Holevo bound

The measurement postulate implies that the von Neumann entropy corresponds exactly to the entropy of the random variable that is the result of the measurement of a given mixed state in the basis of its eigenvectors. However, as we have already said, a „properly“ defined entropy should take into account all possible measurements. The random variable about which we are trying to obtain information by measurement is the random variable with the distribution defining an ensemble of states. The exact relation of von Neumann entropy to the information obtainable by arbitrary measurements is unknown. The most important result in this respect is the so-called Holevo bound.

Věta (Holevo bound). Let X be a discrete random variable with distribution $\Pr[X = i] = p_i$. Let $\rho = \sum_{i=1}^{n} p_i \rho_i$ be a mixed state generated by encoding the value of X using the states of ρ_i. Let Y be the random variable of the results of some measurement of the state ρ. Then

$$I(X:Y) \leq S(\rho) - \sum_{i=1}^{n} p_i S(\rho_i)\,.$$

Holevo bound says that the von Neumann entropy is an upper estimate for the information available by any measurement of the random variable X. If all states of ρ_i are pure, then the inequality has the form $I(X:Y) \leq S(\rho)$. Moreover, we know that $S(\rho) \leq H(X)$, which gives the classical $I(X:Y) \leq H(X)$.

The equality $S(\rho) = H(X)$ occurs precisely when the states are pure and distinguishable. Then it is a classical random variable, it is not important that we understand its values as quantum states. Then also $I(X:Y) = H(X)$ for measurements in the basis containing the chosen states, when $Y = X$.

For the proof of the Holevo bound, consider, in addition to the prepared and measured system denoted by Q, two additional systems. A system P, containing information about the value of the random variable X encoded in basis states, and a system M containing in turn the similarly encoded result Y of the measurement given by the operators (M_j). After preparation, the density matrix of this composite system is

$$\rho_0^{PQM} = \sum_i p_i |i\rangle\langle i| \otimes \rho_i \otimes |0\rangle\langle 0|\,,$$

and after the measurement it is

$$\rho_1^{PQM} = \sum_{i,j} p_i |i\rangle\langle i| \otimes M_j \rho_i M_j^\dagger \otimes |j\rangle\langle j|\,.$$

It turns out that the Holevo bound is actually the inequality

$$S(\rho_1^P : \rho_1^M) \leq S(\rho_0^P : \rho_0^Q)\,.$$

For the right hand side we can verify the following:

$$\begin{aligned}
\rho_0^P &= \sum_i p_i |i\rangle\langle i| & S(\rho_0^P) &= H(X)\\
\rho_0^Q &= \rho = \sum_i p_i \rho_i & S(\rho_0^Q) &= S(\rho)\\
\rho_0^{PQ} &= \sum_i p_i |i\rangle\langle i| \otimes \rho_i & S(\rho_0^{PQ}) &= H(X) + \sum_i p_i S(\rho_i)
\end{aligned}$$

For the left hand side, first note that $\operatorname{tr}(M_j \rho_i M_j)$ is the probability that the measurement result is j, under the condition that the measured state is ρ_i, let us denote it by $p_{j|i}$. Since the measurement result is independent of the choice of X, $p_i p_{j|i}$ is the joint probability of i and j, let us denote it by p_{ij}. Thus:

$$\begin{aligned} \rho_1^P &= \sum_{i,j} p_{ij} |i\rangle\langle i| = \sum_i p_i |i\rangle\langle i| & S(\rho_1^P) &= H(X) \\ \rho_1^M &= \sum_{i,j} p_{ij} |j\rangle\langle j| = \sum_j p_j |j\rangle\langle j| & S(\rho_1^M) &= H(Y) \\ \rho_0^{PM} &= \sum_{i,j} p_{ij} |i\rangle\langle i| \otimes |j\rangle\langle j| & S(\rho_1^{PM}) &= H(X,Y) \end{aligned}$$

Holevo bound is now obtained as follows:

$$S(\rho_0^P : \rho_0^Q) = S(\rho_0^P : \rho_0^{QM}) \geq S(\rho_1^P : \rho_1^{QM}) \geq S(\rho_1^P : \rho_1^M).$$

The derivation follows from three intuitive (and provable) principles:

- mutual information is not changed by adding an additional (uncorrelated) system;
- the mutual information of two systems cannot be increased by any measurement (or any unitary operations);
- the mutual information cannot be increased by removing part of one of the systems.

The first principle simply follows from the relation of entropy of decomposable states $S(\sigma \otimes \rho) = S(\sigma) + S(\rho)$, which we get directly from the definition.

The third principle follows from strong subadditivity. In our case, we have

$$S(\rho_1^{PQM}) + S(\rho_1^M) \leq S(\rho_1^{PM}) + S(\rho_1^{QM}),$$

where we get the required

$$S(\rho_1^P) + S(\rho_1^M) - S(\rho_1^{PM}) \leq S(\rho_1^P) + S(\rho_1^{QM}) - S(\rho_1^{PQM}).$$

Regarding the second principle, let us first note that the matrices $U\rho U^\dagger$ are similar, i.e. they have the same diagonal form, i.e. $S(\rho) = S(U\rho U^\dagger)$. It is natural that the entropy does not change by choosing a different basis. For measurements, we can reduce the principle to the second one by showing that each measurement can be viewed as a unitary transformation of our system along with some external, additional system, which we again remove after the measurement. This elegant and useful construction proceeds as follows.

Let us denote the system to be measured by Q and consider measurements using the operators (M_j). The additional system M will have base elements $|j\rangle$. Then the "indexing" mapping

$$U : |\varphi\rangle \otimes |0\rangle \mapsto \sum_j M_j |\varphi\rangle \otimes |j\rangle$$

is unitary. More precisely, this mapping preserves the scalar product (as can be straightforwardly verified using the completeness relation $\sum_j M_j^\dagger M_j = E$), and can thus be extended to the unitary mapping of the system $Q \otimes M$. The resulting density matrix is thus

$$\rho^{QM} = U(|\varphi\rangle\langle\varphi| \otimes |0\rangle\langle 0|)U^\dagger = \sum_{j,j'} M_j |\varphi\rangle\langle\varphi| M_{j'}^\dagger \otimes |j\rangle\langle j'|$$

and the reduced matrix for the original system is

$$\rho^Q = \sum_j M_j |\varphi\rangle\langle\varphi| M_j^\dagger \, ,$$

as we wanted.