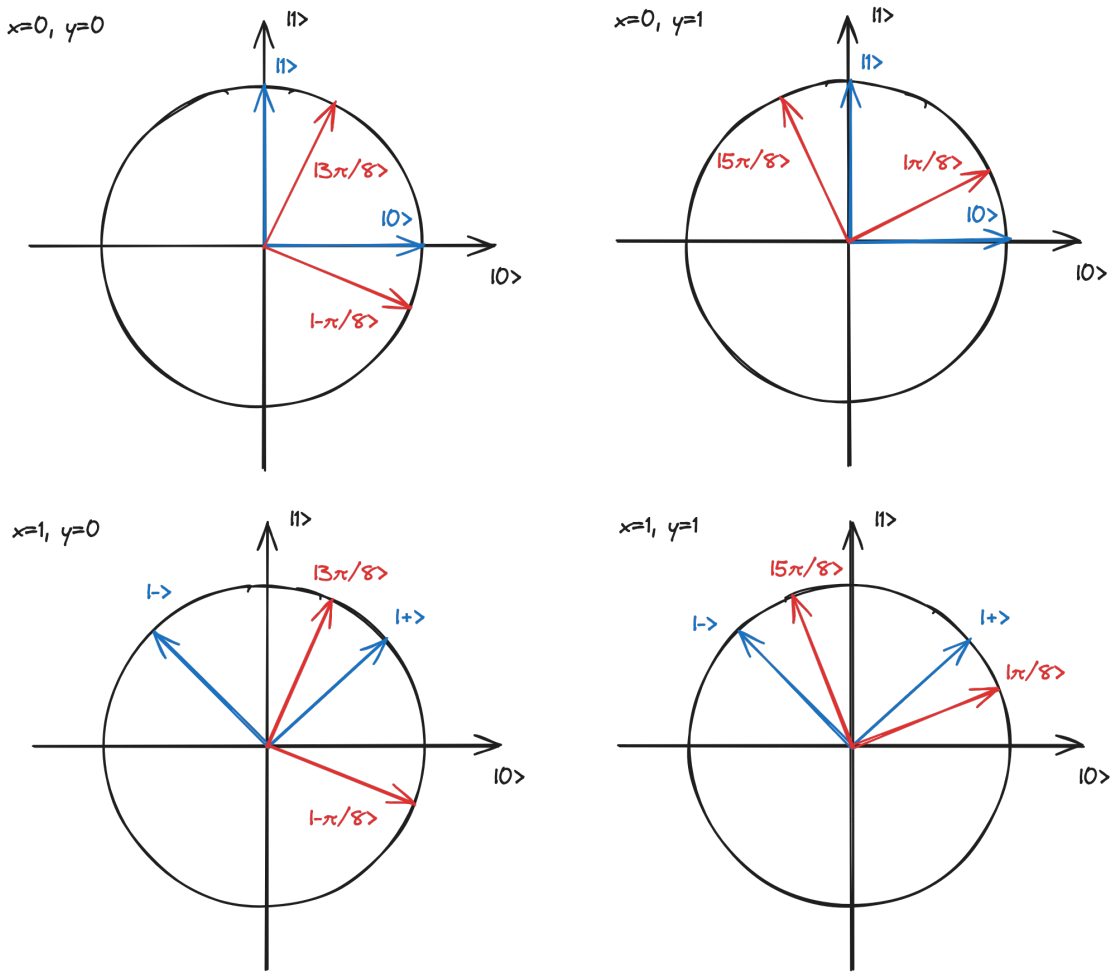
Alice and Bob decide on the following strategy.

Alice	Bob
If $x = 0$, measure in $\{\|0\rangle, \|1\rangle\}$ basis.	If $y = 0$, measure in $\{\|-\pi/8\rangle, \|3\pi/8\rangle\}$ basis.
If $x = 1$, measure in $\{\|+\rangle, \|-\rangle\}$ basis.	If $y = 1$, measure in $\{\|\pi/8\rangle, \|5\pi/8\rangle\}$ basis.
If the outcome is $\|0\rangle$ or $\|-\rangle$, output $a = 0$.	If the outcome is $\|\pi/8\rangle$ or $\|-\pi/8\rangle$, output $b = 0$.
If the outcome is $\|1\rangle$ or $\|+\rangle$, output $a = 1$.	If the outcome is $\|3\pi/8\rangle$ or $\|5\pi/8\rangle$, output $b = 1$.

The following figure draws the bases that Alice and Bob will measure in depending on the results of the random bits.



Question 83. What is the probability that Alice and Bob win against Charlie if both of the random bits they receive are 0?

Again, we won't show it here but the win probability that we get for the strategy stated above is optimal when allowing quantum entanglement. Since this strategy beats the bound that any classical strategy can achieve, we can rule out the hidden variable theory that we stated above (and most other ones!). Many other "non-local" games have been designed where two party quantum strategies using entangled bits outperform any classical strategies.

The CHSH game can be (and has been) tested experimentally. The probability of success can estimated by repeating the experiment many times, and if the probability is over 75%, this is bad news for the Hidden Variable Theory supporters!

Question 84. Why is a higher probability than 75% bad news for the Hidden Variable Theory?

Maybe there is still a loophole in the CHSH game that explains why it violates the Hidden variable theories. One possible loophole that could be considered is what people called "the Locality Loophole".

The designers of this loophole suggested that maybe the entangled qubits send each other some signal after one is measured to inform the other qubit what the collapsed state is.

Question 85. How can we rule out the locality loophole?

9.2 Generating Random Numbers

"Einstein, stop telling God what to do."

- Neils Bohr

Initially, the Bell inequality was taught because it was conceptually important. The CHSH game was only useful as a thought experiment, not something with real applications. However, researchers have come up with some applications for the CHSH game.

Generating *truly* random numbers is an important task in computing, especially for cryptography. Classically, we rely on pseudorandom number generators, which only mimic randomness up to some level of undetectability.

Quantum computers could be useful for generating random numbers.

Question 86. Design a single qubit circuit that outputs a random bit.

However, how can we be sure that the hardware we are using is working correctly and hasn't been tampered by some adversary? We would like some way to **certify** that we have a truly random system.

- Create two boxes that share a pair of entangled qubits.
- The boxes could be faulty or even maliciously designed.
- Play the CHSH game with these two boxes. If they win > 75% of the time, we know that there is some level of randomness in the responses.
- We know of ways to extract small bits of randomness to get longer uniformly random strings.
- Playing the game with $x = y = 0$ most of the time with an occasional "curveball" is sufficient to analyze the randomness.

Similar techniques have been applied to design a strategy using the CHSH game to detect whether or not a computation was performed on a quantum computer or not.

In homework, we will explore some other non-local games and hidden variable theories.