Quantum Teleportation

Next we return to the quantum conditional entropy, and seek an interpretation for the fact it can be negative:

$$S(A|B) = S_{AB} - S_B$$

It turns out that a negative quantum conditional entropy between A and B measures the number of quantum bits that can be sent from A to B using only local operations and classical communication (LOCC).

As we begin to discuss quantum communication protocols it is important to keep the class of LOCC in mind. These are quantum operations that cannot generate entanglement, and necessarily have Kraus operators of the form:

$$\mathcal{E}(\rho_{AB}) = \sum_k (E_{k,A}^\dagger \otimes E_{k,B}^\dagger)\rho_{AB}\,(E_{k,A} \otimes E_{k,B})$$

LOCC operations describe a situation in which Alice and Bob can classically communicate, and can each apply unitaries or measurements to their respective (local) systems. However, Alice and Bob can't directly send qubits to each other (e.g. Alice and Bob are on different continents, they can send each other text messages, but they don't share a fiber optic cable that could be used to send each other photonic qubits).

It turns out that even in such a circumstance, Alice and Bob can transmit qubit states to one another if and only if they share an initial state with negative conditional entropy $S(A|B)$, and they do it by **quantum teleportation**.

Quantum Teleportation

In a quantum teleportation protocol, Alice and Bob use LOCC and shared entanglement to transmit quantum info.

Single qubit example: suppose Alice initially holds an single qubit A_0 in an arbitrary state,

$$(\alpha|0\rangle + \beta|1\rangle)_{A_0}$$

And she also has a qubit A_1 that is maximally entangled with Bob's qubit B_1,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_1 B_1}$$

Therefore the state of the joint system is:

$$\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)_{A_0 A_1 B_1}$$

Quantum Teleportation

Joint state: $\frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right)_{A_0 A_1 B_1}$

Next Alice measures her two qubits A_0, A_1 in the **Bell basis**, projecting onto one of the following states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

Quantum Teleportation

Joint state: $\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)_{A_0A_1B_1}$

To understand the measurement, we express the joint state with Alice's subsystem written in the Bell basis:

$$\left[|\Phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\Phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) + |\Psi^+\rangle(\alpha|1\rangle + \beta|0\rangle) + |\Psi^-\rangle(\alpha|1\rangle - \beta|0\rangle)\right]_{A_0A_1B_1}$$

From this form we can read off the state of Bob's system after the measurement.

The outcome $|\Phi^-\rangle$ projects Bob's state into $(\alpha|0\rangle - \beta|1\rangle)_{B_1}$. Now if Alice sends a classical message that tells Bob the result was $|\Phi^-\rangle$, he will apply a Z operator to his qubit B_1 and obtain

$$Z(\alpha|0\rangle - \beta|1\rangle)_{B_1} = (\alpha|0\rangle + \beta|1\rangle)_{B_1}$$

Which was the original state of Alice's qubit A_0. Using LOCC and shared entanglement Alice has transmitted her qubit state to Bob, but in the process she destroyed the version of it that she held.

Quantum Teleportation

There were four different equally likely measurement possibilities Alice could have obtained:

$$\left[|\Phi^+\rangle(\alpha|0\rangle+\beta|1\rangle)+|\Phi^-\rangle(\alpha|0\rangle-\beta|1\rangle)+|\Psi^+\rangle(\alpha|1\rangle+\beta|0\rangle)+|\Psi^-\rangle(\alpha|1\rangle-\beta|0\rangle)\right]_{A_0A_1B_1}$$

Each one requires a different operator to "correct" the state after the measurement. There are four possible correction operators, {I,X, Y, Z}. Therefore it suffices for Alice to send two classical bits.

This can be expressed in the form of a resource inequality:

$$2 \text{ cbits } + 1 \text{ ebit } \geq 1 \text{ qubit}$$

These are the three main types of (noiseless) channels considered in quantum Shannon theory.

A channel that allows sending qubits is the strongest, since it can simulate either of the others.

$$1 \text{ qubit } \geq 1 \text{ ebit} \quad , \quad 1 \text{ qubit } \geq 1 \text{ cbit}$$

An entanglement distribution channel for distributing Bell pairs and a classical channel are in some sense incomparable because neither can simulate the other.

Quantum Teleportation

(top, left) Richard Jozsa, William K. Wootters, Charles H. Bennett. (bottom, left) Gilles Brassard, Claude Crépeau, Asher Peres. Photo: André Berthiaume.

The term “quantum teleportation” was coined by Charlie Bennet, and published in 1993 with Brassard, Crepeau, Jozsa, Peres, and Wooters.

Along with Shor’s factoring algorithm in 1994, the teleportation protocol was on of the major transformative ideas that sparked the modern quantum information science revolution.

It is an example of truth being much richer than fiction. The science fiction version of teleportation raises philosophical problems of identity: why can’t a functioning teleporter also be a duplicator?

Teleportation has no classical probabilistic analogue because there is no correspondence to the Bell basis. Nature says “teleportation exists, but only quantum mechanically, so no-cloning prevents duplication.”

The speed of information transmission is quantum teleportation is bottlenecked by the classical message that needs to be sent, which prevents “faster than light” transmission.

Quantum Teleportation

To appreciate the impossibility of using teleportation for FTL transmission it is useful to consider the state of the system after Alice's measurement, but before the classical message reaches Bob.

At this intermediate stage, the state of Bob's subsystem is a mixture over the various Paulis that could have scrambled Alice's original state ρ_A ,

$$\rho_B = \frac{1}{4}(\rho_A + X\rho_A X + Y\rho_A Y + Z\rho_A Z)$$

We have seen this depolarizing channel before, and from our previous result we have:

$$\rho_B = \frac{1}{4} I$$

Bob's state is completely random until he receives the message, so no communication has taken place.

You may wonder about "gambling" on getting the $|\Phi^+\rangle$ state so that no correction needs to be applied. But when teleporting multiple qubits, the probability of this happening goes down exponentially.

Superdense Coding

Before going on to analyze teleportation from an information theoretic perspective, we will mention a related protocol called **superdense coding**.

The idea is that Alice will send classical information to Bob at a higher rate than she otherwise may have been able to by using ebits and quantum communication.

Suppose Alice wants to send one of four possible messages (two bits), and she and Bob already share an ebit. By performing a local unitary, Alice can turn this into any one of the four Bell pairs:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

After doing this she may now send her qubit to Bob using a quantum channel, and he can measure in the Bell basis to obtain a deterministic answer, which reveals to him the two bits that Alice chose.

$$1 \text{ ebit } + 1 \text{ qubit } \geq 2 \text{ cbits}$$

Conditional Entropy and Partial Information

Classically, the Shannon entropy of the source determines the optimal rate of communication over a noiseless channel. But what if the receiver already has some partial knowledge of the message that will be sent?

Assume the source X and receiver Y have some mutual information I(X:Y). The number of bits that is necessary and sufficient to reliably send X to Y is called the **partial information**.

This problem is a generalization of Shannon's noiseless coding theorem, and it was solved by Slepian and Wolf in 1971. The partial information is the source entropy reduced by the mutual information:

$$S(X) - I(X:Y)$$

Applying the definition of the mutual information, we see the partial information is just the conditional entropy:

$$S(X) - I(X:Y) = S(X) - S(X) - S(Y) + S(XY) = S(XY) - S(Y) = S(X|Y)$$

which as we've seen can be defined as the expected entropy of the conditional distribution:

$$S(X|Y) = -\sum_{xy} p(y)p(x|y)\log p(x|y)$$

Conditional Entropy and Partial Information

The Slepian-Wolf solution characterizes the cost of communication between correlated sources.

It reinforces the operational meaning of the mutual information, as the information shared between X and Y, and also grants an operational meaning to the conditional entropy.

Attempts to generalize this picture to the quantum setting remained puzzling for a long time.

The notion of a conditional entropy can be applied to measurement distributions (since these are classical probability distributions), but there is no basis-invariant generalization of it for quantum states.

One way to think of the problem is that conditioning on some event seems to necessarily involve a measurement, which in general will disturb the results of future measurements on the state.

Conditional Entropy and Partial Information

The next alternative is the formal definition given by replacing Shannon entropy with von Neumann entropy:

$$S(A|B) = S(AB) - S(B)$$

But how can the quantum conditional entropy defined above be related to the partial information needed to communicated correlated information if the former can be negative for entangled states?

Schrodinger noted this peculiarity that, with entangled states we may know more about the whole than the parts. This intuition can be captured by the negativity of quantum conditional information.

If Alice and Bob hold an ebit, then $S(A|B) = 0 - 1 = -1.$ Every pure bipartite entangled state has negative quantum conditional entropy, but some entangled states ρ_{AB} do not exhibits this negativity.

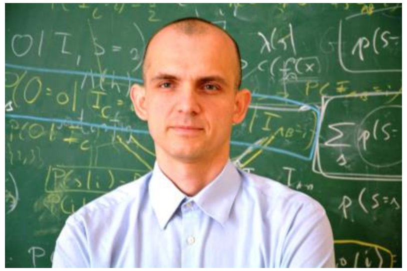
Conditional Entropy and Partial Information

"When two systems, of which we know the states by their respective representatives, enter into temporary physical interaction due to known forces between them, and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. **I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives [the quantum states] have become entangled**. **Another way of expressing the peculiar situation is: the best possible knowledge of a whole does not necessarily include the best possible knowledge of all its parts**, even though they may be entirely separate and therefore virtually capable of being 'best possibly known,' i.e., of possessing, each of them, a representative of its own. The lack of knowledge is by no means due to the interaction being insufficiently known — at least not in the way that it could possibly be known more completely — it is due to the interaction itself."

Erwin Schrödinger

Conditional Entropy and Partial Information

The puzzle of negative quantum conditional entropy was finally resolved in 2005 by Horodecki, Oppenheim, and Winter.



Horodecki

Oppenheim

Winter

They showed that the conditional entropy has the same meaning as it does classically: it is the partial information, the rate at which Alice can send quantum states ρ_A when Bob already knows quantum information ρ_B.

If the partial information is positive, the sender needs to communicate this number of qubits to achieve state transfer.

If the partial information is negative, then state transfer is possible, and in addition the sender and receiver gain the potential for future quantum communication.

S(B) quantifies how much Bob knows, while S(AB) quantifies how much there is to know. If S(AB) ≤ S(B), then in a sense Bob knows too much. If he received Alice's state, at a cost of S(A), then he would have entropy S(AB).
After you receive negative information, you know less!

Conditional Entropy and Partial Information

The proof that the quantum conditional entropy corresponds to the partial information is based on a protocol called **quantum state merging**, which generalizes quantum teleportation.

Before describing the general version, we will formalize teleportation in a slightly different way by introducing a **reference system** R in addition to Alice and Bob.

In this version of teleportation, Alice begins with qubit A_0 maximally entangled with R:

$$|\Psi_{RA_0}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{RA_0}$$

Her goal is to manipulate her system $A = A_0 A_1$ and tell Bob what to do so that in the end his state is:

$$|\Psi_{RB}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{RB}$$

Without ever touching the reference system R.

Conditional Entropy and Partial Information

The proof that the quantum conditional entropy corresponds to the partial information is based on a protocol called **quantum state merging**, which generalizes quantum teleportation.

Before describing the general version, we will formalize teleportation in a slightly different way by introducing a **reference system** R in addition to Alice and Bob.

In this version of teleportation, Alice begins with qubit A_0 maximally entangled with R, A_1 entangled with B:

$$|\Psi_{RA_0}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{RA_0} \qquad |\Psi_{A_1B}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_1B}$$

Her goal is to manipulate her system $A = A_0A_1$ and tell Bob what to do so that in the end his state is:

$$|\Psi_{RB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{RB}$$

(as before A1 begins in an entangled with B) Without ever touching the reference system R.

Conditional Entropy and Partial Information

The joint system is initially in the state $|\Psi_{RA_0}\rangle \otimes |\Psi_{A_1B}\rangle$, and so the solution is for Alice to perform exactly the same measurements and communication from before, leaving A_0A_1 in a Bell state and creating $|\Psi_{RB}\rangle$.

Now we consider the conditional entropy $S(A|B)$. $|\Psi_{A_1B}\rangle$ is pure so doesn't contribute to the joint entropy:

$$S(AB) = -\mathrm{tr}\rho_{AB}\log\rho_{AB} = S(A_0) = 1$$

Meanwhile B is maximally entangled with R, so S(B) = 1, and so $S(A|B) = S(AB) - S(B) = 0.$

We will now proceed to show that teleportation (and more generally state merging) is possible iff

$$S(A|B) \leq 0$$

Conditional Entropy and Partial Information

To see that $S(A|B) \leq 0$ is a necessary condition for teleportation, suppose we start with an arbitrary $|\Psi_{RAB}\rangle$

We are interested in whether Alice can perform a measurement on her system and communicate with Bob to accomplish teleportation. If this is possible then:

1. If Alice performs a measurement and sends the result to Bob, then Bob will know the pure state that describes his system together with the reference system, $|\chi_{RB}\rangle$, and Alice's system will also be in a pure state.

2. For teleportation to succeed, the reduced state of the reference system ρ_R is unaffected by this measurement.

Conditional Entropy and Partial Information

Since the initial state $|\Psi_{RAB}\rangle$ is pure, the entropy of R equals the entropy of AB:

$$S_{AB} = S_R$$

Bob's density matrix is $\rho_B = \mathrm{tr}_{RA}(\rho_{RAB})$, and so the entropy of his system is $S_B = \mathrm{tr}(\rho_B)$.

After Alice performs a measurement $\{\Pi_k\}$ and obtains outcome Π_i , the state of Bob's system is

$$\rho_B^i = \frac{1}{p_i}\mathrm{tr}_{RA}\left(\Pi_i \rho_{RAB}\right)$$

Where we also note that $\rho_B = \sum_i p_i \rho_B^i$ since $\sum_k \Pi_k = I$.

Conditional Entropy and Partial Information

As we established, the system RB is in a pure state after the measurement, and so

$$S(\rho_B^i) = S_R$$

But we also noted that teleportation does not change the state of the reference system, and so

$$S(\rho_B^i) = S(AB)$$

Therefore $S(AB) = S(\rho_B^i) = \sum_i p_i S(\rho_B^i)$, and since by concavity we have

$$S_{AB} = \sum_i p_i S(\rho_B^i) \leq S\left(\sum_i p_i \rho_B^i\right) = S(\rho_B)$$

And so $S(A|B) = S_{AB} - S_B \leq 0$. If teleportation is possible, then conditional entropy is nonpositive.

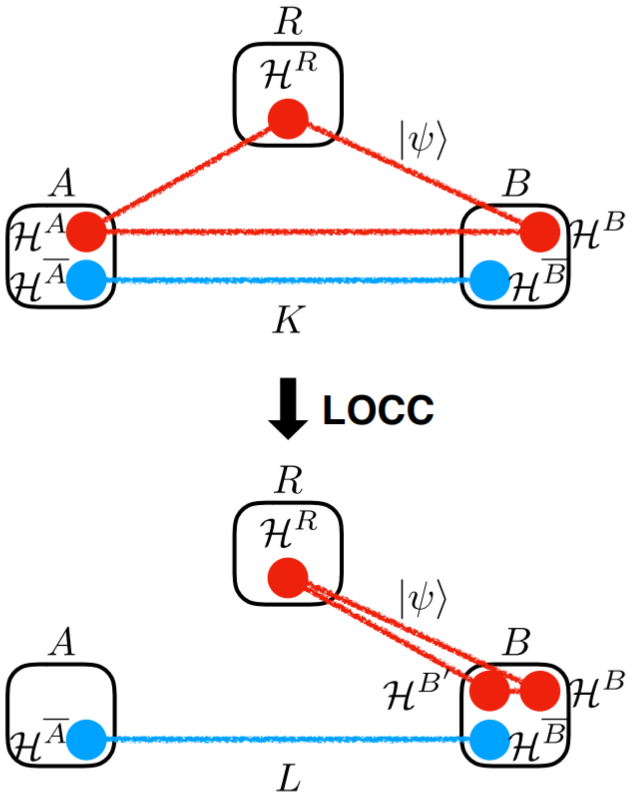
Conditional Entropy and Partial Information

The statement that $S(A|B) \leq 0$ is sufficient applies to the iid regime of a large number of copies of the state

$$|\Psi_{RAB}\rangle^{\otimes N}$$

This multiples all entropies by N, so it preserves $S(A|B) \leq 0$, where A and B are all of Alice and Bob's copies.

State merging: A and B hold K ebits and wish to perform LOCC to transfer A's part of RAB to B, leaving A and B with L ebits.



The key idea in the proof of Horodecki et al. is that a random measurement of Alice's subsystem will suffice with probability approaching 1.

Summary of Quantum Teleportation

Quantum teleportation uses classical communication and entangled resource states to transmit quantum information. It uses measurements that project onto an entangled basis, which have no classical analogue.

The speed of information transmission in teleportation is limited by the classical communication.

Classically, the partial information is the number of bits which must be sent to exchange a message between a source and receiver who hold prior correlations. Slepian and Wolf showed this is exactly the conditional entropy.

This operational meaning of conditional entropy was extended to quantum systems, where the partial information is the number of qubits that must be sent to transfer quantum information between correlated parties.

When the quantum conditional entropy is negative, it means that the receiver can in a sense lose information to recover the full message. State transfer can be achieved using only LOCC, and the negative conditional entropy measures the number of additional ebits harvested by the protocol ($N \cdot S(A|B)$ ebits in the iid limit $N \to \infty$).