CHSH / Bell inequality and application to the Ekert 1991 QKD protocol.

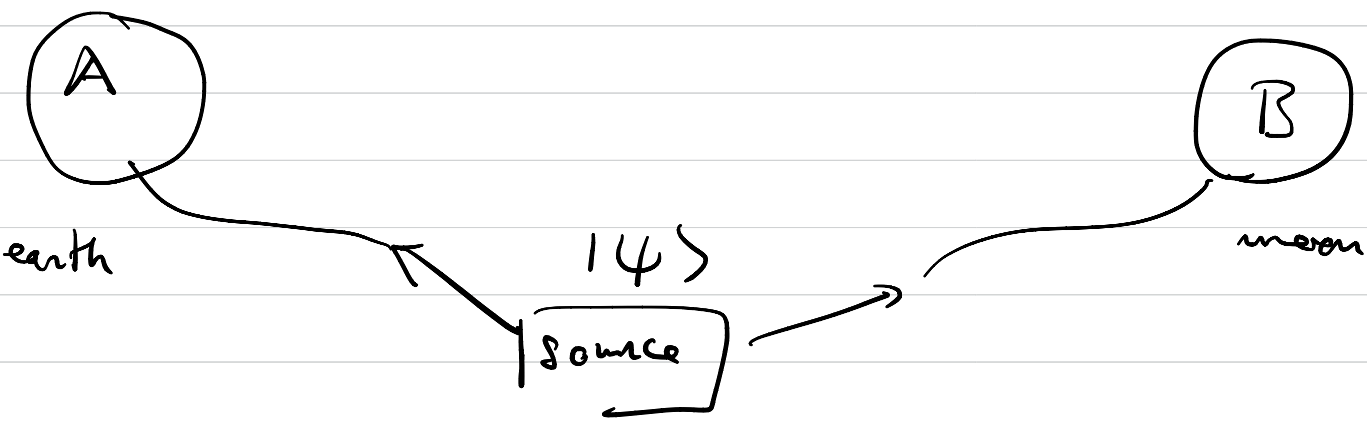
CHSH inequality.

Bell proved an inequality that can be experimentally tested to decide if two parties share "correlations" only explainable by the entangled states of QM or explainable by more mundane correlations coming from a common classical hidden cause (or variable).

Later Clauser, Horne, Shimony and Holt derived an inequality better suited for experiments the CHSH inequality. We briefly review it here. There exist by now a whole zoology of

"Bell inequalities".

Let Alice and Bob be separated by a great distance and assume they cannot communicate. A source distributes a pair of qubits in some arbitrary state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ and they perform local independent measurements



Alice performs measurements in one of two possible orthonormal basis $\{|\alpha\rangle, |\alpha_\perp\rangle\}$ or $\{|\alpha'\rangle, |\alpha'_\perp\rangle\}$ where $\begin{cases} |\alpha\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle \\ |\alpha_\perp\rangle = \sin\alpha\,|0\rangle - \cos\alpha\,|1\rangle \end{cases}$

Similarly Bob performs measurements in one of two possible orthonormal basis $\{|\beta\rangle, |\beta_\perp\rangle\}$ or $\{|\beta'\rangle, |\beta'_\perp\rangle\}$ where
$$\begin{cases} |\beta\rangle = \cos\beta\,|0\rangle + \sin\beta\,|1\rangle \\ |\beta_\perp\rangle = \sin\beta\,|0\rangle - \cos\beta\,|1\rangle \end{cases}$$

This is repeated at each time instant.

Analysis of experiment within classical local hidden variable framework:

Each measurement result of Alice is recorded as a variable $A(\alpha, \lambda) \in \{\pm 1\}$ or $A(\alpha', \lambda) \in \{\pm 1\}$. Each measurement result of Bob is recorded as a variable $B(\beta, \lambda)$ or $B(\beta', \lambda) \in \{\pm 1\}$.

Here λ is a "hidden variable" that characterizes the pair distributed. This can be a deterministic variable or more generally a random variable with distribution $h(\lambda) \geq 0$, $\int d\lambda\, h(\lambda) = 1$.

It is also assumed here that $A(\cdot, \lambda)$ and $B(\cdot, \lambda)$ are <u>local descriptions</u> of the results of Alice and Bob as they depend only on α (or α') and β (or β') and not (α, β) simultaneously. (Of course Alice and Bob should not communicate or there should not be any superluminal hidden communication between them.)

Once all results of measurements are collected Alice and Bob get together and compute the averages:

$$\begin{cases} E(\alpha, \beta) = \int d\lambda\, h(\lambda)\, A(\alpha, \lambda)\, B(\beta, \lambda) \\ E(\alpha, \beta') = \int d\lambda\, h(\lambda)\, A(\alpha, \lambda)\, B(\beta', \lambda) \\ E(\alpha', \beta) = \int d\lambda\, h(\lambda)\, A(\alpha', \lambda)\, B(\beta, \lambda) \\ E(\alpha', \beta') = \int d\lambda\, h(\lambda)\, A(\alpha', \lambda)\, B(\beta', \lambda) \end{cases}$$

and then the <u>correlation coefficient</u>:

$$S = E(\alpha, \beta) - E(\alpha', \beta) + E(\alpha', \beta) + E(\alpha', \beta').$$

<u>Theorem</u> <u>CHSH inequality for local hidden var Theory</u>

$$-2 \leq S \leq +2$$

<u>Proof.</u>

$$S = \int d\lambda \, h(\lambda) \{ A(\alpha, \lambda) B(\beta, \lambda) - A(\alpha, \lambda) B(\beta', \lambda) + A(\alpha', \lambda) B(\beta, \lambda) + A(\alpha', \lambda) B(\beta', \lambda) \}$$

$$= \int d\lambda \, h(\lambda) \{ A(\alpha, \lambda) \left(B(\beta, \lambda) - B(\beta', \lambda) \right) + A(\alpha', \lambda) \left(B(\beta, \lambda) + B(\beta', \lambda) \right) \}$$

Since the A & B functions take values in $\{\pm 1\}$ we have $B(\beta,\lambda) - B(\beta',\lambda) = -2, 0, 2$

and $B(\beta,\lambda) + B(\beta',\lambda) = -2, 0, 2$.

Note also that one of the two <u>must vanish</u>!

Therefore

$$A(\alpha,\lambda)\big(B(\beta,\lambda) - B(\beta',\lambda)\big) + A(\alpha',\lambda)\big(B(\beta,\lambda) + B(\beta',\lambda)\big)$$

$$\in \{-2, 0, 2\}.$$

Since S is an <u>average</u> of these values, it must be in the interval $[-2, +2]$.

$$\Rightarrow \quad -2 \leq S \leq 2$$

$\blacksquare$

In summary if the world is described by some local hidden variable theory we should always find $|S| \leq 2$ in experiments (this is famously <u>not</u> the case for suitable $\alpha, \beta, \alpha', \beta'$).

Analysis of experiment in the framework of QM:

According to QM Alice measures the observable

$$\begin{cases} A = (+1)\,|\alpha\rangle\langle\alpha| + (-1)\,|\alpha_\perp\rangle\langle\alpha_\perp| \\ \text{or} \\ A' = (+1)\,|\alpha'\rangle\langle\alpha'| + (-1)\,|\alpha'_\perp\rangle\langle\alpha'_\perp| \end{cases}$$

and Bob measures

$$\begin{cases} B = (+1)\,|\beta\rangle\langle\beta| + (-1)\,|\beta_\perp\rangle\langle\beta_\perp| \\ \text{or} \\ B' = (+1)\,|\beta'\rangle\langle\beta'| + (-1)\,|\beta'_\perp\rangle\langle\beta'_\perp| \end{cases}$$

If the source distributes a state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$

we have according to the QM:

$$\begin{cases} E(\alpha,\beta) = \langle\psi|\,A\,B\,|\psi\rangle \\ E(\alpha,\beta') = \langle\psi|\,A\,B'\,|\psi\rangle \\ E(\alpha',\beta) = \langle\psi|\,A'B\,|\psi\rangle \\ E(\alpha',\beta') = \langle\psi|\,A'B'\,|\psi\rangle \end{cases}$$

If $|\psi\rangle = |\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right)$

is an EPR-pair a computation shows (exercise!)

$$\begin{cases} E(\alpha,\beta) = \cos\left(2(\alpha-\beta)\right) \; ; \; E(\alpha,\beta') = \cos\left(2(\alpha-\beta')\right) \\ E(\alpha',\beta) = \cos\left(2(\alpha'-\beta)\right) \; ; \; E(\alpha',\beta') = \cos\left(2(\alpha'-\beta')\right) \end{cases}$$

Thus for the correlation coefficient we have

$$S = \cos 2(\alpha-\beta) - \cos 2(\alpha-\beta') + \cos 2(\alpha'-\beta) + \cos 2(\alpha'-\beta').$$

If we maximize this over $\alpha, \alpha', \beta, \beta'$ we find

the max for $\alpha = \frac{\pi}{4}$, $\alpha' = 0$, $\beta = \frac{\pi}{8}$, $\beta' = -\frac{\pi}{8}$.

$$\Rightarrow S = \cos\frac{\pi}{4} - \cos\frac{3\pi}{4} + \cos\frac{\pi}{4} + \cos\frac{\pi}{4} = 4\cdot\cos\frac{\pi}{4} = 2\sqrt{2}.$$

$$\Rightarrow \boxed{S_{max} = 2\sqrt{2} > 2}.$$

Thus the CHSH/Bell inequality is violated. Experimentally this is indeed the case! <u>So QM wins over local hidden var th.</u>

#.

Application: Ekert 1991 QKD protocol.

- Alice & Bob have access to a source of EPR pairs in state $|\psi^+\rangle$ for each time instant.
- Alice measures her qubit by choosing randomly a basis with $\alpha_1 = -\frac{\pi}{4}$, $\alpha_2 = -\frac{\pi}{8}$, $\alpha_3 = 0$ and she records the classical bit $x = +1$ if the outcome is $|\alpha\rangle$ and $x = -1$ if the outcome is $|\alpha_\perp\rangle$.
- Bob measures his qubit by choosing randomly a basis with $\beta_1 = -\frac{\pi}{8}$, $\beta_2 = 0$, $\beta_3 = \frac{\pi}{8}$ and he records the classical bit $y = \pm 1$ if the outcome is $|\beta\rangle$ and $y = -1$ if the outcome is $|\beta_\perp\rangle$.
- Alice & Bob communicate publicly their basis choices. They select the time instants such that their choices were $(\alpha_3\ \beta_3)$, $(\alpha_3\ \beta_1)$, $(\alpha_1\ \beta_1)$, $(\alpha_1\ \beta_3)$ [These are the "CHSH" angles].

and they compute a correlation coefficient

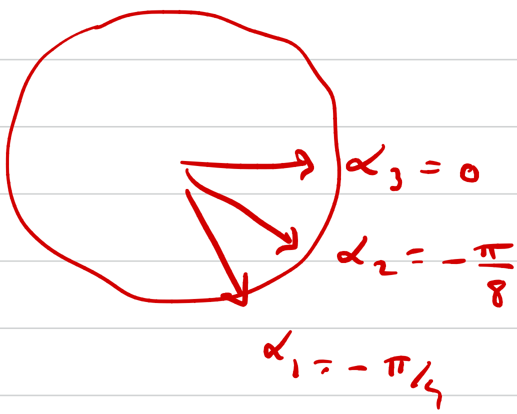
$$S = E(\alpha_3, \beta_3) + E(\alpha_3, \beta_1) - E(\alpha_1, \beta_3) + E(\alpha_1, \beta_1)$$

If there is no eavesdropper they should find

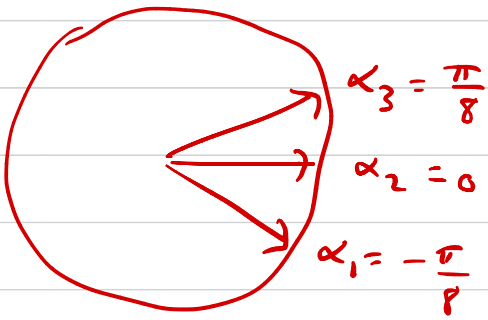
$S = 2\sqrt{2}$ (or with a small amount of noise $2 < S < 2\sqrt{2}$)

- For the secret key (one-time pad) Alice and Bob take the measurement results $x = y$ when their basis choices are identical (α_3, β_2) or (α_2, β_1).

Alice basis choice:



Bob's basis choice:



What is the effect of an Eavesdropper ?

- If Eve captures the two qubits of $|\psi^+\rangle$ and does some measurement and leaves them in a product state then there is no entanglement left and the correlation coefficient will be $|S| < 2$. A & B will notice during their security check.

- If Eve sends an entangled state to A & B (say she copies the EPR pair) and waits until the public communication phase to perform the same measurement than A & B. Some thought shows that she gets the same results than A & B only half of the time,

~~#~~.