Composed systems and entropy

The quantum entropy of a composite system and its subsystems is connected to entanglement. If a pure state is decomposable, then then also its subsystems are pure. However, if the state is entangled, then the subsystems have no definite description, and their density matrix is mixed. This is why in the quantum case, the entropy of a subsystem can be higher than the entropy of the whole system.

An important tool for studying entropies of a composite system and its subsystems is the Schmidt decomposition. It is a direct consequence of the *singular value decomposition*.

Lemma. Let $|\varphi\rangle \in \mathbb{H}_n \otimes \mathbb{H}_m$. Then there exist orthonormal bases $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ and $C = (\mathbf{c}_1, \ldots, \mathbf{c}_m)$ of $\mathbb{H}_n$ and $\mathbb{H}_m$ respectively, a number $r \leq \min(n, m)$ and positive values α_k, $1 \leq k \leq r$ such that

$$|\varphi\rangle = \sum_{k=1}^{r} \alpha_k \mathbf{b}_k \otimes \mathbf{c}_k \,.$$

Důkaz. For bases $(|i\rangle)$ and $(|j\rangle)$ of $\mathbb{H}_n$ and $\mathbb{H}_m$ respectively, we express $|\varphi\rangle$ as

$$|\varphi\rangle = \sum_{i,j} a_{ij} |i\rangle |j\rangle.$$

Consider the matrix $A = (a_{ij})$ (of size $n \times m$) and its singular value decomposition UDV. That is, U and V are unitary (of size n and m), and D is diagonal (of size $n \times m$) with first r diagonal entries positive. Let $\alpha_k = d_{kk}$. Setting

$$\mathbf{b}_k = \sum_{i=1}^{n} u_{ik} |i\rangle, \qquad \mathbf{c}_k = \sum_{j=1}^{m} v_{kj} |j\rangle$$

we get

$$\sum_{k=1}^{r} \alpha_k \mathbf{b}_k \otimes \mathbf{c}_k = \sum_{i,j} \left(\sum_{k=1}^{r} \alpha_k u_{ik} v_{kj} \right) |i\rangle |j\rangle = \sum_{i,j} a_{ij} |i\rangle |j\rangle = |\varphi\rangle$$

as required. □

The density operator of a pure state $|\varphi\rangle$ of a composite system AB written in Schmidt bases is

$$\rho^{AB} = |\varphi\rangle\langle\varphi| = \sum_{i,j=1}^{r} \alpha_i \alpha_j |i\rangle\langle j| \otimes |i\rangle\langle j|.$$

The corresponding partial systems are

$$\rho^A = \mathrm{tr}_B(\rho) = \sum_{k=1}^{r} \alpha_k^2 |k\rangle\langle k|, \qquad \rho^B = \mathrm{tr}_A(\rho) = \sum_{k=1}^{r} \alpha_k^2 |k\rangle\langle k|.$$

Note that the states look exactly the same but the bases $(|i\rangle)$ denote two different bases $(\mathbf{b}_i)$ and $(\mathbf{c}_i)$ respectively. Nevertheless, the two states have the same eigenvalues, and therefore also the same entropy $S(\rho^A) = S(\rho^B)$.

A state

$$|\varphi\rangle^{AB} = \frac{1}{\sqrt{r}} \sum_{k=1}^{r} |k\rangle |k\rangle$$

in which all Schmidt coefficients are the same is called *maximally entangled*. The density matrix ρ^A of the subsystem A of $|\varphi\rangle$ then is $\sum_k \frac{1}{r} |k\rangle\langle k|$, and the entropy

$S(\rho^A) = \log r$, which is the maximal possible entropy of an r dimensional mixed state, corresponding to a uniformly distributed ensemble of pure states.

Another noteworthy property of a maximally entangled state is that for each observable M on ρ^A, the measurement of M on ρ^A yields the same result as the corresponding measurement M^T on ρ^B. This can be seen from the equality

$$M \otimes I|\varphi\rangle = I \otimes M^T|\varphi\rangle,$$

which holds for the maximally entangled state $|\varphi\rangle$. Indeed, for a general Schmidt decomposition we have

$$M \otimes I|\varphi\rangle = \sum_k \alpha_k \left(\sum_i m_{ik}|i\rangle \right) \otimes |k\rangle = \sum_{ij} \alpha_j m_{ij}|i\rangle|j\rangle,$$

$$I \otimes M^T|\varphi\rangle = \sum_k \alpha_k|k\rangle \otimes \left(\sum_i m_{ki}|i\rangle \right) = \sum_{ij} \alpha_i m_{ij}|i\rangle|j\rangle.$$

*

Consider the following *uncertainty game*. Bob prepares a state $|\beta\rangle$ and sends it to Alice. Alice measures β with a measurement R of her choice, and informs Bob what R she used. Bob tries to guess the outcome of the measurement. This game leads to the following question. Given two measurements M and N, what is the trade-off between knowing the outcome of M and knowing the outcome of N? The answer is given by Maassen-Uffink uncertainty relation:

$$H(M) + H(N) \geq -\log c,$$

where c is the overlap of M and N, defined as

$$c := \max_{ij} |\langle m_i|n_j\rangle|^2$$

where m_i and n_j are eigenvectors of M and N, respectively. The relation uses the Shannon entropy of the measurement outcomes. To maximize the right-hand side of the relation we have to minimize c, which is achieved by *complementary* observables for which $|\langle m_i|n_j\rangle|^2 = {}^1\!/_d$ for all i and j, where d is the dimension of the state. An example for $d = 2$ is measurements in bases $|0\rangle$, $|1\rangle$, and $|+\rangle$, $|-\rangle$.

We have seen above, however, that the uncertainty can be removed by *quantum memory*. Namely, if Bob keeps a half of a perfectly entangled state, and sends the second half to Alice, he can reconstruct each measurement with certainty.

A generalized version of the uncertainty relation that takes into account quantum memory reads as follows:

$$H(M \mid B) + H(N \mid B) \geq -\log c + S(A \mid B). \tag{1}$$

Here $S(A \mid B) = S(\rho^{AB}) - S(\rho^B)$ is the conditional von Neumann entropy as defined in previous chapters. $H(R \mid B)$ denotes the conditional von Neumann entropy of the state obtained after measurement R of subsystem A of ρ^{AB}. That state can be written as

$$\rho^{RB} = \sum_j (|r_j\rangle\langle r_j| \otimes I)\rho^{AB}(|r_j\rangle\langle r_j| \otimes I),$$

where $|r_j\rangle$ are eigenstates of the projective measurement R. Recall that $\rho^B := \mathrm{tr}_A(\rho^{AB}) = \mathrm{tr}_A(\rho^{RB})$ according to the principle that the density matrix of a subsystem is independent of what happens to the other subsystem. We can also write

$$\rho^{RB} = \sum_j p_j |r_j\rangle\langle r_j| \otimes \rho_j^B,$$

where

$$\rho_j^B = \mathrm{tr}_A((|r_j\rangle\langle r_j| \otimes I)\rho^{AB})/p_j$$

denotes the state of the subsystem B after the measurement of R on the subsystem A resulting in j, which happens with probability

$$p_j = \mathrm{tr}(|r_j\rangle\langle r_j| \otimes \rho_j^B) = \mathrm{tr}((|r_j\rangle\langle r_j| \otimes I)\rho^{AB}).$$

A state of that form is called a *classical-quantum* state. While it is a mixed state, its first subsystem corresponds to a classical random variable, and the whole state can therefore be understood as a statistical mixture of quantum states of the second subsystem. For the von Neumann entropy of ρ^{RB}, we have

$$S(\rho^{RB}) = H(R) + \sum_j p_j S(\rho_j^B). \tag{2}$$

*

We now apply the uncertainty relation with quantum memory to the situation of BB84. We have a tripartite system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ consisting of subsystems controlled by Alice, Bob and Eve. Consider a pure state ρ^{ABE}. Then $S(\rho^{AB}) = S(\rho^E)$. Moreover for each measurement R, we have $S(\rho^{RB}) = S(\rho^{RE})$. This is true since after measuring A we obtain the classical-quantum state

$$\rho^{RBE} = \sum_j p_j |r_j\rangle\langle r_j| \otimes \rho_j^{BE},$$

where ρ_j^{BE} are pure. Hence $S(\rho_j^B) = S(\rho_j^E)$ for each j, and the conclusion follows from (2). Taking into account the definition of the conditional von Neumann entropy, we can rewrite the uncertainty relation (1) as

$$S(\rho^{MB}) + S(\rho^{NB}) \geq -\log c + S(\rho^{AB}) + S(\rho^B).$$

Using the above equalities we obtain

$$H(M \mid E) + H(S \mid B) \geq -\log c.$$

This result extends to mixed states by concavity of entropy. In other words, if the state ρ^{ABE} is mixed rather than pure, then the inequality holds for each pure component, and the entropy of the mixed state is even larger than the corresponding linear combination of entropies of the pure states. This can be written as

$$H(R \mid E)_{\sum p_i \rho i} \geq \sum p_i H(R \mid E)_{\rho_i}.$$

Moreover, $-\log c = n$ for the register of n qubits of BB84.

Altogether, we have a rough argument for security of BB84 as follows: Any measurement M Eve can perform on her subsystem leaves entropy at least $n - H(S \mid B)$, which is large if the entropy of Bob's measurement on his subsystem is small. The upper bound on Bob's uncertainty is the objective of the testing phase of the protocol.