Bell's theorem and its experimental tests aim to demonstrate that quantum mechanics cannot be explained by local hidden variable theories, which would allow outcomes to be predetermined based on hidden information

6.5 Tsirelson's inequality

The commutator measures the degree to which two operators fail to commute, i.e., the degree to which the order of application of these operators matters. The norm of an operator (or a matrix) ‖A‖. ‖A‖ is a numerical value that represents the "size" or "length" of the operator.

|| [A_1, A_2] || or || [B_1, B_2] || refers to the norm of the commutator of two operators (or matrices) ||[A_1, A_2] || or || [B_1, B_2] ||, respectively. Here these are bounded by 2.

In *classical* probability theory, the (absolute value of the) average value of the CHSH quantity

$$S = A_1(B_1 - B_2) + A_2(B_1 + B_2)$$

is bounded by 2, and this bound can be attained.

In *quantum* theory, the same value is bounded by $2\sqrt{2}$, and this bound can also be attained.

Classical Probability Theory

- Both pairs (A_1 and A_2) and (B_1 and B_2) have 4 possible outcomes where A_k and B_k (k = 1, 2) takes the values of +1 or -1 depending on the observable

To show $\|[A_1, A_2]\| \leq 2$ is bounded by 2

$$\begin{aligned}
\|[A_1, A_2]\| &= \|A_1A_2 - A_2A_1\| \\
&\leq \|A_1A_2\| + \|A_2A_1\| \\
&\leq \|A_1\|\,\|A_2\| + \|A_2\|\,\|A_1\| \\
&= 2
\end{aligned}$$

One may ask if $|\langle S\rangle| = 2\sqrt{2}$ is the *maximal* violation of the CHSH inequality, and the answer is "yes, it is": *quantum* correlations *always* satisfy the bound $|\langle S\rangle| \leqslant 2\sqrt{2}$. This is because, no matter which state $|\psi\rangle$ we pick, the expected value $\langle S\rangle = \langle\psi|S|\psi\rangle$ cannot exceed the largest eigenvalue of S, and we can put an upper bound on the largest eigenvalues of S. To start with, taking the largest eigenvalue (in absolute value) of a Hermitian matrix M, which we denote by $\|M\|$, gives a matrix norm, i.e. it has the following properties:

$$\begin{aligned}
\|M \otimes N\| &= \|M\|\|N\| \\
\|MN\| &\leqslant \|M\|\|N\| \\
\|M + N\| &\leqslant \|M\| + \|N\|
\end{aligned}$$

Quantum Theory

Given that $\|A_k\| = \|B_k\| = 1$ (for $k = 1, 2$), it is easy to use these properties to show that $\|S\| \leqslant 4$, but this is a much weaker bound than we want. However, one can show that

$$S^2 = 4(\mathbf{1} \otimes \mathbf{1}) + [A_1, A_2] \otimes [B_1, B_2].$$

Now, the norms of the commutators $\|[A_1, A_2]\|$ and $\|[B_1, B_2]\|$ are bounded by 2, and $\|S^2\| = \|S\|^2$. All together, this gives

$$\begin{aligned}
\|S^2\| &\leqslant 8 \\
\implies \|S\| &\leqslant 2\sqrt{2} \\
\implies |\langle S\rangle| &\leqslant 2\sqrt{2}
\end{aligned}$$

This result is known as the **Tsirelson inequality**.

$$S_2 = (A_1 \otimes (B_1 - B_2) + A_2 \otimes (B_1 + B_2))^2$$

$$= A_1^2 \otimes (B_1 - B_2)^2 + A_1 A_2 \otimes (B_1 - B_2)(B_1 + B_2) +$$
$$A_2 A_1 \otimes (B_1 + B_2)(B_1 - B_2) + A_2^2 \otimes (B_1 + B_2)^2$$

$$= A_1^2 \otimes (B_1^2 - B_1 B_2 - B_2 B_1 + B_2^2) + A_1 A_2 \otimes (B_1^2 + B_1 B_2 - B_2 B_1 - B_2^2)$$
$$+ A_2 A_1 \otimes (B_1^2 + B_2 B_1 - B_1 B_2 - B_2^2) + A_2^2 \otimes (B_1^2 + B_1 B_2 + B_2 B_1 + B_2^2)$$

$A_k = B_k = 1 \quad A_k^2 = B_k^2 = 1$ where $k = 1, 2$

$$= 1 \otimes (1 - B_1 B_2 - B_2 B_1 + 1) + A_1 A_2 \otimes (\cancel{1} + B_1 B_2 - B_2 B_1 \cancel{-1})$$
$$+ A_2 A_1 \otimes (\cancel{1} + B_2 B_1 - B_1 B_2 \cancel{-1}) + 1 \otimes (1 + B_1 B_2 + B_2 B_1 + 1)$$

$$= 1 \otimes 1 \cancel{- 1 \otimes B_1 B_2} \cancel{- 1 \otimes B_2 B_1} + 1 \otimes 1 + A_1 A_2 \otimes [B_1, B_2]$$
$$+ A_2 A_1 \otimes \underbrace{[B_2, B_1]}_{-[B_1, B_2]} + 1 \otimes 1 \cancel{+ 1 \otimes B_1 B_2} + \cancel{1 \otimes B_2 B_1} + 1 \otimes 1$$

$$= 4 (1 \otimes 1) + A_1 A_2 \otimes [B_1, B_2] - A_2 A_1 [B_1, B_2]$$

$$= 4 (1 \otimes 1) + [A_1, A_2] \times [B_1, B_2]$$

$$= 4 + 2 \times 2$$

$$= 8$$

$$\|S\|^2 = \|S^2\| \leq 4 + 2 \cdot 2 = 8$$

$$\|S\| \leq 2\sqrt{2}$$

To show how $|\langle S \rangle| = \|S\|$

$$|\langle S \rangle| = |\langle \psi | S | \psi \rangle| \leq \sum_{\lambda_i} |a_i|^2 |\lambda_i|$$

initial state

$|\langle \psi || = 1$

eigenvalues of S

$$\leq |\lambda_i| \sum |a_i|^2$$

$$= |\lambda_i|$$

$$= \|S\|$$

6.6 Quantum randomness

The experimental violations of the CHSH inequality have shown us that there are situations in which the measurement outcomes are truly unknown the instant before the measurement is made, and so the answer must be "chosen" randomly. We can make use of this randomness is a number of different ways, the most obvious example of which being a random number generator. Indeed, we have already met one suitable implementation:

$$|0\rangle \;—\boxed{H}—$$

The state before measurement is $(|0\rangle + |1\rangle)/\sqrt{2}$, so the two possible outcomes occur with equal probability. This is a truly random number generator, not like the pseudorandom one that is used if you ask your computer for some random data.

Starting from an initial seed of private randomness (completely unknown to any other party), **randomness expansion** is the process of extending this to a larger amount of randomness that remains completely private.

Using the idea of randomness expansion, let's assume that they start with some shared random private seed: some m-bit string that only they know. They start by generating n of these putative singlet states, and publicly decide on some value $0 < p < 1$. With this, they randomly select $\lceil pn \rceil$ of the pairs to perform a CHSH test on. Each test requires two random bits (to determine Alice and Bob's choice of measurement), so in total we will need the length m of their shared random private seed be roughly

$$m \approx 2pn - pn \log_2 p - n(1-p) \log_2 (1-p)$$

where the $\log$ terms are approximately how many bits are required to randomly choose the subset of pairs to test.

start: m-bit string

decide: $0<p<1$

do: generate x states

select $[p \cdot n]$ of them to test

test requires 2 bits per state

$2 \lceil p \cdot n \rceil$ bits needed to test the states

Def: X discrete variable taking values in $\{x_1, \ldots, x_t\}$

entropy $H(X) = -\sum_{i=1}^{k} \mathbb{P}(X = x_i) \log_2 (\mathbb{P}(X = x_i))$

entropy $= -\mathbb{P}(\text{output } 0) \log(\mathbb{P}(\text{output } 0)) - \mathbb{P}(\text{output } 1) \log(\mathbb{P}(\text{output } 1))$

$= -p \log(p) - (1-p) \log(1-p)$

To select from 1 state, you need this many bits.

in total you need $m \approx 2pn - pn \log p - (1-p) n \log(1-p)$ to select and test.

6.7 Loopholes in Bell tests

To test the idea of hidden variables we introduced some assumptions. Any test that does not satisfy one or more of these assumptions is said to have a **loophole**.

Detector efficiency loophole: When we make a measurement with a real-life device, in practice it doesn't always work — maybe it just fails to notice a photon flying past. Each detector has a parameter η known as its **efficiency**. η is the probability that the measurement succeeds. For testing fundamental physics, it seems reasonable to assume that the successful measurements are a fair sample of what's really going on. But if there's an adversary, they might substitute our detectors for completely perfect one, and then deliberately choose to fake a failure whenever their eavesdropping attempts fail. **This aims to highlight how dependencies on detector efficiency could theoretically be exploited to manipulate experimental outcomes.**

Locality Loophole: if Alice and Bob are physical at distance L from each other, then their random choices of measurement setting, followed by their corresponding carrying out of the measurement, and receipt of the answers, should all be accomplished within a time approximately L/c of each other, where$c$ is the speed of light. If Alice and Bob are not far enough away from each other, then they are said to be within each other's **locality**, and so this is known as the **locality loophole**.

Free-will loophole: The final important assumption that we will mention here involves the availability of true randomness, and emphasises the importance of randomness expansion. It asserts that Alice and Bob must be able to choose their measurement settings randomly. This freedom to make their own choices is glibly referred to as them having "free will", and so this is known as the **free-will loophole**. Resolving the locality loophole puts extremely tight constraints on how quickly choices must be made, to the extent that Alice and Bob cannot make those choices manually — they need to use random number generators. The idea of "free will" here is a shorthand for saying that the choices are made randomly and are not influenced by any factors that could also be influencing the measurement outcomes.

The goal to close these loopholes is to make it extremely unlikely that any hidden variables could influence both the choice of measurement settings and the outcomes simultaneously, thus maintaining the integrity of the experiment.