$ vanishes. Furthermore, since $\overline{H}(\rho)$ is bounded above by $\log d$, we know that

$$0\leqslant Q(\rho)\leqslant\log d-\frac{1}{\ln 2}\left(\frac{1}{2}+\cdots+\frac{1}{d}\right)\leqslant\frac{1-\gamma}{\ln 2}, \tag{26}$$

where γ is Euler's constant. This means that for any ρ, $Q(\rho)$ never exceeds 0.60995 bits.

The interpretation of this result is the following. Even when one has the maximal knowledge about a system one can have under the laws of quantum mechanics—i.e., when one has a pure state—one can predict almost nothing about the outcome of a typical measurement [48]. In the limit of large d, the outcome entropy for a typical measurement is just a little over a half bit away from its maximal value. Having a mixed state for a system reduces one's predictability even further, but indeed not by that much: The small deviation is captured by the function in Eq. (25), which becomes a quantification of ''knowledge'' in its own right.

The two quantifications of knowledge about a quantum system given by Eqs. (20) and (25) are without doubt two of the most well-motivated such quantities. However, because of their particular mathematical structures (involving logarithms and ratios of eigenvalues, etc.), they are often difficult to work with. It is therefore useful to consider quantities $F(\rho)$ that may not have the strictest of interpretations in terms of ''knowledge'' or ''information,'' but nevertheless carry some of the properties essential to the explorations we would like to make. The two properties that appear to be the most important for us is that a function F from density operators to real numbers be (1) unitarily invariant, so that it only depends upon the eigenvalues of the density operator; and (2) concave in its argument. That is, one should have

$$F[p\rho_0+(1-p)\rho_1]\geqslant pF(\rho_0)+(1-p)F(\rho_1) \tag{27}$$

for each pair of density operators ρ_0 and ρ_1, and each real number p in the range $[0,1]$.

A common way of simplifying problems to do with the Shannon entropy is to consider instead a function that is merely quadratic in the probabilities [49,50]. In quantum-mechanical terms, this translates to a function we shall call the *impurity* of a quantum state:

$$P(\rho)=1-\mathrm{tr}(\rho^2)=1-\sum_{k=1}^{d}\lambda_k^2. \tag{28}$$

This function, of course, has our two desired properties [30]. Moreover, it attains its minimum value of 0 when ρ is a pure state (just as S and Q do), and it attains its maximum value of $(d-1)/d$ when ρ is the completely mixed state.

What makes unitarily invariant functions like the $F(\rho)$ in Eq. (27) special is that one can prove an interesting theorem for them in the measurement context. Consider any efficient measurement of a POVM, $\mathcal{E}=\{E_b\}$. Upon finding an outcome b, the observer will update his quantum state for the system from the original ρ to some ρ_b of the form in Eq. (13). What does this say about his expected change of knowledge? Well, one can prove that, whatever F is,

$$F(\rho)\geqslant\sum_b p_bF(\rho_b). \tag{29}$$

In particular, it follows that

$$S(\rho)\geqslant\sum_b p_bS(\rho_b), \tag{30}$$

$$Q(\rho)\geqslant\sum_b p_bQ(\rho_b), \tag{31}$$

$$P(\rho)\geq\sum_b p_b P(\rho_b). \tag{32}$$

These statements—and in fact a stronger statement to do with a majorization relation between the eigenvalues of ρ and those of the ρ_b—will be proven in Appendix A. [See Nielsen [37] for an earlier proof of this result and also Lindblad [38] for a proof of Eq. (30) specialized to von Neumann measurements.]

The fact that Eq. (29) holds for all concave functions F expresses what is meant by the phrase ‘‘the observer *learns* something from a quantum measurement’’ [51]. Note in particular that this need not necessarily be the case that the purity, etc., be nondecreasing in any *individual* trial of a measurement. A simple counterexample suffices for illustration. Take

$$\rho=\frac{1}{3}\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}, \tag{33}$$

and consider a two-outcome efficient measurement without feedback $\mathcal{E}=(E,I-E)$ where

$$E=\frac{1}{3}\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}. \tag{34}$$

Note that if outcome E occurs, the updated density operator for the system will be the completely mixed state

$$\rho_E=\frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \tag{35}$$

which is certainly less pure than the initial state. Thus one can only expect one's ‘‘knowledge’’ to increase *on average* during a measurement.

Going back to our target scenario with Alice and Bob, one can see that this result insures that Alice comes away on average with more information than she started with. Moreover, this holds independently of the particular way in which we choose to quantify her ‘‘information.’’ To make some notation, this means that the quantities

$$\Delta_{\rm in}^F\equiv F(\rho)-\sum_b p_b F(\rho_b) \tag{36}$$

will all be nonnegative for any efficient measurement. The subscript on $\Delta_{\rm in}^F$ denotes that this refers to the change of knowledge from the ‘‘inside’’ point of view of the measurer.

An almost dual result is that from Bob's point of view—the outside point of view—whenever $\mathcal{E}$ is not only an efficient measurement, but also a measurement *without feedback*, his information can never increase from Alice's actions. That is to say, using notation from Eq. (11), the quantity

$$\Delta_{\rm out}^F\equiv F(\tilde{\rho})-F(\rho) \tag{37}$$

is nonnegative for all concave unitarily invariant functions F [52]. Again, the subscript in $\Delta_{\rm out}^F$ makes explicit that we are referring to a change of knowledge from the outside point of view. (The interested reader can find a proof that $\Delta_{\rm out}^F\geq 0$ in Ref. [52].)

We must emphasize that this result is *almost* dual to Eq. (29), for it certainly depends upon the assumption that the measurement is without feedback. Let us show this by way of a quick counterexample. Take $\mathcal{E}$ to be a complete set of orthogonal projectors $E_b=|b\rangle\langle b|$, $b=1,\ldots,d$. One possible measurement with feedback that is consistent with this POVM is given by taking $A_b=|\psi\rangle\langle b|$ for some fixed unit vector $|\psi\rangle$. Clearly $A_b^\dagger A_b=E_b$ as required. However,

$$\tilde{\rho}=\sum_b A_b\rho A_b^\dagger=|\psi\rangle\langle\psi|, \tag{38}$$

completely independently of what the initial state ρ is. So it can certainly be the case that $F(\tilde{\rho})\leq F(\rho)$ if one allows feedback into the picture.

The conclusion to draw is that we are right on track in considering the quantities $\Delta_{\rm in}^F$ and $\Delta_{\rm out}^F$ in the context of measurements without feedback: in a sense, they are compensatory of each other. What we would like to do now is sharpen this idea. Just because Alice's knowledge of the system can only increase through her measurements and Bob's can only decrease, it does not follow that there is necessarily a monotonic relation between these adjustments.

Here is how we will tackle the problem explicitly. As has been the case since the beginning, we imagine the initial state of knowledge for Alice and Bob to be fixed to some density operator ρ. Now, however, we introduce a *fiducial* quantum measurement $\mathcal{M}=(M_b)$ that will also be fixed throughout our considerations. The freedom we give Alice is that she may perform any measurement without feedback that is unitarily equivalent to $\mathcal{M}$. That is to say, we shall consider measurement operators for Alice that are necessarily of the form

$$E_b=UM_bU^\dagger, \tag{39}$$

where U is any unitary operation. Each different U defines a consequent change in both Alice and Bob's total information which we denote by $\Delta_{\rm in}^F(U)$ and $\Delta_{\rm out}^F(U)$, respectively. (This notation makes no reference to ρ and $\mathcal{M}$, because they are fixed background information for the problem.) What we would like to know is the following: Under what conditions is there a nontrivial monotone relation between $\Delta_{\rm in}^F(U)$ and $\Delta_{\rm out}^F(U)$ as we vary U? In the cases where such a monotone relation exists, that will be the tradeoff we have been seeking.

This completes the formulation of our problem. Unfortunately, as opposed to the formulation, we have not settled the issue of a tradeoff relation in complete generality. Study of the two-dimensional Hilbert-space case, however, already turns out to be of significant interest. In Sec. III, we report a careful study of the case where $d=2$ and $\mathcal{M}$ contains two outcome operators M_0 and M_1. Even in this restricted class, there is a large regime of measurements with a nontrivial information tradeoff relation.

III. 2D TWO-OUTCOME PROBLEM

In this section, we assume explicitly that $d=2$, so that Alice and Bob's information is about a single qubit. The canonical measurement $\mathcal{M}$ that sets Alice's standard is taken to consist of only two elements M_0 and M_1, but is otherwise completely general. Alice now has the freedom to choose any unitary operation U, and consequently perform any measurement $\mathcal{E}$ consisting of elements $E_0=UM_0U^\dagger$ and $E_1=UM_1U^\dagger$. The question we should like to address is how $\Delta_{\rm in}^F(U)$ and $\Delta_{\rm out}^F(U)$ change with respect to each other as a function of U.

Note that because there are only two outcomes to the measurement, E_0 and E_1 must commute. There is, therefore, only one diagonalizing basis required in specifying this measurement. Let us relabel the measurement to make this more explicit: We shall simply denote the two outcomes by E and $I-E$. With our previous definitions, this measurement is of finite strength when neither E nor $I-E$ is a rank-1 operator.

We have performed extensive numerical work that shows the following when ρ is impure and $\mathcal{E}$ is of finite strength. For the three concave functions $S(\rho)$, $Q(\rho)$, and $P(\rho)$ considered in Sec. II, there are significant regions in POVM space where $\Delta_{\rm in}^F(U)$ achieves its maximum value precisely when $\Delta_{\rm out}^F(U)$ is nonminimal. That is to say, Alice cannot learn the most unless she also disturbs Bob's information in the process. In this situation, the optimal measurement operator E does not commute with ρ. Alternatively, when E commutes with ρ, the difference $\Delta_{\rm out}^F(U)$ achieves its minimum value, namely, 0—so that Bob's information is not disturbed at all—but then $\Delta_{\rm in}^F(U)$ achieves its minimum value too—so that Alice has learned the least amount possible. In general, the functional relationship $\Delta_{\rm out}^F(\Delta_{\rm in}^F)$ is a monotonic one as $\Delta_{\rm in}^F$ ranges from its minimum to its maximum value. In those regions of POVM space where there is no nontrivial tradeoff relation, the curve for $\Delta_{\rm out}^F(\Delta_{\rm in}^F)$ is simply flat.

What we shall do herein is focus on quantifying the tradeoff explicitly for the case in which ''knowledge'' is identified with the impurity function $P(\rho)$ of Eq. (28). In this case, all calculations can be done analytically and one can obtain a feel for the exact form of things. [In the other cases of $F=S$ or $F=Q$, things are not terribly worse, but because the binary Shannon entropy function cannot be inverted analytically, there is no way to get an analytic expression for the function $\Delta_{\rm out}^F(\Delta_{\rm in}^F)$.] With this restriction, we will hereafter drop the superscript F from our notation and write simply $\Delta_{\rm out}$ and $\Delta_{\rm in}$ for the ''information'' changes we are considering.

Let us start the calculations straight away. From the inside point of view of Alice, the two possible state changes are of the forms

$$\rho\to\rho_E=\frac{1}{\mathrm{tr}\,\rho E}\sqrt{E}\rho\sqrt{E} \tag{40}$$

and

$$\rho\to\rho_{\neg E}=\frac{1}{1-\mathrm{tr}\,\rho E}\sqrt{I-E}\rho\sqrt{I-E}. \tag{41}$$

From the outside point of view of Bob, it is simply

$$\rho\to\tilde{\rho}=\sqrt{E}\rho\sqrt{E}+\sqrt{I-E}\rho\sqrt{I-E}. \tag{42}$$

Keeping in mind that $\sqrt{E}$ and $\sqrt{I-E}$ commute, a little algebra yields that

$$\Delta_{\rm out}=\mathrm{tr}\,\rho^2-\mathrm{tr}\,\tilde{\rho}^2 \tag{43}$$

$$=2\{\mathrm{tr}\,\rho^2E-\mathrm{tr}\,\rho E\rho E-\mathrm{tr}[\rho\sqrt{E(I-E)}\rho\sqrt{E(I-E)}]\}. \tag{44}$$

Similarly,

$$\Delta_{\rm in}=\mathrm{tr}\,\rho E\;\mathrm{tr}\,\rho_E^2+\mathrm{tr}\,\rho(I-E)\;\mathrm{tr}\,\rho_{\neg E}^2-\mathrm{tr}\,\rho^2 \tag{45}$$

$$=\frac{1}{\mathrm{tr}\,\rho E(1-\mathrm{tr}\,\rho E)}[\mathrm{tr}\,\rho E\rho E+\mathrm{tr}\,\rho^2\,\mathrm{tr}\,\rho E-2\,\mathrm{tr}\,\rho E\,\mathrm{tr}\,\rho^2E]-\mathrm{tr}\,\rho^2 \tag{46}$$

$$=\frac{1}{\mathrm{tr}\,\rho E(1-\mathrm{tr}\,\rho E)}[\mathrm{tr}\,\rho E\rho E-2\,\mathrm{tr}\,\rho E\,\mathrm{tr}\,\rho^2E+\mathrm{tr}\,\rho^2(\mathrm{tr}\,\rho E)^2]. \tag{47}$$

Note immediately that if E and ρ commute, then $\Delta_{\rm out}$ vanishes as one would expect.

Since we are dealing with a two-dimensional Hilbert space, it is most convenient at this point to switch to a kind of Bloch-sphere notation for all operators. Then we may write

$$\rho=\tfrac{1}{2}(I+\vec{a}\cdot\vec{\sigma}), \tag{48}$$

where $\vec{a}=(a_x,a_y,a_z)$ is some vector of real numbers with modulus $a\leqslant 1$ and $\vec{\sigma}$ is the vector of Pauli operators. Similarly, if $\alpha=\mathrm{tr}\,E$, then the operator

$$B=\frac{1}{\alpha}E \tag{49}$$

is a density operator, and we may write

$$B=\tfrac{1}{2}(I+\vec{b}\cdot\vec{\sigma}), \tag{50}$$

where $\vec{b}$ also has a length b no greater than unity. In this notation, E and ρ commute if and only if $\vec{b}$ and $\vec{a}$ lie within the same ray.

Since $0\leqslant E\leqslant I$, we must have $0\leqslant\alpha\leqslant 2$. Moreover, we must insure that the larger eigenvalue of E is no greater than unity. Using the fact that the eigenvalues of E in Bloch-sphere notation are given by $\frac{1}{2}\alpha(1\pm b)$, it follows that we must require

$$\alpha\leqslant\frac{2}{1+b}. \tag{51}$$

One can see $\mathcal{E}$ becomes an infinite strength measurement whenever $b=1$ and α is any value, or whenever $b<1$ but $\alpha=2/(1+b)$. The parameter α to some extent captures the amount of symmetry between the two measurement operators E and $I-E$. It is therefore natural to call the case where $\alpha=1$ the *symmetric case*.

With the notations of Eqs. (49) and (50), it becomes a tractable task to calculate the various operators in Eqs. (44) and (47). Using the law of multiplication for Pauli matrices, i.e.,

$$(\vec{m}\cdot\vec{\sigma})(\vec{n}\cdot\vec{\sigma})=(\vec{m}\cdot\vec{n})I+i\vec{\sigma}\cdot(\vec{m}\times\vec{n}), \tag{52}$$

one finds fairly easily that

$$\mathrm{tr}\,\rho^2=\frac{1}{2}(1+a^2), \tag{53}$$

$$\mathrm{tr}\,\rho E=\frac{\alpha}{2}(1+abz), \tag{54}$$

$$\mathrm{tr}\,\rho^2 E=\frac{\alpha}{4}(1+a^2+2abz), \tag{55}$$

$$\mathrm{tr}\,\rho E\rho E=\frac{\alpha^2}{8}[1+a^2+b^2+a^2b^2(2z^2-1)+4abz], \tag{56}$$

where $z=\cos\theta$, and θ is the angle between the vectors $\vec{a}$ and $\vec{b}$.

The only really daunting term that we must calculate is the quantity

$$\mathrm{tr}[\rho\sqrt{E(I-E)}\rho\sqrt{E(I-E)}]. \tag{57}$$

To make some headway, let

$$G\equiv E(I-E)=g_0I+\vec{g}\cdot\vec{\sigma}, \tag{58}$$

where

$$g_0=\tfrac{1}{4}\alpha(2-\alpha-\alpha b^2), \tag{59}$$

$$\vec{g}=\tfrac{1}{2}\alpha(1-\alpha)\vec{b}. \tag{60}$$

We need to find an r_0 and $\vec{r}$ such that

$$\sqrt{G}=r_0I+\vec{r}\cdot\sigma. \tag{61}$$

The method for this is simple: We just need calculate $G=\sqrt{G}\sqrt{G}$ and set the resultant equal to Eq. (58). Carrying this procedure to its conclusion, we arrive at the following identifications:

$$r_0^2=\frac{\alpha}{8}\{2-\alpha-\alpha b^2+\sqrt{(1-b^2)[4-4\alpha+(1-b^2)\alpha^2]}\} \tag{62}$$

$$\vec{r}=\frac{1}{4r_0}\alpha(1-\alpha)\vec{b}. \tag{63}$$

With this, we can finally calculate

$$\mathrm{tr}\,\sqrt{G}\rho\sqrt{G}\rho=\tfrac{1}{2}[1+a^2+c^2+2(\vec{a}\cdot\vec{c})^2-a^2c^2+4\vec{a}\cdot\vec{c}], \tag{64}$$

where the vector $\vec{c}$ and its magnitude c are defined by

$$\vec{c}=\frac{\vec{r}}{r_0}. \tag{65}$$

Putting all these ingredients together, we finally arrive at our sought-after expressions:

$$\Delta_{\mathrm{in}}=\frac{\alpha b^2(1-a^2)(1-a^2z^2)}{2(1+abz)(2-\alpha-\alpha abz)} \tag{66}$$

and

$$\Delta_{\mathrm{out}}=\frac{1}{2}\left(\frac{\alpha ab}{2r_0}\right)^2[(1-\alpha)^2+4r_0^2](1-z^2). \tag{67}$$

These two equations contain everything needed for a complete analysis of the information tradeoff question. Let us first see how this plays out for the simple case described in Eqs. (4) and (5) of Sec. I.

A. Symmetric case

In this case the measurement operators M_0 and M_1 take the form

$$M_0=\kappa\Pi_0+(1-\kappa)\Pi_1, \tag{68}$$

$$M_1=(1-\kappa)\Pi_0+\kappa\Pi_1, \tag{69}$$

where $0<\kappa<1$, and Π_0 and Π_1 are the projectors onto some orthonormal basis. Measurement operators of this form come up quite naturally in the theory of continuous quantum measurements [44]. In our Bloch sphere notation of Eqs. (49) and (50), this case corresponds to taking $\alpha=1$ and $b=2\kappa-1$.

Plugging $\alpha=1$ into Eqs. (66) and (67), we find the significantly simpler expressions

$$\Delta_{\mathrm{in}}=\frac{1}{2}b^2(1-a^2)\frac{1-a^2z^2}{1-a^2b^2z^2} \tag{70}$$

and

$$\Delta_{\mathrm{out}}=\frac{1}{2}b^2a^2(1-z^2). \tag{71}$$

Clearly, Δ_{out} is minimized when $z=1$ or -1 (so that E commutes with ρ) as we have noted before. Moreover, Δ_{out} is maximized when $z=0$—that is to say, when the operator E is diagonal in a basis complementary or mutually unbiased to the diagonal of ρ. On the other hand, since $b\leqslant 1$, Δ_{in} is a strictly decreasing function in z^2. This gives Δ_{in} the same qualitative behavior as Δ_{out} and ultimately leads precisely to our tradeoff relation: Eliminating z^2 from Eqs. (70) and (71), we obtain

$$\Delta_{\text{out}}=\frac{2(1-a^2b^2)\Delta_{\text{in}}-b^2(1-a^2)^2}{2(1-a^2-2\Delta_{\text{in}})}. \tag{72}$$

This example is something of an extreme for the phenomena we have been hoping for. As long as the fiducial measurement $\mathcal{M}$ is of finite strength (i.e., $b\neq 1$), Eq. (72) traces out a nontrivial monotone curve as we go from $\Delta_{\text{in}}^{\min}$ to $\Delta_{\text{in}}^{\max}$. But more than this, Δ_{in} is maximized at precisely the same value of z for which Δ_{out} is also maximized. In common language, this means that if Alice wishes to gather the most information, she must reciprocally cause Bob to lose the most information that her class of measurements will allow. The only means for Alice to lessen the impact of this effect is to develop her technology, so that the limit $b\rightarrow 1$ can be approached asymptotically.

This behavior, at first sight, appears to be quite deep. It helps lend credence to the idea that measurements without feedback are always somewhat destructive by their nature—that is, as long as one's aim is to increase one's information as much as possible under the constraint of having less than ''infinitely powerful'' measurement devices.

Interestingly, however, this type of behavior is not completely generic. There are some fiducial measurements $\mathcal{M}$ of finite strength for which the tradeoff effect disappears. To see this, we must turn back to our base equations (66) and (67).

B. General case

Let us now assume strictly that none of the variables a, b, or α happen to equal unity. Then, as in the symmetric case, the quantity Δ_{out} is clearly minimized when $z^2=1$. Similarly, the disturbance to Bob's knowledge is largest when $z=0$, so that E is diagonal in a basis mutually unbiased with respect to the diagonal of ρ.

The analysis of the general Δ_{in} is significantly more difficult. One can show that the quantity is minimized at $z^2=1$, but whether that occurs at $z=1$ or $z=-1$ now depends upon the size of α. The way to see this is by checking that Δ_{in} is concave as a function of z: The calculation is tedious, but it can be done analytically. The point where the curve changes from a positive slope to a negative slope, i.e., where the function attains its maximum, is given by

$$z=z_0=\frac{1}{\alpha(1-\alpha)ab}[4r_0^2-\alpha(2-\alpha-\alpha b^2)]. \tag{73}$$

This expression is quite revealing. For a fixed value of $b\neq 0$, one can check for those values of α that force $z_0=1$ or $z_0=-1$. These are

$$\alpha|_{z_0=1}=\frac{b(1+a^2)+2a}{b(1+a^2)+a(1+b^2)} \tag{74}$$

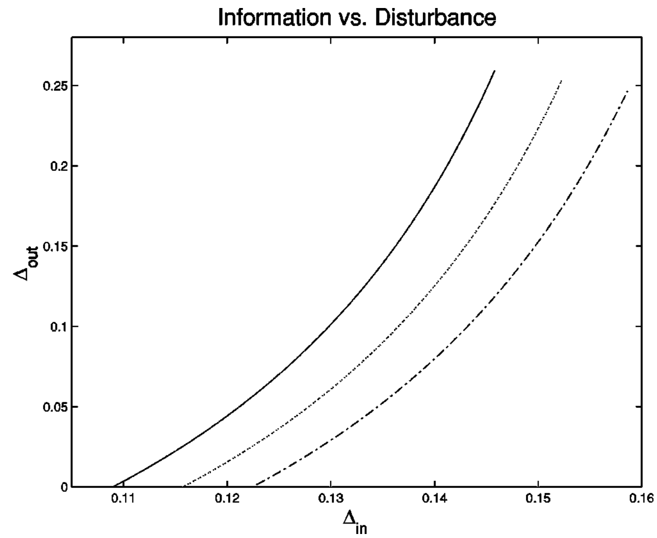

FIG. 2. The tradeoff between information Δ_{in} and disturbance Δ_{out} is plotted here for $\alpha=1$, $b=0.9$, and three values of a. Solid line: $a=0.8$; dotted line: $a=0.79$; dot-dashed line: $a=0.78$.

and

$$\alpha|_{z_0=-1}=\frac{b(1+a^2)-2a}{b(1+a^2)-a(1+b^2)}. \tag{75}$$

This means that for α in the ranges

$$0\leqslant\alpha\leqslant\max\left\{0,\frac{b(1+a^2)-2a}{b(1+a^2)-a(1+b^2)}\right\} \tag{76}$$

and

$$\frac{b(1+a^2)+2a}{b(1+a^2)+a(1+b^2)}\leqslant\alpha\leqslant\frac{2}{1+b} \tag{77}$$

Δ_{in} will always be maximized by choosing $z=1$ or $z=-1$. However, for α outside of either of those ranges, there will always be a nontrivial tradeoff relation: When Alice's information gain Δ_{in} is maximized, Bob's information loss Δ_{out} will be strictly greater than its minimal value.

The general tradeoff relation, when it exists, is found simply enough by eliminating the variable z from the simultaneous equations (66) and (67). (Two examples of the tradeoff relation are given in Figs. 2 and 3.) This time—in contrast to what we did in Eq. (72), however—we leave finding the explicit expression as an exercise for the reader: Seeing it explicitly adds little to the analysis already given.

IV. DISCUSSION

Our conclusion is straightforward: There are regions in the space of finite-strength efficient measurements without feedback for which a nontrivial information tradeoff relation exists as one unitarily varies around any given fiducial measurement $\mathcal{M}$. In a way, it is a shame that we could not make a more unqualified assertion—for instance, that a nontrivial tradeoff relation held for *all* finite-strength quantum mea-

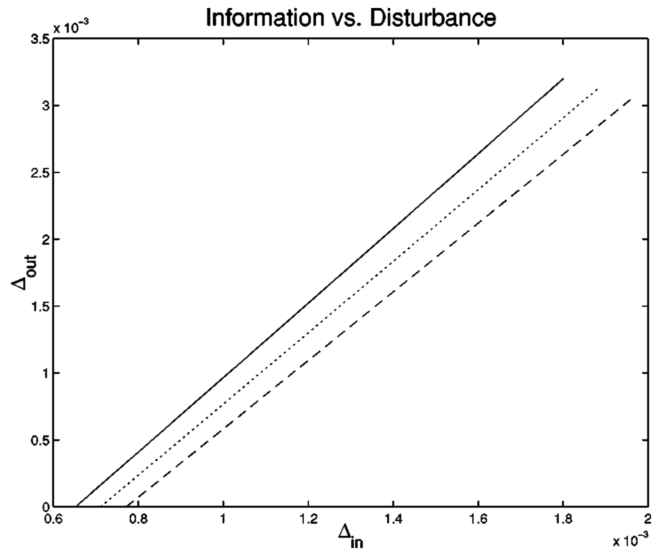

FIG. 3. The tradeoff between information $\Delta_{\rm in}$ and disturbance $\Delta_{\rm out}$ is plotted here for $\alpha=1$, $b=0.1$ and three values of a. Solid line: $a=0.8$; dotted line: $a=0.79$; dot-dashed line: $a=0.78$.

surements without feedback. Indeed the hope that such would be the case was a large part of the motivation for this work.

The question now arises as to the significance of the rather complicated regions defined by Eqs. (76) and (77). What trenchant physical property is implied of a measurement $\mathcal{M}$ that sits in the information-disturbance region of a given density operator ρ?

A toy idea is that the key distinction lies not in finite versus infinite measurement strength, but in whether the measurement sits above or below a certain finite-strength threshold. That is to say, in carrying out the program of this paper, we would imagine not only varying over unitary orbits for defining a tradeoff relation, but rather over any region of POVM space so long as a certain constraint on the measurement strength is obeyed. Unfortunately, if this is going to be the case, it is going to require some thinking more subtle than we have carried out so far. This is because for at least one natural definition of measurement strength we again find no nontrivial tradeoff relation. The failure of this program is described in Appendix B. But the question remains. In general, this paper forms part of a larger effort to fully delimit the information-disturbance tradeoff properties of quantum mechanics.

ACKNOWLEDGMENTS

We thank Tanmoy Bhattacharrya, Salman Habib, Alexander Holevo, Goran Lindblad, Ben Schumacher, and Howard Wiseman for helpful discussions.

APPENDIX A: EFFICIENT MEASUREMENTS INCREASE ALICE'S INFORMATION

In this appendix, we prove that for any efficient quantum measurement, an observer aware of the outcomes will on average increase his ''knowledge'' of the measured quantum system. More precisely, when a measurement causes the observer to update his density operator from ρ to ρ_b—as in Eq. (13)—it holds for any concave unitarily invariant function F that

$$F(\rho)\geq\sum_b p_b F(\rho_b). \tag{A1}$$

Along the way, and as something of an aside, we will also prove a stronger result that deals directly with relations between the eigenvalues of ρ and all the ρ_b. This result is most conveniently couched in terms of the mathematical theory of majorization [53], and will require some notation for its statement.

Let us define $\vec{\lambda}(O)$ to be the vector of eigenvalues of a Hermitian operator O on $\mathcal{H}_d$, with the components arranged in terms of decreasing magnitude. That is to say, let the numbers $\lambda_i(O)$ obey the ordering

$$\lambda_1(O)\geq\lambda_2(O)\geq\cdots\geq\lambda_d(O). \tag{A2}$$

We say that a vector $\vec{\lambda}(O)$ is *majorized* by a vector $\vec{\lambda}(\mathcal{N})$, and write

$$\vec{\lambda}(O)\prec\vec{\lambda}(\mathcal{N}) \tag{A3}$$

when

$$\sum_{i=1}^{k}\lambda_i(O)\leq\sum_{i=1}^{k}\lambda_i(\mathcal{N}) \tag{A4}$$

for all $k=1,2,\ldots,d$, and

$$\sum_{i=1}^{d}\lambda_i(O)=\sum_{i=1}^{d}\lambda_i(\mathcal{N}). \tag{A5}$$

One can also say that a Hermitian operator O is *majorized* by a Hermitian operator $\mathcal{N}$, and write $O\prec\mathcal{N}$, when $\vec{\lambda}(O)\prec\vec{\lambda}(\mathcal{N})$, but we will not have any need for that terminology in this development.

Our main result is this:

$$\vec{\lambda}(\rho)\prec\sum_b p_b\vec{\lambda}(\rho_b). \tag{A6}$$

(As pointed out above, this result has also been obtained recently in Ref. [37].) The proof of this statement is not too difficult if we rely on some results from the mathematical literature [53], and a method of thought promoted by Schumacher on several occasions to great result—see Refs. [54,55], to name only a few.

The trick of Schumacher is this. Whenever we have a quantum system Q and we say that it is in a (mixed) state ρ, there is nothing to prevent us from thinking that the situation has come about because Q is part of a larger system RQ, which we happen to describe via some pure state $|\psi^{RQ}\rangle$. The state ρ then is just a partial trace over the larger pure state:

$$\rho = \mathrm{tr}_R |\psi^{RQ}\rangle\langle\psi^{RQ}|. \tag{A7}$$

There are times when such a conception can be quite useful for simplifying the mathematics of a problem. The problem at hand is one of them.

Let us now describe the measurement process on a system Q from such a point of view. It will be useful to make explicit precisely which system we are referring to at any given time: therefore, we shall add superscripts or subscripts, R, Q, or RQ to all density operators to make that clear. In these new terms, the state change under measurement that we are interested in is given by

$$\rho^Q \rightarrow \rho_b^Q = \frac{1}{p_b} U_b E_b^{1/2} \rho^Q E_b^{1/2} U_b^\dagger \tag{A8}$$

after an outcome b is found. That same measurement, on the other hand, changes the state of the RQ system according to

$$|\psi^{RQ}\rangle \rightarrow |\psi_b^{RQ}\rangle = \sqrt{\frac{1}{p_b}} (I_R \otimes A_b) |\psi^{RQ}\rangle, \tag{A9}$$

where

$$A_b = U_b E_b^{1/2}. \tag{A10}$$

(Recall that pure states remain pure under an efficient measurement.) The operator I_R in this equation, of course, signifies the identity operator on the R system.

Note that the initial density operators ρ^R and ρ^Q for the R and Q systems are unitarily equivalent, i.e.,

$$\rho^R = \mathrm{tr}_Q |\psi^{RQ}\rangle\langle\psi^{RQ}| = V \rho^Q V^\dagger, \tag{A11}$$

for some unitary operator V. In particular, it follows that ρ^R and ρ^Q have the same eigenvalues. We can also note, however, that since a measurement on Q can have no overall effect on R, it must be the case that

$$\rho^R = \mathrm{tr}_Q \left(\sum_b p_b |\psi_b^{RQ}\rangle\langle\psi_b^{RQ}| \right). \tag{A12}$$

One can see this more formally by choosing a Schmidt decomposition for $|\psi^{RQ}\rangle$:

$$|\psi^{RQ}\rangle = \sum_{k=1}^{d} \sqrt{\lambda_k} |r_k\rangle |q_k\rangle. \tag{A13}$$

Then

$$\mathrm{tr}_Q \left(\sum_b p_b |\psi_b^{RQ}\rangle\langle\psi_b^{RQ}| \right) \tag{A14}$$

$$= \sum_{lb} \langle q_l | (I_R \otimes A_b) |\psi^{RQ}\rangle\langle\psi^{RQ}| (I_R \otimes A_b^\dagger) | q_l \rangle \tag{A15}$$

$$= \sum_{kmlb} \sqrt{\lambda_k}\sqrt{\lambda_m} |r_k\rangle\langle r_m| \langle q_l|A_b|q_k\rangle\langle q_m|A_b^\dagger|q_l\rangle \tag{A16}$$

$$= \sum_{kmlb} \sqrt{\lambda_k}\sqrt{\lambda_m} |r_k\rangle\langle r_m| \langle q_m|A_b^\dagger|q_l\rangle\langle q_l|A_b|q_k\rangle \tag{A17}$$

$$= \sum_{kmb} \sqrt{\lambda_k}\sqrt{\lambda_m} |r_k\rangle\langle r_m| \langle q_m|A_b^\dagger A_b|q_k\rangle \tag{A18}$$

$$= \sum_{km} \sqrt{\lambda_k}\sqrt{\lambda_m} |r_k\rangle\langle r_m| \delta_{mk} \tag{A19}$$

$$= \sum_k \lambda_k |r_k\rangle\langle r_k| \tag{A20}$$

$$= \rho^R. \tag{A21}$$

It follows from Eq. (A12) and the statement preceding it that

$$\vec{\lambda}(\rho^Q) = \vec{\lambda}(\rho^R) = \vec{\lambda}\left[\mathrm{tr}_Q \left(\sum_b p_b |\psi_b^{RQ}\rangle\langle\psi_b^{RQ}| \right) \right]. \tag{A22}$$

But tr_Q is a linear mapping. So, defining

$$\rho_b^R = \mathrm{tr}_Q |\psi_b^{RQ}\rangle\langle\psi_b^{RQ}|, \tag{A23}$$

we have

$$\vec{\lambda}(\rho^Q) = \vec{\lambda}\left(\sum_b p_b \rho_b^R \right). \tag{A24}$$

Now comes the point where we rely on the mathematical literature ever so slightly by using Ky Fan's dominance theorem [53]. One can show that for any Hermitian operator O,

$$\sum_{i=1}^{k} \lambda_i(O) = \max_P \mathrm{tr}\, PO, \tag{A25}$$

where the maximization is taken over all rank-k projectors. It follows from this almost immediately that

$$\vec{\lambda}(O + \mathcal{N}) \prec \vec{\lambda}(O) + \vec{\lambda}(\mathcal{N}) \tag{A26}$$

since

$$\max_P \mathrm{tr}\, P(O + \mathcal{N}) \leqslant \max_P \mathrm{tr} PO + \max_P \mathrm{tr}\, P\mathcal{N}. \tag{A27}$$

It follows from this that

$$\vec{\lambda}(\rho^Q) \prec \sum_b \vec{\lambda}(p_b \rho_b^R) = \sum_b p_b \vec{\lambda}(\rho_b^R), \tag{A28}$$

since $\vec{\lambda}(cO) = c\vec{\lambda}(O)$ for any positive number c.

Noting finally that the eigenvalue spectrum of ρ_b^R is the same as that of ρ_b^Q, we have, ultimately,

$$\vec{\lambda}(\rho^Q) \prec \sum_b p_b \vec{\lambda}(\rho_b^Q). \tag{A29}$$

Stripping off the superscript Q, we have the desired result Eq. (A6), and the theorem is proved.

It comes about as a corollary to Eq. (A6), through some theorems in Ref. [52] that our most desired result—namely Eq. (A1)—holds for any concave unitarily invariant function F. However, there is a more direct way to see this, and it seems worthwhile to take that route. We need only back up to Eq. (A24). From this it follows that

$$F(\rho^Q)=F\left(\sum_b p_b\rho_b^R\right). \tag{A30}$$

However, F is concave and so

$$F(\rho^Q)\geq\sum_b p_bF(\rho_b^R) \tag{A31}$$

$$=\sum_b p_bF(\rho_b^Q). \tag{A32}$$

Again, stripping off the superscript Q, we obtain the desired result.

Instructive though it is to derive Eq. (A6) by first extending the problem to an ancillary Hilbert space, there is an even shorter route to the result that is worth recording. The trick to note is this: With each efficient measurement $\mathcal{E}=(E_b)=(A_b^\dagger A_b)$, we can associate a canonical decomposition of the density operator starting from the fact that the E_b form a resolution of the identity. Starting from the equation,

$$I=\sum_b E_b\,, \tag{A33}$$

one simply multiplies it from the left and right by $\rho^{1/2}$ to obtain

$$\rho=\sum_b p_b\omega_b\,, \tag{A34}$$

where

$$\omega_b=\frac{1}{p_b}\rho^{1/2}E_b\rho^{1/2}, \tag{A35}$$

and $p_b=\operatorname{tr}\rho E_b$ as always.

Using the Ky Fan dominance theorem as before, but now on Eq. (A34), we have straight away that

$$\vec{\lambda}(\rho)\prec\sum_b p_b\vec{\lambda}(\omega_b). \tag{A36}$$

However, it is an easy matter to see that the operators $\rho^{1/2}E_b\rho^{1/2}$ and $A_b\rho A_b^\dagger$ have precisely the same eigenvalue structure. We start off with the eigenvalue equation

$$(\rho^{1/2}A_b^\dagger A_b\rho^{1/2})|i\rangle=\mu_i|i\rangle. \tag{A37}$$

Multiplying this from the left by $A_b\rho^{1/2}$ and regrouping terms, one obtains

$$A_b\rho A_b^\dagger(A_b\rho^{1/2}|i\rangle)=\mu_i(A_b\rho^{1/2}|i\rangle), \tag{A38}$$

which means that $\rho^{1/2}E_b\rho^{1/2}$ and $A_b\rho A_b^\dagger$ have the same eigenvalues. Using this, Eq. (A6) follows immediately.

APPENDIX B: FULL VARIATION OVER MEASUREMENTS OF A GIVEN STRENGTH

For this appendix, we drop the distinction of finite vs infinite measurement strength, and attempt to grade all measurements via a single *finite* number. One possible notion of such a measurement strength is the amount by which Alice's purity would change if ρ happened to be the maximally mixed state $\frac{1}{2}I$—that is, the measurement strength would be her change of knowledge if she starts out completely ignorant of the system. We can do this with respect to any of the functions F in Eq. (27), but for convenience we will again adopt the impurity P to be the main function of interest. Also for convenience, we will actually adopt two times the said quantity above, i.e., $2\Delta_{\rm in}(\frac{1}{2}I)$. This choice of prefactor causes our notion of measurement strength to range in the full interval $[0,1]$.

Thus, using Eq. (66) and taking $a=0$, a given measurement strength k for a two-outcome measurement $(E,I-E)$ is defined by

$$k=\frac{\alpha b^2}{2-\alpha}. \tag{B1}$$

The question we shall pose in this appendix is the following. For a given quantum state ρ and a fixed measurement strength k, what is the maximum value of $\Delta_{\rm in}$, and what values of z achieve that maximum? In particular, can we show that the optimal values for z^2 in this problem are strictly less than 1? Unfortunately, we will have to answer the latter question in the negative, regardless of the value a defining the purity of the initial density operator.

This is seen as follows. Fix k anywhere in the range between 0 and 1. For a fixed b this means that α must take on the value

$$\alpha=\frac{2k}{b^2+k}. \tag{B2}$$

Note that for a fixed value of k we are not allowed to choose freely b as we wish. This is because for a fixed k, the variable b cannot be too small or we would never be able to satisfy Eq. (B1). The valid range for b turns out to be

$$k\leq b\leq 1. \tag{B3}$$

The consideration leading to this is simple. The function $\alpha/(2-\alpha)$ is monotonically increasing in α. So to find our smallest value of b, we should place the largest allowed value of α [Eq. (51)] into the right-hand side of Eq. (B2). Doing this gives Eq. (B3).

Inserting Eq. (B2) into Eq. (66) gives a surprisingly simple expression:

$$\Delta_{\rm in}=\frac{k(1-a^2)(1-a^2z^2)b}{2(1+azb)(b-akz)}. \tag{B4}$$

Let us now examine the behavior of this as a function of b. Taking the partial derivative with respect to b, we obtain

$$\frac{2}{k(1-a^2)(1-a^2z^2)}\frac{\partial\Delta_{\rm in}}{\partial b}=-\frac{a(b^2+k)z}{(1+azb)^2(b-akz)^2}. \tag{B5}$$

Therefore $\Delta_{\rm in}(b)$ switches between being an increasing and decreasing function depending upon the sign of z. Thus $\max_b\Delta_{\rm in}(b)$ takes on a piecewise form. If $z\geqslant 0$, we should choose $b=k$; if $z\leqslant 0$, we should choose $b=1$. The resultant of these choices is conveniently summarized as follows:

$$\Delta_{\rm in}^{\rm max}(z)=\frac{1}{2}k(1-a^2)\frac{1+a|z|}{1+ak|z|}. \tag{B6}$$

The function $\Delta_{\rm in}^{\rm max}(z)$ in Eq. (B6) is increasing in $|z|$ since $k\leqslant 1$. Hence it finally follows that the very best strategy on Alice's part for a given measurement strength k is to take $z=1$ or -1. Doing so gives her an absolute maximum purity change of

$$\Delta_{\rm in}^{\rm max}=\frac{1}{2}k(1-a^2)\frac{1+a}{1+ak}, \tag{B7}$$

and that purity change is accompanied by a purity change of $\Delta_{\rm out}=0$ for Bob.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] N. Bohr, Phys. Rev. **48**, 696 (1935).

[3] We should point out that lately it has become fashionable to say that Bohr dropped his rhetoric of ‘‘measurement causing disturbance’’ soon after his reply to the EPR paper [4]. We disagree with this, as the counterevidence is easily exhibited in almost everything that Bohr wrote on the subject thereafter. A prime example is this passage from Ref. [5]: ‘‘The very fact that quantum phenomena cannot be analysed on classical lines thus implies the impossibility of separating a behavior of atomic objects from the interaction of these objects with the measuring instruments which serve to specify the conditions under which the phenomena appear. In particular, the individuality of the typical quantum effects finds proper expression in the circumstance that any attempt at subdividing the phenomena will demand a change in the experimental arrangement, introducing new sources of uncontrollable interaction between objects and measuring instruments.’’

[4] N. D. Mermin (private communication).

[5] N. Bohr, Dialectica **2**, 312 (1948).

[6] W. Pauli, in *Writings on Philosophy and Physics*, edited by C. P. Enz and K. von Meyenn (Springer-Verlag, Berlin, 1995), p. 132.

[7] M. Jammer, *The Philosophy of Quantum Mechanics: The Interpretations of Quantum Mechanics in Historical Perspective* (Wiley, New York, 1974).

[8] M. Beller, *Quantum Dialogue: The Making of a Revolution*, (University of Chicago Press, Chicago, 1999).

[9] We pay no attention to *variants* of quantum mechanics, such as Bohmian mechanics, that incorporate nonlocal hidden variables.

[10] For a clear discussion of this point, see N. D. Mermin, *Boojums All the Way Through: Communicating Science in a Prosaic Age* (Cambridge University Press, Cambridge, 1990), pp. 110–176.

[11] A. Peres, Phys. Rev. A **61**, 022116 (2000).

[12] C. A. Fuchs and A. Peres, Phys. Today **53**(3), 70 (2000).

[13] S. L. Braunstein and C. M. Caves, Found. Phys. Lett. **1**, 3 (1988).

[14] W. Heisenberg, in *Quantum Theory and Measurement*, edited by J. A. Wheeler and W. H. Zurek (Princeton University Press, Princeton, 1983), pp. 62–84.

[15] W. G. Unruh, Phys. Rev. D **18**, 1764 (1978); **19**, 2888 (1979).

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

[17] The first appearance of this idea seems to be in the work of Stephen Wiesner, circa 1970, but remained unpublished until much later. See S. Wiesner, SIGACT News **15**, 78 (1983).

[18] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 10-12, 1984* (IEEE Press, New York, 1984), pp. 175–179.

[19] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[20] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[21] C. A. Fuchs, Fortschr. Phys. **46**, 535 (1998).

[22] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[23] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[24] D. Bruss, Phys. Rev. Lett. **81**, 2598 (1998).

[25] *Studies in Subjective Probability*, 2nd ed., edited by H. E. Kyburg, Jr. and H. E. Smokler (Krieger, Huntington, NY, 1980).

[26] J. M. Bernardo and A. F. M. Smith, *Bayesian Theory* (Wiley, New York, 1994).

[27] One of the authors (C.A.F.) is tempted to speculate that this idea alone (suitably refined) captures the essence of quantum mechanics. The formalism of quantum theory, by this view, is simply the best agreement we can all come to in a world so sensitive to our experimental interventions. This contrasts with the defining property of the classical world, which, at the outset, is assumed to be describable by a set of variables stable enough that we can discover them or, at the very least, safely contemplate their supposed existence.

[28] A. M. Gleason, J. Math. Mech. **6**, 885 (1957).

[29] R. B. Ash, *Information Theory* (Dover, New York, 1965).

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

[31] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).

[32] W. K. Wootters, Found. Phys. **20**, 1365 (1990).

[33] K. R. W. Jones, J. Phys. A **24**, 1237 (1991).

[34] G. Lüders, Ann. Phys. (Leipzig) **8**, 323 (1951).

[35] P. Busch, P. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement*, 2nd revised ed. (Springer-Verlag, Berlin, 1996).
[36] P. Busch and J. Singh, Phys. Lett. A **249**, 10 (1998).
[37] M. A. Nielsen, e-print quant-ph/0008073.
[38] G. Lindblad, Commun. Math. Phys. **28**, 245 (1972).
[39] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[40] H. M. Wiseman and G. J. Milburn, Phys. Rev. A **47**, 642 (1993).
[41] R. Schatten, *Norm Ideals of Completely Continuous Operators* (Springer-Verlag, Berlin, 1960).
[42] H. N. Barnum, Ph.D. thesis, University of New Mexico, 1998.
[43] K. Banaszek, LANL e-print archive, quant-ph/0003123.
[44] A. C. Doherty, K. Jacobs, and G. Jungman, e-print quant-ph/0006013.
[45] A. Fujiwara and H. Nagaoka, IEEE Trans. Inf. Theory **44**, 1071 (1998).
[46] R. G. Gallager, *Information Theory and Reliable Communication* (Wiley, New York, 1968).
[47] R. Jozsa, D. Robb, and W. K. Wootters, Phys. Rev. A **49**, 668 (1994).
[48] C. M. Caves and C. A. Fuchs, in *The Dilemma of Einstein, Podolsky and Rosen—60 Years Later*, edited by A. Mann and M. Revzen [Ann. Isr. Phys. Soc. **12**, 226 (1996)].
[49] E. T. Jaynes, Phys. Rev. **106**, 620 (1957).
[50] J. Aczél and Z. Daróczy, *On Measures of Information and Their Characterizations* (Academic Press, New York, 1975).
[51] M. A. Nielsen also made a similar point in Ref. [37].
[52] T. Ando, Linear Algebr. Appl. **118**, 163 (1989).
[53] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications* (Academic Press, New York, 1979).
[54] B. W. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[55] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, e-print quant-ph/9912039.