Accessible information in quantum measurement

N. J. Cerf[1,3] and C. Adami[1,2,3]
[1] *W. K. Kellogg Radiation Laboratory and* [2] *Computation and Neural Systems*
California Institute of Technology, Pasadena, California 91125
[3] *Institute for Theoretical Physics, University of California, Santa Barbara, California 93106*
(Dated: November 1996)

The amount of information that can be accessed via measurement of a quantum system prepared in different states is limited by the Holevo bound. We present a simple proof of this theorem and its extension to sequential measurements based on the properties of quantum conditional and mutual entropies. The proof relies on a minimal physical model of the measurement which does not assume environmental decoherence, and has an intuitive diagrammatic representation.

A fundamental issue of quantum information theory is the maximum amount of information that can be extracted from a quantum system. Holevo [1] proved that, if a system is prepared in a state described by one of the density operators ρ_i $(i = 1, \cdots n)$ with probability p_i, then the information I (defined in the sense of Shannon theory [2]) that can be gathered about the identity of the state never exceeds the so-called Holevo bound

$$I \leq S\left(\sum_i p_i \rho_i\right) - \sum_i p_i S(\rho_i) \ , \tag{1}$$

where $S(\rho) = -\mathrm{Tr}\rho \log \rho$ is the von Neumann entropy. This result holds for any measurement that can be performed on the system, including positive-operator-valued measures (POVM's). Since the original conjecture by Levitin [3] (proven by Holevo [1]), work on this subject has been devoted to obtaining more rigorous proofs of the theorem, and to derivations of stronger upper or lower bounds on I [4–8]. In this Letter, we start by revisiting the derivation proposed recently by Schumacher *et al.* [8] but in terms of a unified framework of quantum information theory which allows a more general formulation. Ref. [8] is based on a physical model of quantum measurement and constitutes a notable improvement over earlier derivations which are less transparent, and that involve maximizing mutual Shannon entropies over all possible measurements. Here, we show that this proof can be considerably simplified by making use of quantum conditional and mutual entropies, and the constraints on them imposed by the unitarity of measurement [9, 10]. Also, the present formulation allows for a straightforward extension of the Holevo theorem to consecutive measurements. Such a treatment clarifies the physical content of the Holevo theorem, which then simply states that the *classical* mutual entropy (i.e. the information acquired via measurement) is bounded from above by the *quantum* mutual entropy *prior* to measurement. More generally, we will show that

$$H(X{:}Y) \leq S(X{:}Y) \ , \tag{2}$$

where $S(X{:}Y) = S(X) + S(Y) - S(XY)$ is the quantum mutual entropy between X and Y constructed from the density matrix ρ_{XY}, while $H(X{:}Y)$ is the Shannon mutual entropy [11] obtained from the joint probability distribution $p(x,y) = \langle x,y|\rho_{XY}|x,y\rangle$, where $|x,y\rangle$ is an arbitrary basis in the joint Hilbert space. The essence of the proof can be represented by simple arithmetic on quantum Venn diagrams, by making use of unitarity and strong subadditivity [12]. In contrast to the derivation by Schumacher *et al.*, no environment-induced decoherence is needed in the physical model of quantum measurement, while it can be added without difficulty.

Let us assume that a "preparer" is described by a (discrete) internal variable X, distributed according to the probability distribution p_i $(i = 1, \cdots N)$. The internal state of the preparer, considered as a physical *quantum* system, is then given by the density matrix

$$\rho_X = \sum_i p_i |x_i\rangle\langle x_i| \tag{3}$$

with the $|x_i\rangle$ being an orthonormal set of preparer states. The state of the quantum variable X can be copied to another system simply by effecting conditional dynamics (*e.g.*, a controlled-NOT quantum gate in a 2-state Hilbert space). In that sense, X behaves just like a classical variable (it can be "cloned") and therefore refers to the macroscopic (collective) set of correlated internal variables of the preparer. Assume now that the preparer has at his disposal a set of N mixed states ρ_i that can be put on a quantum channel Q according to his internal state (this is an operation which can be performed in a unitary manner). The joint state of the preparer and the quantum channel is then

$$\rho_{XQ} = \sum_i p_i |x_i\rangle\langle x_i| \otimes \rho_i \ . \tag{4}$$

A partial trace over X simply gives the state of the quantum channel:

$$\rho_Q = \mathrm{Tr}_X \rho_{XQ} = \sum_i p_i \rho_i \equiv \rho \ . \tag{5}$$

The quantum entropy of X and Q is $S(X) = H[p_i]$ and $S(Q) = S(\rho)$, while

$$S(XQ) = H[p_i] + \sum_i p_i S(\rho_i) \ , \tag{6}$$

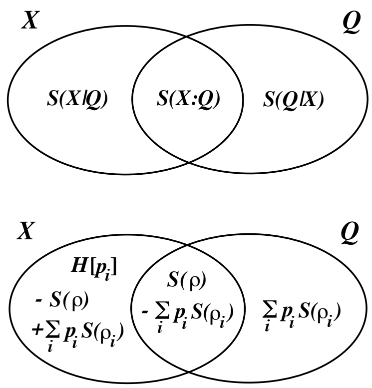


FIG. 1: Entropy Venn diagram for the correlated system XQ *before* measurement.

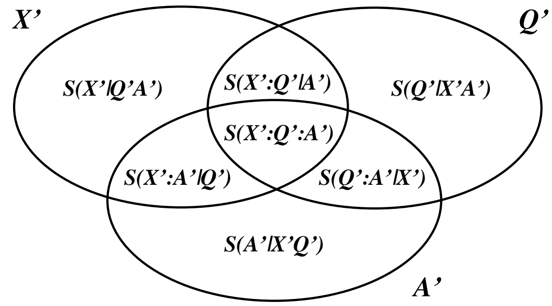


FIG. 2: Venn diagram summarizing the relation between entropies (defined in the text) *after* measurement in the system $X'Q'A'$.

where the last expression results from the fact that ρ_{XQ} is block-diagonal (this is the quantum analogue of the "grouping" property of Shannon entropies [11]). The relation between these entropies is succinctly summarized by the quantum Venn diagram [9] in Fig. 1. First, let us write the quantum mutual entropy (or mutual entanglement) between X and Q before the measurement (see Fig. 1):

$$\begin{aligned} S(X{:}Q) &= S(X) + S(Q) - S(XQ) \\ &= S(\rho) - \sum_i p_i S(\rho_i) \end{aligned} \tag{7}$$

We see that $S(X{:}Q)$ is just the Holevo bound (the quantity denoted $\chi^{(Q)}$ in Ref. [8]). Thus, all we will need to prove is that the information extracted via measurement $I \leq S(X{:}Q)$. Simple bounds for the mutual entanglement $S(X{:}Q)$ can be obtained invoking the upper and lower bounds for the entropy of a convex combination of density matrices (see, e.g., [12]). Using

$$\sum_i p_i S(\rho_i) \leq S(\rho) \leq H[p_i] + \sum_i p_i S(\rho_i) \ , \tag{8}$$

implies

$$0 \leq S(X{:}Q) \leq H[p_i] \ . \tag{9}$$

The upper bound in (9) guarantees that the entropy diagram for XQ represented in Fig. 1 has only non-negative entries and thus appears classical, a consequence of the fact that ρ_{XQ} was *constructed* as a separable state. (Negative values for conditional entropies betray quantum non-locality, see e.g. [9, 13].)

In the following, we describe the measurement of the preparation. This is achieved by bringing about a unitary operation on an ancilla A and the quantum preparation Q that effects entanglement, and subsequently observing the state of this ancilla. The information I extracted from the measurement is then just the mutual entropy between the ancilla and the preparer. Before interaction, the ancilla A is in a reference state $|0\rangle$ and the joint state of the system XQA is a product state $\rho_{XQ} \otimes |0\rangle\langle 0|$. This implies of course that $S(X{:}Q) = S(X{:}QA)$, as A has vanishing entropy. The joint system after interaction via a unitary transformation U_{QA} is described by

$$\rho_{X'Q'A'} = (1_X \otimes U_{QA})(\rho_{XQ} \otimes |0\rangle\langle 0|)(1_X \otimes U_{QA})^\dagger \tag{10}$$

and the corresponding quantum Venn diagram Fig. 2. (We denote by X', Q', and A', the respective systems *after* measurement.) For the moment, let us assume that U_{QA} is arbitrary; we will discuss its specific form later. The key quantity of interest is the mutual entanglement $S(X'{:}A')$ between the physical state of the ancilla A *after* measurement and the physical state of the preparer X (which has remained unchanged). We will show later that, with certain conditions on U_{QA}, $S(X'{:}A')$ is just the Shannon mutual entropy between the preparer and the ancilla, or, in other words, the information I extracted by the observer about the preparer state. Anticipating this, for a proof of Holevo's theorem we need only find an upper bound for $I = S(X'{:}A')$. As the measurement involves unitary evolution of QA while leaving X unchanged ($X' = X$), the mutual entanglement between X and QA is conserved:

$$S(X'{:}Q'A') = S(X{:}QA) = S(X{:}Q) \ . \tag{11}$$

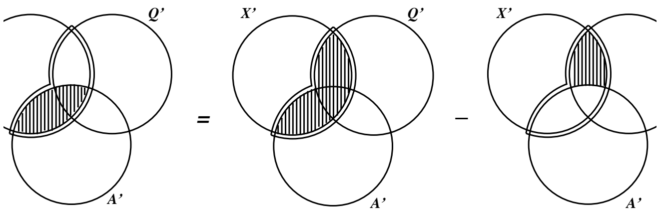
We now split this entropy according to the quantum analogue of the chain rules for mutual entropies [10, 14] to obtain

$$S(X'{:}Q'A') = S(X'{:}A') + S(X'{:}Q'|A') \tag{12}$$

where the second term on the right-hand side is a quantum conditional mutual entropy (the mutual entropy between X' and Q', conditionally on A', see Fig. 2). Combining Eqs. (11) and (12), we find for the mutual entropy between ancilla and preparer after measurement

$$S(X'{:}A') = S(X{:}Q) - S(X'{:}Q'|A') \ . \tag{13}$$

FIG. 3: Diagrammatic representation of the Holevo theorem using the definitions given in Fig. 2. Thea area enclosed by the double solid lines represents the mutual entropy that is conserved in the measurement $S(X'{:}Q'A') = S(X{:}Q)$.



This equation is represented as arithmetic on Venn diagrams in Fig. 3. It indicates that the information extracted is given by $S(X{:}Q)$, the Holevo bound Eq. (7), reduced by an amount which represents the quantum mutual entropy still existing between the preparer's internal variable X' and the quantum state after measurement Q', *conditional* on the observed state of the ancilla A'. The latter, the quantum conditional mutual entropy $S(X'{:}Q'|A') = S(X'A') + S(Q'A') - S(A') - S(X'Q'A')$ is in general difficult to estimate, and we may therefore make use of strong subadditivity [12] to obtain an inequality from Eq. (13). Strong subadditivity implies that the conditional mutual entropy $S(X{:}Y|Z) = S(X{:}YZ) - S(X{:}Z)$ between three quantum variables X, Y, and Z is non-negative. This expresses the physical idea that the mutual entanglement between X and YZ is larger or equal to the mutual entanglement between X and Z only (just as for mutual informations in Shannon theory), so that a mutual entanglement can never decrease when extending a system. In particular we have $S(X'{:}Q'|A') \geq 0$, which implies $S(X'{:}A') \leq S(X{:}Q)$. It remains to show that, for a particular U_{QA} which describes a measurement, the quantum mutual entropy $S(Q'{:}A')$ reduces to a Shannon mutual entropy or information, i.e., that indeed $S(X'{:}A') = I$. Let us focus on the case of a von Neumann measurement; using Neumark's theorem [15] it is easy to show that the same reasoning applies to any POVM.

For the unitary evolution of a von Neumann measurement, we use the explicit form

$$U_{QA} = \sum_\alpha P_\alpha \otimes U_\alpha \qquad (14)$$

where the index α refers to the outcome of the measurement and the P_α's denote projectors in the Q space associated with the measurement ($\sum_\alpha P_\alpha = 1$). The unitary operators U_α act in the A space, and move the ancilla from the initial state $|0\rangle$ to a state $|\alpha\rangle = U_\alpha|0\rangle$ that points to the outcome of the measurement. Let us assume that the $|\alpha\rangle$ are orthogonal to make the outcomes perfectly distinguishable. The joint density matrix after unitary evolution is given by

$$\rho_{X'Q'A'} = \sum_{i,\alpha,\alpha'} p_i |x_i\rangle\langle x_i| \otimes P_\alpha \rho_i P_{\alpha'} \otimes |\alpha\rangle\langle\alpha'| \,. \qquad (15)$$

Now, according to the no-collapse model of the measurement introduced in [10], we need to trace over the quantum system Q' which induces correlations between X' and A'. The corresponding density matrix is

$$\rho_{X'A'} = \sum_{i,\alpha} p_i \mathrm{Tr}(P_\alpha \rho_i) |x_i\rangle\langle x_i| \otimes |\alpha\rangle\langle\alpha| \,. \qquad (16)$$

As it is a *diagonal* matrix, the entropies of X', A', and $X'A'$ can be fully described within Shannon theory. (Our quantum definitions of conditional and mutual entropies reduce to the classical ones in this case [9].) A simple calculation shows that indeed

$$S(X'{:}A') = H\left[\mathrm{Tr}(P_\alpha \rho)\right] - \sum_i p_i H\left[\mathrm{Tr}(P_\alpha \rho_i)\right] \qquad (17)$$

$$= H(A) - H(A|X) = H(X{:}A) \qquad (18)$$

where H stands for the Shannon entropy and $\mathrm{Tr}(P_\alpha\rho_i)$ is the conditional probability $p_{\alpha|i}$. This completes our derivation of the standard Holevo theorem:

$$I = H(X{:}A) \leq S(X{:}Q) = S(\rho) - \sum_i p_i S(\rho_i) \,. \qquad (19)$$

The present derivation emphasizes that ignoring non-diagonal matrix elements in Eq. (4) results in a *classical* density matrix (with diagonal elements $p_{i,\alpha} = p_i p_{\alpha|i}$) whose Shannon mutual entropy is bounded from above by the corresponding *quantum* entropy. Inequality (19) arises because some information about X might still be extractable from the system Q' after the measurement, i.e., $S(X'{:}Q'|A') > 0$ (this happens in an "incomplete" measurement). This does not mean, on the other hand, that if inequality (19) is *not* saturated, all of the remaining entropy $S(X'{:}Q'|A')$ can necessarily be accessed through a subsequent measurement. Indeed, it is known that for non-commuting ρ_i's, the bound can *never* be saturated, and better upper bounds on the accessible information have been proposed [6, 7]. In the picture that we have described, inequality (19) is fundamentally linked to the impossibility of producing a diagonal matrix $\rho_{X'Q'A'}$ with a single U_{QA} which prevents $S(X'{:}Q'|A')$ from vanishing for an ensemble of non-commuting ρ_i.

Note that the physical model of measurement used here [10] is truly minimal: no environment is necessary *a priori*. If coupling to an environment E *is* used in the description of measurement as in [8] for diagonalizing $\rho_{X'Q'A'}$ (using decoherence as a means of selecting a "pointer basis" [16]), part of the information may flow out to this environment. In a sense, E then plays the role of another ancilla and its state after measurement can still contain some additional information about X, i.e. $S(X'{:}E'|Q'A')$ could be non-vanishing. As the environment is by definition uncontrollable, this information can be considered to be irrecoverably lost: $S(X'{:}Q'A') \leq S(X{:}Q)$. As a consequence we obtain a bound [*cf.* Eq. (13)]

$$S(X'{:}A') \leq S(X{:}Q) - S(X'{:}Q'|A') \ . \qquad (20)$$

The mutual conditional entropy $S(X'{:}Q'|A')$ can be calculated explicitly in the decoherence picture using the diagonal matrix

$$\rho_{X'Q'A'} = \sum_{i,\alpha} p_i |x_i\rangle\langle x_i| \otimes P_\alpha \rho_i P_\alpha \otimes |\alpha\rangle\langle\alpha| \ . \qquad (21)$$

giving

$$S(X'{:}Q'|A') = \sum_\alpha p_\alpha \left[S\left(\sum_i p_{i|\alpha}\rho_{\alpha i}\right) - \sum_i p_{i|\alpha} S(\rho_{\alpha i})\right] \qquad (22)$$

where $p_\alpha = \mathrm{Tr}(P_\alpha\rho)$, $p_{i|\alpha} = p_i p_{\alpha|i}/p_\alpha$, and $\rho_{\alpha i} = P_\alpha\rho_i P_\alpha/p_{\alpha|i}$ is the density matrix obtained after measuring α on state ρ_i. (The right hand side of Eq. (22) is the quantity $\sum_\alpha p_\alpha \chi_\alpha^{(Q)}$ of Ref. [8].)

Let us consider now the extension of Holevo's theorem to many sequential measurements. This is a generalization of the treatment of consecutive measurements of *pure* states that was presented in [10]. To that effect, let m ancillae $A_1, \cdots, A_m$ interact successively with Q via unitary evolutions such as Eq. (14) with projectors $P_{\alpha_1}\cdots P_{\alpha_m}$. The notation A_j corresponds to the j-th ancilla at time j or later (i.e., when the j first ancillae have interacted unitarily with Q). As previously, unitarity implies

$$S(X_m{:}Q_m A_1\cdots A_m) = S(X{:}Q) \ , \qquad (23)$$

where X_m and Q_m are the preparer and the quantum state after m interactions. Making use of

$$S(X_m{:}Q_m A_1\cdots A_m) = S(X_m{:}A_1\cdots A_m) + S(X_m : Q_m|A_1\cdots A_m) \qquad (24)$$

we arrive at $S(X_m{:}A_1\cdots A_m) \leq S(X{:}Q)$. Arguing like before, ignoring the non-diagonal matrix elements of $\rho_{XA_1\cdots A_m}$ yields a Shannon mutual entropy $H(X{:}A_1\cdots A_m)$ based on the conditional probabilities

$$p_{\alpha_1\cdots\alpha_m|i} = \mathrm{Tr}\left(P_{\alpha_1}\cdots P_{\alpha_m}\rho_i P_{\alpha_m}\cdots P_{\alpha_1}\right) \qquad (25)$$

bounded by the corresponding quantum mutual entropy. Subsequently using the chain relations for classical entropies, we have the basic upper bound on the *sum* of accessible informations

$$\sum_{j=1}^m H(X{:}A_j|A_1\cdots A_{j-1}) \leq S(X{:}Q) \qquad (26)$$

where $H(X_m{:}A_1|\emptyset) \equiv H(X_m{:}A_1)$. Eq. (26) generalizes Holevo's theorem and emphasizes that the outcome of every measurement is *conditional* on *all* previous outcomes.

Finally, inequality (19) can be shown to be a special case of relation (2). Indeed, for a general density matrix ρ_{XY} describing a bipartite quantum system whose components interact with ancillae A and B that define bases $|x\rangle$ and $|y\rangle$ respectively, we have $S(A'{:}B') = H(X{:}Y)$, the Shannon mutual entropy of the joint probability $p_{xy} = \langle x,y|\rho_{XY}|x,y\rangle$. Using

$$\begin{aligned} S(X{:}Y) &= S(X'A'{:}Y'B') \\ &= S(A'{:}B') + S(A'{:}Y'|B') + S(X'{:}Y'B'|A') \end{aligned} \qquad (27)$$

and the non-negativity of conditional mutual entropies yields $H(X{:}Y) \leq S(X{:}Y)$.

We wish to acknowledge C. Caves, C. Fuchs, and A. Peres for very useful discussions. This research was supported in part by the NSF under Grant Nos. PHY 94-12818, PHY94-20470 at Caltech and PHY 94-07194 at the ITP at Santa Barbara.

[1] A.S. Holevo, Probl. Inform. Transmission **9**, 110 (1973).
[2] C.E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948); *ibid.* **27**, 623 (1948).
[3] L.B. Levitin, in *Proc. of the 4th All-Union Conf. on Information and Coding Theory* (Moscow-Tashkent, Tashkent, 1969).
[4] H.P. Yuen and M. Osawa, Phys. Rev. Lett. **70**, 363 (1993).
[5] R. Josza, D. Robb, and W.K. Wootters, Phys. Rev. **A 49**, 668 (1994).
[6] C. Caves and A. Fuchs, Phys. Rev. Lett. **73**, 3047 (1994).
[7] A. Fuchs, Ph.D. Thesis, quant-ph/9601020.
[8] B. Schumacher, M. Westmoreland, and W.K. Wootters, Phys. Rev. Lett. **76**, 3452 (1996).
[9] N.J. Cerf and C. Adami, Phys. Rev. Lett. **79**, 5194 (1997).
[10] N.J. Cerf and C. Adami, e-print quant-ph/9605002.
[11] R.B. Ash, *Information Theory* (Dover, New York, 1965).
[12] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).
[13] N.J. Cerf and C. Adami, Phys. Rev. **A 55**, 3371 (1997).
[14] C. Adami and N.J. Cerf, Phys. Rev. **A 56**, 3470 (1997).
[15] A. Peres, *Quantum Theory: Concepts and Methods*, (Kluwer, Dordrecht, 1993).
[16] W.H. Zurek, Phys. Rev. **D 26**, 1862 (1982).