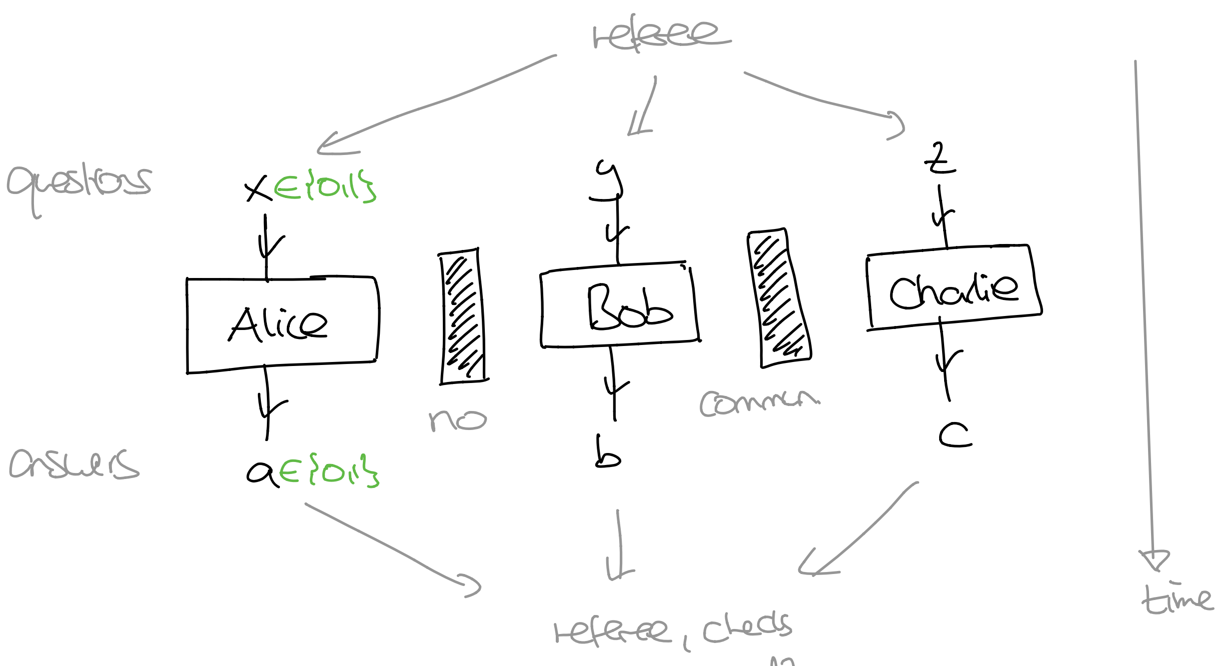
# Quantum correlations

"Strangeness" of QM:
- $|\psi\rangle + |\phi\rangle$ superposition
- $|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$ entanglement
- $[X, Y] \neq 0$ "incompat." measurements

How to study nonclassical correlations? Nonlocal games!
(Thought) experiments




GHZ game (Mermin '90):

| x | y | z | $a \oplus b \oplus c$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 |

$\Big\}\ x \vee y \vee z$

Physics 230:
find ! also,
CHSH game

not all possible bitstrings are questions!

theory assigns pre-existing value to all questions

Classical Strategies: "local", "realistic" physical theories

↳ $a = a(x)$, $b = b(y)$, $c = c(z)$

Before game begins: Players can coordinate strategy!

PHYSICS 230

e.g., flip coin and use it to influence their action

↳ should think of functions $a, b, c$ as random functions (or introduce hidden variables)

Suppose $a(x), b(y), c(z)$ is a perfect strategy:

Then:

$$
\begin{aligned}
1 = 0 \oplus 1 \oplus 1 \oplus 1 = \big(&a(0) \oplus b(0) \oplus c(0)\big) \\
\oplus \big(&a(1) \oplus b(1) \oplus c(0)\big) \\
\oplus \big(&a(1) \oplus b(0) \oplus c(1)\big) \\
\oplus \big(&a(0) \oplus b(1) \oplus c(1)\big) = 0 \quad ↯
\end{aligned}
$$

$a(x) \oplus a(x) = 0$

⇒ Always get one answer wrong!

⇒ $\boxed{P_{win,cl} = \frac{3}{4}}$ if questions selected uniformly at random

just always output $a(x) = b(y) = c(z) = 1$.

## Quantum strategies:

- players share $|\psi_{ABC}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$
- Alice measures $A_x$. outcome $(-1)^a \to$ answer $a$.

  Bob ... $B_y$. .. $(-1)^b \to$ .. $b$

  Charlie .. $C_z$ .. $(-1)^c \to$ .. $c$

CONVENTION: eigenvalues $\{\pm 1\}$ !

Then: $\boxed{A_x \otimes B_y \otimes C_z}$ has eigenvalues $(-1)^{a\oplus b\oplus c}$

eigenvectors $|(-1)^a\rangle|(-1)^b\rangle|(-1)^c\rangle$

E.g.: $Z = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ $Z|0\rangle = +|0\rangle \longrightarrow a=0$

$|1\rangle = -|1\rangle \longrightarrow a=1$

"$Z|a\rangle = (-1)^a |a\rangle$"

$Z\otimes Z\otimes Z\,|abc\rangle = Z|a\rangle \otimes Z|b\rangle \otimes Z|c\rangle$

$= (-1)^a|a\rangle \otimes (-1)^b|b\rangle \otimes (-1)^c|c\rangle = (-1)^{a\oplus b\oplus c}\,|abc\rangle$

A perfect q. strategy satisfies:

$$\left.\begin{aligned}
A_0\otimes B_0\otimes C_0\,|\psi_{ABC}\rangle &= +|\psi_{ABC}\rangle\\
A_1\otimes B_1\otimes C_0\,|\psi_{ABC}\rangle &= -|\psi_{ABC}\rangle\\
A_1\otimes B_0\otimes C_1\,|\psi_{ABC}\rangle &= -|\psi_{ABC}\rangle\\
A_0\otimes B_1\otimes C_1\,|\psi_{ABC}\rangle &= -|\psi_{ABC}\rangle
\end{aligned}\right\} (*)$$

(Ex: $p_{win,q} = \frac{1}{2} + \frac{1}{8}\langle\psi|(A_0\otimes B_0\otimes C_0 - \ldots - \ldots - \ldots)|\psi\rangle$)

Can we achieve this? YES!

- $|\Gamma_{ABC}\rangle = \frac{1}{2}(|000\rangle - |110\rangle - |101\rangle - |011\rangle)$
- $A_0 = B_0 = C_0 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $A_1 = B_1 = C_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Verify (*):

$$Z \otimes Z \otimes Z \, |\Gamma\rangle = |\Gamma\rangle$$

$$X \otimes X \otimes Z \, |\Gamma\rangle = \frac{1}{2}(|110\rangle - |000\rangle + |011\rangle + |101\rangle)$$

$$= -|\Gamma\rangle$$

etc. ✓

(Ex: Relate this to Physics 220 final!)

Summary: QM allows for stronger "nonlocal" cor.

In precise quantitative sense:

$$\boxed{P_{win,cl} = \frac{3}{4} < P_{win,q} = 1}$$

... this is nice – but is it useful?

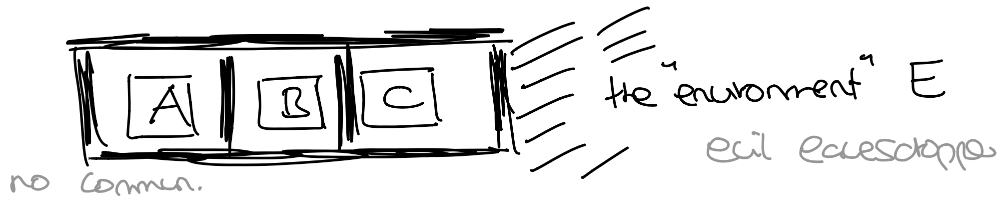
A curious observation: In strategy above,

$a, b \in \{0,1\}$ random bits (and $c$ s.t. $a \oplus b \oplus c = \dots$)

E.g. $x=y=z=0$: Alice, Bob, Charlie each measure $Z$

↳ $abc \in \{000, 110, 101, 011\}$ w. prob. $\frac{1}{4}$.!

Random bits are also private!




$$|\Psi_{ABCE}\rangle = |\Gamma_{ABC}\rangle \otimes |\Psi_E\rangle$$ ~> Problem set!

random bits uncorrelated from E

only way to $\boxed{\text{extend}}$ $|\Gamma\rangle_{ABC}$ to wave fn on ABCE

But cannot trust A, B, C to play above strategy....

... can only pose questions & observe answers!

What if the optimal winning strategy were unique?

Proposal (Colbeck '09):

① Test A, B, C with randomly selected questions (many times).

② If pass tests: use answers as private random bits!

↯ Memory ↯ Robustness ...

But: Idea is sound !!!

→ device-independent quantum cryptography ...

randomness expansion

QKD

Control of adv. q. systems

~> Course project?

Rigidity of GHZ game (also: self-testing property):

Optimal q. strategy is essentially unique!

Warmup: In 3-qubit strategy, $|\Gamma\rangle$ is determined by measurement ops and $\otimes$:

$$Z\otimes Z\otimes Z|\Gamma\rangle = |\Gamma\rangle$$

$$\Longrightarrow \quad |\Gamma\rangle = \alpha|000\rangle + \beta|110\rangle + \gamma|101\rangle + \delta|011\rangle$$

XXZ etc. −XXZ

Consider general optimal strategy:

- $|\psi_{ABC}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$
- $\{A_x\}, \{B_y\}, \{C_z\}$ s.th. $\underbrace{A_x^2 = I,\ B_y^2 = I,\ C_z^2 = 1}_{\text{eigenvalues } \pm 1}$

Claim: $\boxed{\text{"}\{A_0, A_1\} = 0,\quad \{B_0, B_1\} = 0,\quad \{C_0, C_1\} = 0\text{"}}$

Why useful?

Finding a qubit: Given:

$$A_0^2 = A_1^2 = I, \quad \{A_0, A_1\} = 0 \quad \text{on } \mathcal{H}_A$$

Set $A_2 := -\frac{i}{2}[A_0, A_1] = -i A_0 A_1 = i A_1 A_0$. Then:

$$[A_1, A_2] = 2i A_0, \quad [A_2, A_0] = 2i A_1$$

$\rightsquigarrow$ $\mathcal{H}_A$ representation of $su(2)$

$$iZ \mapsto iA_0$$
$$su(2) \ni iX \mapsto iA_1 \in B(\mathcal{H}_A)$$
$$iY \mapsto iA_2$$

$$\mathcal{H}_A = V_{j_1} \oplus V_{j_2} \oplus V_{j_3} \oplus \dots$$

Which irreducible representations appear? Total spin:

$$\hat{J}^2 = \frac{1}{4}(A_0^2 + A_1^2 + A_2^2) = \frac{1}{4}(I + I + I) = \frac{3}{4} I$$

$j(j+1)$ Scalar

$\Longrightarrow$ Only spin $j = \frac{1}{2}$ !

$$\mathcal{H}_A \cong \underbrace{\mathbb{C}^2 \oplus \dots \oplus \mathbb{C}^2}_{m_A \text{ times}} \cong \mathbb{C}^2 \otimes \mathbb{C}^{m_A}$$

$$A_{0,1} \cong \begin{pmatrix} Z\,X & & \\ & \boxed{Z\,X} & \\ & & \ddots \end{pmatrix} \cong Z\,X \otimes I_{m_A}$$

Likewise for Bob, Charlie!

$$\Longrightarrow \mathcal{H}_A \otimes \mathcal{H}_A \otimes \mathcal{H}_C \cong (\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2) \otimes (\mathbb{C}^{m_A} \otimes \mathbb{C}^{m_B} \otimes \mathbb{C}^{m_C})$$

$$A_0 \otimes B_0 \otimes C_0 \cong (Z \otimes Z \otimes Z) \otimes I$$

etc.

WARMUP $\Longrightarrow$ $|\psi_{ABC}\rangle \cong |\Gamma\rangle \otimes |\gamma\rangle$ arbitrary

Still need to prove the claim!

**Anticommutation from correlations:** ⊛ $\Leftarrow$

$$A_0|\psi\rangle = B_0C_0|\psi\rangle = -B_1C_1|\psi\rangle$$
$$A_1|\psi\rangle = -B_1C_0|\psi\rangle = -B_0C_1|\psi\rangle$$

NOTATION: $A_0 = A_0 \otimes I_B \otimes I_C$ etc. !

$$\Rightarrow \quad A_0|\psi\rangle = \frac{1}{2}(B_0C_0 - B_1C_1)|\psi\rangle$$
$$A_1|\psi\rangle = -\frac{1}{2}(B_1C_0 + B_0C_1)|\psi\rangle$$

$$\Rightarrow \quad A_0A_1|\psi\rangle = -\frac{1}{4}(B_1B_0 - B_0B_1 + C_1C_0 - C_0C_1)$$
$$A_1A_0|\psi\rangle = -\frac{1}{4}(B_0B_1 - B_1B_0 + C_0C_1 - C_1C_0)$$

i.e. $$\boxed{\{A_0, A_1\}|\psi\rangle = 0}$$

This almost implies the claim – but have to be a bit more precise: Can always write

$$|\psi_{ABC}\rangle = \sum_i \underset{>0}{s_i}\, \underset{\text{ON}}{|e_i\rangle_A} \otimes \underset{\text{ON}}{|f_i\rangle_{BC}}$$

Schmidt decomposition
$\to$ problem set

Let $\tilde{\mathcal{H}}_A = \text{span}\,\{|e_i\rangle\}$. Then:

- $|\psi_{ABC}\rangle \in \tilde{\mathcal{H}}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$

- $A_x = \left(\begin{array}{c|c} \tilde{A}_x & \\ \hline & * \end{array}\right)$ w.r.t. $\mathcal{H}_A = \tilde{\mathcal{H}}_A \oplus \tilde{\mathcal{H}}_A^\perp$

- $\{\tilde{A}_x, \tilde{A}_y\} = 0$

Likewise: $B, C \longrightarrow$ Claim. $\square$

---

<u>Theorem</u> (GHZ rigidity): Let $\{A_x\}, \{B_y\}, \{C_z\}, |\psi_{ABC}\rangle$ perfect q. strategy. Then: $\exists$ isometries

$$V_A : \mathbb{C}^2 \otimes \mathbb{C}^{m_A} \longrightarrow \mathcal{H}_A$$
$$V_B : \mathbb{C}^2 \otimes \mathbb{C}^{m_B} \longrightarrow \mathcal{H}_B$$
$$V_C : \mathbb{C}^2 \otimes \mathbb{C}^{m_C} \longrightarrow \mathcal{H}_C$$

S.th.

1. $|\psi_{ABC}\rangle = (V_A \otimes V_B \otimes V_C)(|\Gamma\rangle \otimes |\gamma\rangle_{m_A m_B m_C})$

2. $V_A^\dagger A_x V_A = \begin{cases} Z \otimes I_{m_A} & (x=0) \\ X \otimes I_{m_A} & (x=1) \end{cases}$

   etc.

$\hookrightarrow$ $\boxed{\text{Pset}}$ ?