Holevo Bound

Formal statement

Let

$$\mathcal{E} = \{p_x, \rho_x\}_{x \in \mathcal{X}}$$

be a finite quantum ensemble. This means that a classical label x is chosen with probability pₓ, and the receiver is given the quantum state ρₓ on a finite-dimensional Hilbert space mathcal H(B). The receiver does not see x directly. The receiver only receives the quantum system and may perform a measurement in order to learn something about x.

For a POVM M(y)\(y∈mathcal Y), the conditional probability of measurement outcome y given label x is

$$p(y|x) = \mathrm{Tr}(M_y \rho_x).$$

This produces an ordinary classical joint distribution

$$p(x, y) = p_x \, \mathrm{Tr}(M_y \rho_x).$$

The mutual information between the input label X and the measurement result Y is I(X;Y). The accessible information of the ensemble is

$$I_{\mathrm{acc}}(\mathcal{E}) = \max_{\{M_y\}} I(X; Y),$$

where the maximum is over all POVMs on mathcal H(B).

Define the average state

$$\bar{\rho} = \sum_x p_x \rho_x.$$

The Holevo quantity of the ensemble is

$$\chi(\mathcal{E}) = S(\bar{\rho}) - \sum_x p_x S(\rho_x),$$

where

$$S(\rho) = -\operatorname{Tr}(\rho \log \rho)$$

is the von Neumann entropy. Unless stated otherwise, logarithms are base two, so information is measured in bits.

The Holevo bound says that

$$I_{\mathrm{acc}}(\mathcal{E}) \leq \chi(\mathcal{E})$$

or equivalently, for every measurement M(y)\,

$$I(X;Y) \leq S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x).$$

This is the theorem usually meant by the statement that the classical information extractable from a quantum ensemble is bounded by the Holevo quantity. Holevo's original 1973 paper proved a bound of this form for information transmitted by a quantum communication channel, and modern quantum-information texts present it as the standard upper bound on accessible information.

The operational problem

The theorem answers the following question. Alice has a classical random variable X. Instead of sending X directly, she encodes each value x into a quantum state ρ_x. Bob receives the quantum system and chooses a measurement. After the measurement, Bob has a classical outcome Y. How much classical information about X can Bob obtain?

The tempting but wrong answer is: perhaps the quantum state can hide an arbitrarily large amount of classical information, because a quantum state is described by many continuous parameters. The Holevo bound says no. The extractable classical information is not controlled by the number of real parameters used to describe the density matrix. It is controlled by an entropy difference:

$$\chi = S(\bar{\rho}) - \sum_x p_x S(\rho_x).$$

The first term measures the entropy of the average state Bob receives before knowing x. The second term subtracts the average entropy already present inside the conditional states. What remains is the amount of correlation between the classical label and the quantum system.

The right mental image is this. Before measurement, Bob does not have a classical random variable that directly reveals x. He has a quantum memory B correlated with X. A measurement is a quantum-to-classical channel B→ Y. The Holevo bound says that no measurement can create more classical correlation with X than the correlation already present between X and the quantum system B.

The classical-quantum state viewpoint

The cleanest way to understand the theorem is to package the ensemble into a classical-quantum state

$$\omega_{XB} = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_x.$$

Here X is a classical register storing the label, and B is the quantum system given to Bob. The marginal states are

$$\omega_X = \sum_x p_x |x\rangle\langle x|, \qquad \omega_B = \bar{\rho} = \sum_x p_x \rho_x.$$

Because ω_{XB} is block diagonal in the classical register X, its entropy is

$$S(\omega_{XB}) = H(X) + \sum_x p_x S(\rho_x),$$

where $H(X)=-\sum_x p_x \log p_x$ is the Shannon entropy of the classical label. The quantum mutual information between X and B is

$$I(X;B)_\omega = S(\omega_X) + S(\omega_B) - S(\omega_{XB}).$$

Substituting the three entropy expressions gives

$$\begin{aligned} I(X;B)_\omega &= H(X) + S(\bar{\rho}) - \left(H(X) + \sum_x p_x S(\rho_x) \right) \\ &= S(\bar{\rho}) - \sum_x p_x S(\rho_x) \\ &= \chi(\mathcal{E}). \end{aligned}$$

So the Holevo quantity is not an arbitrary expression. It is exactly the mutual information between the classical label X and the quantum system B, before Bob measures.

Proof

Fix an arbitrary POVM M(y)\. This measurement defines a quantum-to-classical channel

$$\mathcal{M}(\tau) = \sum_y \mathrm{Tr}(M_y \tau) |y\rangle\langle y|.$$

Applying this measurement channel to the B register of ω(XB) gives the classical-classical state

$$\omega_{XY} = (I_X \otimes \mathcal{M})(\omega_{XB}) = \sum_{x,y} p_x \,\mathrm{Tr}(M_y \rho_x) |x\rangle\langle x| \otimes |y\rangle\langle y|.$$

This state is just the ordinary joint probability distribution of the input label X and the measurement outcome Y. Its mutual information is the classical mutual information I(X;Y).

Now we use the data-processing principle for mutual information. A local channel acting on B cannot increase its mutual information with X. Since measurement is a channel B→ Y, we have

$$I(X;Y)_\omega \leq I(X;B)_\omega.$$

But we already computed

$$I(X;B)_\omega = \chi(\mathcal{E}).$$

Therefore, for this measurement,

$$I(X;Y) \le \chi(\mathcal{E}).$$

Since the POVM was arbitrary, maximizing over all POVMs gives

$$I_{\mathrm{acc}}(\mathcal{E}) = \max_{\{M_y\}} I(X;Y) \le \chi(\mathcal{E}).$$

This proves the Holevo bound.

The same proof can be written using relative entropy. The mutual information of a bipartite state is

$$I(A;B)_\rho = D(\rho_{AB} \| \rho_A \otimes \rho_B),$$

where D(·\|·) is quantum relative entropy. The measurement channel maps ω(XB) to ω(XY), and monotonicity of relative entropy under channels gives

$$D(\omega_{XY} \| \omega_X \otimes \omega_Y) \le D(\omega_{XB} \| \omega_X \otimes \omega_B).$$

The left-hand side is I(X;Y), and the right-hand side is χ(mathcal E). This is the standard modern proof.

Why the theorem is not just “one qubit gives one bit”

A famous consequence is that transmitting n qubits alone cannot reveal more than n classical bits. Indeed, if all states ρₓ live in a d-dimensional Hilbert space, then

$$\chi(\mathcal{E}) = S(\bar{\rho}) - \sum_x p_x S(\rho_x) \le S(\bar{\rho}) \le \log d.$$

For n qubits, d=2ⁿ, so

$$\chi(\mathcal{E}) \le n.$$

Therefore

$$I_{\mathrm{acc}}(\mathcal{E}) \leq n.$$

This statement must be interpreted correctly. It says that if Bob only receives an n-qubit system, then the classical information he can extract from that received system is at most n bits. It does not forbid protocols such as superdense coding, because in superdense coding Bob also possesses prior entanglement. The relevant output system available to Bob is then larger than the transmitted qubits alone.

Example: orthogonal pure states

Suppose Alice sends one of several orthogonal pure states:

$$\rho_x = |x\rangle\langle x|,$$

with probabilities pₓ. Then

$$S(\rho_x) = 0$$

for every x, and

$$\bar{\rho} = \sum_x p_x |x\rangle\langle x|.$$

The entropy of barρ is the Shannon entropy of the probability distribution:

$$S(\bar{\rho}) = H(X).$$

Thus

$$\chi = H(X).$$

This bound is achievable. Bob measures in the orthonormal basis \|x⟩\ and learns x perfectly. Therefore

$$I_{\mathrm{acc}} = H(X) = \chi.$$

This is the classical case embedded inside quantum theory. Orthogonal states behave like perfectly distinguishable classical symbols.

Example: identical states

Suppose all labels are encoded into the same state:

$$\rho_x = \rho$$

for every x. Then

$$\bar{\rho} = \rho,$$

so

$$\chi = S(\rho) - \sum_x p_x S(\rho) = S(\rho) - S(\rho) = 0.$$

The Holevo bound gives

$$I_{\mathrm{acc}} = 0.$$

This is exactly right. If the received quantum state is independent of the label, then no measurement can reveal anything about the label.

Example: commuting mixed states

Suppose the states commute, so they are diagonal in a common basis:

$$\rho_x = \sum_z p(z|x)|z\rangle\langle z|.$$

Then the average state is

$$\bar{\rho} = \sum_z p(z)|z\rangle\langle z|, \qquad p(z) = \sum_x p_x p(z|x).$$

The Holevo quantity becomes

$$\chi = H(Z) - \sum_x p_x H(Z|X=x) = I(X;Z).$$

Bob can achieve this value by measuring in the common eigenbasis \|z⟩\. Therefore, for commuting ensembles,

$$I_{\mathrm{acc}} = \chi.$$

This example is important because it shows that the Holevo bound reduces to ordinary classical mutual information when the quantum states are simultaneously diagonalizable. The genuinely quantum difficulty appears when the states do not commute.

Example: two nonorthogonal pure states

Let Alice choose between

$$|0\rangle \qquad \text{and} \qquad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

with equal probabilities. The ensemble is

$$\mathcal{E} = \left\{ \frac{1}{2}, |0\rangle\langle 0|; \frac{1}{2}, |+\rangle\langle +| \right\}.$$

Since both states are pure,

$$S(|0\rangle\langle 0|) = S(|+\rangle\langle +|) = 0.$$

Therefore

$$\chi = S(\bar{\rho}),$$

where

$$\bar{\rho} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|.$$

For two equally likely pure states with overlap

$$c = |\langle\psi|\phi\rangle|,$$

the average state has eigenvalues

$$\frac{1+c}{2}, \qquad \frac{1-c}{2}.$$

Here

$$c = |\langle 0|+\rangle| = \frac{1}{\sqrt{2}}.$$

Thus

$$\chi = h_2\left(\frac{1+1/\sqrt{2}}{2}\right) \approx 0.6009 \text{ bits},$$

where h_2 is the binary entropy function.

The label X itself contains one full bit before encoding, because the two labels are equally likely. But Bob cannot extract one full bit from one copy, because the two possible quantum states are not orthogonal. The Holevo bound says that no measurement can extract more than about 0.6009 bits of mutual information.

This example captures the core quantum phenomenon. Nonorthogonal states can carry classical labels, but those labels are not perfectly readable.

Example: a noisy mixed-state ensemble

Consider the ensemble

$$\mathcal{E} = \left\{\frac{1}{2}, |0\rangle\langle 0|; \frac{1}{2}, \frac{I}{2}\right\}.$$

The average state is

$$\bar{\rho} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}\frac{I}{2} = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}.$$

Therefore

$$S(\bar{\rho}) = h_2(3/4) \approx 0.8113 \text{ bits}.$$

The first state is pure, so its entropy is zero. The second state is maximally mixed, so its entropy is one bit. Hence

$$\sum_x p_x S(\rho_x) = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 1 = \frac{1}{2}.$$

Thus

$$\chi \approx 0.8113 - 0.5 = 0.3113 \text{ bits}.$$

This example shows why the second term in the Holevo quantity matters. The average state has entropy about 0.8113 bits, but not all of that entropy is useful for learning the label. Some of it is intrinsic noise inside the conditional state I/2. The Holevo quantity subtracts this average internal entropy.

When the bound is tight and when it is not

The Holevo bound is tight for ensembles of commuting states, because Bob can measure in their common eigenbasis and reduce the problem to a classical one. It is also tight for orthogonal pure-state ensembles, which are a special commuting case after choosing the basis of orthogonal code states.

For noncommuting ensembles, the bound is often not exactly attainable by a single-copy measurement. The Holevo quantity measures the total classical-quantum correlation I(X;B), but a measurement may fail to convert all of that correlation into classical mutual information I(X;Y). The gap between accessible information and Holevo information is a real phenomenon in quantum information theory.

In channel coding, however, the Holevo quantity appears again in an asymptotic setting. By using long block codes and collective measurements, one can often approach rates governed by optimized Holevo information. This leads to the Holevo-Schumacher-Westmoreland theorem for the classical capacity of classical-quantum channels. That is a different theorem from the one-copy accessible-information bound, but it is built from the same quantity.

How to use the theorem

When you are given an ensemble $p_x,\rho_x\$, first compute the average state

$$\bar{\rho} = \sum_x p_x \rho_x.$$

Then compute the entropy of the average state and subtract the average entropy of the signal states:

$$\chi = S(\bar{\rho}) - \sum_x p_x S(\rho_x).$$

The result is an upper bound on the mutual information produced by any measurement:

$$I(X;Y) \leq \chi.$$

If the states commute, the bound is achievable by measuring in the common eigenbasis. If the states are pure, the second term vanishes, and the bound becomes

$$\chi = S(\bar{\rho}).$$

If the Hilbert space dimension is d, then

$$\chi \leq \log d,$$

so a d-dimensional quantum system cannot reveal more than log d bits of classical information without additional resources.

Common mistakes

A common mistake is to say that n qubits cannot contain more than n bits of information in any sense. A pure quantum state can require many continuous parameters to describe, and quantum systems can be correlated with other systems in ways that are not classical. The Holevo bound says something more precise: from an n-qubit system alone, the amount of classical mutual information that can be extracted about a classical label is at most n bits.

A second mistake is to confuse χ with the accessible information itself. The theorem says

$$I_{\mathrm{acc}} \leq \chi.$$

The inequality may be strict.

A third mistake is to forget the average entropy term. For pure-state ensembles,

$$\chi = S(\bar{\rho}),$$

but for mixed-state ensembles, the correct expression is

$$\chi = S(\bar{\rho}) - \sum_x p_x S(\rho_x).$$

The subtraction removes entropy that was already present inside the conditional states and therefore does not represent information about the classical label.

A fourth mistake is to ignore the measurement. The ensemble may mathematically encode labels into states, but Bob obtains classical data only after choosing a POVM. The Holevo bound limits the best possible classical mutual information after that measurement.

Final mental image

The Holevo bound says that a quantum ensemble contains classical information in a very specific operational sense. The classical label X is correlated with a quantum system B. Before measurement, the amount of correlation is

$$I(X;B) = \chi.$$

A measurement converts B into a classical outcome Y. Data processing says this conversion cannot increase correlation with X. Therefore

$$I(X;Y) \leq I(X;B) = \chi.$$

So the Holevo quantity is the classical-quantum correlation available before measurement, and the accessible information is the largest classical-classical correlation obtainable after measurement. The theorem says that measurement can reveal at most the correlation that was already there.

In one sentence:

$$\text{extractable classical information} \leq \text{classical-quantum mutual information of the}$$

That is the operational meaning of the Holevo bound.

References

Holevo, Alexander S. “Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel.” Problems of Information Transmission 9, no. 3 (1973): 177–183.

Holevo, Alexander S. Probabilistic and Statistical Aspects of Quantum Theory. North-Holland, 1982; Springer reprint, 2011.

Nielsen, Michael A., and Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 10th anniversary edition, 2010. See Section 12.1.1 on the Holevo bound.

Watrous, John. The Theory of Quantum Information. Cambridge University Press, 2018. See the treatment of Holevo information, accessible information, and related entropy inequalities.

Watrous, John. “Lecture 12: Holevo’s theorem and Nayak’s bound.” CS 766/QIC 820 Theory of Quantum Information, University of Waterloo, 2011.

Wilde, Mark M. Quantum Information Theory. Cambridge University Press, 2nd edition, 2017; see also From Classical to Quantum Shannon Theory lecture notes.

Schumacher, Benjamin, and Michael D. Westmoreland. “Sending Classical Information via Noisy Quantum Channels.” Physical Review A 56, no. 1 (1997): 131–138.

Document information

Holevo Bound

Project	[QIT 002] State Distinguishability and Measurement Theorems
Document	Primary document
Author	mujirin
Verifier	Not verified
Downloaded	July 03, 2026 19:13 KST
Status	Working
Document link	https://theorytrace.com/projects/state-distinguishability-and-measurement-theorems/documents/untitled-document/