CS 880: Quantum Information Processing 10/26/2010

Lecture 21: Quantum Communication

Instructor: Dieter van Melkebeek Scribe: Mark Wellons

Last lecture, we introduced the EPR pairs which we will use in this lecture to perform quantum communication. In the typical quantum communication setting, two parties, Alice and Bob want to communicate. Beforehand, they create an entangled EPR pair and give one qubit to Alice and the other to Bob. Alice and Bob will exploit the entanglement between the two qubits to exchange information.

In this lecture, we show that quantum communication can outperform its classical counterpart and also explore the limits of quantum communication.

1 Teleportation

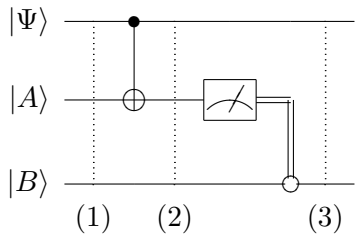
Teleportation is a procedure that allows Alice to send a qubit to Bob using only two classical bits and one EPR pair. Recall that the EPR pair we use is

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

Suppose that Alice has some state

$$|\Psi\rangle = \sum_{b\in\{0,1\}} \alpha_b |b\rangle, \tag{2}$$

that she wishes to send to Bob, and that she and Bob each hold one qubit of an EPR pair. We will denote Alice's qubit as $|A\rangle$ and Bob's as $|B\rangle$. For our first attempt at teleportation, we can try the following circuit, in which Alice entangles $|A\rangle$ with $|\Psi\rangle$,



At the point (1) in our circuit, the system state looks like

$$|\Psi\rangle\left|\Phi^+\right\rangle = \sum_{b,c\in\{0,1\}} \alpha_b |b,c,c\rangle \tag{3}$$

At the point (2), Alice has applied a CNOT gate to her qubit, so the system state becomes

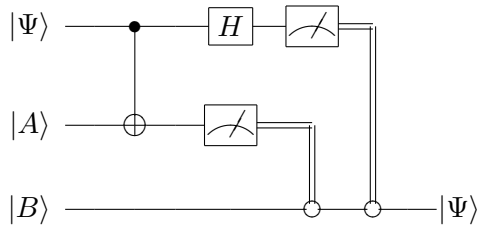
$$\sum_{b,c\in\{0,1\}} \alpha_b |b, b\oplus c, c\rangle \tag{4}$$

Alice then measures her qubit, and gets state $d = b \oplus c$. At (3), she then transmits d to Bob, who will use this to affect his qubit. If $d = 0$, Bob does nothing, otherwise he flips his qubit, giving us the state

$$\sum_{b\in\{0,1\}} \alpha_b \left|b, b \oplus d\right\rangle \Rightarrow \sum_{b\in\{0,1\}} \alpha_b \left|b, b\right\rangle \tag{5}$$

Note that Alice's EPR qubit is omitted from the state equation, as it has been measured and is no longer useful. At this point, Bob's qubit is almost where we want it to be. However, it is still entangled with Alice's qubit. Alice could measure her state to remove the entanglement, but this collapses Bob's as well, which defeats the purpose of sending it to him in the first place.

To resolve this in our second attempt, we will use a similar circuit to the one in the first attempt.



This circuit behaves much as the previous one, except that Alice uses a Hadamard gate before taking a measurement. This functionally means that she is measuring in the $|+\rangle$ basis. Thus, the system state change from the Hadamard is

$$\sum_{b\in\{0,1\}} \alpha_b \left|b, b\right\rangle \Rightarrow \sum_{a,b} \alpha_b (-1)^{ab} \left|a, b\right\rangle \tag{6}$$

Alice then takes her second measurement and sends a to Bob. If Alice measured a 0, then the system state would be

$$\alpha_0 (-1)^{(0)(0)} \left|0\right\rangle + \alpha_1 (-1)^{(0)(1)} \left|1\right\rangle = \alpha_0 \left|0\right\rangle + \alpha_1 \left|1\right\rangle = \left|\Psi\right\rangle, \tag{7}$$

which means Bob has the state Alice wanted to send him, so we are done. In the case that Alice measured a 1, we have

$$\alpha_0 (-1)^{(1)(0)} \left|0\right\rangle + \alpha_1 (-1)^{(1)(1)} \left|1\right\rangle = \alpha_0 \left|0\right\rangle - \alpha_1 \left|1\right\rangle, \tag{8}$$

which means Bob needs to only apply a phase flip to his qubit, and then he will have $|\Psi\rangle$.

2 No Cloning Theorem

It is important to note that Alice was not able to duplicate the qubit that she wanted to send to Bob during the teleportation procedure, as her copy was destroyed in the transfer process when she measured it. This is not a coincidence, as it is impossible for any quantum process to duplicate an arbitrary state. Formally, we can show that there cannot exist a quantum operation that performs the transformation

$$\left|\psi\right\rangle \left|\psi_0\right\rangle \Rightarrow \left|\psi\right\rangle \left|\psi\right\rangle. \tag{9}$$

Proof. Suppose that such a Q exists. Let

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle . \tag{10}$$

Then

$$Q |\psi\rangle |\psi_0\rangle = |\psi\rangle |\psi\rangle = \alpha_0^2 |00\rangle + \alpha_0\alpha_1 |01\rangle + \alpha_0\alpha_1 |10\rangle + \alpha_1^2 |11\rangle . \tag{11}$$

Since Q is a quantum operation, it must be linear, so

$$Q |\psi\rangle |\psi_0\rangle = Q (\alpha_0 |0\rangle + \alpha_1 |1\rangle) |\psi_0\rangle = \alpha_0 Q |0\rangle |\psi_0\rangle + \alpha_1 Q |1\rangle |\psi_0\rangle = \alpha_0 |00\rangle + \alpha_1 |11\rangle . \tag{12}$$

Since equations (11) and (12) must be equal, it follows that $\alpha_0\alpha_1 = 0$, which implies that the only states we can possibly clone are the basis states $|0\rangle$ and $|1\rangle$. □

Note that this proof shows that in the {0,1} basis, only the states $|0\rangle$ and $|1\rangle$ can be cloned. If we changed into a different basis, the {+, -} basis for example, we could repeat the proof to show that we could make a quantum operator to copy the $|+\rangle$ and $|-\rangle$ states, but nothing else. This can be generalized to the statement that a quantum operator can only be constructed to clone basis states for a specific basis.

3 Superdense Coding

In teleportation, we used two classical bits and an EPR pair to send a qubit. We can also do the reverse in a process known as superdense coding. In this context, Alice will use an EPR pair and a single qubit to communicate two classical bits to Bob.

To start, Alice and Bob jointly prepare their EPR pair and as before, Alice takes $|A\rangle$ and Bob takes $|B\rangle$. At this point, the system state is

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) . \tag{13}$$

Later, when Alice wants to send a two-bit message $b_1 b_2$ to Bob, she transmits $|A\rangle$ to Bob, but first she applies some transformations to it. If $b_1 = 1$, she applies the phase-flip operation, and if $b_2 = 1$, she applies the bit-flip operation. These two operations in matrix form are

$$\text{phase-flip} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \ \text{bit-flip} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} . \tag{14}$$

Depending on which operations Alice applied, the EPR pair will be in one of the four states

$$|\Phi\rangle \in \left\{ \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle) , \frac{1}{\sqrt{2}} (|10\rangle \pm |01\rangle) \right\} . \tag{15}$$

These states are called the Bell states, and they are all orthogonal. Thus Bob merely needs to measure in the appropriate basis (the Bell basis in this case), and he can determine the system state with perfect accuracy. From this, he can infer Alice's message.

4 Bounds on Quantum Communication

Superdense coding allows us to transmit two bits with a single qubit and an EPR pair. It immediately follows that any n bit message can be transmitted with $n/2$ qubits if we allow prior entanglement. Naturally, we are interested in whether we can do better. The answer is no, a reduction by a factor of two is the best quantum communication can do over classical communication.

Theorem 1. *Given a quantum communication protocol that allows Alice to send any message x where $x \in \{0,1\}^n$ to Bob with probability of correctness[1] $\geq p$, let m_{AB} be the number of qubits Alice sends to Bob, and m_{BA} be the number of qubits Bob sends to Alice, then without prior entanglement*

$$m_{AB} + m_{BA} \geq n - \log\left(\frac{1}{p}\right), \tag{16}$$

and with prior entanglement

$$m_{AB} \geq \frac{1}{2}\left[n - \log\left(\frac{1}{p}\right)\right]. \tag{17}$$

We now prove the special case of one-way communication without prior entanglement.

Proof. Given message x and some optimal protocol, Alice will send $|\psi_x\rangle$ over the channel to Bob, where $|\psi_x\rangle$ consists of m_{AB} qubits. Bob then applies some quantum operation D on $|\psi_x\rangle$, and then performs a projective measurement onto P_y for $y \in \{0,1\}^n$.

The probability that Bob gets the correct result is

$$\Pr[\text{Bob reads the correct } x] = \|P_x D\,|\psi_x\rangle\|^2. \tag{18}$$

The average probability over all possible messages x would then be

$$p \leq \frac{1}{2^n}\sum_x \|P_x D\,|\psi_x\rangle\|^2. \tag{19}$$

Since $|\psi_x\rangle$ lives in a subspace of dimension $d \leq 2^{m_{AB}}$, then so does $D\,|\psi_x\rangle$. Let $|\phi_i\rangle, i = 1, 2, \ldots d$ be an orthonormal basis for the $D\,|\psi_x\rangle$ subspace, then

$$D\,|\psi_x\rangle = \sum_{i=1}^{d} \alpha_{x,i}\,|\phi_i\rangle. \tag{20}$$

Substituting this back into equation (19) and choosing our projection operators such that all P_x's have orthogonal ranges gives

$$p \leq \frac{1}{2^n}\sum_x \left\| P_x \sum_{i=1}^{d} \alpha_{x,i}\,|\phi_i\rangle \right\|^2, \tag{21}$$

$$p \leq \frac{1}{2^n}\sum_x \sum_{i=1}^{d} |\alpha_{x,i}|^2 \|P_x\,|\phi_i\rangle\|^2, \tag{22}$$

$$p \leq \frac{1}{2^n}\sum_{i=1}^{d} \underbrace{\left\| \sum_x \alpha_{x,i} P_x\,|\phi_i\rangle \right\|^2}_{\leq 1}. \tag{23}$$

[1] This is the probability that Bob receives the message that Alice actually sent. Obviously, this needs to be very close to 1.

The last equation is true as

$$\|P_x |\phi_i\rangle\|^2 = |\text{length of the projection of } \phi_i|^2 \leq \||\phi_i\rangle\|^2 = 1. \tag{24}$$

Thus

$$p \leq \frac{d}{2^n} \leq 2^{m_{AB}-n}, \tag{25}$$

which leads to

$$m_{AB} \geq n - \log\left(\frac{1}{p}\right). \tag{26}$$

□

5 Holevo's Theorem

The previous proof can be generalized into a more powerful theorem, but first let us review some information theory terminology.

Given some random variable X with range R, we define its classical entropy H to be

$$H(X) \equiv \sum_{x \in R} p_x \log\left(\frac{1}{p_x}\right) \text{ where } p_x = \Pr[X = x]. \tag{27}$$

H has the property that

$$0 \leq H(X) \leq \log |R| \tag{28}$$

where $H(X) = \log |R|$ if X is the uniform distribution and $H(X) = 0$ if X is completely deterministic.

For a mixed state $|\psi\rangle$ with density operator ρ, we define the Von Neumann entropy to be

$$S(\rho) \equiv H(\text{Probability distribution induced by the eigenvalues of } \rho). \tag{29}$$

Finally, we define the mutual information of random variables X and Y to be

$$I(X, Y) = H(X) + H(Y) - H(X, Y). \tag{30}$$

Informally, the mutual information says how much information X gives about Y, and vise versa.

We can now state Holevo's Theorem,

Theorem 2. *Suppose Alice has a random variable x and sends ρ_x over the channel. Bob receives ρ_x and applies some operations on it to obtain y. Then $I(X, Y) \leq S(\rho) - \sum_x \rho_x S \rho_x$ where $\rho = \sum p_x \rho_x$.*

Let's consider the example where X is uniform over $\{0, 1\}^n$ and we want zero error in our channel. Note that zero error is equivalent to $x = y$ in Holevo's Theorem.

In this example, we can see that $I(X, Y) = \log 2^n = n$, and $S(\rho) = m_{AB}$. Putting these into Holevo's Theorem gives

$$n \leq m_{AB} - \sum_{\rho_x} S\rho_x \leq m_{AB}. \tag{31}$$

Thus, classically, Bob cannot learn more bits of information than the number of qubits Alice transmits.

Next lecture, we will expend on quantum communication protocols where Alice and Bob want to jointly compute a boolean function rather than just transmit a string.