PHYSICAL REVIEW
LETTERS

VOLUME 75 | 31 JULY 1995 | NUMBER 5

Lower Bound for Mutual Information of a Quantum Channel

H. Scutaru*

Department of Theoretical Physics, Institute of Atomic Physics, POB MG-6, Bucharest-Magurele, Romania
(Received 10 November 1994; revised manuscript received 17 April 1995)

We obtain a lower bound for the mutual information of a quantum transmission channel, which is perfectly analogous with Holevo's upper bound. The Uhlmann inequality for relative entropies is used, in a reverted order, for a completely positive mapping related with the mixed coherent states introduced by us seventeen years ago. Possible applications to quantum cryptography are discussed.

PACS numbers: 03.65.Bz, 05.90.+m, 42.50.Dv

In this paper we show that, as a manifestation of the uncertainty principle, the possible amount of information transfer via a quantum channel is bounded below through an expression containing quantum entropies of some quantum states associated to the quantum channel [1–9]. The fact that the mutual information of a quantum channel cannot be arbitrarily small is a completely new result which reflects the quantum nature of the transmission channel. This fact is important in the quantum cryptography where the problem of the vanishing of the mutual information is often considered (see example 1 given below). The lower bounds obtained until now are only for the accessible information of a quantum channel. In example 2 given below a quantum system is found where the mutual information happens to be equal with the subentropy [4] (and hence with the accessible information) which gives a lower bound for the accessible information. Only for this particular case is the subentropy bigger than our lower bound.

Twenty years ago, Holevo [1] obtained the first result of this kind: an upper bound for the mutual information of a quantum channel. Recently, Yuen and Ozawa [2] generalized Holevo's result for quantum channels with input and output alphabets described by any measure space.

Let (X, Σ, m) be a measure space [3] which describes the input alphabet and (Y, Ξ, μ) a measure space which describes the output alphabet. For simplicity we shall suppose that X and Y are compact spaces.

We stipulate [4–6] the *a priori* probability density $p_i(x)$ standing for the initial information available about the symbol x. The Shannon information for the input alphabet is [4–6]

$$I_i = \int_X p_i(x) \ln p_i(x)\, dm(x). \tag{1}$$

When the input symbol $x \in X$ is transmitted, the output symbol $y \in Y$ is registered with the (conditional) probability $p(y|x)$. This conditional probability is central to the study of information transmission and characterizes the transmission channel.

To obtain the *a posteriori* probability $p_f(y)$ we employ the Bayes rule [4–6]

$$p(x|y)\, p_f(y) = p(x,y) = p(y,x) = p(y|x)\, p_i(x), \tag{2}$$

where $p(x,y) = p(y,x)$ is the joint probability distribution for the input and output alphabets. The final information is given by [5]

$$I_f = \int_X p(x|y) \ln p(x|y)\, dm(x). \tag{3}$$

The information gain for the outcome y is thus [5]

$$\Delta I(y) = I_f(y) - I_i. \tag{4}$$

The expected information gain is then given by

$$\langle \Delta \mathbf{I} \rangle = \int_X \int_Y p(y,x) \ln\left[\frac{p(y,x)}{p_f(y)\, p_i(x)}\right] d\mu(y)\, dm(x). \tag{5}$$

0031-9007/95/75(5)/773(4)$06.00

This is called [1–9] the mutual information (or correlation information) of the joint distribution $p(y,x)$. This quantity is non-negative, and it is zero if and only if $p(y,x) = p_f(y)\, p_i(x)$, i.e., if and only if the variables x and y are independent. Independent variables provide no information about each other. The mutual information can also be given as the mean value of the relative entropies:

$$S(p(\cdot|x)|\, p_f) = \int_Y p(y|x)\, \ln\left[\frac{p(y|x)}{p_f(y)}\right] d\mu(y) \quad (6)$$

and

$$S(p(\cdot|y)|\, p_i) = \int_X p(x|y)\, \ln\left[\frac{p(x|y)}{p_i(x)}\right] dm(x), \quad (7)$$

i.e.,

$$\langle \Delta \mathbf{I} \rangle = \int_X S(p(\cdot|x)|\, p_f)\, p_i(x)\, dm(x) = \int_Y S(p(\cdot|y)|\, p_i)\, p_f(y)\, d\mu(y). \quad (8)$$

The quantum transmission channel is a quantum system with the Hilbert space H [1–9]. The modulation, transmission, and noise are described by a mapping $x \to \rho_x$ where ρ_x is a density operator on H. The user determines the state ρ_x through the result of a quantum measurement. A quantum measurement will be described by a positive operator valued function defined on $Y, y \to A(y)$, with $A(y)$ a decomposition of the identity operator I on H:

$$\int_Y A(y)\, d\mu(y) = I. \quad (9)$$

Then we have

$$p(y|x) = \mathrm{Tr}[A(y)\, \rho_x], \quad (10)$$

and from (9) it follows that

$$\int_Y p(y|x)\, d\mu(y) = 1. \quad (11)$$

From (10) and from (2) we obtain

$$p_f(y) = \int_X p(y|x)\, p_i(x)\, dm(x) = \mathrm{Tr}[A(y)\, \rho], \quad (12)$$

where the density operator ρ, which is called in [2] the mixture of parametrized states ρ_x, is defined by

$$\rho = \int_X p_i(x)\, \rho_x\, dm(x). \quad (13)$$

As was remarked in [2] the decomposition of the identity $A(y)$ defines a completely positive map $\Phi : C(Y) \to B(H)$ by

$$\Phi(f) = \int_Y f(y) A(y)\, d\mu(y), \quad (14)$$

where $C(Y)$ is the C^* algebra of complex valued continuous functions on Y. This map preserves the identity

$$\Phi(1) = I. \quad (15)$$

Then from (8) and from Uhlmann's inequality [10] one obtains Holevo's upper bound for the mutual information [1,2]

$$\langle \Delta \mathbf{I} \rangle \le S(\rho) - \int_X p_i(x)\, S(\rho_x)\, dm(x). \quad (16)$$

In the present paper we use also Uhlmann's inequality but in the case of a completely positive map $\Psi : B(H) \to C(X)$ defined by

$$\Psi(b)(x) = \mathrm{Tr}(b\rho_x). \quad (17)$$

Evidently this is an identity preserving map [$\Psi(I) = 1$]. The dual map $\Psi^* C(X)^* \to B(H)^*$ between the state spaces of the C^* algebras $C(X)$ and $B(H)$ is defined [11,12] (see also [13–15]) by

$$\Psi^*(h) = \int_X h(x)\, \rho_X\, dm(x). \quad (18)$$

We remark that $\rho = \Psi^*(p_i)$. The role played in [2] by the parametrized states ρ_x will be taken by the states σ_y defined by

$$\sigma_y = \int_X p(x|y)\, \rho_x\, dm(x) = \Psi^*(p(\cdot|y)). \quad (19)$$

The fact that $\mathrm{Tr}\sigma_y = 1$ follows from $\mathrm{Tr}\rho_x = 1$. Also it is easy to see that

$$\rho = \int_X \rho_x p_i(x)\, dm(x) = \int_Y \sigma_y p_f(y)\, d\mu(y). \quad (20)$$

From Uhlmann's inequality we have

$$S(\sigma_y|\rho) = S(\Psi^*(p(\cdot|y))|\Psi^*(p_i)) \le S(p(\cdot|y)|p_i), \quad (21)$$

and combining this inequality with (8) we obtain the announced lower bound for the mutual information

$$\langle \Delta \mathbf{I} \rangle \ge \int_Y p_f(y)\, S(\sigma_y|\rho)\, d\mu(y). \quad (22)$$

Because the relative entropy is given by

$$S(\sigma_y|\rho) = \mathrm{Tr}[\sigma_y \ln\sigma_y - \sigma_y \ln\rho], \quad (23)$$

it follows that

$$\langle \Delta \mathbf{I} \rangle \ge S(\rho) - \int_Y p_f(y)\, S(\sigma_y)\, d\mu(y). \quad (24)$$

The equality is attained if and only if the map Ψ is a C^* homomorphism [12]. This is possible if and only if the measure spaces (X, Σ, m) and (Y, Ξ, μ) are purely atomic [12].

Example 1: In this case the initial states $\{|\psi_k\rangle, k \in X\}$ are orthogonal states which give an orthogonal decomposition of the unit operator I on H:

$$\sum_{k=1}^{n} |\psi_k\rangle\langle\psi_k| = I, \tag{25}$$

where $n = \dim H$ and

$$\rho = \sum_{k=1}^{n} p_i(k)|\psi_k\rangle\langle\psi_k|. \tag{26}$$

So $\{p_i(k); k = 1, \ldots, n\}$ are the eigenvalues of the density operator ρ and

$$S(\rho) = -\sum_{k=1}^{n} p_i(k) \ln p_i(k). \tag{27}$$

Also we have

$$\sigma_j = \sum_{k=1}^{n} p(k|j)\,|\psi_k\rangle\langle\psi_k| \tag{28}$$

and

$$S(\sigma_j) = -\sum_{k=1}^{n} p(k|j) \ln p(k|j). \tag{29}$$

Hence the equality is attained in (24) and in this case

$$\langle \Delta \mathbf{I} \rangle = S(\rho) - \sum_{j=1}^{n} p_f(j)\, S(\sigma_j). \tag{30}$$

The vanishing of this lower bound is obtained when $p_f(j) = 1/n$ and $S(\sigma_j) = S(\rho)$, for any $j = 1, \ldots, n$. In this situation we also have $p(k|j) = p(j|k) = 1/n$, i.e., the bases $\{|\psi_k\rangle\}$ and $\{|\alpha_j\rangle\}$ are conjugated [16] or mutually unbiased [17]. The corresponding density operators are given by $\rho = I/n$ and $\sigma_j = I/n$.

Example 2: Another very interesting example is that given by the following situation: The Hilbert space H is a finite dimensional space with $\dim H = n$ and X is the homogeneous manifold $\mathrm{U}(n)/\mathrm{U}(n-1)$ with the unique invariant measure dm induced by the unique Haar measure on $\mathrm{SU}(n)$ [6]. We denote the element $x \in X$ by the corresponding element $|\psi\rangle \in H$. We shall take

$$\rho_\psi = |\psi\rangle\langle\psi| \tag{31}$$

and the condition

$$\int_X \rho_\psi \, dm(\psi) = I \tag{32}$$

is satisfied [11,12]. Let $\{\phi_1, \ldots, \phi_n\}$ be a basis in H and $A(j) = |\phi_j\rangle\langle\phi_j|$ the corresponding positive operator valued measure (POM). Then $p(j|\psi) = |\langle\phi_j|\,\psi\rangle|^2$. Let us suppose that $p_i(\psi) = 1/n$. Then $p(j, \psi) = p(j|\psi)/n = p(\psi, j)$, $p_f(j) = 1/n$, and $p(\psi|j) = p(j|\psi)$. The density operator $\sigma_j = \int_X \mathrm{Tr}[A(j)\,\rho_\psi]\,\rho_\psi \, dm(\psi)$ is called in [6] the unique density operator estimator assigned to ϕ_j (we take N from [6] equal to 1). The mutual information is given [6] by

$$\langle \Delta \mathbf{I} \rangle = -\sum_{j=1}^{n} p_f(j) \ln p_f(j) + \sum_{j=1}^{n} \int_X \mathrm{Tr}[A(j)\,\rho_\psi] \ln \mathrm{Tr}[A(j)\,\rho_\psi] \, dm(\psi). \tag{33}$$

Because $\mathrm{Tr}[A(j)\,\rho_\psi]$ and $p_f(j) = \mathrm{Tr}[A(j)\,\rho]$ are, respectively, the contravariant and the covariant symbols of $A(j)$ and ρ [12], we have from Theorem 3 of [12] that $S(\rho) \le -\sum_{j=1}^{n} p_f(j) \ln p_f(j) = \ln(n)$ and $-S(\sigma_j) \le \int_X \mathrm{Tr}[A(j)\,\rho_\psi] \ln \mathrm{Tr}[A(j)\,\rho_\psi] \, dm(\psi) = -(1/n)[\frac{1}{2} + \cdots + (1/n)]$. Hence

$$\langle \Delta \mathbf{I} \rangle = \ln(n) - \left(\frac{1}{2} + \cdots + \frac{1}{n}\right) \ge S(\rho) - \sum_{j=1}^{n} p_f(j)\, S(\sigma_j). \tag{34}$$

But using the concept of subentropy $Q(\rho)$ defined in [4] we can rewrite this result in the following form:

$$\langle \Delta \mathbf{I} \rangle = Q(\rho) \ge S(\rho) - \sum_{j=1}^{n} p_f(j)\, S(\sigma_j), \tag{35}$$

i.e., our lower bound is smaller than the subentropy $Q(\rho)$ which gives a lower bound for the accessible information defined as the maximum of the mutual information over all POMs [4]. The result is valid only for this example in which the mutual information happens to be equal with the subentropy.

Finally, we shall illustrate how the above estimation can be useful in quantum cryptography. The quantum channels with zero mutual information are considered in connection with the problem of optimal security. But the vanishing of the lower bound is a necessary condition for the vanishing of the mutual information. The lower bound is equal to the difference between the entropy of a convex combination of states and the same convex combination of the entropies of these states. This difference vanishes only in the case when the density operators describing these states are the same [18]. Hence the lower bound is equal to zero only when $p_i(x) = p(x|y)$. Then $p(y|x) = p_f(y)$ and $p(x, y) = p(y, x) = p_i(x)\,p_f(y)$, i.e., the variables x and y are independent and $\langle \Delta I \rangle = 0$. Conversely, from the vanishing of the mutual information it follows that the variables x and y are independent, and then relation $p(x|y) = p_i(x)$ holds. A particular solution of these equations was given in example 1. In general, these conditions are very effective and bring a new light to the problem of the vanishing of the mutual information. Indeed, an eavesdropper may cause the vanishing of the mutual information flow, in spite of the fact that the lower bound is not equal to zero,

and exactly this disturbance allows the detection of the presence of this unauthorized user.

*Electronic address: scutaru@ifa.ro

[1] A. S. Holevo, Problemy Peredachi Informacii **9**, 31 (1973).
[2] H. P. Yuen and M. Ozawa, Phys. Rev. Lett. **70**, 363 (1993).
[3] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[4] R. Jozsa, D. Robb, and W. K. Wootters, Phys. Rev. A **49**, 668 (1994).
[5] K. R. W. Jones, Phys. Scr. **T48**, 100 (1993).
[6] K. R. W. Jones, Ann. Phys. (N.Y.) **207**, 140 (1991).
[7] A. S. Holevo, Problemy Peredachi Informacii **9**, 3 (1973).
[8] A. S. Holevo, Problemy Peredachi Informacii **15**, 31 (1979).
[9] A. S. Holevo, Rep. Math. Phys. **12**, 273 (1977).
[10] A. Uhlmann, Commun. Math. Phys. **54**, 21 (1977).
[11] H. Scutaru, Lett. Math. Phys. **2**, 101 (1977).
[12] H. Scutaru, Rep. Math. Phys. **15**, 79 (1979).
[13] S. T. Ali, Riv. Nuovo Cimento Soc. Ital. Fis. **9**, 1 (1985).
[14] A. Amann, J. Math. Phys. (N.Y.) **27**, 2282 (1986).
[15] A. S. Holevo, *Itoghi Nauki i Tehnichi* (English translation: *Quantum Probability and Quantum Statistics*) (VINITI, Moscow, 1991), Vol. 83.
[16] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. A **48**, 96 (1993).
[17] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[18] G. Lindblad, Commun. Math. Phys. **33**, 305 (1973).