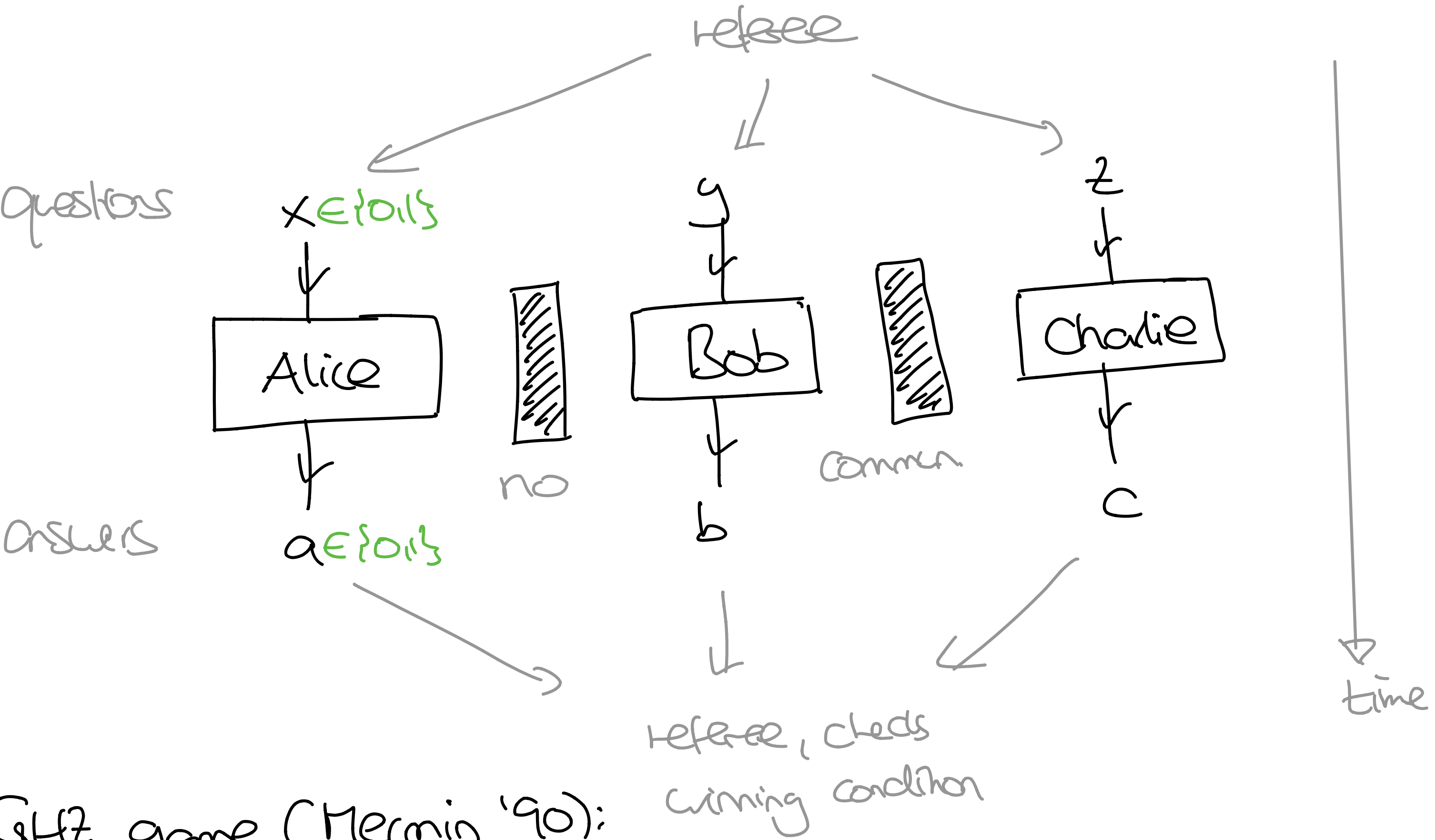
Quantum correlations

How to study nonclassical correlations? Nonlocal games!

↳ Bell inequalities

Thought experiments w/ a CS flavor.



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

$x \vee y \vee z$

not all possible bitstrings are questions!

theory assigns pre-existing value to all questions

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

$\to$ $a = a(x)$, $b = b(y)$, $c = c(z)$

Before game begins: Players can coordinate strategy!
e.g., flip coin and use it to influence their action
$\to$ should think of functions a, b, c as random functions
or introduce hidden variables $\to$ $\boxed{\text{PSET}}$

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

Then:

$$1 = 0 \oplus 1 \oplus 1 \oplus 1 = \big(a(0) \oplus b(0) \oplus c(0)\big) \oplus \big(a(1) \oplus b(1) \oplus c(0)\big) \oplus \big(a(1) \oplus b(0) \oplus c(1)\big) \oplus \big(a(0) \oplus b(1) \oplus c(1)\big) = 0 \quad \lightning$$

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

$\Rightarrow$ Always get one answer wrong!

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

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

BELL INEQUALITY

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.: $Z = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ $\quad Z|0\rangle = +|0\rangle \to a=0$
$\quad |1\rangle = -|1\rangle \to a=1$

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

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

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!

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

Verify (*):

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

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

etc. ✓

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

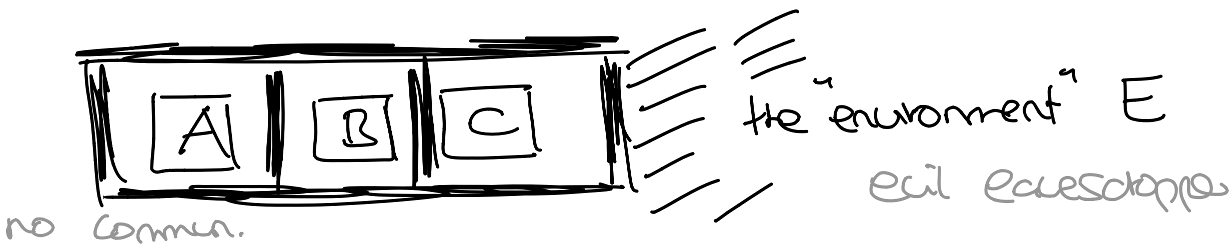
... this is nice – but is it useful?

A curious observation: In strategy above, $a, b \in \{0,1\}$ random bits (and c s.t. $a \oplus b \oplus c = \ldots$)

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!



$$|\psi_{ABCE}\rangle = |\Gamma_{ABC}\rangle \otimes |\psi_E\rangle$$ → NEXT WEEK

$|\Gamma_{ABC}\rangle$: random bits uncorrelated from E

$\otimes$: only way to extend $|\Gamma_{ABC}\rangle$ 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

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 $\otimes$:

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

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

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

Why useful?

Finding a qubit: Given:

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

* If $A_0|\phi\rangle = \pm|\phi\rangle$:

$$A_0(A_1|\phi\rangle) = -A_1A_0|\phi\rangle = \mp A_1|\phi\rangle$$

↳ unitary A_1 interchanges ± 1 eigenspaces of A_0

(just like X & Z) $\Downarrow$

* Eigenspaces have same dimension m_A!

& $|e_{0j}\rangle$ basis of $+1$-eigenspace

$\Rightarrow |e_{1j}\rangle := A_1|e_{0j}\rangle$ basis of -1-eigenspace

* Thus can identify

$$U_A : \mathcal{H}_A \longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^{m_A}$$

$$|e_{ij}\rangle \longmapsto |i\rangle \otimes |j\rangle$$

s.th. $U_A A_0 U_A^\dagger = Z \otimes I$ ← e.g.

$U_A A_1 U_A^\dagger = X \otimes I$

$$\boxed{\begin{aligned} &U_A A_0 U_A^\dagger |i\rangle \otimes |j\rangle \\ &= U_A A_0 |e_{ij}\rangle \\ &= (-1)^i U_A |e_{ij}\rangle \\ &= (-1)^i |i\rangle \otimes |j\rangle \\ &= Z|i\rangle \otimes |j\rangle \end{aligned}}$$

Likewise for Bob, Charlie!

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

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

etc.

WARMUP $\Rightarrow$ $|\psi_{ABC}\rangle \cong |\Gamma\rangle \otimes |\gamma\rangle$ 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. !

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

$B_y^2 = I,\ C_z^2 = I$

$B_yC_z = C_zB_y$

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

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

Almost the claim! How to conclude?

SCHMIDT DECOMPOSITION

will learn this next week...

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

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

- $|\psi_{ABC}\rangle \in \tilde{\mathcal{H}}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$
- $\{\tilde{A}_x, \tilde{A}_y\} = 0$
- $A_x = \begin{pmatrix} \tilde{A}_x & \\ & * \end{pmatrix}$ w.r.t. $\mathcal{H}_A = \tilde{\mathcal{H}}_A \oplus \tilde{\mathcal{H}}_A^{\perp}$

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