CMSC 657: Introduction to Quantum Information Processing
Lecture 27

Instructor: Daniel Gottesman

Fall 2024

1 Bell Inequalities

Recall that we are considering a game played by spatially-separated Alice and Bob who are trying to replicate a non-local box:

Definition 1. *A perfect* non-local box *is a operation which takes two single-bit inputs a and b and gives two single-bit outputs x and y such that x and y each separately have a probability distribution of* 50% 0 *and* 50% 1 *for all inputs but $x \oplus y = ab$. (That is, x and y agree unless $a = b = 1$, in which case they disagree.)*

These conditions imply that for a perfect non-local box,

$$P((x,y) = (0,0)|(a,b) \neq (1,1)) = P((x,y) = (1,1)|(a,b) \neq (1,1)) = 1/2 \tag{1}$$
$$P((x,y) = (0,1)|(a,b) = (1,1)) = P((x,y) = (1,0)|(a,b) = (1,1)) = 1/2. \tag{2}$$

First, we can consider what Alice and Bob can do if they are purely classical, but can pre-agree on strategy and some random numbers λ, a *hidden variable*. Then we will look at what happens when Alice and Bob share entanglement.

Consider some possibilities for strategy for Alice and Bob. One option is for them to say, λ is one random bit, and just let your output (x or y, respectively) be equal to λ. Then when a and b are not both 1, their answers are the same, which is correct, but when $a = b = 1$, the answers are still the same but they are supposed to be different. Thus, if the pair (a, b) is uniformly random, they "win" the game 3/4 of the time. Or they could do something that actually uses a and b. For instance, they could have Alice always use the bit λ but Bob uses λ when $b = 0$ and $1 - \lambda$ when $b = 1$. This works when $(a, b) = (0, 0)$, $(a, b) = (1, 0)$, and $(a, b) = (1, 1)$, but not when $(a, b) = (0, 1)$. Again, they win with probability 3/4.

Theorem 1. *For any strategy and distribution on λ, Alice and Bob can never win with probability greater than* 3/4*.*

Proof. Let us relax the condition that x and y must be each separately uniformly distributed. Then the overall probability that Alice and Bob can win with uniform (a, b) is

$$\begin{aligned} P(\text{win}) = &\frac{1}{4}[P(x = y|(a,b) = (0,0)) + P(x = y|(a,b) = (0,1)) + \\ &+ P(x = y|(a,b) = (1,0)) + P(x \neq y|(a,b) = (1,1))] \end{aligned} \tag{3}$$

Also,

$$P(x = y|(a,b) = (0,0)) = P((x,y) = (0,0)|(a,b) = (0,0)) + P((x,y) = (1,1)|(a,b) = (0,0)), \tag{4}$$

and similarly for the other $P(x = y|a, b)$.

All of these Ps are averaged over values of λ. We have that

$$P((x,y)=(0,0)|a,b)=\sum_{\lambda}P(\lambda)P(x=0|a,\lambda)P(y=0|b,\lambda), \tag{5}$$

and so on. Since $P(\text{win})$ is just a linear function of things of the form $P(x,y|a,b)$, the sum over λ can be moved to the front, writing

$$P(\text{win})=\sum_{\lambda}P(\lambda)P(\text{win}|\lambda), \tag{6}$$

which means that an upper bound of $P(\text{win})$ can be set by the maximum value of $P(\text{win}|\lambda)$ over λ. That is, choosing a random λ doesn't help Alice and Bob to get the relative values of x and y right (although they do actually have to vary λ in order get x and y equally likely to be 0 and 1). They should just pick the best value of λ.

For this particular value of λ, when $a=0$ either $x=0$ or $x=1$. We can pick either without loss of generality since the equations are all invariant if we flip both x and y. Let us say $x=0$. Thus, $P(x=0|a=0,\lambda)=1$ and $P(x=1|a=0,\lambda)=0$. This means that

$$P(x=y|(a,b)=(0,0),\lambda)=P(y=0|b=0,\lambda) \tag{7}$$
$$P(x=y|(a,b)=(0,1),\lambda)=P(y=0|b=1,\lambda). \tag{8}$$

Let us consider two cases. In one case, $P(x=0|a=1,\lambda)=0$, and in the other case, $P(x=0|a=1,\lambda)=1$. In the first case,

$$P(x=y|(a,b)=(1,0),\lambda)=P(y=1|b=0,\lambda) \tag{9}$$
$$P(x\neq y|(a,b)=(1,1),\lambda)=P(y=0|b=1,\lambda), \tag{10}$$

so

$$P(\text{win}|\lambda)=\frac{1}{4}[P(y=0|b=0,\lambda)+P(y=0|b=1,\lambda)+P(y=1|b=0,\lambda)+P(y=0|b=1,\lambda)]. \tag{11}$$

Now, $P(y=0|b,\lambda)+P(y=1|b,\lambda)=1$, so

$$P(\text{win}|\lambda)=\frac{1}{4}[1+2P(y=0|b=1,\lambda)]\leq 3/4. \tag{12}$$

In the second case, when $P(x=0|a=1,\lambda)=1$,

$$P(x=y|(a,b)=(1,0),\lambda)=P(y=0|b=0,\lambda) \tag{13}$$
$$P(x\neq y|(a,b)=(1,1),\lambda)=P(y=1|b=1,\lambda), \tag{14}$$

so

$$P(\text{win}|\lambda)=\frac{1}{4}[P(y=0|b=0,\lambda)+P(y=0|b=1,\lambda)+P(y=0|b=0,\lambda)+P(y=1|b=1,\lambda)] \tag{15}$$
$$=\frac{1}{4}[2P(y=0|b=0,\lambda)+1] \tag{16}$$
$$\leq 3/4. \tag{17}$$

□

So now we know that the best a local hidden variable theory can do, basically a classical theory, is to win the non-local box game with probability 3/4. It turns out that quantum mechanics can do better!

Theorem 2. *If Alice and Bob share entanglement, they can win the non-local box game with probability* $\frac{1+\sqrt{2}}{2\sqrt{2}}=0.85\ldots$.

Proof. Alice and Bob share a Bell state $1/\sqrt{2}(|00\rangle + |11\rangle)$. When $a = 0$, Alice measures in the standard (Z) basis. When $a = 1$, Alice performs a Hadamard rotation and then measures. In either case, Alice lets x be equal to the measurement result. When $b = 0$, Bob rotates by

$$U = \begin{pmatrix} \cos \pi/8 & \sin \pi/8 \\ -\sin \pi/8 & \cos \pi/8 \end{pmatrix} \tag{18}$$

and then measures. When $b = 1$, Bob rotates by $U^\dagger$ and then measures. In either case, Bob lets y be the measurement result.

Let us calculate the various probabilities: When $b = 0$, Bob rotates his qubit by U, giving the state

$$\frac{1}{\sqrt{2}}(\cos(\pi/8)|00\rangle - \sin(\pi/8)|01\rangle + \sin(\pi/8)|10\rangle + \cos(\pi/8)|11\rangle). \tag{19}$$

Thus,

$$P(x = y|(a, b) = (0, 0)) = \cos^2 \pi/8 = \frac{1}{2}(1 + \cos \pi/4) = \frac{1 + \sqrt{2}}{2\sqrt{2}}. \tag{20}$$

When $(a, b) = (1, 0)$, Alice also rotates by the Hadamard, giving the state

$$\frac{1}{2}[(\cos(\pi/8)+\sin(\pi/8))|00\rangle+(-\sin(\pi/8)+\cos(\pi/8))|01\rangle+(\cos(\pi/8)-\sin(\pi/8))|10\rangle+(-\sin(\pi/8)-\cos(\pi/8))|11\rangle], \tag{21}$$

so

$$P(x = y|(a, b) = (1, 0)) = \frac{1}{2}(\cos \pi/8 + \sin \pi/8)^2 = \frac{1}{2}(1 + 2\cos \pi/8 \sin \pi/8) = \frac{1}{2}(1 + \sin \pi/4) = \frac{1 + \sqrt{2}}{2\sqrt{2}}. \tag{22}$$

When $b = 1$, we get the same states with $\pi/8$ replaced by $-\pi/8$, so

$$P(x = y|(a, b) = (0, 1)) = \cos^2 \pi/8 = \frac{1 + \sqrt{2}}{2\sqrt{2}} \tag{23}$$

$$P(x \neq y|(a, b) = (1, 1)) = \frac{1}{2}(1 + 2\cos \pi/8 \sin \pi/8) = \frac{1 + \sqrt{2}}{2\sqrt{2}}. \tag{24}$$

The total win probability is therefore

$$P(\text{win}) = \frac{1 + \sqrt{2}}{2\sqrt{2}}. \tag{25}$$

□

Thus, the quantum strategy beats the best classical strategy. By now, this is probably not too surprising, since we are used to quantum systems being better than classical ones, but it has a number of important consequences. The first is that it is a death knell for any attempt to explain quantum mechanics by any sort of local classical physics, even one with exponentially many degrees of freedom (to explain any computational speedups). It also has important practical implications, making possible certain kinds of quantum protocols. One such example is quantum key distribution, which we will talk about next class.

2 Quantum Communication Complexity

Bell inequalities can be viewed as a quantum advantage for performing a certain kind of distributed computational task, that of generating certain correlated distributions. But quantum communication can give an advantage to more practical distributed computational tasks as well. This is the realm of *quantum communication complexity.*

To be specific, Alice and Bob each have their own inputs a and b. They wish to compute some function $f(a, b)$. They are not very concerned about the computational time – it may well be an easy function to compute if you have both a and b. However, Alice doesn't know b and Bob doesn't know a, and communication between them is slow enough to count. So in communication complexity, we count the number of bits of communication needed to compute the function f.

As a concrete example, suppose you (Bob) are trying to arrange a Zoom meeting with your advisor (Alice) while she is away. Each person's input is a string of bits representing their calendar, 0 if that time slot is full and 1 if it is available. You are trying to find a time slot t such that $a_t = b_t = 1$ if such a time slot exists (or for a simpler version, just whether such a time slot exists at all). You could certainly do so if one person sends their whole calendar to the other. If there are N time slots, this needs N bits of communication. It turns out that indeed, using classical communication, $\Omega(N)$ bits of communication are required.

What if Alice and Bob can send qubits back and forth? Notice that they can do the following:

1. Suppose Alice has the state $\sum_t \alpha_t |t\rangle$ to start. She coherently computes $|a_t\rangle$ in a second register, to get the state $\sum_t \alpha_t |t\rangle|a_t\rangle$.
2. Alice sends both systems to Bob, requiring $\lceil \log N \rceil + 1$ qubits of communication.
3. Bob coherently computes b_t from t in a new register, giving the state $\sum_t \alpha_t |t\rangle|a_t\rangle|b_t\rangle$.
4. Bob does a controlled-Z operation on the last two qubits, giving $\sum_t \alpha_t (-1)^{a_t b_t} |t\rangle|a_t\rangle|b_t\rangle$.
5. Bob uncomputes b_t and sends the state back to Alice, requiring another $\lceil \log N \rceil + 1$ qubits of communication.
6. Alice uncomputes a_t, producing the state $\sum_t \alpha_t (-1)^{a_t b_t} |t\rangle$.

Notice that this sequence of steps, requiring $O(\log N)$ qubits of communication, has the same effect on Alice's state as a phase oracle computing the function $f(t) = a_t b_t$. Remember that our goal in this problem is to find a t such that $f(t) = 1$. This is exactly what Grover's algorithm is good for! So by running Grover's algorithm implementing the oracle as above, Alice and Bob can find a time to meet using only $O(\sqrt{N} \log N)$ qubits of communication, potentially much faster than the classical answer of $\Theta(N)$.

The quantum protocol can be reduced to $O(\sqrt{N})$ qubits of communication, but that is the limit.