※ Information 3: Hidden Variable Theories and the CHSH Game

"[Quantum mechanics] delivers much but it hardly brings us closer to the Old One's secret. In any event, I am convinced that He is not playing dice."

- Albert Einstein

Classical physics allow us to predict the exact trajectories and outcomes of physical systems, given that we know enough information in the beginning. We model coin flips as being events that have a 0.5 probability of landing in heads or tails, but in principle, if we had enough precise control over our coinflip setup, we could predict exactly where the coin would land.

Quantum physics however, does not seem to have this property. As we discussed before, if Alice and Bob share a qubit from a Bell pair, no matter how far away they are, Alice's measurement result seems to affect what Bob's measurement result is! $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alice measures in some basis $\{|v\rangle, |v^\perp\rangle\}$

State collapses to either

- $|vv\rangle$
- $|v^\perp v^\perp\rangle$

Question 20. Why is it problematic that Alice's measurement result affects Bob measurement result no matter how far they are separated?

It would imply information is being shared faster than the speed of light.

There's also too many bases!

To reconcile this conflict, scientists hypothesized that particles had "hidden variables" representing the possible outcomes they would be in if they were measured. One computer scientist type hidden variable theory might hypothesize the following: When Alice and Bob's qubits first get entangled, they decide what their measurement result will be across all possible bases. If they are too far apart to communicate fast enough, they will just consult the local list to decide what state to collapse to.

A — B

s.b. $|0\rangle$

H.b. $|+\rangle$

$|v\rangle$ $|v^\perp\rangle$

⋮

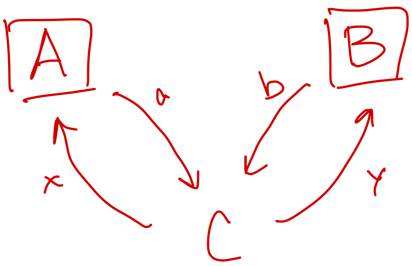
John Bell and others designed an experiment which ruled out most known hidden variable theories, including the one we mentioned above. Here, ruling out means that the experiment behaves in a way which would contradict the assumption that a hidden variable theory exists. Instead of looking at the experiment, we will study a game that isolates the critical parts.

8.1 The CHSH Game

Here are the rules of the game:

- Alice and Bob will be separated with no way to communicate with each other.
- Charlie will flip two coins, and send a bit to Alice and Bob depending on the outcomes. Let's say he sends a 0 if tails, and a 1 if heads.
- After receiving the random bit x, Alice sends back an answer bit a to Charlie.
- After receiving the random bit y, Bob sends back an answer bit b to Charlie.
- Alice and Bob win against Charlie if the answer bits and random bits satisfy

$$\boxed{a + b \ (\mathrm{mod}\ 2) = xy.} \tag{9}$$



Question 21. If Charlie flipped heads for Alice's bit, and tails for Bob's bit, what is a choice for Alice and Bob's response for them to win?

Alice → H → $x=1$

Bob → T → $y=0$

$x \cdot y = 0$

$a=0,\ b=0 \Rightarrow a+b=0.$

$a=1,\ b=1 \Rightarrow a+b=0$

Question 22. If Charlie flipped heads for both coins, what is a choice for Alice and Bob's response for them to win?

x	y	xy	Win condition
0	0	0	$a=b.$
0	1	0	$a=b.$
1	0	0	$a=b.$
1	1	1	$a \neq b.$

Alice and Bob can discuss a strategy and share as many bits of information as they would like with each other, but they are not allowed to communicate once the game begins.

Question 23. If Alice and Bob decide to use the strategy that they *always* output $a = 0$ and $b = 0$, what is the probability that they win?

Bell inequality

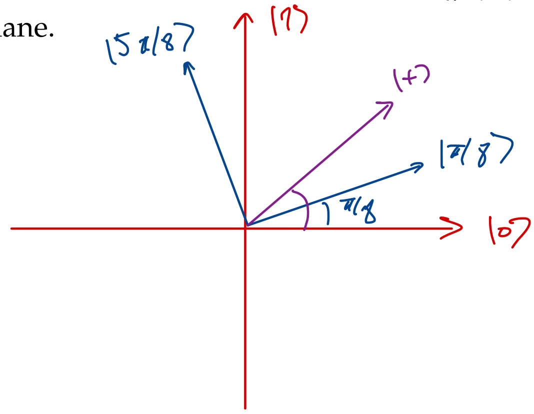
$3/4$ or $0.75.$

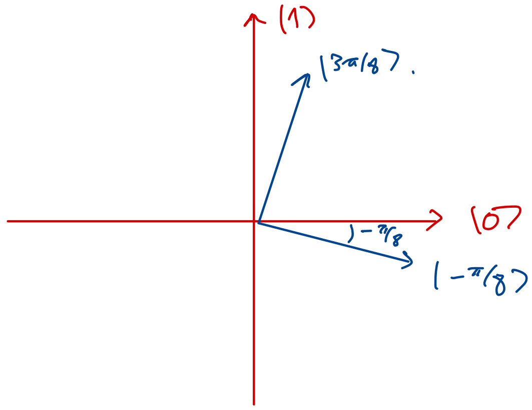
We won't prove it here, but the above winrate is the best classical strategy for Alice and Bob. A hidden variable theory is trying to explain quantum mechanics in a classical way, so if qubits do store hidden variables, there should be no way to consistently beat the CHSH game with a probability higher than we calculated above.

For the remainder of the chapter, we will use the following shorthand to describe a state with real amplitudes:

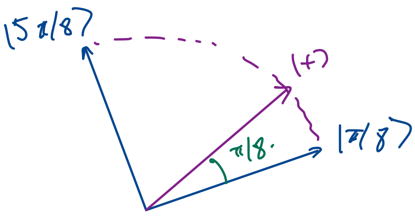
$$|\theta\rangle := \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \tag{10}$$

Question 24. Draw the two bases $\{|\pi/8\rangle, |5\pi/8\rangle\}$ and $\{|-\pi/8\rangle, |3\pi/8\rangle\}$ in the $|0\rangle$, $|1\rangle$ plane.





Question 25. Suppose the state $|+\rangle$ is measured in the $\{|\pi/8\rangle, |5\pi/8\rangle\}$ basis. What is the probability of each outcome? Express your answer as a function of $\cos\theta$ and $\sin\theta$.



$|+\rangle = \alpha\,|\pi/8\rangle + \beta\,|5\pi/8\rangle$

prob. of $|\pi/8\rangle$: $|\alpha|^2$

$\alpha = \cos \pi/8$ $\quad \beta = \sin \pi/8.$

Prob. of $|\pi/8\rangle$: $\cos^2 \pi/8.$ ≈ 0.85

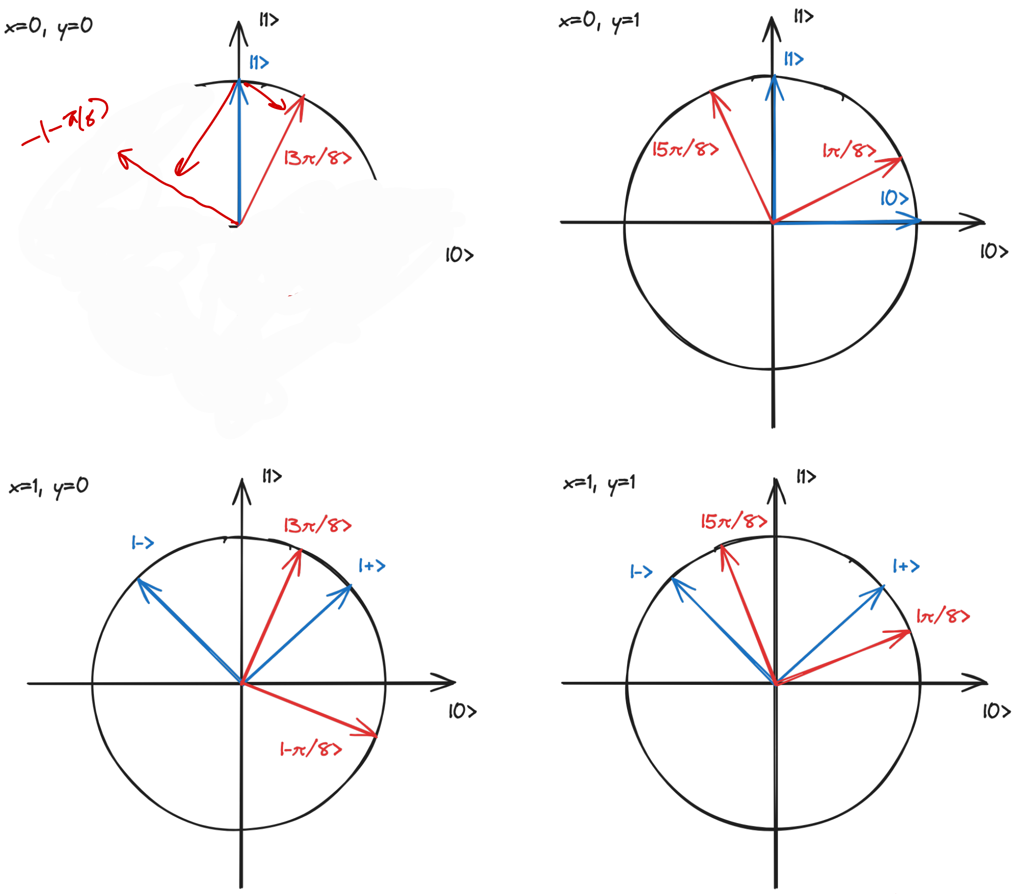
Prob. of $|5\pi/8\rangle$: $\sin^2 \pi/8.$ ≈ 0.15

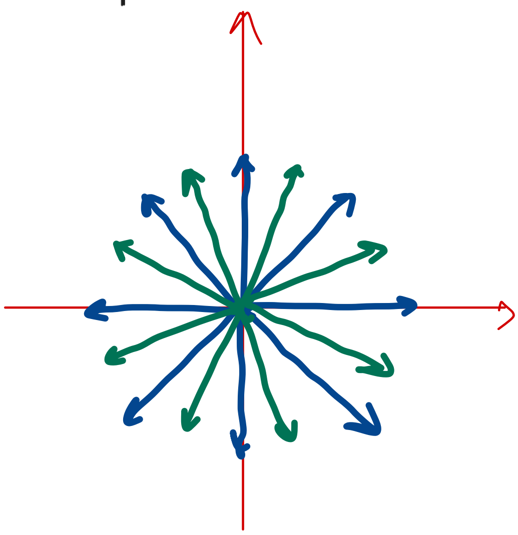
Alice and Bob take one qubit each from a Bell pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

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.

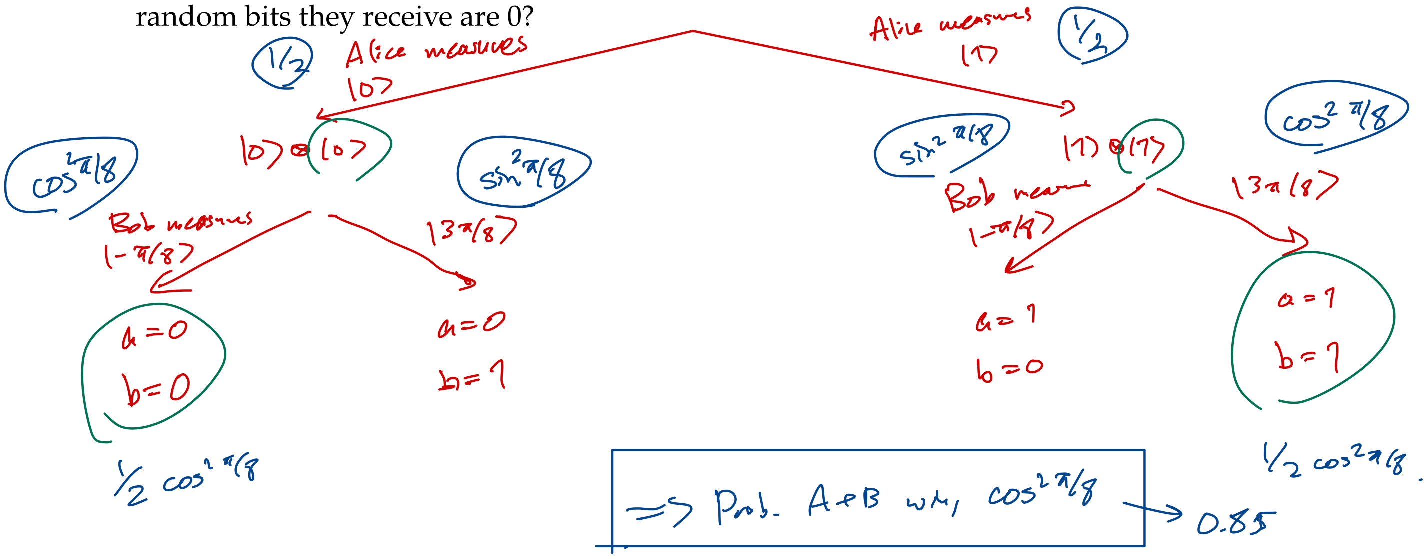




$1/\sqrt{2}\,(|00\rangle + |11\rangle)$

$\{|0\rangle, |1\rangle\}$ $\{|-\pi/8\rangle, |3\pi/8\rangle\}$.

Question 26. What is the probability that Alice and Bob win against Charlie if both of the random bits they receive are 0?



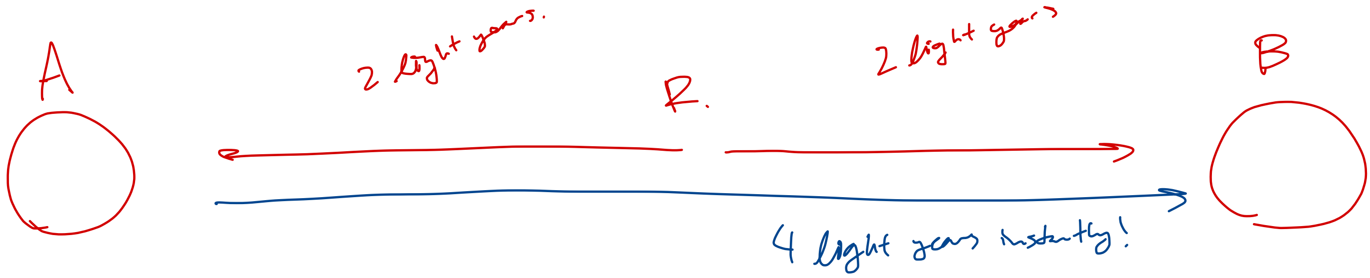
Again, we won't show it here but the win probability that we get for the strategy stated above is optimal when allowing quantum entanglement. Since this strategy beats the bound that any classical strategy can achieve, we can rule out the hidden variable theory that we stated above (and most other ones!). 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!

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 27. How can we rule out the locality loophole?



8.2 Generating Random Numbers

"Einstein, stop telling God what to do."

- Neils Bohr

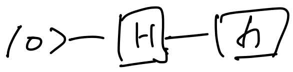
Initially, the Bell inequality was taught because it was conceptually important. The CHSH game was only useful as a thought experiment, not something with real applications. However, researchers have come up with some applications for the CHSH game.

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.

Assume some problem is NP-hard

Question 28. Design a single qubit circuit that outputs a random bit.



↳ s.b. measurement.

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.

$(|00\rangle + |11\rangle)$

$\downarrow$

$|00\rangle$