QUANTUM INFORMATION THEORY

The CHSH Inequality

Stuti Shah
Kapitza Society, Spring 2022, Prof. S.G. Rajeev
University of Rochester

April 27, 2022

1 Introduction

This paper is a compilation of the content I covered in two of the lectures I gave for Kapitza meetings this semester. We continued studying quantum information from last semester and in this paper we begin by looking at the CHSH inequality, followed by the CHSH game, and nally a di erent topic yet one with remote similarities with the previously mentioned topics, a quantum analog of Shannon's noiseless coding theorem.

2 The CHSH Inequality

ω here is the unknown or `hidden' variable from assumption 1, and A_x and B_y do not depend on y and x respectively.

The Causer-Horne-Shimony-Holt (CHSH) Inequality

Statement: The description of ± 1 valued measurements made by the devices $A_1; A_2; B_1; B_2$, satisfies

$$|\langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle| \leq 2 \tag{1}$$

Proof[2]: From assumption 3, we have,

$$\langle A_1 B_1\rangle = \int A_1(\omega)B_1(\omega)dP(\omega)$$
$$\langle A_1 B_2\rangle = \int A_1(\omega)B_2(\omega)dP(\omega)$$
$$\langle A_2 B_1\rangle = \int A_2(\omega)B_1(\omega)dP(\omega)$$
$$\langle A_2 B_2\rangle = \int A_2(\omega)B_2(\omega)dP(\omega)$$

So the left hand side of (1) becomes,

$$\begin{aligned} LHS &= \int A_1(\omega)B_1(\omega)dP(\omega) + \int A_1(\omega)B_2(\omega)dP(\omega) + \int A_2(\omega)B_1(\omega)dP(\omega) - \int A_2(\omega)B_2(\omega)dP(\omega) \\ &= \int [A_1(\omega)B_1(\omega) + A_1(\omega)B_2(\omega) + A_2(\omega)B_1(\omega) - A_2(\omega)B_2(\omega)]dP(\omega) \\ &= \int [A_1(\omega)\{B_1(\omega) + B_2(\omega)\} + A_2(\omega)\{B_1(\omega) - B_2(\omega)\}]dP(\omega) \end{aligned}$$

$A_1(\omega)$ and $A_2(\omega)$ are in $\{\pm 1\}$.

For a particular $\omega \in \Omega$, we can have two conditions:

1. $B_1(\omega) = B_2(\omega)$

2. $B_1(\omega) \neq B_2(\omega)$

For case 1., $B_1(\omega) - B_2(\omega) = 0$ and $B_1(\omega) + B_2(\omega) \in \{\pm 2\}$.

For case 2., since either 1 or -1 is the only value possible, $B_1(\omega) = -B_2(\omega)$; that is, $B_1(\omega) + B_2(\omega) = 0$ and $B_1(\omega) - B_2(\omega) \in \{\pm 2\}$. Hence, the desired result is acheived.

3 The CHSH Game

“The whole point of the CHSH game [and Bell's inequality] is to prove that quantum entanglement exists! The CHSH game shows us how the physical systems of the universe are more aligned to, and better represented by, quantum physics rather than classical physics." (Eamonn Darcy)

The CHSH game is a two-player game consisting of players Alice and Bob who each receive a bit $x \in \{0, 1\}$ and $y \in \{0,1\}$

3.1 Classical strategy

A little bit of thought should convince us that in any classical scenario, Alice and Bob have a $\leq 75\%$ chance of winning.

Let us look at a proof using the CHSH inequality[3]:

Suppose that Alice and Bob return values in $\{\pm 1\}$ instead of $\{0, 1\}$. For questions x and y in $\{0, 1\}$, let's say Alice and Bob answer r_A and r_B in $\{\pm 1\}$ and that they returned a and b in $\{0, 1\}$ originally. Then, we have:

(x, y)	$a \oplus b$	$r_A r_B$
(0,0)	0	1
(0,1)	0	1
(1,0)	0	1
(1,1)	1	-1

Consider measuring devices A_0 (for $x = 0$) and A_1 (for $x = 1$) for Alice and B_0 (for $y = 0$) and B_1 (for $y = 1$) for Bob. For $x, y \in \{0, 1\}$, from assumption 2,

$$\langle A_x B_y \rangle = \sum_{r_A, r_B \in \{\pm 1\}, r_A = r_B} p(r_A, r_B | x, y) - \sum_{r_A, r_B \in \{\pm 1\}, r_A \neq r_B} p(r_A, r_B | x, y)$$

The above equation gives us difference in the probability of winning and losing for inputs equal to and not equal to (1,1).

$$P_{\text{win}} - P_{\text{lose}} = \frac{1}{4}[\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle] \leq \frac{1}{2}$$

$$P_{\text{win}} - (1 - P_{\text{win}}) \leq \frac{1}{2}$$

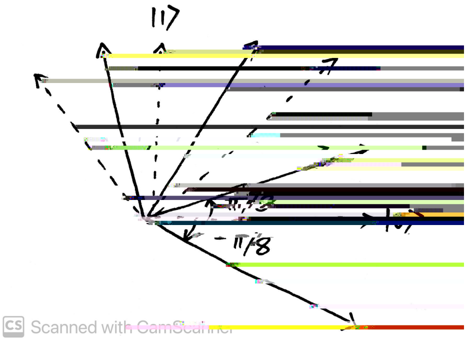
$$P_{\text{win}} \leq \frac{\frac{1}{2} + 1}{2} = \frac{3}{4} = 75\%$$

3.2 Quantum strategy

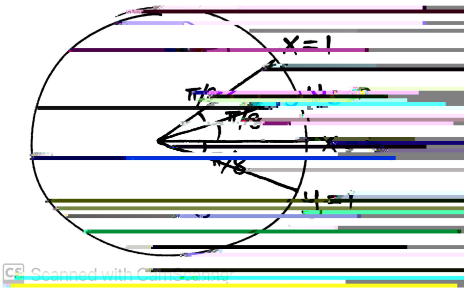
What happens if Alice and Bob were to share a Bell pair (i.e. if Alice had one qubit of the Bell state $|$

If her input is 0, she measures her qubit in the $\{|\ _0(0)\rangle, |\ _1(0)\rangle\}$ basis.
If her input is 1, she measures her qubit in the $\{|\ _0(\frac{\pi}{4})\rangle, |\ _1(\frac{\pi}{4})\rangle\}$ basis.

Here's what Bob does: Based on the input given to him, he measures his qubit in one of two bases,



If his input is 0, he measures his qubit in the $\{|\ _0(\frac{\pi}{8})\rangle, |\ _1(\frac{\pi}{8})\rangle\}$ basis.
If his input is 1, he measures his qubit in the $\{|\ _0(-\frac{\pi}{8})\rangle, |\ _1(-\frac{\pi}{8})\rangle\}$ basis.



Recall the rotational invariance of bell state: if one measures a qubit in a certain basis and measures the other qubit in a basis that is rotated by with respect to the original basis, then the probability of getting the same outcome, $P_{same} = \cos^2$.

x	y	P_{same}	$P_{different}$
0	0	$\cos^2 \frac{\pi}{8}$	-
0	1	$\cos^2 \frac{\pi}{8}$	-
1	0	$\cos^2 \frac{\pi}{8}$	-
1	1	$\cos^2 \frac{3\pi}{8}$	$1 - P_{same} = 1 - \cos^2 \frac{3\pi}{8} = \sin^2 \frac{3\pi}{8} = \cos^2 \frac{\pi}{8}$

Thus, the probability of getting the correct answer (i.e. meeting the rules of the game) is $\cos^2 \frac{\pi}{8} = 0.85 = 85\%$ for all the 4 cases. Thus, if Alice and Bob incorporate quantum strategies as opposed to classical strategies to play this game, they have a better chance at winning.[5]

4 Quantum analog of Shannon's noiseless coding theorem [6]

There are two things [7] that Shannon's noiseless coding theorem tells us:

1. It is impossible to compress data • the code rate, i.e. $\frac{\text{average no. of bits}}{\text{symbol}}$ < Shannon entropy of the source, without any certainty that no information will be lost in the process.

2. It is possible to get the code rate arbitrarily close to Shannon entropy with negligible probability of loss.

[5] Lecture 4 3 chsh inequality - youtube, (n.d.), Retrieved, 2022
[6] Preskill, J., Lecture Notes for Physics 229: Quantum Information and Computation, 1998
[7] Wikimedia Foundation, March 30, 2022, Shannon's source coding theorem, Wikipedia, Retrieved 2022

In this section, we look at quantum analog of Shannon's noiseless coding theorem. The content in this section was the topic of my second lecture for Kapitza this semester. A reason to include this topic in this paper is to illustrate that similar numbers appear in the discussion of di erent topics.

Let's say we have a message comprising of n letters that we want to deliver. There exists no bias and each n has an equal probability of being chosen, from an ensemble of pure states described by

$$\{|\psi_x\rangle; p_x\}$$

Note that the $|\psi_x\rangle$'s do not have to be necessarily orthogonal (for example, as I described in my earlier paper on density matrices, the polarization state of a photon). Based on arguments drawn from my previous paper, each letter has a density matrix

$$\rho = \sum_x p_x |\psi_x\rangle\langle\psi_x| \qquad (2)$$

to fully describe it. Since our message consists of n letters, the density matrix for the entire message is just

$$\rho^n = \rho \otimes \rho \otimes ...$$

(n times). Our task .962016 1.494 Td [(i)]TJ/F22 9.9626 Tf 3.874 0 Td [(;)-167(p)]TJ/F21 6.9738 Tu TfJ/F19 9.9626 Tf 9.3

$$
\begin{aligned}
(0') \cdot (1') &= \cos^2\frac{\pi}{8}\cdot\sin^2\frac{\pi}{8} \\
&= \frac{1}{4}\left(2\sin\frac{\pi}{8}\cos\frac{\pi}{8}\right)^2 \\
&= \frac{1}{4}\left(\sin\frac{\pi}{4}\right)^2 \\
&= \frac{1}{8} \\
&= \det
\end{aligned}
$$

and second, from (3), (4), (5), and (6):

$$|\langle 0'|\varphi_z\rangle|^2 = |\langle 0'|\varphi_x\rangle|^2 = \cos^2\frac{\pi}{8} = 0.8535$$

$$|\langle 1'|\varphi_z\rangle|^2 = |\langle 1'|\varphi_x\rangle|^2 = \sin^2\frac{\pi}{8} = 0.1465$$

Equalities (5) and (6) tell us that the $|0'\rangle$ state has equal and large overlap with both the signal states and the $|1'\rangle$ state has equal and small overlap with both the signal states, which suggests that if the input signal state is unknown to us, the best guess we can make is $|\psi_x\rangle = |0'\rangle$ and the $|0'\rangle$ state has the maximal fidelity,

$$F = \frac{1}{2}|\langle\varphi_z|\psi\rangle|^2 + \frac{1}{2}|\langle\varphi_x|\psi\rangle|^2 = \frac{1}{2}(0.8535) + \frac{1}{2}(0.8535) = 0.8535$$

Let us talk about a more specific example now that we've established some background. Say that Alice has a message that consists of three letters that she wants to send to Bob. However, she can only afford to send two of the three letters since quantum communication is expensive. The goal is for Bob to construct Alice's message (state) with maximum correctness, or fidelity. Since Alice discloses two of the letters in her message to Bob, the two letters have $F = 1$. From our previous understanding, we can figure that Bob guesses $|0'\rangle$ ($F = 0.8535$) in order to try and construct Alice's message with maximum fidelity. The total fidelity is therefore $F = 0.8535$. This seems pretty good, although, there is a better strategy for Bob to guess Alice's message with even more correctness.

Let us make our methods explicit:
What we did: We decomposed the H of one qubit into a "likely" subspace spanned by $|0'\rangle$ and an "unlikely" subspace spanned by $|1'\rangle$.
What we can do now: We can decompose the H of three qubits (since Alice's message contains 3 'letters') into "likely" and "unlikely" subspaces. Let the input signal state $|\psi\rangle$

Case 2: She measures the third qubit to be $|1\rangle$, which would mean that her input state has been projected to $\psi^{\perp}$. From (9) and (10),

$$P_{\psi^{\perp}} = 3(0.0183) + 0.0031 = 0.0581$$

For case 1, Alice sends the remaining (unmeasured, compressed) two qubits $|\psi_{\text{comp}}\rangle$ to Bob, who decompresses it to obtain:

$$|\psi'\rangle = U^{-1}(|\psi_{\text{comp}}\rangle|0\rangle)$$

For case 2, Alice sends a state that Bob would decompress to get the most likely state. Thus:

$$|\psi'\rangle = U^{-1}(|\psi_{\text{comp}}\rangle|0\rangle) = |0'0'0'\rangle$$

Through this process, Bob finds his state ρ' to be:

$$\rho' = |\psi'\rangle\langle\psi'| = E|\psi\rangle\langle\psi|E + |0'0'0'\rangle\langle\psi|1 - E|\psi\rangle\langle 0'0'0'|$$

where E is the projection onto Λ. Hence,

$$\begin{aligned} F &= \langle\psi|\rho'|\psi\rangle \\ &= (\langle\psi|E|\psi\rangle)^2 + (\langle\psi|1 - E|\psi\rangle)(\langle\psi|0'0'0'\rangle)^2 \\ &= (0.9419)^2 + (0.0581)(0.6219) \\ &= 0.9234 \end{aligned}$$

Clearly, the fidelity in this case (0.9234) is better than before (0.8535). It should only be true that as the number of letters in a message increases, the fidelity of the compressed message should increase too.

$$S(\rho) = H\left(\cos^2\frac{\pi}{8}\right) \approx 0.$$