Lecture 27: Nonlocality

Instructor: Dieter van Melkebeek Scribe: Balasubramanian Sivan

The general idea in quantum communication protocols we have seen was to exploit the power of entanglement present in EPR pairs. Today, through various other examples, we illustrate several strange tasks that can be accomplished through that same power of entanglement.

1 What does nonlocal mean?

We begin by discussing what nonlocal doesn't stand for. Let two parties Alice and Bob share one qubit each of a Bell state and separate. One interpretation of nonlocality could be that as soon as Alice makes a measurement, the resultant change in the system is instantaneously reflected in Bob's view of the world. This is not the right interpretation of nonlocality though it seems true at first sight. In fact, this would contradict the postulate that no information can be transmitted faster than the speed of light. To see that instantaneous information transmission is indeed not happening here, consider the reduced density operator of Bob, which completely describes Bob's view of the world. We discussed earlier that the reduced density operator contains all information that Bob needs to know about the rest of the world, to find how his state evolves, the effect of the operations that he performs, etc. Now, when Alice performs an operation on her qubit, the reduced density operator of Bob does not change. One way to see this is through the Schmidt decomposition. When Alice performs a unitary operation, the orthonormal basis given by the Schmidt decomposition changes, but this does not have any effect on Bob's reduced density operator. (This was a fact that we exploited when we proved that perfect bit commitment is not possible even with quantum computers.) Similarly, when Alice performs a measurement, it can be interpreted as purification of the system on Alice's part, and this does not affect Bob's reduced density operator. Thus nonlocality is not immediate signaling.

Nonlocality refers to the fact that the entanglement exhibited by the EPR pairs cannot be explained by the theory of local hidden variables. Hidden variable theory, proposed by Einstein, Podolsky and Rosen, states that for an entangled system, somehow, the two parties Alice and Bob have some local variables, which describe how the system behaves for each possible measurement. That is, before separating, Alice and Bob make a list of how the system behaves for every possible measurement, and thus, the information contained in these "hidden variables" explains entanglement. Today we illustrate through various examples that this is not the case.

2 GHZ paradox

The GHZ paradox is named after Greenberger, Horne and Zeilinger. We discuss this from a computer science perspective. Consider a three-party game, with Alice, Bob and Carol. They receive one bit each, r, s, and t, respectively, with the promise that $r \oplus s \oplus t = 0$. Thus there are four possible inputs, corresponding to all zeroes, and exactly two ones. These inputs are drawn from a uniform distribution over the four possible inputs. The goal is, without any communication after the inputs were given, for Alice, Bob and Carol to output a single bit each, a, b, and c, such that $a \oplus b \oplus c = r \vee s \vee t$.

What is the probability of success achieveable classically? We can achieve a probability of success of 0.75 through a very simple protocol. Two of Alice, Bob and Carol shall always output zero, and the third person shall always output one. This way, the XOR of all their outputs will always be one. But in fact, we require the XOR of the outputs to be one for three out of the four inputs, namely for the three inputs apart from all the zeroes input. Thus this simple protocol manages to be correct for three of the four possible inputs, giving a success probability of 0.75. We now prove that this is in fact the highest possible probability of success that can be achieved classically. Let a_0, b_0 and c_0 denote the output of Alice, Bob and Carol when they receive an input of zero, and let a_1, b_1, and c_1 denote the same when they receive an input of one. We require the following:

$$\begin{aligned}
\text{Input} = 000 &\Rightarrow a_0 \oplus b_0 \oplus c_0 = 0 \\
\text{Input} = 011 &\Rightarrow a_0 \oplus b_1 \oplus c_1 = 1 \\
\text{Input} = 101 &\Rightarrow a_1 \oplus b_0 \oplus c_1 = 1 \\
\text{Input} = 110 &\Rightarrow a_1 \oplus b_1 \oplus c_0 = 1
\end{aligned}$$

This is something that cannot be true, because if we XOR all the four implied equalities, we have a one in the RHS, but the LHS must be zero as we have each variable appearing exactly twice. Thus, it is inevitable to err on one input, making it impossible to exceed a success probability of 0.75. Randomized strategies cannot exceed 0.75 either, as any randomized strategy is just a convex combination of deterministic strategies, and hence cannot yield a higher success probability. Hidden local variables are not of any help either, since the above argument still remains valid.

2.1 Quantum Setting

We now show that we can get a success probability of one in the quantum setting! Alice, Bob and Carol prepare the entangled state $|\psi\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$ take one qubit each and separate out. They decide on the following strategies. Alice's strategy is that if she gets an input of 1, she applies a Hadamard operation on her qubit and outputs the outcome of the measurement on her qubit. If her input is zero, she does not perform the Hadamard operation, and just outputs the outcome of the measurement on her qubit. Bob and Carol have identical strategies. We now verify that for each input, the output satisfies the required condition. For example, when the input is 000, no Hadamard operation is performed, leaving the state $|\psi\rangle$ undisturbed. For the state $|\psi\rangle$, irrespective of who measures first, the output will have an even number of ones, thus XORing to zero, which is what we require. When the input is 011, then, after the Hadamard operation, the state can be verified to be $|\psi'\rangle = |001\rangle + |010\rangle - |100\rangle + |111\rangle$. Here, irrespective of who gets to measure first, the XOR of the outputs will be one. By symmetry, the other two inputs are similar to this input. This means that we have a success probability of one.

This proves that the local hidden variable theory cannot explain the power of entanglement in EPR pairs, for otherwise, the probability of success with hidden variables should have been one. But as we proved, even with hidden variables, the probability of success is at most 0.75.

3 Bell inequality

The Bell inequality was specifically designed to refute the local hidden variable theory. It is an inequality which has to be true if nature were to obey the local hidden variable model, i.e., if the following two assumptions were true.

1. Observables of a system have an intrinsic value irrespective of any measurement being performed.

2. Local measurements by any one party in an entangled system do not have any effect on the result of measurements made by the other party.

However, this inequality is violated according to the quantum mechanical model of nature. From the experiments that have been conducted, it has been verified that nature overwhelmingly violates the Bell inequality, thereby proving that the local hidden variable theory does not explain entanglement. In particular, one or both of the above two assumptions must be false.

We now derive Bell's inequality, which as we noted, is really an inequality only if we disbelieve the quantum mechanical model. Thus, for deriving this inequality, we assume that both of the above assumptions are true.

The setup here is somewhat similar to the GHZ paradox setup. We have two parties Alice and Bob, who have a qubit each. They perform their measurements far away from each other, so there is not enough time for any signal to have reached Bob from Alice (and vice versa), and thus Alice's measurement had no chance of influencing the result of Bob's measurement. (Recall that by our assumption 2, local measurements do not influence the result of other party's measurements. Thus sending an explicit signal is the only way to have an influence, which we prevent by designing the experiment as above.) There are two possible observables that Alice and Bob can measure. The outcomes of the measurements are bits. Let M_0^A and M_1^A denote the two measurements that Alice can perform, and let a_0 and a_1 denote the respective outputs of these measurements. As noted, both $a_0, a_1 \in \{0, 1\}$. The quantities M_0^B, M_1^B and b_0, b_1 have similar meanings. We define the quantities $A_i = (-1)^{a_i}$ and $B_i = (-1)^{b_i}$ for $i = 0, 1$. Note that by our assumption 1, a_0 (and others) being 0 or 1 is something intrinsic to the system, and will take the same value irrespective of the number of measurements we do. Thus the only randomness in the a_i's and b_i's, (and hence the A_i's and B_i's) is the randomness of the initial state of the system. That is, initially, the system is set such that the a_i's and b_i's are assigned specific values with some joint probability.

Consider the following quantity: $A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1$. This can be rewritten as $A_0(B_0 + B_1) + A_1(B_0 - B_1)$. Since B_0 can be either B_1, or $-B_1$, this sum satisfies Thus $-2 \leq A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \leq 2$. Thus,

$$\begin{aligned} \mathrm{E}[A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1] &= \mathrm{E}[A_0B_0] + \mathrm{E}[A_0B_1] + \mathrm{E}[A_1B_0] + \mathrm{E}[-A_1B_1] \\ &\leq 2, \end{aligned}$$

where the expectation is over the randomness in the initial state of the system. Thus, by running the experiment many times, we can compute each of these four expectations individually, and then sum them up. If our belief that nature obeys the local hidden variable theory were true, the expected value of this sum must be at most 2.

3.1 Quantum Setting

Here Alice and Bob have one qubit each of the entangled system $|\phi^-\rangle = |00\rangle - |11\rangle$. Measurement M_A^0 corresponds to Alice performing a rotation by an angle $\theta_A^0 = -\pi/16$, and then performing a measurement in the standard basis. Measurement M_A^1 corresponds to Alice performing a rotation by an angle $\theta_A^1 = 3\pi/16$ and then performing a measurement in the standard basis. We similarly define M_B^0 and M_B^1 with the values $\theta_B^0 = \theta_A^0$, and $\theta_B^1 = \theta_A^1$. We now drop the superscripts in the θ's, and write the state of the system after these rotations:

$$\cos(\theta_A + \theta_B)(|00\rangle - |11\rangle) + \sin(\theta_A + \theta_B)(|01\rangle - |10\rangle). \tag{1}$$

Alice and Bob now each measure their qubit, resulting in outcomes $a, b \in \{0, 1\}$. Notice that for the first two components in (1) the quantity $(-1)^a \cdot (-1)^b$ has value 1, whereas for the last two it is -1. Thus, $\mathrm{E}[(-1)^a \cdot (-1)^b] = \cos^2(\theta_A + \theta_B) - \sin^2(\theta_A + \theta_B)$.

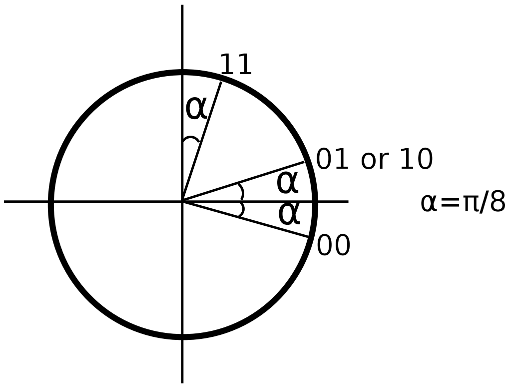

Figure 1: Figure depicting the value of $\theta_A + \theta_B$ for the four possible measurement types.

The value of $|\theta_A + \theta_B|$ is $\pi/8$ for the three measurement types (M_A^0, M_B^0), (M_A^0, M_B^1) and (M_A^1, M_B^0). For the fourth measurement type (M_A^1, M_B^1), the value of $|\theta_A + \theta_B|$ is $3\pi/8$. (See Figure 1). Thus for the first three types of measurement pairs, their corresponding quantities, namely, $\mathrm{E}[A_0B_0]$, $\mathrm{E}[A_0B_1]$, and $\mathrm{E}[A_1B_0]$ are all equal to $\cos^2(\pm\pi/8) - \sin^2(\pm\pi/8) = 1/\sqrt{2}$. For the fourth type of measurement, the quantity $\mathrm{E}[-A_1B_1] = \sin^2(3\pi/8) - \cos^2(3\pi/8) = 1/\sqrt{2}$. Thus, the sum of the expectations of all these four quantities is $2\sqrt{2} > 2$. That is, Bell's inequality doesn't hold in the quantum mechanical model.

As we mentioned, experiments conducted verify that the sum of these expectations indeed matches what is predicted by quantum mechanics, and in particular, is above 2.

3.2 Computer Science interpretation of the Bell inequality

Consider the following two party game with Alice and Bob. Alice and Bob receive a one bit input each, namely r and s, chosen uniformly at random. These input bits say which measurement is going to be performed. The goal is for both of them to output one bit each, namely a and b, such that $a \oplus b = r \wedge s$, without any communication after the inputs have been given. Classically (deterministic or randomized), the probability of success is at most 0.75.

In the quantum setting, Alice and Bob have a single qubit each of the entangled system $|\phi^-\rangle = |00\rangle - |11\rangle$. Alice's strategy is to apply the measurement M_A^r above, i.e., when $r = 0$ she rotates her qubit by $\theta_A^0 = -\pi/16$ before measurement, and when $r = 1$ she rotates her qubit by $\theta_A^1 = 3\pi/16$ before measurement. Bob follows a similar strategy, using the angles θ_B. By the above analysis, in the three cases where $r \wedge s = 0$, the probability of success is $\Pr[a \oplus b = 0] = \cos^2(\theta_A + \theta_B) = \cos^2(\pi/8)$, whereas in the one case where $r \wedge s = 1$, the probability of success is $\Pr[a \oplus b = 1] = \sin^2(\theta_A + \theta_B) = \sin^2(3\pi/8) = \cos^2(\pi/8)$. So, the overall probability of success is $\cos^2(\pi/8) \geq 0.85$, which exceeds the classical limit of 0.75.

4 Magic Square

This is the final example that we give to refute the local hidden variable theory. This is again a two party game with Alice and Bob. Alice's and Bob's strategies can each be described by a 3-by-3 matrix over $\{0, 1\}$. Alice and Bob receive a number from $\{1, 2, 3\}$ chosen uniformly at random. Alice outputs the values of the entries in that row of her matrix, and Bob outputs the values of the entries in that column of his matrix. They succeed if the sum of the elements in Alice's row is even, the sum of the elements in Bob's column is odd, and the row and column agree at the point of intersection in the matrix.

Classically, no protocol can have a success probability more than 8/9. This is because it cannot be the case that all the row sums are even in Alice's matrix, and all the column sums are odd in Bob's matrix, and both matrices agree everywhere, as that would mean that the sum of all the elements in the matrix is simultaneously odd and even! Thus, for any deterministic strategies there is at least one input on which they fail. It follows that the success probability of deterministic (or even randomized) strategies is at most 8/9, a value that can be achieved.

But quantum mechanically, we can achieve a success probability of 1. We omit the proof here.