Efficient measurements, purification, and bounds on the mutual information

Kurt Jacobs
Centre for Quantum Computer Technology, Centre for Quantum Dynamics, School of Science, Griffith University, Nathan 4111, Brisbane, Australia

(Received 25 July 2003; published 4 November 2003)

When a measurement is made on a quantum system in which classical information is encoded, the measurement reduces the observers' average Shannon entropy for the encoding ensemble. This reduction, being the *mutual information*, is always non-negative. For efficient measurements the state is also purified; that is, on average, the observers' von Neumann entropy for the state of the system is also reduced by a non-negative amount. Here we point out that by rewriting a bound derived by Hall [Phys. Rev. A **55**, 100 (1997)], which is dual to the Holevo bound, one finds that for efficient measurements, the mutual information is bounded by the reduction in the von Neumann entropy. We also show that this result, which provides a physical interpretation for Hall's bound, may be derived directly from the Schumacher-Westmoreland-Wootters theorem [Phys. Rev. Lett. **76**, 3452 (1996)]. We discuss these bounds, and their relationship to another bound, valid for efficient measurements on pure state ensembles, which involves the subentropy.

DOI: 10.1103/PhysRevA.68.054302 PACS number(s): 03.67.−a, 03.65.Ta, 89.70.+c, 02.50.Tt

In what follows we will be concerned with the situation in which one observer, the sender, transmits information to another observer, the receiver, by encoding that information in a quantum system and having the receiver make a subsequent measurement on the system. It is useful at this point to define all our terminology and notation regarding this information transmission process.

To encode the information in the quantum system the sender uses an alphabet consisting of a set of possible states, and prepares the system in one of these states ρ_i, with probability P_i. The set of states along with their respective probabilities is referred to as the encoding or the ensemble and we will denote it by $\varepsilon \equiv \{P_i, \rho_i\}$. When the system has been prepared by the sender, the state-of-knowledge of the receiver regarding the system is $\rho = \Sigma_i P_i \rho_i$. We will always denote the dimension of the system used for encoding by N, and we will refer to ρ as the ensemble state.

The measurement made by the receiver is described by a set of operators A_j such that $\Sigma_j A_j^\dagger A_j = I$ [1–3]. We will denote the measurement by $\mathcal{M} \equiv \{A_j\}$. Where convenient we will denote the operators $A_j^\dagger A_j$ as E_j. For efficient measurements, with which we will be concerned in the following unless otherwise stated, each of the operators A_j corresponds to a measurement outcome, and the outcomes are therefore labeled by j. The final state of the system from the point of view of the observer, having obtained the outcome j, is $\rho_j' = A_j \rho A_j^\dagger / Q_j$, where $Q_j = \mathrm{Tr}[E_j \rho]$ is the probability that outcome j will result. For clarity we will denote probability densities over i as P, and those over j as Q.

The amount of information transmitted to the receiver in the process of preparation and measurement, which we will refer to as ΔI_{i}, is given by the mutual information $H(I{:}J)$ between the preparation, indexed by i, and the outcomes, indexed by j [4]. Thus

$$\Delta I_{\mathrm{i}} = H(I{:}J) = H[P_i] - \sum_j Q_j H[P(i|j)], \tag{1}$$

where H is the Shannon entropy and $P(i|j)$ is the receiver's probability density for the prepared state, after having received outcome j. (That is, the receiver's final state-of-knowledge about which state has initially been prepared.) The mutual information is thus the average difference between the receiver's initial information about the preparation, and her final information after the measurement. We denote this by ΔI_{i} to reflect this fact, with the subscript indicating that it constitutes information about the initial preparation. The maximum of ΔI_{i} over all measurements, for a fixed encoding, is referred to as the accessible information of the encoding [5], and we will denote this by ΔI_{acc}.

The celebrated Holevo bound provides a limit to the accessible information of an encoding [6–8]. The Holevo bound is

$$\Delta I_{\mathrm{i}} \leqslant S[\rho] - \sum_i P_i S[\rho_i] \equiv \chi(\varepsilon), \tag{2}$$

where $S[\rho]$ denotes the von Neumann entropy of ρ.

One can also consider another problem, which may be viewed as being complementary to that of finding the accessible information; that of obtaining the maximum of ΔI_{i} given that it is the receiver's measurement and the ensemble state ρ which are fixed, and it is instead the sender which has the ability to use any encoding consistent with ρ. Hall has shown that it is possible to use Holevo's bound, along with a duality relation between encodings and measurements, which he refers to as source duality, to derive a bound on ΔI_{i} for this case. Hall's dual Holevo bound is [9]

$$\Delta I_{\mathrm{i}} \leqslant S[\rho] - \sum_j Q_j S\left[\frac{\sqrt{\rho} E_j \sqrt{\rho}}{Q_j}\right]. \tag{3}$$

The Holevo bound and (as we will show) Hall's bound, may both be derived directly from the more general bound obtained by Schumacher, Westmoreland, and Wootters (SWW) in 1996 [10]. We state this theorem now, and will return to it later.

Theorem (Schumacher-Westmoreland-Wootters). The information transmitted from sender to receiver ΔI_{i} when the sender uses the encoding ε, and the receiver uses measurement $\mathcal{M}$, is bounded such that

$$\Delta I_{\mathrm{i}} \leqslant S[\rho] - \sum_i P_i S[\rho_i] - \sum_j Q_j \left[S[\rho_j'] - \sum_i P(i|j) S[\rho_{ji}'] \right], \quad (4)$$

where all quantities are as defined above, and the quantity ρ_{ji}' is introduced, which is the final state that the receiver *would* have had, *if* she knew that the initial state was ρ_i. Thus $\rho_{ji}' = A_j \rho_i A_j^\dagger / Q(j|i)$, where $Q(j|i)$ is naturally the probability density for the measurement outcomes, given that the initial state is ρ_i. Because of the final term on the right-hand side (RHS) of this inequality, to which we will return later, this bound is, in general, stronger than the Holevo bound.

While ΔI_{i} quantifies the information which the observer obtains about the initial preparation, there exists another quantity which can be said to characterize the average amount of information which the receiver obtains about the final state which she is left with after the measurement [11,12]. We will denote this by ΔI_{f}, the expression for which is

$$\Delta I_{\mathrm{f}} = S[\rho] - \sum_j Q_j S[\rho_j']. \quad (5)$$

This is the average difference between the receiver's initial von Neumann entropy of the quantum system, and her final von Neumann entropy. This quantity is useful when considering quantum state preparation and, more generally, quantum feedback control [11].

While we have introduced ΔI_{i} and ΔI_{f} in terms of initial states and final states, the former is not really any more connected with initial states than it is with final states, since the Shannon entropy of the ensemble after measurement is independent of whether it is written in terms of the initial states or the final ones. A more fundamental difference between ΔI_{i} and ΔI_{f} is that the former is the average change in the observers Shannon entropy regarding the ensemble, where as the latter is the average change in the observers von Neumann entropy regarding the overall state of the quantum system. That is, $\Delta I_{\mathrm{i}} = \langle \Delta H(\varepsilon) \rangle$ and $\Delta I_{\mathrm{f}} = \langle \Delta S[\rho(\varepsilon)] \rangle$.

We now show that when the measurement and ensemble state are fixed, ΔI_{i} is bounded by ΔI_{f} (or, alternatively, $\langle \Delta H \rangle \leqslant \langle \Delta S \rangle$). This is readily done by showing that this relationship is merely an alternative form for Hall's bound. To do this one notes that if we use the polar decomposition theorem [13] to write $A_j = U_j \sqrt{E_j}$, where U_j is unitary, and define $B_j = \sqrt{E_j}\sqrt{\rho}$, then the Hermitian operators which appear in Hall's bound are

$$\sqrt{\rho} E_j \sqrt{\rho} = B_j^\dagger B_j, \quad (6)$$

while the final states are

$$Q_j \rho_j' = U_j B_j B_j^\dagger U_j^\dagger. \quad (7)$$

But $B_j^\dagger B_j$ and $B_j B_j^\dagger$ have the same eigenvalues [14]. Thus since the von Neumann entropy is only a function of the eigenvalues, we can replace $\sqrt{\rho} E_j \sqrt{\rho}$ with $Q_j \rho_j'$ in the original expression for Hall's bound, and the result is

$$\Delta I_{\mathrm{i}} \leqslant \Delta I_{\mathrm{f}}. \quad (8)$$

One can interpret this as saying that an observer cannot learn more about the classical information encoded in a quantum system than she learns about the state of the quantum system. This provides a physical interpretation for Hall's bound. Further, as was pointed out by Hall [9], this bound can only be saturated when all the operators E_j commute.

The above result may also be obtained from the SWW theorem. To do this one first rewrites the second and fourth terms of the RHS of Eq. (4), using the fact that $Q_j P(i|j) = P_i Q(j|i)$:

$$\begin{aligned} -\sum_i P_i S[\rho_i] + \sum_j Q_j \sum_i P(i|j) S[\rho_{ji}'] &= -\sum_i P_i [S[\rho_i] - Q(j|i) S[\rho_{ij}']] \\ &= -\sum_i P_i \Delta I_{\mathrm{f}i}, \end{aligned} \quad (9)$$

where $\Delta I_{\mathrm{f}i}$ is the information that would have been obtained about the final state *if* the initial state had been ρ_i. This gives

$$\Delta I_{\mathrm{i}} \leqslant S[\rho] - \sum_i P_i \Delta I_{\mathrm{f}i} - \sum_j Q_j S[\rho_j']. \quad (10)$$

Now, since Nielsen has shown that ΔI_{f} is always non-negative [15] (see also Ref. [12]), the RHS is maximized when the $\Delta I_{\mathrm{f}i}$ are zero for all *i*. Since this is true for all pure state ensembles, the result is the bound given in Eq. (8).

One consequence of Eq. (8) is that, if we choose an ensemble which has the maximal accessible information for a fixed ρ, we can only obtain all this information if all the final states are pure. As SWW point out in their paper, measurements which leave the final state impure, leave some information in the system. That is, if the final state is mixed, in general it depends on the initial ensemble, and as a result subsequent measurements can obtain further information about the initial preparation, whereas this is not possible if the final state is pure.

For a given ρ not all ensembles have an accessible information equal to $S[\rho]$. We may ask then, if it is possible for measurements which leave the final state impure to extract all the accessible information from *these* encodings. In fact, this is only possible if the encoding satisfies special conditions; in general, incomplete measurements will not even extract the accessible information from an ensemble. To see this, consider the final states, ρ_j', which result from the measurement. Each of these consists of an ensemble, ε_j over the states $\rho_{i|j}$, introduced above. In particular,

$$\rho'_j = \sum_i P(i|j)\rho_{i|j}. \tag{11}$$

Since these ensembles consist of states indexed by *i*, they can, in general, be measured to obtain further information about the initial preparation. Since the accessible information is the maximal amount of information that can be obtained about *i* by making measurements, we have the inequality

$$\Delta I_{\mathrm{i}}(\varepsilon,\mathcal{M}) \leqslant \Delta I_{\mathrm{acc}}(\varepsilon) - \sum_j Q_j \Delta I_{\mathrm{acc}}(\varepsilon_j). \tag{12}$$

Thus, $\Delta I_{\mathrm{i}}(\varepsilon,\mathcal{M})$ can only be equal to $\Delta I_{\mathrm{acc}}(\varepsilon)$ if the $\Delta I_{\mathrm{acc}}(\varepsilon_j)$ are zero for all *j*. If ρ'_j is pure, then $\Delta I_{\mathrm{acc}}(\varepsilon_j)$ is zero. If ρ'_j is not pure, then the accessible information of ε_j is only zero if, for any given *j*, the $\rho_{i|j}$ are the *same* for all *i*. A little algebra shows that this is only true if

$$P_{A_j}\rho_i P_{A_j} - \alpha_{ikj} P_{A_j}\rho_k P_{A_j} = 0, \quad \forall i,k \tag{13}$$

for some non-negative real numbers α_{ikj}, where P_{A_j} is a projector onto the support of the operator A_j. This means that for a measurement to extract all the accessible information, all the coding states ρ_j must be identical, up to a multiplier, on the supports of the operators A_j, separately for every *j*.

For pure-state ensembles it is easy to see the effect of the conditions given by Eq. (13). Consider merely the *j* for which the corresponding A_j has the support with the largest dimension, and call this dimension $M_{\max}$. Then the effect of Eq. (13) for this *j* alone is simply to limit the dimension of the space from which the pure states in the ensemble can be drawn to $N - M_{\max} + 1$. The accessible information of pure-state ensembles which satisfy Eq. (13) is therefore bounded by $\ln(N - M_{\max} + 1)$.

As was noted by SWW, the expression in the square brackets in Eq. (4) is the Holevo χ quantity for the ensemble ε_j which results from measurement outcome *j*. Thus their bound may be written as

$$\Delta I_{\mathrm{i}} \leqslant \chi[\varepsilon] - \sum_j Q_j \chi[\varepsilon_j]. \tag{14}$$

Now, $\chi[\varepsilon_j]$ is the Holevo bound on the information that the receiver could extract when making a subsequent measurement after obtaining result *j*. The SWW bound is therefore very interesting because it shows that, if the initial ensemble ε is chosen so that its accessible information is maximal [i.e., equal to $\chi(\varepsilon)$], then the information obtained by an incomplete measurement will be reduced by the *maximal* amount of information which could be accessible from the final ensembles ε_j, and not merely the *actual* information available in these ensembles, which would imply the bound given in Eq. (12). In general, therefore, there is a gap between the information lacking in an incomplete measurement, and that which can be recovered by subsequent measurements. It is natural to ask therefore if this is true for all ensembles. That is, whether the inequality in Eq. (12) can be strengthened by replacing the final term on the RHS by the final term in the RHS of Eq. (14). However, this is not the case. As the following theorem shows, for pure-state ensembles a tight upper bound is obtained by replacing the final term in Eq. (12) by the average of the subentropies of the final states [16], rather than the corresponding Holevo quantities.

Theorem. For an initial pure-state ensemble ε, and a general efficient measurement $\mathcal{M}$, one has

$$\Delta I_{\mathrm{i}} \leqslant \Delta I_{\mathrm{acc}}[\varepsilon] - \sum_j Q_j Q[\rho'_j], \tag{15}$$

where $Q[\cdots]$ is the subentropy as defined by Jozsa, Robb, and Wootters (JRW) [16], and this bound is tight in the sense that there exists a pure-state ensemble which saturates the inequality.

Proof. If the initial ensemble ε is pure, then the final ensembles ε_j are also pure. As a result, the accessible information of each of these ensembles is bounded below by $Q[\rho'_j]$ [16]. We can therefore replace the final sum in Eq. (12) by $\Sigma_j Q_j Q[\rho'_j]$, which gives Eq. (15).

That the bound can be achieved can be shown by calculating ΔI_{i} for the uniform ensemble over pure states, being the unique distribution over pure states which is invariant under unitary transformations. In this case the ensemble state is given by

$$\rho = \int |\psi\rangle\langle\psi|\, d|\psi\rangle = \frac{I}{N}, \tag{16}$$

where $d|\psi\rangle$ represents integration over the unitarily invariant, or Haar, measure [17,18]. The accessible information is given by $Q[I/N]$ [16]. The information obtained by a general measurement may be calculated directly:

$$\begin{aligned}\Delta I_{\mathrm{i}} &= H[Q_j] - \int H[Q(j||\psi\rangle)]d|\psi\rangle \\ &= \ln N + \sum_j \mathrm{Tr}[E_j]\int \langle\psi|\rho'_j|\psi\rangle \ln(\langle\psi|\rho'_j|\psi\rangle) d|\psi\rangle \\ &= Q[I/N] - \sum_j Q_j Q[\rho'_j],\end{aligned} \tag{17}$$

where the integral in the second line is performed using the techniques in Ref. [16]. ■

The above result reveals a special property of the uniform ensemble: no matter what incomplete measurement is performed on it, the information which is not retrieved by the measurement can always be extracted by subsequent measurements. To see this we first use the polar decomposition theorem as before to write $A_j = U_j\sqrt{E_j}$. The final state is then given by $\rho'_j = U_j E_j U_j^\dagger / \mathrm{Tr}[E_j]$. It is convenient to write the final ensemble as a distribution over unnormalized states, $|\tilde{\phi}_j\rangle$. Writing these states in terms of the final state ρ'_j, we have

$$|\tilde{\phi}_j\rangle = \sqrt{\rho'_j}|\psi'_j\rangle, \tag{18}$$

where $|\psi'_j\rangle = U_j|\psi\rangle$. The probability density of these states in the final ensemble (with respect to the Haar measure) is $P(|\tilde{\phi}_j\rangle) = \langle\tilde{\phi}_j|\tilde{\phi}_j\rangle$. Since the ensemble of states $|\psi\rangle$ is uniform, so is the ensemble of states $|\psi_j'\rangle$. The final ensemble, $\varepsilon_j=\{P(|\tilde{\phi}_j\rangle),|\tilde{\phi}_j\rangle\}$, is referred to as a "distortion" of the uniform ensemble by the state ρ_j'. Since JRW have shown that such a distortion has an accessible information equal to $Q[\rho_j']$, all the information missing in the incomplete measurement is accessible in the final ensembles ε_j.

While Hall's bound is saturated for pure-state ensembles which maximize the accessible information (and measurements whose operators commute with the ensemble state), the bound given by Eq. (15) is saturated by pure-state ensembles which minimize the accessible information. Since we have considered only efficient quantum measurements so far, we complete our discussion by examining classical measurements and inefficient quantum measurements. For this purpose it is best that we first introduce the latter. Inefficient measurements are simply efficient measurements in which the observer knows only that one of a subset of the possible results was obtained. As a result, the observers final state of knowledge is given by averaging over a subset of the states ρ_j'. Thus, if we now label the measurement results by two indices k and l, then, in general, we can write the actual final states for an observer who makes an inefficient measurement as $\tilde{\rho}_k=\sum_l A_{kl}\rho A_{kl}^\dagger/Q_k$, where Q_k is the probability that the final state is $\tilde{\rho}_k$.

Now, classical measurements are described by the subset of quantum measurements in which all the encoding states ρ_i and all the measurement operators A_j are mutually commuting (for a discussion, see, e.g., Ref. [18]). As a result it is easily shown that inefficient classical measurements are merely efficient classical measurements, and thus Eq. (8) remains true for all classical measurements. In fact, if the encoding states are pure classical states (i.e., individual classical states rather than distributions), then the bound is always saturated with equality.

For inefficient quantum measurements, however, Eq. (8) does *not* hold. The reason for this is that for inefficient measurements ΔI_{f} can be negative (whereas ΔI_{i} is always nonnegative). An example of such a situation is one in which the initial state ρ is not maximally mixed, and the observer performs a von Neumann measurement in a basis unbiased with respect to the eigenbasis of ρ. If the observer has no knowledge of the outcome, then her final state is maximally mixed. Further, if one mixes (in the sense of Ref. [19]) this measurement with one whose measurement operators commute with ρ, it is not hard to obtain a measurement in which both ΔI_{i} and ΔI_{f} are positive, but which violates Eq. (8).

The author is grateful to Michael J. W. Hall for helpful discussions.

[1] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[2] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Lecture Notes in Physics Vol. 190 (Springer-Verlag, Berlin, 1983).
[3] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[4] C.E. Shannon and W. Weaver, *The Mathematical Theory of Communication* (Illini Books, Chicago, 1963).
[5] B. Schumacher, in *Complexity, Entropy and the Physics of Information*, edited by W.H. Zurek (Addison-Wesley, Redwood City, CA, 1990).
[6] A.S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973) [Probl. Inf. Transm. **9**, 110 (1973)].
[7] H.P. Yuen and M. Ozawa, Phys. Rev. Lett. **70**, 363 (1993).
[8] C.A. Fuchs and C.M. Caves, Phys. Rev. Lett. **73**, 3047 (1994).
[9] M.J.W. Hall, Phys. Rev. A **55**, 100 (1997).
[10] B. Schumacher, M. Westmoreland, and W.K. Wootters, Phys. Rev. Lett. **76**, 3452 (1996).
[11] A.C. Doherty, K. Jacobs, and G. Jungman, Phys. Rev. A **63**, 062306 (2001).
[12] C.A. Fuchs and K. Jacobs, Phys. Rev. A **63**, 062305 (2001).
[13] R. Schatten, *Norm Ideals of Completely Continuous Operators* (Springer-Verlag, Berlin, 1960).
[14] A.W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications* (Academic Press, New York, 1979).
[15] M.A. Nielsen, Phys. Rev. A **63**, 022114 (2001).
[16] R. Jozsa, D. Robb, and W.K. Wootters, Phys. Rev. A **49**, 668 (1994).
[17] K.R.W. Jones, Phys. Rev. A **50**, 3682 (1994).
[18] K. Jacobs, Quantum Information Processing **1**, 73 (2002).
[19] G.M. D'Ariano and P. LoPresti, quant-ph/0301110 (unpublished).