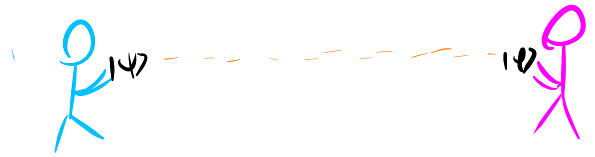
CMPT 476 Lecture 8

Bell's inequality and non-local games

Last class we discussed the EPR paradox which seemed to allow instantaneous communication between Alice and Bob. This led Einstein and others to believe that quantum theory was incomplete since it appeared to violate relativity. They posited that a complete picture of reality should be based on local hidden variables. Today, we look at Bell's theorem which famously showed that quantum mechanics cannot be predicted by any local hidden variable model.

(Local hidden variable models)

Let Alice and Bob share an entangled pair



(e.g. for concreteness, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$)

A local hidden variable model asserts that for a set (or all?) possible single-qubit measurements M_i the result of measuring M_i on Alice or Bob's qubit was pre-determined at the time of entanglement.

What does this mean?

Say we have 2 measurements M_x & M_z, each with 2 results, 0 or 1. Denote the result of measuring Alice or Bob's qubit $M_{\{x,z\}}(A)$ & $M_{\{x,z\}}(B)$. This means that the 4 values $M_x(A)$, $M_z(A)$, $M_x(B)$, $M_z(B)$ exist in the universe and are independent of who measures first and in which bases they measure.

(Bell's inequality)

Let $A_0 = (-1)^{M_x(A)}$, $A_1 = (-1)^{M_z(A)}$

$B_0 = (-1)^{M_x(B)}$, $B_1 = (-1)^{M_z(B)}$

Then (on average) ← needed to violate the inequality later

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 \leq 2$$

Pf

Note that $B_0 = \pm B_1$. If $B_0 = B_1$ then

$$A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 = 2A_0 = \pm 2$$

Over n times, the average is hence

$$\frac{\sum_i A_0^i B_0^i + A_0^i B_1^i + A_1^i B_0^i + A_1^i B_1^i}{n} \leq \frac{2n}{n} = 2$$

(Bell's theorem)

The inequality above can be violated with an entangled quantum state:

1. Start with the entangled state
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

2. Let $M_X(A)$ be meas. in $\{|0\rangle, |1\rangle\}$
$M_Z(A)$ be meas. in $\{|+\rangle, |-\rangle\}$
$M_X(B)$ be meas. in $\{\overset{|a_0\rangle}{\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle}, \overset{|a_1\rangle}{-\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle}\}$
$M_Z(B)$ be meas. in $\{\underset{|b_0\rangle}{\cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle}, \underset{|b_1\rangle}{\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle}\}$

3. Now we calculate meas. statistics... yuck

$$|\langle 0|\langle a_0| \cdot |\psi\rangle|^2 = |(\cos\frac{\pi}{8}\langle 00| + \sin\frac{\pi}{8}\langle 01|)\frac{1}{\sqrt{2}}\underbrace{(|00\rangle + |11\rangle)}_{\text{only non-zero term}}|^2$$
$$= \frac{1}{2}\cos^2\frac{\pi}{8}$$

$$|\langle 0|\langle a_1| \cdot |\psi\rangle|^2 = \frac{1}{2}\sin^2\frac{\pi}{8}$$
$$|\langle 1|\langle a_0| \cdot |\psi\rangle|^2 = \frac{1}{2}\sin^2\frac{\pi}{8}$$
$$|\langle 1|\langle a_1| \cdot |\psi\rangle|^2 = \frac{1}{2}\cos^2\frac{\pi}{8}$$

So
$$A_0 B_0 = (-1)^0(-1)^0\frac{1}{2}\cos^2\frac{\pi}{8} + (-1)^0(-1)^1\frac{1}{2}\sin^2\frac{\pi}{8} + (-1)^1(-1)^0\frac{1}{2}\sin^2\frac{\pi}{8} + (-1)^1(-1)^1\frac{1}{2}\cos^2\frac{\pi}{8}$$
$$= \cos^2\frac{\pi}{8} - \sin^2\frac{\pi}{8}$$
$$= \frac{\sqrt{2}}{2}$$

(formally this is the expected value of $A_0 B_0$)

4. By a similar argument, the expected values are:

$$\mathbb{E}(A_0 B_1) = \frac{\sqrt{2}}{2}, \ \mathbb{E}(A_1 B_0) = \frac{\sqrt{2}}{2}, \ \mathbb{E}(A_1 B_1) = -\frac{\sqrt{2}}{2}$$

5. Now, what is the expected value of the sum?

$$\begin{aligned}
&\mathbb{E}(A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1) \\
&= \mathbb{E}(A_0 B_0) + \mathbb{E}(A_0 B_1) + \mathbb{E}(A_1 B_0) - \mathbb{E}(A_1 B_1) \\
&= 4 \cdot \frac{\sqrt{2}}{2} \\
&= 2\sqrt{2} \\
&> 2
\end{aligned}$$

(Non-local games)

A common theme in Quantum computer science is to phrase the above in a more computational way: as a game where Alice and Bob are not allowed to communicate directly, but share entanglement. It's helpful to see both perspectives, though non-local games fail* to capture the modern generalization of Bell's theorem to the Kochen-Specker theorem and notions of contextuality, which we lack the language to express at this point.

* Others may disagree with me here

(CHSH game (Clauser, Horne, Shimony & Holt))

The game is a co-operative one where Alice and Bob try to win against a referee. They are allowed to communicate before the game begins, but not while the game is on. Here are the rules:

1. The referee gives Alice and Bob each a bit a, b respectively in secret.

2. Without communicating, Alice and Bob each give the referee a bit back, x and y

3. Alice and Bob win if and only if

$$\underbrace{x \oplus y}_{\text{exclusive OR, i.e. } x+y \bmod 2} = a \cdot b$$

(The classical strategy)

$x = y = 0$. Observe that $x \oplus y = 0 = a \cdot b$ unless $a = b = 1$, so if a & b are random, win $3/4$ times

(Optimality for classical)

Note that any deterministic strategy, i.e. functions

$$f : a \longmapsto x, \quad g : b \longmapsto y$$

fails on at least one input (25% of the time), since

$$\sum_{a,b \in \{0,1\}} f(a) \oplus g(b) = 0 \bmod 2$$

$$\sum_{a,b \in \{0,1\}} a \cdot b = 1 \bmod 2$$

To see the previous fact we often arrange the outcomes in a table (called a parity argument)

a	b	$f(a) \oplus g(b)$	$a \cdot b$
0	0	$f(0) \oplus g(0)$	0
0	1	$f(0) \oplus g(1)$	0
1	0	$f(1) \oplus g(0)$	0
1	1	$f(1) \oplus g(1)$	1

Summing the rows mod 2 we see that $f(a)$ and $g(b)$ appear twice for each value of a & b, hence they cancel, since $x+x=0 \bmod 2$ for all $x \in \{0,1\}$

Since any probabilistic strategy is a weighted sum of deterministic ones, no such strategy can succeed more than 75% or $3/4$ on average.

(Quantum strategy)

Pre-game: Alice and Bob prepare the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alice: if $a=0$ then measure in the $\{|0\rangle, |1\rangle\}$ basis
$a=1$ then measure in the $\{|+\rangle, |-\rangle\}$ basis

Bob: if $b=0$ then measure in $\{|a_0\rangle, |a_1\rangle\}$
$b=1$ then measure $\{|b_0\rangle, |b_1\rangle\}$

Claim: Alice and Bob win 85% of the time.

Proof: Suppose $a=b=0=a\cdot b$. Then Alice & Bob win if they measure 0&0 (i.e. $|0\rangle|a_0\rangle$) or 1&1 (i.e. $|1\rangle|a_1\rangle$). We computed these probabilities before:

$$\langle 0|\langle a_0| \cdot |\psi\rangle + \langle 1|\langle a_1| \cdot |\psi\rangle = \cos^2\frac{\pi}{8} \approx 0.85$$

The other cases are similar $\square$

(Non-locality and Quantum computation)

The key take-away is that with shared entanglement, only local operations (i.e. operators & measurements only on individual qubits or subsystems) are needed to perform some tasks which would classically require communication.